DİJİTAL DELİL KILAVUZU SÜRÜM 3.0

Funded
by the European Union
and the Council of Europe

EUROPEAN UNION

COUNCIL OF EUROPE
CONSEIL DE L'EUROPE

Implemented
by the Council of Europe

DİJİTAL DELİL KILAVUZU

POLİS MEMURLARI, SAVCILAR ve HÂKİMLER İÇİN TEMEL KILAVUZ

SÜRÜM 3.0

Bilişim Suçları Birimi
İnsan Hakları ve Hukukun Üstünlüğü Genel Müdürlüğü
Strazburg, Fransa
4 Nisan 2022

Bu kılavuzun hazırlanmasında aşağıdaki projelerden elde edilen sonuçlardan yararlanılmıştır:
CyberCrime@IPA
GLACY - Global Action on Cybercrime
Cybercrime@EAP
Cybercrime@Octopus
CyberEast
iPROCEEDS-2

Bu Kılavuz, "Türkiye'de Ceza Adalet Sisteminin Güçlendirilmesi ve Avrupa İnsan Hakları Sözleşmesi İhlallerinin Önlenmesi için Yargı Mensuplarının Kapasitesinin Artırılması" Avrupa Birliği – Avrupa Konseyi Ortak Projesi kapsamında 3100 adet olmak üzere basılmıştır.

Bilgilendirme

Bu kılavuzun ilk baskısı Güneydoğu Avrupa'da siber suçlarla mücadelede işbirliğine yönelik Avrupa Konseyi ve Avrupa Birliği ortak projesi olan CyberCrime@IPA Projesi kapsamında 2013 Mart'ında yayımlanmıştır. Belge üzerinde gerçekleşen çalışmaların eşgüdümü Nigel Jones (İngiltere) tarafından sağlanmıştır. Bu yayın, CyberCrime@IPA Projesi'nin uygulandığı ülke ve alan siber suç uzmanları ile Afrika, Asya ve Avrupa bölgelerinden diğer uluslararası uzmanların değerli katkılarıyla hazırlanmıştır.

GLACY bünyesinde Viktor Völzow (Almanya) tarafından (Sürüm 2.0) ve Avrupa Birliği ile Avrupa Konseyi ortak projesi olan CyberEast (Sürüm 2.1) kapsamındaki güncellemelere Kılavuzun 2.0 ve 2.1'nci sürümlerinde yer verilmiştir. Sürüm 3.0, Avrupa Birliği ve Avrupa Konseyi ortak projesi iPROCEEDS-2 kapsamında hazırlanmış olup Budapeşte Bilişim Suçları Sözleşmesi 2. Ek Protokolü gereklerini de dikkate alan çeşitli güncellemeler içermektedir.

Düzeltmeler

Sürüm	Tarih	Fonlayan Proje	Hazırlayanlar
1,0	Mart 2013	CyberCrime@IPA	Esther George (Birleşik Krallık) Nigel Jones (Birleşik Krallık) Fredesvinda Insa Mérida (İspanya) Uwe Rasmussen (Danimarka) Victor Völzow (Almanya)
2,0	Aralık 2014	GLACY	Victor Völzow (Almanya)
2,1	Mart 2020	CyberEast	Victor Völzow (Almanya)
3,0	Nisan 2022	iPROCEEDS-2	Mark Cameron (Birleşik Krallık) Jan Kerkhofs (Belçika) Victor Völzow (Almanya)

İRTİBAT

Bilişim Suçları Birimi

İnsan Hakları ve Hukukun Üstünlüğü Genel Müdürlüğü

Avrupa Konseyi, F-67075 Strazburg Cedex (Fransa)

Telefon +33 3 9021 4506

Faks +33 3 9021 5650

Eposta alexander.seger@coe.int

İçindekiler

1 Giriş

Dijital Delil Kılavuzu, Katılım Öncesi Destek (IPA) kapsamında siber suçlarla mücadelede işbirliği amacıyla ilk olarak Avrupa Birliği ve Avrupa Konseyi bölgesel ortak projesi olan Cybercrime@IPA kapsamında hazırlanmıştır.

Cybercrime@IPA projesi ve Avrupa Konseyi'nin Octopus (Ahtapot) Konferansları sürecinde taraflar, dijital delillerin kullanımında yetkili bir makamın rehberliği ve iyi uygulamalara duyulan ihtiyaca işaret etmişlerdir. Dijital Delil Kılavuzu da bu ihtiyaca cevaben hazırlanmıştır.

Dijital Delil Kılavuzu bir kavram olarak öncelikle Cybercrime@IPA projesi kapsamında gerçekleştirilen bir dizi çalıştayda ve Octopus Konferanslarında ortaya çıkmıştır.

Kılavuzun ilk baskısı (Sürüm 1.0) 18 Mart 2013 tarihinde yayınlanarak çeşitli ülkelerin kolluk ve adli birimleri açısından yaygın bir kaynak haline gelmiş, aynı ülkelerin kendi diline de tercüme edilmiştir.

Sürüm 1.0 üzerinde yapılan değişiklikler üzerine Kılavuzun 2. Sürümü (Sürüm 2.0) okuyucu geribildirimleri ışığında yeniden düzenlenerek 2014 senesi Aralık ayında yayınlanmıştır. 2. Baskıda adli bilişim ve dijital delillerin analizine ilişkin tamamen yeni bir bölüme de yer verilmiştir.

2020 Mart'ında yayınlanan Kılavuzun 3. Baskısındaysa tüm bölümler yeniden gözden geçirilerek güncellenmiş, temassız kartlar, otomotiv sistemleri ve IoT (Nesnelerin İnterneti) konularında yeni bölümler de ilave edilmiştir.

4. Baskı (Sürüm 3.0) Nisan 2022'de yayınlanmış olup tüm bölümler güncellenerek Budapeşte Bilişim Suçları Sözleşmesi 2. Ek Protokolü'nün kabulünü müteakip gerekli ilaveler yapılmıştır.

1.1 Kılavuzun Hedefi

Bu Kılavuzun amacı dijital delillerin tespit ve ileriki süreçlerde mahkemede geçerliliklerine halel getirmeksizin bozulmadan kullanımına ilişkin ceza yargı birimlerine destek ve rehberlik sağlamaktır. Kılavuz adım adım bir yönergeler sistematiği içerisinde bir kullanım kılavuzu olarak tasarlanmamış olmakla birlikte dijital delillerle çalışma sırasında karşılaşılan sorunlara bir genel bakış ve buna yönelik çeşitli tavsiyelere de yer verilmiştir. Okuyucuların da kendi ulusal belgelerinde de benzer bilgi ve tavsiyelerin bulunup bulunmadığını kontrol etmeleri tavsiye edilir. Avrupa Konseyi'nce bu kılavuzda yer alan bilgileri tamamlayıcı olarak başkaca belgeler de hazırlanarak kullanıma sunulmaktadır (bkz. Bölüm 1.4).

Kılavuz ve içeriğinde yer alan bilgiler 31 Aralık 2023 tarihine kadar geçerlidir. Kılavuz, teknoloji alanında kaydedilen ilerlemeler dikkate alınarak ve koşullar elverdiği ölçüde bu tarihten önce gerekli güncellemeler yapılmak suretiyle teknolojide ve ilgili usul ve uygulamalardaki değişiklikleri yansıtır mahiyette olması sağlanacaktır Belirtilen geçerlilik tarihinden önce Kılavuzdan faydalanmak isteyen şahıs veya kuruluşların en son sürüm için Avrupa Konseyi ile irtibata geçmesi gerekmektedir.

1.2 Kılavuzun Hedef Kitlesi

Bu Kılavuz, dijital delil kullanımına ilişkin kendi protokol ve kurallar çerçevesini hazırlamakta olan ülkelerin kullanımına yönelik olarak hazırlanmıştır. Mevcut kılavuzlar büyük ölçüde kolluk birimleri için hazırlanmış olmakla birlikte, bu Kılavuz hâkim ve savcılar ile diğer yargı birimleri kadar dijital delil hakkında bilgi sahibi olması gereken özel araştırmacılar ve savunma avukatları gibi tarafların da yer aldığı daha geniş bir kitle düşünülerek tasarlanmıştır. Temel seviyede bir belge olmakla birlikte Kılavuzun kimi bölümlerinde daha fazla ayrıntıya girilerek uzmanlar açısından da ilgi çekici olabilecek uygulamaya dönük kimi tavsiyelere de yer verilmiştir.

1.3 Kılavuzun Kullanımı

Bu Kılavuz, ülkelerin kendi ulusal mevzuat, usul ve uygulamalarına göre düzenleyebilecekleri bir tip belge olarak değerlendirilmelidir. Kılavuzda açıklanan temel prensipler dijital delillerle çalışılması hususunda genel kabul gören iyi uygulamalarla uyumludur.

Okuyucuların Kılavuz içeriğinin dijital deliller ve dijital delillerin kabul edilebilirliğine ilişkin kendi ulusal mevzuatlarına uygun olmasını sağlamalıdır. İlk başvuru kaynağı her zaman için ulusal mevzuattır. Kılavuzda yer alan tavsiyelerde ulusal mevzuata herhangi bir karşıtlık hedeflenmemiş olup, esasen Kılavuz ulusal yasa, usul ve kurallara tabidir.

Metin, olası delillerin ilk olarak tespit edilmesinden başlayarak soruşturma safahatına uygun olarak bu tür delillerin aranarak el konulmasından internetten delil çekilmesine ve delillerin incelenmesinden, hazırlanarak bildirimine ve mahkemeye sunulmasına kadarki süreçler zamandizinsel bölümlere ayrılarak, devamında kolluk, hâkim ve savcılar ile özel araştırmacı, avukat ve diğer adli birimlerin işlevlerine göre 'ilgisine göre' özel bölümlere de yer verilmiştir.

Soruşturmacılara yardımcı olmak adına Kılavuza ek olarak faydalı araçlara da yer verilmiştir. Bunlar:

- **Ek A -** Arama ve Elkoyma Akış Şeması
- **Ek B -** Canlı Veri Adli İncelemesi Akış Şeması
- **Ek C -** Özel Sektör Hazırlığı Akış Şeması
- **Ek D -** Özel Sektör Arama ve Elkoyma Akış Şeması
- **Ek E -** Dijital Delil Toplama Akış Şeması
- **Ek F -** Delil zinciri kaydı
- **Ek G -** Delil Muhafaza Anketi
- **Ek H -** Delil etiket şablonları
- **Ek I -** Görüntü Alma Kaydı

Bu Ekler de Kılavuzun kendisi gibi birer şablon ya da tip belge olarak değerlendirilerek ihtiyaca göre gerekli uyarlamalar yapılmak suretiyle kullanılabileceklerdir.

Kılavuz içerisinde bulundukları bölümlerin içerik açısından önem veya zorluk derecesini belirtir çeşitli simgeler kullanılmıştır.

Bu simge ilgili bölümde bilgiye yer verilmiş olduğunu belirtir.		Bu simge ilgili bölümde önemli bilgiye yer verilmiş olduğunu belirtir.		Bu simge üst seviyede teknik bilgiye işaret eder.	
Bu simge ilgili bölümde temel seviyede bilgi yer aldığını belirtir.		Bu simge ilgili bölümde ileri düzey bilgiye yer verilmiş olduğunu belirtir.		Bu simge ilgili bölümde uzmanlık düzeyinde bilgiye yer verilmiş olduğunu belirtir.	

Hareket tarzı konusunda emin olamamaları durumunda okuyucuların Bölüm 1.7 - Temel İlkelere başvurması önerilir. Karşı karşıya bulunulan durumun bu Kılavuz veya başkaca eğitimlerin kapsamını aşması durumunda okuyucular uzman desteği almalıdır.

1.4 İlave Araçlar

Dijital Delil Kılavuzunu tamamlayıcı bir dizi kaynak ve araç bulunmaktadır. Bunlara örnek olarak;

- **Budapeşte Bilişim Suçları Sözleşmesi**[1] - Sözleşme taraflarının dijital delillerin muhafazası ve etkin uluslararası işbirliğinin sağlanmasını kolluk eliyle gerçekleştirmesi beklenmektedir. Md. 14'e göre, bu yetki *suça bakılmaksızın* tüm dijital deliller için geçerlidir Bu yetkiler:
  - Trafik verilerinin kısmi paylaşımı (Md. 17 ve Md. 30) da dahil olmak üzere, verinin yurtiçi (Md. 16) ve uluslararası (Md. 29) seviyede uzun süreli olarak muhafazası;
  - Depolanmış bilgisayar verilerinin arama ve el konma süreçleri (Md. 19);
  - Trafik verilerinin, ulusal (Md. 20 ve Md. 21) ve uluslararası (Md. 33 ve Md. 34) seviyeler de dahil olmak üzere gerçek zamanlı olarak toplanması ile içerik verilerinin engellenmesi;
  - Veriye hızlı erişim maksadıyla yabancı yargı daireleriyle ivedi karşılıklı destek (Md. 31);
  - Sınır aşan verilere karşılıklı destek olmaksızın erişim (Md. 32).

http://www.coe.int/en/web/cybercrime/the-budapest-convention

[1] Avrupa Konseyi Bilişim Suçları Sözleşmesi (CETS No. 185)

- **Budapeşte Bilişim Suçları Sözleşmesi 2. Ek Protokolü'nde** ek hükümlere ilave olarak işbirliğinin ilerletilmesi, mevcut koşulların iyileştirilmesine yönelik önlemler ile kimi güvence mekanizmaları ve nihai hükümlere de yer verilmiştir. Dijital delil bağlamında doğrudan işbirliğinin ilerletilmesine ilişkin olarak aşağıdaki usuller özellikle çeşitli sağlayıcılar ve diğer Taraflar bünyesinde yer alan teşekküllerin ilgi alanına girmektedir.
  - Alan adı kayıt bilgisi talebi (Md. 6)
  - Üyelik bilgilerinin açıklanması (Md. 7)
  - Kullanıcı bilgisi ve trafik verilerinin üretilme süreçlerinin hızlandırılmasına yönelik olarak diğer Tarafların talimatlarının yerine getirilmesi
  - Saklanan bilgisayar verilerinin acil durumlarda ivedi paylaşımı
  - Acil durumlarda karşılıklı destek (Md. 10)
  - Video konferans (Md. 11) ve Ortak Soruşturma Ekipleri ile ortak soruşturma süreçleri (Md. 12)

  https://www.coe.int/en/web/conventions/new-treaties
- Avrupa Konseyi'nin kapasite geliştirme programları kapsamında hazırlanan **Kılavuzlar**:
  - Dijital Delillerin Toplanması, analizi ve Sunumuna Yönelik Standart Uygulama Usulleri;
  - Adli bilişim laboratuvarının yönetimine ve usullerine ilişkin temel kılavuz;
  - Kripto Para Müsadere Kılavuzu;
  - Bilişim Suçları Soruşturmalarına İlk Müdahale Ekipleri için Kılavuz;
  - ve eklerine farklı dillerde aşağıdaki adresten erişebilirsiniz:

  https://www.coe.int/en/web/octopus/training
- Avrupa Konseyi tarafından kapasite geliştirme programları kapsamında geliştirilen aşağıdaki **Eğitim Kursları**:
  - Bilişim Suçları, Dijital Delil ve Çevrimiçi Suç Gelirleri Giriş Seviyesi Eğitim Modülü;
  - Yargıya Giriş Eğitimi (Hâkim ve Savcılara Yönelik Bilişim Suçları/Dijital Deliller Konularına Giriş);
  - İleri Seviye Yargı Eğitimi (Hâkim ve Savcılara Yönelik Bilişim Suçları/Dijital Deliller Konularında İleri Seviye Bilgi);
  - İlk Müdahale Ekipleri için Eğitim Paketi (İlk Müdahalecilere Yönelik Olarak Suç Mahallerinde Dijital Delil Sevk ve İdare Eğitimi);
  - Çevrimiçi Suç Gelirleri Arama, Zabıt ve El Koyma Temel Eğitimi (Hâkim ve Savcılara Yönelik Eğitim);
  - Çevrimiçi Suç Gelirleri Arama, Zabıt ve El Koyma Temel Eğitimi (Kendi Kendine Eğitim El Kitabı);

  https://www.coe.int/en/web/octopus/training

- Bilgilendirici **rapor ve çalışmalar**:
  - GLACY ve Cybercrime@EAP projeleri kapsamında hazırlanan yargı ve kolluk eğitim stratejileri;
  - Bilişim Suçları ve Siber Güvenlik Stratejileri, (Yay. 2019);
  - CyberCrime@IPA Projesi Kapsamında Hazırlanan Uzman Siber Suç Birimleri İyi Uygulamalar Çalışması CyberCrime@IPA Projesi Kapsamında Hazırlanan Hukuk Korumasına Gereksinim çalışması (Budapeşte Sözleşmesi, Md. 15);
  - Bilişim Suçlarına ilişkin mevzuat, ulusal yargı eğitim imkan ve kabiliyetleri, ceza yargı istatistiklerine yönelik siber suçlar ve dijital delil, vs. kılavular gibi diğer bir çok ilginç başlıktaki rapor ve çalışmalara da aşağıdaki adresten ulaşabilirsiniz:

https://www.coe.int/en/web/cybercrime/all-reports

- 2008 Yılında Avrupa Konseyi Octopus Konferansı'nda Benimsenen Kolluk Kuvvetleri/İnternet Servis Sağlayıcı İşbirliği Kılavuzları;

https://www.coe.int/en/web/cybercrime/lea-/-isp-cooperation

- **Octopus Topluluğu**, bilişim suçlarına ilişkin mevzuat ve politikalar ile kamu-özel işbirliği alanında ülkeye özel bilgi, yukarıda anılan eğitim materyalleri ve Karşılıklı Hukuki Yardıma yönelik şablonlar ile veri muhafaza talepleri gibi ülkeye özel bilgi içeren bir kaynak kütüphanesi olarak işlerlik göstermektedir.

https://www.coe.int/en/web/octopus/home

- İki haftada bir yayınlanan **Cybercrime Digest** (Bilişim Suçları Mecmuası) ilee 3 ayda bir yayınlanan **Cybercrime@CoE** (Avrupa Konseyi Bilişim Suçları) raporları.

https://www.coe.int/en/web/cybercrime/cyber-digests-and-updates

Tüm bu standart ve araçlar Avrupa Konseyi Bilişim Suçları Birimi'nin internet sitesinde erişime açıktır.

https://www.coe.int/en/web/cybercrime/home

1.5 Dijital Delil Nedir?

Deliller, tüm ceza soruşturmalarında, sanığın suçlu veya masum olup olmadığına veya hukuk davalarında davanın esasına yönelik karar verilebilmesine dayanak teşkil eder. Geleneksel ve tarihsel anlamıyla ele alındığında deliller, evrak, fotoğraf gibi somut veya tanık beyanı gibi sözlü olabilmektedir.

Dijital deliller, bilgisayar ve çevre birim donatıları, bilgisayar ağları, mobil telefon, dijital kamera ve veri depolama aygıtları dahil olmak üzere taşınabilir diğer cihazlar ve internetten elde edilir. Burada içerilen bilgi, kendi başına fiziksel bir formata sahip değildir.

Ancak, hukuki süreçlerde dijital deliller ortaya koyan tarafların bu dijital delillerin suçun işlendiği andaki koşul ve somut bilgileri yansıtır mahiyette olduğunu göstermeleri gerekliliğinden hareketle, dijital delillerle geleneksel deliller arasında pek çok açılardan benzerlikler bulunduğu söylenebilir. Diğer bir ifadeyle, dijital delillerde de

herhangi bir değişiklik, silme, ekleme veya başkaca müdahalelerde bulunulmamış olduğunun gösterilebilmesi gerekir.

Dijital formatta saklanan her tür veri veya bilgi, soyut tabiatından ötürü geleneksel delillere kıyasla manipülasyona ve üzerinde değişiklikler yapılmasına daha elverişlidir. Bu durum, bu tür verilere dayalı delillerin bütünselliğinin bozulmaması amacıyla farklı bir yaklaşımla ele alınması gerektiği dikkate alındığında, yargı sistemi açısından özel zorlukları beraberinde getirmektedir.

Kendine has özelliklerine göre dijital delilleri şu şekilde tanımlamak mümkündür:

Yasal süreçlerde ele alınan herhangi bir olgunun ispat veya aksinin ispatında daha sonradan ihtiyaç duyulabilecek, dijital formatta oluşturulan, saklanan veya iletilen her türlü bilgi olarak da tanımlanabilir**.**

1.5.1 Dijital Delilin Özellikleri

Geleneksel delillerle aynı pek çok özelliği olmakla beraber, dijital delillerin kendilerine has özellikleri de bulunmaktadır:

Dijital deliller ancak ehil bir gözle fark edilir: Dijital deliller çoğunlukla sadece uzmanların erişebileceği veya ancak özel bir takım araçlarla erişilebilecek yerlerde bulunur.

Dijital deliller çok hassas ve değiştirilmeye açık delillerdir: Belirli cihazlar ve belirli koşullarda bilgisayar hafızaları ve içerdikleri verilerin üzerine aynı cihazların işlevsel veya işletimsel imkanları dahilinde yazılabilmekte veya bunlar üzerinde değişiklikler yapmak mümkün olabilmektedir. Güç kesintisi veya hafıza da yeterli yer kalmamış olmasından ötürü sistemin yeni verileri eski verilerin 'üzerine yazması' bu duruma neden olabilmektedir. Elektronik bileşenler üzerinde saklanan (depolanan) bilgisayar verileri aynı zamanda aşırı sıcak veya nem veyahut da elektromanyetik alanların varlığı gibi ortam şartlarından ötürü de bozularak, kaybedilebilmektedir.

Dijital deliller normal kullanım sırasında da değiştirilerek yok edilebilir: Bilgisayarlar ister kullanıcı istemiyle ('belgeyi kaydet,' 'belgeyi kopyala,' vs.) veya işletim sisteminin kendisi tarafından otomatik olarak ('bu program için yer aç,' 'cihazlar arasında aktarım için veriyi geçici depola,' vs.) ve hatta saklama ortamını kontrol edenler tarafından ('veriyi tüm bloklara eşit paylaştır,' 'bloklarda eski sayfaları boşalt,' vs) hafıza durumunu sürekli değiştirmektedir.

Dijital veriler bozulmadan kopyalanabilir: Dijital veriler, her bir kopya esas delil ile tıpa tıp aynı veriyi içerecek şekilde istenen sayıda kopyalanabilir. Bu farklı özellik sayesinde delilin birden çok kopyası özgün kopyaya herhangi bir zarar vermeksizin birbirinden ayrı ve ancak birbirine paralel olarak farklı uzmanlar tarafından farklı amaçlarla incelenebilmektedir.

Diğer adli inceleme delillerine benzer olarak, dijital verilerin de doğru şekilde edinimi ve kullanılması davanın sonucu açısından hayati önemdedir. Genel kural ve kılavuzlara her an riayet edilmesi hususunda azami dikkat edilmelidir.

Dijital deliller sadece ehil ellere teslim edilmelidir: Her türde elektronik cihazın, uygun ve doğru prosedürle müdahale edilmesini gerektiren kendine has özellikleri vardır. Burada en büyük tehlikelerden biri delillerin istemeden değiştirilebilmesidir. Onaylı usul ve süreçlere uyulmaması neticesinde mahkeme önünde delile halel getirebilecek veya geçersiz kılabilecek yasal zorluklarla karşı karşıya kalınabilmektedir.

Dijital delil kaynakları hızlı bir dönüşüme tabidir: Yeni teknolojiler baş döndüren bir hızla ortaya çıkmakta ve büyük bir süratle geliştirilmektedir. Bunun neticesinde, bu deliller için geçerli usuller ve tekniklerin de sıklıkla yeniden gözden geçirilerek gerekli güncellemelerin yapılması gerekmektedir.

Dijital deliller usulüne uygun, uygun teknik ve araçlar kullanılarak değerlendirilmelidir: Adli incelemenin daha geleneksel alanlarında olduğu gibi, adli bilişim alanında da uzmanlar soruşturmayı gereğince yürütebilmek açısından özel bilgi ve araçlara gereksinim duyarlar. Karşılaşılan durumlarda doğru teknik ve araçlar kullanılmalıdır. elde edilen verinin delil değeri taşıması durumunda ise uygulanan usullerin de denetime açık ve diğer uzmanlarca yinelenebilir olması gerekir.

Dijital delillerin kabul edilebilirliği: Nihai hedefin deliller sayesinde uyuşmazlık konusu olguların ispat veya aksinin ispat edileceği dikkate alındığında, dijital delillerin mahkemede kabul edilebilirliği düşünülerek mevcut mevzuat ve en iyi uygulamalara uygun şekilde elde edilmesi esastır.

1.5.2 Dijital Delillerin Kabul Edilebilirliği

Dijital delillerin kabul edilebilirliği konusunda ayrıntılar farklı yargı bölgelerine göre değişiklik göstermekle birlikte mahkeme için dijital delillerin değerlendirilmesinde aşağıdaki kıstasların genel olarak dikkate alınması gereklidir:

Gerçeklik	Verilerin gerçekliğine ilişkin delilleri hazırlamak ve sunmak, kabul edilecek delilleri arayan tarafın sorumluluğundadır.
Tamlık	Delilin analizi veya delile dayalı herhangi bir görüş, hikayenin tamamını anlatmalı ve daha olumlu veya arzu edilen bir bakış açısına uyacak şekilde uyarlanmamalıdır.
Güvenilirlik	Delilin toplanma ve daha sonra ele alınma şekli hakkında, gerçekliği veya doğruluğu konusunda şüphe uyandırabilecek hiçbir şey olmamalıdır.
İnanılırlık	Delil, temsil ettiği gerçekler konusunda ikna edici olmalı ve mahkeme sürecinde mahkeme heyeti ona gerçek olarak güvenebilmelidir.
Orantılılık	Delilleri toplamak için kullanılan yöntemler adil ve adaletin çıkarları ile orantılı olmalıdır; herhangi bir tarafın haklarına yönelik önyargı (yani haksız müdahale veya zorlama düzeyi), delilin "ispat değerinden" (yani delil olarak değerinden) daha ağır basmamalıdır.

1.6 Dijital Delil Neden Önemli?

Suçlular esasen birer avcı gibi çalışır ve internet ve dijital ortamların kitlesel olarak kullanılmaya başlaması da bu suçlulara suç işleyebilecekleri farklı fırsatları beraberinde getirmiştir. Bu yeni iletişim kanallarını suistimal eden suçlular, geleneksel suçları işleyebilmek için farklı stratejiler geliştirmiş ve süreç içerisinde yeni suç türleri ortaya çıkmıştır. Dolayısıyla, hukuk sistemi içerisinde ilgili tarafların farklı dijital delil türlerinin neler olduğu ve bunlardan ne şekilde istifade edilebileceği hususunda *"alışkanlıklarının"* olması büyük öneme sahiptir.

Günümüzde hemen hemen her türlü suçta bir hafıza veya programa sahip bir elektronik cihaz yer almaktadır. Hatta suçun kendisi bu tür bir cihaz içermese bile failin hareket ve eylemleri bir kapalı devre kamera sistemine veya bir Küresel Konumlandırma Sistemi (GPS) veya mobil cihaz veya bir araç üstü sistemde kaydedilmiş olabilmektedir. Dijital delillerin adli bilişim inceleme ve soruşturmasından geçirilmesi suçluların adalet önüne getirilmesinde başvurulan öncelikli bir araç olmuştur.

İnternet ve internet uygulamalarının gelişmesi sayesinde artık deliller sadece kişisel bilgisayar ve mobil cihazlarda değil aynı zamanda ağ siteleri, sosyal ağ, e-posta ve mesajlaşma platformlarından de elde dilebilmektedir. Uygulama ve verilerin ulusal sınırlar arasında belirsiz lokasyonlarda uzaktan depolanmasına imkan veren 'bulut bilişimin' ortaya çıkması ve gelişimiyle birlikte olası dijital delillerin hali hazırda denenerek güvenilirliği kanıtlanmış ilke ve uygulamalara uygun olarak işlenmesi daha da önem kazanmıştır.

1.7 Dijital Delillere İlişkin İlkeler

Dijital delillerle ilgili çalışmalarında aşağıdaki ilkeler okuyucuya yol gösterici olacaktır. Bu ilkelerin ilk olarak düzenlenmesini takip eden on yıllık süreçte teknoloji dünyasında pek çok büyük değişiklikler olmuş, ilkeler, günümüzün operasyonel koşullarında karşılaşılan güçlükler ışığında gözden geçirilerek gerekli değişiklikler yapılmıştır.

Ülkeler, bu belgede önerilen önlemlere ilişkin olarak kendi hukuk çerçeve ve düzenlemelerini dikkate almalıdır. Bu husus, önemine binaen ilerleyen sayfalarda da tekrar edilecektir.

1.7.1 İlke 1 - Verilerin Bütünselliği

İlerleyen süreçlerde mahkemede delil olarak kullanılma olasılığı bulunan hiç bir veri, elektronik cihaz veya ortamın önemli oranda değişmesine neden olacak eylemlerden kaçınılmalıdır.

- Dijital araç ve veriler üzerinde ne yazılım ne donatıyla ilişkili hiç bir değişiklik yapılamaz. Suç mahallinden veya delillerin toplanmasından sorumlu olanlar elde edilen malzemenin bütünlüğü ve adli delil zincirinin güvenliğini sağlamakla yükümlüdür. Söz konusu cihaz ve/veya verileri emanet alanlarında bu sorumluluğu yerine getirmesi şarttır.

- Verinin çalışan cihazlar veya flaş belleklerdeki başkaca verilerde değişikliğe neden olmadan elde edilmesine imkan bulunmaması halinde bu işlem yetkilisi tarafından ve veri üzerinde asgari etki yaratacak şekilde yerine getirilir. İlke 2 ve İlke 5 söz konusu eylemin gerekli görülmesi durumunda uygulanır.

1.7.2 İlke 2 - Denetim İzi

Dijital delillerle çalışıldığı durumlarda gerçekleştirilen her türlü işlemin müteakip denetimler için kayıt ve muhafaza edilmesi gerekir. Buna göre, gerçekleştirilen bu işlemler bağımsız üçüncü taraflarca ve yine aynı sonucu elde edecek şekilde yinelenebilmelidir.

- Mahalde yürütülen tüm faaliyetlerin doğru olarak kaydedilerek gerekmesi durumunda aynı eylemlerin bir üçüncü tarafça da tekrar edilebilir olması büyük önem arz etmektedir. Dijital verilerin arama, el koyma, erişim, muhafaza veya aktarımına ilişkin her türlü eylemler kesinlikle eksiksiz olarak belgelenerek saklanmalı ve gözden geçirme amaçlı olarak ulaşılabilir olması sağlanmalıdır.
- Dijital delillerin işlenmesi ve incelenmesine ilişkin her türlü müteakip eyleminde daha sonraki süreçlerde denetim amaçlı erişilebilir olması gerekir.

1.7.3 İlke 3 – Uzman Desteği

Planlanan bir operasyon sırasında dijital delil elde edilmesi beklenen durumlarda, uzman/dışarıdan danışmanların operasyonun başındakiler tarafından zamanında uyarılmak suretiyle operasyon sırasında hazır bulunmaları sağlanmalıdır.

- Dijital delillerin aranarak elde edilmesi durumunda bu delillere el konulacağı soruşturmalarda mümkün olduğunca dijital delil uzmanlarının da sürece dahil olması tercih edilir. Bu tür dijital delil uzmanları ister kurum içinden olsun ister dışarıdan sözleşmeli çalışılsın (yüklenici) dijital delillerle çalışma konusunda uygun ve tarafsız olarak doğrulanabilir düzeyde bilgili olmalıdır. Bu tür uzmanlardan;
- Konuya dair uzmanlık ve deneyime sahip olmaları,
- Soruşturma yürütme konusunda gerekli bilgi ve beceriye sahip olması,
- Eldeki konuya dair bilgili olması,
- Gerekli hukuki bilgiye sahip olması,
- Gerekli (yazılı ve sözlü açıklamalar dahil) iletişim becerilerine sahip olmaları,
- Gerekli dil becerilerine sahip olmaları,
- Faaliyet içerisinde yer almalarının gerekli yetkilendirme ve/veya hukuki dayanağa sahip olması beklenmektedir.

1.7.4 İlke 4 – Uygun Eğitim

Dijital delil üzerinde çalışacak olanların gerekli seviyede eğitimli olmaları gerektir.

- Elde uzman olmayan durumlarda, herhangi bir elektronik cihaz veya dijital depolama aygıtı üzerinde yer alan özgün veriyi arama, el koyma ve/veya bu verilere ilk olarak erişimi olacak ilk müdahale ekiplerinin hukuken gerekli görülen süreçlere uygun olarak bu işlemler hakkında gerekli eğitimi almış olması ve gerçekleştirmiş olacağı eylemlerin uygunluğu ve sonuçlarını gereğince açıklayarak gerekçelendirilebilecek bilgiye sahip olması gerekir.

1.7.5 İlke 5 - Hukuka Uygunluk

Davadan sorumlu kişi veya kurumların ise hukuk, delil himaye yöntemleri ile genel adli ve usul ilkelerinin harfiyen uygulanmasında sorumlulukları bulunmaktadır.

2 Delil Kaynakları

Soruşturma sırasında karşılaşılabilecek her türlü elektronik cihaz veya ekipmanın delil kaynağı olabileceği hususu araştırmacılar tarafından her zaman dikkate alınmalıdır. Bu tür cihaz veya ekipman her zaman göz önünde ve araştırmacılar tarafından kolaylıkla tespit edilebilecek mahiyette olmayabilir.

Dijital delil içeren cihazlar her gün çeşitlilik kazanmaktadır. Aşağıda, nihai olmamakla beraber uygulamalarda en sık karşılaşılan dijital delil kaynakları sıralanmıştır.

2.1 Bilgisayar Sistemleri

Bir **bilgisayar sistemi** farklı bileşenlerden meydana gelir. Bu farklı bileşenler şunları içerecektir:

- Devre kartları, mikroişlemciler, depolama ortamı, hafıza ve diğer cihazlarla bağlantıları içeren bir kasa,
- Monitör veya başkaca bir ekran,
- Klavye,
- Fare,
- Bağlantılı harici sürücüler,
- Çevre birim donatıları,
- Yazılım.

Bilgisayar sistemleri masaüstü, dizüstü, kula bilgisayar, raflı sistem, mini bilgisayar ve ana sistem bilgisayarları olarak farklı biçimlerde olabilir. Yazıcılar, tarayıcılar, yönlendiriciler, harici depolama ortamları ve (birden fazla bağlantının yapılmasına imkan tanıyan) bağlantı terminalleri gibi diğer cihazlar genellikle bu sistemlere bağlanacaktır.

Budapeşte Bilişim Suçları Sözleşmesi'nde yer alan 'bilgisayar sistemi' ve 'bilgisayar verisi' tanımlamalarına dikkat edilmelidir:

Madde 1 - *Tanımlar*

İşbu Sözleşme amaçları bakımından:

a. *'Bilgisayar sistemi' terimi, bir veya birden fazlası, bir program uyarınca otomatik veri işleyebilen herhangi bir cihaz veya birbiriyle bağlantılı veya ilgili bir grup cihazı ifade eder;*

b. *'Bilgisayar verisi' terimi, bilgisayar sisteminin bir işlevi yerine getirmesini mümkün kılan bir programı da kapsayan, olguların, bilginin veya kavramların bir bilgisayar sisteminde işlenmeye uygun haldeki her türlü temsilini ifade eder.*

Tabletler, akıllı telefon ve aşağıda belirtilen diğer cihazlar bu tanım içerisinde yer almaktadır.

Desktop / Tower

Laptop

Mainframe

Bilgisayar sistem imgeleri[2]

2.1.1 Depolama Aygıtları

Depolama aygıtları da farklı biçim ve ebatta olabildiği gibi veri saklama yöntemleri açısından da değişiklik gösterebilir. Aşağıdaki bölümde bu tür cihazlar sahip oldukları imkan ve kabiliyetlere ilişkin ayrıntılara yer verilmiştir.

2.1.1.1 *Hard disk sürücüler ve katı hal diskler*

Sabit Disk Sürücüler (HDD), bilgisayar sistemleri içerisinde kullanılan başlıca depolama aygıtları olup bir devre kartı, veri ve güç bağlantılarından meydana gelmektedir. Sabit Disk Sürücüler içerisinde yüksek hısda dönen manyetik yüklü seramik, metal veya cam plakalar (diskler) bulunur. Disk yüzeyinde çalışan, eski plakçalarlardakine (pikap) benzeyen ve disk üzerinde veri 'yazan' veya yazılı veriyi 'okuyan' bir kol bulunur. Arama sırasında bilgisayar sistemi üzerinde kurulu veya bağlantılı olmayan sabit disk sürücülere de rastlanabilir. Masaüstü bilgisayarlarda kullanılan bir sabit disk sürücü genellikle 3.5 inç (8.9 cm) çapındayken, düzüstü bilgisayarlarda kullanılan sabit diskler ise 2.5 inç (6.35 cm) çapa sahiptir.

Katı Hal Diskler (SDD) ise günümüz bilgisayar sistemlerinde yaygın olarak kullanılmaktadır. Sabit Disklere kıyasla farklı bir yapıya sahiptirler. Manyetik yüklü diskler üzerinde veri toplamaktansa, katı hal diskler üzerinde depolanan veri mikroçipler üzerinde depolanır ve bu disklerin hareketli elemanları yoktur. Buna göre, katı hal disklerin düşmesi veya darbeye maruz kalması durumunda hasarlanması daha nadir bir durum olmakla birlikte, veriye daha süratli erişim de sağlamaktadır. SSD disklerin de farklı türleri mevcut olup, 2.5 inçlik muhafaza içerisinde mSATA veya M.2 PCVI-e bellek genişletme kartları gibi slot-in kartlar kurulabilir veya doğrudan ana karta lehimlenmiş olarak bulunabilir.

---

[2] İmge Kaynağı
[1] zdnet2.cbsistatic.com/hub/i/r/2015/09/01/dfa86998-089b-473c-8b63-73b1051b0935/thumbnail/770x578/fb90fb0770a3826f70c9577df2f6e8cd/lenovo-s500-business-desktop-all-in-one-enterprise-pc.jpg
[2] bhphotovideo.com/images/images2500x2500/lg_14z990_r_aas7u1_gram_i7_8565u_16gb_256ssd_1459833.jpg
[3] delimitercomau.c.presscdn.com/wp-content/uploads/2013/11/ibm-mainframe.jpg

Computer Hard Disk

Computer Hard Disk Interior

Solid State Disk

Farklı dahili depolama türleri[3]

2.1.1.2 *Değiştirilebilir ortamlar*

Büyük ses veya görüntü dosyalarının saklanmasında daha çok Kompakt Disk (CD), Dijital Video/Çok Yönlü Disk[4] (DVD) Blu-ray Diskler (BD) kullanılır. Ancak, bu ortamlar üzerinde aynı zamanda delil değeri bulunabilecek daha pek çok başka veri de büyük miktarda yer alır. Birbirlerine fazlasıyla benzemekle beraber, bu disklerin depolama kabiliyetleri arasında büyük farklılıklar bulunur.

Compact Disk (CD)

Digital Video Disk (DVD)

Blu-ray Disk (BD)

Farklı çıkartılabilir optik bellekler[5]

2.1.1.3 *Hafıza kartları*

Dijital kameralar, cep telefonları, dizüstü bilgisayar, müzik oynatıcılar ve oyun konsollerinde de kullanılan ve 'flaş bellek' olarak da bilinen hafıza kartları dijital veri depolamaya yarayan aygıtlardır. İlave bir güç beslemesi gerektirmeyen bu belleklerde büyük miktarlarda veri depolanabilmektedir. Hafıza kartlarının en yaygın türü SD, Mini SD ve Mikro SD formatlarında karşılaşılabilen Güvenli Dijital (Secure Digital - SD) kartlardır. Bundan ayrı olarak daha az yaygın olan formatlar arasında daha çok eski cihazlarda kullanılan Kompakt Flaş Bellek (CF - Compact Flash Card), xPicture Kartlar, Hafıza Çu-

[3] İmge Kaynağı
[4] https://stock.adobe.com/tr/images/computer-hard-drive/73144110
[5] https://stock.adobe.com/tr/images/inside-of-hard-disk-hdd-isolate/343334980
[6] https://in.micron.com/products/ssd
[7] https://in.micron.com/products/ssd

[4] Aynı zamanda DVD (Dijital Çok Yönlü Disk) olarak da bilinir

[5] İmge Kaynağı
[08] jetmedia.co.uk/cdmada80.jpg
[09] 3.bp.blogspot.com/_RzAQQvY1zGw/TPHH3KzB3rI/AAAAAAAAAWg/ctwmTTfTgew/s1600/icon-DVD.png
[10] 4.bp.blogspot.com/_N3kyjbXGs0I/S3OK_6rfzLI/AAAAAAAAADY/S76APQ9wVPE/s320/sony-blu-ray-disc-format-us.jpg

bukları (MS - Memory Stick), Çoklu Ortam Kartları (MMC) ve Akıllı Ortam Kartları (MMC) sayılabilir.

Secure Digital Card (SD) | Micro SD Card and Adaptor | Compact Flash Card (CF)

Hafıza kartı türleri[6]

2.1.1.4 *USB veri depolama aygıtları*

Evrensel Seri Veriyolu (USB - Universal Serial Bus) terimi bilgisayarlara bağlanarak kullanılan cihazlarda kullanılan iletişim, bağlantı ve güç besleme 'protokolü' veya kurallarını ifade eder. USB'nin ortaya çıktığı 90lı yıllardan bu yana bu protokolü kullanan cihaz sayısında büyük bir artış yaşanmıştır. Daha sık karşılaşılan USB cihazlar aşağıda görülebilir. USB özellikleri, konektör tipi ve aktarım hızları ağır USB-A konektörlü USB 1'den USB-C konektörlü, çok daha hızlı USB 4 düzeyine varıncaya kadar yıllar içerisinde büyük bir evrim de geçirmiştir.

Sık karşılaşılan USB bellekler[7]

Ancak tüm cihazlar göründükleri gibi değildir. Dijital delillerle çalışanların bu aygıtlarla ilgili yenilikler konusunda 'uyanık' olamaları gerekir. USB depolama aygıtlarının farklı şekillerde nasıl 'görünmez' olabileceğine birkaç örnek...

---

[6] İmge Kaynağı
[11] boygeniusreport.files.wordpress.com/2016/09/sandisk-1tb-extreme-pro-sd-card1.jpg?quality=98&strip=all&w=782
[12] portal.lynxmobility.com/images/Accesssories/microSD_2GB_02.jpg
[13] heise.de/imgs/18/4/8/6/8/6/8/SP128GBCFC400V10.jpg-777a6b1cc6a3f2fc.jpeg

[7] İmge Kaynağı
[14] brain-images-ssl.cdn.dixons.com/0/4/10142340/u_10142340.jpg
[15] sandisk.com/content/dam/sandisk-main/en_us/assets/product/retail/Extreme-PRO-USB-3.1-FlashDrive-right.png

Alışılmadık şekillerde USB bellekler[8]

2.1.1.5 *Veri depolama kasetleri*

Kaset üzerinde veri depolama ev kullanımından ziyade iş kullanımına yöneliktir. Günümüzde de kullanılmakta olan en yaygın veri depolama kaset uygulaması, 1990'larda açık format olarak geliştirilmiş olan LTO - Linear Tape-Open[9] türü kasetlerdir. Normalde yedekleme amaçlı olarak kullanılan kasetler geriye dönük, tarihsel bir analiz gerektiren veya asıl bilgisayarın erişilebilir olmadığı durumlarda faydalı olabilmektedir.

Linear Tape-Open Storage LTO Tape Drive

Veri depolama kasetleri[10]

[8] İmge Kaynağı
[21] ohgizmo.com/images/imation_4gb_micro_hard_drive.jpg
[22] media.gdgt.com/img/product/11/8ov/oakley-thump-i3m-800.jpg
[23] technabob.com/blog/wp-content/uploads/2006/09/imation_usb_wristbands.jpg
[24] ae01.alicdn.com/kf/HTB1uqhqbrSYBuNjSspfq6AZCpXaI/Lovers-Gift-Jewelry-Usb-Flash-Drive-Necklace-Pendrive-32-GB-64GB-Usb-Flash-Meomory-Stick-Card.jpg
[25] schweizer-messer.eu/img/Victorinox_Classic_Serie/46125TG4B_victorinox_usb_stick.jpg
[26] latestmsgs.files.wordpress.com/2010/10/watermelon_usb_flash_pen_drive_8gb_04.jpg

[9] açık format' kullanıcıların birbiriyle uyumlu birden çok depolama ortamına erişebilir olmasını ifade eder. Kaynak: http://searchstorage.techtarget.com/definition/Linear-Tape-Open

[10] İmge Kaynağı
[27] 2.imimg.com/data2/LO/TG/MY-3658176/fujifilm-linear-tape-open-lto5-250x250.jpg
[28] global.tdk.com/csr/ecolove/img/eco_med03.jpg
[29] 3000newswire.blogs.com/.a/6a00d83452e85869e20134809149c4970c-320wi

2.1.2 Çevre Birim Donatıları

Çevrebirim donatıları bilgisayarların bir parçası olmayıp bilgisayarın işlevlerini arttırabilmek maksadıyla bilgisayara bağlanan cihazlardır. Örnek vermek gerekirse, tarayıcı, yazıcı, veri depolama kasetleri, ağ kameraları, hoparlör, mikrofon, hesap makineleri, faks cihazları, telesekreter ve kart okuyucular çevrebirim donatılarına örnek olarak sayılabilir. Bu cihazların çoğu kendi veri depolama imkanına sahip olup farklı soruşturmalar kapsamında da kullanılabilmektedir (örn. bir kart okuyucu kredi kartı kopyalama soruşturmasında kullanılabilmektedir). Karşılaşılabilecek farklı türde çevrebirim donatılarına ait bazı görüntüler aşağıdadır:

Çevrebirim Donatıları[11]

2.2 Taşınabilir (Mobil) Cihazlar

2.2.1 Cep Telefonları

Telefonların arama yapma ve arama alma özelliğinden ibaret olduğu dönemler artık tarihe karıştı. Günümüzde, cep telefonları metin ve multimedya mesajları gönderip almaktan, internet erişimine, e-posta uygulamalarından, oyun oynama, müzik dinleme, kişisel sağlık/spor uygulamalarından banka işlemlerine ve hatta fotoğraf makinesi olarak pek çok farklı kullanıma sahiptir. En yeni cep telefonları, bağlantı anlamında farklı gerekleri olmakla beraber, artık gerçek anlamda birer bilgisayar halini almışlardır. Farklı telefonların farklı yeteneklere sahip olduğunu ve bağlantı biçimlerinin ("bağlantı arayüzleri") delil toplamak amacı ile özel ekipman gerektirebileceğini unutmamak önemlidir.

[11] İmge Kaynağı
[30] softwaretutor.files.wordpress.com/2010/04/fax.jpg
[31] superwarehouse.com/images/products/hpQ3851AA2L.jpg
[32] static.bhphoto.com/images/images345x345/504534.jpg
[33] carolinabarcode.com/images/ArticleImages/RunMyStore/CreditCardReader.jpg
[34] xactcommunication.com/itempics/48_xlarge.jpg
[35] labelprinter.org.uk/wp-content/uploads/2009/03/dymo-labelwriter-400.jpg

Cep Telefonları[12]

2.2.2 Tabletler

Tablet bilgisayarlar, klavye ya da fare yerine ekrana dokunarak işletilen cihazlardır. Cep telefonu veya Kişisel Dijital Yardımcılardan (PDA) normalde daha büyüktürler. Tabletler genellikle anlık bellek üzerinde veri depolamakla birlikte kullanıcı tarafından oluşturulan verileri artık giderek daha fazla bulut üzerinde depolanmaya başlamıştır. Tabletler son yıllarda hayli popülerlik kazanmıştır. Kendi işletim sistemlerine sahip olan tabletler **WLAN** (Kablosuz Yerel Alan Ağı) veya mobil veri ağları **(3G, 4G, 5G)** üzerinden internet erişimi sağlarlar.

Tablet bilgisayarlar[13]

2.2.3 Giyilebilir Teknolojiler

Elbise veya başka ca aksesuarlara entegre çok küçük bilgisayar sistemlerinin kullanıldığı farklı türde giyilebilir cihazlar da bulunmaktadır. Bu cihazlar, GPS, gyro, nabız, vs. bir dizi sensör ile WLAN, Bluetooht, hücresel ağ gibi iletişim işlevlerini bir arada barındırırlar.

[12] İmge Kaynağı
[36] i.ytimg.com/vi/xTKqEPnd_vc/maxresdefault.jpg
[37] i-cdn.phonearena.com/images/articles/355377-image/galaxy-s20-colors.jpg
[38] 5gmobilephone.net/wp-content/uploads/2019/04/Galaxy-Fold-5G.jpg

[13] İmge Kaynağı
[39] find-cool.net/wp-content/uploads/2012/09/Windows-8-Tablet-PC.jpg
[40] vedainformatics.com/blogs/wp-content/uploads/2010/01/apple-ipad-tablet-pc.png
[41] comparetablets.co.uk/wp-content/uploads/2011/09/galaxy-tab-8.9.jpg
[42] cache.gizmodo.com/assets/images/4/2007/12/delltablet.jpg

Akıllı saat, giyilebilir teknolojiler ve akıllı mercekler/gözlükler[14]

Bu cihazlar mesaj ve rehber, randevu, takvim, kullanıcı aktivitesi, coğrafi veri ve notlar gibi ilave bilgiler saklayabildikleri gibi akıllı telefon veya bilgisayarlarla eşleşerek 'senkron' çalışma imkanına da sahiptir. Olası deliller arasında;

- Rehber
- Randevu takvimleri
- E-postalar
- Coğrafi konum bilgileri
- Aktiviteler
- Notlar
- Telefon numaraları sayılabilir.

Bazı giyilebilir teknolojilerde de anlık bellek, akıllı çubuk hatta kamera gibi depolama aygıtları bulunabilmektedir. Akıllı saat ve sağlık/spor takip uygulamaları giyilebilir teknolojilerin en yaygın olanlarıdır.

2.3 Multimedya (Çoklu Ortam) Cihazları

2.3.1 Dijital Kameralar

Dijital kameralar fotoğraf veya video çekerken görüntüleri 'piksel' adı verilen binlerce küçük ışık noktası olarak algılar. Günümüzdeki dijital kameraların çoğu görüntünün yanısıra ses kaydı da alabilmektedir. Küçük hafıza kartlarında veya kendi belleklerinde dijital kameralar binlerce görüntü kaydederek saklayabilir (bkz. 2.1.1.3). Fotoğrafların da bulunduğu soruşturmalarda, resim ile birlikte bazı meta veriler de kaydedildiği

[14] İmge Kaynağı
[43] www.marcommnews.com/wp-content/uploads/2015/10/tech.jpg

için, bir fotoğrafın hangi makineyle çekildiğini kanıtlamak mümkün olabilir.[15] Gizli kameralar dahil, yaygın kullanılan kamera modelleri aşağıda gösterilmiştir.

Dijital Kamera Görüntüleri[16]

2.3.2 Dijital Video Kameralar

Dijital video kameralarda elde edilen görüntüler daha çok taşınabilir ortamlarda saklanmakla beraber kamera içerisinde yer alan sabit diske de kaydedilebilmektedir. Bu kameralar dijital fotoğraf makinelerine de çok benzer (kaldı ki dijital fotoğraf makineleri ile video, dijital kameralarla da fotoğraf çekilebilmektedir). Bazı video kamera modelleri aşağıdaki gibidir.

Dijital Video Kameralar[17]

[15] Örneğin EXIF (Paylaşılabilir Görüntü Dosyası Formatı) standardının kullanımı.

[16] İmge Kaynağı
[44] cdn-4.nikon-cdn.com/e/Q5NM96RZZo-YRYNeYvAi9beHK4x3L-8u4h56I3YwHLAQ4G0XzTY4Dg==/Views/1590_D3500_front.png
[45] upload.wikimedia.org/wikipedia/commons/d/d1/Nikon_J1_image%2C_10-30mm_lens.jpg
[46] cdn.hasselblad.com/hasselblad-com/fe6809c9-4c18-43ca-b923-6c768130b2fb_X1D+II+45P+front-right+white.jpg?auto=format&q=97&rect=0,0,3999,2667&w=1024&h=683
[47] iseupshop.com/media/catalog/product/cache/1/image/9df78eab33525d08d6e5fb8d27136e95/w/i/wiseup2_7.jpg
[48] cnet4.cbsistatic.com/img/Y-HjkDvbcLt1CamB1tauGJUMKKc=/fit-in/300x250/filters:no_upscale()/2018/02/22/a5714392-97fe-4b0a-8e09-a4ae0d8de1f8/41mvjkhmojl.jpg
[49] wholesales-shopping.com/wp-content/uploads/2011/09/17.jpg
[50] itechde1.nextmp.net/media/catalog/product/cache/1/image/650x650/9df78eab33525d08d6e5fb8d27136e95/2/1/21738_-_copy_2_1.jpg

[17] İmge Kaynağı
[51] alpha.akihabaranews.com/wp-content/uploads/images/6/66/16666//1.jpg
[52] sils.unc.edu/sites/default/files/it/CanonGL2.jpg
[53] pembrokeshirefilmfestival.files.wordpress.com/2012/12/panasonic-hcv100.png

2.3.3 Video/HDD Kayıt Cihazları

Daha çok evlerde ve televizyon programları veya diğer yerel faaliyetlerin kaydedilmesinde kullanılan video kayıt cihazları aynı zamanda önceden kaydedilmiş film, müzik ve diğer verileri tekrar oynatmak için de kullanılır. Daha sonrasında dijital akrabaları gelinceye kadar, 1970li yıllara eğin VHS (Ev Video Sistemi) kayıt cihazları öne çıkmıştır. VHS sistemlerde kayıt ve geri oynatma işlevleri günümüzde hala karşılaşabileceğiniz büyük kasetler sayesinde gerçekleştirilmekteydi. Ardından belli bir dönem DVD ve Blu-Ray kayıt cihazları kullanılmış, günümüzde de sabit sürücülü veya flaş belleğe sahip kayıt cihazları kullanılmaktadır. Günümüzde, televizyon veya uydu/kablo alıcılarının da kayıt işlevine sahip olmasıyla birlikte kayıt cihazlarının 'modası geçmiştir.' Diğer bir yandan da internet üzerinden ses/görüntü yayınları günümüzde çok daha yaygın hale gelmiştir. Kapalı devre (CCTV) televizyon kullanılan durumlarda kamera görüntüleri tüm bu formatlarda kaydedilmektedir.

Video Kayır Cihazları[18]

2.3.4 Dijital Ses Kayıt Cihazları

Dijital ses kayıt cihazları, elde tutulmak suretiyle bir yonga (çip) üzerinde ses kaydederek kayıtlı ses dosyasını geri oynatma imkanına sahip küçük cihazlardır. Azami kayıt süresi ve kaydın kalitesi açısından dijital ses kayıt cihazları da farklı kapasitelerde olabilmektedir. USB imkan ve kabiliyetlerine sahip kimi kayıt cihazları sayesinde elde edilen kayıtlar bilgisayara yüklenebilmekte, konuşma tanıma yazılımları sayesinde otomatik olarak kaydedilen ses dosyasının taslak halde deşifrajı yapılabilmektedir. Bu tip kayıt cihazları daha çok iş dünyası, akademi veya basın çevrelerinde kullanılmaktadır.

Dijital Ses Kayıt Cihazları[19]

[18] İmge Kaynağı
[54] s14.favim.com/610/160724/news-vcr-vhs-video-cassette-recorder-Favim.com-4547444.jpeg
[55] geraldgiles.co.uk/wp-content/uploads/2017/07/HDD-DMRHWT250EB-3.jpg

[19] İmge Kaynağı
[56] i.ebayimg.com/t/8GB-Digital-Voice-Recorder-650Hr-Dictaphone-MP3-Player-w-U-Disk-Iron-gray-US-/00/s/MTAwMFgxMDAw/$(KGrHqNHJEgFDTE6vHM3BQ7nlu,LGg~~60_35.JPG

2.3.5 Kapalı Devre (CCTV) Kameralar

Kapalı Devre (CCTV) kameralar firmalar, devlet kurumları ve özel kişilerce kullanılmaktadır. CCTV kameralar aralıksız olarak veya belirli bir faaliyeti izlemek maksadıyla kullanlabilir. Kapalı devre kameralar, bazı ülkelerde, toplumsal olaylar veya cezai faaliyetlerin önlenebilmesine yönelik olarak trafik veya insan hareketlerinin izlenmesi gibi kamusal alanların takibinde araçsallaşmıştır. Kimi kapalı devre kameralarda görüntü hafıza ortamında saklanmakla birlikte başka modeller kaydedilenleri internet üzerinden aktararak saklayabilmektedir. Bazı kapalı devre sistemleri ise sadece canlı izleme/takip amaçlı kullanılmaktadır. Bu sistemler hareketle etkinleşebilmekte veya çok az ışık veya kızılötesi koşullarda dahi çalışabilmektedir. Suç mahalli yakınlarında bulunması durumunda kapalı devre sistemlerin de dijital delil elde edilebilecek olası birer delil kaynağı olarak dikkate alınmaları gerekir. Buna ilaveten, kapalı devre kameraların polisin devam etmekte olan operasyonlarında kaydederek yayınlayabileceği unutulmamalıdır. Aşağıda bazı CCTV kamera modelleri görülmektedir.

CCTV kameralar[20]

2.3.6 Taşınabilir Medya Oynatıcılar

iPod veya **MP3**[21] gibi taşınabilir medya oynatıcılar ile de dijital medya saklanarak oynatılabilmektedir. Burada, dijital medya denildiğinde müzik ve diğer ses, fotoğraf ve video içerikler ile diğer belge ve dosya türleri ifade edilmektedir. Tekrarla, bu cihazların tümü de bir çok yönden bilgisayarlara benzemektedir. Bu cihazların bazısında taşınabilir bellek bulunurken bazısındaysa onbinlerce dosya depolama imkanı veren büyük sabit diskler bulunur. Bazı modeller aşağıda gösterilmektedir.

[57] c773974.r74.cf2.rackcdn.com/0330731_617464.jpg
[58] fl12.shopmania.org/files/p/bg/t/472/m-audio-micro-track-ii~3964472.jpg

[20] İmge Kaynağı
[59] 9to5mac.com/wp-content/uploads/sites/6/2017/08/netatmo-homekit.jpg?quality=82&strip=all&w=1600
[60] cdn.lorex.com/originals/images/products/_BF2017/LNB8921BW/1200x800/4K-Ultra-HD-IP-Camera-LNB8921-L1.png
[61] scan.co.ok/images/products/2717762-a.jpg
[62] i.ebayimg.com/images/g/TxYAAOSwRZtc48di/s-l300.jpg

[21] 'Moving Picture Expert Group Audio Layer'3

Taşınabilir Medya Oynatıcılar[22]

2.3.7 Video Oyun Konsolları

1970'li yılları başından beri kullanılmakta olan video oyun konsolları son yıllarda büyük bir ilerleme kaydetmiştir. Bu konsollarda da oyuncuların oyun oynayabilmesinden ayrı olarak internette gezinmesine ve video, fotoğraf ve müzik depolayarak oynatabilmelerine imkan tanıyacak şekilde entegre veya taşınabilir bellekler kullanılmaktadır. Geçmişte iletişim amaçlı olarak teröristler tarafından da kullanılmış olan video oyun konsolları sıklıkla çocuklar tarafından kullanılmasından ötürü iletişim özellikleri pedofiller tarafından kötücül kullanıma alet edilebilmektedir. Bu sebeplerden ötürü, ilk bakışta 'zararsız' görünebilmekle birlikte oyun konsolları[23] dijital delil kaynağı olarak asla göz ardı edilmemelidir. Oyun ve konsol sektörünü büyük ölçüde bu alanın önde gelen Sony, Nintendo ve Microsoft gibi önde gelen konsol üreticileri elinde bulundurmaktadır.

Video Oyun Konsolları[24]

[22] İmge Kaynağı
[63] store.storeimages.cdn-apple.com/4974/as-images.apple.com/is/image/AppleInc/aos/published/images/i/po/ipod/nano/ipod-nano-product-spacegray-2015
[64] 3.bp.blogspot.com/-Cm55ohrNTTc/UKEvulE8Zyl/AAAAAAAADLw/_l9wi1igPrQ/s1600/1.jpg
[65] i.ebayimg.com/images/i/281795555482-0-1/s-l1000.jpg
[66] src.discounto.de/pics/Angebote/2011-06/128207/151759_MP3-Player-S2-GO-4GB-rot_xxl.jpg
[67] ecodigital.co.uk/estore/images/sandisk-sansa-fuze.jpg

[23] http://blogs2.law.columbia.edu/cjel/preliminary-reference/2016/communicating-terror-the-role-of gaming-consoles-and-backdoors/

[24] İmge Kaynağı
[68] rafflecreator.s3.amazonaws.com/f52fce0f-f64d-4c56-a3d3-9d40600b7e36.jpeg
[69] gadgetsin.com/uploads/2011/01/sony_psp_2_codenamed_ngp_1.jpg
[70] cbs42.com/wp-content/uploads/sites/81/2019/12/Xbox-2.jpg?w=1280&h=720&crop=1
[71] assets.vg247.com/current/2018/01/Nintendo_switch_new_6.jpg
[72] d.ibtimes.co.uk/en/full/1534113/xbox-one-s-microsoft.png

2.4 Nesnelerin İnterneti ve Akıllı Evler

Hemen her fiziksel cihaz üzerinde bu cihazların kablolu veya kablosuz olarak yerel bir ağa veya internete veyahut da bunların ikisine birden bağlanmasına olanak veren elektronik sistemler bulunmaktadır. Birbirine bağlı ve/veya internet üzerinden kumanda edilebilen bu tür bağlantılı cihaz sistemleri 'Nesnelerin İnterneti' (IoT) olarak ifade edilmektedir. Eİ içerisinde yer alan cihazların başlıca üç işlevi vardır:

- sensörler (ısıya duyarlı/termal sensörler, hareket, açıklık, nem, lokasyon, bağlantı, vs. sensörler)
- cihazlar (durum bildirimi, ses/görüntü girdisi, veri depolama, aktörler, vs.)
- geçitler (cihaz bağlama, veri transferi, kontrol/filtreleme, tetikleyici eylemler, vs.)

Bu cihazlara, aralarında 'akıllı ev, akıllı bahçe' uygulamalarından, sanayideki robot uygulamaları, alarm sistemleri, trafik sensörleri ve trafik yönetim sistemlerine ve tedarik zincir yönetim sistemlerine kadar sınırsız sayıda örnek verilebilir. Bu otomasyon ortamları (akıllı eve, vs.) aynı zamanda bağlantılı olmayan ve/veya internet üzerinden kumanda edilmeyen yerel sistemleri de içerebilmektedir.

Bir akıllı ev içerisinde yer alan sensörler ve aktörler[25]

Eİ uygulamalarında yer alan cihazlar genellikle kullanılmaları durumunda uyarı vermektedir. Mevcut IoT kaynaklarından veri derlemek suretiyle davalara saat ve tarih eklenebilmekte, davaların belgelenmesine kayda değer katkı sağlanabilmektedir. Kimi durumlarda bir zamandizin sayesinde olayların akışı ve oluş sırası daha iyi anlaşılabilmekte, görgü tanıklığı geçerli/geçersiz kılınabilmekte veya kimi isimler sanık listesinden düşürülebilmektedir.

[25] İmge Kaynağı
[73] d2h1t9243qzgjg.cloudfront.net/uploads/attachment/image/97838/untouched_200229_smarthome_zuhause.png

2.5 Otomotiv Sistemleri

Ağ bağlantılı araç-içi elektronik bileşenlerin sayısı ve buna bağlı olarak bu bileşenlerden elde edilebilecek delil olasılığı bulunabilecek veri miktarı da her geçen gün artmaktadır. Bu bileşenlerin büyük çoğunluğu mutlaka internete bağlı olmaları gerekmemekle birlikte Eİ kapsamında yer alan cihazlardır (bkz. 3.4.11). Araç-içi elektronik sistemler daha çok iki sınıfa ayrılırlar:

- Bilgi-eğlence sistemleri (GPS konumlandırma, Bluetooth, mesajlar, çağrı, internet geçmişi, kameralar, vs.)
- Araç sistemleri (GPS, fren kontrolleri, hız, gaz kontrolü, çarpma sensörü, aydınlatma/sinyal durumu, stabilite kontrol, mesafe algılayıcı, yağmur sensörü, basınç sensörü, hava yastığı, doluluk, servis, vs.)

Araç-içi sensör veri ağları[26]

Sensörlerden gelen veriler ile aktüatör kontrolleri araç-içi entegre sistemler tarafından kaydedilir. Bu bilgiler ışığındaysa seyir durumuna (navigasyon) ilişkin soruşturma açısından faydalı olabilecek önemli ipuçları elde edilebilmektedir. Olası deliller arasında;

- Tarih damgalı seyir verileri (hız, yöne, rakım, coğrafi konum, GPS düzeltmeleri, vs.),
- Kapı, bagaj kapağı, kaput, vs. açma/kapama verileri,
- Kullanılan farklı koltuk ayarları,
- Koltuk kullanım verisi;
- Çağrılar, rehber, gelen-giden mesajlar, bağlantılı cihazlardan kopyalanan rehber verileri,

[26] İmge Kaynağı
[74] privateinternetaccess.com/blog/wp-content/uploads/2021/01/Car-data-is-increasingly-being-used-by-law-enforcement-in-criminal-cases.jpg?x97235

2.6 Diğer Elektronik Cihazlar

2.6.1 Kripto Paralara İlişkin Veriler

Vergi kaçırmadan para aklamaya veya uyuşturucu kaçakçılığına kadar işledikleri suçlarda şüpheliler gizlilik ve kimlik vermeden çalışabilme düşüncesiyle kripto para birimleri kullanmaktadır.

Kripto para birimlerinin artık birer yenilik olmaktan çıkmasıyla birlikte kullanıcıların gerçek kimliklerinin gizlenmesinde kullanılan şifreleme teknolojileri, işlemlerin sınır-aşan doğası, finansal işlemler konusunda zaman zaman tutarsızlık gösterebilen düzenlemeler ve yasadışı faaliyetler konusunda ulusal mevzuat arasındaki uyuşmazlıklar gibi nedenler suçluların kripto para birimlerine yönelmesi arkasındaki başlıca sebeplerdir.

Bitcoin'den bu yana hem sanal para birimleri hem de blok zincir teknolojisini tanımlamakta kullanılan çeşitli terimler de ortaya çıkmıştır. Ulusal mevzuatların ne denli farklı ve çeşitli olabildiği dikkate alındığında, bu kılavuzun ulusal yaklaşımların ötesinde uluslararası bir kapsamda olmasından hareketle, elinizdeki bu kılavuzda da Mali Eylem Görev Gücü terminolojisine dayalı bir terimce tercih edilmiştir.[27]

Sanal Para Birimi nedir?

- herhangi bir takas aracının dijital temsili
- ve/veya bir hesap birimi
- ve/veya bir değer saklama aracı
- ve sanal para birimi kullanıcıları arasında mutabakata dayalı olarak yukarıdaki işlevleri yerine getiren bir meta olarak ifade edilebilir.

Mali Eylem Görev Gücü ise, **Sanal Para Birimini** şu şekilde tanımlamaktadır:

- matematik-temelli bir para birimi
- merkezi olmayan dönüştürülebilir sanal para birimi.
- Bu para birimleri kripto (şifre) korumalı olup,
- (özel/tüzel) kişiler arasında değer aktarımı için açık veya özel anahtar gerektirir ve
- her aktarım için kriptolojik bir imza gerektirir.

Avrupa Konseyi tarafından "Kripto Para Birimleri El Koyma Kılavuzu" (bkz. Bölüm 1.4) yayınlanmış olup kılavuzda kripto para birimleri, ilgili kavramlar ve el koyma süreçlerine ilişkin ayrıntılı bilgi verilmektedir.

İlk müdahale ekipleri açısından iç hukuk ve usullere dayanarak kripto para birimlerine kolluk marifetiyle el koyulabildiğini bilmek önemli bir husustur. Bunun suçtan elde edilen parasal ve diğer gelirlere el konulmasıyla benzer değerlendirmesi gerekmek-

[27] http://www.fatf-gafi.org/media/fatf/documents/reports/Virtual-currency-key-definitions-and-potential-aml-cft-risks.pdf

tedir. Ancak, genel olarak kripto para birimlerinin tutulduğu sanal cüzdanlar koruma altındadır. Bilgisayar sistemlerinde saklanan olası şifre, vs. yanı sıra başkaca parola, anahtar kelime dizileri (seed phrase) veya iki-faktörlü yetkilendirme araçlarına da ihtiyaç olabilir. Bu nedenle, ilk müdahale ekiplerinin aşağıdaki araç ve izleri dikkate almaları gerekir:

Donatı veritabanı/defteri[28]

(Solda) 24 kelimelik metal plaka üzerine işlenmiş anahtar kelime dizisi, (sağda) özel anahtara sahip kağıt cüzdan[29]

2.6.2 İHAlar (İnsansız Hava Araçları)/Dronlar

İHAlar[30]

İnsansız Hava Araçları son yıllarda sadece askeri veya ticari kullanımda değil aynı zamanda bireysel kullanım için de hayli popülerlik kazanmıştır. Daha çok hemen her açıdan sabit/hareketli görüntü alabilme (foto/film) özellikleri ile öne çıkmakla beraber suçlular tarafından uyuşturucu kaçakçılığı, yasadışı takip ve diğer suçlar için de tercih edilmektedirler. ‹Dron› olarak da bilinen İnsansız Hava Araçları (İHA) aynı zamanda İnsansız Hava Sistemleri (İHS), İnsansız Küçük Hava Sistemleri (İkHS) veya Uzaktan Pilotajlı Hava Araç Sistemleri (UP-HAS) olarak da anılır.

[28] İmge Kaynağı
[75] shop.ledger.com/products/ledger-nano-x

[29] İmge Kaynağı
[76] cdn-images-1.medium.com/max/1600/1*4o0R_RCB3mRtROwD21Eqqw.jpeg
[77] miguelmoreno.net/wp-content/uploads/2013/05/NOTA-BITCOIN-cor-16JUL2012-51-1024x548.jpg

[30] İmge Kaynağı
[78] pngimg.com/uploads/drone/drone_PNG199.png
[79] pngimg.com/uploads/drone/drone_PNG204.png

Taşıdıkları resim ve video görüntüleri kadar coğrafi konum, güzergah, uçuş istatistikleri ve tarih damgalarıyla da İHA'lar dijital delil olarak ilgi çekicidir. Bir drona elkoyma sırasında tipik olarak ilgilenilmesi gereken dört elektronik bileşen vardır:

- Dahili anlık bellek (mikro)SD kartları içermesi muhtemel olan dronun kendisi
- Depolama verileri bulundurabilecek uzaktan kumanda
- Dronu kumanda etmek, canlı yayın gerçekleştirmek ve yerel olarak veya bulut üzerinde bilgi depolamakta kullanılabilecek mobil cihaz uygulamaları.

2.6.3 Analog Görünümler: Karekod, Barkod

Bu bağlamda ilginç bir sorunsal da barkod veya karekodların bilgisayar verisi ve dijital delil sayılıp sayılamayacağı konusudur. 'Bilişim Suçları Sözleşmesi Madde 1.b'de yer alan 'bilgisayar verisi' tanımına göre, "bilgisayar sisteminin bir işlevi yerine getirmesini mümkün kılan bir programı da kapsayan, olguların, bilginin veya kavramların bir bilgisayar sisteminde işlenmeye uygun haldeki her türlü temsilini ifade eder" denmektedir. Karekod veya barkod taşıyıcısının mutlaka bir bilgisayar sistemi olması gerekmediği, bunun aynı zamanda bir parça kağıt, diğer bir deyişle tam anlamıyla analog bir taşıyıcı da olabileceği ortadadır. Karekod veya barkodlar kendi başlarına bitler/baytlar veya 1 ve 0lardan meydana gelen elektronik veriler olmamakla birlikte yine de 'olguların, bilginin veya kavramların bir bilgisayar sisteminde işlenmeye uygun haldeki her türlü temsilini ifade' etmektedir. Bu nedenle, karekod ve barkodların da bilgisayar verisi ve dijital delil olarak ve bilgisayar verileri ve dijital delillere geçiş sağlayan birer geçit olarak dikkate alınmaları ve aynı sebepten, dijital delil olarak değerlendirilmeleri gerekir.

Karekod, bilgisayar sistemlerinde yorumlanacak olan bir veri taşıyıcısını, diğer bir ifadeyle analog bir temsili ifade eder. Hızlı Tepki (Quick Response) kodu demek olan QR Kodu/karekod iki boyutlu bir matriks kodu olarak otomotiv sanayii için Japonyada geliştirilmiştir. Barkod ise üzerinde kullanıldığı malzemeye dair makineler tarafından okunabilir bilgi içeren bir optik etikettir. Uygulamada, karekodlar bir internet sitesi veya uygulamaya işaret eden konum belirleyici, kimlikleyici veya izci/izleyiciler içerir. Veriyi daha verimli ve etkin biçimde saklayabilmek maksadıyla karekodlar üzerinde nümerik, alfanimerik, sekizli (bayt)/ikili ve kanji gibi 4 standart şifreleme modeli kullanılmakta olup aynı zamanda uzatmalar da kullanılabilmektedir.

Kare bir çerçeve içerisinde beyaz zemin üzerinde siyah kareciklerden oluşan karekodlar fotoğraf makinesi/kamera gibi görüntüleme cihazları yardımıyla okunarak elde edilen görüntünün doğru yorumlanabilmesi amacıyla Reed-Solomon hata düzeltme yöntemiyle düzeltilmesi sağlanır. Bu aşamadan sonra, ihtiyaç duyulan veri ortaya çıkan imgenin hem yatay ve hem de dikey bileşenleri içerisinde yer alan örüntülerden elde dilir.

Karekod

Barkod

Önceden belirtildiği gibi, dışarıdaki sunucular ve/veya veriye erişim sağlaması açısından karekod ve barkod taramaları özenle gerçekleştirilmelidir. Belirli bir bilgisayarda yer alan verilere erişilerek gerekmesi durumunda bu verilere dijital delil olarak el konulması veya kopyalanması süreçleri de itina ile ve sıkı gözetim altında gerçekleştirilmelidir. Aynı durum karekod/barkodun bulunduğundan ayrı bir fiziksel ortamda saklanan bilgisayar verileri için de geçerlidir. Bu bağlamda, sınıraşan dijital delil toplanmasına ilişkin ilkelerin burada da gözetilmesi gerekir.

2.6.4 Biyometrik Görünümler: Parmak İzi, Retina Taraması, Yüz Tanıma

Bilgisayar sistemlerine elektronik erişim için kullanılmaları durumunda, alttaki damar örgüsü ile veya bu örgü olmaksızın elde edilen parmak izleri, göz/retina yapıları veya yüz imgeleri de bilgisayar sistemlerinde işlenmeye uygun dijital veri kaynaklarıdır.

Parmak izi veya retina dijital delil olmaya yeterli elektronik özellikler barındıran biyometrik 'anahtarlar' olabilir. Bir parmak izi veya retinanın yapısına bağlı girdiler sayesinde bilgisayar sistemlerinde çeşitli süreçler veya işlemler başlatılabilmektedir. Söz konusu biyometrik verileri elektronik olarak tanınır ve bu verileri tarayan bilgisayar sistemi tarafından bu bilgisayar sistemi içerisinde yer alan bilgisayar verilerine dönüştürür.

Dolayısıyla, parmak izi, retina veya yüz taramaları bilgisayar sistemleri için elektronik açıdan uygun olduğu ölçüde (ki böyle olması bunların biyometrik anahtar olarak kullanıldığı anlamına gelir)

- ya bilgisayar sisteminde işlenmeye uygun bir bilgi formatında olmaları veyahut da
- çoğu durumda el koyulmuş bir bilgisayar sistemi ile bu sistemi kullanan veya kontrol eden kişi arasındaki ilişkiyi kesinlikle ortaya koymalarından ötürü iki şekilde dijital delil sayılırlar.

Parmak izi | Retina Taraması | Yüz tanım[31]

Bu tür biyometrik anahtarlara 'el konması' veya bunların dijital delil olarak kullanılması özellikle sorunlu bir alandır. Biyometrik anahtarları ne şekilde kullanıyorsunuz? Somut bir senaryo üzerinden değerlendirmek gerekirse; henüz yakalanmış bir çocuk kaçırma zanlısı üzerinde kaçırılan çocuğun arama çalışmalarında daha fazla zaman kaybetmemek adına parmak izi veya yüz tanıma ile akıllı telefonuna erişim sağlamak için sınırlı oranda fiziksel güç kullanımını uygun bulup bulmadığınız size sorulmuş olsun.

[31] İmge Kaynağı
[80] https://www.theguardian.com/technology/2019/jul/29/what-is-facial-recognition-and-how-sinister-is-it

Zorla parmak izi uygulaması

Zorla yüz tanıma uygulaması

Bu soruya çok net bir cevap verilemeyeceği gibi aynı zamanda ulusal mevzuat ve içtihadın da dikkate alınması gerekecektir. Elbette, biyometrik anahtarlar ve hukuki açıdan bunların nasıl değerlendirilebileceğine ilişkin ulusal mevzuatın kendine özgü usulleri olacağı unutulmamalı ve iyi anlaşılmalıdır. Özellikle bu konuya ilişkin Avrupa İnsan Hakları Mahkemesinin bir kararı bulunmamaktadır. Bu konuda hukuki ve insan hakları açısından kapsamlı bir yaklaşıma elinizdeki Dijital Delil Kılavuzu, Bölüm 10'da yer verilmektedir. Bu gibi zorlayıcı yöntemler uygulanır veya uygulanma yetkisi tanınırken ne denli özenli olunması ve ulusal mevzuata uygun hareket içerisinde olunması gerektiğini söylemeye bile gerek olmadığı açıktır.

2.7 Bu Cihaz ve Taşıyıcılar Üzerinde Olası Deliller

Bilgisayar yazılım ve donatıları kadar cihazların bağlı bulundukları ağ ve sistemler üzerinde cihazın kendisi tarafından otomatik olarak veya kullanıcı tarafından oluşturulabilecek önemli veriler barındırıyor olabilir. Elektronik açıdan kullanıma uygun karekod, barkod ve biyometrik anahtarlar muazzam bir dijital delil topluluğunun da anahtarlarıdır. Kullanıcı tarafından oluşturulan veriler arasında belge, fotoğraf, görüntü dosyaları, e-postalar ve ekleri ile veritabanları ve finansal veriler sayılabilir. Bilgisayar sistemleri tarafından oluşturulan verilere ise internette arama geçmişi ve önbellek, eylem günlükleri ile cihazın bağlı bulunduğu başkaca cihaz, bilgisayar ve ağlara ilişkin veriler örnek gösterilebilir.

Aşağıda, elektronik cihazlarda bulunabilecek kimi deliller görülmektedir.

Uygulama verileri
E-posta alıcıları, sohbet geçmişi, veritabanları, konfigürasyon (yapılandırma) verileri, kötücül yazılım analizleri

Kullanıcıya özel veriler
Kullanılan programlar, girilen internet siteleri, yapılan aramalar, açılmış/kaydedilmiş dosyalar, gönderilen iletiler, gidilen konumlar...

Kısmi deliller
Delil teşkil eden görsel, belge, geçmiş, günlük dosya parçaları

Exif verileri
Bir fotoğrafın nerede ve ne zaman çekildiği ve fotoğraf makinesine ilişkin veriler, seri nu., önizleme görselleri

Delil teşkil eden belgeler
Hesap dökümleri, şantaj mesajları, yasal olmayan

Erişilemeyen veriler
Gizli, şifreli dosyalar, silinmiş

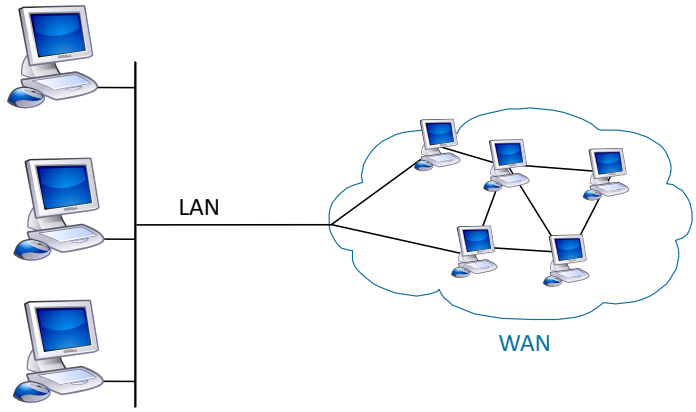
Bu Kılavuzda dijital delil konusuna odaklanılmakla birlikte, araştırmacılar, failin bir cihaz veya bir veri taşıyıcısı ile eşleştirilmesinde geleneksel adli tıbbın (parmak izi, DNA ve diğer izler gibi) önemini göz ardı etmemelidir.

2.8 Bilgisayar Ağları

İki veya daha çok sayıda bilgisayarın veri kablosu veya kablosuz olarak birbirine bağlanması durumunda bir ‹ağ› oluşur. Ağ bilgisayarları aralarında veri ve başkaca kaynaklar paylaşabilir ve sıklıkla kendi kapsamlarını arttırıcı/genişleten ve kendilerine başkaca işlevler kazandıran ilave donatıları bulunmaktadır. Bilgisayar ağları, ev ortamında aile fertlerinin bir modem paylaştığı türden sınırlı ağlardan gibi büyük firmalar veya devletler tarafından kullanılan, yüzlerce hatta binlerce bilgisayarın irtibatlandığı çok büyük ağlara kadar çok geniş bir yelpazede karşımıza çıkabilmektedir.

Yerel Ağ (LAN) - Yerel Ağ, bir ev, işyeri veya örneğin okullarda görülen bir binalar grubu gibi belirli bir 'mahal ile sınırlı' ağlardır. LAN özellikleri tanımlanırken ağ bilgisayarları arasında veri aktarımında daha yüksek hız sağlayabilmeleri, coğrafi kapsamlarının sınırlı olması ve telekom firmalarından hat kiralanmasını gerektirmemelerinden bahsedilebilir.

Geniş Alan Ağı (WAN) - Geniş Alan Ağı, daha geniş bir alanda ve kentsel, bölgesel ve ulusal sınırlardan geçen ağları da kapsayabilen bilgisayar ağlarını ifade eder. WAN terimi, yönlendirici[32] ve kamusal iletişim bağlantılarını kullanan ağları ifade eder.



LAN ve WAN düzeni[33]

[32] Yönelticiler (router) ağ üzerinde veya ağlar arasında veri paketlerini yönlendiren 'güzergah tanımlayıcı' cihazlar olarak tanımlanabilir.

[33] İmge Kaynağı
[81] Wikimedia commons, Harald Mühlböck, https://es.wikipedia.org/wiki/Archivo:LAN_WAN_scheme.svg

Bu ağlar, sırasıyla oda, bina, yerleşke veya bir belediye sorumluluk alanı ile sınırlı olarak düşünülebilecek Kişisel Alan Ağı (PAN), Kampüs Alan Ağı (CAN) veya Şehir Alan Ağları (MAN) ile kıyaslanabilir. Geniş Alan Ağlarına (WAN) en büyük ve en yaygın olarak bilinen internet örnek olarak gösterilebilir.

Ağlarla ilgili olarak karşılaşılabilecek terim ve cihazlar şunlar olabilir:

Bağlantı Noktası (Port) - (i) Bilgisayar veya donatı bağlantı noktaları ve (ii) ağ bağlantı noktaları olmak üzere iki tür bağlantı noktası bulunur. Bilgisayar bağlantı noktası, bir bilgisayar ile diğer bir cihaz arasında bilgi alışverişini sağlayan (USB, Ethernet ve audio bağlantı noktaları gibi) bağlantıları ifade eder. Ağ bağlantı noktası ise yazılım üzerinde yazılımın ağ hizmetlerine bağlantısını sağlayan bağlantı noktasıdır. Bu bağlantı noktaları bir binanın kapı ve pencereleri olarak düşünülebilir. Bilgisayar programlamasında bağlantı noktaları ayrı ayrı numaralandırılır. Bağlantı noktasına verilen bu numara o bağlantı noktasının işlev ve görevlerini belirlediği gibi ortak standartlara göre belirlenir.

Bant Genişliği - Bir borunun çapı gibi, bant genişliği de belirli bir telefon veya kablo hattı ya da uydu yayını üzerinden taşınabilecek azami veri miktarını ifade eder. Bant genişliği ne denli artarsa, veri indirme ve yükleme hızları da buna göre artacaktır.

Ortam Erişim Kontrol (MAC) Adresi - MAC adresi, üretici tarafından ağ bağdaştırıcı veya ağ arayüz kartlarına (NIC) atanan özgün bir koddur. MAC adresleri, cihazların tespit edilerek uygun verilerin cihazlara iletilmesini sağlayan ağ adresi olarak işlev gösterir.

Ağa Bağlı Depolama (NAS) - Tek bir kişisel bilgisayar yerine tüm bir ağa depolama alanı sağlayan NAS sistemleri bu anlamda harici sabit disklere benzetilebilir. Sadece veri depolamanın ötesinde başka kabiliyetlere de sahip olan NAS sistemleri otomatik indirme sunucusu (örn. Torrent) hatta küçük bir ağ sunucusu olarak da kullanılabilirler. Birçok NAS sisteminde birden çok sürücü ve RAID işlevleri yer alır.

Bağımsız Diskler Yedek Dizisi olarak ifade edilen **RAID** veri depolama işlevinin çoklu disk sürücüler kullanılmak suretiyle düzenlenmesini (veri konfigürasyonu) ifade eder. En iyi performans ve/veya en üst düzeyde veri güvenilirliği sağlamak üzere verileri tek tek diskler üzerinde depolanır. İşletme sistemi RAID'e sanki tek bir sabit diskmiş gibi erişim sağlar. Erişim kontrolü ve koordinasyon ya bir yazılım le veya donatılı RAID kontrol kartı üzerinden sağlanır. Bağımsız RAIDler daha çok ağ konfigürasyonlarında yer alır ve büyük miktarlarda dijital delil içerebilir.

RAID donatılı NAS sistemleri[34]

[34] İmge kaynağı:
[82] mpcomp.co.uk/5/graphics/import/105481.jpg
[83] resexcellence.com/wp-content/uploads/2013/01/5big_NAS_Pro_back_34_left.jpg

Ağ Arayüz Kontrol Kartı (NIC) - Ağ Arayüz Kontrol Kartları bir bilgisayar üzerinde kurulu, bilgisayarın ağa bağlanmasını sağlayan bir devre kartıdır. Yeni dönem bilgisayar ve diğer elektronik cihazlarda bu kontrol kartları ana kart üzerinde (monteli) olarak sunulmaktadır.

Ağ Arayüz Kontrol Kartları[35]

Ağ Göbeği - Ağ göbeği veya yoğunlaştırıcısı, çok sayıda bilgisayarı veya internet cihazlarını tek bir parça veya ağ sektörü olarak ortak hareket edebilecek şekilde bir araya getiren cihazı ifade eder. Böyle bir sektör içerisinde yer alan tüm bilgisayarlar birbirleriyle de iletişim içerisindedir. Göbek, ağdan gelen verileri kendisine bağlı bulunan diğer tüm cihazlara aktaran yapıdır. Temelde benzer olmalarından ötürü, bir araştırmacı açısından göbek ve anahtarları birbirinden ayırmak kolay olmayabilir ancak günümüzde ağ anahtarları büyük ölçüde göbeklerin yerine geçmiş durumdadır. Göbek ve anahtar arasında asıl fark ise; anahtar paketleri sadece hedef bağlantı noktasına iletirken, göbeğin paketleri tüm bağlantı noktalarına göndermesidir.

Ağ Göbeği[36]

Ağ Anahtarı - Ağ anahtarı, ağ göbeğine çok benzer. Anahtarlar genellikle birkaç ağ cihazını bir grup olarak bağlantılandırmakta kullanılır. Göbeklerin aksine, anahtarlar hangi MAC adresinin anahtar üzerindeki hangi bağlantı noktasını kullanmış olduğunu hatırlamak üzere kendi içerisinde sakladığı veritabanlarından istifade eder. Bu sayede, anahtar veri paketlerini tüm cihazlara değil de belirli bir cihaza yönlendirebilmektedir.

[84] gadgetreview.com/wp-content/uploads/2011/03/D-Link-DNS-321-Network-Attached-Storage-Enclosure.jpg

35 İmge kaynağı:
[85] intel.com/content/www/us/en/products/details/ethernet/800-network-adapters/e810-network-adapters.html
[86] sandberg.world/en-us/product/USB-C-to-Network-Converter
[87] images-na.ssl-images-amazon.com/images/I/51iJnzOQmfL._SY300_.jpg

36 İmge Kaynağı
[88] omnisecu.com/images/basic-networking/network-ethernet-hub.jpg

Ağ Anahtarı[37]

Yönlendirici (Router) - Yönlendirici, bir postanede mektupları tasnif eden bir 'ayırıcı' olarak düşünülebilir. Bir veri parçası veya veri paketinin alıcı adresini tespit ederek söz konusu veri paketini gönderildiği adrese en yakın bir noktaya iletilmesi yönlendirici sayesindedir. Yönlendiriciler ağ geçitlerinde yer alması gerekmekle birlikte mutlaka internete bağlı olmak zorunda değildir. Yönlendiriciler genellikle evlerde, evlerin geniş bant bağlantısını sağlamakta kullanılır. Böyle bir durumda yönlendiriciler hemanahtar, hem erişim noktası, hem bir güvenlik duvarı (firewall), hem yönlendirici ve hem de bir geçit noktası olarak birden çok amaca hizmet eder.

Yönlendirici[38]

Sunucu - Ağ üzerinde yer alan diğer bilgisayarlara bilgi ve/veya çeşitli hizmetler sunan bilgisayar veya cihazlar 'sunucu' olarak adlandırılır. Doğru yazılım ile birlikte, ağ bağlantılı herhangi bir bilgisayarı sunucu olarak yapılandırılabilmek mümkündür. 'Sunucular' çoğu zaman 'her zaman emre amade, kullanıma hazır' vaziyette güçlü bilgisayarlardır. Bir bilgisayar sunucusu, ağ sunucusu, e-posta sunucusu, dosya sunucusu, yazdırma sunucusu vs. birkaç hizmet birden sunabilir. İş dünyasındaysa güvenlik amacıyla ve yaşanabilecek herhangi bir arızanın etkisini asgaride tutabilmek açısından farklı hizmetleri farklı makineler üzerinden sunmak daha anlamlıdır.

Sunucular[39]

---

[37] İmge kaynağı
[89] upload.wikimedia.org/wikipedia/commons/thumb/5/5f/Linksys48portswitch.jpg/220px-Linksys48portswitch.jpg

[38] İmge Kaynağı:
[90] netgear.com/images/support/networking/wifi-router/XR450_Hero_Transparent.png

[39] İmge Kaynağı:
[91] x3me.info/wp-content/uploads/2011/10/server.jpg

Güvenlik Duvarı (Firewall) – Güvenlik Duvarı, yetkisiz erişimi engellemek suretiyle ağların güvenlik seviyesini arttırmakta kullanılan bir donatı veya yazılımdır. Örnek vermek gerekirse, güvenlik duvarları, gelen veri trafiğinin geçişine izin verilen bağlantı noktaları haricinde çoklu bağlantı noktaları üzerinden ağ erişimini tespit ederek engelleyecek şekilde yapılandırılabilir. Ev ortamında güvenlik duvarları daha çok yazılımlarda kullanılmaktayken iş ortamındaysa araştırmacılar daha sık donatı tipi güvenlik duvarlarıyla da karşılaşabilmektedir.

Donatı Tipi Güvenlik Duvarları[40]

Kablosuz Erişim Noktası (WAP) – Kablosuz Erişim Noktası kablosuz LAN cihazlarının ağın geri kalan kısmıyla bağlantısını sağlar. İkiden fazla cihaz bulunması durumunda her Kablosuz Yeral Alan Ağ (WLAN) altyapısında bir erişim noktasına ihtiyaç vardır. Yeni model yönlendiriciler de çokluklar Erişim Noktası olarak işlerlik gösterebilmektedir. Bir bilgisayarın Ağ Arayüz Kontrol Kartı hatta bir cep telefonu bile Erişim Noktası olacak şekilde yapılandırılabilir.

Erişim Noktaları[41]

Yukarıda sayılmış olan ağ cihazları resimlerde görüldüğü üzere bağımsız, tek başına çalıştırılabileceği gibi tek bir cihaz birden çok işlevi de yerine getirebilir. Ev ortamındaki yönlendiriciler sıklıkla hem modem, güvenlik duvarı, anahtar ve de erişim noktası olarak kullanılabildiği gibi Ağa Bağlı Depolama (NAS) sistemleri de aynı zamanda hem anahtar hem de erişim noktası kabiliyetleriyle bir Sanal Özel Ağ, e-posta ve ağ sunucusu olarak kullanılabilmektedir.

[92] chost.pl/templates/whm/images/servers.png
[93] electroguardpaint.com/images/computerServerRoom.jpg

40 İmge Kaynağı
[94] hacker10.com/wp-content/uploads/2011/04/Hardware-firewall-WatchGuard-XTM-2Series.jpg
[95] plug.4aero.com/Members/lmarzke/talks/plug_utm/screenshot1.png/image_preview
[96] cloverline-guardline.com/images/firewall.jpg

41 İmge Kaynağı:
[97] solwise.co.uk/images/imageswifi/net-el-ecb3500-1.jpg
[98] shop.allnet.de/media/image/3a/fb/15/12221557bd729fe3565.jpg
[99] amlabels.co.uk/files/images/products/5397.jpg

2.9 Hangi Delillerin Toplanması Gerektiğine Nasıl Karar Verilir?

Suç mahalinde hangi cihaza el koymak gerektiği ve hangi delillerin toplanacağı konusu göründüğü kadar kolay olmayabilir. Bu hususta dikkate alınması gerekenler 'Arama ve Müsadere' başlığı altında daha ayrıntılı olarak ele alınmıştır. Ancak, özenli bir planlama ve ön hazırlık yapmak suretiyle sahada karşılaşılabilecek zorluklardan kaçınmak mümkün olduğu gibi, dikkate alınması gereken hususlardan bazıları aşağıda ele alınmıştır:

2.10 Ne Tür Bir Yetkiye İhtiyacınız Var?

Cebri her türlü faaliyet planlanırken dikkate alınması gereken ilk husus alınması gereken hukuk izin ve/veya yetkinin ne düzeyde ve mahiyetinin ne olması gerektiğine karar vermektir. Yetki ve yetkilendirme farklı biçimlerde olabilir. Bunlardan en basiti el konulacak söz konusu ekipman veya veri sorumlusunun onamını almaktır. Bu onam her zaman yazılı olmalı ve araştırmacılar bu onamı veren kişinin hem kendi hakları ve hem de onamının olası sonuçlarının ne olabileceğini tam olarak anlamış olmasını sağlamalıdır. Elbette, bu noktada ulusal mevzuat ve kılavuzların da gerekleri öncelikle yerine getirilecektir.

Diğer yetki kademeleri kanunla belirlenir. Bunların hangileri olacağı yürütülen soruşturmanın mahiyeti ve yetki talebinde bulunanların yetkili mercii mi yoksa özel hukuk alanında mı çalıştıklarına göre değişecektir. Çoğu durumda, mahkeme veya arama emrine gerek olacaktır. Dijital verilerin davayla ilgili olduğunun değerlendirilmesi durumunda mahkeme veya arama emri delillerin aranmasına ve el konmasına ilişkin hükümler de içermelidir.

Gerekli seviyede yetkilendirme olmaksızın ekipman veya verilere el konulmasını da içeren hiç bir zorlayıcı fiil gerçekleşmemelidir.

2.11 Hazırlık ve Planlama

Bir operasyon planlama aşamasında bir takım soruların önceden dikkate alınması gerekir.

Veri nerede depolanmaktadır (tutulmaktadır)?

Söz konusu verilerin ekipmanın bulunduğu mahalden başka yerlerde saklanması ender karşılaşılan bir durum değildir. Arama yapılacak mahale geçildiğinde bu ihtimalin gözden kaçmış olması halinde (özellikle de verilerin başka bir yetki alanında bulunması durumunda) ilave yetki talebinde bulunulması gerekebilir veya ilave teknik beceri veya ekipman ihtiyacı doğabilir.

Şüpheli ne kadar bilgili ve tecrübeli olabilir?

Şüpheliler hakkında elden geldiğince çok miktarda istihbari bilgi elde etmek akıllıca olacaktır. Bilgisayar becerileri ileri seviyedeki bir şüpheli adli bilişim alanında ekipman veya verilerin ele geçirilmesine karşı, veri depolama cihazlarını şifrelemek veya tek anahtarlı veri silme özelliklerini etkinleştirmek, vs. karşı teknikler kullana-

bilecektir. Böyle bir durumda, çeşitli önlemler de alınmış olmalıdır. Şüpheli tarafından veriler aynı zamanda bulut veya başkaca çevrim içi mecralarda da depolanış olabileceğinden, bu durumda ekipman üzerinde herhangi bir veriye rastlanamayabilir.

Alternatif veya tamamlayıcı başka delil kaynakları var mı?

Şüpheli ile doğrudan temas içerebilecek veya ekipman veya veriye el konmasını gerektirebilecek bir eyleme girişmeden önce planlama aşamasında aynı bilgilere ulaşılabilecek daha tercih edilebilir başkaca kaynaklar bulunup bulunmadığı değerlendirilmelidir. Örneğin, çevrim içi bir işlemle ilgili olarak (e-posta yazışmaları olabilir) yazışmanın diğer tarafı ile, İnternet Servis Sağlayıcı (ISP) veyahut da çevrim içi hizmet sağlayıcılarıyla irtibat kurulması hususu da dikkate alınmalıdır. Bulut kullanımının giderek arttığı dikkate alındığında, aynı verilerin bu tür üçüncü taraf kaynaklarından elde edilebilmesi de mümkün olabilmektedir.

Verilerin şüpheliden mi yoksa alternatif veri sahibinden mi kurtarılacağı taktiksel bir karardır. Bazı yargı alanlarında, üçüncü taraflar yasa gereği, bir şüpheliyi uygunsuz bir şekilde uyarabilecek ve onu delilleri gizlemeye veya yok etmeye teşvik edebilecek herhangi bir veri erişimi talebini müşterilerine bildirmelidir. Sorumlu müfettiş veya savcı, (özellikle de veriler başka bir yargı alanında tutuluyorsa) üçüncü şahıslardan veri kurtarma prosedürünün bir soruşturmanın etkinliğini nasıl etkileyebileceğini değerlendirmelidir. Hangi delil kaynağının soruşturmanın amaçları bakımından en iyisi ve nihai sonucu bakımından en değerlisi olduğuna karar vermek de önemli olacaktır.

2.12 Adli Bilişim Uzmanları

Adli bilişim konusunun hayli karışık olması ve bir çok farklı disiplini bir araya getirmesinden ötürü bir adli bilişim inceleme uzmanı da elektronik delillere ilişkin bir alanda uzmanlaşmaktadır. Bu, bir müfettişin veya savcının bazen belirli teknik durumlarda yardımcı olması için bir adli bilişim uzmandan hizmet alması gerekebileceği anlamına gelir.

Uzman seçerken, saygın bir akademik veya profesyonel kuruluş tarafından verilmiş resmi bir akreditasyon görmek faydalı olabilir. Akreditasyon, belirli bir eğitim düzeyini ifade eder ve uzmanların uzmanlıkları mahkemede incelendiğinde bağımsız bir yeterlilik değerlendirmesi yapılabilmesini sağlar. Benzer şekilde, tanınmış hakemli dergilerde bir yayın geçmişi olması, önceki vakalardaki deneyimi ve mesleki itibarının tümü de bu güveni güçlendirmeye yardımcı olur.

Seçim süreci gelişigüzel olmamalı, başından itibaren etkin ve yapılandırılmış olmalıdır. Bilişim suçları birimlerinin, seçim kriterleri hakkında ilave tavsiyelerde bulunması mümkün olabilir, ancak aşağıdaki kriterler bağımsız bir danışman tanığın değerini ve itibarını belirlemeye yardımcı olabilir.

Uzmanlık vasıfları

a. İlgili akademik ve profesyonel yeterlilikler ve akreditasyon;

b. Vaka ile ilgili özel beceriler;

c. İlgili herhangi bir uzman meslek enstitüsünde veya derneğinde katılım;

d. Gerekli uzmanlık alanındaki faaliyetlerine ilişkin itibarına dair bir onay (örneğin, uzmanın çalışmaları için aldığı herhangi bir ödül var mı?).

Uzmanlık deneyimi

a. Bu tür bir işteki deneyimin uzunluğu ve niteliği;

b. Ulaşılan seviye ve kıdem;

c. Mahkemede katılım gösterdikleri dava sayısı;

d. Uzmanın müdahil olduğu davaların türü ve karmaşıklığı;

e. Deneyimin düzeyini ve kalitesini gösteren deliller (örneğin; saygın etkinliklere davetli konuşmacı olarak katılmış olmak; saygın hakemli dergilerinde yapılmış yayınlar, uzmanlık konusu ile ilgili resmi ve fahri görevlendirmeler).

Soruşturma bilgisi

Bir soruşturmanın niteliğinin ve ihtiyaçlarının; gizlilik, ilgililik ve bilgi, istihbarat ve delil arasındaki ayrım bakımından anlaşılması, bilinmesi.

Bağlamsal bilgi

Kolluğun ve hukuk kurumunun yaklaşımları, dili, felsefeleri, uygulamaları ve rolleri arasındaki farkı ve Bilgi Teknolojilerine ilişkin gerekli teknik bilginin yanı sıra olasılık kavramına en geniş anlamıyla aşinalık ve bilimsel ve yasal delil standartları arasındaki farkın anlaşılması, bilinmesi.

Hukuk bilgisi

Aşağıdakilerle ilgili olarak hukukun ilgili yönlerinin anlaşılması, bilinmesi:

a. İfadeler/beyanlar;

b. Devamlılık;

c. Delil kuralları;

d. Mahkeme prosedürleri (savunmanın ve savcılık makamının rollerindeki farklılıklar dahil);

e. Bilirkişinin rol ve sorumluluklarının net bir şekilde anlaşılması, bilinmesi.

İletişim becerileri

Aşağıdaki hususları günlük dilde ifade etme ve açıklama yeteneği:

a. Uzmanlık alanının niteliği;

b. İncelemede kullanılan teknikler ve ekipmanlar;

c. Kullanılan yorumlama yöntemleri;

d. Delilin güçlü ve zayıf yönleri;

e. Ortaya çıkarılan olgulara ilişkin olası alternatif açıklamalar.

Genel

a. Uzmana, delil niteliğindeki materyali (sübut vasıtasını) incelemesi için uygun güvenlik düzeyine göre erişim yetkisi verilmesi gerekebilir;

b. Uzman, (inceleme sırasında edindiği bilgilerin gizli kaldığından emin olunmasını sağlamak amacıyla) bir Gizlilik Sözleşmesi imzalamalıdır;

c. Gerektiğinde uzman, pedofili ile ilişkili materyallerin ilgili diğer kişiler üzerindeki etkisi de dahil olmak üzere, bu tür materyaller hakkındaki tüm ilgili kılavuzlardan haberdar edilmeli ve bu hususta gereğince risk değerlendirmesi yapması istenmelidir;

d. Uzmanın herhangi bir çıkar çatışması olmamalı ve bu yönde bir beyanda bulunması istenmelidir.

3 Arama ve Elkoyma

Bu bölüm, bir şüpheli tarafından kontrol edilen binalardan potansiyel elektronik delil kaynaklarının kurtarılması sırasında yapılacak işlemlerle ilgilidir.

3.1 Olay Yerine Kim ve Ne Götürülmeli?

Olay yerinde ne düzeyde bir adli bilişim desteği gerekeceğini belirlemek için planlama ve hazırlık sürecinin yeterince özenli olması gerekir. Adli bilişim uzmanlığına ihtiyaç olduğunun tespit edildiği hallerde, aramadan sorumlu kişi, gereken desteğe erişilebilmesini sağlamak için en kısa zamanda bunu yerel adli bilişim birimine ve/veya harici uzmanlara bildirmelidir.

Planlı bir operasyonda potansiyel elektronik delillere ilişkin verilecek ilk karar, arama yapılan konumun niteliği ve gerekli olabilecek elkoyma türü/türleri olacaktır; ya o anda kullanılmayan ekipmana (yani "kapalı kutu") elkoyma ve çıkarma ya da açık ve çalışır durumdaki cihazlardan canlı verilerin ele geçirilmesi veya her ikisinin bir kombinasyonu.

Bu tür kararların, koşullar netleştiğinde olay yerinde gözden geçirilmesi gerekebilir, ancak kullanılan BT sistemi hakkında mümkün olduğunca çok bilgi önceden toplanmalıdır. Ulusal kanunların gerektirdiği durumlarda, arama emri için bu tür ayrıntılar gerekli olabilir.

Planlama sürecine ilişkin sorular aşağıdakileri içerecektir:

- Hangi bilgisayar donanımı/işletim sistemi/yazılım/uygulamalar ve depolama ortamı, iletişim ve ağ ile ilgili ekipman (LAN/WLAN ağ ekipmanı) bulunması muhtemeldir?
- Bilgisayar sisteminden ve/veya ağdan kim sorumludur (ör. kadrolu bir yönetici mi var yoksa sistem harici bir şirket tarafından mı idare ediliyor)?
- Muhtemelen ne miktarda ekipman var?
- Ne miktarda verinin kopyalanması gerekiyor? Ve
- Depolama ortamı içinde bir sistem yedeği var mı?
- İlk planlama ve düşünme tamamlandıktan sonra, fiili giriş ve aramaya yönelik hazırlık aşağıdaki adımları içermelidir.
- Binaya girişin ve elektronik delillere el konulmasına kanunen uygun şekilde izin verildiği kontrol edilmeli (örneğin geçerli yasalar uyarınca bir arama emri çıkarılmalı veya başka bir izin alınmalı);
- Hızlı ve güvenli giriş yollarının mevcut olduğundan ve ayarlanmış olduğundan emin olunmalı;
- Ekip üyeleri (gerekirse harici uzmanlar da dahil olmak üzere) seçilmeli;
- Ekip üyelerine münferit görevler verilmeli;

- Ekip üyeleri görevlerini nasıl yerine getirecekleri konusunda bilgilendirilmeli (ilgili temel eğitimden geçmiş olmaları gerekir); ve
- Gerekli elkoyma araç ve gereçleri temin edilmelidir.

Tüm faaliyetlerin ulusal ve yerel kanunlara ve kurum politikasına uygun olması gerektiği unutulmamalıdır.

Olay yerinde elektronik delil bulunabileceği biliniyorsa veya bundan şüpheleniliyorsa, arama ekibi bu alanda özel olarak eğitim almış üyelerin yanı sıra gerekirse bağımsız bir uzman da içermelidir. Sistem harici bir şirket veya yönetici tarafından yönetiliyor veya bakılıyorsa, müfettiş onları uzman tanık olarak dahil etmeyi düşünebilir (elbette, şüpheli olarak kabul edilmezlerse ve başka bir çıkar çatışmaları yoksa).

En azından elektronik delillerle uğraşanlar (ve ideal olarak orada bulunan herkes), bu tür delillerin potansiyel kaynaklarını belirleme ve toplama konusunda temel eğitim almış olmalıdır. Mümkünse, elektronik delilleri toplamakla görevlendirilen her grup en az iki memurdan oluşmalıdır, böylece yapılan her işlem için iki tanık olabilir.

Tüm ekip üyeleri, elektronik delilleri incelerken uygulanacak ilkelerin yanı sıra diğer fiziksel delilleri incelemek için kullanılan ilkeleri de bilmelidirler. Gerekli herhangi bir özel önlemin (örneğin elektronik cihazlardan parmak izi toplamak için alüminyum tozu kullanmamanın) bilincinde olmalıdırlar. Ayrıca, belirli durumlarda uzman bir birime başvurmaları gerektiğini ve aramaya katılan bir uzman yoksa bu iletişim bilgilerini hazır bulundurmaları gerektiğini de bilmelidirler.

Bazen elektronik delilleri toplamak için özel araç ve gereçlere ihtiyaç duyulur ve teknolojideki gelişmelerin daha önce kullanılan herhangi bir ekipmana ilaveler yapılmasını gerektirmesi mümkünse de, aşağıdaki temel araç seti birçok durumda yardımcı olacaktır.

- Demontaj ve söküm araçları:
  - Tornavidalar (düz başlı, çapraz başlı ve üreticiye özel (örneğin Hewlett Packard, Apple));
  - Anahtarlar (altıgen somun, yıldız tipi somun ve güvenli uç);
  - Penseler (standart ve kargaburun);
  - Kablo kesiciler (kablo bağlarının çıkarılması için);
  - Küçük cımbızlar;
- Dokümantasyon:
  - Arama ve elkoyma tutanağı (eşya kaydı – bu kılavuzun Ekine bakınız);
  - Etiketler ve bant (kablolar ve prizler de dahil olmak üzere sistem bileşeni parçalarını işaretlemek ve tanımlamak için);
  - Kablo etiketleri;
  - Delil etiketleri (bağlı ve yapışkan – bu kılavuzun Ekine bakınız);
  - Olay yerinde doldurulması gereken diğer gerekli formlar ve belgeler (bu kılavuzun Ekine bakınız);
  - Silinmez renkli keçeli kalemler (sökülen parçaları kodlamak ve tanımlamak için);

- Fotoğraf makinesi ve/veya video kamera (olay yerinin ve ekranlardaki herhangi bir görüntünün fotoğrafını çekmek için);

- Paketleme ve taşıma malzemeleri:
  - Antistatik torbalar (sökülen, devre kartları gibi ekipmanların korunması için). Statik elektrik üretebilecek (polietilen torbalar gibi) malzemelerden kaçınılmalıdır;
  - Faraday torbaları ve/veya alüminyum folyo;
  - Antistatik baloncuklu ambalaj;
  - Kablo bağları (kabloları bağlamak için);
  - Delil torbaları ve bant;
  - USB cihazları, DVD'ler veya CD'ler gibi harici depolama ortamlarını paketlemek için koliler;
  - Ambalaj malzemeleri (45katı köpük veya 45köpük dolgular gibi statik elektrik üretebilecek malzemelerden de kaçınılmalıdır);
  - Sonradan birleştirilen kutular veya çeşitli boyutlarda sabit kutular (eğer varsa, orijinal ambalaj kullanılmalıdır);

- İletişim araçları:
  - Tavsiye almak için cep telefonu veya diğer iletişim cihazları (bilgisayar ekipmanlarının yakınında kullanılmamalıdır);
  - Yardım için iletişim bilgileri (örneğin uzman biriminin telefon numaraları)

- Diğer malzemeler:
  - Kelepçeli küçük şaloma pürmüz;
  - Eldiven;
  - El arabası (yani çuval arabası veya 2 tekerlekli araba);
  - Büyük lastik bantlar;
  - Büyüteç;
  - Yazıcı kağıdı;
  - Tüm standart adli bilişim araçları yüklenmiş bir dizüstü bilgisayar;
  - Ağ kabloları (Çift Bükümlü kablolar ve Çapraz kablolar);
  - WiFi tarayıcı (WiFi ağlarını ve cihazlarını ortaya çıkarmak ve belgelemek için);
  - Yeterli Sabit Disk Sürücüsü kapasitesi (örneğin birkaç Terabaytlık harici Sabit Disk Sürücüleri);
  - Donanım Yazma Engelleyiciler (yerinde görüntüleme ve öncelik belirleme amacıyla);
  - Adli Bilişim Önyükleme DVD'leri (eğitimli memurlar tarafından kullanılmak üzere);
  - Canlı Veri adli inceleme araçları (eğitimli memurlar tarafından kullanılmak üzere);
  - Ulaşım (ekip üyeleri, elkoyma araç ve gereçleri ve elkonulan deliller için olay yerine gidiş geliş).

3.2 Olay Yerinin Emniyete Alınması

Aramadan sorumlu kişi, olay yerindeki tüm kişilerin güvenliğini ve hem geleneksel hem de elektronik tüm delillerin bütünlüğünü sağlamalıdır. Bilgisayarlar ve diğer elektronik cihazlar üzerindeki potansiyel delillerin kolayca değiştirilebileceğini, silinebileceğini veya yok edilebileceğini, ama geleneksel adli bilişim delillerinin de bir rolü olduğunu ve çapraz bulaşmaya duyarlı olduğunu unutmayın.

Olay yerinin emniyete alınması aşağıdaki adımları içerir:

- Olay yerinin emniyete almak için kendi yetki alanınızdaki standart politika ve prosedürü izleyin;
- Sahadaki verilerin kurcalanmasını önlemek için olay yerindeki tüm personelin kendi cihazlarındaki WiFi ve Bluetooth işlevlerini devre dışı bırakması tavsiye edilir. Aksi takdirde personel cihazları örneğin akıllı ev cihazlarına bağlanabilir ve verileri değiştirebilir (örneğin yeni kayıt günlüğü girdileri oluşturabilir, eski kayıt günlüğü girdilerinin üzerine yazabilir);
- Herkesi, (ekipman ve güç kaynağı da dahil olmak üzere) toplanacak herhangi bir delilin yakınından uzaklaştırın;
- Kişisel ve taşınabilir cihazlar da dahil olmak üzere tüm elektronik cihazları güvence altına alın;
- Herhangi bir yetkisi olmayan kişilerden gelen yardım veya teknik destek tekliflerini reddedin.
- Zaten kapatılmış olan bilgisayarları veya elektronik cihazları kapalı halde bırakın.
- Eğer bir bilgisayar açıksa veya açık olup olmadığı belirlenemiyorsa, müfettiş bölüm 3.4.3 içinde açıklanan adımları izlemelidir.
- Geçici verileri, bölüm 3.5 içinde açıklanan adımları izleyerek fiziksel ve elektronik olarak koruyun.
- Toplanmayacak ilgili elektronik bileşenleri belirleyin ve belgeleyin;
- Cihazlara bağlı telefon ve ağ hatlarını tanımlayın, belgeleyin ve etiketleyin;
- Elkonulacak bir cihazdan (örneğin DNA, parmak izleri, uyuşturucular, hızlandırıcılar gibi) başka herhangi bir delil gerekip gerekmediği konusunda vaka istihbarat görevlisine danışın ve karar verin;
    - Eğer gerekiyorsa, ilgili kılavuzda belirtilen delil türüne ilişkin genel inceleme prosedürlerini izleyin. Acil bir veri kaybı riski yoksa, diğer delilleri gerektiği şekilde güvence altına alın. Takip işlemlerinin (örneğin klavye/fare/dokunmatik ekran kullanımının) bu delilleri yok edebileceğini unutmayın.
    - Tahribatlı teknikleri, elektronik delil kurtarma işleminin tamamlanmasından **sonraya** erteleyin;
    - Diğer delilleri toplamak için tahribatlı teknikler kullanılıyorsa, önce elektronik delil kurtarma ve elde etme işlemleri tamamlanmalıdır;
    - Ekipmana ve verilere zarar verebileceği için, olay yerinden parmak izi toplamak için alüminyum tozu **kullanmayın**.

- Olay yerinde elektronik olmayan, ancak aşağıdakiler gibi ilgili delilleri arayın:
  - yazılmış parolalar ve diğer elle yazılmış notlar;
  - yazı izi geçmiş boş kağıt desteleri (ancak kara kalemle gölgelendirme yapmayın);
  - donanım ve yazılım kılavuzları;
  - takvimler veya günlükler;
  - metin veya grafik bilgisayar çıktıları;
  - fotoğraflar; veya,
  - daha sonra parola/şifre kırma süreci için yararlı olabilecek kişisel ilgi alanları hakkındaki bilgiler (çoğu parola; plakalar, ortaklar/çocuklar, telefon numaraları, hobiler ve benzerleri gibi doğrudan kişisel ortam ile ilgili bilgilerdir);
- Ön görüşmeleri (ifade alma işlemlerini) yapın;
  - Olay yerindeki tüm kişileri (tanıkları, kurbanları veya diğerlerini) ayırın ve tanımlayın ve giriş zamanındaki konumlarını kaydedin;
  - Bu kişilerden bilgi toplamak ve kaydetmek için bir kontrol listesi kullanın;
  - Kurum politikası ve yürürlükteki yasalar (örneğin kendini suçlamaya karşı/susma hakkı veya haklar listesine ilişkin bir uyarı sağlama şartı) ile tutarlı davranın, bu bireylerden aşağıdaki bilgileri alın:
  - Cihazın/sistemin kullanım amacı (örneğin muhasebe);
  - Olay yerinde bulunan cihazların/sistemlerin sahipleri ve/veya kullanıcıları yanı sıra parolaları (aşağıya bakın), kullanıcı adları ve İnternet Servis Sağlayıcı;
  - Sisteme, yazılıma veya verilere erişmek için gereken tüm şifreler. Bir kişinin birden fazla parolası olabilir (örneğin BIOS, sistemde oturum açma, ağ veya ISP, uygulama dosyaları, örneğin PGP/Truecrypt/Veracrypt/Bitlocker/FileVault/dm-crypt ve benzerleri için e-posta, erişim belirteci gibi şifreleme parolası, zamanlayıcı veya kişi listesi);
  - Herhangi bir eşsiz güvenlik planı veya silici cihaz;
  - Çevrimiçi sosyal ağ web sitesi hesap bilgileri.
  - Herhangi bir site dışı veri deposu; ve
  - Sistemdeki donanımları veya kurulu yazılımları açıklayan herhangi bir dokümantasyon;
  - Tüm diğer ilgili bilgiler.

3.3 Olay Yerinin Belgelendirilmesi

Olay yerinin belgelendirilmesi **tüm elkoyma prosedürü boyunca** devam eden bir işlemdir. Bilgisayarların, depolama ortamlarının ve diğer elektronik ve geleneksel cihazların konumunu ve durumunu doğru bir şekilde belgelemek çok önemlidir. Bu bölümde, belgelenecek bilgilerin sadece bir özeti verilmektedir.

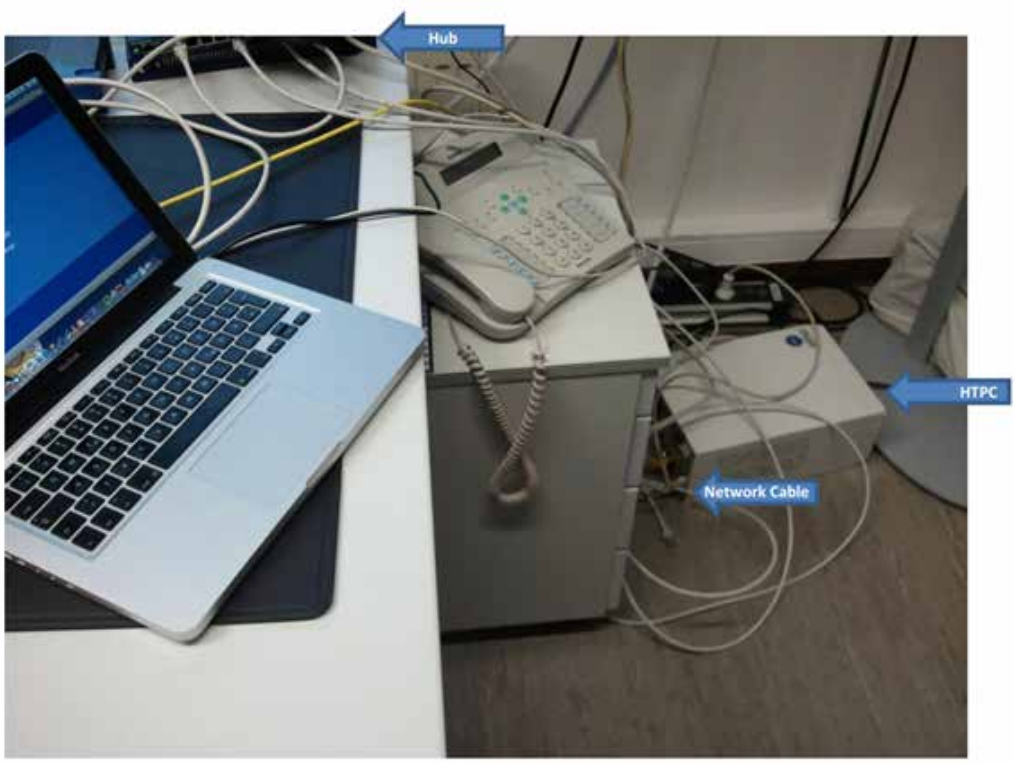
Genel olarak, aşağıdakiler belgelenmelidir, ancak delil toplama aşaması sırasında ilave belgeler oluşturulabilir:

- Fiziksel olay yeri;
  - Sistemin bir taslak planını çizin (farenin konumu ve bileşenlerin konumu gibi ayrıntılar da dahil olmak üzere);
  - Tüm olay yerinin fotoğraflarını çekin/videosunu çekin/belgeleyin (mümkünse 360 derecelik kapsama alanı ile);
  - Bilgisayar sistemlerinin ve elektronik bileşenlerin/cihazların/ekipmanların konumunu ve nasıl bağlandıklarını belirleyin.
- Aşağıdakileri belgeleyin:
  - Bulunan tüm ilgili ekipmanlara ilişkin (marka, model ve seri numarası da dahil olmak üzere) ayrıntılar;
  - Bilgisayarın açık/kapalı (açık, kapalı veya uyku modunda) olma durumu da dahil olmak üzere elektronik delil içeren veya sunan her bilgisayar sisteminin durumu ve konumu;
  - Bilgisayar sistemine veya diğer cihazlara (örneğin akıllı ev cihazlarına) giren ve bunlardan çıkan tüm bağlantıları (kablolu veya kablosuz) belgeleyin;
  - Tüm bağlantı noktalarını ve (çevresel aygıtlara bağlantılar da dahil olmak üzere) kabloları, daha sonra aynı şekilde yeniden bağlamaya imkan tanıyacak şekilde etiketleyin; kullanılmayan bağlantı noktalarını "kullanılmayan" olarak etiketleyin;
  - Diğer depolama ortamlarını tespit etmek için dizüstü bilgisayar bağlantı terminallerini belirleyin;
  - Müdahale edildiği sırada monitöre ilişkin ayrıntıları belgeleyin;
  - Bilgisayarın ön tarafının yanı sıra monitör ekranının ve diğer bileşenlerin de fotoğrafını çekin;
  - Monitör ekranında görünenler ile ilgili yazılı notlar alın;
  - Çalışan programların videosunu çekin veya monitör ekranı etkinliğine ilişkin daha kapsamlı belgeleme yapın;
  - Toplanmayacak ilgili elektronik bileşenleri belgeleyin;
- Olay yerinde bulunan kişilerden alınan bilgiler;
- Söz konusu kişilerin ifadelerini alın ve formları doldurarak yanıtlarını belgeleyin;
- Aşağıdakileri belgeleyin:
  - Arama yapılan tesiste bulunan tüm kişilere ilişkin ayrıntılı bilgiler;
  - İlgili bilgisayar sistemini ve ekipmanını kullanan tüm kişilere ilişkin ayrıntılı bilgiler;
  - Bilgisayar kullanıcıları/sahipleri/tanıkları tarafından yapılan açıklamalar, yorumlar ve verilen bilgiler;
  - Olay yerinde yapılan tüm işlemler;

- Gerçekleştirilen işlemin açıklamasını ve tam zamanını içeren denetim izi/elkoyma günlüğü oluşturun.

Bir müfettişin bir arama ve elkoyma senaryosunda nelerle karşılaşabileceğine ve olay yerini nasıl belgeleyebileceğine dair bazı örnekler şunlardır:

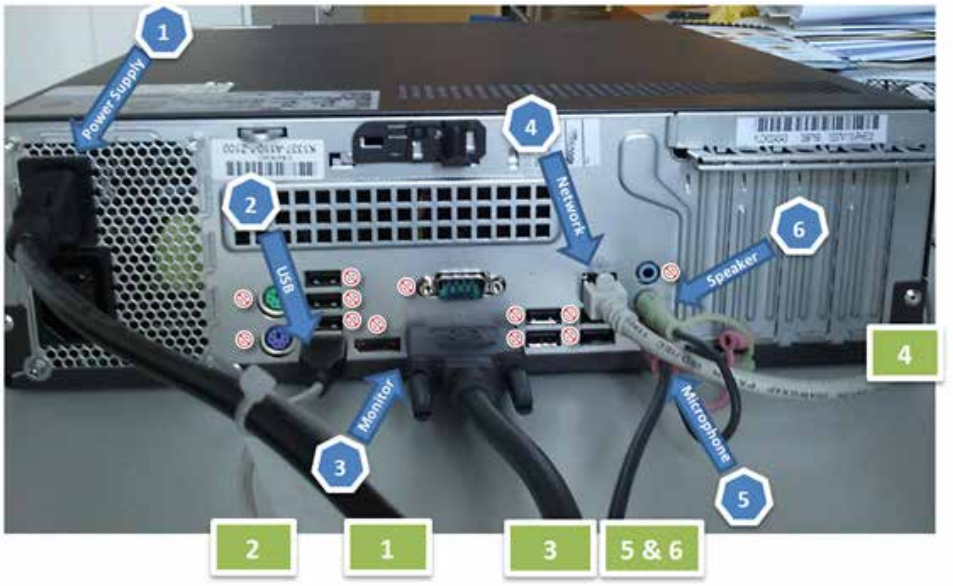
Genel görünüm fotoğrafları:


Hub
HTPC
Network Cable


Connected network cables
Access Point
Switch
LINKSYS
Hub

Ayrıntılar:

Kablolu bir Masaüstü Bilgisayarın Ayrıntılı Bağlantı Durumu:



3.4 "Kapalı Kutu" Senaryolarında Arama ve Elkoyma

Sadece olay yerinde bulundu diye bir bilişim sistemine delil olarak elkonulmamalıdır. Bu tür bir önlem, söz konusu suçla orantılı olarak gerekçelendirilmelidir, bu nedenle arama emrini veren kişi, bir eşyanın alınıp alınmayacağına dair bilinçli bir karar vermelidir. Elkoymayı gerekçelendirmek için makul bir şüpheye veya yeterli delile sahip olunmalıdır.

Bir "kapalı kutu" senaryosu, arama sırasında kapatılmış durumda bulunan ekipmanı ifade eder. Kapalı kutu cihazlar, olay yerinden çıkarılacak ve daha sonra bir kolluk kuvveti veya adli bilişim laboratuvarında incelenecektir.

Elektronik delil, diğer her türlü delil için geçerli olduğu gibi, dikkatli ve delil değerini koruyacak bir şekilde ele alınmalıdır. Bu, sadece bir eşyanın veya cihazın fiziksel bütünlüğüyle değil, aynı zamanda içerdiği elektronik verilerle de ilgilidir. Bazı elektronik delil türleri özel toplama, paketleme ve nakliye işlemleri gerektirecektir. Elektronik delil, (örneğin statik elektrik, mıknatıslar, radyo vericileri ve diğer cihazlar tarafından oluşturulan) elektromanyetik alanlardan kaynaklanan hasara veya değişikliğe karşı hassas olabilir ve yeterli düzeyde korunmalıdır.

Elektronik olmayan delillerin (veya geleneksel delillerin) alınması da soruşturmada çok önemli olabilir ve bu tür delillerin alınıp korunmasını sağlamak için gereken özen gösterilmelidir. Soruşturmayla ilgili diğer eşyalar, çoğunlukla bilgisayarın veya ilgili donanım parçalarının yakınında bulunur ve bunlara da elkonulmalıdır. Her zaman olduğu gibi, tüm delil kalemleri, kurum politikalarına ve geçerli yasalara uygun olarak tanımlanmalı, güvence altına alınmalı, paketlenmeli ve korunmalıdır.

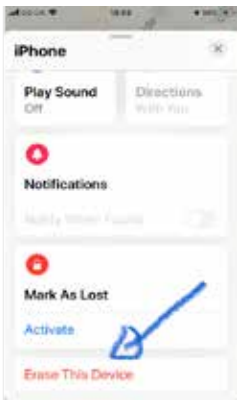
3.4.1 Paketleme, Taşıma ve Depolama

Bilgisayarlar ve ilgili cihazlar; sıcaklığa, neme, fiziksel şoka, statik elektriğe, manyetik kaynaklara ve hatta bazı operasyonel işlevlere (örneğin açma/kapamaya) karşı hassas olan narin elektronik aletlerdir. Bu nedenle elektronik delilleri paketlerken, taşırken ve depolarken özel önlemler alınmalıdır. Delil güvenlik zincirini muhafaza etmek için, paketleme, taşıma ve depolama işlemleri kaydedilmeli ve elkonulan eşyanın gözetimindeki veya durumundaki herhangi bir değişiklik ve zamanı not edilmelidir.

Uzman olmayan kişilerce yapılan işlemler elektronik delillerin zarar görmesine veya yok olmasına neden olabilir ve aşağıdaki önlemler alınmalıdır:

- **Paketleme:**
  - Toplanan tüm elektronik delillerin, paketleme öncesinde doğru şekilde belgelendiğinden ve etiketlendiğinden emin olun;
  - Mümkün oldukça, toplanan elektronik delilleri orijinal ambalajlarında taşıyın;
  - Orijinal ambalaj yoksa antistatik ambalaj (örneğin kağıt veya antistatik plastik torbalar) kullanın. Standart plastik poşetler gibi statik elektrik üretebilecek malzemeler kullanmaktan kaçının;

- Optik ortamlar ve bantlar gibi depolama ortamlarını katlamayın, bükmeyin veya çizmeyin;
- Depolama ortamlarının yüzeyine yapışkan etiketler yapıştırmayın. Depolama ortamlarını paketlemek için, mümkün oldukça kutular veya zarflar kullanın;
- Delil içeren tüm kapların uygun şekilde etiketlendiğinden emin olun;
- Birden fazla cihaz toplandıysa, her sistemi, bulunduğu gibi yeniden monte edilebilecek şekilde etiketleyin;
- Hücresel, mobil veya akıllı telefonları bulundukları güç durumunda (açık veya kapalı) bırakın;
- Cep telefonlarını veya akıllı telefonları, veri mesajlarının veya kilitleme/silme komutlarının cihazlar tarafından gönderilmesini veya alınmasını önlemek için Faraday izolasyon torbaları, radyo frekans geçirmez malzemeler gibi sinyal engelleyici malzemelere veya başka bir seçenek yoksa alüminyum folyoya sarılmış şekilde paketleyin. Yanlış ambalajlanması veya korumalı ambalajdan çıkarılması durumunda, cihaz veri mesajlarını gönderebilir ve alabilir hale gelir.
- Cihazları sinyal engelleme ambalajı içinde tutmanın pil ömrünü önemli ölçüde azaltabileceğini unutmayın. Pil seviyesinin düşük olduğu durumlarda, cihazı "uçuş moduna" almayı tercih edin veya cihazı taşınabilir bir güç kaynağına bağlayın.



- **Taşıma:**
  - Elektronik delilleri manyetik kaynaklardan uzak tutun. Elektronik delillere zarar verebilecek örnek nesneler arasında, radyo vericileri, hoparlör mıknatısları ve ısıtmalı koltuklar sayılabilir;
  - Ekipmanın şok ve darbelerden (yani mekanik hasardan), ısıdan ve nemden korunduğundan emin olun;
  - Bilgisayarların ve kaplarda paketlenmemiş diğer cihazların taşınmaları sırasında şok ve aşırı titreşimleri önleyecek şekilde sabitlendiğinden emin olun. Örneğin bilgisayarlar araç zeminine, monitörler ise ekranları aşağıya bakacak şekilde koltuk üzerine yerleştirilmeli ve emniyet kemeri ile sabitlenmelidir;

- Daha küçük ekipman/depolama ortamı parçalarının üzerine ağır nesneler **koymayın**;
- Mümkün olduğunca, elektronik delilleri uzun süreler boyunca araçlar içinde **bırakmayın**;
- Dijital delillerin taşınma işlemini belgeleyin ve taşınan tüm deliller için delil güvenlik zincirini muhafaza edin.

- **Depolama:**
  - Delillerin ilgili politikalara uygun şekilde envantere geçirildiğinden emin olun;
  - Delilleri aşırı sıcaklıklardan ve nemden uzak, güvenli bir alanda saklayın;
  - Manyetik kaynaklardan, nemden, tozdan ve diğer zararlı parçacıklardan veya kirleticilerden koruyun;
  - Aşağıdaki uygun imkanlara sahip yeterince güvenli bir depolama odası kullanın:
    - erişim denetimi;
    - yangından korunma ve yangın söndürme sistemleri (örneğin alarm, yangın söndürücüler, depolama alanında veya çevresinde sigara içilmemesi);
    - sıcaklık ve nem kontrolü; ve,
    - manyetik kaynaklara karşı korumalı (örneğin, yönlendirilmiş radyo cihazlardan izole edilmiş).
  - Herhangi bir yanıcı maddeyi (örneğin temizlik kimyasallarını veya kağıt yığınlarını) aynı odada veya civarında **tutmayın**;
  - Statik yüklerden kaçınmak için uygun zemin kaplaması kullanın;
  - Elektronik delilleri, özellikle tavan boyunca su boruları bulunan odalarda **saklamayın**;
  - Tarih, saat ve sistem yapılandırması gibi potansiyel delillerin, uzun süreli depolama sonucunda kaybolabileceğini unutmayın. Piller sınırlı bir ömre sahip olduğundan, arızalanmaları durumunda veri kaybı olabilir. Pillerle çalışan bir

cihaz (örneğin mobil cihaz veya PC/CMOS[42]) ile derhal ilgilenilmesi gerektiği konusunda ilgili personel bilgilendirilmelidir.

3.4.2 Bilgisayar Sistemi ve Elektronik Cihaz Toplama

Dizüstü bilgisayarlar, masaüstü bilgisayarlar, kule sistemler, modüler rafa monte edilmiş sistemler, mini bilgisayarlar ve merkezi işlem bilgisayarları da dahil olmak üzere birçok farklı türde bilgisayar sistemi vardır. Bunlar üzerinde, potansiyel deliller büyük çoğunlukla dahili (örneğin bellek, sabit diskler, flash bellek) ve harici (örneğin optik ortam, USB / Thunderbolt) depolama cihazlarında ve ortamlarında tutulan dosyalarda bulunur.

Kişisel bilgisayarlar (PC); harici depolama, ekranlar, klavyeler, yazıcılar, fareler ve diğer çevresel aygıtları bağlamak için çeşitli tür ve sayıda bağlantı noktasına (yani bu durumda USB gibi fiziksel bağlantı noktalarına) sahiptir. Cihazlar, bir PC'ye, ayrıca bir kablosuz (örneğin WLAN, Bluetooth, kızılötesi) bağlantı üzerinden de bağlanabilir.

PC'lerde genellikle aşağıdaki işletim sistemleri kullanılır: Microsoft Windows, Unix, Linux veya Apple MacOS. Bir bilgisayar sistemi bağımsız olabilir veya bir ağa bağlı olabilir. Bir bilgisayar ağında, genellikle kablosuz bir bağlantı sağlayabilen ek ağ bileşenleri (örneğin ağ kabloları, ağ yönlendiriciler, bağlantı kutuları ve anahtarlar) de bulunur.

Daha önce de gördüğümüz gibi, depolama ortamı ve diğer elektronik cihazlar her zaman bu kadar kolayca tanımlanamayabilir. Kol saatleri, mücevherler, anahtarlar, oyuncaklar vb. içinde gizlenmiş olabilirler.

Dijital depolama aygıtları genellikle bilgisayar sisteminin yakınında değil, ayrı bir odada veya hatta farklı bir binada depolanır. Bazı durumlarda, söz konusu medya özel kutular veya dolaplar (örneğin veri güvenliği kasaları) içinde kilitli de olabilir

Son olarak, aşağıdaki öğelerin de toplanması düşünülebilir ve bir bilgisayar sistemi incelenirken ilave bir yardım sağlayabilir:

- Donanım ve yazılım kılavuzları;

[42] Tamamlayıcı metal oksit yarı iletken (CMOS) pil, bir bilgisayarın başlatılmasını sağlayan BIOS'a (temel girdi çıktı sistemi) güç sağlamak için kullanılır.

- Parolaların veya diğer ilgili bilgilerin kaydedilmiş olabileceği notlar, günlükler, takvimler ve benzeri öğeler;
- Yazı izi geçmiş boş kağıt desteleri;
- Bilgisayarla ilgili kaynaklar;
- Bilgisayar çıktıları;
- İlgili fotoğraflar; ve

Bilgisayarla ilgili anahtarlar.

Aşağıdaki bölümde, bir bilgisayara elkonulmasına ilişkin gereken adımlar açıklanmaktadır. Başlangıç adımlarından bazıları önceki bölümlerde halihazırda açıklanmıştır.

Unutmayın:

- Olay yerini sürekli olarak **belgeleyin** ve yaptığınız tüm eylemleri ve eylemleriniz sonucunda monitörde, bilgisayarda, yazıcıda veya diğer cihazlarda gözlemlediğiniz tüm değişiklikleri kaydedin.
- **Potansiyel bir şüphelinin doğrulanmamış herhangi bir tavsiyesine uymayın**.
- Bir **bilgisayar ağı** ile karşılaşırsanız, yardım için kurumunuzdaki **bir adli bilişim uzmanına** veya kurumunuz tarafından belirlenen bir harici uzmana başvurun.
- Bazı cihazların bir **kablosuz** bağlantı (örneğin WLAN, Bluetooth, diğer kablosuz protokoller) üzerinden bağlı olabileceğine **unutmayın**;
- Herhangi bir **ağ bağlantısı** varsa, bilgisayar sistemine elkoyma sırasında (yani, her açıldığında ve ağ bağlantısının erişimi dahilinde) erişilebileceğini ve değişiklik yapılabileceğini **unutmayın**.

Olay yerini güvence altına almak ve ekipmana elkoymak için izlenecek adımlar:

- Alanda aşağıdaki bileşenleri/öğeleri arayın:
  - bilgisayar sistem bileşenleri;
  - dijital depolama ortamı;
  - ilave bileşenler;
  - diğer elektronik cihazlar; ve,
  - elektronik olmayan deliller.
- Ön görüşmeleri (ifade alma işlemlerini) yapın;
- Bilgisayar sistemini gözlemleyin ve açık mı kapalı mı olduğunu belirleyin **(aşağıya bakın);**
- Tüm bağlantıları ve bileşenleri belgeleyin ve her bağlantıyı ve cihazı etiketleyin:
  - Bilgisayara giren/bilgisayardan çıkan bağlantıların ve ilgili kabloların fotoğrafını çekin ve/veya şemasını çizin;
  - Delilleri kurumunuzun prosedürlerine göre kaydedin.
- Ekipmanı dikkatlice çıkarın ve tüm seri numaralarını veya kimlik numaralarını kaydedin. Paketlemeden ve çıkarmadan önce ekipmanın soğumasını bekleyin.
- Taşıma gerekiyorsa, bileşenleri paketleyin.

Ek A ve B'deki çizelgeler, elkonulan cihazlar ile ilgili olarak izlenmesi kolay bir akış şeması sağlamaktadır. Kullanıcılar, bu çizelgelerde belirtilen prosedürlerin tüm ulusal mevzuata veya usule ilişkin kılavuz ilkelere uygun olmasını sağlamaktan sorumludur.

3.4.3 Güç Durumunu (Açık/Kapalı) Kontrol Etme

Bu bölümde, bilgisayar ekipmanına ve depolama ortamına elkonulması ile ilgili bazı tavsiyeler sunulmaktadır.

Bilgisayar sisteminin açık mı kapalı mı olduğunu belirleyin.

Çoğu bilgisayarda, bilgisayarın açık olduğunu gösteren durum ışıkları bulunur. Fan sesi duyuluyorsa, sistem muhtemelen açıktır. Bilgisayar kasası sıcaksa, aynı zamanda bu da açık olduğunu veya yakın zamanda kapatıldığını gösterebilir.

Lütfen dikkat: Bazı taşınabilir cihazlar, kapağı açıldığında etkin hale gelir.

Mümkünse her zaman taşınabilir bilgisayarların ve cihazların pilini çıkarmayı düşünün.

Taşınabilir (örneğin dizüstü) bilgisayarlarda genellikle adaptöre ek olarak bir pil bulunur. Bu tür cihazların pilleri, taşınabilir bilgisayar bir güç kaynağına bağlandığında şarj olur ve tam olarak şarj edilmişse pilin bitmesi birkaç saat sürebilir. Bekleme modundayken bir taşınabilir bilgisayarın açık mı kapalı mı olduğunu belirlemek genellikle zordur.

Kapalı gibi görünen bir bilgisayar sistemi uyku modunda olabilir. Eğer öyleyse, uzaktan etkinleştirilip erişilebilir ve dosyalar değiştirilmesi veya silinmesi mümkündür.

Bazı ekran koruyucular bilgisayarın kapalı olduğu izlenimini verir. Monitörü gözlemleyin ve bilgisayarın açık mı, kapalı mı, yoksa uyku modunda mı olduğunu belirlemeye çalışın.

Aşağıdaki durumlardan biriyle karşılaşabilirsiniz:

Durum 1: Monitör açık ve yapılan iş ve/veya masaüstü görünüyor.

- Müdahale edildiği sırada monitöre ilişkin ayrıntıları belgeleyin
- Aşağıda açıklanan "Düzenek B" adımına ilerleyin.

Durum 2: Ekran açık ve boş ekran (uyku modu) veya ekran koruyucu (örneğin bir resim) görünüyor.

- Fareyi hafifçe hareket ettirin (düğmelere basmadan). Ekran görüntüsü değişmeli ve yapılan işi göstermeli veya bir şifre istemelidir.
- Eğer farenin hareket ettirilmesi ekranda bir değişikliğe neden olmazsa, herhangi bir tuşa basmayın veya fareyle başka bir işlem yapmayın.
- Müdahale edildiği sırada monitöre ilişkin ayrıntıları belgeleyin
- Aşağıda açıklanan "Düzenek B" adımına ilerleyin.

Durum 3: Monitör kapalı.

- "Kapalı" durumda olduğunu not edin.
- Monitörü açın, ardından monitörün yukarıda açıklanan 1. veya 2. durumda olup olmadığını belirleyin ve ona göre ilgili adımları izleyin.

Bilgisayarın açık mı kapalı mı olduğunu belirledikten sonra aşağıdakilerden birini yapmanız gerekecektir:

Düzenek A: Sistemin kapalı olduğunu belirlediniz; **açmayın**!

- Elektrik kablosunu hedef ekipmandan çıkarın (duvardaki prizden **kapatmayın**) ve bu işlemi yaptığınız zamanı kaydedin.
- Eğer taşınabilir bir cihazla uğraşıyorsanız, mümkünse pili de çıkarın. Varsa ilave pilleri çıkarın (bazı taşınabilir cihazların çok amaçlı kullanılan bölmesinde optik sürücü yerine ikinci bir pil bulunur).

Bilgisayar sistemi kapalıysa, başlatma işlemi bilgisayar verilerini değiştireceği ve delilleri potansiyel olarak yok edeceği için kapalı durumda bırakın.

Düzenek B: Sistemin açık olduğunu belirlediniz; **kapatmayın**!

- Bir uzmana ulaşmaya çalışın:
  - Bir uzmana ulaşabilirseniz, tavsiyelerine uyun;
  - Bir uzmana ulaşamazsanız, bir sonraki talimatla devam edin.
- Klavyeye veya diğer giriş cihazlarına **dokunmayın**.
- Bölüm 3.5'te açıklanan adımlarla devam edin.

Unutmayın: Elektrik kablosunun bilgisayar sisteminden çıkarılması, çalışmakta olan tüm programları etkileyecek ve o sırada bilgisayarın RAM'inde saklanan (parolalar gibi önemli veriler de dahil olmak üzere) tüm veriler kaybolacaktır. Buna; her tür İnternet bağlantısı, yazdırma işlemi, kaydedilmemiş belgeler, özel tarama geçmişi ve şifreli birimlere/taşıyıcılara erişim de dahildir.

Unutmayın: Bir sistem açıldığında, şüphelinin emniyete alınması ve sigorta kutularından, güç anahtarlarından ve mobil iletişim cihazlarından uzak tutulması çok önemlidir. Sadece şüphelinin sigorta kutusuna ulaşabilmesi veya uzaktan kontrol edilebilir bir güç adaptörüne sinyal gönderebilmesi yüzünden arama sırasında tam disk şifrelemeli çalışır durumdaki sistemlerin kapatıldığı durumlarla karşılaşılmıştır.

Düzenek C: Sistemin açık mı yoksa kapalı mı olduğunu belirleyemediniz.

- Kapalı olduğunu varsayın. Açma/kapama tuşuna/anahtarına **basmayın**.
- Elektrik kablosunu hedef ekipmandan çıkarın (duvardaki prizden **kapatmayın**) ve bu işlemi yaptığınız zamanı kaydedin.
- Eğer taşınabilir bir cihazla uğraşıyorsanız, ayrıca pilini de çıkarın. Varsa ilave pilleri de çıkarın (bazı taşınabilir cihazların çok amaçlı kullanılan bölmesinde disket sürücüsü veya CD sürücüsü yerine ikinci bir pil bulunur).

3.4.4 Elektronik Cihazlar İçin Genel Elkoyma Talimatları

Başka herhangi bir elektronik cihaza elkonulurken aşağıdakiler göz önünde bulundurulmalıdır:

- Cihaz açıksa kapatmayın çünkü kapama işlemi bir kilit mekanizmasını etkinleştirebilir:
  - Ekranın (varsa) fotoğrafını çekin ve görüntülenen bilgileri kaydedin;
  - Cihazda bir "uçuş modu" veya "çevrimdışı mod" varsa, verilerin uzaktan kilitlenmesini veya silinmesini önlemek için cihazı bu moda geçirin;
  - Tüm güç kaynağı kablolarını çıkarın (genellikle bunları duvardaki prizden değil de hedef ekipmandan çıkarmak daha iyidir);
  - Dahili belleğe veya herhangi bir depolama ortamına erişmeye çalışmayın.
- Kapalıysa açmayın çünkü bu, (bilgisayar sistemlerinde de olduğu gibi) delilleri değiştirebilir/yok edebilir;
- Ağ ve elektrik kablolarını cihazdan ziyade duvardan çıkarın ve ardından belgeleyin ve etiketleyin;

- Önemli bilgileri toplayın/kaydedin:
  - Varsa kılavuzları ve diğer talimatları toplayın;
  - Cihazlara erişim kodlarını (örneğin PIN/PUK numaralarını) içeren belgeleri toplayın;
  - İlgili verileri (örneğin telefon numarasını) kaydedin.
- Genel paketleme, taşıma ve saklama talimatları için lütfen yukarıdaki bilgilere bakın:
  - Piller sınırlı bir ömre sahip olduğundan, arızalanmaları durumunda veri kaybı olabilir. Bu nedenle, ilgili personel, pille çalışan bir telefon ile derhal ilgilenilmesi gerektiği konusunda bilgilendirilmelidir;
  - Elkoymanın ardından cihazı mümkün olan en kısa sürede bir uzmana teslim edin. Mobil cihazlar (örneğin akıllı telefonlar, tabletler) söz konusu olduğunda, bu hemen yapılmalıdır.

Unutmayın: Elkoymanın ardından cihaz en kısa sürede bir uzmana teslim edilmelidir. Cep telefonları söz konusu olduğunda, bu derhal yapılmalıdır.

3.4.5 Dijital Depolama Ortamı

Aşağıdaki ortamlar genellikle bilgisayarın yakınında değil, ayrı bir odada veya farklı bir binada saklanır (yukarıda bölüm 3.4.2'de belirtildiği gibi, bazı durumlarda ortamlar, veri güvenlik dolapları adı verilen özel kutularda kilitlenebilir) :

- Yedekleme ortamları (örneğin manyetik bantlar);
- Optik ortamlar;
- Bilgisayara bağlı olmayan HDD'ler ve SSD'ler;
- PC kartları;
- Manyetik şeritli kart;
- Hafıza kartları;
- USB bellek kalemleri/anahtarları/çubukları;
- Dongle'lar;

Genel elkoyma, paketleme, taşıma ve depolama talimatları için lütfen yukarıdaki bilgilere bakın.

3.4.6 Çevre Birimleri ve Ek Bileşenler

Yukarıda belirtildiği gibi, bir bilgisayar sistemi aşağıdakiler gibi bazı ek bileşenler içerebilir:

- Sürücü çoğaltıcılar;
- MP3 çalarlar;
- Akıllı kartlar ve akıllı kart okuyucular;

- Yazıcılar;
- Tarayıcılar;
- Bağlantı terminalleri;
- Bağlantı noktası çoğaltıcılar;
- PC kartları ve PC kartı okuyucular;
- Web kameraları (dijital kameralar) ve mikrofonlar;
- Kablosuz cihazlar;
  - Bluetooth etkinleştiren cihazlar (örneğin harici çevre birimleri için Bluetooth USB dongle'ları); ve,
  - Bluetooth özellikli cihazlar (örneğin kulaklıklar, PDA'lar, dizüstü bilgisayarlar, telefonlar, GPS alıcıları).

Unutmayın: Bazı bileşenler, farklı bir işlevi varmış (örneğin kalem, saat, mücevher) gibi görünebilir.

Genel elkoyma, paketleme, taşıma ve depolama talimatları için lütfen yukarıdaki bilgilere bakın.

3.4.6.1 *Akıllı kartlar ve manyetik şeritli kartlar*

Akıllı kart; bir parasal değeri, şifreleme anahtarını veya kimlik doğrulama bilgilerini (parola), dijital sertifikayı veya diğer bilgileri depolayabilen bir mikroişlemci (yani bir "çip". Bazen bir çip kartı olarak da adlandırılır) içeren küçük bir elde taşınır cihazdır. Bazı akıllı kartlar, aynı zamanda bir işletim sistemine (yani bir akıllı kart işletim sistemine) sahip oldukları için aslında küçük bilgisayarlardır.

Akıllı kartlar farklı amaçlar ve uygulamalar için kullanılabilir, örneğin:

- Kısıtlı alanlara/binalara/odalara fiziksel erişim sağlayan anahtar kartlar olarak;
- Bilgisayarlar, programlar veya işlevler için erişim kontrolü sağlamak için (örneğin bir şifreleme anahtarı olarak);
- ATM'lerden nakit çekme imkanı tanımak için;
- Elektronik cüzdan/cüzdan olarak kullanılmak üzere (örneğin perakende mağazalarındaki ödemeler için);
- Marka müşterisi kartı veya banka kartı olarak;
- Sosyal güvenlik kartı veya resmi kimlik kartı olarak;
- Belirli devlet hizmetlerine erişim yetkisi olarak;
- Dijital imza oluşturmak için;
- Ankesörlü telefon kartı olarak; veya,
- Kişisel verileri, adresleri, erişim kodlarını başka bir şekilde saklamak için.

Bu çeşitli kullanımları ve içerebileceği bilgiler nedeniyle bir akıllı kart, bir bilgisayar sistemine benzer şekilde potansiyel deliller barındırabilir.

Uluslararası standartlara göre bir akıllı kart, 85,6 x 54 x 0,76 mm (yani "ATM kartı boyutu" olarak adlandırılan ID-1 formatında) olmalıdır ve kartın ön tarafında bir elektrik temas plakası olmalıdır. Ayrıca genellikle akıllı kartların arkasında bir manyetik şerit bulunur.

Başka çipli kart standartları da bulunmaktadır. Örneğin, cep telefonlarında kullanılan ID-0/1FF formatı (tam boyutlu SIM kart) (25 x 15 x 0.76 mm boyutunda) ve ondan sonra çıkan 2FF (Mini-SIM), 3FF (Mikro-SIM), 4FF (Nano-SIM) ve eSIM (Cihaza lehimlenmiş halde olan Gömülü SIM).

USB belirteçler[43] hem bir çip (akıllı karttaki çip ile aynı standartlara dayalıdır), hem de çipli kart okuyucu işlevselliğini içerir. Bu, dijital hizmetlerin alınması için kullanılan iki aşamalı kimlik doğrulama açısından giderek daha da popüler hale geldiklerini gösterir.

Temas plakası yerine indüksiyon teknolojisi kullanan ve temassız olarak adlandırılan bazı akıllı kartlar mevcuttur. Bu kartlarda, kart okuyucu ile fiziksel temas gerekmemekte, sadece okuyucu cihazın yakınına yaklaştırılması gerekmektedir. Aynı zamanda bir dahili pili, küçük bir LCD ekranı ve bir entegre tuş takımı olan "Süper" akıllı kartlar da geliştirilmiştir. Bu kartlar önemli ölçüde geliştirilmiş bir güvenlik düzeyine sahiptir.

Çoğu akıllı kart verisi ve işlevi genellikle (kişisel kimlik numarası veya PIN numarası olarak adlandırılan) gizli bir kişisel kodla korunur ve bilgisayar klavyesi üzerinde, kart okuyucu klavyesi üzerinde (veya süper akıllı kartın kendisi üzerinde) doğru kod girildikten sonra karttaki veriler erişilebilir hale gelir.

Akıllı kartlar üzerinde yapılacak işlemlere ilişkin bazı kurallar vardır:

- Katlamayın;
- Aşırı sıcaklıklara maruz bırakmayın;
- Elektrik temas plakasına elle dokunmayın;
- Çiziklere, sıvılara, manyetik etkilere vb. karşı koruyun;
- PIN numarasını bulmaya çalışın (kartla birlikte saklanıp saklanmadığına bakın veya güvenilir kullanıcıya/kullanıcılara sorun).

- Potansiyel bir şüpheli size PIN numarasını söylediğini iddia etse bile, karttaki verilere/işlevlere erişmeye çalışmayın. Birkaç kez yanlış PIN numarası girilmesi, geri alınamaz veri kaybına ve kartın bloke olmasına neden olabilir (bazı durumlarda, kişisel bloke açma anahtarı veya PUK adı verilen başka bir gizli kişisel kodla kartın blokesini kaldırmak mümkündür).
- Kart üzerine yazılmış olan bilgileri (örneğin kart sahibi kimliği, hesap numaraları, kredi kartı şirketleri, iş bağlantıları vb.) fotoğraflayın/not edin/kopyalayın.
- Verilerin temassız olarak değiştirilmesini önlemek için Radyo Frekansı Tanımla-

[43] Bilişim alanında bir belirteç, belirli bir eylemin yapılmasına imkan tanıyan bir şey anlamına gelir. Çoğu zaman, korunan bir sisteme veya programa veya bir tür bilgisayar hizmetine elektronik erişim sağlayan fiziksel bir nesne olacaktır.

mayı (RFID) engelleyen kart muhafazaları kullanın;

- Varsa, bulunan akıllı kart okuyuculara da elkoyun.

3.4.6.2 *Manyetik şerit okuyucular*

Manyetik şerit okuyucular (örneğin kredi kartı kopyalayıcılar) plastik kartların üzerindeki manyetik şeritte bulunan bilgileri okurlar. Manyetik şerit üzerinde bulunan potansiyel deliller şunları içerir:

- Kart sahibi bilgileri;
- Kartın son kullanma tarihi ve kredi kartı numaraları; ve,
- Güvenlik bilgileri.

Genel elkoyma, paketleme, taşıma ve depolama talimatları için lütfen yukarıdaki bilgilere bakın.

3.4.6.3 *Faks makineleri*

Faks makinesi, görüntüleri ve metinleri tarayıp telefon hattı üzerinden göndermek için kullanılan bir cihazdır. Bu işlevsellik bilgisayarlar için de mevcuttur (örneğin faks/modem PC kartları). Faks makineleri aşağıdaki delilleri içerebilir:

- Film kartuşu;
- Önceden programlanmış telefon numaraları (yani hızlı arama listeleri);
- İletilen ve alınan belgelere ilişkin geçmiş bilgisi;
- Çok sayfalı giden faksların daha sonra taranmasına, saklanmasına ve gönderilmesine veya gelen faksların saklanmasına ve daha sonra yazıcıya gönderilmesine imkan tanıyan bellek;
- Faks iletim protokolü (yani gönderme/alma günlüğü);
- Başlık; ve,
- Saat ayarı.

Genel elkoyma, paketleme, taşıma ve depolama talimatları için lütfen yukarıdaki bilgilere de bakın.

3.4.6.4 *Yazıcılar*

Yazıcılar; kullanım günlüklerini, saat ve tarih bilgilerini tutabilir ve bir ağa bağlı olmaları halinde ağ kimlik bilgilerini depolayabilirler. Buna ek olarak, bir çıktıdaki benzersiz özellikler, belirli bir yazıcının tanımlanmasını sağlayabilir.

Bir yazıcıdan elde edilen potansiyel deliller şunları içerir:

- Dokümanlar;
- Sabit disk, anlık bellek;

- Mürekkep kartuşları;
- Ağ kimliği/bilgileri;
- Silindir üzerine geçmiş görüntüler;
- Saat ve tarih damgası; ve,
- Kullanıcı kullanım kütüğü.

Genel elkoyma, paketleme, taşıma ve depolama talimatları için lütfen yukarıdaki bilgilere bakın.

3.4.6.5 *Tarayıcılar*

Tarayıcılar, metin belgelerini ve basılı resimleri tarayan ve bunları dijital formatta kaydeden dijital cihazlardır. Cihazın kendisi delil olabilir. Buna ek olarak, taranan suretlerde çoğaltılan tarayıcı kusurları, belirli bir tarayıcının yasa dışı bir eylemde kullanılan bir cihaz olarak tanımlanmasına imkan tanıyabilir.

Genel elkoyma, paketleme, taşıma ve depolama talimatları için lütfen yukarıdaki bilgilere bakın.

3.4.6.6 *Fotokopi makineleri (kopya makineleri)*

Bazı fotokopi makineleri, kullanıcı erişim kayıtlarını ve yapılan tüm kopyalara ait bir geçmiş verisi tutarlar. "Bir kez tara/birçok kez yazdır" özelliğine sahip fotokopi makineleri, taranan belgeyi daha sonra yazdırmak üzere belleğe kaydederler. Fotokopi makinelerinden elde edilen potansiyel deliller, belgeleri, saat ve tarih damgasını ve kullanım günlüğünü içerir.

Genel elkoyma, paketleme, taşıma ve depolama talimatları için lütfen yukarıdaki bilgilere bakın.

3.4.6.7 *Çok fonksiyonlu makineler*

Önceki dört paragrafta açıklanan cihazlar (örneğin bir fotokopi makinesi, bir tarayıcı, bir faks makinesi ve bir (ağ) yazıcısı) tek bir cihaz içinde birleştirilebilir. Fiziksel olarak ayrılmış birkaç cihaz da, bir ağ üzerinden bağlandıklarında, çok fonksiyonlu bir makine olarak birlikte çalışabilirler.

3.4.7 Telefonlar ve Mobil Cihazlar

Telefon, bir el terminali olup;

- Ya kendi başına (cep telefonlarındaki gibi);
- Veya bir uzak baz istasyonuyla (kablosuz);
- Ya da doğrudan karasal sabit hat sistemine bağlı olarak kullanılabilir.

Bir cep telefonunda tipik olarak (örneğin dijital fotoğraf çekme yeteneği gibi) bazı ilave işlevler de bulunur. Modern cep telefonlarında genellikle, kullanıcının tipik olarak e-posta alma ve gönderme, mesajlar, İnternet'e erişme, oyun oynama vb. de dahil olmak üzere geleneksel bilgisayar sistemleriyle ilişkilendirilen görevleri yerine getirmelerine imkan tanıyan (iOS, Android gibi) bir işletim sistemi bulunur. Bu tür genişletilmiş işlevselliğe sahip cep telefonlarına akıllı telefon denmektedir.

Bir telefon gücünü dahili bir pilden, elektrik bağlantısı soketinden veya doğrudan telefon sisteminden alabilir. Bir el terminalinden diğerine çift yönlü iletişim, karasal sabit hatlar, radyo iletimi, hücresel sistemler veya ilgili sistemlerin bir kombinasyonu kullanılarak sağlanır. Birçok telefon; isimleri, telefon numaralarını ve arayan tanımlama bilgilerini saklayabilir. Birçok cep telefonu aynı zamanda isimleri, adresleri, takvim bilgilerini, gelen aramalarla ilgili ayrıntıları saklayabilir, e-posta alabilir, metin gönderebilir, ses kaydedici olarak ve İnternete erişmek için kullanılabilir (böylece İnternete erişim verilerini içerir). Birçok cep telefonuna erişim için PIN numaraları, parolalar, biyometrik kimlik doğrulama veya diğer erişim kodları gerekecektir.

Tablet cihazlar akıllı telefonlara çok benzer ancak daha büyük bir ekrana sahiptir. İşletim sistemlerinin cep telefonu sürümlerine dayalı olan kendi işletim sistemleriyle gelirler. Akıllı telefonlar gibi onlar da neredeyse sonsuz çeşitlilikte işlev sunarlar ve kullanıcının kendi uygulamalarını (mobil uygulamaları) yüklemesine imkan tanırlar.

Genel elkoyma, paketleme, taşıma ve depolama talimatları için lütfen yukarıdaki bilgilere bakın (bölüm 3.4.1). Bu cihazların tipik olarak WiFi veya mobil veri bağlantıları ile bağlı olduklarını ve verileri uzaktan kilitleme, değiştirme ve hatta güvenli bir şekilde silme işlevleri sunabileceğini özellikle hatırlayın. Ayrıca şu bölümlere de bakınız: **Error! Reference source not found.**

3.4.7.1 *Telesekreterler*

Telesekreter, bir telefonun parçası olan veya bir telefon ile sabit hat bağlantısı arasına bağlanan bir elektronik cihazdır. Eski modellerde mikro manyetik kasetler kullanılırken, modern makinelerde bir elektronik (dijital) kayıt sistemi kullanılmaktadır. Günümüzde telesekreterler çoğu zaman telefonlara, akıllı telefonlara veya İnternet yönlendiricilere gömülü işlevlerdir. Bir telesekreter, aranan taraf müsait olmadığında veya bir aramayı cevaplamamayı tercih ettiğinde arayandan gelen sesli mesajları kaydeder. Genellikle telefon sahibi tarafından kaydedilen ve arayanın mesaj bırakmasını isteyen bir mesajı dinletir.

Telesekreterler sesli mesajları ve bazı durumlarda mesajların ne zaman bırakıldığına ilişkin saat ve tarih bilgilerini saklayabilir. Ayrıca başka ses kayıtları da içerebilirler.

Bir telesekreterden elde edilen olası deliller şunları içerebilir:

- Arayan tanımlama bilgileri;
- Silinen mesajlar;
- Arayan son numara;
- Sesli bilgi notları;
- Telefon numaraları ve isimler; ve,

- Mikro kasetler.

Genel elkoyma, paketleme, taşıma ve depolama talimatları için lütfen yukarıdaki bilgilere de bakın.

3.4.7.2 *Çağrı cihazları*

Çağrı cihazı, sayısal (örneğin telefon numaraları) ve alfanümerik (genellikle e-posta da dahil metin) mesajları göndermek ve/veya almak için kullanılabilen bir cihazdır. Çağrı cihazları günümüzde çok yaygın değildir, ancak yine de örneğin tıp sektöründe kullanılabilir.

Günümüzde akıllı telefonlardaki mesajlaşma uygulamaları ve diğer uygulamalar, çağrı cihazlarının yerini almaktadır.

Genel elkoyma, paketleme, taşıma ve depolama talimatları için lütfen yukarıdaki bilgilere bakın.

3.4.7.3 *Giyilebilir Teknolojiler*

Giyilebilir cihazlar üzerinde mesaj ve rehber, randevu, takvim, kullanıcı aktivitesi, coğrafi veri ve notlar gibi ilave bilgiler saklanabilmektedir. Ayrıca bir akıllı telefon veya bilgisayar ile bilgi senkronize etme yeteneğine de sahiptirler. Olası deliller arasında;

- Adres defteri;
- Randevu takvimleri;
- E-posta;
- Konum bilgileri;
- Aktiviteler;
- Notlar ve,
- Telefon numaraları sayılabilir.

Bazı giyilebilir teknolojilerde de anlık bellek, akıllı çubuk hatta kamera gibi depolama aygıtları bulunabilmektedir. Akıllı saat ve sağlık/spor takip uygulamaları giyilebilir teknolojilerin en yaygın olanlarıdır.

Genel elkoyma, paketleme, taşıma ve depolama talimatları için lütfen yukarıdaki bilgilere bakın.

3.4.8 Dijital Kameralar

Daha önce de açıklandığı gibi dijital kamera, resim ve video çekmek için kullanılan bir cihazdır. Dahili bir belleğe, ilgili depolama ortamına ve resimleri ve videoları bilgisayarlara aktarabilen dönüştürme donanımına sahiptir.

Olası deliller aşağıdakilerden elde edilebilir:

- Kameranın kendisinden;
- Resimler (Exif-Meta veriler[44] ile birlikte);
- Çıkarılabilir hafıza kartları;
- Ses;
- Saat ve tarih damgası; ve,
- Video.

Genel elkoyma, paketleme, taşıma ve depolama talimatları için lütfen yukarıdaki bilgilere de bakın.

3.4.9 GPS Cihazları ve Diğer Uydu Konumlandırma Cihazları

Küresel Konumlandırma Sistemleri (GPS) cihazları; hedef bilgileri, yol noktaları ve rotalar da dahil olmak üzere önceki konumlar ve seyahat günlükleri hakkında bilgi sağlayabilir. Bazı GPS cihazları bu bilgileri otomatik olarak kaydeder. Bir GPS cihazında bulunacak olası deliller aşağıdaki gibi olabilir:

- Ev konumu;
- Önceki varış noktaları;
- Önemli noktalar;
- Seyahat günlükleri;
- İz sürme/güzergah bilgileri;
- Yol noktası koordinatları; ve,
- Yol noktası adı.

Genel elkoyma, paketleme, taşıma ve depolama talimatları için lütfen yukarıdaki bilgilere bakın.

3.4.10 Otomotiv Sistemleri

Sensörlerden gelen veriler ile aktüatör kontrolleri araç-içi entegre sistemler tarafından kaydedilir. Bu bilgiler ışığındaysa seyir durumuna (navigasyon) ilişkin soruşturma açısından faydalı olabilecek önemli ipuçları elde edilebilmektedir. Olası deliller arasında;

- Tarih damgalı seyir verileri (hız, yönler, rakım, coğrafi konum, GPS düzeltmeleri, vb.);
- Kapı veya bagaj açma/kapama verileri;
- Kullanılan farklı koltuk ayarları;
- Koltuk kullanım verisi;
- Çağrılar, rehber, gelen-giden mesajlar, bağlı cihazlardan kopyalanan rehber verileri;

[44] Paylaşılabilir Görüntü Dosyası Formatı (EXIF), resimler, ses, kameralar ve tarayıcılar vb. için standart bir formattır. EXIF kullanan cihazlar, genellikle resimleri, resmin çekilmesi ile ilgili belirli verilerle birlikte etiketler. Birçok modern cihaz ayrıca ("coğrafi etiketleme" olarak adlandırılan) GPS konum verilerini de ekler.

Toplanan bilgiler, soruşturma zaman çizelgesini iyileştirebilir ve hatta arabanın kullanıcısı ve eylemleri hakkında göstergeler sağlayabilir.

Aramalar sırasında arabalar ve diğer araçlar, diğer olay yerleri için geçerli olanlarla aynı dikkat ve ilkeler ile ele alınmalıdır. Otomotiv sistemlerine elkonulurken bölüm **Error! Reference source not found.**'de verilen talimatlara ek olarak aşağıdakiler de dikkate alınmalıdır:

- Bir aracın elektronik sistemleri üzerindeki verilerin kurcalanmasını önlemek için olay yerindeki tüm personelin kendi cihazlarındaki WIFI ve Bluetooth işlevlerini devre dışı bırakması tavsiye edilir. Aksi takdirde, cihazları sistemlere bağlanabilir ve verileri değiştirebilir (örneğin yeni günlük girişleri oluşturabilir, eski günlük girdilerinin üzerine yazabilir);
- Elektronik sistemler güçlerini tipik olarak araçtaki aküden almaktadır. Güç durumuna bağlı olarak, geçici veri kaybını önlemek için ekranda görünen verilerin belgelenmesine ve araba sistemlerinin güç tasarrufu moduna alınmasına öncelik verilebilir;
- Mümkünse bir uzman, aracın sistemleri hakkındaki bilgileri çalışır durumdayken analiz edebilir, çünkü sistemler kapatıldığında bazı veriler kaybolabilir;
- Bir araçtaki elektronik sistemler harici olarak, örneğin mobil ağlara bağlı olabilir. Bazı sistemler uzaktan kontrol edilebilir. Bu nedenle araç izole edilmelidir;
- Bir araçtan bilişim sistemlerini fiziksel olarak çıkarma işlemini sadece kalifiye personel yapmalıdır. Çıkarılan bileşenlerin hasarlı olduğu kabul edilmeli ve bu nedenle gerçek trafikte asla yeniden kullanılmamalıdır;

3.4.11 Nesnelerin İnterneti (IoT) ve Akıllı Ev Cihazları

Çoğu IoT cihazı, en azından ne zaman kullanıldığı hakkında bilgi sağlayacaktır. Mevcut IoT kaynaklarından veri derlemek suretiyle davalara saat ve tarih eklenebilmekte, davaların belgelenmesine kayda değer katkı sağlanabilmektedir. Kimi durumlarda bir zamandizin sayesinde olayların akışı ve oluş sırası daha iyi anlaşılabilmekte, görgü tanıklığı geçerli/geçersiz kılınabilmekte veya kimi isimler sanık listesinden düşürülebilmektedir.

IoT/akıllı ev cihazlarına elkonulurken bölüm **Error! Reference source not found.**4'de verilen talimatlara ek olarak aşağıdakiler de dikkate alınmalıdır:

- Bazı IoT cihazları kendi korumasız WiFi erişim noktalarını oluşturduğundan veya Bluetooth üzerinden bağlantı kurmaya çalıştığından, olay yerindeki tüm personelin kendi cihazlarındaki WiFi ve Bluetooth işlevlerini devre dışı bırakması tavsiye edilir. Aksi takdirde, cihazları korumasız ağlara bağlanabilir ve verileri değiştirebilir (örneğin yeni günlük girişleri oluşturabilir, eski günlük girdilerinin üzerine yazabilir) veya hatta bazı işlemleri bile tetikleyebilir;
- Tüm IoT cihazları manuel olarak tanımlamak zordur. Mevzuat izin veriyorsa, bir ağ tarayıcısı ve/veya spektrum analiz cihazı, bu tür cihazların bulunmasına yardım edebilir. Farklı IoT standartlarının farklı bantlarda farklı frekanslar kullandığına dikkat edilmelidir;

- Çoğu IoT cihazı kapatıldığında verilerinin bir kısmını kaybettiğinden, bir uzman IoT hakkındaki bilgileri mümkünse cihaz çalışırken analiz etmelidir. Yapılan tüm işlemler ayrıntılı olarak belgelenmelidir;
- IoT cihazları büyük olasılıkla harici olarak bağlı ve erişilebilir durumdadır. Örneğin verilerinin çalışır haldeyken alınmasından sonra elektriklerinin kesilmesi suretiyle ağlarından izole edilmeleri gerekir.
- Cihazları; diğer eşyalardan, değerli eşyalardan veya belgesel delillerden ayrı olarak, plastik malzemelerden ziyade karton kutular veya kağıt torbalar içinde paketleyin;

3.4.12 Kripto Paralara İlişkin Veriler

Kripto paralara elkonulacağı durumlarda, soruşturma sırasındaki çoğu adımda ve aynı zamanda arama sırasında da bir uzmanın sürece dahil edilmesi önemlidir. Kripto paralara elkonulması, ancak sanal cüzdana erişilebilirse mümkündür.

Bu nedenle bilgisayar sistemleri, mobil cihazlar ve diğer elektronik delillere elkonulmalı ve buna ek olarak metal levhalar veya kurtarma ibareleri bulunan kağıtlar gibi diğer eşyalar da aranmalıdır. 12, 18 veya 24 rastgele İngilizce kelimenin herhangi bir kombinasyonunun, yüksek miktarda bir mali suç gelirini tutabilecek bir kripto para cüzdanı için potansiyel bir kurtarma ibaresi olduğu düşünülebilir. Bu kurtarma ibarelerinin yanı sıra, kimlik bilgilerini depolayabilecek veya iki faktörlü kimlik doğrulama bileşeni olarak gerekli olabilecek diğer cihazlara da elkonacaktır.

Cüzdanlara her yerden erişilebildiği için şüpheliyi (ve yakınlarını) cep telefonu gibi herhangi bir iletişim cihazından derhal ayırmak önemlidir.

Bir devlet cüzdanına erişimi olan daha deneyimli müfettişler, aşağıdaki tavsiyeyi izleyerek bir arama sırasında kripto paralara elkoymaya çalışabilir:

- En kolay durum, ya şüphelinin cüzdanının açık olduğu ya da kurtarma ibaresinin (örneğin bir ev araması sırasında) bulunduğu durumdur. Bu durumda müfettiş, fonları devlet kontrolündeki bir cüzdana aktararak bu varlıkları güvence altına almalıdır.
- Şüphelinin cüzdanı kilitliyse ancak e-posta hesabına erişilebiliyorsa, cüzdana erişim sağlamak için cüzdanın şifresi değiştirilebilir. Bu durumda müfettişin bir yasal izne sahip olması gerekir. Çoğu durumda, bir çevrimiçi cüzdan oluşturulurken, kullanıcıyı doğrulamak ve oturum açma girişimlerine izin vermek için bir e-posta hesabı gereklidir.
- Cüzdan kimliği de doğrulama e-postasının alt kısmında belirtilmektedir.
- Bağlı e-posta hesabına erişmek için (yasal çerçeveye bağlı olarak) sulh hâkimi/hâkim/savcı onayı alınması gereklidir.

Tüm bu bilgilere sahip olarak müfettiş cüzdanı devralabilir ve sanal paraları devlet kontrolündeki bir cüzdana aktarabilir. Avrupa Konseyi'nin "Kripto Paralara Elkoyma Kılavuzunda" daha fazla yönlendirme bulunabilir (bkz. Bölüm 1.4).

3.4.13 Dronlar/İnsansız Hava Araçları

Bu bölüm sadece uçmayan bir drona elkoyma adımlarını kapsar. Uçan nesneler ile ilgili talimatlar ve dronlar hakkında daha derinlemesine bilgi için lütfen Interpol'ün "İlk Müdahale Görevlileri ve Adli Bilişim Uygulayıcıları için bir İHA Olayına Müdahale Çerçevesi"[45] dokümanına bakın.

Dronlar, resim ve video materyallerinin yanı sıra coğrafi koordinatlar, rotalar, uçuş istatistikleri ve zaman damgaları gibi değerli elektronik deliller içerebilir. Bir drona elkoyma sırasında tipik olarak ilgilenilmesi gereken dört elektronik bileşen vardır:

- Dahili anlık bellek (mikro)SD kartları içermesi muhtemel olan dronun kendisi;
- Depolama verileri tutuyor olması muhtemel olan uzaktan kumanda;
- Dronu kumanda etmek, canlı yayın gerçekleştirmek ve yerel olarak veya bulut üzerinde bilgi depolamakta kullanılabilecek mobil cihaz uygulamaları.

Bir drona elkonulurken aşağıdakilere dikkat edilmelidir:

1. Cihazın açık mı kapalı mı olduğunu belirleyin (genellikle üzerindeki ışıklardan veya gürültüden anlaşılır). Cihazın açık/kapalı olma durumunu ve geldiğinizden beri açıldığına şahit olup olmadığınızı belgeleyin. Cihaz açıksa, herhangi bir ekranında o anda bulunan bilgileri gözden geçirin ve kaydedin. Belirli bir dron markasının/modelinin veriler bozulmadan güvenli bir şekilde nasıl kapatılacağından emin olana kadar, cihazın uçma kabiliyetini (cihazı kurcalamadan - örneğin cihazın üzerine bir ceket veya ağ koymak veya ters çevirmek suretiyle) devre dışı bırakın.
2. Dron ve uzaktan kumandasıyla herhangi bir fiziksel etkileşime girmeden önce DNA ve parmak izi gibi geleneksel adli delilleri güvence altına alın. Elkoyma ve paketleme seçeneklerini değerlendirirken, cihazlar üzerindeki tüm işlemlerde bu tür fırsatların korunmasına dikkat edildiğinden emin olun. Örneğin eldiven giyin, ıslanmaması gereken kısımları (güç düğmeleri, kablo alanları, kumanda kolları vb.) göz önünde bulundurun ve dikkatlice paketleyin.
3. Çoğu dronun üzerinde bir kamera bulunur. Cihaz açık durumdaysa, polis eylemlerinin izlenmesini ve yayınlanmasını önlemek için tüm video kameranın (tipik olarak 360 derecelik kamera) üzerini örtün.
4. Dronun üzerinde çıkarılabilir bir pil varsa, bunu cihazdan çıkarın. Çıkarılamaz bir pil varsa, güç düğmesine bir kez basarak ve ardından tekrar basıp iki saniye boyunca basılı tutarak (DJI modelleri için) cihazı kapatın veya (modele bağlı olarak) anahtarını "kapalı" konumuna getirin. Bu adımların her birinin tamamlandığı zamanı kaydedin. DİKKAT – Pilde herhangi bir hasar veya sızıntı belirtisi varsa pili çıkarmayın veya kurcalamayın çünkü piller yaralanmaya veya patlamaya neden olabilir.
5. Cihazın markası, modeli ve seri numarası da dahil olmak üzere dronu tanımlayan temel unsurları kaydedin. Tanımlayıcı unsurlar, incelenen modele bağlı olarak cihazın farklı yerlerinde olabilir. Bazı dronlarda, tanımlamalarını kolaylaştırmak için taranabilen QR kodları bulunmaktadır.

[45] https://www.interpol.int/content/download/15298/file/DFL_DroneIncident_Final_EN.pdf

6. Dron üzerinde kolayca tespit edilebilen tüm değişiklikleri veya cihaz üzerinde/yakınında bulunan, ek işlevsellik sunabilecek tüm ilave çözümleri ve faydalı yükleri kaydedin.
7. "Kablosuz" kontaminasyonu ve uzaktan silmeyi önlemek için dron ve uzaktan kumandayı ayrı faraday muhafazaları/torbaları içinde bağımsız olarak paketleyin. Ek bağlı/ilişkili cihazları ayrı faraday torbaları içinde paketleyin, ancak bunların civarda bulunduğunu kaydedin. Cihaza bağlı ancak cihazdan ayrı/uzakta bulunan cihazlar, bağımsız deliller olarak ele alınmalı ve buna göre paketlenmelidir.

3.5 Canlı Veri Senaryolarında Arama ve Elkoyma

Bir suç mahallinde bilgisayarlar ve elektronik cihazlar açık ve çalışır durumdaysa, Canlı Veri Adli İnceleme gerekli olabilir. Bilgisayar adli incelemesinin ilk yıllarında, bir müfettiş arama ve elkoyma işlemi sırasında çalışan bir sistem bulduğunda verilen tavsiye "Fişi çekin" idi! O zamandan beri, bellekte tutulan geçici veri miktarı, uzak bağlantıların ve şifreleme yazılımlarının kullanımı önemli oranda artmıştır. Fişin çekilmesi, soruşturmada tüm uçucu verilerin kaybedilmesi, uzak bağlantıların kesilmesi ve açık dosyaların kilitlenip şifrelenebilmesi anlamına gelir. Bu tür veriler ve bilgiler yüksek delil değerine sahip olabilir ve canlı verileri yakalama ihtiyacı, bir dizi prosedürün ve kılavuzun revize edilmesine yol açmıştır. Delilleri değiştirme ve hatta üzerine yazma olasılığı çok yüksektir ve canlı veri adli inceleme çok daha yüksek düzeyde teknik bilgi ve uzmanlık gerektirir.

Canlı Veri Adli İnceleme için, bu Kılavuzun giriş bölümünde tanımlanan 1. ve 2. ilke özellikle önemlidir. Müfettişler, gerekli adımları atacak ve sistem üzerindeki etkiyi en aza indirecek teknikleri kullanacak düzeyde kalifiye ve yetkin olmalıdır. Atılan tüm adımların, zamanları ile birlikte ayrıntılı bir denetim izi hayati önem taşımaktadır.

Çalışır durumdaki bir sistemin adli incelemesi; özel eğitim, bizzat uygulama deneyimi ve bir dizi onaylanmış adli araç gerektirir. Olay yerinde bu becerilere sahip bir inceleme uzmanı yoksa, derhal bir uzman birimden destek istenmelidir. Bununla birlikte, kimseye ulaşılamazsa, fişi çekmek ve geçici verileri kaybetmek, canlı verileri yakalamaya yönelik bilgisiz girişimlerle delillerin olası bozulması riskinden daha mantıklı olabilir.

Farklı türlerde geçici verilerin nasıl elde edileceğine ilişkin ayrıntılara girmeden önce, geçici verileri ve ne tür deliller sağlayabileceklerini tanımlamalıyız.

3.5.1 Geçici Veriler

Bu Kılavuzun amaçları doğrultusunda 'Geçici Veriler' aşağıdaki şekilde tanımlanmıştır:

> *Geçici veriler, dijital olarak depolanan, insan eylemleri veya otomatik işlemler ile kısa bir süre içinde silinme, üzerine yazılma veya değiştirilme olasılığı çok yüksek olan verilerdir.*

Geçici Veriler son derece hassastır ve hızlı ve doğru bir şekilde kaydedilmezse kaybolur. Modern bilişim sistemlerinde, geçici Rastgele Erişim Belleği (RAM) içinde tutulan

bilgi miktarı, 16 GB veya 32 GB (yaklaşık yüz binlerce resme eşdeğer) veri kadar büyük olabilir ve kaybolabilen veriler sadece RAM içinde depolanan veriler değildir. Modern bilişim ortamlarındaki veriler her zaman yerel olarak depolanmaz ve işlenmez. Geniş bir hizmet yelpazesi içinde, uzak sistemler üzerinde (yani Bulutta) ucuz ve hatta ücretsiz depolama ve güçlü işleme kaynakları sunulmaktadır. Bu verilere erişim, verilerin bulunduğu ülkenin mevzuatına tabi olacaktır ve arama sırasında elde edilen dışında bir erişim imkanı olmayabilir. Nitekim, bazı ülkelerdeki ulusal yasalar, çalışır durumdaki bir sistemde bile bu tür verilere erişimi veya bu tür verilerin elde edilmesini yasaklayabilir.

Müfettişin aşina olması gereken farklı türlerde geçici veriler vardır:

1. Açık ağ bağlantıları, çalışan işlemler ve hizmetler, ARP[46] ve DNS[47] önbellekleri, kaydedilmemiş belgeler, parolalar, şifreleme anahtarları ve bilgisayarda RAM içinde depolanan diğer bilgiler, **fiziksel bilgisayardaki geçici verilerdir**.

2. Doğası gereği geçici olmayan ancak yalnızca olay yerinde erişilebilen **kısa süreli veriler**. Şifrelenmiş birimler ve uzak kaynaklar bu tür verilerin örnekleridir. Müfettiş, bunları arama sırasında elde edemezse, bu veriler erişilemez hale gelebilir, değiştirilebilir veya silinebilir.

Bu kategorilerin her ikisi de aşağıda daha ayrıntılı olarak incelenmektedir.

Farmer ve Venema[48] tarafından hazırlanan bu tablo, farklı veri türlerinin elde edilmesi için olası zaman çerçevesini açıklamaktadır:

Veri Tipi	Geçicilik Derecesi
Kütükler, çevresel bellek, önbellekler vb.	Nanosaniyeler
Ana bellek	On nanosaniye
Ağ durumu	Milisaniyeler
Koşan (çalışan) süreçler	Saniyeler
Disk	Dakikalar
Disketler, yedekleme ortamı vb.	Yıllar
CD'ler, çıktılar vb.	Onyıllar

Geçici Veriler zengin delil kaynakları olabilirler. 'Canlı' bir bilgisayar, o anda koşmakta olan süreçleri (yani bilgisayarın hangi işlemleri yaptığını), önbellekleri (verilerin geçici olarak depolandığı yeri), ağ bağlantılarını ve bellekte depolanan tüm verileri gösterebilir. Bellek ayrıca parolalar veya şifresi çözülen uygulamalar (ancak bir makinede kurulu şifreleme yazılımı varsa yararlıdır) gibi yararlı bilgiler ve hatta bazen diske kay-

---

[46] ARP, Adres Çözümleme Protokolü anlamına gelir. Bir ağdaki mesajların doğru cihaza gönderilmesi için bir IP Adresini bir fiziksel donanım adresine dönüştürmek amacıyla kullanılan, yaygın olarak kabul edilmiş bir dizi kural ve standarttan oluşur.

[47] DNS, Alan Adı Sistemi anlamına gelir. DNS, IP Adresi olarak kullanılan sayı dizilerini daha kullanıcı dostu olan alan adlarına bağlayan bir tür veritabanıdır.

[48] D. Farmer ve W. Venema (2006), Adli Delil Toplama, Addison & Wesley, ISBN 0-201-63497-X

dedilmemiş zararlı (kötü amaçlı) kodlar içerebilir. Geleneksel "fişi çekme" yaklaşımı izlenecek olursa, bu tür yararlı bilgiler kaybolacaktır. Bununla birlikte, veriler gücü kesmeden önce elde edilirse, müfettiş sabit diskteki delillere eklenecek çok sayıda ek bilgiye sahip olacaktır.

Aşağıdakilerin geçici bellekte saklanması muhtemeldir:

- Koşan (çalışan) süreçler;
- Çalışan servisler;
- Şifreleme anahtarları;
- Sistem bilgileri;
- Oturum açmış kullanıcılar;
- Dinleme portları ve açık portlar (bağlantı noktaları);
- ARP (adres çözümleme protokolü) önbelleği;
- DNS önbelleği;
- Otomatik başlatma bilgisi;
- Henüz diske yazılmamış kütük bilgileri;
- Kaydedilmemiş belgeler;
- İşlem ikili kodları, sadece bellekte bulunan Kötü Amaçlı Yazılımlara ait olanlar da dahil servisler.

Bir arama ve elkoyma senaryosunda, müfettiş geçici verileri aşağıdaki şekilde koruyabilir:

- Geçici verileri barındıran her cihazı tespit eder, emniyete alır, belgeler ve fotoğraflar;
- Potansiyel şüphelileri ve diğer kişileri gözlemler ve ekipmandan izole eder ve delilleri değiştirmelerini veya yok etmelerini önler;
- Bilişim teknolojisi bileşenlerini izler ve delillerin otomatik olarak değiştirilmesini veya yok edilmesini önler.

3.5.2 Fiziksel Erişim

Bir aramaya dahil olunduğunda, bir bilgisayarın açık olup olmadığını kolayca belirlemek mümkün olmayabilir. Bölüm 3.4 içinde açıklanan adımlara ek olarak, bu tür durumlarda ne yapılması gerektiğine dair bazı ipuçları aşağıda verilmiştir.

- Bir fotoğrafını çekerek bilgisayarın durumunu belgeleyin.
- Bilgisayarın açık olduğuna dair emarelere bakın ve sesini dinleyin. Çalışan fanların, dönen sürücülerin sesini dinleyin veya ışık veren diyotların (LED'lerin) yanıp yanmadığını kontrol edin.
- Fareyi hareket ettirmeye çalışın, ancak herhangi bir düğmeye basmayın.
- Ekran koruyucu veya oturum açma ekranına ilişkin herhangi bir belirti olup olmadığını görmek için ekranı gözlemleyin.
- Bir fotoğrafını çekerek ekranın durumunu belgeleyin.

Bilgisayarın açık olduğu ortaya çıkar, ama bir ekran koruyucu görünürse yapılacak ilk işlemler şunlardır:

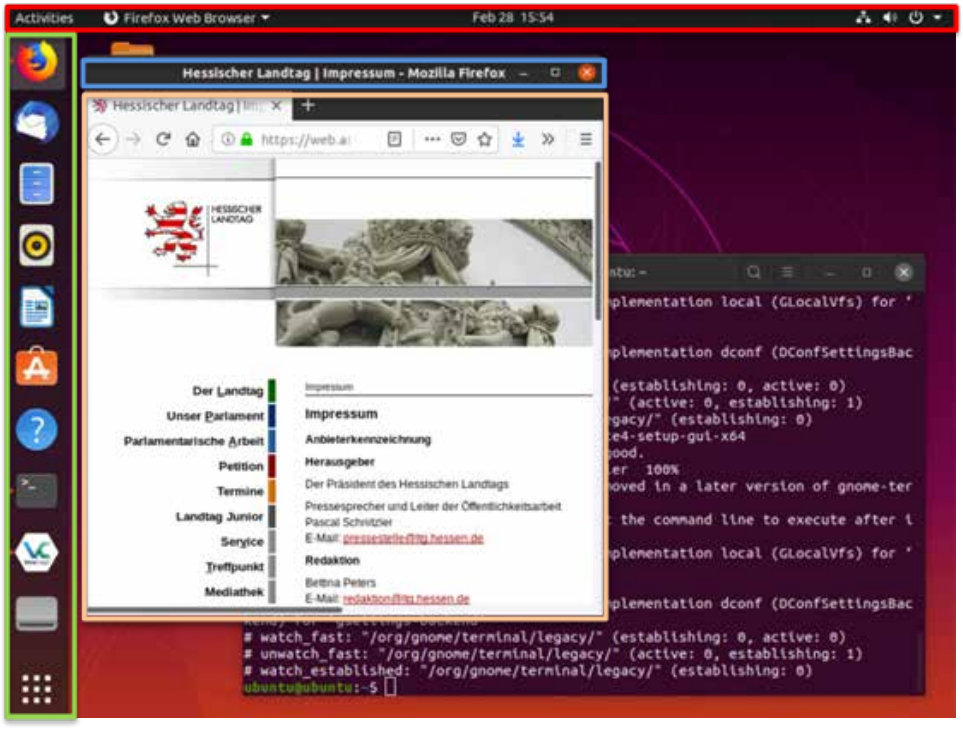
- Fareyi hareket ettirerek o sırada ekranı gözlemleyin;
- Ekran koruyucu kaybolursa ve şifre sorulmadan sisteme erişirseniz, sonraki Canlı Veri Adli İnceleme adımlarına geçebilirsiniz (bunu yapmak konusunda tam eğitimli ve yetkinseniz);
- Ekran koruyucu bir parola ile kilitlenmişse, şüpheliye sorun, ekran koruyucu arayüzünde parola ipucunun etkinleştirilip etkinleştirilmediğini kontrol edin, notları veya diğer ipuçlarını arayın. Parola elde edildiyse, devre dışı bırakın ve sonraki Canlı Veri Adli İnceleme adımlarına geçin.
- Parolayı bulamazsanız, FireWire ve Thunderbolt arabirimleri aracılığıyla, parola atlama mekanizmalarını veya "soğuk önyükleme" yöntemini kullanarak RAM'i ele geçirme teknikleri mevcuttur. Bu teknikler sadece Canlı Veri Adli İnceleme uzmanları tarafından kullanılmalıdır.
- **Her halükarda: Bir fotoğrafını çekerek ekranın durumunu belgeleyin.**

Bilgisayar açıksa, ancak bir ekran koruyucu veya kimlik doğrulama ekranı tarafından korunmuyorsa veya parolayı elde edebildiyseniz:

- Dijital delilin yok edildiğini gösteren emareler için ekranı kontrol edin. Bakılması gereken kelimeler şunları içerir: "sil", "biçimlendir", "kaldır", "kopyala", "taşı", "kes" veya "temizle";
- Kullanılan şifrelemeye dair emarelere bakın (daha sonra açıklanacaktır);
- Bilgisayara uzak bir bilgisayardan veya cihazdan erişildiğini gösteren emarelere bakın;
- Bulut hizmetlerinin kullanıldığına dair emarelere bakın (Bölüm 3.5.3.1 içinde açıklanmıştır);
- Anlık mesajlaşma pencereleri veya sohbet odaları gibi diğer bilgisayarlar veya kullanıcılar ile aktif veya devam eden iletişim emarelerine bakın;
- Kameraların veya web kameralarının (internet kameralarının) aktif olduğuna dair emarelere bakın;
- Bir ekran koruyucunun veya kilidin etkinleştirilmesini önlemek için fareyi hareket ettirmeye devam edin;
- Açık olan ve belki de tam ekran modunda olan sanal makinelere ilişkin emarelere bakın;
- **Tüm bu durumlarda: Bir fotoğrafını çekerek ekranın durumunu belgeleyin.**

Canlı Veri Adli İncelemesi için her durumu kapsayan bir Standart Operasyon Prosedürü yoktur. Her arama farklı olduğundan, deneyimli inceleme uzmanı ilgili koşullara göre uygun önlemleri seçmek zorunda kalacaktır. Bazı temel prosedürlere ilişkin bir akış şeması **Ek B** içinde bulunabilir:

Bir bilgisayar ekranında nelerin görülebileceğini daha iyi anlamak için, simülasyonu yapılan arama ve elkoyma senaryolarına ait bazı fotoğraflar aşağıdadır.



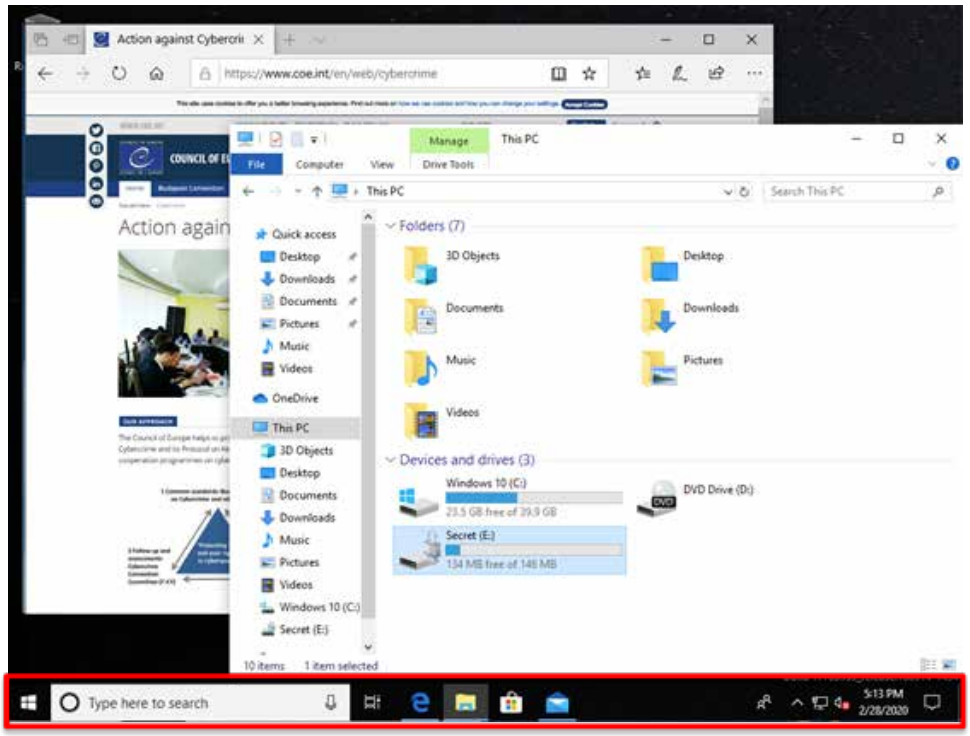
Bu, "Gnome" Grafik Kullanıcı Arayüzü (GUI)[49] ile "Ubuntu" Linux işletim sistemini çalıştıran bir dizüstü bilgisayardır. Resmin üst kısmındaki kırmızı dikdörtgen, bazı aktif pencereleri (örneğin Firefox tarayıcısı), geçerli tarih ve saati (ortada) ve sistem çubuğu (tepsi) simgelerini ve ayrıca bir kullanıcı/güç simgesini (sağda) gösterir.

[49] Grafik Kullanıcı Arayüzü veya GUI, kullanıcının bilgisayarla nasıl etkileşime girdiğinin, bilgisayar ekranında görüntüler ve simgeler aracılığıyla kullanıcı dostu gösterimine verilen addır.

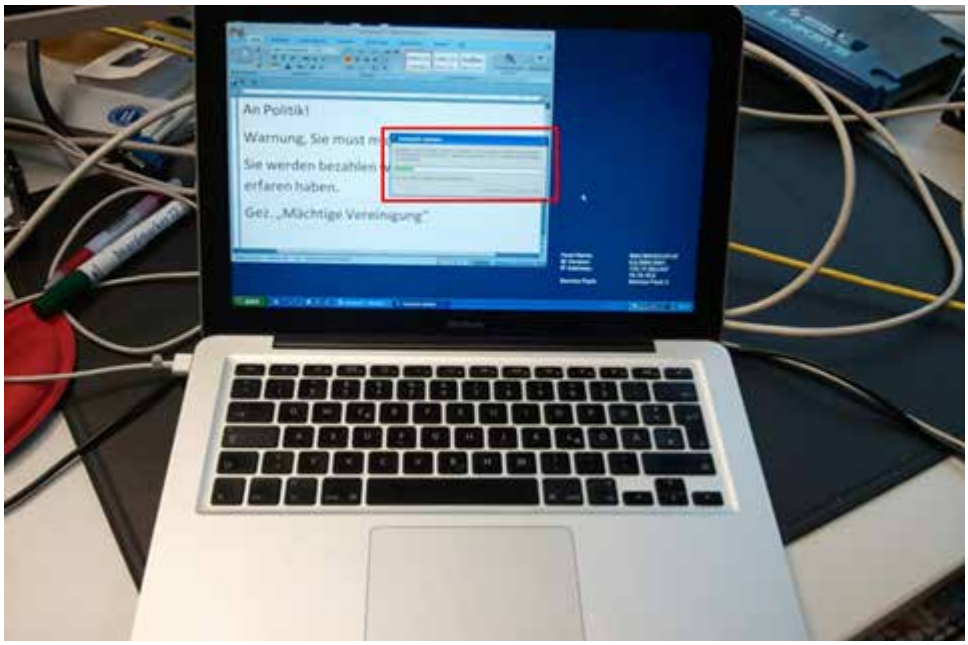
Mavi dikdörtgen, o anda açık olan pencerenin başlık çubuğunu gösterir. Bu durumda, o anda açık olan web sayfasını ve bir İnternet tarayıcısı olan "Mozilla Firefox"un açık olduğunu göstermektedir!

Yeşil dikdörtgen (solda), kullanıcının favori programlarının yanı sıra o sırada çalışan uygulamaları (simgesinin yanında küçük bir nokta bulunanlar) gösterir. Deneyimli bir müfettiş, Veracrypt'in o sırada çalıştığını gösteren Veracrypt simgesini not edebilir. Bunun böyle olması gerekmez, tipik olarak Veracrypt arka planda çalışır.

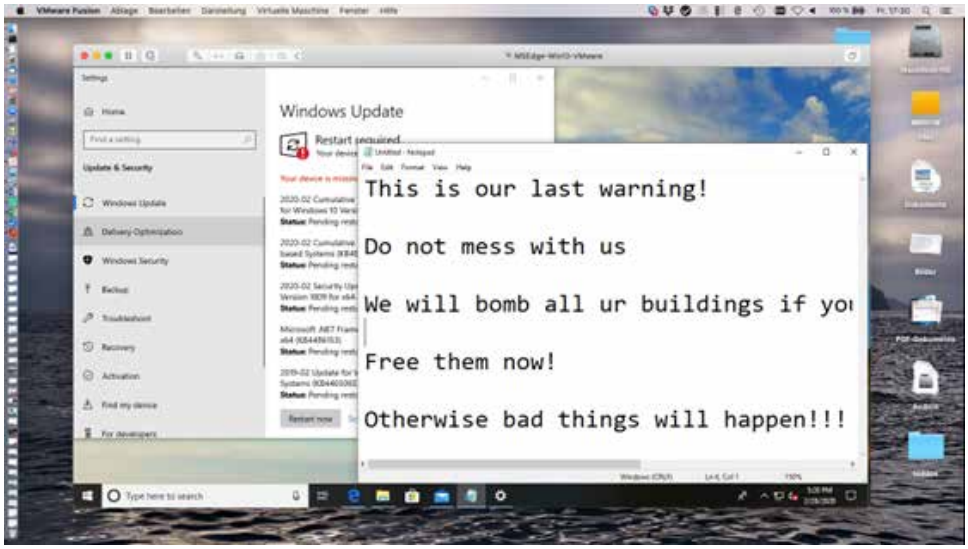
Turuncu dikdörtgen, bir web sitesinin açılmış olduğunu gösterir.



Bu, Windows 10 çalıştıran bir bilgisayar örneğidir. Kırmızı dikdörtgen, üzerinde bir program menüsü, bir arama çubuğu ve kısayollar (solda), etkin pencereler (ortada) ve tepsi simgeleri ve saat (sağda) bulunan görev çubuğunu gösterir. Simgelerinin altında mavi bir çubuk olduğu için etkin programlar kısayollarından kolayca tespit edilebilir. Bu durumda, Windows Explorer (mavi dikdörtgen) ve Windows Edge (Soldaki Pencere) ekranda açıktır ve arka planda Windows Mail (yeşil dikdörtgen) çalışmaktadır.



Bu resim, bir MacBook olduğu görünen bir dizüstü bilgisayarı göstermektedir. MacBook bilgisayarda bir müfettiş macOS işletim sisteminin çalışmasını bekler, ancak bu durumda makinede Windows 10 çalışıyor gibi görünüyor. Ekranın solundaki "Windows Update" (Windows Güncellemesi) penceresine özellikle dikkat edilmelidir. Eğer müfettiş hemen harekete geçmezse, bir Windows güncelleme işlemi bilgisayarı yeniden başlatacaktır. Bu, ekranda görünen kaydedilmemiş belgenin sonsuza kadar kaybolabileceği anlamına gelebilir.



Dizüstü bilgisayara daha yakından bakıldığında, aslında Windows 10'un sanal bir makine içinde çalıştırıldığı ortaya çıkmaktadır, dolayısıyla bu belgeyi kurtarma şansı daha da düşük olacaktır. Elbette bunu fark eden bir müfettiş, her iki makinede de, hem sanal makinede hem de MacBook "host" üzerinde canlı veri adli inceleme yapacaktır.

Fotoğraflardaki gibi senaryolarda canlı veri adli inceleme yapılırken sistemde değişiklik yapılması kaçınılmazdır. Canlı inceleme, çalışmakta olan sistemde kaçınılmaz olarak değişiklik yapacak araçların kullanılmasını içerir. Bununla birlikte inceleme uzmanının, eylemleriyle olabildiğince küçük bir ayak izi bırakırken, mümkün olduğu kadar çok miktarda geçici veriyi yakalamaya çalışması gerekir.

Veri yakalamanın gerçekleştirildiği sıra da çok önemli olabilir ve inceleme uzmanı veri toplama sırasını dikkatlice değerlendirmelidir. Her arama ve elkoyma senaryosu olaya özgü yaklaşımlar gerektirse de, geçicilik sırasına göre önceden tanımlanmış bir metodoloji izlenmesi tavsiye edilir.

Standartlaştırılmış bir iş akışı oluşturmak için, (örneğin Bash (Linux), Batch (Windows) veya Python'da) basit bir program yazılarak kullanılabilir. İlk Müdahale Ekibinin Tarama Aracı "FiRST" (FREETOOL Hub[50] aracılığıyla kolluk kuvvetleri için ücretsiz) gibi ek işlevlere sahip mevcut çerçeveler, programlama konusunda eğitim almamış bir müfettişe destek olabilir. FiRST'nin amacı, risklere karşı ve sistem kapatıldığında kaybolabilecek geçici veriler olup olmadığını görmek için sistemi taramaktır. Araç; şifrelemeleri, kripto para cüzdanlarını, parola kasalarını, bulut/ağ depolarını ve çok daha fazlasını tarar. Tarama tamamlandığında, FiRST, fişi çekmenin mi yoksa bir uzmanla iletişime geçmenin mi da güvenli olduğunu belirten bir trafik ışığı simgesi görüntüler.

[50] https://thefreetoolproject.eu/

Geçici verileri elde etmek için doğru araçları arayan müfettişler için Kuhlee ve Voelzow[51], aşağıdaki konularda yardımcı olmak üzere bir program parçaları ve araçlar listesi oluşturmuştur:

Geçici parçacık	Windows Araçları	Linux Araçları
Bilgisayar bellegi (RAM) içerikleri	Winpmem, Dumpit	Lime, AVML
Yönlendirme Tabloları, ARP önbellekleri, Kernel istatistikleri	Route PRINT, arp –a, netstat	netstat –r –n route arp –a
DNS Önbelleği	Ipconfig /displaydns	rndc dumpdb (kurulu ise)
Süreç listeleri	PsList, ListDLLs, CurrProcess, tasklist	ps –ef, lsof
Etkin ağ bağlantıları (soketler)	netstat –a	netstat –a, ifconfig
Ağ bağlantılarını kullanan programlar/ servisler	sc queryex, netstat -ab	netstat -tunp
Açık dosyalar	Handle, PsFile, Openfiles, net file	lsof, fuser
Ağ paylaşımları	Net share, Dumpsec	showmount –e, showmount –a smbclient –L
Açık portlar (bağlantı noktaları)	OpenPorts, ports, netstat –an	netstat –an, lsof
O sırada oturumu açık olan kullanıcılar	Psloggedon, whoami, ntlast, netusers /l	w, who -T, last
Takılı durumda olan şifrelenmiş dosya sistemleri	Manage-bde (Bitlocker), efsinfo (EFS)	mount -v, ls /media
Geçici olarak bağlanmış dosya sistemleri	Fsinfo, reg (Mounted Devices)	mount -v, ls /media
Uzaktan kayıt ve izleme verileri	psloglist	/etc/syslog.conf Port UDP 514
Fiziksel konfigürasyon, ağ topolojisi	Systeminfo, msinfo32, ipconfig /all	ifconfig –a ip addr
Depolama ortamları	reg (Mounted Devices), Net share, netstat –a	mount -v, ls /media
Sistem saati (radyo saatine göre kaydırma miktarını belirlemek için)	time /T, date /T, uptime	time, date, uptime
Ortam değişkenleri	cmd /c set	env, set
Pano	Pclip	xclip
Disklerin içerikleri	FTK Imager, EnCase, Tableau Imager	Dc3dd, ewfacquire, Guymager

[51] Kuhlee ve Voelzow (2012), *Adli Bilişim Kestirmeleri*, O'Reilly, ISBN 978-3-86899-121-5, http://www.forensikhacks.de

Bu araçların çoğu, Microsoft'un SysInternals[52] paketinde veya Linux için CERT deposunda bulunabilir.[53]

Bu liste kesinlikle eksiksiz değildir. Örneğin Linux sistemlerde, müfettiş her zaman sanal /proc dosya sisteminde depolanan geçici bilgileri de elde edebilen araçları da değerlendirmelidir.

Bir dizi canlı veri adli incelemesi oluştururken, müfettiş aşağıdakileri dikkate almalıdır:

- Sadece sistem üzerinde en az etkiye sahip olan araçları seçin. Örneğin RAM bilgisini elde etmek için, "FTK Imager"[54] gibi ağır bir grafik araç yerine "WinPMem " gibi küçük bir araç tercih edilmelidir.
- Araç, kendi yürütülebilir dosyalarıyla birlikte gelmeli, böylece müfettiş, sistemdeki güvenilmeyen ikili dosyaları[55] kullanmadan ilgili aracı çalıştırabilmelidir. Müfettiş ayrıca, sadece işlevlerini mahkemede açıklayabileceği araçları ve komut dosyalarını kullanmalıdır.
- Araç/komut dosyası otomatikleştirilmiş olmalı ve çok fazla kullanıcı etkileşimi gerektirmemelidir. Müfettiş, ne tüm komutlara ilişkin tüm seçenekleri hatırlamalı ne de birden fazla cihazdaki her işlemi izlemelidir.
- Şirket ortamlarında araçlar, bir olayın gerçekleşip gerçekleşmediğine karar vermesi bakımından müfettişe yeterli bilgi sağlayan bir öncelik belirleme işlevi içermelidir.
- Araç sadece geçici olan verileri toplamalıdır. Analiz edildikten sonra aynı zamanda bilgisayarın sabit diskinde de bulunabilecek verilerin elde edilmesi gerekli değildir.

Ayrıca, içinde çok çeşitli canlı veri adli inceleme araçları bulunan önceden yapılandırılmış bazı Adli İnceleme DVD'leri de bulunmaktadır. Her ne kadar müfettişin kendi kişisel ihtiyaçlarına, baktığı vakalara ve ilgili mevzuata uyarlanmış kendi araç setini oluşturması şiddetle tavsiye edilse de, bu DVD'ler hangi araçları kişisel araç kutusuna dahil edeceği konusunda iyi bir fikir verebilir ve ayrıca Canlı Veri Adli İncelemesi alanında yeni başlayan müfettişler için iyi bir alternatif olabilir.

İçinde NirLauncher bulunan Caine Live-CD, Nanni Bassetti vd., www.caine-live.net

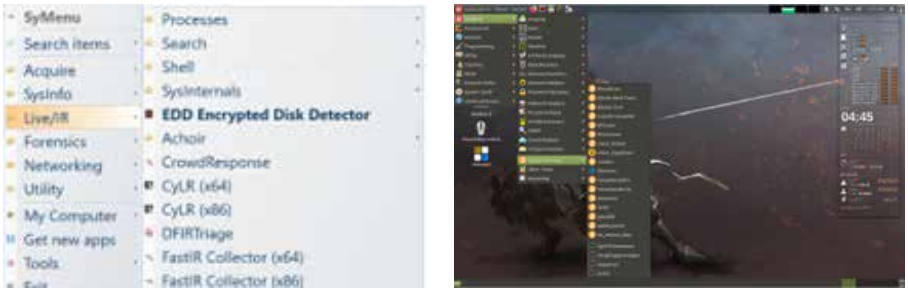
[52] http://technet.microsoft.com/en-gb/Sysinternals

[53] https://forensics.cert.org

[54] https://github.com/Velocidex/c-aff4/releases

[55] "İkili" dosya, bilgisayar tarafından yürütülebilen bir bilgisayar programıdır.

Tsurugi Acquire Live-CD ve Bento DFIR taşınabilir araç seti, Giovanni Rattaro vd., https://tsurugi-linux.org/downloads.php



Paladin Edge, Sumuri Forensics, https://sumuri.com/software/paladin/

Diğer Tavsiyeler

Müfettişler bir sistem üzerinde canlı veri adli incelemesi yaparken, elde edilen verileri asla hedef bilgisayarın depolama ortamlarında saklamamalı, hazırlanmış olan harici depolama ortamlarına bağlanmalıdır. Bu harici depolama ortamlarında ayrılmış bir alan sağlanmasına ek olarak, canlı veri adli inceleme araçlarını içeren diğer cihazlar da ayarlanmış ve kullanıma hazır durumda olmalıdır.

Depolama cihazlarına ilişkin seçenekler aşağıdakileri içerir:

- **USB Çubuklar**: Bunlar çok hızlıdır ve güvenilirdir, ama RAM miktarına eşit bellek kapasitelerine sahip USB çubuklar kullanılması gereklidir;
- **Harici Sabit Disk Sürücüler (HDD'ler) veya SSD'ler:** Büyük hacimli bellekler kopyalanacağı zaman bu tür bir seçenek tercih edilmelidir. Bir dizi olası konektöre (USB-A/USB-C/eSATA) sahip modeller daha esnek kullanım imkanına sahiptir.
- **DVD'ler:** Hedef sistemde kullanılacak canlı veri adli inceleme araçları için idealdir. DVD-R'lerin yazma koruması, güvenilir ikili dosyaların (programların) değiştirilmesini önler.
- **Sanal DVD'lere sahip harici HDD'ler/SSD'ler:** Bunlar, harici sabit sürücünün hızlı erişilebilir, güvenilir depolaması ile DVD-ROM'un yazma koruması avantajlarını birleştirir. Bir müfettiş, kendi adli inceleme önyükleme disklerini özel bir klasöre ISO[56] dosyaları olarak kaydedebilir ve doğrulanmış ikili dosyaları etkileme riski olmadan

[56] Bir ISO dosyası, bir diskin tam bir kopyasını, arşivini veya görüntüsünü içeren bir kutu gibidir.

sanal bir DVD-ROM olarak bağlayabilir.[57,58] Bu tür cihazların bir örneği Zalman ZM-VE500'dür.

Elde etme ortamını ve canlı veri adli inceleme araçlarını hazırlarken müfettiş aşağıdakileri dikkate almalıdır:

- Ortamlarınızı NTFS[59] ile biçimlendirin (FAT[60] dosya sisteminin dosya boyutu ve miktar sınırlamaları vardır);
- Farklı bir dosya sistemi (örneğin Linux sistemler için EXT4 ve macOS sistemler için HFS+/APFS) formatına sahip ikinci bir ortam seti hazırlamayı düşünün;
- Windows, Mac ve Linux gibi çoklu işletim sistemleri ile karşılaşmayı bekleyin ve bunun için hazırlık yapın;
- Kullanmadan önce güvenilir ikili dosyaları doğrulayın[61];
- Önyükleme DVD›nizin[62]/depolama kurulumunuzun doğru çalıştığını test edin;
- Olay yeri aramasından ÖNCE araçlarınızı bildiğinizden emin olun;
- Yanınızda yeterince depolama alanı olsun;
- Her arama öncesinde hedef sürücülerinizi tamamen silerek çapraz bulaşmayı önleyin;
- RAM üzerindeki etkiyi sınırlandırmak için düz bir klasör yapısı kullanın.

---

57 yani onları sistem tarafından erişilebilir hale getirir.

58 Bozulmamış olduğu garanti edilen program türleri.

59 NTFS, Yeni Teknoloji Dosya Sistemi anlamına gelir ve Windows dosyalarını dosyalamanın ve düzenlemenin bir yoludur.

60 FAT, bir sabit sürücüde depolanan dosyaları takip etmek için kullanılan Dosya Tahsis Sistemi anlamına gelir.

61 Başka bir deyişle, kullanacağınız yazılım araçlarının test edildiklerinden ve doğru sonuç verdiklerinden emin olun.

62 Önyükleme DVD'si, bir işletim sistemini veya yardımcı (faydalı) programı "önyüklemek" veya yüklemek için kullandığınız DVD'dir.

3.5.2.1 *Şifreleme*

Şifreleme, özellikle de «tam disk şifreleme», sadece suç faaliyetlerini gizlemek isteyen kişiler için değil, ticari açıdan hassas veya özel mülkiyet niteliğindeki bilgilere sahip ve kişisel verileri koruması gereken şirketler için de daha popüler hale gelmektedir. Çoğunlukla şirket politikaları, (harici ortam ve dizüstü bilgisayarlar da dahil olmak üzere) tüm taşınabilir cihazların Microsoft BitLocker, Steganos, PGP vb. yazılımlar kullanılarak şifrelenmesini gerektirmektedir. Günümüzde donanım satıcıları, dizüstü bilgisayarlarında ve sabit disklerinde şifreleme seçenekleri de sunmaktadır.

Bir sabit sürücü üzerindeki şifreleme etkinleştirildiğinde, soruşturma için artık çok geç olabilir. Güçlü şifreleme, özel kripto kümeleri ve çözülebilmesi için oldukça çok zaman gerektirir ve bunlar olsa bile çözülmesi mümkün olmayabilir. En kötü durumda, şifreleme herhangi bir verinin analiz edilmesini engelleyerek terabaytlarca bilgi içeren en büyük sabit diskleri bile değersiz hale getirir.

```
00000000: 21bb 6b1e ee4e 0eea 7430 0b3b 5bde 39c7  !.k..N..t0.;[.9.
00000010: f370 ac1e 14cf 5f1d 59d8 2865 df4f f7fb  .p...._.Y.(e.O..
00000020: 73f9 59ab 18b7 03eb 5b31 eaeb 28e2 7e1b  s.Y.....[1..(.~.
00000030: 20f8 79c9 03de 4068 2809 b888 67d0 0d57   .y...@h(...g..W
00000040: fe43 c63d 1561 9e0d 69a7 7337 1e35 6d4c  .C.=.a..i.s7.5mL
00000050: 9065 291e ad79 0104 e616 0369 9cbe e72f  .e)..y.....i.../
00000060: 3e7b ffe3 30e6 0bf9 a37e 3716 f451 5558  >{..0....~7..QUX
00000070: 3e6f a6af d0f0 d75a 49f4 db63 b234 9319  >o.....ZI..c.4..
00000080: fa0f 1269 9f03 1c4b 0287 aa0f aa55 392d  ...i...K.....U9-
00000090: e6e1 4e74 4b29 0c6c c2ad 047a f202 5b5d  ..NtK).l...z..[]
000000a0: eb6b fe0f 5dd3 7e69 751a 8f27 1771 66b3  .k..].~iu..'.qf.
000000b0: 6ade d759 2b61 f51a 1233 4e95 0eac 5a82  j..Y+a...3N...Z.
000000c0: 2b9c fef5 d2d8 5b01 ae88 0888 26d7 9e7f  +.....[.....&...
000000d0: a5a9 07fe 3b5b 61c7 f7b6 cb22 8565 f8b9  ....;[a....".e..
000000e0: 69b5 1251 fc10 8819 0ef1 2676 38a7 731f  i..Q......&v8.s.
000000f0: 4eb0 6a9b 2fb9 4379 6165 1438 6d1c 65c6  N.j./.Cyae.8m.e.
00000100: cf1b 6db6 7122 5678 5086 bbd4 fa9e 680b  ..m.q"VxP.....h.
00000110: a993 46bf 2839 912e 2ac8 0984 ca21 0114  ..F.(9..*....!..
00000120: 0a1b 1781 80df 5640 0c68 adfc 0c9c 6e5f  ......V@.h....n_
00000130: d96c 852c bf87 2a89 d020 43dc 1b74 61a3  .l.,..*.. C..ta.
00000140: e248 e1c6 ccc6 ca15 b386 e6aa 3127 989f  .H.........1'..
00000150: 537c 7535 140a f4c3 374d 3cbf 1cd4 9161  S|u5....7M<....a
00000160: dead 9e77 f2b6 2971 0e11 76de 222d 6903  ...w..)q..v."-i.
00000170: 33df daa5 a36d e16c a516 de03 08a9 9fa7  3....m.l........
00000180: 2813 47ad 25a4 2d6c af05 0fc8 ccae c180  (.G.%.-l........
00000190: 24e8 0f4e 812f 7c20 b5b2 dbc5 b721 b1d3  $..N./| .....!..
```

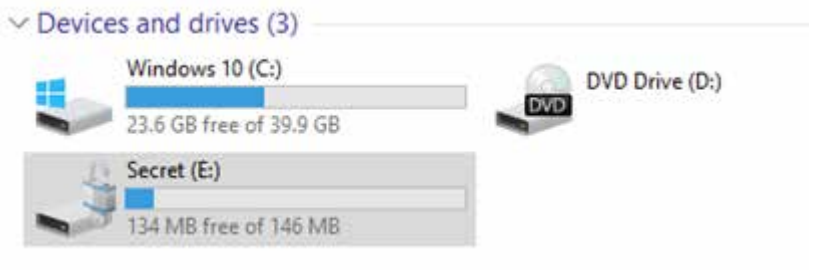
Şifrelenmiş veri örneği

O zaman müfettiş bir diskin şifrelenmesini nasıl engeller? Şifreleme nasıl tespit edilebilir ve şifreleme ile karşılaşıldığında ne yapılmalıdır?

İyi bir başlangıç noktası, kullanılan şifreleme yazılımının görünür emarelerini aramaktır. Tipik yazılım adları, yukarıda da belirtildiği gibi Microsoft BitLocker, VeraCrypt, TrueCrypt, Steganos ve PGP›dir ve bunların simgeleri görülebilir.

Şifreleme yazılımlarına ait tepsi simgesi örnekleri

Şifreleme yazılımlarının izleri ayrıca çalışan işlemlerde, kurulu yazılım iletişim kutusunda, kayıt defterinde (örneğin takılı cihazlar, kurulu yazılımlar, ilişkili dosya uzantıları) ve aynı zamanda Windows Gezgini içinde de bulunabilir.



Windows Gezgini görünümünde Microsoft Bitlocker şifreli disk

Microsoft BitLocker kullanıldığında, işletim sistemi, aşağıdaki komutu girerek müfettişe takılı halde bulunan şifreli sürücüler hakkında bilgi verebilir[63]:

manage-bde –status

Müfettiş, şifreleme kullanıldığına dair ipuçları görürse, aşağıdaki şekilde hareket etmelidir:

- Şifrelenmiş disklerin veya taşıyıcıların hala sistemde takılı olduğunu tespit ederseniz, o çalışan sisteme hala erişiminiz varken bunları kopyalayın;
- BitLocker'ın şifrelenmiş bir birimi takmak için kullanılması durumunda, aşağıdaki komutu kullanarak 48 basamaklı Kurtarma Anahtarını kaydedin:

manage-bde -protectors -get <volume name>

- Daha sonra dosyaları kaydedin. Şifrelenmiş birimler veya taşıyıcılar takılı halde değilse ve hala şifrelenmiş durumdaysa, şüpheliden parolayı, şifre çözme anahtarlarını/ortamlarını ve dosyaların şifresinin nasıl çözüleceğini sorun (şüphelinin yanlış bilgi vermeye çalışabileceğini unutmayın);
- Sorgulama başarılı olursa, verilerin şifresini çözün ve verileri kopyalayın;
- Herhangi bir ekran koruyucu, düşük pil veya enerji tasarrufu özelliğinin şifrelenmiş dosyaların kaydedilmesini kesintiye uğratmadığından ve engellemediğinden emin olun.

Önemli: Başarılı şifre çözme işlemi, sadece parolalara değil, aynı zamanda sistem donanımı içindeki Güvenilir Platform Modülü (TPM) yongalarına, yerel olarak veya (USB Anahtarı gibi) harici ortamda depolanan anahtar dosyalarına da bağlı olabilir. İki aşamalı kimlik doğrulama kullanılmışsa, ikinci bileşen bulunmadıkça parolaya sahip olmak bir anlam ifade etmeyecektir. Tesislerdeki tüm dijital delil kaynaklarını ele geçirmek bu yüzden çok önemlidir.

Önemli: TrueCrypt[64]/VeraCrypt Tam Disk Şifreleme yapılması durumunda, sabit sürücüyü iki farklı parolayla iki parçaya bölmek mümkündür – bir parça tüm gizli verileri içerirken, diğer parça ise sadece önemsiz verileri içerebilmektedir. Geliştiriciler, bu özelliği, kullanıcının parolasını kendi isteği dışında vermek zorunda kaldığı durum-

[63] Komut, bir bilgisayarın doğrudan işletim sistemine verilen bir talimattır.

[64] TrueCrypt geliştirilmesi artık durdurulmuştur ama yine de karşılaşılabilir. Onun resmi olmayan halefi VeraCrypt'tir.

larda kullanılmak üzere eklemiştir. İşbirliği yaptığını göstermek ve cezadan kaçınmak için kullanıcı sadece önemsiz verileri içeren dış kısma ait parolayı verir.

Yukarıda açıklanan prosedürler **Ek B** içinde bulunabilir.

3.5.3 Uzaktan Erişim

Daha önce de belirtildiği gibi, çalışan sistemlerde arama yapan bir müfettiş, yalnızca bilgisayarın bileşenleri içinde yerel olarak depolanan geçici verilerle değil, aynı zamanda çalışan bilgisayarın dışında depolanmış olabilecek kısa süreli verilerle de uğraşmak zorundadır. Özellikle kurumsal ortamlarda, ağ grubundaki farklı taraflar arasında paylaşılan, merkezi sunucularda barındırılan (saklanan) kullanıcı verileri ile ağ altyapılarını bulmak mümkündür. Şirketin operasyonel kısıtlamaları ve ticari yükümlülükleri dolayısıyla çoğu zaman şirketin sunucuları kapatılamaz ve donanıma elkonulamaz. Ayrıca bir gizlilik kısıtlaması da olabilir. Aramaya izin verilen bir arama emri veya mahkeme kararı, çoğunlukla sadece şüpheliye ait verilerin veya şüphelinin erişimine açık olan verilerin elde edilmesini kapsayacaktır. Yargı izni kapsamında olmayan verileri içeren bir sunucunun tamamının veya paylaşılan bir sistemin disk görüntüsünün alınması bir seçenek olmayacaktır.

Bu tür ticari senaryolara yaklaşmanın iyi bir yolu, (soruşturma içine hiçbir şekilde dahil edilmedikleri sürece) sorumlu olan kişilerin işbirliği yapmasını ve rıza göstermesini istemektir. Daha büyük ölçekli şirketlerin sistemlerinde arama yapılırken, baş müfettişin; şirketin başındaki kişi, hukuk departmanından bir temsilci ve şirketin bilişim altyapısı departmanından bir temsilci ile bir toplantı düzenlemesi iyi uygulamadır. Bu toplantılarda, ilgili tüm tarafların işbirliği ile, bir arama emrinin çıkarılmasını içeren bir sonraki adım planlanmalıdır. Alt bölüm 3.5.4, bir sistem yöneticisinin rızasının değerini daha ayrıntılı olarak açıklamaktadır.

Çoğu durumda müfettiş ya konutlarla ya da küçük ve orta ölçekli işletmelerle karşılaşacaktır. Bu gibi durumlarda, söz konusu ağ, bir ağ içindeki bazı münferit bilgisayarlardan ve şirketin muhasebe yazılımı için merkezi veritabanını barındıran bir sunucudan, çalışma grupları için paylaşılanların tahsisinden, bazı ev dizinlerinden[65] ve belki de e-postalar için bir exchange (gelen-giden) sunucusundan oluşabilir.

Böyle bir ortamda Canlı Veri Adli İncelemesi yürüten bir müfettiş, her zaman ağ altyapısından sorumlu kişiden (şüpheli değilse) işbirliği yapmasını istemelidir. Ağ ne kadar büyükse, bu tür bir desteğe duyulan ihtiyaç da o kadar fazla olur, çünkü altyapıyı kuran ve onu günlük olarak yöneten kişi, şüphelinin hangi kaynaklara erişmiş olabileceğini en iyi bilen kişidir. Ancak, müfettişin şüpheciliği koruması ve kendi kararlarını vererek sonuca varması gerekir. Yardım istediği kişinin şüphelinin arkadaşı olabileceğini aklından çıkarmamalıdır.

Yönlendiriciler ve güvenlik duvarları, müfettişe, Erişim Kontrol Listeleri (ACL'ler) veya güvenlik kuralı kümeleri aracılığıyla ağ yapılandırması hakkında bir fikir verebilir.[66] Bu, yapılandırma ekranlarını cihaz yöneticisi olarak görüntülemek suretiyle başarılabilir, ancak daha önce bulunan veya elkoyma anında elde edilen kullanıcı adları ve şif-

---

[65] Belirli kullanıcılar için dosyaların depolandığı bir yer.

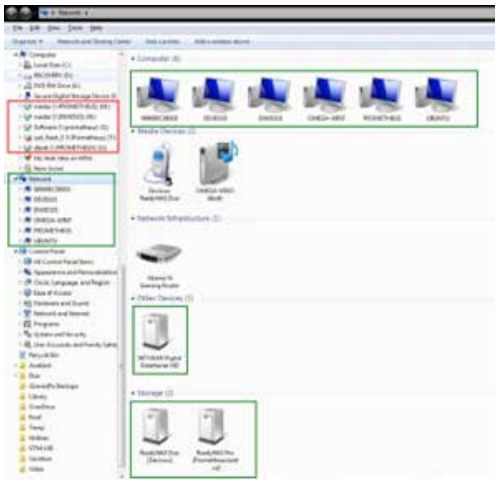
[66] Ağın güvenliğini sağlamak ve kullanım erimini yönetmek için oluşturulan kurallar dizisi.

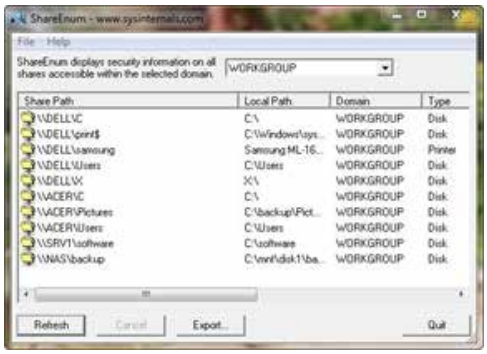
releri gerekecektir. Önceki bölümde bahsedilen Araç DVD'leri aynı zamanda çeşitli ağ keşif araçları da içerir. Ağ altyapısına dair bir diyagramın çizilmesi iyi uygulamadır. Bu, müfettişin, bilgisayar ile ağın geri kalanı arasındaki bağlantıları daha etkili bir şekilde anlamasına ve hatırlamasına yardımcı olacaktır.

Şüphelinin bilgisayarı açıksa ve diğer geçici veriler ele geçirilmişse, müfettiş verilerin uzaktan depolanıp depolanmadığına dair bir ipucu aramalıdır. Bu ipucu, şunları içerebilir:

- Diğer ağ bilgisayarları üzerinde paylaşılan klasörler;
- Bir sunucudan eşlenen ağ sürücüleri;[67]
- IMAP veya Exchange sunucusunda depolanan E-postalar;
- Bulut servisleri ve çevrimiçi depolama.

Diğer ağ bilgisayarlarındaki paylaşılan klasörler ve bir sunucudan eşlenen ağ sürücüleri, basitçe Windows Gezgini içinde aranmak suretiyle veya SysInternals paketindeki ücretsiz ShareEnum aracı kullanılarak soruşturulabilir[68]. Her iki yaklaşımı da aşağıda görmek mümkündür:





SysInternals içindeki ShareEnum

Windows Gezgini görünümü:
Yeşil: Paylaşımlı Ağ Aygıtları, Kırmızı: Eşlenmiş Ağ Sürücüleri

Böyle bir düzenleme keşfedildiğinde, müfettiş bu paylaşılanları kopyalamalıdır. Aslında mümkünse, müfettiş bu paylaşılanların bulunduğu bilgisayarların bir imajını (yani tam bir kopyasını) almayı düşünmelidir çünkü sıradan bir kopya silinen dosyaları veya sürücü üzerindeki ayrılmamış "boş alanı" içermeyecektir.

Bir IMAP[69] veya Exchange Sunucusu üzerinde uzaktan depolanan e-postalar, ilgili e-posta istemcilerinin hesap ayarları analiz edilerek bulunabilir. POP3 ve hatta IMAP hesapları için – ayarlara bağlı olarak – yerel veritabanları olacaktır. Bu tür veritabanları

---

67 Sürücü eşleme, bir ağın, sürücüleri (ayrılmış alan) bir ağ üzerinden, depolama alanlarını paylaşan farklı bilgisayarlar ile eşleştirme yoludur.

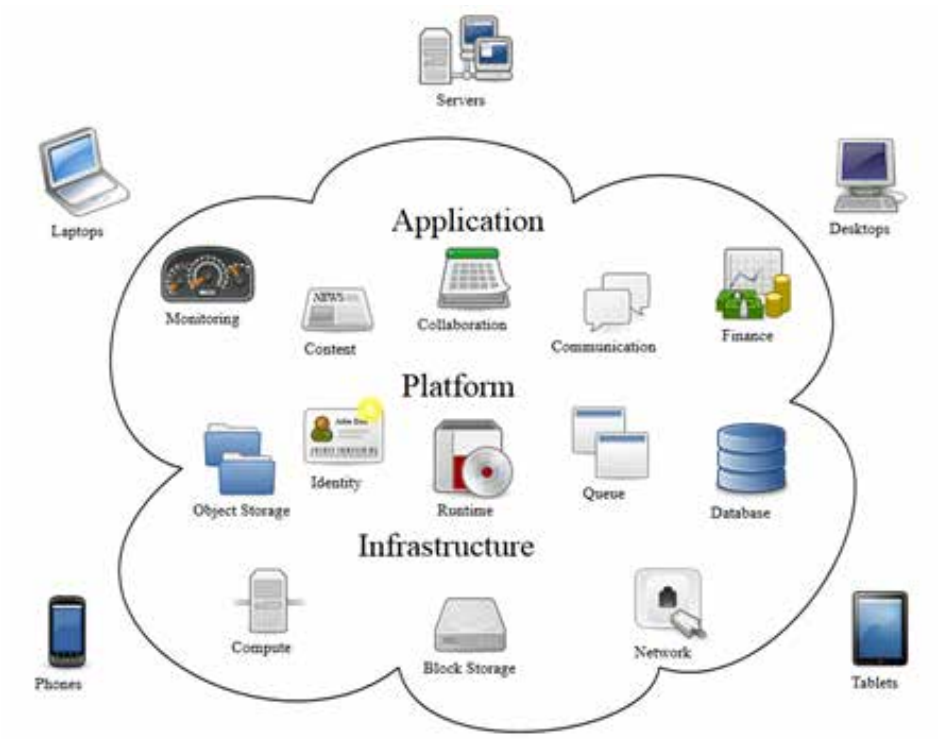
68 http://technet.microsoft.com/de-de/Sysinternals/bb897442

69 IMAP, İnternet Mesajı Erişim Protokolü anlamına gelir

geçici değildir ve canlı adli incelemede elkoyulması gerekmez. Yerel veritabanı dosyası yoksa, müfettiş e-posta hesabının içeriğini doğrudan exchange sunucusundan kaydetmeye çalışmalı veya hesabı barındıran bilgisayarı bunu yapması için görevlendirmelidir.

3.5.3.1 *Bulut Bilişim*

Bulut servisleri ve çevrimiçi depolama, giderek daha da çok önem kazanan bir konudur. Bu servisleri tanıyabilmesi ve anlayabilmesi için müfettişin bulut bilişimin ne olduğunu, ne tür hizmetlerin sunulduğunu ve bunların nasıl çalıştıklarını bilmesi gerekir. Aşağıdaki grafik ve tanım faydalı bir genel bakış sağlamaktadır.



Cloud Computing[70]

Bulut Bilişimin Tanımı

Bulut bilişim, asgari yönetim çabası harcanarak veya hizmet sağlayıcı etkileşimi ile hızla sağlanabilen ve yayınlanabilen, ortak bir yapılandırılabilir bilgi işlem kaynakları (örneğin ağlar, sunucular, depolama, uygulamalar ve hizmetler) havuzuna her yerden, kullanışlı şekilde, isteğe bağlı ağ erişimi sağlayan bir modeldir. [71]

Ulusal Standartlar ve Teknoloji Enstitüsü'nden (NIST) Mell ve Grance, Bulut Bilişim için üç hizmet modeli tanımlamaktadır. [72]

---

[70] Grafik kaynağı: Sam Johnston, Wikipedia.com

[71] Mell ve Grance, NIST, 2011, http://csrc.nist.gov/publications/PubsSPs.html#800-145

[72] Mell ve Grance, NIST, 2011, http://csrc.nist.gov/publications/PubsSPs.html#800-145

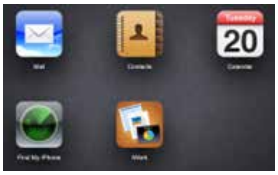
Hizmet Olarak Yazılım (SaaS): Tüketiciye, bulut altyapısı üzerinde çalışan sağlayıcı uygulamalarını kullanma imkanı sağlanır. Uygulamalara, bir web tarayıcısı gibi bir küçük istemci arabirimi (örneğin web tabanlı e-posta) veya bir program arabirimi aracılığıyla çeşitli istemci cihazlardan erişilebilir. Tüketici, kullanıcıya özgü olası sınırlı uygulama ayarları istisnası dışında, (ağ, sunucular, işletim sistemleri veya depolama da dahil olmak üzere) altta çalışan bulut altyapısını ve hatta münferit uygulamaları yönetmez veya kontrol etmez.

Hizmet Olarak Platform (PaaS): Tüketiciye, sağlayıcı tarafından desteklenen programlama dilleri, kitaplıklar, hizmetler ve araçlar kullanılarak, tüketici tarafından oluşturulan veya edinilen uygulamaları bulut altyapısı üzerine kurma imkanı sağlanır. Tüketici, (ağ, sunucular, işletim sistemleri veya depolama da dahil olmak üzere) altta çalışan bulut altyapısını yönetmez veya kontrol etmez, ancak kurulan uygulamalar ve muhtemelen uygulama barındırma ortamına ilişkin yapılandırma ayarları üzerinde kontrole sahiptir.

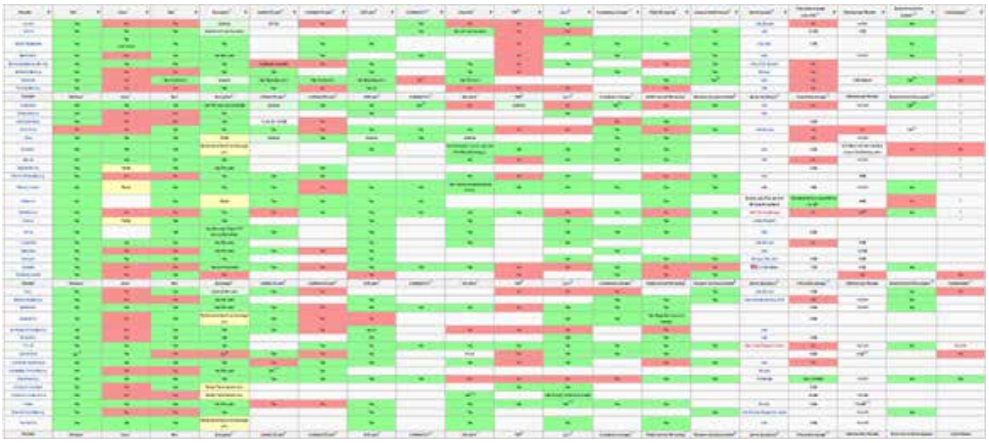
Hizmet Olarak Altyapı (IaaS): Tüketiciye; veri işleme, depolama, ağ ve diğer temel bilgi işlem kaynakları sağlanır ve (işletim sistemleri ve uygulamalar da dahil olmak üzere) isteğe bağlı yazılımlar kurma ve çalıştırma imkanı sağlanır. Tüketici, altta çalışan bulut altyapısını yönetmez veya kontrol etmez, ancak işletim sistemleri, depolama ve kurulmuş uygulamalar konusunda "kapsamlı seçme özgürlüğüne" ve muhtemelen belirli ağ bileşenlerine (örneğin ana bilgisayar güvenlik duvarları) ilişkin sınırlı kontrole sahiptir.

Bulut ve çevrimiçi depolama hizmetlerine ilişkin bazı örnekler:

Hizmet (Servis)	Tanım	Ekran görüntüsü
amazon web services	Amazon, çok çeşitli web hizmetleri sunmaktadır. Sahip oldukları Elastic Compute Cloud (EC2), dünya çapındaki en büyük bulut hizmetlerinden biridir. Tipik IaaS hizmetleri sunmaktadırlar. http://aws.amazon.com/en/ec2/	
OneDrive	Microsoft OneDrive, müşterilerine, Microsoft Office entegrasyonu ile büyük miktarda çevrimiçi depolama alanı sunmaktadır. https://onedrive.live.com	
Google	Google Dokümanlar, belgeler için büyük miktarda ücretsiz çevrimiçi depolama alanı sunmaktadır. Tarayıcı içinde elektronik tablolar, metin belgeleri, sunumlar vb. oluşturmak için çok kullanıcılı Wysiwyg (ekranda gördüğünüzle aynı çıktıyı elde edersiniz) tipi editörler sunmaktadırlar. https://docs.google.com/	

Hizmet (Servis)	Tanım	Ekran görüntüsü
Google Drive	Google Drive, bir aylık ücret karşılığında yükseltilebilen, sınırlı miktarda ücretsiz çevrimiçi depolama alanı sunmaktadır. Kullanıcı, her türlü veriyi yükleyebilir, senkronize edebilir ve paylaşabilir, ayrıca Google dokümanlar belgelerine de erişebilir. https://drive.google.com/	
Dropbox	Dropbox, profesyonel planlar satın alınarak genişletilebilecek sınırlı miktarda ücretsiz çevrimiçi depolama alanı sunmaktadır. Onların uzmanlığı; Windows, Linux, MacOS, iOS, Android vb. gibi çok çeşitli farklı cihaz işletim sistemleri arasında dosyaların senkronizasyonudur. https://www.dropbox.com	
iCloud	Apple, müşterilerine iCloud üzerinde ücretsiz sınırlı, genişletilebilir depolama alanı sunmaktadır. Bu hizmet, verileri Apple cihazlar ve iTunes yazılımını çalıştıran bilgisayarlar arasında senkronize edebilir. https://www.icloud.com	

Çevrimiçi depolama sağlayıcıların ve bulut sağlayıcıların tam listesi Wikipedia›da bulunabilir:[73]



Müfettiş açısından bulut bilişimin ilginç yönü, verilerin tek bir fiziksel bilgisayarda değil, birden çok sunucuda saklanmasıdır. Çoğu zaman bir bulut hizmetinin sağlayıcısı bile belirli verilerin nerede depolandığını söyleyemez. Diğer bir ilginç yönü ise, bulut hizmetlerinin, kelime işlemci veya muhasebe yazılımı gibi yazılım hizmetlerinden başlayarak tüm çalışan iş istasyonlarının tamamen değiştirilmesine kadar bir şirketin bilişim altyapısının hemen her parçasının yerini alabilmesidir.

[73] http://en.wikipedia.org/wiki/Comparison_of_online_backup_services.

Sonuç olarak, bir şirketin bilgisayarlarından bir tek bayt boyutunda bile veri alınamayan durumlar olacaktır, çünkü bunlar yalnızca kendilerine ait herhangi bir deposu olmayan, ancak buluttaki bir sanal makinenin kaynaklarını kullanan "küçük istemciler"[74] olacaktır. Bunun avantajı, teknik olarak sanal makinenin kolaylıkla kopyalanabilmesidir. Ancak ilgili ve geçerli mevzuata bağlı olarak, bu tür verilerin ele geçirilmesi için uygun yasal iznin tespit edilmesi ve alınması bir sorun olabilir. Aynı zamanda verilerin, talepte bulunan ülkedeki yasal prosedürlere uygun olarak elde edilmiş olduğundan emin olmak da zor olabilir.

Diğer bir dezavantaj, muhtemelen bulunabilecek çok daha az kurtarılabilir veri olmasıdır. Nitekim, bir şüpheli işlediği suçları işlemek amacıyla geçici bir sanal makine oluşturur ve ardından da bu makineyi silerse, kurtarılacak hiçbir delil olmayabilir.

Bir müfettiş, ağ erişimi olan çalışır durumdaki bir sistemle karşılaşırsa ve bulut bilişim kullanıldığından şüphelenirse, şunları yapmalıdır:

- Yukarıda bahsedilen hizmetlerin logolarına benzeyen tepsi simgelerine bakın;
- Bulut hizmetlerine ilişkin yüklenmiş yazılımları kontrol edin;
- Bulut hizmetlerinin adları için işlem listesine bakın;
- Ağ paylaşımlarına ve eşlenmiş ağ sürücülerine bakın;
- Ağ trafiğini gözlemleyin;
- Şüpheli etkinlik için açık soketlerin veya dinleme soketlerinin listesini izleyin;
- Uzaktan depolanmış gibi görünen tüm verileri alın. Her ne kadar bir çevrimiçi depolama hizmetinin, verileri bilgisayarın sabit sürücüsü ile senkronize etmesi mümkünse de, bu senkronizasyona asla güvenilmemelidir.

Müfettiş tüm geçici verileri ve kısa süreli verileri elde ettikten sonra aşağıdaki şekilde ilerleyebilir:

- Güç kaynağı kablosunu hedef ekipmandan çıkarın ve bu işlemi yaptığınız zamanı kaydedin (bilgisayar sistemi bir kesintisiz güç kaynağına (UPS) bağlı olabileceği için bilgisayarı, fişi prizden çekmek suretiyle **kapatmayın**).
- Depolama ortamlarını ilgili sürücülerden çıkarın; söz konusu ortamları orijinal kutularına/kılıflarına yerleştirin ve uygun şekilde etiketleyin. DVD'leri **çıkarmayın** veya DVD sürücüsündeki herhangi bir düğmeye dokunmayın.
- Bağlı olan tüm ağ bağlantılarını sökün
- Eğer taşınabilir bir cihazla uğraşıyorsanız, ayrıca pilini de çıkarın. Varsa ek pil paketlerini de çıkarın.

---

[74] Bir "küçük istemci", aslında sadece başka bir uzak konumda çalışan bilgisayar programlarına erişmek için kullanılan bir portaldır. Aslında bilgisayarın kendisinde hiçbir şey yapılmamaktadır.

3.5.4 Yönetici İzni

Bazen bir şirketin ağ kaynaklarının bir kısmı veya tamamı dahi harici şirketler tarafından yönetilir ve uzak konumlarda barındırılır. Uzak depolamayla ilgili sorunlardan biri, müfettişin muhtemelen oraya şahsen gitme veya başka müfettişleri gönderme imkanına sahip olmamasıdır. Bu gibi durumlarda, uzak sistem yöneticisinin işbirliği çok değerli olabilir. Koşullara bağlı olarak, uzak sistem yöneticisi ve şirketin başındaki kişi ve hukuk departmanı temsilcisi ile bir telefon görüşmesi/sesli konferans düzenlemek iyi bir fikir olabilir (soruşturma altındaki konuyla ilgili olarak şüpheli oldukları düşünülmüyorsa).

Çoğu durumda yöneticiler, bir soruşturmada işbirliği yapmalarına izin verilip verilmediğinden emin değildir. Talebin hukuka uygun olarak yapıldığı hukuki yaptırım davalarında, ancak söz konusu uzak konumun farklı yasal kurallara ve prosedürlere sahip başka bir ülkede bulunması durumunda bu bir sorun olabilir. Verilerin sahibi olan şirketin başındaki kişi hukuk departmanından izin alabilirse ve yöneticiye soruşturmada işbirliği yapma yetkisi verirse işler daha kolay hale gelebilir.

Bu gibi durumlarda "işbirliği" uzak sistem yöneticisinin tüm veri edinme işini yapacağı anlamına gelmez. Aslında durum bunun tam tersidir: Müfettişlerin tüm delil niteliği taşıyan verileri kendilerinin araması ve elde etmesi gerekirken, yöneticinin sisteme ancak gerektiği ölçüde erişmesine izin verilmelidir. Yöneticinin işbirliğine sadece altyapı hakkında bilgi vermesi ve bir sunucunun, iş istasyonunun veya yazılım işlevlerinin belirli alanlarına erişim haklarını vermesi için ihtiyaç duyulur. Büyük bir işletmenin elinde ayrıca elektronik keşif (bulma) çözümleri de olabilir. Müfettiş bunu özellikle sormalıdır çünkü bu sayede tespit edilemez uzaktan aramalar yapabilecek ve şirketin belirli sistemlerine veya tüm sistemlerine (geçici veriler de dahil olmak üzere) erişip ele geçirebilecektir.

4 İnternetten Delil Toplama

Bu bölümde, çevrimiçi delillerin elde edilmesi ile ilgili teknik ve metodolojik prosedürleri inceleyeceğiz. Elde edilen delillerin "şeffaflığı" ve "kalitesi" gibi hususları vurgulayacağız, çünkü bu özellikler daha sonra delillerinizin kabul edilebilirliği sorgulandığında çok önemli bir rol oynayacaktır. Bu bölümde, internetteki herkese açık bilgilerden delil elde edilmesinin yanı sıra gizli internet soruşturmaları ile ilgili hususlar da ele alınmaktadır. Bunlardan ikincisi çok daha karmaşıktır çünkü farklı yetki alanları arasında önemli mevzuat ve uygulama farklılıkları vardır. Bu tür soruşturmaların yürütülmesi, Bölüm 3'te özetlenen faaliyetlerin yürütülmesi için gerekenlere göre ilave bir takım bilgi ve beceriler gerektirmektedir.

Delillerin kabul edilebilirliği hususunda, bu belgede belirli bir yasal çerçeve referans alınmayacak ve dolayısıyla bu husus belirli bir yasal düzenleme rejimine dayandırılmayacaktır. Okuyucular, faaliyet gösterdikleri yargı bölgesinde yasal olan eylemlerde bulunduklarından emin olmalıdırlar. Ayrıca, açık kaynaklı bilgi ve istihbaratın ne olduğu ve dolayısıyla çoğu ülkede yürütülmesi için daha üst düzeyde yetki gerektirecek olan gizli istihbarat faaliyetinin kapsamına nelerin gireceği de bilinmelidir.

Genel yaklaşım, okuyucuların veri elde etme sürecinin arkasındaki mantığı anlamalarına olanak tanıyacaktır ve bu da onların genel kavramları mevcut kaynaklara ve ilgili mevzuata göre uyarlamalarını sağlamalıdır. Müfettiş, belirli bir ülkedeki ve yasal çerçevedeki kullanım amacına yönelik olarak bugün elde edilen herhangi bir delilin gelecekte pekala başka bir yerde de gerekebileceğinin özellikle bilincinde olmalıdır. Bu nedenle, veri toplama işleminin gerçekleştirilmesi; kullanılabilir, aktarılabilir ve istihbarat ve kovuşturma sürecinde incelenebilir olmasını sağlamak için biraz tutarlılık ve bir miktar da denetim ve kayıt gerektirir.

Son olarak okuyucuya bu bölümün, bu Kılavuzdaki önceki bölümlerden biraz daha yüksek bir teknik altyapı gerektireceği belirtilmelidir. Az teknik altyapıya sahip olanların da genel kavramları kavramaları açısından bu bölümü okumaları faydalıdır. Bu, ekipteki diğer teknik uzmanlardan geçerli bir veri elde etme metodolojisi kullanmasını beklemelerini ve kullanıldığından emin olmalarını sağlayacaktır.

4.1 Delil Olarak "Karma (Mashup)" Web Siteleri

Güncel bir Wikipedia makalesine göre:

"Karma (mashup) web sitesinin temel özellikleri birleştirme, görselleştirme ve bir araya toplamadır… [...] Geçtiğimiz yıllarda [metinde aynen], gittikçe daha çok web uygulaması, yazılım geliştiricilerin verileri ve işlevleri kendi başlarına oluşturmak yerine kolayca entegre etmelerini sağlayan API'ler[75] yayınlamıştır."

Bu karma konseptini internet soruşturmalarına uygulamak için müfettiş, ham veriyi Amazon S3[76] üzerinde depolayan, Facebook kimlik doğrulaması kullanan, PayPal[77]

[75] Uygulama Programı Arayüzü (API), programcıların belirli bir işletim sistemi için yazılım geliştirirken kullanabileceği bir dizi komut, işlev ve protokoldür. Kaynak: www.techterms.com/definition/api

[76] Amazon Basit Depolama Hizmeti.

[77] Güvenli bir çevrimiçi ödeme sistemi.

aracılığıyla ödeme alan ve abone kullanıcılarına Twitter üzerinden ilgili etkinlik hakkında gerçek zamanlı "push" bildirimleri sağlayan bir web hizmeti düşünebilir. Böyle bir çevrimiçi hizmet, geniş bir yelpazedeki çeşitli alt hizmetleri (veya ilgili web sitelerini) "bir araya getirir". Bizim için daha önemli olan husus, çevrimiçi delillerin bu alt hizmetler/sağlayıcılar/şirketler arasında da dağılmış olmasıdır. Çevrimiçi delil toplama sürecinde gerçek dünya senaryosuna hoş geldiniz!

Bu "bir araya getirme" örneği internette son derece yaygındır ve her ne kadar ilk bakışta tüm bu farklı kaynaklardan delil "toplamak" zor bir iş gibi görünse de, bazen müfettişe daha büyük delil değerine sahip veriler sağladığı ortaya çıkabilir: Soruşturmanızın olası sonucu ile ilgili olarak menfaatleri/beklentileri olan tek bir delil kaynağı (şirket) yoktur. Birçok çevrimiçi hizmetin karma (toplam) kalitesi, dolayısıyla herhangi bir işlemde dahli olan birçok "üçüncü taraf" oluşturabilir. Bu, daha sonra da göreceğimiz gibi, müfettişin daha güvenilir olma şansı olan deliller sunmasına yardımcı olacaktır.

Diğer durumlarda müfettiş, farklı çevrimiçi sağlayıcıların belirli bir gerçeği farklı ve bağımsız kaynaklardan doğrulayabildiğini bulacaktır (İnternetin doğası göz önüne alındığında, gerçeklerin hepsinin tek bir kaynaktan alıntı yapmamasına dikkat edilmelidir). Örneğin, Gmail'in "X" IP adresine sahip bir makineden okunan ETrade Inc.[78] (çevrimiçi ticaret şirketi) için bir kullanıcı adı ve şifre aldığı bir içeriden bilgiye dayalı ticaret senaryosunu ele alalım. Dakikalar sonra XE.com (bir döviz kuru bilgi portalı), aynı "X" IP adresinden, soruşturmanızla ilgili belirli döviz kurlarını öğrenmek isteyen sorgular alıyor. ETrade Inc. daha sonra yine aynı "X" IP adresinden satın alma talimatları almaya başlıyor. Müfettiş artık aynı IP adresine yapılan bağlantılar ile birbirini doğrulayacak olan ETrade günlüklerine, Gmail günlüklerine ve XE.com günlüklerine başvurabilir.

Tüm bu "Çevrimiçi Deliller", ortaya çıkan delillerin kabul edilebilirliklerini garanti altına almak için elde edilmeleri konusunda özel prosedürler gerektirir.

4.2 Sanal Konum ile Fiziksel Konum Karşılaştırması

İnternet, dünyadaki bilgisayarları cihazlar ve protokoller aracılığıyla birbirine bağlayan küresel bir ağdır. Düzenlemeleri ve standartları belirleyen birkaç kuruluş olmasına rağmen, küresel ağdaki her bir ağ düğümü, tasarımı ve bakımı sadece tek bir kuruluşa bağımlı olmayan bağımsız bir alt ağ olabilir. İnternete farklı türde teknolojiler aracılığıyla erişilebilmekte ve bu da internet aracılığıyla sunulabilecek hizmetlerin ufkunu genişletmektedir.

Çevrimiçi delillerle uğraşırken, müfettiş *"sanal"* dünya ile *"fiziksel"* dünyayı net bir şekilde ayırt edebilmeli ve bunları birbirlerine dönüştürebilmelidir. Sanal dünyada bir «konum» (benim delilim *nerede*?) genellikle URI/URL[79] veya nihayetinde bir IP adresi olarak adlandırılan bir şeye dönüştürülür. İhtiyaç duyan okuyucular için, URL, DNS ve IP adresleri gibi terimlerin teknik arka planına dair basit ve anlaşılır bir inceleme aşağıdadır. Teknik okuyucu bu bölümü atlamak isteyebilir.

---

[78] Bu isim, bu belge amacıyla kullanılan hayali bir isimdir ve gerçekte herhangi bir tüzel veya gerçek kişilikle bağlantısı yoktur.

[79] Tekdüzen Kaynak Tanımlayıcı veya Tekdüzen Kaynak Konum Belirleyici, Dünya Çapında Ağ üzerindeki bir konumun adı veya adresi olarak işlev gören karakter dizisidir.

4.2.1 IP (İnternet Protokolü) Adresi

İnternet Protokolü, internet üzerinden veri göndermek veya almak için kullanılan en yerleşik standartlar ve kurallar kümesidir. IP Adresi, internette bulunan en temel kaynak bilgi türüdür. Veri paketlerinin nereden geldiğini ve nereye teslim edileceğini gösterir. IPv4 (IP sürüm 4, yaygın olarak sadece «IP» olarak anılır) ve IPv6 (IP sürüm 6) adresleri olmak üzere iki tür IP adresi vardır.

Bir **IPv4** adresi, nokta (".") ile ayrılmış dört sayıdan oluşan bir dizgidir. Her sayı 0 ile 255 arasında bir değer alabilir. (Örneğin 192.168.1.252).

Bir **IPv6** adresi ise dört adet onaltılık basamaktan oluşan sekiz gruptan ibarettir. Her grup iki nokta üst üste ile ayrılır (örneğin 2001:0db8:85a3:0042:0000:8a2e: 0370:7334).

Onaltılık (Hex) her bilgi işlem konuşmasında ortaya çıkan ve bu kılavuzu okuyanların bazısına garip gelebilecek bir kavramdır. Hex, 16 tabanını kullanan bir numaralandırma sistemidir. Bu, bizim 10 tabanlı ondalık numaralandırma sistemimizden ve bilgisayarın 2 tabanlı ikilik numaralandırma sisteminden önemli ölçüde farklıdır. Bu nedenle onaltılık sayılar, 0 ile 9 arasındaki rakamlar ve A ile F arasındaki harfler olarak 16 farklı karaktere sahiptir. İkisinin bir karışımı olan sayılar görmemizin nedeni budur.

İnternet Tahsisli Sayılar Kurumu (IANA), IP adreslerini düzenler ve bölgesel kuruluşlar aracılığıyla Bölgesel İnternet Kayıtları (RIR) olarak bilinen IP adreslerinin tahsisini koordine eder:

RIPE	(Avrupa ve Asya'nın bazı bölgeleri)
APNIC	(Asya ve Pasifik Bölgesi)
ARIN	(Kuzey Amerika)
LACNIC	(Latin Amerika ve Karayipler)
AfriNIC	(Afrika)

IANA aynı zamanda özel ağlara (yani yerel ağlara) tahsis edilecek adres alanlarını da tanımlamıştır. Bu alanlar şunlardır:

10.0.0.0 ila 10.255.255.255	– *Sınıf A*
172.16.0.0 ila 172.31.255.255	– *Sınıf B*
192.168.0.0 ila 192.168.255.255	– *Sınıf C*

Bu adreslere genellikle "özel IP adresleri" denir ve "yönlendirilemez" oldukları söylenir. Başka bir deyişle, dahili bir ağ üzerindeki cihazları bağlarlar ancak internet üzerinde kullanılamazlar.

Bir İnternet Servis Sağlayıcısına bir IP adresi tahsis etmeye yönelik işlem oldukça basittir. IANA, her bölgesel kuruluşu, kendi bölgesindeki başvuru sahipleri için hangi IP adreslerinin müsait olduğu konusunda bilgilendirir. İnternet Servis Sağlayıcıları (ISP) daha sonra bölgesel kuruluşlarından IP adreslerinin tahsis edilmesini talep eder. Bir ISP bir dizi IP adresi aldığında, daha sonra bunları kendi müşterileri (son kullanıcılar) arasında dağıtarak devam edebilir ve her ISP kendisinin sorumlu olacağı ağı oluşturacaktır.

Diğer bir deyişle, IANA "pastayı" büyük parçalara böler, bölgesel kuruluşlar kendi parçalarını tekrar birden çok dilime bölerek ISP'ler arasında dağıtır ve ISP'ler de daha sonra kendi "pasta" dilimlerini müşterilere ayrı ayrı kiralanan kırıntılara indirger.

İnternete tam olarak aynı anda bağlı olan, birbiri ile tamamen aynı olan iki genel IP adresi olması mümkün değildir. Gerçek dünyadaki posta adresi gibi, etkin bir şekilde veri göndermek ve almak için katılan her makinenin benzersiz bir şekilde tanımlanması gerekir. Evdeki bir bilgisayar tarafından internete bağlantı yapıldığında, ISP bağlantı süresi boyunca o bilgisayara benzersiz bir IP adresi kiralar. Bu, IP adresinin, o bilgisayar tarafından o süre boyunca gerçekleştirilen tüm internet etkinlikleriyle ilişkilendirileceği anlamına gelir. Bağlantı iptal edildiğinde, söz konusu IP adresi başka bir bilgisayara yeniden tahsis edilebilir.

4.2.2 Dinamik IP Adresleri ile Statik IP Adresleri Karşılaştırması

IPv4 adresleri kavramına biraz matematik uygulanırsa, bu adreslerden müsait olanların sınırlı sayıda olduğu anlaşılır. IPv4 adresleri dört sayı kümesinden oluşur ve her sayı yalnızca 0 ile 255 arasında bir değer alabilir. Bu da, küresel olarak *sadece* 4,294,967,296 farklı benzersiz IPv4 adresi kombinasyonunun mevcut olduğu anlamına gelir (bu sayı 256 x 256 x 256 x 256 hesaplaması ile bulunur).

Kelimenin tam anlamıyla milyarlarca bilgisayar, cihaz ve insan internete bağlandığından, 4 milyar adresin yetersiz kalacağı açıktır. Bu durum, bu adreslerin ilk zamanlarda verimsiz bir şekilde tahsis edilmesiyle de birleşmektedir.

Bu nedenle İnternet Servis Sağlayıcıları, IP adresi havuzlarını, dinamik IPv4 adresleme adı verilen bir yöntem veya Operatör-düzeyi NAT[80] (CGN) adı verilen bir yöntem kullanarak (yani her IP adresi için ek bağlantı noktası adreslerinden yararlanarak) yönetmektedir. Diğer yandan, dört onaltılık sayıdan oluşan sekiz gruplu IPv6 adres formatı, sadece dünyadaki herkes için değil, aynı zamanda onların evlerindeki her cihaz ve tüm cihazlar için de yeterli IP adresi olduğu anlamına gelir (bkz. bölüm 4.2.3).

Daha önce de belirtildiği gibi, her İnternet Servis Sağlayıcısına bir dizi IP adresi tahsis edilmiştir. Bazı durumlarda, bir ISP'ye tahsis edilen IP adresi sayısı, sahip olduğu müşterilerin sayısından daha azdır. Ancak, müşteri sayısını elindeki adres sayısına uyacak şekilde sınırlamak ticari açıdan bir anlam ifade etmeyeceğinden, bu sorunu çözmeye yönelik teknolojiler ve protokoller geliştirilmiştir. En yaygın olanı Dinamik Ana Bilgisayar Yapılandırma Protokolüdür (DHCP).

DHCP, bir grup cihaza otomatik olarak bir IP adresi havuzu tahsis etmek için kullanılan bir protokoldür[81]. Bu protokolün iç işleyişi oldukça "basittir". Bir cihaz internete bağlanmak istediğinde ISP'sinden bir IP adresi ister. Daha sonra ISP "kullanılabilir IP adresleri listesine" bakar. O anda başka bir cihaza tahsis edilmemiş olan IP adreslerini kontrol eder ve bu "boş" IP adreslerinden birini talep eden istemciye (cihaza) tahsis eder. ISP, bunu yaparken, tarihi ve saati ve müşterinin kimliğini kütüğe kaydeder. İstemci İnternet'te oturumu kapatır kapatmaz, bu IP adresi başka bir cihaza tahsis edilmek üzere "kullanılabilir IP adresleri listesine" geri döner.

---

[80] Bu, mevcut sınırlı sayıdaki IPv4 adresini en üst düzeye çıkarmaya yönelik bir mekanizmadır.

[81] Yani, cihazların birbirleriyle iletişim kurması için bir dizi kural.

Bu, bir istemcinin veya cihazın, internete her bağlantı yapıldığında farklı bir IP adresi alabileceği anlamına gelir. Bazı durumlarda, IP adresi tek bir oturum sırasında bile birkaç kez değişebilir. Dolayısıyla bu bir "dinamik IP adresi" olacaktır.

Gerçek dünyada bir kişinin adresi sürekli değişseydi, o kişiye bir mektup göndermek neredeyse imkansız olurdu çünkü postane onu nereye teslim edeceğini bilemezdi. İnternette, IP adresinin her zaman bilinmesi gereken belirli cihaz türleri vardır. Bu gibi durumlarda "Statik IP adresleri" kullanılır. Bu, söz konusu cihazın sahibi ISP'nin müşterisi olarak kaldığı sürece, ISP'nin tek bir cihaza (müşteriye) belirli bir IP adresi tahsis etmesi anlamına gelir.

Çoğu ISP, Statik IP adresi olarak kullanılacak bir dizi IP adresi ve Dinamik IP adresi olarak kullanılacak başka bir dizi IP adresi tutmaktadır. Her iki durumda da, belirli bir zamanda bir IP adresinin kime tahsis edildiğini her zaman bilirler. Her ne kadar internete erişim sözleşmelerinin çoğu bir kuruluş veya bir kişi ile yapılacak olsa da, IP adreslerinin kişilere değil cihazlara tahsis edildiğini unutmayın.

Bir internet soruşturması sırasında bir IP adresi tespit edildiğinde, müfettiş, ilgili zaman aralığında IP adresinin tahsis edildiği cihaza ve hizmet sözleşmesine ilişkin ayrıntıları (genellikle bir mahkeme kararı ile) ISP'den isteyebilir. Müfettişin, belirli bir IP adresinin yürüttükleri soruşturma açısından önemli hale geldiği zamanı mutlak bir kesinlikle tam olarak belirleyebilmesi gerektiği vurgulanmalıdır. Aşağıdakilere bir göz atın:

Ne zaman?	Gizli tehlikeler...
30/03/2022 tarihinde IP X.X.X.X	O bir günün içinde o IP adresinin tahsis edildiği çok sayıda farklı kullanıcı olabilir.
30/03/2022 tarihinde, saat 16:30:12'de IP X.X.X.X	Tamam gibi görünüyor, ama "16:30:12" tam olarak ne zaman?
30/03/2022 tarihinde, saat 16:30:12'de (UTC-10) IP X.X.X.X	İlgili saat dilimini de içeren kesin saat budur

"UTC-10", bu durumda "(***C***) *Eşgüdümlü* (***U***) *Evrensel* (***T***) *Zaman* eksi 10 saat" (yani Hawaii) anlamına gelen, "zaman dilimi" olarak adlandırılan şeyi belirler. ISP'lere yapılan, IP adreslerine ilişkin isteklerde daima zaman dilimi gösterilmelidir.

Kullanılabilir IPv4 adreslerinin sayısının azalmasından bu yana, Operatör-düzeyi NAT'nin (CGN) bir süredir kolluk kuvvetleri için bir sorun olduğu netleşmiştir. NAT (Ağ Adresi Dönüşümü), birçok ağda, özel ve genel adreslerin birbirlerine dönüştürülmesinin ve böylece verilerin internet üzerinden gönderilebilmesinin yolu olarak kullanılmaktadır. Ancak aynı ilke, şebeke operatörlerinin (örneğin cep telefonu sağlayıcılarının) müşteri sayılarının, kendilerine sunulan IP adresi sayısını aştığı durumlarda onlar tarafından da kullanılmıştır. Mobil erişimli cihazların ve Nesnelerin İnterneti'nin (IoT) büyük ölçüde yaygınlaşmasıyla artık bu çok sık rastlanan bir senaryodur.

Her internet kullanıcısının, tanımlanması ve izlenmesi kolay olacak benzersiz bir IP adresine sahip olması yerine, kullanıcılar potansiyel olarak diğer birçok kişiyle birlikte, daha sonra NAT kullanılarak hizmet sağlayıcının ağı içinde dahili olarak yönetilen aynı adrese sahiptirler. İnternetteki etkinliklerin daha derinlemesine soruşturulmasını sağlayacak kayıtların tutulması sağlayıcılara bırakılmakta ve sıklıkla da yapılmamaktadır. Bunun anlamı, CGN kullanımının, İnternet Sağlayıcıların ve Hizmet Sağlayıcıların kim-

lik belirleme sürecinde kanun uygulayıcılardan gelen yasal taleplere uymasını teknik olarak imkansız kılmasa da zorlaştırabileceği ve suçluları tanımlamaya yönelik bilgilere erişimin mümkün olmayabileceğidir.

IPv6 uygulaması ile bu sorun elbette ortadan kalkacaktır (bir sonraki bölüme bakınız) ancak bunun gerçekleşmesinin zaman alacak olmasının teknik, lojistik ve mali sebepleri vardır.

4.2.3 IPv6

Yukarıda da görüldüğü gibi, kullanılabilir IPv4 adreslerinin sayısı sınırlıdır. IPv4'ü 1982 yılından beri kullanıyoruz, ancak yakın zamanda tahsis edilmemiş IPv4 adres alanı resmen tükenmiştir. Başka bir deyişle, daha fazla kullanılabilir IPv4 adresi kalmamıştır.

Neyse ki IPv6 imdada yetişmektedir! IPv6 da sınırsız adres alanına sahip değildir ancak onun alanı kesinlikle son derece büyüktür:

> 340 undesilyon; yani 340 trilyon, trilyon, trilyon adres
> (veya 340.000.000.000.000.000.000.000.000.000.000.000).

IPv6 adresleri, her biri iki nokta üst üste (":") ile ayrılmış 16 bitlik onaltılık değer bloklarına bölünmüş 128 bitlik bir sayı ile temsil edilir. Her blok, '0000' ile 'FFFF' arasında değişebilir - onaltılık sayı sistemi, 16 tabanına kadar bir numaralandırma sistemidir ve bu nedenle, 16 farklı olasılığı temsil etmek üzere 0 ila 9 arasındaki sayılar ve A ila F arasındaki harfler kullanılır.

Harflerin büyük/küçük olması fark etmez ve bir bloğun başındaki 0'lar (sıfırlar) gözardı edilebilir. Örneğin, Google'ın IPv6 adreslerinden biri şu şekilde gösterilir: 2001:4860:b002::68, ancak tam olarak yazıldığında IP adresi aslında 2001:4860:b002 :0000:0000:0000:0000:0068 biçimindedir.

Artık her cihazın veya bilgisayarın kendisine ait benzersiz IP adresi olabilir ve bu durum muhtemelen bir müfettişin hayatını kolaylaştıracaktır. IPv6'nın en çok ifade edilen faydalarından biri, İnternet Protokolü Güvenliği'nin (IPSec)[82] IPv6 standardına entegrasyonudur. IPv6 özellikle, (diğer şeylerin yanı sıra) veri gizliliği, veri bütünlüğü ve veri kaynağı kimlik doğrulaması sağlamaktadır. Tüm bunlar, nerede durduğunuza göre size iyi veya kötü haber gibi gelecektir. Örneğin, "veri gizliliği", bir şüphelinin veri göndermesi için serbestçe şifrelenmiş bir kanal sağlayana kadar veya sizin NIDS sisteminiz (*Ağa İzinsiz Giriş Tespit Sistemi*), yeni IPv6 ağının çoğu uçtan-uca şifreli olduğu için işini yapamayacağına karar verene kadar kulağa hoş gelmektedir.

Karşılaşacağınız temel sorunlar şunlar olacaktır:

IPv6 kullanımını geciktirenler. Bazı kuruluşlar, IPv6'nın kaçınılmaz olan tam ölçekli kullanımını geciktirmektedir. Bu gibi durumlarda, DHCP ve Operatör-düzeyi NAT teknolojilerinin kullanımı hızla artmaktadır. DHCP/NAT uygulama düzeyinde yeterli "kayıt tutma" işlemi yapılmamışsa, bu durum izlenebilirlik açısından kötü bir şey olabilir.

---

[82] İnternet Protokolü Güvenliği (IPSec), internet üzerinden kimlik doğrulamaya ve şifrelemeye imkan tanıyan bir güvenlik çerçevesidir.

IPv6'yı "test edenler". Birçok ISP, yeni sistemin kontrollü bir şekilde "yayınlanması" sürecinin bir parçası olarak IPv6 için kurulum test platformlarına sahiptir. Bu platformlar genellikle yeni IPv6 test imkanını, IPv4'te çalışan bir çekirdek ağa bağlar. Platform sadece test/kısmi kullanım aşamasında olduğundan, eksik kayıt tutulmaktadır ve kolluk kuvvetleri IP adreslerini sadece IPv4'ün IPv6 ile buluştuğu yere kadar takip edebilir.

Tembel ISP'ler. Bölgesel İnternet Kayıtları (RIR), ISP›ler üzerinde, Whois[83] veritabanlarını güncel tutmaları için gayri resmi olarak bir miktar baskı uygulamaktadır. Devasa IPv6 adresi bloklarının tahsis edilmesi, RIR'nin uygulayabildiği baskıyı sınırlamıştır. Bu, Whois verilerinin geçmişte olduğu kadar güvenilir veya kolay erişilir olmayabileceği anlamına gelir.

Yeni teknoloji/eski sorunlar. Her yeni sistemde olduğu gibi, IPv6 da yeni güvenlik sorunları doğurmaktadır. Örneğin, IPv6 yığınlarında yeni güvenlik açıkları bulunmaktadır, yanlış IPv6 düzenlemeleri ve yapılandırmaları nedeniyle güvenlik duvarları birden tamamen açılmaktadır, IDS'ler (İzinsiz Giriş Tespit Sistemleri) IPv6'yı işlemek üzere güncellenmemiştir, vb.

Siperlerin kazılması. IPv6 tamamen uygulamaya koyulana kadar, bir müfettiş IPv4 üzerinden tünellenmiş IPv6 veya tam tersi ile karşı karşıya kalabilir! Başka bir deyişle, bir IPv6 paketi bir veya daha fazla IPv4 paketi içinde kapsüllenmiş ("içine doldurulmuş") veya tam tersi olabilir. Elbette bu, mevcut diğer tüm tünelleme teknolojileriyle de karışacaktır; dolayısıyla IPv6'nın IPv4 üzerinde gittiğini ve onun da diğer taşıma protokolleri üzerinde kendisi de daha fazla kapsüllenmiş olabilecek bir VPN tüneli üzerinden gittiğini görmek mümkündür. Diğer bir deyişle, geçiş dönemi boyunca IP adresleri, etkileşimleri nedeniyle maskelenebilir ve karıştırılabilir ve bu nedenle de takip edilmesi zor olabilir.

4.2.4 DNS veya Alan Adı Sistemi

Daha önce de belirtildiği gibi, İnternette belirli bir düğüm noktası ile iletişim kurmak için IP adresi hakkında bilgi sahibi olmak gereklidir. Sorun şu ki, insanlar noktalarla ayrılmış dört sayının birleşiminden oluşan adresleri veya bir IPv6 adresindeki sayı ve harf yığılarını hatırlamak konusunda pek iyi değillerdir. Her cihazın bir dizi sayı yerine insan için hatırlaması kolay bir adresi olsa, bu bizim için kesinlikle işleri kolaylaştıracaktı. Buna imkan tanımak amacıyla Alan Adı Sistemi (DNS) adlı bir protokol oluşturulmuştur.

İnsan dostu adresler, genellikle Tam Tanımlanmış Alan Adları (FQDN›ler) veya kısaca «alan adları» olarak bilinir ve belirli bir biçim içinde sıralanmış harflerden ve sayılardan oluşur (örneğin www.coe.int).

DNS, büyük bir dinamik telefon rehberi gibi davranan ve hangi IP adresinin/adreslerinin hangi "ad"a ve hangi adın hangi IP adresine/adreslerine tahsis edildiğinin kaydını tutan bir sistemdir. Aralarındaki ilişki her zaman bir IP adresine bir ad biçiminde değildir (örneğin bir ad birden fazla IP adresine tahsis edilebilir ve bunun tersi de mümkündür).

---

[83] Bu, alan (web sitesi) adreslerinin kime ait olduğuna ilişkin ayrıntıları içeren bir veritabanıdır.

Her zaman erişilebilir olması gereken bir internet hizmeti hayal edelim (Bu tür hizmetler; internet arama motorlarını, çevrimiçi bankacılığı, internet postasını vb. içerir). Kullanıcıların o hizmete her zaman bağlanabilmesini sağlamak için hizmet sağlayıcı, bir web sitesinin birden çok kopyasını farklı bilgisayarlar içinde oluşturur. Bu bilgisayarların her birinin farklı bir IP adresi vardır, ancak hepsi ortak bir ada cevap verebilir. Öte yandan, tek bir IP adresinin birkaç alan adına yanıt verdiği senaryolar da mevcuttur. Site barındırma şirketleri, her bir alan adını farklı bir bilgisayarda (yani farklı IP adresleriyle) barındırmak yerine maliyetleri ve yönetimi azaltmak için bu mekanizmayı kullanmaktadır.

Alan adları, internet üzerinde iki kuruluş tarafından etkin bir şekilde yönetilmektedir:

- .com, .net, .org, .biz vb. gibi Genel Üst Düzey Alan Adları (gTLD'ler), ICANN (Tahsis Edilen Adlar ve Numaralar için İnternet Kurumu - www.icann.org) tarafından tescil edilmektedir.
- .us, .uk, .de, .ie, vb. gibi Ülke Kodu Üst Düzey Alan Adları (ccTLD'ler), tescil görevini Nominet UK, Denic eG, IE Domain Registry Limited ve benzerleri gibi yerel Tescil Kuruluşlarına devreden IANA (İnternet Tahsisli Numaralar Kurumu) tarafından tescil edilmektedir.

Bir alan adı bir gizlilik koruma şirketi tarafından tescil edilmediyse, bu kayıtlar bir alan adının sahibi hakkında müfettişin erişimine açık olabilecek değerli bilgileri açığa çıkarabilir. ICANN Tescil Kuruluşlarının bir listesi ICANN web sitesinde (www.icann.org/registrar-reports/accreditation-qualified-list.html), tüm ccTLD Tescil Kuruluşlarının bir listesi de IANA web sitesinde (www.iana.org/domains/root/db) bulunabilir.

Son yıllarda bu kayıtlardan elde edilen bilgilere erişim, GDPR (Genel Veri Koruma Yönetmeliği) gibi gizlilik kurallarından ve düzenleyici kurallardan etkilenmiştir. Bu, bilgilerin sicillere sağlanması ve onlar tarafından saklanması gerekmesine rağmen, artık çevrimiçi taleplerde bulunulduğunda ayrıntıları gizleyebilecekleri anlamına gelir. Müfettiş için bunun anlamı, verilerin sahibini belirlemek için sağlanan bilgileri kullanmak ve ardından da onları daha "çevrimdışı" bir şekilde görmek için resmi talepte bulunmaktır.

Tahmin edilebileceği gibi, milyonlarca FQDN bulunmaktadır ve bu devasa veritabanını yönetmek tek bir makine için imkansız bir görevdir. Bu görevi basitleştirmek için Alan Adı Sistemi, ad çözümlemelerini gerçekleştirmek üzere birden çok küresel olarak dağıtılmış sunucu ve (alan adını IP adresine bağlayan) bir ağaç yapısı kullanmaktadır.

Bir FQDN'nin her bir bölümü farklı bir "alanı" ifade eder ve belirli bir anlama sahiptir. Belirsizlik olmamasını sağlamak için belirli bir düzen içinde yerleştirilmişlerdir ve sadece tek bir şekilde yorumlanabilirler. Bir FQDN genellikle bir ana bilgisayar adından ve en az bir üst düzey alan adından oluşur. Her zaman TLD ile bitmelidir.

Örnek olması açısından, aşağıda Avrupa Konseyi ile ilgili bir FQDN verilmiştir: https://rm.coe.int

Sağ tarafından okunmaya başlanırsa:

- "int" - TLD (Üst Düzey Alan)
- "coe" - TLD içindeki (bazen ikinci düzey alan olarak da adlandırılan) üst alan adı,

söz konusu TLD içinde böyle adlandırılmış sadece tek bir alan olabilir

- "rm" - ana alan içindeki ana bilgisayar adı. Bu, onu, "coe" alanı içindeki ana bilgisayar olduğu için, internette var olabilecek diğer "rm" ana bilgisayarlardan benzersiz bir şekilde ayırır.

Bu yapı takip edilerek belirsizlik ortadan kaldırılmış ve çok düzenli bir yapı oluşturulmuş olur. Bu, DNS'nin IP adreslerini çözümlemesine yardımcı olur. Bazen FQDN (yani https://rm.coe.int.) ardından '.' (nokta) karakterini görmek mümkündür. Bu, gerekli olduğu yerlerde DNS yapısındaki "kök" anlamına gelir.

Yukarıdaki çizim, DNS'nin gerçekte nasıl işlediğini göstermektedir. Pek çok yerde tutulan yerel DNS önbellekleri vardır, ancak nihayetinde, eğer internette bir kaynak bulma ihtiyacı varsa, o durumda da yerel olarak bilinmiyorsa, biri bilgi sağlayana kadar sorgu köke doğru yukarıya ilerletilir. Nihayetinde sorgu, onu nasıl ve nerede çözeceğini bilen "kök"e kadar gidebilir.

Çizimde sol taraftaki dizgiyi basitleştirirsek, ‹kök›, TLD olan ‹.org›un nerede olduğunu bilir, TLD içinde «wikipedia.org» olduğunu bilir ve bu üst alan içinde ‹en› - Wikipedia›nın İngilizce versiyonu - olduğunu bilir. Kurallara uyulduğu sürece, DNS söz konusu kaynağı bulacak ve bağlantının kurulabilmesi için ilgili IP adresini sağlayacaktır.

Bu durum göz önünde bulundurulduğunda, DNS iki nedenden dolayı internet bağlantılı soruşturmalar için çok zengin bir bilgi kaynağıdır:

- Bir FQDN'nin var olması için bir tescil sözleşmesi yapılması gereklidir. Her sözleşme bir yöneticinin iletişim bilgilerini içermelidir. Bu nedenle, o belirli FQDN'den hangi kuruluş veya kişinin sorumlu olduğunu bulmak mümkündür. Elbette bu bilgiler yanlış veya alan adı tescil kuruluşu tarafından korunuyor veya gizlilik düzenlemeleri nedeniyle gizlenmiş olabilir.
- FQDN'ler daha sonra IP adreslerine dönüştürüldüğü için, (önceki paragrafta da açıklandığı gibi IP adreslerinin dağıtılma şekli nedeniyle) bu IP adreslerini ayrıca birer internet erişimi sözleşmesine bağlamak da mümkündür.

4.2.5 Tekdüzen Kaynak Tanımlayıcı (URI)

URI, bir bilgisayar sistemindeki bir "kaynağın" veya bileşenin konumunu tanımlamak için kullanılan etikettir. URI'ler, bir kaynağa aynı ağdaki diğer cihazlar tarafından erişilmesi için bir yol sağlar. En yaygın URI, bir web sayfası adresidir ve Dünya Çapında Ağ boyunca etkileşime imkan tanır.

Dünya Çapında Ağ (WWW), internet üzerinden erişilebilen bağlantılı belgeler (web sayfaları) sistemidir (interneti kullanan fakat internet ile eşanlamlı olmayan bir ağdır). Web sayfaları, diğer nesnelere ve sayfalara bağlanmayı veya gitmeyi (yani Dünya Çapında Ağ'da gezinmeyi) mümkün kılan ve genellikle Bağlantılı Metin Biçimlendirme Dili (HTML) kodunda yazılan "bağlantılı metinler" kullanır. Web sayfaları genellikle Web Siteleri adı verilen yapılar içinde gruplandırılır.

Web tarayıcısı olarak bilinen (Microsoft Edge (eski adıyla Internet Explorer), Mozilla Firefox veya Google Chrome gibi) bir yazılım uygulaması kullanılarak Dünya Çapında Ağ'a ve alan adı veya URL'si (aşağıya bakın) bilinen bir özel web sayfasına erişilebilir. Bu sayfalar genellikle dünyanın herhangi bir yerinde bulunabilen Web Sunucularında barındırılmaktadır.

Web sitesi adreslerini ifade ettiğinde FQDN, Tekdüzen Kaynak Konum Belirleyici (URL) olarak bilinir. Bir FQDN ile bir URL arasındaki temel fark, URL'nin belirli bir kaynağa erişmek için gereken bilgileri içermesi ve o kaynak (veya sunucu) üzerinde tam olarak neye erişmek istediğinizi belirtmesidir.

Bağlantılı metin belgelerine erişmek ve bunları aktarmak için HTTP (veya HTTPS) protokolü kullanıldığından, herhangi bir web sitesi için URL'nin yapısı şöyle görünecektir:

http://www.web-sitesinin-ismi.com/web-sayfasının-ismi.php

4.2.6 URL ile URI Karşılaştırması

Tekdüzen Kaynak Konum Belirleyici (URL), Tekdüzen Kaynak Tanımlayıcı'nın en yaygın ve bilinen alt türüdür. Temel farkları, bir URI'nin web sayfaları veya web siteleri dışındaki kaynaklara erişmek için de kullanılabilmesidir.

URI'nin nasıl göründüğüne dair bazı örnekler şunlardır:

P2P ağları: ed2k://|file|Galactic_Council_Show.avi|14997504|345c013e991ee1d63d45ea71954d4d|/

Skype: callto:<screenname>

FaceTime: facetime://<address>|<MSISDN>|<mobile number>

Spotify: spotify: track:2jCnn1QPQ3E8ExtLe6INsx

4.2.7 Çevrimiçi Soruşturmalarınızda IP ve DNS Kayıtları

Okuyucular artık IP adreslerinin nasıl tahsis edildiğini ve DNS adlarının nasıl tescil edildiğini bildiğine göre, en temel çevrimiçi soruşturmalarına başlamaya hazırdır. DNS tescil şirketlerinden iletişim bilgilerini nasıl talep edeceklerini ve DNS'yi IP adreslerine nasıl çözümleyeceklerini (bağlayacaklarını) ve soruşturmaları sırasında bu IP adresle-

rini kimlerin kendilerine tahsis ettirdiği hakkında nasıl bilgi edineceklerini bilmektedirler.

DNS kayıtlarını sorgulamak ve DNS'yi IP adreslerine çözümlemek için kullanılan resmi kanallara ek olarak, bu konuda otomatikleştirme ve müfettişe yardımcı olma amacıyla tasarlanmış birçok araç ve web sitesi vardır. En bilinenlerden bazıları; DnsStuff (www.dnsstuff.com), DomainTools (www.domaintools.com) ve CentralOps (www.centralops.net) olup, daha birçokları da vardır. Bu siteler faydalı olsa da, veriyi asıl tescil şirketlerinden almanın en iyi uygulama olduğunu unutmamak önemlidir (bkz. bölüm 4.2.4). Üçüncü taraf sağlayıcıların sadece hangi isteğin gönderildiğini değil, aynı zamanda hangi IP adresini talep ettiğini de saklayamayacağını ve bu durumun bir kolluk IP adresini de ortaya çıkarabileceğini lütfen unutmayın.

4.2.7.1 *Whois araması*

Whois kayıtları, bir müfettişin belirli bir alan adının sahibini keşfetmesine yardımcı olabilir. Kayıtlar, bir alanın sahibinin *kim* olduğu, adı, soyadı, e-posta adresi ve fiziksel adresi, telefon numarası ve ilgili olabilecek diğer hususlar hakkında bilgiler içerir. Müfettiş, bu veriler üzerinde herhangi bir kalite veya doğruluk kontrolü yapılmadığını bilmelidir. Ayrıca GDPR'nin ortaya çıkmasıyla birçok yönden kısıtlanmıştır.

Domain Whois record

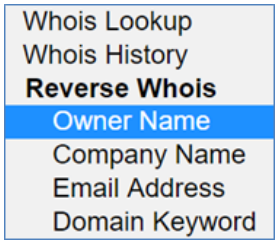
Queried **whois.iana.org** with **"coe.int"**...

```
domain:       COE.INT

organisation: Council of Europe
address:      Avenue de l'Europe
address:      Strasbourg  67000
address:      France

contact:      administrative
name:         Marc ULRICH
address:      Avenue de l'Europe
address:      Strasbourg  67000
address:      France
phone:        +3338841200
e-mail:       marc.ulrich@coe.int

contact:      technical
name:         Jean-Francois BILGER
address:      Avenue de l'Europe
address:      Strasbourg  67000
address:      France
phone:        +3338841200
e-mail:       jean-francois.bilger@coe.int
```

Yukarıdaki resim, popüler Whois araçlarından biri kullanılarak elde edilebilen www.coe.int alanı adıyla ilişkili bazı tescil ayrıntılarını göstermektedir.

4.2.7.2 *Tersine Whois*

Bu hizmet türü, sağlanan kimlik bilgisi altında (site/araç tarafından bilinen) tescilli tüm DNS/IP kayıtlarını listeler. Müfettiş genellikle ad, e-posta, telefon numarası veya fiziksel adres ile arama yapabilir.



Yukarıdaki resim, diğer bir popüler Whois aracında bulunan menü seçeneklerini göstermektedir.

4.2.7.3 *IP araması*

IP araması, müfettişin belirli bir IP adresi ile ilişkili tüm erişilebilir bilgileri bulmasına yardımcı olabilir. Müfettiş, Tescil Kuruluşunun hangisi olduğunu ve ait olduğu Ters DNS ve IP blok aralığını bulabilir. Çoğu araç/site, bulunduğu ülkeyi de belirleyecek ve hatta coğrafi konum, şehir ve hatta enlem ve boylam koordinatlarını sağlayacaktır.

Müfettiş, IP adresleri için coğrafi konum tekniklerinin kesin olmadığını ve doğruluğun bir hizmet sağlayıcıdan diğerine değişebileceğini bilmelidir. Daha fazla doğrulama yapılmadan asla bunlara güvenilmemelidir.

4.2.7.4 *Whois, Tersine Whois ve IP Araması Zaman Makinesi*

Müfettiş, DNS kayıtlarının zaman içinde değiştiğini veya doğru olmayabileceğini bilmelidir. Örneğin, bir DNS kaydında sahibi değiştirebilir veya bir alan adının sahibi, bir takım yasa dışı faaliyetlerde bulunmadan önce DNS kayıtlarındaki bilgilerini tahrif edebilir ve web sitesini uzak bir ülkeye taşıyabilir.

"Zaman Makinesi" adını verdiğimiz şey, temel olarak müfettişin DNS kayıtlarından geçmiş verileri almasına imkan tanıyan bir arayüzdür. Bu, bazı durumlarda ücretsiz olabilir veya diğer durumlarda küçük bir ödeme karşılığında elde edilebilir.

4.3 Çevrimiçi Bilgi Kaynakları

Bir soruşturma için faydalı olabilecek birçok çevrimiçi bilgi kaynağı mevcuttur. Bu bölümde, en yaygın çevrimiçi kaynak türleri, sağlayabilecekleri delil türleri ile birlikte listelenmiştir.

Çoğu açık kaynaklı soruşturmanın amacı, söz konusu soruşturma ile ilgili bilgi, istihbarat veya delil toplamaktır. Söz konusu veriler muhtemelen insanlar, işletmeler

veya yerler hakkında kişisel veya mesleki bilgiler içerecektir. Bu veriler; metin içerik, resimler veya video içerebilir. Potansiyel kaynakların sayısı düşünüldüğünde, günümüzde şaşırtıcı miktarda veri mevcuttur. Deliller etkili ve düzgün bir şekilde araştırılıp toplandığında diğer delil toplama yöntemlerinden önemli ölçüde daha ucuz olduğu gibi son derece de zorlayıcı olabileceğinden, birçok soruşturma kurumu artık büyük ölçüde çevrimiçi içeriğe güvenmektedir.

Çevrimiçi materyal toplamak için gittiğimiz platformların çoğu, aynı zamanda müfettişin toplaması ve anlaması gereken materyaller hakkında kullanılabilir başka bilgiler de sunacaktır. Aşağıdaki bölümlerde, kurtarılabilecek veri türleri ve bu işlemin nasıl yapılacağına ilişkin örnekler verilmektedir.

4.3.1 OSINT Araçları

İnsanlar internet üzerinden sosyal ağları giderek daha fazla kullanmaya ve içerik paylaşmaya yöneldikçe, sosyal medya profillerinde, web sitelerinin yorum bölümünde ve internetteki daha birçok yerde iz bırakmaktadır. Açık Kaynak İstihbarat (OSINT) araçları, müfettişlerin sadece bir ad, e-posta adresi veya anahtar sözcük girerek arama yapmasına ve bilgi elde etmesine yardımcı olabilir.

Birçok farklı platforma (örneğin Facebook, Twitter, Instagram, Pastebins, YouTube, vb.) yönelik birçok özel OSINT aracının yanı sıra daha ileri düzeydeki açık kaynak soruşturmaları için de başka birçok teknik araç bulunmaktadır. Bu bölümde sadece birkaç iyi bilinen araç listelenecek ve internette daha sık güncellenen ek referans listelerine dikkat çekilecektir.

Bir açık kaynak analizci tarafından kullanılabilecek ve kılavuz yayınlanmadan önce güncelliğini yitirecek tüm kaynakları listelemek mümkün değildir. Tarayıcı tabanlı olan ve tarayıcı eklentileri biçiminde olan araçlar bulunmaktadır. Ayrıca soruşturmalara yardımcı olmak için tasarlanmış bağımsız araçlar ve ısmarlama açık kaynaklı araştırma araçları da mevcuttur.

Suç ile ilgili açık kaynak araştırmasından bahsettiğimiz zaman, açık kaynak araştırması dünyasının, bir kolluk kuvveti analiz uzmanından daha yüksek teknik becerileri olabilecek bilgisayar ve güvenlik uzmanlarıyla dolu olduğunu da göz önünde bulundurmalıyız. Kolluk kuvvetleri için bu alanda araç kullanımı, kullanıcıların yeteneklerine uygun olmalıdır.

OSINT araştırması yapması gereken bir müfettiş, aşağıdaki web sitelerinde çok sayıda kaynak bulacaktır:

- github.com/Ph055a/OSINT_Collection
- github.com/jivoi/awesome-osint
- start.me/p/wMdQMQ/tools
- github.com/0x90/osint-arsenal
- osintframework.com
- www.toddington.com/ (kaynaklar)
- rr.reuser.biz/

- onstrat.com/osint/
- www.osintessentials.com/
- technisette.com/p/tools
- sector035.nl/links

Bu, hiçbir bakımdan eksiksiz bir liste değildir. Bu siteler tipik olarak kaynakları birlikte gruplayan; Instagram araştırmalarına yönelik araçlar, DNS bilgilerine yönelik araçlar, IP bilgilerine yönelik araçlar vb. gibi kategoriler içinde sıralanır.

Müfettişler ayrıca açık kaynak toplamaya yönelik ısmarlama araçların kullanımını da değerlendirebilirler; örneğin:

- OSIRT Tarayıcı - osirtbrowser.com
- Paliscope - www.paliscope.com
- Hunchly - www.hunch.ly
- Maltego - www.maltego.com

4.3.2 Google Arama İşleçleri

Google gibi arama motorları aslında birçok insanın düşündüğünden daha becerikli-dir. Çeşitli filtreleri ve arama işleçlerini yorumlayabilirler. Bir müfettiş, sorgusunu özel olarak çerçevelemek için bunu kullanabilir. Bu, yanlış pozitif bulguları azaltarak daha iyi ve hedefli sonuçlar alınmasına yol açabilir. Aşağıdaki liste, bazı arama işleçlerini ve bunların anlamlarını içerir:

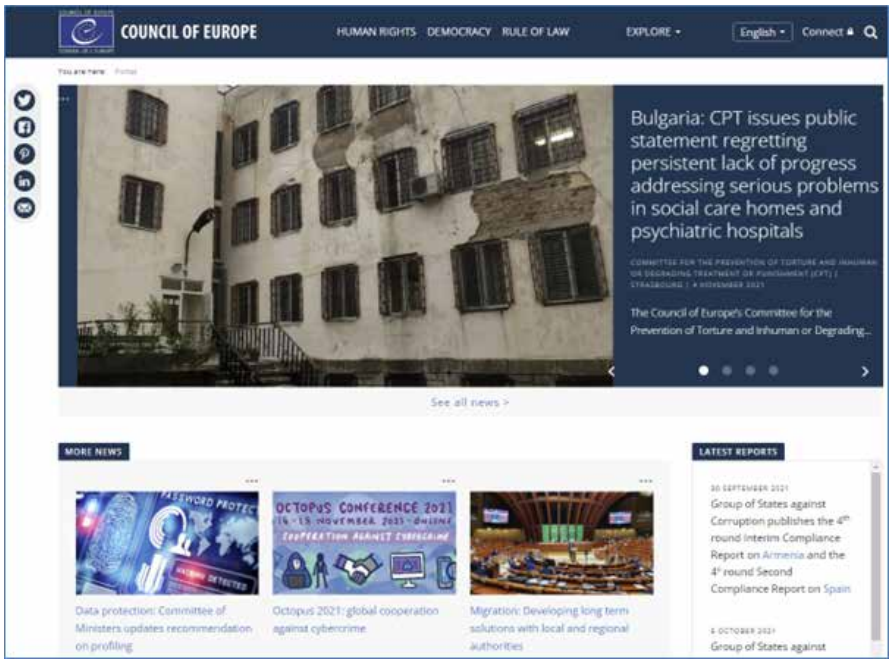
İşleç	Tanım	Örnekler
site:	Arama sorgusunu belirli bir alan adı veya web sitesi ile sınırlayın.	site:ornek.com
filetype:	Aramayı belirli bir dosya türü içinde bulunan metinle sınırlayın	blueprint filetype:pdf
link:	İstenen URL'ye bağlantı veren sayfaları arayın	www.coe.int
cache:	Bir web sayfasının Google tarafından tarandığı zaman görünen sürümünü arayın ve görüntüleyin.	cache:coe.int
intitle:	Bir metin dizgisini bir sayfanın başlığında arayın.	intitle:"index of"
inurl:	Bir dizgiyi bir URL içinde arayın	inurl:passwords.txt
related:	İlgili siteleri arayın	related:coe.int
imagesize:	Belirli bir boyuta sahip bir resim arayın	imagesize:300x200
scr:	Bir resme bağlantı veren tüm web sitelerini arar	src:example.com/logo.gif
AND veya +	Anahtar kelimeleri eklemek için kullanılır. Tüm anahtar kelimelerin bulunması gerekir.	konsey ANDavrupaANDsiber suç konsey + avrupa + siber suç
NOT veya –	Anahtar kelimeleri hariç tutmak için kullanılır. Tüm anahtar kelimelerin bulunması gerekir.	Elektronik delil NOT avrupa Elektronik delil –avrupa
OR veya |	Biri veya diğeri eşleşen anahtar kelimeleri dahil etmek için kullanılır. Tüm anahtar kelimelerin bulunması gerekir.	"avrupa konseyi" OR coe "avrupa konseyi" | coe

İşleç	Tanım	Örnekler
Yaklaşık işareti (~)	Eş anlamlıları ve benzer kelimeleri eklemek için kullanılır.	web uygulaması ~güvenlik
Çift tırnak (")	Tam eşleşmeleri eklemek için kullanılır.	"avrupa konseyi"
Nokta (.)	Tek bir joker karakter eklemek için kullanılır.	.vrupa konseyi
Asterisk (yıldız işareti) (*)	Tek bir joker kelime eklemek için kullanılır.	avrupa *
Parantez (())	Sorguları gruplandırmak için kullanılır	("avrupa konseyi" | coe)
Heşteg (başlık etiketi) (#)	Bir başlık etiketini arayın	#sibersuç
@ İşareti	Örneğin Twitter'da, sosyal medya profillerini arar	@coe

4.3.3 Web Siteleri

Web siteleri, internette bulunan en temel bilgi kaynağıdır. İlk potansiyel delil parçası, sitenin fiili olarak "görünür" olan içeriğidir. İkinci parça, o kadar bariz olmayan, bu siteler ile ilişkili olan "görünmez" veya arka plan içeriğidir. Buradaki görünmez içerik, web sayfasını oluşturmak için kullanılan "programlama dili" (HTML, CSS, Javascript, vb.) ve dolayısıyla sunucunun tarayıcıya gönderdiği asıl içeriktir. Tarayıcının yorumladığı ve ekranda görülen web sayfasını oluşturmak için kullandığı içerik budur.

Potansiyel olarak ekranda görünenden daha fazla bilgiye erişilebilir. Aşağıda bir web sayfası örneği ve aynı sayfanın altında yatan "kaynak kodun" kısmi dökümü (veya çıktısı) görülebilir.



Yukarıdaki resim, bir tarayıcı penceresinde görüldüğü haliyle Konseyin ana sayfasını göstermektedir. Tarayıcı bu içeriği siteyi barındıran web sunucusundan almakta ve

daha sonra aldığı bilgileri görüntülemeden önce yorumlamaktadır. Ancak gördüğümüz şey, sayfayı oluşturan kodun içindeki her şey değildir. Tarayıcı, kendisine verilen talimata göre görüntüler.

Bir web sayfasının temelini oluşturan kodu görmek için müfettiş, aşağıda görüldüğü gibi sayfadaki "beyaz alanın" herhangi bir yerine sağ tıklayıp "Sayfa Kaynağını Göster"i seçebilir.

Bu işlem, yeni bir tarayıcı penceresi açacak, ancak sayfayı görüntülenebilir biçiminde görüntülemek yerine, sayfayı oluşturan kaynak kodu gösterecektir. Aşağıda, daha önce sayfanın görünmesini sağlayan HTML kodunun baş kısmı verilmiştir. Her ne kadar ilk bakışta oldukça karmaşık görünse de, kaynak kodun nasıl yazıldığı hakkında biraz bilgi ile yorumlanabilir.

```
<!DOCTYPE html>
<html class="aui ltr default-site" dir="ltr" lang="en-GB">
<head>
<title>Council of Europe</title>
<meta content="text/html; charset=UTF-8" http-equiv="content-type" />
<meta content="The Council of Europe is the continent&#39;s leading human rights organisation. It includes 47 member states, 27
of which are members of the European Union." lang="en-GB" name="description" />
<meta name="format-detection" content="telephone=no"/>
<meta property="og:site_name" content="" />
<meta property="og:image" content="https://www.coe.int:443/documents/22041/2068574/1200x630_Portail__47943_031.jpg/64b59ca3-
54f2-c03e-791f-4ed97f73f90f?t=1552032757000" />
<meta property="og:description" content="The Council of Europe is the continent's leading human rights organisation. It
includes 47 member states, 27 of which are members of the European Union." />
<meta property="og:type" content="website" />
<meta property="og:title" content="Council of Europe" />
<meta property="og:url" content="https://www.coe.int/web/portal/home" />
<meta property="twitter:image"
```

HTML kodu, aşağıda görülen tanımlanmış bir yapı çerçevesine girecektir.

Sayfadaki her alanın bir başlangıç ve daha sonra da bir bitiş noktası vardır. Bitiş noktası '/' karakteriyle tanımlanır, böylece HTML kodunun tüm alanının belirli bir başlangıç ve bitiş noktası olduğunu görebiliriz, diğer yandan sayfanın diğer bileşenleri (başlık alanı ve gövde alanı) de benzer başlangıç ve bitiş noktalarına sahiptir. Bu noktaların arasında kalan her şey sayfanın ilgili kısmını oluşturur.

Görülebileceği gibi, daha fazla bilgi mevcuttur ve bunların bazıları çok faydalı olabilir. Bu şekilde elde edilebilecek bazı veri örnekleri şunlardır:

- Kullanıcı/geliştirici yorumları (şifreler, kimlik veya konum referanslarını bulmak son derece kolaydır ve bazen çok da aydınlatıcıdır);
- Gizli alanlar;
- Bağımsız bir delil kaynağı sağlayabilecek harici sitelere yapılan atıflar (örnek için daha sonra İçerik Ağları'na bakın).

Bu bilgilere ulaşmak için sıklıkla kullanılan bir diğer prosedür, tarayıcıda "geliştirici araçları"nı açmak ve ardından sayfayı ve temel bilgileri bir "bölünmüş" görünüm içinde sunmaktır. Bu görünümden, bir web kaynağı istendiğinde, bazıları müfettiş için çok yararlı olabilecek, internet üzerinden taşınan veri miktarına ilişkin bir takım göstergeler almaya başlarız. Geliştirici Araçları, çoğu tarayıcıda "F12" fonksiyon tuşu kullanılarak açılabilir.

Bir sitenin kaynak kodu, şüpheli İnternet Geçmişi kayıtlarını silmiş ve önbelleğini boşaltmış olsa bile, açık kaynak müfettişinin canlı soruşturma yürütmesine veya "kapalı kutu" adli bilişim uzmanının bir bilgisayarın siteye eriştiğini kanıtlamasına yardımcı olabilir.

Son olarak, web sayfasının kendisi hakkında üst düzeyde teknik bilgi sağlayabilecek "tanımlayıcı (meta) veriler" bulunmaktadır. Bazı web siteleri, belirli bir web kaynağı (web sayfası, resim, vb.) için bir Son Değişiklik tarihi tutmaktadır. Basit bir web sayfasından daha da fazla bilgiyi kolayca sağlayacak Google Chrome geliştirici uzantıları gibi araçlar mevcuttur.

Bu "gizli" bilgilerin işleyen bir örneği olarak, popüler bir web sitesi olan www.disney.com'a bakmanız yeterli olacaktır. Bu sayfa içinde sağ tıklayıp "Sayfa Kaynağını Göster" denildiğinde, sayfanın başında "gizli" bir motivasyon mesajı bulunur.

```
<!DOCTYPE html>
<!--

    "We keep moving forward, opening up new doors and
      doing new things, because we're curious ...
        and curiosity keeps leading us down new paths."

                              Walt Disney

-->
<html class="no-js" version="HTML+RDFa 1.1" lang="en-GB">
<head prefix="og: http://ogp.me/ns#" dir="ltr">
  <title>Disney UK | The Official Home For All Things Disney</title>
  <link rel="preconnect" href="//static-mh.content.disney.io">
<link rel="preconnect" href="//lumiere-a.akamaihd.net">
<link rel="preconnect" href="//kaltura.akamaized.net">
<link rel="preconnect" href="//cdnapisec.kaltura.com">
<link rel="preconnect" href="//a.dilcdn.com">
```

Söz konusu metin, öncesinde '< ! - -' ve sonunda '- - >' kullanılarak web sitesini görüntüleyenlerden gizlenmektedir.

4.3.4 Sosyal Ağ Siteleri

Sosyal ağ siteleri, sıradan web sayfaları olarak başlamış ve sahip oldukları karmaşıklık açısından muazzam bir evrim geçirmiştir. Karmaşıklık dijital müfettişler açısından iyidir çünkü sorgulanabilir satır sayısını artırması muhtemeldir. Ne yazık ki, zaman içinde bazı sosyal ağlar, gizlilik sorunları nedeniyle, müfettişler tarafından açık kaynak sorgulamalarında aranabilecek veri miktarını önemli ölçüde kısıtlamıştır. Bilgi miktarı aynı zamanda hesap sahibi tarafından kullanılan gizlilik ayarları ile de kısıtlanmaktadır. Gizli çevrimiçi teknikler kullanılarak daha fazla bilgi elde edilebilir, ancak bu, çoğu ülkede önemli izinlerin yanı sıra, elde edilen çıktının bir soruşturma kapsamında kullanılabilir olmasını sağlamak bakımından sağlam teknikler ve veri yakalamanın kaydedilmesini gerektirmektedir. Müfettişin Sosyal Ağ Sitelerinde dikkat etmesi gereken genel hususlar arasında aşağıdakiler sayılabilir:

- **Dahili kimlikler (ID'ler)**. Bu siteler, bilgileri (kullanıcılar, resimler, sohbetler, oturumlar, gruplar, beğeniler/ beğenmemeler vb.) izlemek için yoğun bir şekilde "tanımlayıcılar" (ID'ler) kullanır ve bu ID'ler çoğunlukla hizmet sağlayıcıya açık dahili ID'ler ile ilişkilidir. Facebook, yoğun bir şekilde "fbid" (Facebook ID) kullanmaktadır (örneğin www.facebook.com/photo.php?**fbid**=389359417758298). Şüpheli bir kişinin Facebook profilinin/kullanıcısının/resminin vb. anlık görüntüsünü almış olmak faydalıdır, ancak Facebook'un veritabanında bulunan dahili kimliği çok daha ilgi çekici olabilirdi.

- **Açık konu başlıkları içindeki sohbetler**. Bu siteler, kullanıcılara bilinen veya bilinmeyen diğer kullanıcılarla görüntülü, sesli veya yazılı diyaloglar kurmalarını sağlayan hizmetler sunar. Bunlar, eğer düzgün bir şekilde ve soruşturmanın yapıldığı ülkenin yasaları uyarınca toplanır ve işlenirse, yüksek kalitede bilgi sağlayabilirler. Tüm web etkileşimli öğelerde müfettiş için temel husus, sadece web tarayıcısı tarafından ekranda gösterilen verileri değil, mümkün olduğu kadar çok veri toplamaktır.

- **Resimler**. Çoğu yüksek profilli sosyal ağ sitesi, kendilerine yüklenen resimlerde kullanılmak üzere "temizleme" filtreleri sunmaktadır. Müfettiş yine de, yüklenen resimleri doğrudan yayınlayan bazı sosyal ağ sitelerine ve diğer türlerdeki web sitelerine rastlayabilir. Görüntüyü oluşturan cihazda gösterildiği gibi çekim tarihi ve saati, bu cihazın markası ve modeli, odak mesafesi, bakılan yön ve fotoğrafın çekildiği yerin enlem ve boylamını içeren (esasen EXIF[84] biçiminde kodlanmış) bu resimlere eklenmiş olan tanımlayıcı (meta) verilerden haberdar olunmalıdır. Belirli siteler içinde çok sayıda resim aramak ve indirmek ve ilgili tüm EXIF meta verileri birkaç dakika içinde çıkarmaya yönelik programlar vardır veya kolayca oluşturulabilir.

Sosyal ağlarda daha fazla soruşturma yapmak için OSINT araçlarına (bkz. Bölüm 4.3.1) daha yakından bakmak en kolay yöntem olabilir.

[84] Kaynak: http://en.wikipedia.org/wiki/Exchangeable_image_file_format

4.3.5 Blog ve Mikro Blog Siteleri

Geçmişte, birçok farklı motor (yani yazılım türleri) tarafından desteklenen birden fazla blog sitesi vardı. Bunlar kalite bakımından farklılıklar gösteriyordu. Daha popüler olan motorlardan birinde, her gönderinin (girdinin) eklendiği IP adresi etiketleniyordu. Bir müfettiş, sadece web sayfasına veya "kaynak koduna" bakarak IP adresini kolayca elde edebilirdi. O günlerin üzerinden çok zaman geçti (buna karşın müfettiş yine de hala eski bir blog çerçevesi ile karşılaşabilir). Günümüzde birkaç blog motoru mevcuttur ve neredeyse herkes blog yazarlarının gizliliğini korumak için büyük zahmetlere girmektedir. Diğer yandan, blog platformları artık blog yazarı siteye mesaj göndermeden önce genellikle daha sıkı bir kimlik doğrulama süreci gerektiriyor.

Google'ın blogger (eski adıyla Blogspot) hizmeti, kullanıcının (kendi alanını kullanıyorsa) ana sitesine aşağıdakine benzer bir şey yükleyerek kendi alan adını doğrulamasını gerektirir:

```
<meta name="verify-v1" content="h+kBXIgekCCDbSWyZ+jVGQ4LXeZbGnUZOlyZeQTQB04=" >
```

Bu HTML meta veri kodu parçası daha sonra Google tarafından bir Google e-posta hesabı ile Blogger tarafından kullanılan alan arasında bir doğrudan bağlantı kurmak için kullanılır. Kullanıcı, bağlantı yapıldıktan sonra bu meta verileri siteden kaldırabilir, fakat neredeyse hiç kimse bunu yapmaz ve bu bilgiler sonsuza kadar orada kalır. Twitter, Facebook, Google Analytics ve AdSense gibi sitelerin tümü, belirli bir blogun arkasında gerçekte kimin olduğunu belirlemek için ek sorgulama satırları sunar.

Google Web Yöneticisi Araçları için de benzer bir kullanıcı doğrulaması gereklidir:

```
<meta name="google-site-verification" content="abcdefghijklmnopqrstuvwxyz0123456789"/>
```

Google'ın Site Kimliğini sitenin URL'sinden ve bu siteyi doğrulamak için kullanılan e-postadan aldığı bilinmektedir.

Son olarak, "ciddi" blog platformları bugün oldukça güvenli olsa da, bazı platformların hala yararlı olabilecek sınırlı aktif içerik gönderme imkanı tanıması da bir o kadar önemlidir.

Yerleşik blog hizmeti sağlayıcıları kullanmanın yanı sıra, yetenekli web geliştiricisi, blog yazmak için tasarlanmış bir içerik yönetim sistemi (CMS) kullanarak kendi web alanı içinde bir blog kurabilir. Bu tür CMS sistemlerinin en ünlü örneği muhtemelen Wordpress'dir. Müfettişin özel bir web alanında barındırılan bir blog hakkında bilgi alması gerektiğinde, o web alanını barındıran sağlayıcıya, ilgili Ağ Arayüzü Kartına (NIC) başvurabilir ve ayrıca (bu bölümde gösterilen Web Yöneticisi Araçları veya Google Analytics parçacıkları gibi araçlarla) kaynak kodundan bilgi alabilir.

4.3.6 Webmail (Web Posta) Hizmetleri

Çoğu web posta platformu, gönderenin IP adresini, «genişletilmiş» bir başlık olarak, kendisi aracılığıyla gönderilen e-postalara ekler. Diğer yandan Gmail ve başka bazı hizmet sağlayıcılar, kullanıcılarının gizliliğini koruma ihtiyacını öne sürerek bu bilgileri başlıkta açıkça ortaya koymaz. Daha büyük web posta platformlarının her birini

anlatmak için birkaç bölüm harcanabilir, ancak aşırı düzeyde teknik içerikli olur ve bu Kılavuzun kapsamını aşar. Ancak, müfettiş, bir delil kaynağı olarak bu siteler ile ilgili delillerle uğraşırken başlık bilgilerinin sahip olduğu potansiyelin farkında olmalıdır.

Gerçek bir vaka[85] örneği olarak, bir şüphelinin sabit diskinde birden alakalı hale gelen aşağıdaki URL bağlantısı dosyası bulunmuştur:

https://mail.google.com/mail/h/1fghjf56gshi2/?view=att&th=35hyfdfghdfgdfgwe67ti-d=0.1&disp=attd&realattid=f_gnt1i7j37&zw

Biraz araştırma yapıldıktan sonra, söz konusu "realattid"[86] URI'sının son bölümünün "Gerçek Ek Kimliği" anlamına geldiği keşfedilmiştir. Google, aynı dosyayla ilişkili kaç farklı e-posta olursa olsun, eklerin sadece bir kopyasını sunucularında sakladığı için, bu durum, müfettişlerin ekin içeriğinin ne olduğunu belirlemesine ve şüpheliyi soruşturma altındaki olaylarla ilişkilendirmesine imkan tanımıştır.

4.3.7 URL Kısaltıcılar

Bunlar internette ve özellikle de Twitter gibi sosyal ağ sitelerinde son derece yaygın olarak kullanılmaktadır. "Kısaltıcının" amacı, URL gibi bir web bağlantısının boyutunu küçülterek Twitter gönderisi gibi boyut sınırlı bir mesaj içinde daha az yer kaplamasını sağlamaktır. Twitter bağlantıları hakkında günlükler tutulması (*delil amacıyla kullanılması açısından iyidir*) dışında, müfettiş ayrıca bazı hizmetlerin açık bağlantı izleme istatistikleri sağladığını da bilmelidir. Yani herkes belirli bir kısaltılmış URL'nin kullanımıyla ilgili istatistikleri bulabilir. Hatta bazı hizmetler, bu istatistikleri bir zaman çizelgesi üzerinde sağlamakta, oradan da kısaltılmış bağlantının ne zaman oluşturulduğu görülebilmektedir.

URL kısaltıcıların örnekleri arasında; Bitly (www.bitly.com), Short URL (www.shorturl.at), Tiny URL (www.tinyurl.com) ve Blink (www.bl.ink) sayılabilir.

Bir kısaltıcının tipik bir kullanımı, aşağıdaki URL'yi alıp;

www.coe.int/en/web/cybercrime/-/20-years-of-the-convention-on-cybercrime-join-the-celebration

internette şu şekilde görünmesini sağlamaktır:

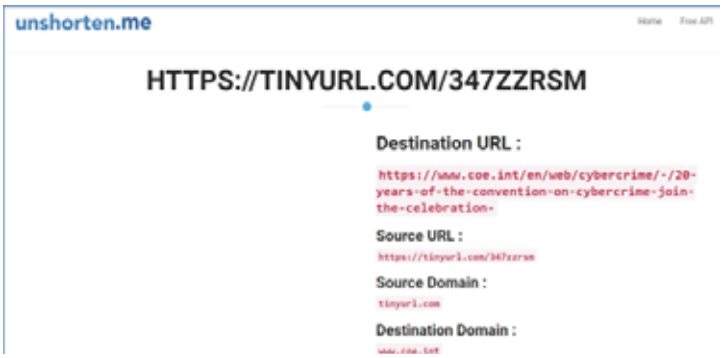
tinyurl.com/347zzrsm

Müfettiş, bir URL'nin "kısaltılmamış hale getirmek" için UnshortenMe (www.unshorten.me) veya UnshortenIt (www.unshorten.it) gibi bir takım araçlar kullanabilir. Co-E'nin kısaltılmış sitesinin çıktısının bir "kısaltılmamış hale getirici" içinden geçirilmiş çıktısının bir örneği şöyle görünecektir:

---

85 Gizlilik için ince ayar yapma ve anonimleştirme

86 Tekdüzen Kaynak Tanımlayıcı



4.3.8 Reklam Ağları

Çevrimiçi reklamlar, genellikle gözden kaçan bilgi kaynaklarından biridir. Reklamlar, şüpheli bir web sitesinde göründüklerinde, Google AdSense, AdBrite, 24/7 RealMedia, Microsoft PubCenter/adCenter vb. gibi bir reklam ağına yönlendireceklerdir. Bunlar aslında (reklam ağına bağlı olarak az çok güvenilir olan) bir kimlik sağlayabilir ve çevrimdışı bir «para izi» için ipucu verebilir.

Ek bir not olarak ve tam olarak reklamla ilgili olmasa da, Google Analytics kodları, birçok web sitesi kodu içinde gömülü olarak bulunabilir. "UA-17576257-1" gibi bir formata sahiptirler ve iş zekası (istihbaratı) ve kullanıcı tercihleri toplamak için kullanılırlar. Suçlular da bunları, her tür saldırının ve dolandırıcılığın etkinliğini izlemek için kullanır. Bir Google Analytics hesabına bağlı kimlikler, genellikle aslında bir Google hesabına bağlıdır ve bu da daha sonra bir cep telefonu numarası bulunmasına yol açabilir.

4.3.9 İçerik Depolama Ağları

İçerik depolama ağları, materyallerin çevrimiçi olarak depolanmasına ve paylaşılmasına izin veren ve Bulut Bilişim olgusunun bir parçası olan hizmetlerdir.

Müfettiş muhtemelen bu ağları geri planda çalışan ve görünmez bir teknoloji olarak değerlendirecektir. Bununla birlikte bunlar, bu teknolojiye tam anlamıyla aşina olunmadığı takdirde gözden kaçabilecek ek bilgi veya soruşturma ipuçları sağlayabileceğinden, müfettiş bunların varlığından haberdar olmalıdır. Amazon'un S3'üne karşılık, Google'ın Google Apps için ve Microsoft'un Azure için birer içerik depolama ağı vardır. Diğer birçok uygulama da aynı teknolojiyi kullanmaktadır. En iyi bilinen örneklerden biri, dahili olarak Amazon S3'e dayalı olan DropBox adlı bulut depolama ve paylaşım hizmetidir.[87]

[87] Bu hizmet sağlayıcılardan resmi olarak veri talep edebilirlerse, müfettişler başka yararlı deliller de bulabilirler. Örneğin Amazon S3, adreslenmiş nesneler, tam erişim günlükleri ve hatta dosya/nesne/parça sürümleri sağlayabilir!

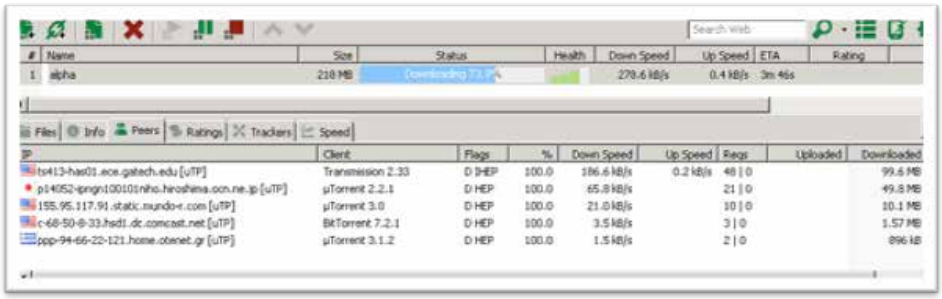
4.3.10 Dosya Paylaşımı - Eşler Arası (P2P) Ağlar

Eşler Arası (P2P) ağlarda bilgisayarlar (yani "eşler") birbirine, merkezi bir sunucu olmadan bağlanır. P2P ağları geleneksel olarak telif hakkıyla korunan müzik ve video gibi materyallerin bulunduğu bir kaynak olmuştur. Kanuni yaptırım bağlamında P2P, hızlı bir şekilde çocuk istismarı görüntüleri (Çocuk Cinsel İstismar Materyalleri – CSAM/Çocuk Cinsel Sömürü Materyalleri – CSEM) gibi yasa dışı materyalleri paylaşmaya yönelik bir yer haline gelmiştir ve birçok soruşturma artık bu ağlara odaklanmaktadır.

Napster gibi erken dönem P2P ağlarının merkezi bir yönetim noktası vardı, yani tüm trafik oradan geçtiği için müfettişler açısından bir odak noktası oluyordu. Bu merkezileşmenin suçlanacak birinin bulunmasını sağlaması nedeniyle 2001 yılında Napster'in eğlence endüstrisi tarafından kapatılmasıyla, merkezi olmayan türde P2P ağlarına bir geçiş olmuştur. Bununla birlikte, genellikle soruşturulacak değişmeyen odak noktaları olmadığından ve hedefler sürekli hareket edebildiğinden, soruşturma çok daha zor hale gelmiştir.

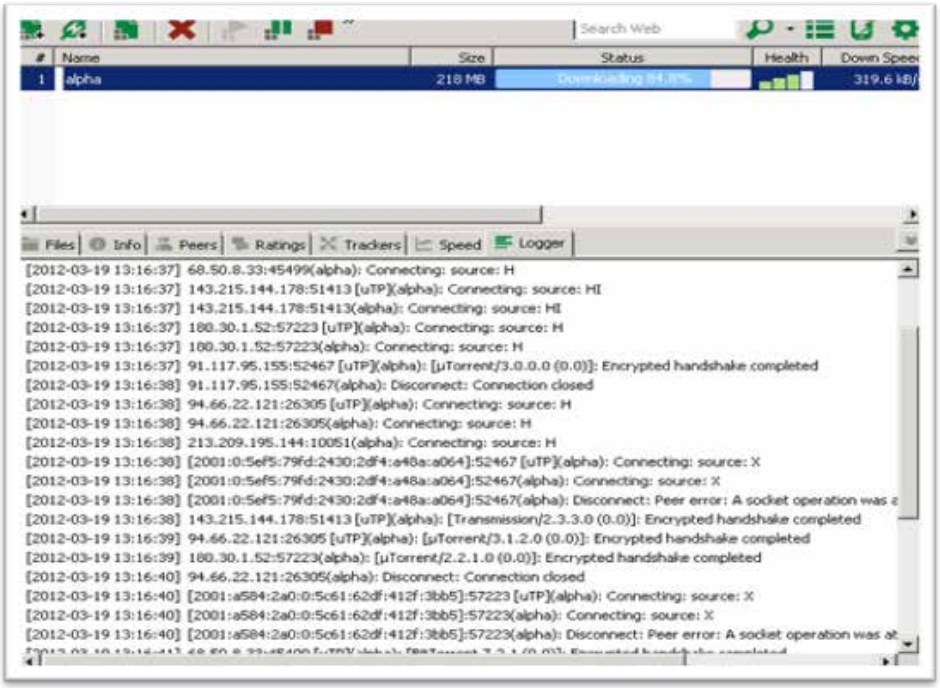
P2P ağı üzerindeki her bilgisayar bir istemcidir ancak ağ üzerinde (UltraPeer veya SuperNode olarak bilinen) bir sunucu haline de gelebilir. Aynı ağa bağlı diğer tüm bilgisayarlar (eşler) ile dosya paylaşabilirler, fakat asıl bir sunucu haline geldikleri zaman oradaki materyallerin dağıtımını kolaylaştırabilirler. Çoğu P2P ağı aracılığıyla paylaşılan veya indirilen dosyalar, yalnızca P2P ağına katılarak ve uygun P2P işlemlerini günlüğe kaydederek elde edilebilir. Bir kullanıcı, çoğu P2P istemcisini, işlemleri günlüğe ve sonuçları otomatik olarak bir dosya olarak kaydedecek şekilde yapılandırabilir. Ulusal mevzuata bağlı olarak, bu dosya delil olarak kullanılabilir.

Çalışır haldeki bir uTorrent istemcisinin anlık görüntüsü aşağıdadır. Eşler, aynı torrenti (dosyayı) aynı anda indirirken gösterilmektedir.



Bu istemci için günlük kaydı açıksa, gerekli tüm ayrıntılar (IP, bağlantı noktaları, zaman damgaları, işlemler) doğrudan bir dosyaya kaydedilecektir. Bu örnekte işlem, alfanümerik parolalar için shmoo.com gökkuşağı parola kırma dosyalarını[88] aktif olarak kimin indirdiğini gösteren bir dosyayla sonuçlanmıştır.

[88] Bunlar aslında daha sonra bir hedef sistemin şifre kutusuna otomatik olarak girilen potansiyel şifrelerden oluşan uzun harmanlanmış listelerdir.



Bu basit yaklaşım, kurcalamaya karşı korumalı günlük kullanımına imkan tanıyan, gerçek dosya dağıtım sürecinde işbirliği yapmadan (yani diğer eşlerden dosyaları alıp dağıtmadan) torrent RSS[89] beslemelerinden kendilerini otomatik olarak besleyen özel olarak değiştirilmiş P2P istemcileri oluşturularak (veya satın alınarak) daha da geliştirilebilir. Bir P2P ağına katılmak, yargı bölgesine bağlı olarak bir soruşturma bakımından yasal sorunlara neden olabilir. Daha gerçek zamanlı soruşturma, verileri bir veritabanı içinde sıralamayı veya daha fazla veri toplamak için sorgulamaya dahil edilen IP adreslerinde gerçek zamanlı ek sorgulamayı içerebilir. P2P ağları çoğunlukla yasa dışı içerik dağıtımı için kullanılmakta olup, kolluk kuvvetleri tarafından da dünya çapında proaktif çocuk istismarı soruşturmaları için yoğun bir şekilde kullanılmaktadır.

Çocuk Kurtarma Koalisyonu›nun Çocuk Koruma Sistemi (CPS) buna bir örnektir; bu, çocukları tespit ederek korumaya çalışan ve belirli P2P ağları üzerinden bir kullanıcıyla paylaşıldığı bilinen yasa dışı çocuk istismarı görüntülerinin, aktif olarak bunları dağıtmakla uğraşan insanları bulmak için hedefli olarak soruşturulmasına imkan tanıyan, sadece kolluk kuvvetleri tarafından kullanılan bir uygulamadır.

4.3.11 "Derin Web" ve "Karanlık Web"

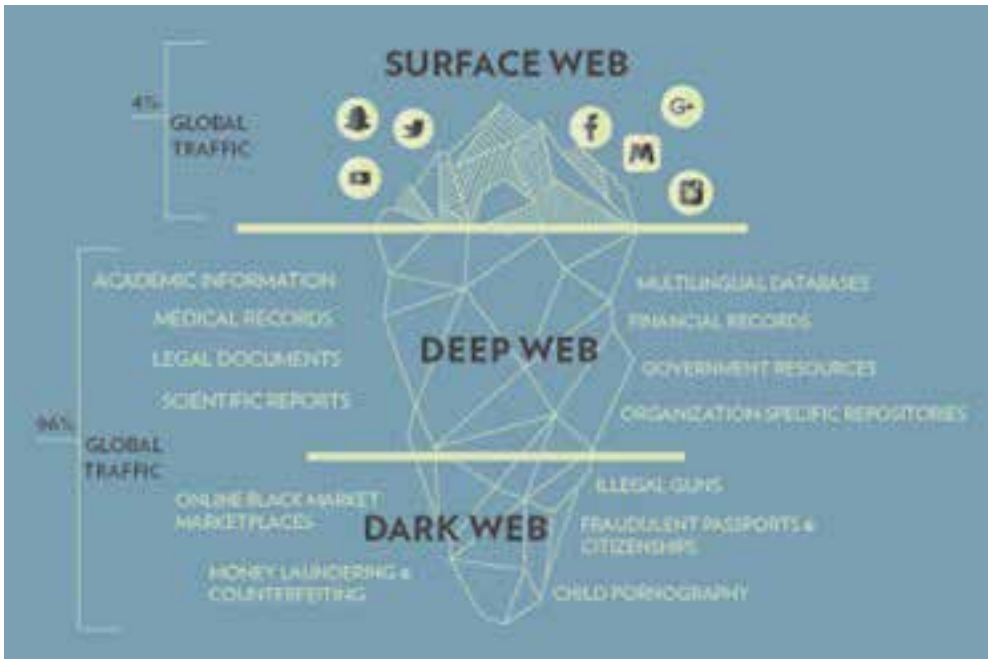
Her ne kadar internet, hizmet ve bilgi sağlayıcıların tipik olarak veri yayınlamak ve bunları genel halkla paylaşmak istediği bir yer olsa da, sınırlı bir grup insanın özel amaçlarla erişebileceği daha özel alanlara ilişkin bir talep de vardır. Bu alanlardan bazıları, sadece doğru adrese sahip kişiler tarafından bulunabilecek halka açık yerlerdir. Örneğin, düğünlerinin fotoğraflarını aileleri ve arkadaşları ile paylaşmak isteyen bir çifti ele alalım. Her internet kullanıcısının bu fotoğrafları görmesini istemezler. Bu

[89] RSS, Gerçekten Basit Dağıtım ifadesinin kısaltmasıdır. Ağdan, bir içeriği yüklendiği sırada sunmak için kullanılan bir sistemdir. Çoğunlukla bir haber veya medya hizmeti ile ilgili olacaktır.

durumda resimleri bir bulut hizmetine yükleyebilir ve galerinin bağlantısını sadece kişisel arkadaşlar ve aile ile paylaşabilirler. Tabii bu yöntem özel verileri paylaşmak için çok güvenli bir yol değildir ama kolaydır ve fotoğraflar çok gizli kabul edilmeyeceğinden bu çözüm çoğu insan için yeterli olabilir.

İnternette ayrıca, oturum açma bilgilerinin gerekli olduğu başka gizli alanlar da vardır. Tipik bir ilan panosu ve normal bir web posta hesabı, bir arama motoru tarafından bulunamayan veya oturum açma gereksinimleri nedeniyle erişilemeyen özel alanlara sadece iki örnektir. Genel arama motorlarından kasıtlı olarak gizlenen sitelerin yanı sıra, içeriği ulaşılamaz, anlaşılamaz veya analiz edilemez olduğu için arama motorları tarafından indekslenmesi mümkün olmayan web siteleri ve veritabanları da bulunmaktadır. Google veya diğer arama motorları, sadece yüzey web (açık veya net web olarak da bilinir) içindekileri bulabilir ve buradaki bağlantıları izleyerek bulabildiklerini «kazıyabilir».

İnternetin arama motorlarından gizlenen tüm alanlarının toplu adı «**Derin Web**" olarak adlandırılır (diğer adları "Gizli Web", "Görünmez Web" ve "Deepnet"tir).



Yaygın olarak bilinen bir internet gösteriminde, yukarıda görüldüğü gibi, aslında içeriğinin çoğu su hattının altında olan bir buz dağı model olarak kullanılmıştır. Bu örnek, www.medium.com'dan alıntıdır. Bunun sayısız başka örneği vardır ve her birinin, o çizginin üzerinde olduğu için kolayca bulunabilenler ile altında kalan bulunamayanlar arasında bir bütün olarak internetin nasıl bölündüğüne dair kendi tahminleri vardır. Teknoloji geliştikçe ve veri depolama alanları eklendikçe sürekli olarak büyüdüğü için tüm boyutunu ölçmek neredeyse imkansızdır.

Derin Web'in tüm internetin %85 ila 96'sı arasında bir alan kapladığına dair tahminler olsa da kimse İnternet'in tam boyutunu bilmediğinden, bunların hepsi varsayımdır. Derin Web'in depolama alanı bakımından Yüzey Web'de kullanılan alanı önemli ölçüde aştığı belirtilmelidir.

Yukarıdaki örneklerde gösterildiği gibi, Derin Web olağandışı veya yasa dışı değildir ve illa suç ile bağlantılı olmak zorunda da değildir. İnternetin ilk günlerinden beri var olagelmiştir. Aslında, internet üzerindeki ilk sunucular ve Dünya Çapında Ağ üzerinde bulunan ilk web siteleri, pekala Derin Web'in bir parçası olarak düşünülebilir. Arama motorlarının ve genel dizinlerin bu kadar karmaşık hale gelmesinden önceki günlerde, insanlar sayfaları ancak tam adresini bilmeleri durumunda ziyaret edebilirlerdi - diğer herkes için sunucu veya web sitesi görünmezdi.

Derin Web konusundan ayrılmadan önce, kılavuzun bu noktasında durmak ve önemli bir soruşturma hususunun kullanıcılar tarafından anlaşılmasını sağlamak yerinde olacaktır. Bu kılavuzun kullanılacağı yargı bölgeleri arasında, internetten bilgi, istihbarat ve delil toplamanın tamamen Yüzey Web'deki halka açık bilgilerle sınırlı olduğu bazı yargı bölgeleri olabileceği gibi, Derin Web'in çeşitli bölümlerine meşru ve yasal olarak girilebilen bazı yargı bölgeleri de olabilir.

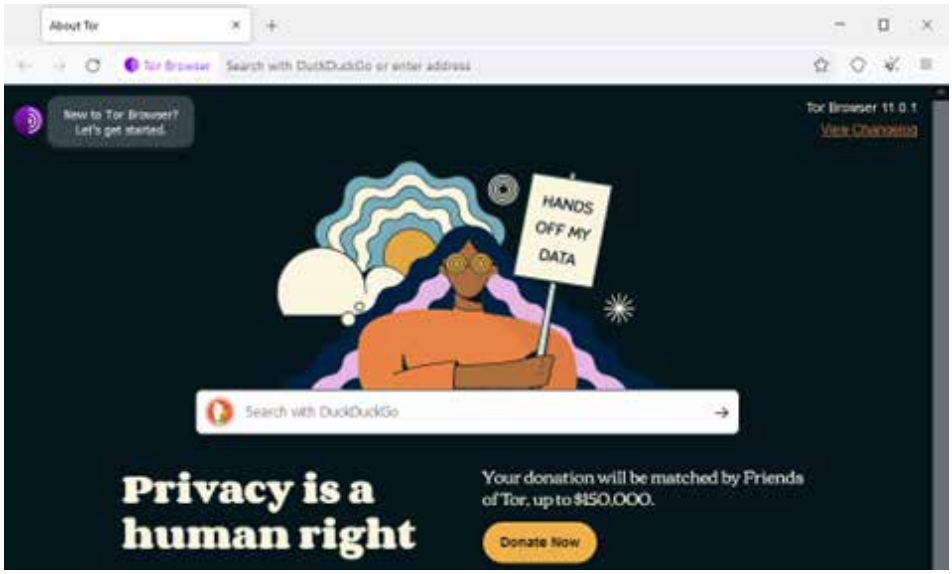
Materyal Derin Web'de olduğunda ve erişmek için bazı oturum açma bilgileri gerektiğinde veya açık erişimi durdurmak için koruma uygulanan hallerde, her yargı merciinin verilere erişmeden ve toplamadan önce kendi yasal konumundan ve verileri toplama amacına ve kanuna uygun olarak kullanabileceğinden emin olması gerektiği vurgulanmalıdır.

Arama motorları tarafından indekslenmeyen web siteleri, veritabanları ve belgelerin yanı sıra, Derin Web'in "**Karanlık Web**" (Dark Net olarak da bilinir) adı verilen başka bir katmanı da vardır. Tıpkı Derin Web gibi Karanlık Web içinde de standart arama motorları ile arama yapılamaz. Ancak, ziyaretçi adresi veya oturum açma bilgileri biliniyorsa normal bir web tarayıcısı ile Derin Web sitelerine erişilebilirken, Karanlık Web siteleri ve hizmetleri için bu durum geçerli değildir.

Karanlık Web, Derin Web ve Yüzey Web ile aynı fiziksel internet ağını kullanmasına rağmen, farklı bir dahili ağ ve adres alanı kullanmaktadır. Bir müfettişin, Karanlık Web adresini bilmenin yanı sıra, içeriği görmek için aynı zamanda Karanlık Web'in dahili ağı üzerinden bağlanması da gerekecektir.

Karanlık Web ağları, eşler arası ağlardır, yani her kullanıcı doğrudan başka bir kullanıcıya bağlanmaktadır. Gerekli becerilere sahip herkes bir Karanlık Web oluşturabilir ve bir grup güvenilir insanı bu küçük ağa katılmaya davet edebilir. Fakat binlerce kullanıcısı olan bazı Karanlık Web'ler de vardır. Bunlardan en öne çıkanı bir zamanlar Freenet idi ve şimdi de The Onion Routing (Tor) 'Soğan Hizmetleri'dir (Onion Services) (eski adıyla Hidden Services).

Onion Yönlendirici, ilk olarak 2002 yılında Amerika Birleşik Devletleri Savunma Bakanlığı tarafından anonim bir iletişim platformu olarak sipariş edilmiş ve yayınlanmıştır. Karanlık Web'e erişim imkanı tanıyan özel bir tarayıcı olan ilk Tor Tarayıcı 2008 yılında ortaya çıkmıştır. Bu tarayıcının amacı, tüm bilgisayar kullanıcılarına sunduğu anonimlik temasını sürdürmekti.

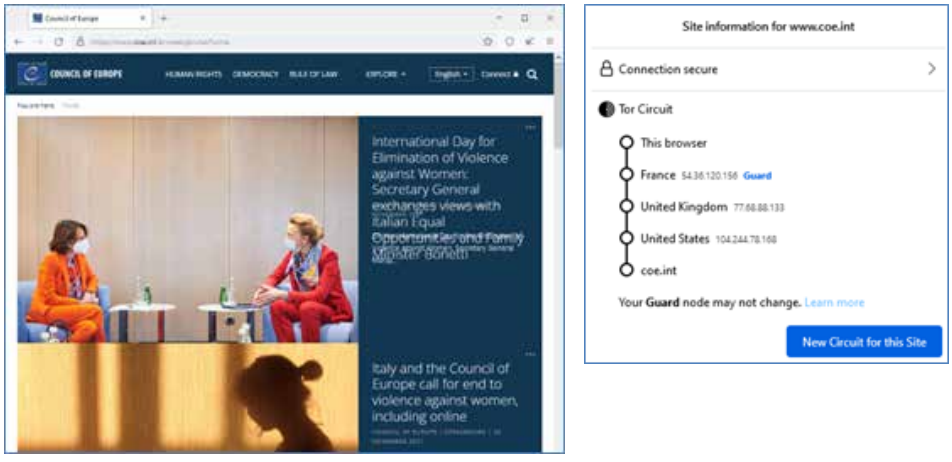


Tor ağına erişim genellikle yukarıda görülen Tor Tarayıcı ile sağlanmaktadır.

Tor ağı, trafiği birkaç düğüm noktası üzerinden yönlendiren anonimleştirici bir kanaldır. Her düğüm yalnızca doğrudan komşusunu bilir, bu nedenle zincirdeki herhangi bir düğümün (veya kullanıcının) tam olarak kimin hangi isteği gönderdiğini veya aldığını söylemesi mümkün değildir.

Aşağıdaki resim (solda), Tor Tarayıcı aracılığıyla erişilmiş Avrupa Konseyi web sitesini göstermektedir. Bu tarayıcıyı kullanarak "normal" web sitelerine erişmek de gayet mümkündür. Ancak Tor Tarayıcının amacı, kullanıcıya söz konusu düzeyde bir anonimlik sunmaktır.

Aşağıdaki resim (sağda), tarayıcının web sitesi ile bağlantı kurarken kurduğu "Tor Devresi"ni göstermektedir. Bu örnek, ağın, site talebini önce Fransa'daki bir "koruyucu" (giriş) düğümü aracılığıyla yönlendirdiğini, sonra Birleşik Krallık'a ve Konsey sitesine bağlanmadan önce son olarak Amerika Birleşik Devletleri'ne sıçradığını göstermektedir. İlk talep aslında İspanya'dan yapılmıştı. Tor Ağı içindeki tüm bağlantı, uçtan uca veya en azından son Tor düğümünden ayrılıp gereken web sunucusuna gidene kadar şifrelenmektedir.



Daha önce de belirtildiği gibi bu, Karanlık Web ağı üzerindeki iletişimin soruşturulmasının zor olduğu anlamına gelmektedir. Bu durum, Tor Tarayıcının arka planda yaklaşık 10 dakika sonra Tor Devresini otomatik olarak değiştirmesi veya kullanıcının sağdaki resimde sağlanan düğmeyle de elle değiştirebilmesi nedeniyle daha da karmaşık hale gelmektedir. Tor Tarayıcıdaki iki ayrı sekme aynı koruyucu düğümüne sahip olacak, fakat daha sonra hedeflerine farklı yolları kullanarak gidecektir.

Bir müfettiş, Tor ağına, Tor tarayıcısını[90] indirerek erişebilir. Ağa bağlandıktan sonra, müfettiş orada bulunan onion hizmetlerine erişebilir ve bunları yapılandırabilir. Onion hizmetlerine FQDN'ler yerine ".onion" adresleri aracılığıyla erişilebilir (bkz. bölüm 4.2.4). Böyle bir ".onion" adresinin bir örneği şöyledir:

https://duckduckgogg42xjoc72x3sjasowoarfbgcmvfimaftt6twagswzczad.onion/

Bu, anonim arama hizmetleri sunan meşru arama motoru DuckDuckGo'nun Karanlık Web hizmetidir. Elektronik Delil Kılavuzunun bu güncellenmesi sırasında bu adres hala geçerli idi. Tor Ağının yapısı ve sunmaya çalıştığı güvenlik ve anonimlik hususları nedeniyle, konum değiştikçe ve bağlantı güncellendikçe bu URL'nin kısa bir süre içinde yanlış hale gelme olasılığı yüksektir.

Gizli Tor Hizmetleri, aşağıdakilere ilişkin portallar içermektedir:

- Dizinler, portallar ve bilgiler;
- Arama motorları;
- Dosya depolama;
- Eşler arası dosya paylaşımı;
- Sosyal medya;
- E-posta;
- Anlık mesaj uygulaması;
- Pazar yerleri (özellikle de yasa dışı materyallere ve hizmetlere yönelik);
- Haberler, muhbirlik ve belge arşivlerine ait arşivler;
- Pornografi.

Derin Web ve özellikle de Karanlık Web, kolluk kuvvetleri soruşturmaları açısından önemlidir, çünkü Karanlık Web'in anonimliği; silah, uyuşturucu, sahte para, sahte kimlik kartları, çalıntı kimlikler, botnet'ler, bilgisayar korsanlığı hizmetleri, çocuk istismarı materyalleri ve hizmetleri ve kiralık katiller gibi yasa dışı materyal ve hizmet ticareti yapan tüccarları ve müşterileri cezbetmektedir. Bu tür pazar yerlerinin en belirgin örneği "İpek Yolu" idi.

Derin Web ve Karanlık Web'de soruşturma, bu temel kılavuzun kapsamını aşan düzeyde uzmanlık gerektiren bir görevdir. Ancak, aşağıdaki okuma listesi okuyucuları doğru yöne yönlendirebilir:

- Karanlık Ağı keşfetmeye yeni başlayanlar için kılavuz: https://turbofuture.com/internet/A-Beginners-Guide-to-Exploring-the-Darknet

[90] https://www.torproject.org/projects/torbrowser.html.en

- Derin Web Bağlantıları:

  deepweblinks.org

- Derin Web Dizinleri ve arama motorları:

  www.thehiddenwiki.net/deep-web-directories-search-engines/

- TOR Onion hizmetleri ve TOR ağının öğelerine ilişkin kılavuz:

  en.wikibooks.org/wiki/Guide_to_Tor_hidden_services_and_elements_of_the_Tor_network

- Karanlık Web'de Soruşturma – Adli Bilişim İnceleme Uzmanları için Çevrimiçi Anonimliğin Zorlukları,

  articles.forensicfocus.com/2014/07/28/investigating-the-dark-web-the-challenges-of-online-anonymity-for-digital-forensics-examiners/

- Gizli Web'i Kazımak, Raghavan vd., Çok Büyük Veritabanları konusunda 27. Uluslararası Konferans (VLDB 2001), 11-14 Eylül 2001, Roma, İtalya

  ilpubs.stanford.edu:8090/725/

- Gizli Web İçeriğinin İndirilmesi, Alexandros Ntoulas vd., UCLA Bilgisayar Bilimleri

  oak.cs.ucla.edu/~cho/papers/ntoulas-hidden.pdf

- Karanlık Web'de Deliller ile İlgili Cezai Soruşturmaların Yürütülmesine Yönelik Kolluk İhtiyaçlarının Belirlenmesi -

  www.rand.org/pubs/research_reports/RR2704.html

4.4 Veri ile Delil Karşılaştırması

Çevrimiçi soruşturma için öne çıkan delil kaynaklarından bazıları gözden geçirildikten sonra, sistematik bir yaklaşım bunun mahkemede kullanılabilir olmasını sağlayacaktır. Ceza davalarında çevrimiçi proaktif araştırma çalışmaları üç nedenden dolayı gerçekleştirilir:

- Yardımcı olabilecek **bilgiler**
- Geliştirilebilecek **istihbarat**
- Sunulabilecek **delil**

Açık kaynak soruşturma içindeki çevrimiçi çalışmada, materyalleri ispata yönelik bir standart ile toplamanın diğer iki neden için kullanılmalarına imkan tanıyacağı, fakat bu standarda uygun çalışmamanın onları delil olarak kullanılamaz hale getirebileceği daima göz önünde bulundurulmalıdır. Dolayısıyla, mümkün olduğu ölçüde daima en yüksek standarda uygun çalışmak mantıklı olacaktır.

O zaman müfettiş ayrıca çevrimiçi araştırmaya başlarken kendi kendine sorular sormayı da düşünmelidir.

- Ne biliyorum? Ve bildiğim, ne anlama geliyor?
- Neyi bilmem gerekiyor ve benden neyi bulmam isteniyor?

- Onu nasıl bulacağım?

Buna genellikle Boşluk Analizi denir - nerede olduğumuz ile nerede olmak istediğimiz arasındaki fark - ve ardından tanımladığımız "boşluğu" nasıl kapatacağımızı belirlememiz gerekecektir. Aynı zamanda, bulmak istediğimiz şeye odaklandığımız anlamına da gelir. Çevrimiçi araştırma, çok büyük miktarda bilgiye bakmak anlamına gelir ve çoğu zaman bulunan verilerin çokluğu nedeniyle araştırmanın nihai amacının kaybedilmesine sebep olur. Net bir hedefe sahip olmak, değerli soruşturma zamanını boşa harcamamanın anahtarıdır.

4.4.1 Söz Konusu Verileri Ne Sebeple İstiyorsunuz?

Bir müfettiş, aşağıdaki soruların bazılarını veya tümünü yanıtlamaya hazır olmalıdır:

- Veriler nereden geliyor?
- Bu verilerin geçerliliğinden emin misiniz?
- Bu verilerin tam olduğundan emin misiniz?
- Vardığınız sonuçları geçersiz kılabilecek, farkında olmadığınız herhangi bir şey olmadığından emin misiniz?

Ya da sadece:

- Delilinizin bütünlüğünü garanti edebilir misiniz?

Kapalı kutu soruşturmalarda bu soruların çoğu zorluk çıkarmaz. Sadece bu amaç için tasarlanmış, önceden oluşturulmuş bir metodoloji ve araç seti vardır. Ancak, belirli bir siteyi ziyaret ederken bir tarayıcı kullandığınız zaman, size sunulan bilgilere ait bir ekran görüntüsü sunuyorsanız, bu sorular gerçekten zorlayıcı olabilir.

Aşağıda "Galaktik Konsey resmi web sitesi"nin bir anlık görüntüsü verilmiştir:

Yasal Uyarı: Bu sahte bir web sitesidir!

Elbette, bir Galaktik Konsey web sitesi yoktur. Bu, okuyucuya ilk elden sahte delil sağlamak için değiştirilmiş başka bir web sitesidir.

Söz konusu anlık görüntünün sahtesinin yapılması yaklaşık 60 saniye sürmüştür (bunun 40 saniyesi de içine ne yazılacağı düşünülerek harcanmıştır). Bu görüntünün sahtesini yapmanın kolaylığı göz önüne alındığında, çevrimiçi içeriğin basit bir anlık görüntüsü, bir mahkeme için görüntünün içeriğini kanıtlamak açısından asla yeterince iyi olmayacaktır. Fakat bir web sayfasının kaynak kodu, bu bölümde daha sonra bahsedilecek olan içerik doğrulamaya yardımcı olabilir.

4.4.2 Çevrimiçi Etkinlik Kayıtları

Daha sonra bir kolluk kuvvetleri operasyonu veya kovuşturması kapsamında kullanılmaya devam edebilecek bir çevrimiçi veri toplama uygulaması gerçekleştirilirken, çalışmanın başında bir İnternet Etkinliği Kaydı (IAR) başlatılmalı ve o çevrimiçi materyali aramak için internette ziyaret edilen yerlere ve içeriğe, ziyaret zamanlarına dair bir kayıt olmalıdır. Bu, ekran görüntüleri için de referans sağlar. Bulduğumuz bir şeyin nasıl elimize geçtiğini ve onu nereden aldığımızı söyleyebilmemiz gerekir. Bilgi, istihbarat ve delillerin çevrimdışı dünyadaki toplanma ve sunulma biçimi de bundan farklı değildir.

IAR; bir şeyin yapıldığı saat ve tarihten, internet üzerinde bulunduğu yerden, müfettişin bilgisayarına almak için ona ne yapıldığından başka hiçbir şey içermeyen ve tanımlanabilmesini sağlamak için benzersiz bir referans sağlayan basit bir belgedir. Bir soruşturma başladığı sırada bir örneği şöyle görünebilir:

RESTRICTED WHEN COMPLETE

INTERNET ACTIVITY RECORD

Case Reference	245/2021 – Op Council
Open Source Analyst	Investigator ABC
Start Date	28 November 2021
Start Time	13:56

Date	Time	Activity/Resource/Location	Action Needed	Ref
28/11	13:57	Time check – time.is 	None	N/A
28/11	13:58	System configuration 	None	N/A
28/11	13:59	IP Address info 	None	N/A

Söz konusu belgenin, biçimlendirilmiş bir Word belgesinden başka bir şey olmaması gerekir ve yukarıdaki örnek, bir müfettişin her kayıt alma oturumunun başında belirli bir dava için nasıl zemin hazırlayacağını göstermektedir. En üstte dava ile ilgili bazı arka plan bilgileri, sonrasında güvenilir bir kaynak kullanılarak yapılan zaman doğrulaması bulunmaktadır. Bunun için, AtomTimePro[91] veya NetTime[92] gibi küçük bir program kullanılabilir. Örnek IAR içindeki zaman kaydı, dünya genelinde zaman senkronizasyonu sağlayan bir web sitesi olan Time.is[93] üzerinden alınmıştır.

Bu uygulamanın amacı, kullanılan cihazın saat ayarının tam doğru olmayabileceği kayıtlar için bir dayanak sağlamaktır. Çevrimiçi verilerin kaydedilmesi sırasında kesin zamanlama kritik öneme sahip olacaktır.

İkinci kayıt, kullanılan cihazın gerçekte ne olduğunu ve neye benzediğini göstermektir. Bu bilgilerin bazı parçaları, çevrimiçi kayıt alma sırasında internet üzerinden iletilebilir ve bu nedenle, kayıt işleminin başında, soruşturma ilerledikçe başka yerlerde nelerin ortaya çıkabileceğini göstermek yardımcı olur. Örneğin, bir web sunucusunda barındırılan bir web sayfasında bir kayıt almak için yapılan basit ziyaret, o ziyarete ait bir ayak izi bırakacaktır ve alınan kayda daha sonra itiraz edilirse, bu kayıt içindeki makine bilgileri doğrulama için kullanılabilir.

Bu bilgi, Windows tuşuna basılarak ve ardından uygun yanıtları gösterecek olan "sistem bilgisi (system information)" yazılarak kolayca elde edilebilir. Bu işlem, diğer işletim sistemleri kullanıldığında da benzer bir şekilde yapılabilir.

Bu ilk aşamadaki son kayıt, çevrimiçi kayıt işlemi gerçekleştirilirken cihazın kullandığı IP adresinin girilmesidir. Bu işlem de, bir tarayıcı açıp "whatsmyip" gibi bir arama terimi yazılarak yapılabilir. Makinenin o sıradaki harici IP adresini birden fazla kaynak döndürecektir ve müfettişin ziyaret etmekte olduğu kaynaklara ve konumlara hangi IP adresinin gösterileceğini, kayıt içerisinde basit bir ekran görüntüsü gösterecektir. Bu da yine müfettişin işlem ve faaliyetlerindeki şeffaflığın gösterilmesine yardımcı olur.

IAR içinde az önce yaptığımız şeyi, bir kolluk görevlisinin mahkemeye sunmak amacıyla yazdığı ve "28 Kasım 2021 Pazar günü saat 13:57'de, tam üniformalı olarak görevdeydim ve Herhangibirşehir'in Ana Caddesi'nde yürürken gördüm ki ……" diye başlayan ifadesine benzetebiliriz.

Zemin hazırlandıktan sonra, materyalleri fiilen toplamak için yapılan işlemin bir kaydının alınması gerekir.

Bu, yukarıda gösterilen belgenin bir devamı olup, her kayıt işlemi için benzersiz bir referans ile birlikte saat, tarih ve yer kaydedilmektedir. Ayrıca, ne yapıldığına dair kısa bir açıklama sağlanmakta ve bunun sonucunda yapılması gereken bir ilave istem veya işlem olması durumunda, müfettişin kendisine bir hatırlatma notu yazabileceği bir sütun bulunmaktadır. Bunun her kayıt işlemi için yapılması zahmetli görünür - ancak soruşturma amaçlı çevrimiçi kayıtta aradığımız şeffaflığı sağlamak gerekir.

---

91 https://atomtime-pro.soft32.com/

92 https://www.timesynctool.com/

93 https://time.is/

28/11	14:35	https://www.coe.int/en/web/portal/home - Selective area capture	None	ABC1
	14:40	https://www.coe.int/en/web/portal/home - Scrolling page capture	None	ABC2
	14:42	https://www.coe.int/en/web/cybercrime/the-budapest-convention - Right click Save as capture	None	ABC3
	14:44	https://www.coe.int/en/web/cybercrime/home - Right click Save as capture	None	ABC4
	14:46	https://www.coe.int/en/web/cybercrime/octopus-interface-2021 - Right click Save as capture	None	ABC5
	15:05	https://www.coe.int/en/web/portal/home - Page captures by video regording	None	ABC6

Bu ayrıca, soruşturma içindeki her işlemi ve o işlemin sonucunu açıkça tanımlamaktadır.

Sağ sütunda bir kayıt varsa ve verilerin kaydedilmesi durumunda, kayıt klasöründe buna karşılık gelen bir dosya (veya bir dizi dosya) olmalıdır. Aşağıdaki örnekte, dosyalara saat ve tarih referansı sağlayabilecek bazı ekran görüntüleri için Snagit programı kullanılmıştır.

Bu sayede, IAR içindeki kayıtları Kayıt klasöründeki kayıtlarla eşleştirmek kolaydır ve örneğin ABC5'i bir soruşturmada kullanmak isteyen herkes, 'https://www.coe.int/en/web/cybercrime/octopus-interface-2021' konumunda "Sağ tıklama - Farklı Kaydet" ile kayıt alınarak, 28 Kasım 2021 tarihinde (yerel saatle) saat 14:46'da kaydedildiğini tespit edebilir. Söz konusu veriler hala aynı yerdeyse, bunun tekrar edilmesi de mümkün olacaktır. Artık orada değilse, işlem tekrar edilemediği için nereden gelmiş olduğunu kanıtlar.

Okuyucu muhtemelen gidip küçük bir bilgi parçası toplamak için neden bu zahmete katlanmak zorunda olduğunu veya alternatif olarak, kayıt işlemi çok büyük olduğunda bunun epey bir iş olduğunu düşünecektir. Müfettiş için sorun, çevrimiçi çalışmaları sırasında ele geçirdiklerinin soruşturma boyunca inanılabilir ve güvenilebilir olmasını sağlamaktır. Ayrıca denetimden de geçebilmelidir.

Buna ek olarak, bugünlerde birçok soruşturmanın sadece yerel değil, sınır ötesi ve yargı bölgesi ötesi olduğu ve ihtiyaç duyabilecek tüm tarafların ihtiyaçlarını karşılayan, çevrimiçi veri toplamaya yönelik kapsamlı ve standart bir yaklaşıma sahip ol-

manın önemi açıkça ortaya çıkmaktadır. Bu, aynı zamanda bir başkasının sizin kayıtlarınızı alabileceği, topladığınız veriler ile birlikte okuyabileceği ve onları toplamak için tam olarak ne yapıldığını - ne zaman, nereden ve nasıl - anlayabileceği anlamına da gelir!

Çevrimiçi soruşturma geliştikçe, içerik elde etmek için kullanılan teknoloji de gelişmiştir. Geçmişte ekranın veya içeriğinin harici bir fotoğraf veya video kaydı yapılabilirken, müfettişin artık çevrimiçi verileri elde etmeye yönelik daha teknik bir yaklaşım benimsemesi gerekmektedir. Uygun bilgisayar ekipmanı ve ekran görüntüsü kaydetme yazılımlarının kullanımı artık yaygın uygulamadır.

4.4.3 Uygun Bilgisayar Ekipmanı

Kolluk kuvvetleri, çevrimiçi soruşturmaları yürütmek için hangi ekipmanın kullanılması gerektiğini düşünmelidir. İnternete bağlı olup, aynı zamanda diğer gizli işler için de kullanılan ofis bilgisayarının ve doğrudan teşkilata bağlı bir IP adresinin kullanıldığı günler artık geçmişte kalmalıdır. Aynı şekilde müfettişin kişisel ekipmanının kullanılması da bir seçenek olmamalıdır. Çevrimiçi verilerin toplanması için, bir soruşturmanın bütünlüğünü sağlayan ve çevrimiçi delilin uygun ve profesyonel bir şekilde toplanmasına, saklanmasına ve sunulmasına olanak tanıyan özel ekipmanlar sağlanmalı ve kullanılmalıdır. Geleneksel olarak bu ya bir masaüstü bilgisayar ya da bir dizüstü bilgisayar olacaktır. Fakat, internet erişimli cihazlarda çok fazla "Uygulama" tabanlı verinin geliştirilmesiyle, tablet cihazlar veya cep telefonları gibi daha yeni teknolojiye sahip ekipmanlar kullanmak zorunda kalma olasılığı da vardır.

Bu bölüm, en basit çevrimiçi sorgulama için bile uygulanması gereken dijital hijyene dair ancak üst düzey bir genel bakış sağlayabilir. Dijital hijyen derken, internet ve web tabanlı kaynakları arayan, ele geçiren ve kaydeden bir cihaz veya kişiler tarafından bırakılan izleri kastediyoruz. Bir müfettiş tarafından "dijital ayak izi" bırakılabilecek alanlar arasında basit web tarama, e-posta iletişimi ve sosyal medya etkileşimi sayılabilir.

Kullanılan bilgisayar veya cihazın, teşkilata dönük geri izlenebilirliği olmaması gerekir. Bu nedenle, satın alması teşkilatın bilişim departmanı tarafından yapılmamış, ayrı ve anonim olarak temin edilmiş ve bir çevrimiçi istihbarat ve delil toplama cihazı olarak kullanıma tahsis edilmiş olmalıdır. İnternetin bağlanma şekli ve dünya çapındaki ağın, varlıkları (ve özellikle de sosyal medyayı) birbirine bağlama şekli, cihazın başka amaçla kullanılmaması gerektiği anlamına gelir. Teknik becerisi yüksek bir şüpheli tarafından teşkilata kadar bir miktar geri izleme olasılığı olduğu daima göz önünde bulundurulmalıdır.

Ekipman, internet üzerinden arama yapıldığında teşkilatı tanımlamayan bir IP adresine sahip olmalıdır. Sağlanan tahsisli ekipmanın yanlış kullanımıyla soruşturmaların ve operasyonların tehlikeye düştüğü birçok örnek vardır. Bu bölümün baş kısmında, bir IP adresini araştırmanın ne kadar kolay olduğunu görmüştük; ve bir kolluk kuvveti teşkilatına çıkan bir IP çözümlemesi, potansiyel bir şüpheliye kendisi ile ilgilenildiğini gösterecektir.

Ekipmanı kimin kullandığı konusunda kısıtlamalar olmalı ve nasıl ve ne zaman kullanıldığına dair kayıtlar tutulmalıdır. Ayrıca yetkili kullanıcılar için ayrı oturum açma

bilgilerine ilişkin bir politikanın yanı sıra veri toplamaya yönelik de bir yapı olmalıdır. Her kişinin ve her sorgunun belirli bir depolama alanı olmalı, böylece verilerin çapraz bulaşma riski önlenebilmeli ve bütünlüğü korunmalıdır. Ayrıca, ekipmanın arızalanması durumunda iş sürekliliğini sağlamak için cihazdan uzakta (sabit disk, sunucu veya hatta bulut tabanlı) güvenli bir depoya yedekleme düzeninin olması gerekir.

Benzer şekilde Çocuk Cinsel İstismar Materyali (CSAM) gibi yasa dışı materyaller içerebilecek web sitelerine veya internet alanlarına yapılan ziyaretleri içeren veriler toplanırken, bu verilerin uygun şekilde toplanmasını, düzgün ve güvenli bir şekilde tutulmasını ve bu materyallere erişimin uygun şekilde kısıtlanmasını sağlamaya yönelik yerleşik süreçler olmalıdır.

Son olarak, işletim sisteminin tamamen güvenli ve korumalı olduğundan emin olmak için ekipmanın düzenli olarak güncellenmesi ve kullanılan tüm yazılımların da güncellenmiş ve lisanslı olması gerekir. Lisanssız yazılım veya kayıtsız bir işletim sistemi kullanmak, verinin bir kovuşturmada veya mesleki durumda kullanıldığı zaman test edilmesi veya sorgulanması durumunda, iyi araştırılmış ve uygun şekilde toplanmış bir materyalin güvenilirliğini azaltır.

Teşkilatlar, vekil sunucular (proxy'ler) veya sanal özel ağlar (VPN'ler) kullanılması ve web sitesi önbellek ve arşivlerinin kullanılması gibi çevrimiçi proaktif araştırmaya yardımcı olacak diğer teknolojileri kullanmayı düşünebilir. Bunlar, teşkilatın ve bireysel olarak müfettişin korunmasına yardımcı olabilir.

4.4.4 İşletim Sistemleri ve Yazılım Çözümleri

Çevrimiçi sorgularda kullanılan işletim sistemi tercihi tamamen söz konusu kaynağın kurulumunu yapan teşkilata bağlıdır. Dünyada en çok kullanılan işletim sistemi Windows olduğundan ve proaktif çevrimiçi çalışma ve delil toplamanın gereksiz dikkat çekmeden yapılması gerektiğinden, Windows uygun bir tercih olacaktır. Kılavuzun bu güncellemesi sırasında, Windows 10 en çok kullanılan işletim sistemidir ancak Windows 11 piyasaya sürülmüştür ve popülerlik kazanacaktır.

Bununla birlikte, herhangi bir teşkilatı Mac tabanlı bir çözüm veya Linux kullanmaktan alıkoyan hiçbir şey yoktur, ancak bu durum normalden farklı olarak öne çıkacaktır ve bu da dikkatli bir şüphelinin dikkatini çekebilir, ayrıca çevrimiçi sorgularda standart hale gelmiş bazı yazılımların kullanılmasında bir sorun olabilir. Ancak tüm olasılıklar değerlendirilmelidir ve bazı durumlarda bunlardan yararlanmak tamamen uygun olabilir. Daha önce de belirtildiği gibi, bir işletim sisteminin tescil edilmesi ve lisanslı bir ürünün kullanılması bir öncelik olmalıdır.

Müfettiş tarafından çevrimiçi veri toplamak için kullanılabilecek bir dizi yazılım çözümü bulunmaktadır. Müfettişin çalışmalarının sonucunda ortaya çıkan bulguları kaydetmesi için ekran görüntüsü alma yazılımı kullanılmalıdır. Çevrimiçi bir sorgulamada herhangi bir bilgi, istihbarat ve delil büyük olasılıkla bir web tarayıcısı içerisinde görünecektir. Bu nedenle, bu içeriğin tutarlı bir şekilde ve zamanında toplanması gereklidir.

Bazıları ücretsiz, bazıları ücretli olan birçok farklı ekran görüntüsü alma yazılımı ürünü mevcuttur. Tercih teşkilata kalmalıdır. İşletim sistemlerinin kendileri de ekran görün-

tüsü almak için basit çözümler sunmaktadır. Windows ortamında; Ekranı Yazdır, Ekran Alıntısı Aracı, Sorun Adımları Kaydedici ve başka hiçbir şey çalışmıyorsa veya müfettiş resmi veya dosyayı dahili meta verileri ile bir bütün olarak gerçekten kaydetmek istiyorsa potansiyel olarak bir "Sağ Tıklama > Farklı Kaydet" seçeneği bulunmaktadır. Diğer işletim sistemlerinin de kendi uygulamaları vardır.

Tercih, belki de hem "sabit görüntü" çekimlerini hem de "video" çekimlerini kaydedecek bir araca indirgenmektedir. Kaydedilmesi gereken tüm materyaller tek bir sitede ve tek ekranda görünmeyecektir, bu nedenle farklı kayıt gereksinimlerini karşılamak için biraz çok işlevli olması gerekmektedir.

Sabit görüntü alma işlemi gerçekleştirecek üçüncü taraf araçlar mevcuttur (örneğin, Screenshot Captor[94], EasyCapture[95], TinyTake[96], FastStone[97] ve SnagIt[98]). Bu, eksiksiz bir liste değildir. Video kayıt işlemi gerçekleştirecek benzer araçlar da vardır (Free Screen Recorder[99], CamStudio[100], oCam[101], Debut Video Recorder[102], Snagit, FastStone ve Camtasia[103]). Bu araçların kullanımı sezgisel ve son derece basittir. Çoğu durumda, "Ekran Görüntüsü Al" veya "Kaydet" düğmesine basın ve başlatın.

Müfettiş, söz konusu kaydın delil olarak kullanılmasının amaçlandığının her zaman bilincinde olmalıdır. Efektler eklenmemeli ve videoların herhangi biri hiçbir şekilde düzenlenmemeli ve hatta kod çevrimi (yani diğer cihazlarda kullanmak üzere format değiştirme) dahi yapılmamalıdır. Orijinal "delil kaydı" her zaman için çıkarılabilmesi ve sunulabilmesi mümkün olan asıl kayıt olmalıdır.

Şeffaflık seviyesini artıracak şekilde daima tam ekran kaydı yapılması önerilir. Müfettiş ekranın bir alanını yakınlaştırarak herhangi bir şeyi vurgulamak isterse, internet tarayıcısının yakınlaştırma işlevleri (veya windows büyüteci) kullanılmalıdır. Düzenleme sırasında daha sonra bir yakınlaştırma ekleme isteğine karşı konulmalıdır. Son olarak, mümkünse delilin tek bir dosya içine kaydedilmesi, kayıt sırasında kesme ve duraklamadan kaçınılması çok önemlidir. Bu, özellikle de sayfanın kaydırılmasını gerektiren bir sosyal medya görüntüsünün alınması sırasında zor olabilir.

Aynı zamanda kayıt yaklaşımında da bazı zayıflıklar vardır. Örneğin, bir web sunucusunun sahte bir web sayfasının/sitesinin bir kopyası ile kurulduğu ve bilgisayardaki DNS kayıtlarının/yönlendirmesinin gerçek çevrimiçi web sitesi yerine kopyayı gösterecek şekilde değiştirildiği durumlarda karşımıza çıkar.

---

94 https://download.cnet.com/Screenshot-Captor/3000-20432_4-10433616.html

95 https://easycapture.en.softonic.com/

96 https://tinytake.com/

97 https://www.faststone.org/

98 https://www.techsmith.com/screen-capture.html

99 https://www.bandicam.com/free-screen-recorder/

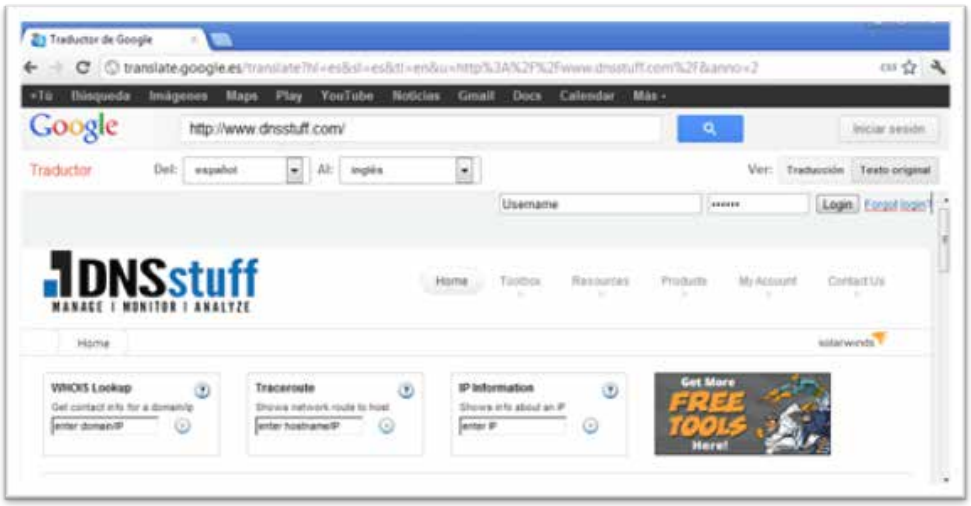
100 https://camstudio.org/

101 https://ohsoft.net/eng/ocam/intro.php?cate=1002

102 https://www.nchsoftware.com/capture/index.html

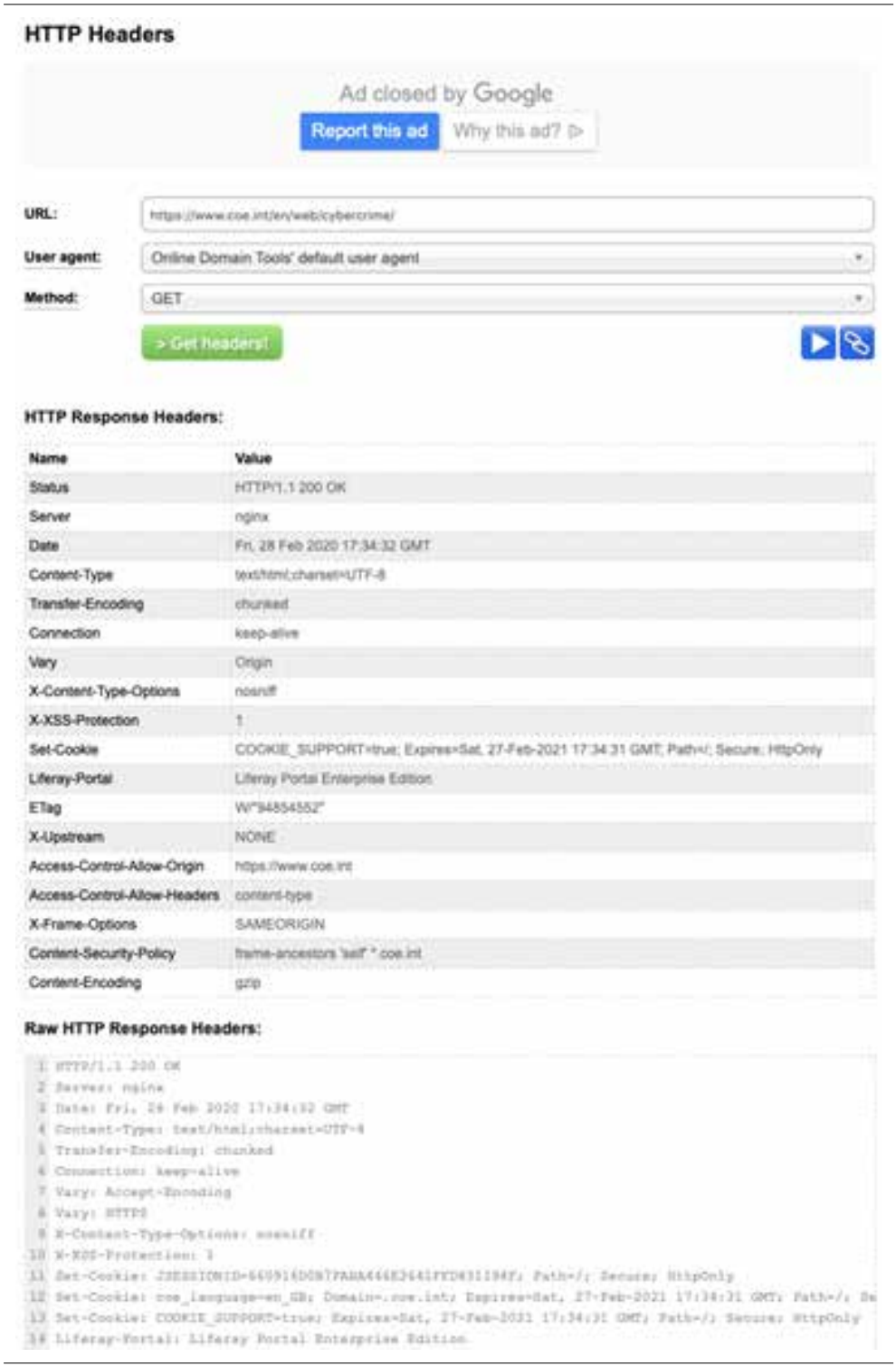
103 https://www.techsmith.com/video-editor.html

Bu tam da müfettişin olabileceğini beklemesi gereken türden bir zorluktur. Bu özel sorunu aşmanın bir yolu, orijinal olduğunu göstermek için kaydedilen çevrimiçi içeriğe "dolaylı erişimi" de kaydetmek olabilir. Örneğin, bunu yapmanın basit bir yolu, hedef siteye erişmek için Google Çeviri gibi bir araç kullanmaktır (Google Çeviri'nin, çevrilmemiş dolaylı görünümün görüntülenebilmesi için bir "Orijinal İçeriği Göster" düğmesi sunduğunu unutmayın).



Bu görüntüde, DNSstuff web sitesi (masum) hedeftir ve ekrandaki görüntünün bir bilgisayar korsanı tarafından oluşturulan klonlanmış bir web sitesi olmadığını doğrulamak için Google çeviri kullanılmaktadır. Böylece, DNSstuff'a doğrudan bilgisayarınızın bağlanması yerine, bir Google sunucusu bu web sitesiyle bağlantı kurar ve ana sayfayı ister. Bu, incelemenin gerçekten de orijinal web sayfası üzerinde yapıldığını bir video kaydında "canlı" olarak gösterebilir. Aynı zamanda, Google Çeviri ziyaretinin saati ve tarihi, IP adresi ve çevrilen URL, Google Sunucularının günlüklerine de kaydedilmiş olacaktır.

Videoya kaydedilen delili daha sağlam hale getirmenin bir başka yolu, hedef web sayfaları ile ilgili bazı ilave, daha "teknik" verileri de kamerada göstermek olabilir. Olası bir seçenek, belirli bir alan adı için "HTTP başlıklarını" gösteren http://http-headers.online-domain-tools.com adresine gitmek olabilir. Başlıklar genellikle doğrudan siteyi barındıran web sunucusu tarafından sağlanan ve verilerin barındırıldığı web sunucusundaki saati gösteren bir "Tarih" alanı sağlar.



HTTP Headers

Ad closed by Google

Report this ad | Why this ad? ▷

URL: https://www.coe.int/en/web/cybercrime/

User agent: Online Domain Tools' default user agent

Method: GET

> Get Headers!

HTTP Response Headers:

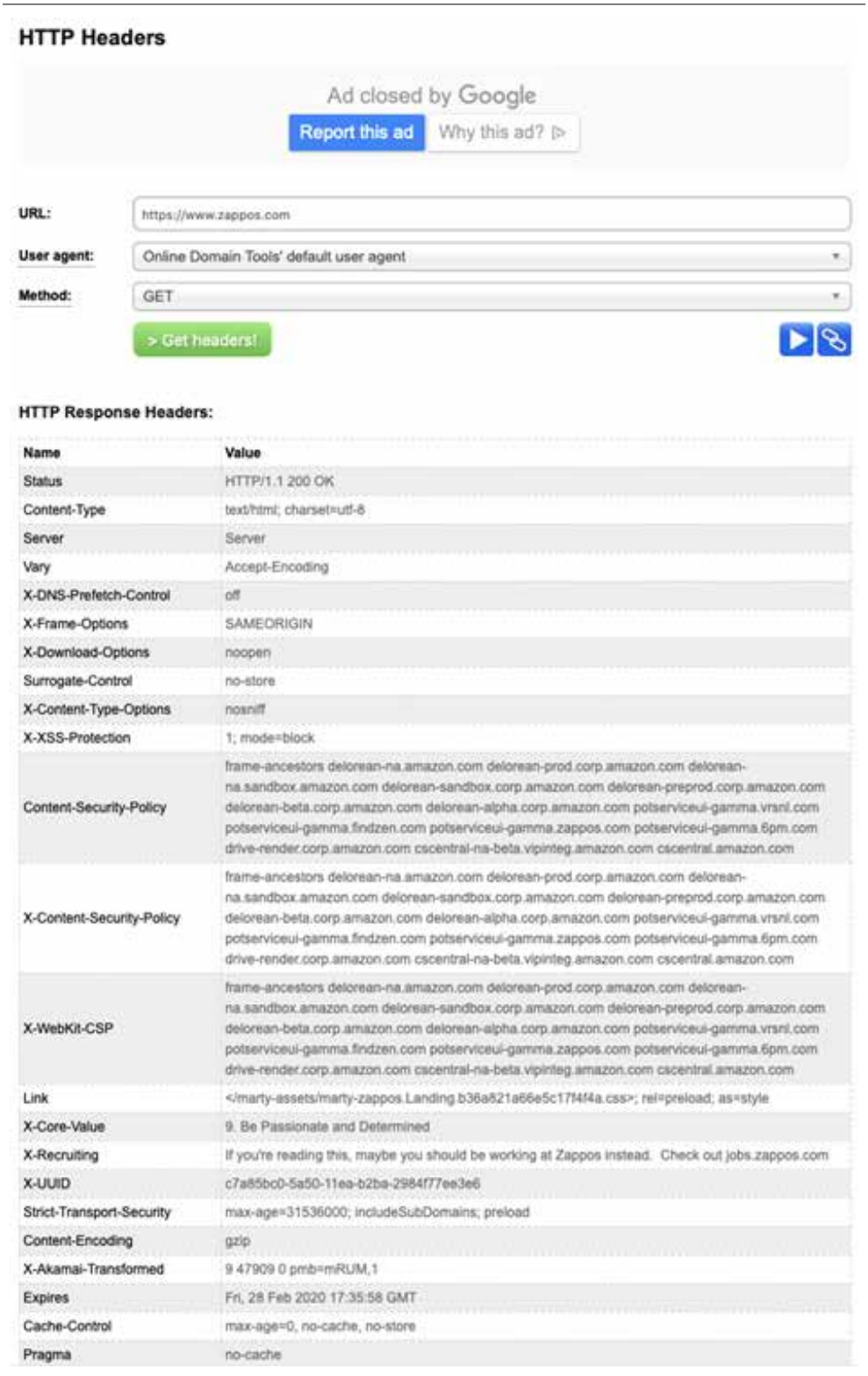
Name	Value
Status	HTTP/1.1 200 OK
Server	nginx
Date	Fri, 28 Feb 2020 17:34:32 GMT
Content-Type	text/html;charset=UTF-8
Transfer-Encoding	chunked
Connection	keep-alive
Vary	Origin
X-Content-Type-Options	nosniff
X-XSS-Protection	1
Set-Cookie	COOKIE_SUPPORT=true; Expires=Sat, 27-Feb-2021 17:34:31 GMT; Path=/; Secure; HttpOnly
Liferay-Portal	Liferay Portal Enterprise Edition
ETag	W/"94854552"
X-Upstream	NONE
Access-Control-Allow-Origin	https://www.coe.int
Access-Control-Allow-Headers	content-type
X-Frame-Options	SAMEORIGIN
Content-Security-Policy	frame-ancestors 'self' *.coe.int
Content-Encoding	gzip

Raw HTTP Response Headers:

```
1 HTTP/1.1 200 OK
2 Server: nginx
3 Date: Fri, 28 Feb 2020 17:34:32 GMT
4 Content-Type: text/html;charset=UTF-8
5 Transfer-Encoding: chunked
6 Connection: keep-alive
7 Vary: Accept-Encoding
8 Vary: HTTP2
9 X-Content-Type-Options: nosniff
10 X-XSS-Protection: 1
11 Set-Cookie: JSESSIONID=6605916D0B7FA8A644E2641FFD831194; Path=/; Secure; HttpOnly
12 Set-Cookie: coe_language=en_GB; Domain=.coe.int; Expires=Sat, 27-Feb-2021 17:34:31 GMT; Path=/; Se
13 Set-Cookie: COOKIE_SUPPORT=true; Expires=Sat, 27-Feb-2021 17:34:31 GMT; Path=/; Secure; HttpOnly
14 Liferay-Portal: Liferay Portal Enterprise Edition
```

Burada, sunucu yazılımının (nginx) ve bazı çerez verilerinin gösterildiği bir başlık örneği verilmiştir:

Bazı başlıkların ek bilgiler de sağlayabileceğini gösteren bir diğer örnek aşağıdadır:



HTTP Headers

Ad closed by Google

Report this ad | Why this ad?

URL: https://www.zappos.com

User agent: Online Domain Tools' default user agent

Method: GET

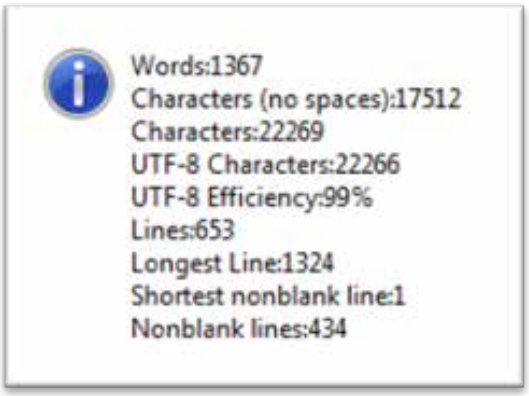
> Get headers!

HTTP Response Headers:

Name	Value
Status	HTTP/1.1 200 OK
Content-Type	text/html; charset=utf-8
Server	Server
Vary	Accept-Encoding
X-DNS-Prefetch-Control	off
X-Frame-Options	SAMEORIGIN
X-Download-Options	noopen
Surrogate-Control	no-store
X-Content-Type-Options	nosniff
X-XSS-Protection	1; mode=block
Content-Security-Policy	frame-ancestors delorean-na.amazon.com delorean-prod.corp.amazon.com delorean-na.sandbox.amazon.com delorean-sandbox.corp.amazon.com delorean-preprod.corp.amazon.com delorean-beta.corp.amazon.com delorean-alpha.corp.amazon.com potserviceui-gamma.vrsnl.com potserviceui-gamma.findzen.com potserviceui-gamma.zappos.com potserviceui-gamma.6pm.com drive-render.corp.amazon.com cscentral-na-beta.vipinteg.amazon.com cscentral.amazon.com
X-Content-Security-Policy	frame-ancestors delorean-na.amazon.com delorean-prod.corp.amazon.com delorean-na.sandbox.amazon.com delorean-sandbox.corp.amazon.com delorean-preprod.corp.amazon.com delorean-beta.corp.amazon.com delorean-alpha.corp.amazon.com potserviceui-gamma.vrsnl.com potserviceui-gamma.findzen.com potserviceui-gamma.zappos.com potserviceui-gamma.6pm.com drive-render.corp.amazon.com cscentral-na-beta.vipinteg.amazon.com cscentral.amazon.com
X-WebKit-CSP	frame-ancestors delorean-na.amazon.com delorean-prod.corp.amazon.com delorean-na.sandbox.amazon.com delorean-sandbox.corp.amazon.com delorean-preprod.corp.amazon.com delorean-beta.corp.amazon.com delorean-alpha.corp.amazon.com potserviceui-gamma.vrsnl.com potserviceui-gamma.findzen.com potserviceui-gamma.zappos.com potserviceui-gamma.6pm.com drive-render.corp.amazon.com cscentral-na-beta.vipinteg.amazon.com cscentral.amazon.com
Link	</marty-assets/marty-zappos.Landing.b36a821a66e5c17f4f4a.css>; rel=preload; as=style
X-Core-Value	9. Be Passionate and Determined
X-Recruiting	If you're reading this, maybe you should be working at Zappos instead. Check out jobs.zappos.com
X-UUID	c7a85bc0-5a50-11ea-b2ba-2984f77ee3e6
Strict-Transport-Security	max-age=31536000; includeSubDomains; preload
Content-Encoding	gzip
X-Akamai-Transformed	9 47909 0 pmb=mRUM,1
Expires	Fri, 28 Feb 2020 17:35:58 GMT
Cache-Control	max-age=0, no-cache, no-store
Pragma	no-cache

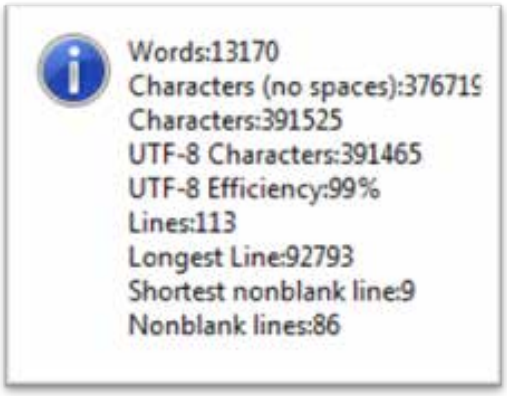
4.4.5 Kaynak Kodu Kullanın

HTML kaynak kodu, bir web sayfasının, mahkemede delil olarak kullanılacak anlık görüntüsünü oluşturmak konusunda yardımcı olabilir. Alan sınırlamaları nedeniyle kaynak kodunun tamamı yeniden üretilmeyecektir, fakat burada daha önce sunulan sahte web sayfasının altında yatan kaynak kodu ile ilgili bazı istatistikler bulunmaktadır.



Bu meta veri sayılar görselin içeriği ile karşılaştırılarak oldukça çok verinin eklendiği gösterilebilir.

Örnek web sayfası gerçekten basitti, ancak bir standart Facebook ana sayfasına ait istatistikler aşağıdaki gibidir:



Burada oldukça fazla veri bulunmaktadır ve bunların çok azı tarayıcı tarafından fiilen ekran görüntüsüne dönüştürülmektedir.

Bir yan not olarak, söz konusu Facebook ana sayfasının HTML ve Javascript'i, (100001248123456'ya benzeyen) kullanıcı fbid[104]'sine 38 atıf ve ayrıca resimler ve Facebook arkadaşları olan diğer kullanıcılar için yüzlerce kimlik içeriyordu. Birinin kaynak kodundaki tüm referansları gizlemesi veya değiştirmesi muazzam bir iş olacaktır.

[104] Facebook kimliği

4.4.6 Bir Web Sayfasına Ait HTML Kaynak Kodunun Bulunması ve Kopyalanması

Tüm tarayıcılarda bir web sayfasını kaydetme seçeneği bulunur ve bunu yaparken gerçekte kaynak kodunu kaydedecektir. Tarayıcı menüleri, "Sayfayı Farklı Kaydet" veya "Dosya -> Farklı Kaydet" gibi seçenekler sunacaktır. Alternatif olarak, çoğu tarayıcı "Kaynağı göster" olarak ifade edilen bir seçenek sunar. Belirli bir web sayfasına sağ tıklandığında, kopyalanıp bir metin dosyasına veya Word belgesine yapıştırılabilen veya (bir tarayıcı ile açılması gereken) bir HTML belgesi olarak kaydedilebilen HTML kaynak kodu ortaya çıkacaktır.

4.4.7 Bir Web Sitesinin Görüntülenebilir Bir Kopyasını Oluşturma

Bir web sitesinin içeriğini daha sonra incelenmek üzere saklamaya yönelik başka bir teknik, görüntülenebilir bir çevrimdışı kopyasını oluşturmaktır. Bunu yapabilen birkaç tane yazılım vardır. Bunlara örnek olarak HTTrack[105], InSpyder[106], Blackwidow[107] ve DarcyRipper[108] verilebilir. Bunlar, web sitelerinin tüm içeriğinin yanı sıra medya dosyalarını da internetten indirme kabiliyetine sahiptir.

Söz konusu araçlar çoğunlukla kaynak kod içindeki tüm yolları medya dosyalarına ve bağlantılı sitelere işaret edecek şekilde değiştirebilir, böylece web sitesi ilişkili tüm resimlerle çevrimdışı olarak görüntülendiğinde etkin bir şekilde yeniden oluşturulur. Bu, bir web sitesi içeriğinin mahkemeye sunulması gerektiğinde iyi bir yaklaşım olabilir, ancak müfettiş kaynak kodunun araç tarafından değiştirildiğini unutmamalıdır. Bu tür araçlar, mevcut bağlantıları takip ettikleri ve bağlantısız sayfaları bulamayacakları için genellikle web sitesinin tamamını kopyalayamazlar.

Müfettiş, bu araçların kullanımının olağandışı bir dijital ayak izi oluşturma potansiyeline sahip olduğunun - bir web sitesindeki tüm sayfalar çok hızlı bir şekilde görüntülendiği için, web sunucusu kayıtları bilgili bir web yöneticisi tarafından incelenirse "insan olmayan" tarama kullanımı tespit edileceğinin - bilincinde olmalıdır.

4.4.8 Veri Toplamada Kullanılmak Üzere Çevrimiçi Profiller Oluşturma

İçerik için erişilmesi ve değerlendirilmesi gereken çevrimiçi kaynakların çoğu, içlerine girmek için müfettişin bir profile sahip olmasını gerektirir. Bu, özellikle de Facebook, Twitter, Instagram vb. gibi sosyal medya siteleri ile ilgilidir. Bu sorunun, buna izin verecek profilleri oluşturmayı düşünmek dışında kolay bir çözümü yoktur. Bu, bazı yargı bölgelerinde sorun yaratabilir. Diğer yargı bölgelerinde bu basit olabilir ama şeffaflık unsurları gerektirebilir, bu nedenle çevrimiçi olma ve veri toplama işlemlerinin sorgulandığı durumlarda müfettiş ve soruşturma sorumlu olacaktır.

Gizli Çevrimiçi soruşturmaya bu bölümde daha sonra bakacağız, ancak bu noktada çevrimiçi profillerin kullanımını artırmanın ağır basan tarafı, her müfettişin kendi yargı

---

[105] https://www.httrack.com/

[106] https://www.inspyder.com/

[107] https://blackwidow.en.softonic.com/

[108] https://darcyripper.com/

bölgesinin hukuk sistemi kapsamındaki gerekler konusunda eksiksiz bilgi sahibi olması ve daha sonra yasal sorunlara yol açacak bir hesap oluşturmaya kayıtsız kalmaması gerekliliğidir.

Bu kılavuzu kullanan her yargı bölgesi, aynı ülke içinde bile farklı kural ve düzenlemelere sahip olabilir, bu işin nasıl yapıldığı konusunda teşkilatlar arasında da farklı görüşler olabilir.

Çevrimiçi kaydı kolaylaştırmak amacıyla bir çevrimiçi kimlik oluşturulmasına izin verenler açısından, bunların kullanımına ilişkin kayıtların tutulması ve kullanma yetkisi, düzgün ve etkili bir şekilde kullanılmasını sağlamak ve nihayetinde elde edilen materyal delil olarak kullanıldığında sorunlara neden olmamasını sağlamak bakımından çok önemlidir.

4.4.9 Noter

Delil hazırlamaya yardımcı olmak üzere bir Noter veya başka bir hukuk görevlisinin tercih edilebileceği durumlar vardır. Noterin medeni hukuk yargı bölgelerindeki görevlerinden biri, belirli yasal belgeleri ve anlaşmaları bir mahkeme tarafından kabul edilebilir bir şekilde gözden geçirmek ve doğrulamaktır. Delil olarak ihtiyaç duyulan her türlü çevrimiçi materyale, bilgisayarlarını ve internet bağlantılarını kullanarak erişmek için bir noter davet edilebilirse, açığa çıkarılan delilin gerçekliğini resmi olarak onaylayabilirler. Uluslararası işbirliğinin gerekli olduğu durumlarda, birçok ülke arasında noter tasdikli belgeleri tanıma anlaşmaları bulunmaktadır.

4.4.10 Mevcut Yaklaşımlarla İlgili Sınırlamalar

Çevrimiçi delillerin otomatik olarak elde edilmesini sağladığı iddia edilen ve delillerin kabul edilebilirliğini garanti ediyormuş gibi görünen birçok araç ve hizmet vardır. Her ne kadar bu araç ve hizmetlerin birçoğu delilin mahkemede kabul edilme olasılığını artırsa da, herhangi bir yasal çerçeve altında %100 kabul edilebilirliği garanti edebilecek bir araç yoktur.

İki temel sınırlama bulunmaktadır:

1. Tüm yazılım araçları, bazen elde edilmesi zor ve üçüncü bir tarafa kanıtlanması neredeyse imkansız olan "güvenilir" bir bilgi işlem ortamına ihtiyaç duymaktadır. Basit bir ifadeyle, bir müfettişin bilgisayarında çalışan herhangi bir araç ele geçirilebilir ve değiştirilebilir. Son zamanlarda bu konuda (örneğin Güvenilir Platform Modülü ile) bazı büyük ilerlemeler kaydedilmiştir, ancak bu tür sistemler delil amacıyla kullanılmak üzere henüz yeterince olgunlaşmış değildir.

2. Ticari bir hizmetin güvenilirliği, ancak söz konusu hizmeti sunan şirketin güvenilirliği kadardır. Bu tür hizmetler kendilerini, "zaman damgası", "şifreleme", "dijital mühürler", "mikro adresleme" gibi etkileyici bir dizi işlev sunarak pazarlama eğilimindedir. Zayıf nokta genellikle en başta verilerin toplanmasıdır. Hizmetin sahte verilerle bozulmaya karşı savunmasız olabilme riski varsa, sağladığını iddia ettiği herhangi bir delil için de aynı risk geçerli olacaktır.

4.4.11 Çevrimiçi Etkinliğin Sonlandırılması

Çevrimiçi etkinliğin sonunda, birden fazla oturum üzerinden yapılıyorsa her oturum veya soruşturmanın sonunda veya soruşturmanın sonunda, fakat herhangi bir kovuşturma ve mahkeme davası öncesinde ele alınması gereken bir takım başka hususlar da vardır.

- **Veri Depolama**

Çevrimiçi (başta yerel olarak kaydedilmiş olan) verilerin depolanması; tüm kayıtların güvenli bir yerde tutulması, süreklilik amacıyla ayrı bir yere kopyalanması ve kopyalanmak, açıklanmak veya ilgili makamlara sunulmak üzere hazır tutulması durumunda çok önemli bir husustur. Bu bölümde daha önce çevrimiçi soruşturma yapmaya uygun ekipmanlara yapılan atıf, uygun bir medya depolama imkanını da içermelidir. Bu; özellikle amaca yönelik bir harici sabit disk sürücüsü veya USB sürücü de olabilir, tüm materyaller için sağlanan bir depolama sunucusu veya materyallerin kopyalandığı bir ağ kaynağı da olabilir. Her teşkilatın kendi çözümü olacaktır ve bu konuda genellikle çözümün teminine yönelik kullanılabilir fonlar belirleyicidir.

Kaçınılması gereken durum, bazı çevrimiçi araştırmalar tamamlandığında toplanan içeriğin teşkilat içindeki bir makinede bulunan masaüstü klasöründe saklanması ve eldeki tek kopyanın bu olmasıdır. O makinenin veya içindeki sabit disk sürücüsünün arızalanması, bu verilere dayalı herhangi bir işlemi tehlikeye atar. Teşkilatlar bununla başa çıkmak için kendi prosedür ve protokollerini geliştirecektir, ancak müfettişlerin ve onların amirlerinin bunun yapılmasını sağlamaları gerekir.

- **Adresleme (hashing)**

İkinci hususta, "dijital mühürler" ve "mikro adresleme (hashing)" vurgulanarak önceki bölümde zaten bahsedilmiştir. Bu kılavuz, müfettişi çevrimiçi materyalleri nasıl toplayacağı konusunda yönlendirmek için yeterli bilgi içermektedir ve müfettişlerin deneyimleri arttıkça becerileri de gelişecektir. Ancak, çevrimiçi etkinliğin her oturumunun sonunda, elde edilen verilerin bütünlüğünü sağlamak için dosya düzeyinde "adresleme (hashing)" adı verilen bir işlemin gerçekleşmesi önemlidir.

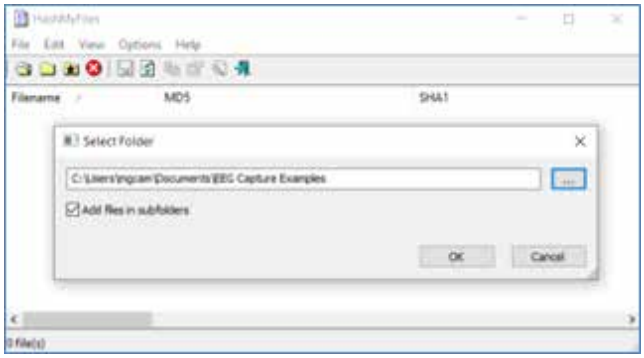
Bir şeyi adresleme süreci oldukça basit olmasına karşın arkasındaki teknoloji basit olmaktan çok uzaktır. Bir adres (hash), basit anlamda "dijital parmak izi" olarak tanımlanabilir - herkes parmak izi kavramını ve parmak izinin bir kişiye özgü ve eşsiz olduğunu anlar. Bu sayede bir kişi parmaklarının ucundaki desen ile tespit edilebilmektedir. Bu benzetme veriler için de uygulanabilir.

Bir adres (hash), herhangi bir şeyin değişmediğine dair bir güvence sağlamak için matematiksel bir algoritma kullanılarak verilere tahsis edilen bir değerdir. Yani bir dosya, adres (hash) değeri ile tespit edilebilir, ancak daha önemlisi, bir dosyada yapılan **değişiklikler** de, adres değerindeki **değişiklik** ile tespit edilebilir.

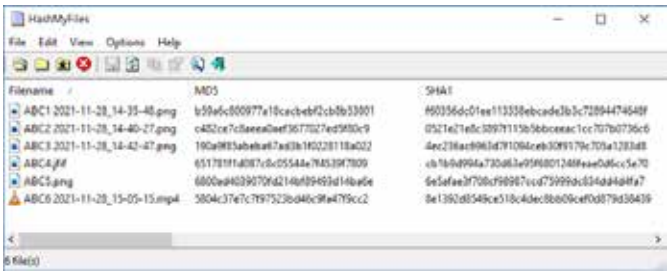
Dolayısıyla çevrimiçi kayıt süreci; bir müfettişin çevrimiçi olması, sorguları ile ilgili ekran görüntülerini, dosyaları, videoları vb. kaydetmesi ve bunları kayıt oturumu/oturumları boyunca tutulan İnternet Etkinlik Raporunda açıklandığı şekilde belirli bir yere koyması olmalıdır. Söz konusu oturumdaki çalışma bittiğinde, müfettiş tüm dosyalar üzerinde bir "adresleme (hashing)" programı çalıştırır ve bu program da her dosya için kaydedildikleri noktada benzersiz bir tanımlayıcı oluşturacaktır.

Aşağıdaki örnek, bu bölümde daha önce gösterildiği şekilde elde edilen dosyaları göstermektedir.

HashMyFiles[109] gibi bir yazılım programı kullanarak, kayıt klasörünün tüm içeriğini (alt dizinler de dahil olmak üzere) içe aktarabiliriz.



Daha sonra bu 6 dosyanın her birini "adreslersek", her biri için aşağıda gösterildiği gibi bir dijital değer üreteceğiz.



Şu anda kullanılan iki temel adresleme algoritması MD5 ve SHA1›dir. Yazılım bunların her ikisini de aynı anda hesaplayacaktır. Mevcut başka adresleme algoritmalar da vardır, ancak birlikte çalışan bu iki algoritma, herhangi bir veri değişikliğini kanıtlamak için gereken güvenliği sağlayacaktır. HashCalc[110] veya Karen's Hasher[111] gibi başka adresleme programları da mevcuttur.

---

[109] https://www.nirsoft.net/utils/hash_my_files.html

[110] https://www.slavasoft.com/hashcalc/

[111] https://www.karenware.com/powertools/karens-hasher

Adresleme işleminin doğruluğu daha önce de dijital delil arenası genelinde sorgulanmıştır. Adres çakışmaları (aynı adrese sahip farklı veriler) yapay olarak üretilmiş, ancak farklı algoritmalar arasında aynı uyumsuzluğun sağlanması gerçekleşmemiştir. Bu nedenle adresleme, bir istihbarat ve delil sürecinden geçerken verileri doğrulamanın ve bütünlük sağlamanın büyük ölçüde kabul edilebilir bir yoludur.

Çevrimiçi kayıtlarla ilgili klasörün ve alt klasörlerin içinde yüzlerce dosya olabilir. Bunların hepsi bu yolla işlenecektir. Adresleme algoritması, dosyanın veri içeriğine bakmakta ve bütün içeriğin adreslemesini hesaplamaktadır.

Adresleme, deliller bakımından güvenilirlik sağlayacak ve kayıtların doğrulanmasını sağlayacaktır. Bu konuyu daha geniş ele almak için, bu 6 dosya kaydedilmiş ve adreslenmiştir. Daha sonra depolanmak üzere bir harici sürücüye veya ağ konumuna gönderilir ve elektronik ortamda savcıya sunulurlar. Kayıt sırasında hesaplanan adres her zaman aynı kalacak ve orijinal dosyayla birlikte saklanacaktır. Karşı tarafa ulaşan dosya yeniden hesaplama sonucunda aynı adrese sahip çıkmazsa, o dosyada onu orijinalinden daha az güvenilir kılan bir değişiklik olmuştur. Müfettişlerin, verilerin değişmediğinden ve sistemde çalışan herkesin buna tam olarak güvendiğinden emin olması gereklidir. Bu nedenle adresleme, çevrimiçi kayıt sürecinin hayati öneme sahip bir parçasıdır.

4.4.12 Toparlama

Artık anlaşıldığı üzere, çevrimiçi dijital delillerin herhangi bir yerdeki herhangi bir mahkemede kabul edilebilirliğini garanti edecek şekilde güvence altına alınması için ideal bir metodoloji veya araç seti yoktur. Günümüzde en iyi uygulama, elde edilen verilerin kalitesinin en üst düzeye çıkarılmasını ve delillerin bütünlüğünü ve elde edildiği sürecin şeffaflığını mümkün olduğunca sağlamak için gereken tüm adımların atılmasını içerir. Yerel yasalar izin veriyorsa, ek bir nesnel doğrulama unsuru eklemek için noter veya benzeri bir devlet memuru veya güvenilir bir devlet Zaman Damgası Kurumunun hizmetleri kullanılabilir. **Tüm bunlar göz önünde bulundurularak, bir prosedürün veya metodolojinin kabul edilebilirliği, bunlar benimsenmeden önce adli müşavirler ile kontrol edilmelidir.**

4.5 Gizli Çevrimiçi Soruşturmalar

Bu Kılavuz, bir kolluk görevlisinin gizli görevi hakkında sadece genel tavsiyelerde bulunabilir. Gizli soruşturmaya (internette veya gerçek dünyada) dahil olan herkes, daima gerektiği şekilde eğitilmiş, yetkin ve yetkili olmalıdır.

Bazı yargı bölgelerinde bu görev olmayabilir veya ulusal yasalarca yasaklanmış bile olabilir. Gizli memur görevlendirmenin söz konusu olduğu her durumda, mevzuata, politikalara, prosedürlere, uygulama kurallarına ve söz konusu yargı bölgesinde soruşturmaların yürütülmesine ilişkin geçerli standartlara daima gereken saygı gösterilmelidir.

Herhangi bir çevrimiçi soruşturmaya başlamadan önce, yetkilendiren amir ve gizli ajan, söz konusu soruşturmanın kapsamını ve gerekliliklerini ve ayrıca gizli çevrimiçi

müfettişin görevinde ve çalışmasında geçerli olacak parametreleri belirlemelidir. Bir risk değerlendirmesi hazırlanmalı ve görev boyunca sürekli olarak tekrar değerlendirilmeli ve gözden geçirilmelidir.

Tüm kararlar ve işlemler, geçerli politika ve mevzuata uygun olarak belgelendirilmelidir. Bu günlük, herhangi bir kararın nasıl ve ne zaman alındığını göstermeli ve uygun olduğunda, bu kararların nedenlerine ilişkin bir not içermelidir.

Herhangi bir harekete geçilmeden önce, bilgi ve istihbarat paylaşımına ilişkin çerçeve resmi olarak oluşturulmalıdır. Bu, soruşturmanın doğrultusunda herhangi bir öngörülemeyen değişiklik olması durumunda çevrimiçi ajana yardımcı olması için bir destek görevlisinin kullanılmasını gerektirebilir. Destek görevlisi aynı zamanda, yetkilendiren amir ile çevrimiçi etkileşimi kesintisiz olarak sürdürmek için gereken diğer hizmetler arasında da bir aracı görevi görecektir.

Ajan, gizli operasyonlar yürütürken, mevcut ekipman, kaynaklar ve destek ve internet tabanlı yardımcı programlara ilişkin kendi bilgilerini dikkate alarak, bir dizi soruşturmaya uygun geçerli gizli çevrimiçi kimlikler oluşturmalı ve bunları muhafaza etmelidir.

Bu tür bir soruşturmayı gizli ve takip edilemez bir şekilde yürütmek için gereken ekipmanlara ve ilgili hizmetlere kaynak ayrılmasına önem verilmelidir. Herhangi bir ekipmanın veya hizmetin hiçbir koşulda kolluk kuvvetine kadar geri takip edilmesi mümkün olmamalıdır.

Ekipmanlar ve tüm potansiyel kayıt sistemleri, düzgün çalıştıklarından emin olmak adına ve bu tür işlemler için sürekli olarak uygun olduklarını doğrulamak amacıyla düzenli olarak test edilmelidir.

Ajanlar, gizli kimlikleri altında çalışırken uygun standartlara ve etik standartlara bağlı kalmalıdır. Bilgilerin toplanması sırasında, soruşturmanın öznesi ile temas kurarken ve bu teması sürdürürken, ilk görevlendirme talimatları içinde belirtilen tüm koşullara uygun olarak hareket etmelidirler.

Çevrimiçi soruşturmalar çok hızlı bir şekilde gelişebildiğinden, ajanlar bir etkileşim sırasında ortaya çıkabilecek olası çatışmalar veya zorluklar ile başa çıkmak için önceden hazırlanmalı ve stratejiler geliştirmelidir. Örneğin aşırı durumlarda bu, uygun yanıtı değerlendirmek için yeterli zamanı kazanmak amacıyla ekipman arızası olmuş gibi yapılmasını gerektirebilir.

Ajanlar şunları yapmalıdır:

- Eylemlerinin yasal sınırlarını belirleyebilmek (nelerin suça iştirak teşkil ettiğini bilebilmek de dahil olmak üzere);
- Delilleri doğrulama ihtiyacını derinlemesine anlamak;
- Öznenin ve soruşturmadan etkilenen diğer tüm tarafların İnsan Haklarını göz önünde bulundurmak.

Ajanlar, soruşturma ile ilgili tüm materyallerin daima muhafaza edildiğinden ve sağlam ve tekrar kullanılabilir bir biçimde kaydedildiğinden emin olmalıdır. Bu, normalde ilgili kurumda mevcut olmayan güvenli sistemlerin geliştirilmesini gerektirebilir.

4.5.1 Teknik Riskler

Teknik açıdan bakıldığında, herhangi bir gizli görevde olduğu gibi, çevrimiçi ajanın gerçek kimliğini korumak için de adımlar atılmalıdır. Çoğu e-posta çözümü, ajanın IP adresini şüpheliye sağlayacaktır; hatta orijinal IP adreslerini sağlamayan (Gmail gibi) e-posta hizmetleri bile ajanı tespit etmek için kullanılabilir.

Bir siber suçlu tarafından kullanılan klasik bir teknik, bir kez açıldığında ajanın bilgisayarından IP adresini ve diğer ilgili bilgileri ortaya çıkaracak "yem" ekler göndermeyi içerir. Daha ayrıntılı başka teknikler de mevcuttur. Blog yazıları da aynı derecede açık olabilir ve (zaman içinde bir anda) sohbet genellikle her iki taraf arasında IP adresini tekrar ortaya çıkaracak doğrudan bir bağlantı kuracaktır. Bu nedenle, gizli görev ekipmanları, çevrimiçi olmadan önce test edilmelidir.

Deneyimli müfettişler, daha sonra sadece abonelik ile ödeme yapıldığında güvenli olduğu ortaya çıkan bir "Anonim e-posta yönlendirme" platformunu güvenli şekilde kullandıklarını düşünen suçluların kimliğini ortaya çıkarmıştır. İki kez kontrol edin ve daima ajanın bilgisayarına kadar geri takip etmeye çalışın.

"Açık kaynak" çevrimiçi soruşturma ve gizli "kapaklı" çevrimiçi soruşturma olarak adlandırılabilecek şeyler arasında çok sıkı sinerjiler bulunmaktadır. Bununla birlikte, özetle ilkinin hedefle herhangi bir doğrudan iletişim içermesi olası değildir ve çevrimiçi kaynaklardan kamuya açık bilgiler bulmaya çalışmaktır. Öte yandan ikincisinin ise niyeti tam olarak bir temas kurmak ve iletişim ve etkileşim başlatmaktır.

5 Üçüncü Tarafların Elindeki Veriler

Bölüm 3 ve 4 içinde açıklandığı gibi bir cihaza fiziksel olarak veya uzaktan erişim her zaman mümkün olmayabilir. Büyük karmaşık cihazlarda (örneğin büyük İnternet Servis Sağlayıcıların cihazlarında) depolanan verilere, İnternet Servis Sağlayıcının işbirliği ve yardımı olmadan erişilmesi neredeyse imkansız olabilir. Bunu aşmanın bir yolu, günlük dosyaları ve hizmet kayıt verilerini sağlayabilecek olan, (barındırma sağlayıcısı gibi) bir üçüncü tarafın işbirliği yapmasını istemek olabilir. Üçüncü taraflardan veri alınması, bölüm 5.1'de daha ayrıntılı olarak tartışılmaktadır.

Üçüncü taraflar ayrıca, bir bilişim suçunun gerçekleştiğini belirtip, kolluk kuvvetlerinin soruşturma başlatmasını isteyerek, geçici olarak elektronik delil toplayabilir. Bu husus, bölüm 5.2›de daha ayrıntılı olarak tartışılmaktadır. İnternetin devasa büyüklüğü ve her dakika gerçekleştirilen işlem sayısı, kolluk kuvvetlerinin elindeki kıt kaynaklarla interneti etkili bir şekilde izlemesinin imkansız olduğu anlamına gelir.

İnternetin bazı kısımları her internet kullanıcısı için tamamen erişilebilir olsa da, diğer kısımları kısıtlıdır ve kayıt olunmasını gerektirir. Suç, kapalı iletişim kanalları aracılığıyla işlendiğinde (örneğin kişisel e-posta veya mesajlaşma hizmetleri kullanılarak işlendiğinde), bu özel kanala erişimi olan bir birey tarafından bildirilmedikçe, kolluk kuvvetlerinin bu suçu fark etme veya suçla ilgili belgesel delil elde etme şansı çok azdır.

5.1 Bağımsız Veri Tutanlar

İnternet üzerinden işlenen suçun failini tespit etmek zor olabilir. Çoğu zaman, suçun kaynağı hakkında bilinen tek bilgi bir IP adresi, bir MAC[112] adresi, bir e-posta adresi, bir alan adı veya bir İnternet rumuzu veya "takma ad" olacaktır. İnternet adresinin arkasındaki gerçek kişiyi tespit edebilmek için, müfettişin İnternet Servis Sağlayıcıları tarafından tutulan verileri elde etmesi gerekir. İnternet erişimi, e-posta veya barındırma hizmeti sağlayıcılar genellikle, failin siber kimliği ile gerçek dünya kimliği arasındaki önemli bağlantıyı sağlayabilecek yegane kuruluşlardır. Bu nedenle bağımsız veri tutanlar çoğunlukla bir şüpheliyi adalete teslim etmenin anahtarı olabilir.

Aşağıdaki senaryo, aracı kuruluşların bir suçluyu nasıl tespit edebileceğini açıklamaya yardımcı olabilir: Bir kurbanın bilgisayarının güvenliği ihlal edilmiş ve fail, kurbanın (banka kayıtları ve çeşitli web sitelerine giriş şifreleri de dahil olmak üzere) tüm bilgisayar dosyalarına tam erişim sağlamıştır. Adli analiz, kurbanın makinesine casusluk yazılımı yükleyen kötü amaçlı yazılım içeren bir e-postanın kurban tarafından alındığını ortaya koyuyor. Konuyu araştıran polis memuru, hem virüslü e-postayı göndermek için kullanılan e-posta hesabını hem de gönderildiği IP adresini tespit edebiliyor. İnternet Servis Sağlayıcısı tarafından sağlanan bilgiler, e-postanın Finlandiya'nın büyük bir kasabasında bulunan bir şirket ağından gönderildiğini ortaya koyuyor. E-posta hesabı sağlayıcısı, aynı e-posta hesabına aynı gün içinde sadece Finlandiya'dan değil, aynı zamanda üç farklı ülkeden de erişildiğini gösteriyor. Açıkça görülüyor ki fail, ele geçirilmiş bilgisayarlar veya bir vekil ağ aracılığıyla e-posta gönderiyor. Ancak, e-posta hesabı sağlayıcısı, e-posta hesabı için bloke edilmiş bir kredi kartı numarası ile ödeme

[112] Medya Erişim Kontrolü adresi, bir ağ üzerindeki bir cihazı tanımlayan benzersiz bir numaradır.

yapılmaya çalışıldığını da ortaya koyuyor. Müfettiş, kredi kartının sahibi hakkında bilgi almak için kredi kartı şirketine bir talepte bulunuyor. Bilgiler, kredi kartı hesabının yaşlı bir Japon beyefendiye ait olduğunu, ancak numaranın internette bazı dolandırıcılık amaçlı alımlar için kullanılmasından sonra kısa süre önce kapatıldığını gösteriyor. Dolandırıcılık amaçlı alımlardan biri, bilgisayar ekipmanı için posta siparişi ile yapılmış. Bilgisayar donanımı satan perakendeci, malların sevk edildiği Hollanda'daki teslimat adresini bildirebiliyor. Hollanda'daki bu adreste arama yapıldığında, bir dizüstü bilgisayar bulunuyor ve hafızasında, ilk kurbana gönderilen kötü amaçlı yazılımın bulunduğu e-postanın bir kopyası bulunuyor.

Bu örnek, bir internet suçu failinin tespit edilmesinin, nasıl güçlü uluslararası işbirliği ihtiyacının yanı sıra, geniş bir dizi bağlantılı soruşturma içerebileceğini göstermektedir. Bu tür sorgulamalar (özellikle de yurt dışından delil talep edildiğinde[113]) zaman alabilir ve üçüncü bir tarafça saklanan verilerin, talepte bulunulana kadar artık erişilebilir olmaması gibi gerçek bir risk de vardır. Bu, özellikle de dolaşım verisi IP adresleri aranırken bir zorluk olabilir. Farklı yargı bölgelerinde, sağlayıcıların gerekli olabilecek veriler açısından uyması gereken farklı düzenlemeler vardır.

Müşteriler hakkında veya müşterilerin internet faaliyetleri hakkında herhangi bir kişisel veriyi açıklamadan önce, bağımsız üçüncü tarafların bir mahkeme emri veya başka bir yasal izin süreci talep etmesi kuvvetle muhtemeldir. Bu tür bilgiler, genel olarak ulusal gizlilik ve kişisel veri mevzuatı ve hizmet sözleşmelerinin şartları ile korunmaktadır. Ancak, kabul edilen yasal uygulamaya uygun olarak açıklanan delil niteliğindeki veriler mahkemede kabul edilir olacaktır.

Kullanıcılar verilerini giderek daha çok ISP'lerle bulutta depoladıkça, bu verilere erişim için üçüncü taraflara başvurma ihtiyacı da giderek daha yaygın hale gelmiştir. 2008 yılında Avrupa Konseyi, "***Bilişim suçlarına karşı kolluk kuvvetleri ile internet hizmet sağlayıcıları arasındaki işbirliğine yönelik kılavuz ilkeler***" başlığı altında delilleri güvence altına almak için ISP'lerle çalışmaya yönelik bir iyi uygulamalar ve tavsiyeler özeti yayınlamıştır.[114]

2020 yılında bu husus, internetin değişen dinamiğini ve orijinal çalışma yayınlandığında emekleme döneminde olan bulut depolama, şifreleme, Karanlık web ve kripto paralar gibi yeni teknolojilerin ortaya çıkışını yansıtmak amacıyla ***"Bilişim suçlarına karşı kolluk kuvvetleri ile İnternet servis sağlayıcıları arasındaki işbirliği: Ortak kılavuz ilkelere doğru"***[115] belgesinde önemli ölçüde güncellenmiştir.

5.1.1 Bağımsız Veri Tutanlar ile Kolluk Kuvvetleri Arasındaki İşbirliğinin Teşvik Edilmesi

Suçluları tespit etmek için veri tabanlarını kullanmak, ceza hukuku sistemi içinde yerleşik bir süreçtir. Parmak izi ve DNA veritabanları, birçok yargı bölgesinde cezai soruşturmanın temel dayanakları haline gelmiştir. Bununla birlikte, elektronik delillerle ilgili veri tabanlarının kolluk kuvvetlerine veya devlet kurumlarına ait olması pek muh-

[113] Yargılama yetkisi konusunda bkz. Bölüm 8.

[114] https://www.coe.int/en/web/cybercrime/lea-/-isp-cooperation

[115] https://rm.coe.int/2088-33-law-enforcement-isp-guidelines-2020/1680a091a7

temel değildir. Elektronik delillere ilişkin veritabanları, interneti oluşturan çok sayıda özel şirket genelinde yayılmış durumdadır. Bu da, özel şirketler ile ilişki kurmanın ve işbirliğinin son derece önemli olduğu anlamına gelmektedir. Ancak, ISP'ler tarafından tutulan müşteri tanımlayıcı bilgiler hakkında merkezi bilgi eksikliği, bilgi alışverişine yönelik standartlar oluşturmayı zorlaştırmaktadır. Bu şirketlerin her birinin ağları üzerindeki suç faaliyetleri ile başa çıkmak, istenen verileri korumak ve aldıkları koruma taleplerini önceliklendirmek için kendilerine has yöntemleri vardır.

Bağımsız veri tutan tarafla doğrudan düzenli diyalog kurmak, yanlış anlamaların önlenmesi açısından yardımcı olabilir ve hangi taleplerin acil ve hangilerinin daha düşük önceliğe sahip olduğu konusunda yönlendirme sağlayabilir ve ayrıca bir işbirliği kültürünün geliştirilmesine de yardımcı olabilir. İşbirliğine dayalı bir diyalog, bir suça tanık olan hizmet sağlayıcıları da kolluk kuvvetleriyle temasa geçip suçu ihbar etmeye teşvik edebilir.

Avrupa Konseyi'nin ***Bilişim suçlarına karşı kolluk kuvvetleri ve internet hizmet sağlayıcıları arasındaki işbirliğine ilişkin Kılavuz İlkeleri*** ile birlikte daha yeni olan "***Bilişim suçlarına karşı kolluk kuvvetleri ve internet hizmet sağlayıcıları arasındaki işbirliği: Ortak kılavuz ilkelere doğru***", işbirliğinin nasıl teşvik edileceğine ilişkin bir dizi öneri sunmaktadır. Öneriler, talep ve yanıtlar sunulurken standart biçimlerin kullanılmasını ve bilgi alışverişini kolaylaştırmak için tek başvuru noktalarının belirlenmesini içerir. Kılavuz İlkeler ayrıca her iki tarafın da taleplerin nasıl işleme konulacağını ve yönetileceğini düzenleyen yazılı prosedürler hazırlamasını önermektedir. Bu prosedürler, verilerin muhafaza ve elde edilme şekline güven duyulmasını sağlayabilir ve veri sahiplerinin insan haklarının ve gizlilik beklentilerinin korunmasını sağlayabilir.

Kılavuz İlkeler ayrıca kolluk kuvvetleri ile ISP'ler ve diğer üçüncü taraf veri tutanlar arasında düzenli toplantılar yapılmasını önerir. Bu, hem işbirliğine ilişkin zorlukların, hem de ortaya çıkan trendlerin ve tehditlerin, stratejik ve ileriye dönük bir şekilde tartışıldığı bir toplantı olabilir. İşbirliği aynı zamanda kolluk kuvvetleri ile özel sektör arasında ortak eğitim de içerebilir. Bu tür bir eğitim, önyargıları ortadan kaldırmaya ve katılımcılar arasında bir güven ortamı oluşturmaya yardımcı olabilir.

5.1.2 Verilerin Korunması

Bir yargı bölgesinde yürürlüğe giren bir usul hukuku (örneğin İnternet Hizmet Sağlayıcıdan bilgi istenen ibraz talimatları, resmi talepler veya mahkeme celpleri) başka bir yargı bölgesinde infaz edilebilir olmayacaktır. Yabancı bir ISP'den delil almak için, bir talebin Bölüm 8'de açıklandığı gibi onaylı bir karşılıklı adli yardım sürecinden geçmesi gerekir. Bu, zaman alabilir ve verileri tutan taraf (hizmet sağlayıcı) söz konusu talebi aldığında, istenen bu tür verilerin artık erişilebilir olmama riski bulunmaktadır. İletişim hizmeti sağlayıcılar, trafik verilerini süresiz olarak saklamazlar ve normalde bu tür verileri faturalandırma amacıyla gerekenden daha uzun süre saklamazlar.

Bunu önlemeye yönelik veri saklama mevzuatının bir örneği, 2006/24/EC sayılı Avrupa Birliği Direktifidir. Bu Direktif, elektronik iletişim sağlayıcıların iletişim trafiği verilerini saklayacağı süreyi uyumlaştırma amacı taşımaktadır.[116] Direktif, Üye Devletlerin hizmet sağlayıcıların verileri 6 aydan az ve 24 aydan fazla olmamak kaydıyla saklama-

[116] yani, söz konusu iletişimin içeriği değil, veri iletişimi ile ilgili veriler.

larına yönelik mevzuat düzenlemelerini gerektirmektedir. Ancak, Nisan 2014'te Avrupa Adalet Divanı, İrlanda ve Avusturya'dan çıkar grupları tarafından açılan bir davada, Direktifin uygulanması bakımından orantısız olduğuna ve bu nedenle temel haklarla bağdaşmadığına karar vermiştir. Bu nedenle Direktif yürürlükten kaldırılmıştır. O tarihten beri, veri saklama doktrini Avrupa Birliği içinde gözden geçirilmektedir. Birleşik Krallık, bu tür verilerin muhafaza edilmesini sağlamak için derhal acil durum yenileme yasasını yürürlüğe koymuştur. Diğer AB Üyesi Devletler bu hususta daha sessiz kalmışlardır.

İnternet ile ilgili herhangi bir soruşturma için, trafik verileri bir elektronik iletişimi fiziksel olarak bir kişiye bağlayan yegane delil olabilir. Veriler, müfettiş talep etmeden önce silinirse, bu bağlantı sonsuza dek kaybolur. Ne yazık ki, bir soruşturmanın başlatılması uzun zaman alabilir ve soruşturmanın (izini gizlemiş olması muhtemel) bir suçlu tarafından kullanılan internet kaynaklarını belirlemesi daha da uzun sürebilir. Uluslararası yardım talepleri için geleneksel diplomatik kanallar da önemli ölçüde uzun zaman alabilir ve bir talebin ilgili hizmet sağlayıcıya zamanında iletilmesini engelleyebilir.

Bu nedenle Budapeşte Sözleşmesi'nin 16. Maddesi, Sözleşme taraflarının, bir mahkeme emri alınmadan önce bile bilgisayar verilerinin korunmasını talep etmesine izin vermektedir. Trafik verileri ile ilgili 17. Madde, verilerin hızlıca korunmasını talep etme prosedürü oluşturmanın yanı sıra, bir yetkili makamın, "Sözleşme Tarafının hizmet sağlayıcıları ve iletişimin aktarıldığı yolu belirlemesini sağlamak için" "hızlı bir şekilde" yeterli trafik verisini ifşa etmesine de imkan tanır. Sözleşme Taraflarından biri, diğer bir Tarafa, Budapeşte Sözleşmesinin 35. Maddesi uyarınca oluşturulan 7/24 iletişim ağını kullanarak trafik verilerinin ve içerik verilerinin korunması için talepte bulunabilir.

Verilerin korunmasına ilişkin bir talepte bulunurken, bir müfettişin ayrıca hem verilerin korunduğuna dair onay, hem de depolanan veriler için bir referans numarası talep etmesi önerilir.

Budapeşte Sözleşmesi Tarafları için 7/24 iletişim noktası ağını kullanmaları zorunlu değildir. Nitekim, İSP'ler ve Kolluk Kuvvetleri Yetkilileri arasındaki doğrudan işbirliği, potansiyel olarak daha esnek olabilir ve ilgili ihtiyaçlarının ve kısıtlamalarının daha iyi anlaşılmasına yol açabilir.

5.2 Bilişim Suçları ile İlgili İhbarların Alınması

Birçok durumda, bir internet suçunun mağduru, verilerinin yasa dışı olarak kopyalandığını, çalınan veriler suçlu tarafından gerçek dünyada kullanılmaya başlayıncaya kadar bilemez. Aslında mağdurlar verilerinin çalındığını asla da bilemeyebilirler. Mağdur olduklarını bilmiyorlarsa, asla ihbar etmeyeceklerdir; kolluk kuvvetleri de suçu asla kaydetmeyecek ve bu suç resmi istatistiklerde asla görünmeyecektir. Bilişim suçlarının büyük oranda ihbar edilmediğine inanılmaktadır.

Kolluk kuvvetleri için bir başka zorluk da, internette izlenebilecek nispeten az halka açık alan olmasıdır. Çoğu internet iletişimi, (gerçek dünyada da olduğu gibi) özel olarak, özel kişiler arasında, müstakil alanda gerçekleşmektedir. Mahkemeden özel izin alınmadan, kolluk kuvvetleri sadece halka açık web sayfalarında yayınlanan küçük miktardaki internet içeriğini izleyebilir.

İnternet üzerinden işlenen suçlar büyük ölçüde görünmez olduğundan, kolluk kuvvetleri daha çok şüpheli faaliyetler ile ilgili olarak üçüncü taraflardan gelen ihbarlara ihtiyaç duymaktadır. Mağdur ve tanık ihbarlarına ilişkin aşağıdaki bölümler, kolluk kuvvetlerinin suçları tespit etmesine yardımcı olmak üzere elektronik delillerin nasıl toplanabileceğini açıklamaktadır.

Elektronik delillerle doğrulanmış güvenilir ihbarların alınması, kolluk kuvvetlerine, bilişim suçlarını bir olgu olarak anlamaları, ortaya çıkan trendleri ve gelişen tehditleri belirlemeleri ve ayrıca topluma en çok zararı veren bu uygulama yöntemine odaklanmaları bakımından stratejik düzeyde yardımcı olabilir. Üçüncü taraflardan gelen ihbarlar, ağlarının ve verilerinin ele geçirildiğinin farkında olmayan ticari şirketler için de değerli olabilir. Örneğin botnetler[117] söz konusu olduğunda, bir internet güvenlik şirketi gibi bir üçüncü taraf, virüslü IP adreslerinin bulunduğu bir liste ile birlikte ISP ile iletişime geçene kadar, birçok masum kullanıcı, suç ağı tarafından virüs yüklenerek makinelerinin köleleştirildiğini fark etmeyecektir.

Normalde, bilişim suçu mağdurları bir suçu, kayıplarının olması veya kendilerini kişisel olarak etkileyen bir tür zarara uğramaları durumunda bildireceklerdir. Fakat, bilişim suçu mağdurlarının bazıları, kayıplarının küçük olması, karışmak istememeleri, suç ihbarının kendilerini uzun süreli bürokrasiye bulaştıracağını düşündükleri ve/veya kolluk kuvvetlerinin suçluyu adalete teslim edebileceğine güvenleri olmadığı için bir suçu bildirmemeyi tercih edebilir.

Bir mağdur için önemsiz görünebilecek, ancak daha büyük bir suç ayak izine sahip olabilecek küçük sorunlara bir örnek, istenmeyen (spam) mesajlar olabilir. İstenmeyen e-postalar tüm yargı bölgelerinde yasa dışı değildir, ancak istenmeyen e-postaların yasa dışı olduğu bir ülkede bile, tek bir istenmeyen e-posta mesajı gören bir kullanıcı normal olarak onu gereksiz klasörüne ekleyecek ve unutacaktır. Kullanıcı, gönderilen ve organize suç faaliyetlerini desteklemek için kullanılan milyonlarca benzer mesajı düşünmez. Benzer şekilde, bir kullanıcının bilgisayarına, bir bilgisayar korsanının erişmesini sağlayan bir bilgisayar virüsü bulaşmış olabilir, ancak anti-virüs yazılımı bilgisayarı temizler temizlemez, söz konusu mağdur, suçu polise ihbar etmek zorunda hissetmeyebilir. Bütün bunlara rağmen, bu tür suçlardan mağdur olanlar, bilgi vermenin daha basit bir yolu olsaydı kolluk kuvvetlerine önemli bilgiler sağlayabilirlerdi.

2002 yılından bu yana Amerika Birleşik Devletleri Federal Ticaret Komisyonu (FTC), trendleri analiz edebilmesi ve istenmeyen posta önleme çabalarına daha etkili bir şekilde odaklanabilmesi için kullanıcıları, gelen her istenmeyen postayı spam@uce.gov e-posta adresine iletmeye davet etmektedir.

Bazı ulusal polis güçleri de internet tabanlı suçların ihbar edilmesi için kullanıcı dostu yöntemler kullanmaya başlamıştır. Europol, aşağıdakileri de içeren, farklı AB ülkelerindeki ihbar mekanizmaları hakkında iyi bir özet sunan bir web sitesi barındırmaktadır (https://www.europol.europa.eu/report-a-crime/report-cybercrime-online):

- Fransız ulusal polisi https://www.internet-signalement.gouv.fr/
- Fransız STK https://www.signal-spam.fr/en/

---

[117] Botnet, roBOT ve NETwork (ağ) kelimelerinin birleşmesinden meydana gelmektedir. Belirli bir virüsün bulaştığı, böylece bazı yasadışı internet faaliyetini sürdürmek için hepsi uzaktan kullanılabilen bilgisayarlardan oluşan bir ağı ifade etmektedir. Söz konusu bilgisayarlar, sahiplerinin bilgisi olmaksızın kullanılmaktadır.

- İtalyan Ulusal Polisi https://www.commissariatodips.it/
- Birleşik Krallık https://www.actionfraud.police.uk
- Amerika Birleşik Devletleri FBI İnternet Suçları Şikayet Merkezi https://www.ic3.gov/

Bu tür ihbar merkezlerinin acil durumların ihbar edilmesi için kullanılmadığına dikkat edilmelidir.

5.2.1 Bir Dava Oluşturmak Üzere Birkaç Mağdur İhbarının Harmanlanması

Yukarıda da açıklandığı gibi bir bilişim suçu, bir bireye sadece sınırlı bir maddi kayıp getirebilir, ancak bu münferit küçük miktarlar, suça karışan siber suçlular tarafından elde edilen toplam kazançları veya suçluların bir bütün olarak topluma verdiği zararı yansıtmamaktadır. Birlikte ele alınan birden fazla küçük vakanın analizi, ayrı görülen bir küçük suç için tahsis edilmeyen kaynakların ve soruşturma süresinin tahsis edilmesi için gerekçe teşkil edebilir. Nitekim, uluslararası bir yardım talebini işleme koymak için bile, bazı ülkeler bir dizi küçük suçu bir arada değerlendirirken, davanın asgari eşik kriterlerini daha kolay karşılamasını şart koşmaktadır.

Bilişim suçlarının hedefleri muhtemelen tüm dünyaya yayılmış olacağından, ihbarların da uluslararası düzeyde alınması ve derlenmesi faydalı olabilir. Europol, Avrupa Birliği kolluk kuvvetlerinin veri girebildiği bir trans-Avrupa soruşturma veritabanı oluşturmuştur. Benzer şekilde Inhope Vakfı (https://www.inhope.org/EN), Çocuğa Cinsel İstismar ve Sömürü Materyalleri barındırdığı bildirilen adreslerin bulunduğu bir küresel veritabanına sahiptir. Vakıf, kolluk kuvvetlerinin söz konusu içeriğin kaldırılmasını talep etmek ve daha fazla soruşturma yapmak için delil olarak kullanabileceği ortak ihbarları belirlemek üzere bağlı ihbar hatlarıyla işbirliği yapmaktadır.

Dünyanın her yerindeki kolluk kuvvetleri Interpol ile birlikte çalışabilir (https://www.interpol.int). Lyon şehrindeki Interpol Genel Merkezi, delil olarak kullanılabilecek bilinen çocuk istismarı görüntülerinden oluşan bir veri tabanı tutmaktadır. Interpol ile irtibat, her ülkede bulunan Ulusal Merkez Bürosu aracılığıyla kurulmalıdır.

İhbar merkezleri aynı zamanda kamu-özel sektör ortaklığı biçiminde de kurulabilir. Toplumun genelinden istenmeyen posta ihbarlarını toplayan ve derleyen Fransız derneği https://www.signal-spam.fr/en/ buna iyi bir örnektir. Signal-spam bulgularını sadece kolluk kuvvetlerine değil, aynı zamanda e-posta yönlendiricilerine de bildirmektedir. Bu, e-posta sağlayıcılara, hizmetlerinin kötüye kullanımından sorumlu olan kullanıcıların aboneliklerini iptal etme seçeneği sunmaktadır.

5.2.2 Bilişim Suçunun Tanıkları

Ağ operatörleri, bilgisayar ağlarındaki etkinliği izlerken bazen bir saldırının gerçekleşmekte olduğunu keşfedebilirler. E-posta barındırma hizmeti sağlayıcılar, belirli bir adrese giden veya belirli bir adresten gönderilen alışılmadık derecede fazla sayıda e-posta görebilirler. Yeni bir kötü amaçlı yazılım biçimini analiz eden bir anti-virüs yazılımı yayıncısı, bir botnet komuta ve kontrol merkezi olarak kullanılan bir bilgisayar sunucusu ile bir barındırma hizmeti sağlayıcısı tespit edebilir. Bunların hepsi bilişim

suçunun tanıklarıdır fakat suç davranışının nasıl veya kime bildirilmesi gerektiğini bilemeyebilirler.

Tanıkların suçu ihbar etmeleri için merkezi bir ihbar merkezine sahip olmak çok faydalı olabilir (ve yukarıda belirtilen mağdurlara yönelik merkez ile birleştirilebilir). Böyle bir ihbar merkezinin merkezi ve erişilebilir olması ve toplumun geneline doğru bir şekilde anlatılması gerekir.

ABD İnternet Suçları Şikayet Merkezi IC3 (https://www.ic3.gov/default.aspx), gerçek mağdurdan veya şikayetçi sahibi bir üçüncü taraftan çevrimiçi İnternet suçu şikayetleri almak için kurulmuştur. IC3; federal, eyalet, yerel ve uluslararası kolluk kuvvetlerinin yanı sıra düzenleyici kurumlar ile birlikte de çalışır ve bilgileri alır, geliştirir ve ardından soruşturmanın ve kovuşturmanın dikkatine sunar. Sektör temsilcileri (örneğin çevrimiçi perakendeciler, finans kurumları, internet servis sağlayıcıları ve paket teslimat sağlayıcıları) ile ittifaklar kurmuştur. IC3'e gönderilen şikayetler arasında, fikri mülkiyet haklarının çalınması, bilgisayara izinsiz giriş, ekonomik casusluk, çevrimiçi gasp ve uluslararası kara para aklama da dahil olmak üzere bir dizi bilişim suçu sayılabilir. Kimlik hırsızlığı, kimlik avı, istenmeyen posta, yeniden gönderme, açık artırma dolandırıcılığı, ödeme dolandırıcılığı, sahte mallar, romantizm dolandırıcılıkları ve malların teslim edilmemesi gibi çok sayıda dolandırıcılık planı da IC3'e ihbar edilmektedir.

Tanık bilgileri ve elektronik delil deposuna başka bir örnek, tanıkların kötü amaçlı faaliyet içeren web sayfalarını ihbar edebildiği https://www.malwareurl.com web sitesidir.

Bir ihbar merkezi, herkese açık olabileceği gibi, (https://portal.ops-trust.net web sitesi gibi) sadece üyelerle de sınırlandırılabilir. Hem kamuya açık ihbar merkezleri, hem de özel olanlar, operasyonel düzeyde olmasa da stratejik düzeyde kolluk kuvvetlerinin bilgilendirilmesine yardımcı olabilecek çok miktarda bilgi toplar.

Son olarak, ihbar merkezlerinin, bazı suç türleri için kullanıcıları ihbarda bulunmaya teşvik etmesi, fakat kendi soruşturmalarını yürütmekten veya aktif olarak kanuna aykırı materyalleri araştırmaktan caydırması gerektiği belirtilmelidir. Nitekim, çocuk istismarı görüntüleri gibi bazı durumlarda, bu tür materyalleri arama eyleminin kendisi de yasa dışı olabilir.

6 Delillerin Analiz Edilmesi

Önceki üç bölümde anlatıldığı gibi bir bilgisayar sisteminden delil elde edildikten sonra, soruşturmanın bir sonraki aşaması, ele geçirilen verilerden önemli unsurların çıkarılmasıdır. Burada kastedilen unsurlar, soruşturma içinde gerçeklerin belirlenmesiyle ilgili olan unsurlardır.

Bu bölümde; Adli Bilişim kavramı, adli incelemelerin temelini oluşturan süreç modeli, inceleme sırasında uyulması gereken ilkeler ve belirli görevleri yerine getirmek için kullanılan yaygın yöntemler anlatılacaktır. Ayrıca, adli bilişim uzmanları tarafından yaygın olarak kullanılan (sabit disk analizi, dijital fotoğraf analizi ve trafik günlüğü analizi gibi) dijital izlere ve delile dayalı analiz türlerine de daha yakından bakılacaktır.

Bölüm 1.7 içinde sıralanan, verilerin elde edilmesine yönelik ortak ilkeler, aynı zamanda analiz aşamasında da geçerlidir. Aslında, analiz sırasında veriler yasal delil olarak oluşturulacağı için burada daha da önemlidir.

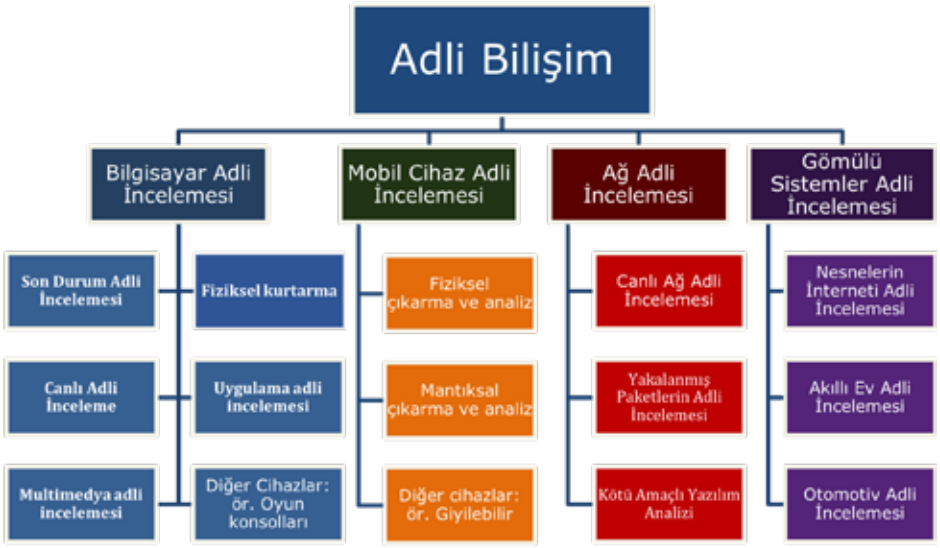
International Data Corporation (IDC) tarafından yapılan bir araştırma[118], 2025 yılında dünya çapında toplam 175 zeta bayt (175 trilyon gigabayt) verinin üretileceğini ve tüketileceğini tahmin ediyor. IDC araştırması, dünya çapındaki veri miktarının her iki yılda bir ikiye katlandığı ve bu verilerin çoğunlukla bilgisayar kullanıcısının etkinliklerine ilişkin kayıtlardan oluştuğu varsayımına dayalıdır. Bir soruşturmada bu tür veriler, kullanıcının etkinliğine ilişkin değerli bilgiler sağlayabilir. COVID-19'un neden olduğu ani veri artışı ve birçok kişi ve kuruluşun evden çalışması nedeniyle veri oluşturmaya ve depolamaya geçmesi göz önüne alındığında, bu rakamlar eksik değerlendirilmiş bile olabilir.

6.1 Adli Bilişim

Adli bilişim, bir bilgisayar sisteminde, dijital cihazda veya diğer depolama ortamlarında depolanan verileri elde etmeye, işlemeye, analiz etmeye ve sunmaya odaklanan adli bilim dalıdır.

Adli Bilişimin her bir dalı, kapsamlı bir eğitim ve deneyim gerektirir, bu da bir adli bilişim inceleme uzmanının tüm alanlarda uzman olmasını imkansız hale getirir. Aşağıdaki şema, Adli Bilişimin ana alt kategorilerini ve konu alanlarını göstermektedir:

[118] Seagate sponsorluğunda Kasım 2018'de yapılan "Veri Çağı 2025" başlıklı IDC araştırması, https://www.seagate.com/files/www-content/our-story/trends/files/idc-seagate-dataage-whitepaper.pdf adresinde bulunabilir.



Dört ana kategori bulunmaktadır:

1) **Bilgisayar Adli İncelemesi**, bu kategorilerin en eskisidir. Kişisel bilgisayarları, sunucuları ve depolama ortamlarını inceler. Bilgisayar Adli İncelemesinin dört alanı bulunmaktadır. Bunlar:

   - **Son Durum Adli İncelemesi** - elkoyma sırasında açık olmayan bilgisayar sistemlerinde saklanan verilerin nasıl elde edileceğini, işleneceğini, analiz edileceğini ve sunulacağını inceler. Bilgisayar adli incelemesinin en geleneksel alanıdır. Son durum adli incelemesi aynı zamanda geniş bir alan olan fiziksel disk kurtarmayı, dosya sistemi adli incelemesini ve diğer gelişmiş teknikleri de içerir.

   - **Canlı Adli İnceleme** - açık olan bir bilgisayar sisteminde bulunan verilerin nasıl elde edileceğini, işleneceğini, analiz edileceğini ve sunulacağını inceler. Olaylara Müdahale, bilgisayar sistemlerinde meydana gelen (örneğin güvenlik ihlalleri gibi) olaylar ve bunların nasıl önleneceği ve bunlara nasıl reaksiyon gösterileceği ile ilgili Canlı Adli İnceleme dalıdır. Artık çok fazla verinin geçici olarak, uzaktan veya şifreli olarak depolandığı veya olaylara müdahale durumunda çalışan sistemler acil müdahale gerektirdiği için giderek daha önemli hale gelen, Son Durum Adli İncelemesi ile karşılaştırıldığında nispeten yeni bir alandır.

   - **Multimedya adli incelemesi** - CCTV ve DVR sistemlerinden verilerin alınması ve analizinin yanı sıra video, ses ve resim dosyalarının (örneğin sahtecilik bakımından) derinlemesine analizini içerir.

   - **Fiziksel kurtarma** - hasar görmüş veya tahrip olmuş olabilecek depolama ortamının fiziksel olarak demonte edilmesini (örneğin disk kafalarının değiştirilmesini, parçalarına ayırmayı) içerir

   - **Uygulama adli incelemesi** - binlerce farklı uygulamanın (programın) bıraktığı izleri analiz etmeye odaklanan alandır.

   - Bilgisayar adli incelemesinin son alanı, dijital video kaydediciler, yönlendiriciler, oyun konsolları, banka/kredi kartı kopyalama cihazları ve daha birçokları gibi

diğer donanım cihazları ile ilgilidir. Bu cihazların birçoğu kendilerine ait dosya ve işletim sistemlerine sahiptir.

2) **Mobil Cihaz Adli İncelemesi** daha yeni bir adli inceleme alanıdır, ancak akıllı telefonlar ve tablet bilgisayarlar gibi mobil cihazların iş ve toplum hayatının genelinde kitlesel olarak benimsenmesiyle soruşturmalar için elzem hale gelmiştir. Bu kategorideki alanlar birçok farklı işletim sistemini yansıtmakla birlikte şu anda en popüler mobil cihaz işletim sistemleri Google Android ve Apple iOS'tur. Mobil cihaz adli incelemesinde uzmanlar, cihazların mantıksal, dosya sistemi ve fiziksel olarak alınmasını gerçekleştirir ve ardından içerikleri analiz eder.

Akıllı telefonların hızlı gelişimi ve 'veri çipi' düzeyinde şifreleme kullanan daha yeni işletim sistemleri ile birlikte, mobil cihaz adli incelemesi alanı önemli ölçüde daha çok vasıf gerektirir hale gelirken, cihazları doğru erişim bilgileriyle en uygun şekilde güvence altına alma gereksiniminin önemi ne kadar vurgulansa abartılmış olmaz.

3) **Ağ adli incelemesi**, kablosuz veya kablolu, internet veya yerel alan ağı (LAN) gibi bir ağ üzerinden iletilen elektronik deliller üzerinden yapılmaktadır. Canlı ağ adli incelemesinde müfettişler normalde bir ağ bağlantısını ele geçirirler ve veri akışlarını "anında" analiz etmeleri gerekir. "Yakalanmış paketlerin adli incelemesi" aşamasındayken, halihazırda kayıtlı ağ trafiğini içeren dosyaları analiz ederler. Kötü amaçlı yazılım analizi, davranış analizi ve tersine mühendislik de dahil olmak üzere kötü amaçlı yazılımların işlevselliğini analiz etmeye ve anlamaya odaklanmıştır.

4) **Gömülü sistemlerin** adli analizi, daha fazla IoT ve Akıllı ev/bahçe/vb. cihazlarının kullanılması nedeniyle daha popüler hale gelmektedir. Aynı zamanda çok geniş bir alan olan Otomotiv bilişim sistemleri adli incelemesini de içerir. Nesnelerin İnterneti adli incelemesi, bölüm 3.4.11 içinde açıklandığı gibi, gömülü cihazların birbirine bağlı sistemlerinin adli olarak elde edilmesine ve analizine odaklanan alandır. Otomotiv bilişim teknolojileri adli incelemesi, sadece iletişim verilerinin bir kısmı benzer olduğu için değil, aynı zamanda örneğin eğlence sistemleri için mobil işletim sistemi sürümlerini de kullandığından, mobil cihaz adli incelemesinin diğer alanlarıyla tipik olarak bazı örtüşmelere sahiptir. Mobil cihaz adli incelemesi ve bilgisayar adli incelemesi arasındaki sınırı aşan oldukça özel bir alan da anlık bellek adli incelemesidir. Bu alan, cihaza takılı bellek yongasının fiziksel olarak çıkarılmasına odaklanmakta ve bazı durumlarda, inceleme veya veri toplama için yonganın orijinal cihaza veya bir donör cihaza geri takılmasını gerektirmektedir.

6.2 Adli Bilişim Süreç Modeli

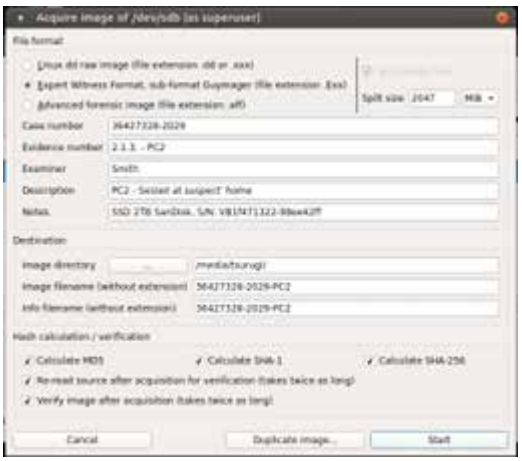
Adli bilişim ile ilgili bir durumda standart prosedür tipik olarak aşağıdaki adımlardan oluşur:

Bilgisayar adli incelemesi

Mobil cihaz adli incelemesi

İzolasyon: Mobil cihazların çok kendine has iletişimsel niteliği, bir ağa bağlı olmalarını çok muhtemel kıldığı için, çoğu cihaz uzaktan kilitleme ve silme işlevleri sunarken, bu cihazların bağlı oldukları ağlardan izolasyonlarının sağlanması ve muhafaza edilmesi çok önemlidir.

Elde etme: Dijital delilin tespit edilmesi, güvence altına alınması ve ardından da elde edilmesi gerekmektedir. Bu, bir ev araması sırasında geçici veriler toplayarak, ele geçirilen bir bilgisayardan bir şüphelinin diskini alarak veya bir soruşturma sırasındaki başka bir süreçte gerçekleşebilir. Geri dönüşü olmayan hataların yapılabileceği çok büyük bir uygulama kapsamı olduğu için, elde etme aşamasında doğru ve sağlam prosedürlerin uygulanması çok önemlidir. Delil zincirini sağlam tutmak, tüm adımları dikkatlice belgelemek ve elde edilen tüm görüntüleri ve kopyaları doğrulamak önemlidir.



Elde etme sürecinde, mümkün olduğunda, elkonulan herhangi bir dijital depolama içeriğinin tam bir kopyası veya "anlık görüntüsü"[119] üretilecektir. Veriler ancak güvenli ve emniyetli bir şekilde elde edildikten sonra işlenebilir. Anlık görüntü alma, dünya genelindeki adli bilişim laboratuvarlarında yaygın olarak kullanılan ve en iyi uygulama olarak kabul edilen bir süreçtir.

İşleme: **İşleme sırasında, adli bilişim inceleme uzmanları belirli cihazlara veya verilere öncelik verebilir (buna bazen ‹triyaj› da denir) ve kaydedilen verileri işlemek için mümkün olan her durumda muteber adli bilişim araçları kullanılır. ‹Anlık Görüntü› üzerinde çalışılarak (ve önemli gerekçeler olmadıkça asla orijinal üzerinde çalışılmadan), akıllı, duruma özel filtreler (Veri Madenciliği) uygulanabilir veya anlık görüntü işlenebilir (örneğin silinmiş dosyalar geri kurtarılabilir, veri depoları kurulabilir, şifreleme kırılabilir, internet geçmişi, sohbet günlükleri vb. gibi uygulama verileri analiz edilebilir).**

[119] İmaj (Anlık Görüntü), bir depolama ortamının detaylı bire bir kopyasıdır. Genellikle ayna kopya, ikiz görüntü veya veri akışı kopyası olarak adlandırılır. Bu "anlık görüntü"; canlı dosyalar, "boş alan", "kullanılmayan disk alanı" ve en önemlisi silinen veriler de dahil olmak üzere veri depolama ortamındaki her şeyi kaydeder.

Analiz: Analiz aşamasında incelemeyi yapan kişi, alınan anlık görüntüler üzerinde, vakanın gereksinimlerine ve gönderen müfettişin talimatına uygun olarak dijital deliller arar. Bu adım çok zaman alabilir ve çeşitli dosya sistemlerinden, işletim sistemlerinden ve uygulamalardan gelen izleri yorumlayabilmek için uzman bilgisi gerektirebilir.

İbraz**:** Analiz adımında deliller bulunduktan sonra, inceleme uzmanının müfettiş veya savcı için herhangi bir davada delil olarak sunabileceği bir rapor oluşturması gerekir. İnceleme uzmanının görevi, karmaşık teknik bağlamları hâkimlerin, savcıların ve ilgili diğer tarafların kolayca anlayabileceği olgularla göstermek ve açıklamaktır. Ayrıca, duruşmalarda bir "uzman" olarak kabul edilirlerse, bu olguları yorumlamaları ve anlamları hakkında bir görüş bildirmeleri de beklenebilir.

6.3 Elektronik Delillerin Analiz Edilmesine İlişkin Ortak İlkeler

Ortak ilkeler, elektronik delilin bütünlüğünü koruyacak bir şekilde ve doğrulanabilir bir yöntemle elde edilmesini sağlamaya yardımcı olur.

Bilgisayarlar modern yaşamın ayrılmaz bir parçası haline geldiğinden, artık yalnızca ticari faaliyetler için kullanılmamakta, kullanıcıyla ilgili özel ayrıntıları ortaya çıkarabilecek her türlü kişisel bilgiyi içermektedir. Bunun sonucu olarak, yasal zorluklara ve temel hak sorunlarına yol açabilecek özel, gizli veya yasal olarak ayrıcalıklı bilgilerin er ya da geç açığa çıkması muhtemeldir.[120] Bu tür sorunlar ortaya çıkarsa, anında çözüme kavuşturulması kolay olmayacaktır, ancak bu tür bir zorluk nedeniyle verileri göz ardı etmek de akıllıca olmaz. İtiraz etmek yanlış olabilir. Bir çözüm, verilere elkoymak, ancak yasal durum çözülene kadar bir mübaşir veya icra memuru ile mühür altında tutmaktır. Nitekim, verilerin mühür altına alınması, gerçekten gizli olsalar bile verilere erişim yetkisi elde etmek için zaman tanıyabilir. Bu, bölüm 6.3.5 içinde daha ayrıntılı olarak açıklanmaktadır.

6.3.1 Veri Bütünlüğü

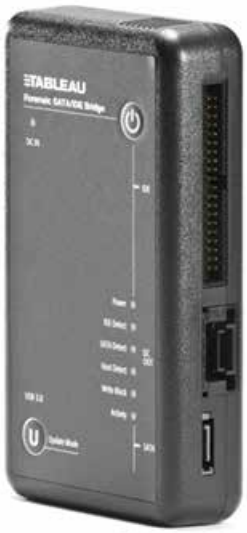
Delillerin bozulmadan, orijinal durumuna mümkün olduğunca yakın ve virüsten arındırılmış olarak korunması gerektiği için, bir bilgisayar cihazının analiz edilmesi, müfettişin fiziksel olay yeri incelemesine benzer.

Benzer şekilde, adli bilişim analistleri, adli laboratuvarda inceledikleri elektronik verilerin hiçbirini değiştirmemeye dikkat etmelidir. Bir cihaza uygulanan en ufak bir işlem bile belleğinin içeriğini değiştirebilir. Sadece bir dosya dizininin içeriğini listelemek veya bir dosyayı açmak bile dosyanın "son erişim tarihi" kaydını değiştirebilir. İçerdiği veriler üzerinde çalışmadan önce ilk fırsatta adli bir anlık görüntü oluşturmanın temel sebebi budur.

Adli anlık görüntülerin çeşitli biçimleri vardır, ancak kullanılan başlıcaları DD (İşlenmemiş) görüntüler ve E01 (Gömülü) görüntülerdir. Her ikisi de geçerli olduğu ve adli bakımdan sağlam kabul edildiği için hangisinin kullanıldığı önemsizdir. Ulusal Teknoloji Standartları Enstitüsü (NIST) adlı bir ABD kuruluşu, anlık görüntü araçlarının ne

[120] Özellikle özel hayata ve aile hayatına saygı hakkı, Avrupa İnsan Hakları Sözleşmesinin 8. Maddesi

yapması gerektiğini ve kullanıldığında hangi görevleri yerine getirmesi gerektiğini tanımlar ve bu anlık görüntü türlerinin her ikisi de tam olarak gerekeni yapmaktadır.



Elkonulan verilerde değişiklikten kaçınmanın temel yollarından biri, bir yazma engelleme cihazı kullanmaktır. Bir dizi farklı yazma engelleme donanımı mevcuttur - solda bunlardan birinin resmi gösterilmektedir. Bu cihazın amacı, şüphelinin depolama ortamı (sabit disk sürücüsü, USB sürücüsü, vb.) ile adli bilişim analistinin bilgisayarı arasında durmak ve anlık görüntü alma işlemi gerçekleşirken yazma girişimlerini önlemektir. Bu, orijinal verilerin bütünlüğünü korur.

Anlık görüntü oluşturulduktan sonra, orijinal cihazın bir çalışma ortamında yeniden açılması için çok az neden vardır.

Bazen farklı koşullarda kullanılan 'yazma engelleyici' yazılımlar vardır ve adli bilişimde kullanılan belirli işletim sistemleri, şüpheli cihazların 'salt okunur' moduna alınmasına imkan tanır ve benzer şekilde orijinal cihaza yazma işlemlerini de durdurur. Veri bütünlüğü ve orijinal verilerin değişmesini önlemeden çıkarılacak ana fikir, değişikliğin neredeyse kaçınılmaz olduğu durumlarda cihazın normal şekilde çalıştırılmaması gerektiğidir.

Daha önce bölüm 4.4.11 içinde adresleme (hashing) konusu anlatılmıştı. Adresleme, birçok adli bilişim sürecinde ve kesinlikle bir depolama ortamının anlık görüntüsünün alınması sürecinde önemli bir rol oynar. Adresleme, adli bilişimde iki temel amaç için kullanılmaktadır - verilerin doğrulanması (adresleme sırasında ve sonrasında) ve aynı zamanda verilerin tespit edilmesi. İkinci amaç burada alakalı değildir, ancak kısa bir açıklama olarak, herhangi bir miktardaki veri (bir karakter, ad, sabit sürücü veya daha da önemlisi bir dosya) adreslenebilir. Dosyalar, adresleme değerleri (veya dijital parmak izleri) bilinerek ve daha sonra aynı dosyalar için adli inceleme araçları içinde bu değerler kullanılıp aranarak bulunabilirler. Bu teknik bu kılavuzun kapsamı dışındadır ancak adli bilişimde sıklıkla kullanılan bir tekniktir.

Anlık görüntü alma sürecinin bir parçası olarak, her orijinal verinin adres değeri hesaplanır ve adli inceleme süreci boyunca onunla birlikte saklanır. Günümüzde adli bilişimde iki farklı adresleme algoritması saklanmaktadır ve bunlar önceki bölümde bahsedilenlerin aynısıdır – MD5 ve SHA1. SHA256 veya SHA512 gibi başka algoritmalar da vardır ve gelecekte adli inceleme sürecinde kullanılır hale gelebilirler.

Adresleme kullanmanın amacı çok basittir. Orijinal veri için bir adres hesaplanırsa ve bu adreste en ufak bir değişiklik olursa (disk seviyesinde bir karakterlik hatta bir bitlik veri), adresleme işlemi tekrarlandığında adres tamamen farklı olacaktır. Bu da önemlidir, çünkü böylece savcılık başta ellerine geçen verilerin değiştirilmemiş olduklarını kategorik (kesin) olarak ifade edebilir. Adresleme, bu nedenle adli bilişimde bir doğrulama aracı olarak kullanılır çünkü orijinal görüntü müfettişler ve kuruluşlar arasında paylaşıldığında veya kovuşturma veya mahkeme sürecine taşındığında da bu tür bir değişiklik çok kolay tespit edilebilir. Anlık görüntünün kopyasını alan herkes, her adımda bütünlüğünü kontrol etmelidir; eşleşen adresler veriye güvenilebileceği anlamına gelir.

Son olarak, veri bütünlüğü ilkesinin bir parçası olarak, deneyimli bir inceleme uzmanı, delil karartma teknikleri kullanılma olasılığına karşı her zaman tetikte olmalıdır. Gerçek göründüğünden ve kolluk kuvvetleri tarafından elkonulmadan önce değiştirilmiş veya tahrif edilmiş olabileceğini düşündüren herhangi bir özellik sergilemediğinden emin olmak için verileri incelemelidirler. Delil karartma tekniklerine ilişkin bilgiler, her zaman adli bilişim inceleme uzmanının eğitim müfredatının bir parçası olmalıdır.

6.3.2 Denetim İzi

Özel bir şirketin sunucusunun saldırıya uğradığı ve çalışan bilgileri de dahil olmak üzere tüm verilerin kopyalanmış olduğu senaryoyu hayal edin. Sunucu üzerindeki soruşturmalar, bilgisayar korsanlığının komşu bir kasabadaki bir konut interneti bağlantısından kaynaklandığını gösteriyor. Saldırının yapıldığı evin sakini olan şüpheli, masum olduğunu ve failin muhtemelen evdeki bilgisayarını ele geçirdiğini ve şirket sunucusunu uzaktan ele geçirmek için onu kullandığını iddia ediyor. Bulmacayı daha da karmaşık hale getiren şey, şüphelinin bir sunucuyu ele geçirmek için gerekli bilgiye sahip olabilecek bir bilgisayar bölümü mezunu olmasıdır.

Her karmaşık soruşturmada, düzgün kayıt tutulması ve bu kayıtların indekslenmesi gereklidir. Bu, sadece durumu anlamaya ve yeni sorgu hatları oluşturmaya yardımcı olmakla kalmaz, aynı zamanda daha sonra incelenebilecek ve araştırma sürecini doğrulamak için kullanılabilecek bir denetim izi de sağlar. Sunucuda ve şüphelinin bilgisayarında yapılan tüm soruşturmalar, soruşturma prosedürü boyunca dikkatlice kaydedilmelidir. Bu kayıtlar, inceleme uzmanının delillere metodik olarak yaklaşmasına ve boşlukları daha kolay tespit etmesine yardımcı olacaktır. Denetim izi, tüm makul sorgulama hatlarının takip edildiğini ve bir şüphelinin alternatif hesabının soruşturulduğunu ve hiçe sayıldığını göstermek için de yeterli olmalıdır. Söz konusu senaryoda bu, evdeki bilgisayarının bilinmeyen bir tarafça saldırıya uğramadığını göstermeyi içerecektir.

Birçok analist, analizlerini belgelemek ve gerekli tüm işlemleri ve incelemeleri yaptıklarından emin olmak için standart formlar veya kontrol listeleri kullanır. Soruşturma boyunca, belirli işlemlere (veya yapılmayan işlemlere) ilişkin bulgulara, sonuçlara ve gerekçelere ilişkin eşzamanlı notlar tutulmalıdır. Varsa zaman damgaları bu tür notların doğrulanmasına yardımcı olabilir.

Elbette söz konusu dokümantasyon, düzgün bir şekilde etiketlenmeleri ve doğrulanmaları koşuluyla ekran görüntüleri, fotoğraflar ve video kayıtları da içerebilir.

6.3.3 Uzman Desteği

Daha önce de açıklandığı gibi, elektronik delillerin teknik niteliği, nereye bakılacağını ve delil niteliğindeki verilerin nasıl alınacağını bilen uzmanların kullanılmasını gerektirmektedir. Davanın koşulları, canlı adli bilişim, kötü amaçlı yazılımların tersine mühendisliği veya hasarlı bilgisayar sistemlerinden veri kurtarma gibi konularla ilgili belirli becerileri içerebilecek olan gereken uzmanlık türlerini belirleyecektir. Ancak, uzmanın beceri ve deneyim düzeyi ne olursa olsun, yeterli kaynak ve donanım olmadan bu becerileri kullanması mümkün olmayacaktır.

Bu kaynaklar, belirli muayeneleri otomatikleştirmek için uygun yazılım araçlarıyla donatılmış tam donanımlı bir adli bilişim laboratuvarına, cihazların anlık görüntülerini almaya yönelik tesislere, bir Faraday kafesi ile korunan iklim kontrollü bir odada güvenli depolamaya ve bölüm 3.1 içinde listelenen türde yardımcı ekipmanlara erişimi içerebilir.

6.3.4 Uygun Eğitim

Her meslekte olduğu gibi, adli bilişim uzmanının da bilgilerini güncel tutması ve alanındaki yeni gelişmelerden haberdar olması gerekir. Bu, sürekli mesleki eğitim ve yetkinlik çerçevelerinin düzenli olarak yeniden değerlendirilmesi anlamına gelir. Bilgisayar adli incelemesi dünyası, bilgisayar teknolojisiyle aynı hızda ilerlemektedir ve bir yıl önce kullanılan adli bilişim prosedürleri halihazırda güncelliğini yitirmiş olabilir.

Bazı durumlarda, uygun beceri seviyeleri resmi eğitim ve sertifikalar aracılığıyla ölçülebilir ve değerlendirilebilir. Ulusal düzeyde verilen kurumlar arası bir eğitim çerçevesinin bir takım avantajları olabilir ve bu eğitim uluslararası iyi uygulamalar ile uyumlu hale getirilmelidir.

Adli inceleme uzmanları, en son teknikler ve gelişen trendler hakkında bilgi edinmek için diğer adli bilişim uzmanlarıyla bilgi ve deneyim alışverişinde bulunmaya ve akademi ve endüstri ile işbirliği geliştirmeye teşvik edilmelidir. Ülke düzeyinde ve uluslararası düzeyde düzenli toplantılar ve çalıştaylar ile bu teşvik edebilir.

Adli bilişim uzmanlarının yanı sıra, müfettişler, ilk müdahale ekipleri, hâkimler ve savcılar düzeyinde de kapasitenin geliştirilmesine gereksinim vardır. Bir dizi kapsamlı eğitim konsepti ve materyali ücretsiz olarak bulunabilir ve ulusal eğitim girişimlerini geliştirmek için birer şablon olarak kullanılabilir. Bunlar, aşağıdakileri içerir:

- GLACY ve Cybercrime@EAP projeleri kapsamında hazırlanan adli eğitim ve kolluk eğitimi stratejilerine ilişkin raporlar;

  https://www.coe.int/en/web/cybercrime/all-reports

- Doğu Ortaklığı bölgesi içindeki bilişim suçları ve siber güvenlik stratejileri ile ilgili olarak 2019 yılında yayınlanan raporlar;

  https://www.coe.int/en/web/cybercrime/all-reports

- Avrupa Konseyi tarafından kendi kapasite geliştirme programları çerçevesinde geliştirilen aşağıdaki kılavuzlar:
  - Dijital Delillerin Toplanmasına, Analiz Edilmesine ve Sunumuna Yönelik Standart Uygulama Usulleri;
  - Adli bilişim laboratuvarının yönetimine ve prosedürlerine ilişkin temel bir kılavuz;
  - Kripto Para Müsadere Kılavuzu;
  - Bilişim Suçları Soruşturmalarına İlk Müdahale Ekipleri için Kılavuz;
  - ve eklerine farklı dillerde aşağıdaki adresten erişebilirsiniz:

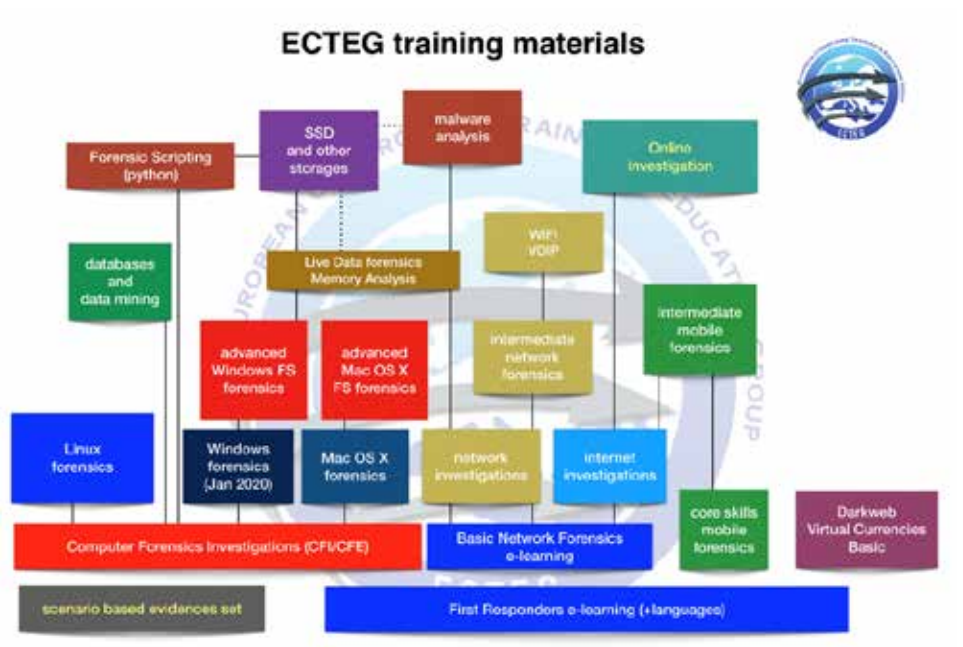
https://www.coe.int/en/web/octopus/training

- Avrupa Konseyi tarafından kendi kapasite geliştirme programları çerçevesinde geliştirilen aşağıdaki eğitim kursları:
  - Bilişim Suçları, Dijital Delil ve Çevrimiçi Suç Gelirleri Giriş Seviyesi Eğitim Modülü;
  - Yargıya Giriş Eğitimi (Hâkim ve Savcılara Yönelik Bilişim Suçları/Dijital Deliller Konularına Giriş);
  - İleri adli eğitim (Hâkimler/savcılar için bilişim suçları/ elektronik deliller hakkında ilave düzeyde bilgi);
  - İlk Müdahale Ekipleri için Eğitim Paketi (İlk Müdahalecilere Yönelik Olarak Suç Mahallerinde Dijital Delil Sevk ve İdare Eğitimi);
  - Çevrimiçi Suç Gelirleri Arama, Zabıt ve El Koyma Temel Eğitimi (Hâkim ve Savcılara Yönelik Eğitim);
  - Çevrimiçi Suç Gelirleri Arama, Zabıt ve El Koyma Temel Eğitimi (Kendi Kendine Eğitim El Kitabı);

https://www.coe.int/en/web/octopus/training

Bu belgeler www.coe.int/cybercrime adresinde mevcuttur.

Bilgisayar adli incelemesi konuları hakkındaki eğitim materyalleri için bir başka mükemmel kaynak da Avrupa Bilişim Suçları Eğitim ve Öğretim Grubu'dur (ECTEG). Kurs paketleri; öğrenci kılavuzları, eğitmen kılavuzları, ders planları, slaytlar ve (resimler gibi) diğer öğretim materyallerini içerir. ECTEG, bu kursları sadece kolluk kuvvetlerine ve ücretsiz olarak sağlamaktadır. Bu kılavuz yazılırken aşağıdaki kurslar verilmekteydi:



Mevcut kurslar https://www.ecteg.eu/course-packages/ adresinde güncellenmektedir.

Aynı zamanda bazı bilgisayar donanımı ve yazılımı şirketleri de adli bilişim ürünleri hakkında ek bilgi ve eğitim sağlayabilmektedir. Adli bilişim çalışma ortamı genelinde bir tür standardizasyona başvurmaya yönelik bir hareketle, mahkemelere delil hazırlamak ve sunmak için kullanılan bu ticari araçların kullanımında bireylerin sertifikalandırılmasını düşünmek gittikçe daha önemli hale gelmektedir.

Özel sektör ayrıca, sundukları ticari araçları esas alan, ürünlerinin adli bilişim yeteneklerini açıklayan destek forumları sağlamak suretiyle kolluk kuvvetlerine yardımcı olma rolünü de oynamıştır. Ayrıca, hem sadece kolluk kuvvetlerine açık olan hem de benzer düşünen profesyonellerin bilgi ve deneyimlerini paylaştığı başka birçok forum da vardır.

6.3.5 Hukuka Uygunluk

Yukarıda bölüm 6.3 içinde de açıklandığı gibi, insanlar giderek daha fazla kişisel ve gizli veriyi bilgisayarlarında ve akıllı telefonlarında saklamaktadır. Bir bireyin bilgisayar sisteminde yapılan her inceleme, kimi zaman alakasız, gizli ve muhtemelen yasal ayrıcalığa tabi olan özel verileri açığa çıkaracaktır. Müfettişlerin bu tür verilere izinsiz giriş yapma veya erişme niyeti olmasa da, bunlar her zaman kişisel olarak işaretlenmiş olmaz ve gizli bilgilerin nerede başlayıp nerede bittiğine karar vermek de her zaman mümkün olmayabilir. Aynı e-posta klasörü içinde, soruşturma ile alakalı olan e-postalar olabileceği gibi, bazıları yasal olarak korunan ve soruşturma içinde hiçbir rolü olmayan başka birçok e-posta olabilir.

Bazı yargı bölgelerinde, bir müfettiş soruşturma kapsamı dışında kişisel verilere rastlarsa, derhal bu verileri görüntülemeyi bırakması ve kişisel olarak ve gelecekte değerlendirilecek ve karar verilecek veriler biçiminde işaretlemesi gereklidir. Fakat suçluların, adli bilişim uzmanını yanıltmak ve aşılması gereken engeller yaratmak için verileri kişisel olarak etiketlenmiş bir klasörde gizledikleri bilinmektedir.

İhtilaflı verilerin mahkeme mührü altına alınması ve statüsünün bir mahkeme kararı ile belirlenmesi suretiyle saklanması olasılığını daha önce açıklamıştık.

6.4 Dijital İzler

Nasıl bir suçlu bir suç mahallinde fiziksel izler bırakırsa, bir suçu bilgisayar aracılığıyla işleyen suçlu da "dijital suç mahallinde" izler bırakacaktır. Locard'ın adli inceleme yasası, suç mahalline giren kişinin oraya bir şey getireceğini ve oradan bir şey alarak terk edeceğini söyler. Bu, bilgisayarlar için de aynen geçerlidir.

Bir inceleme uzmanının adli analiz sırasında keşfedebileceği dijital iz türleri hakkında daha iyi bir fikir edinmek için iki tür dijital iz arasında ayrım yapmak anlamlı olacaktır:

Önlenebilir izler: Bunlar, işletim sistemi ve uygulamalar tarafından kendiliğinden depolanan ancak sistemin saklamamak üzere yapılandırılabileceği izlerdir. Örnek olarak bir web tarayıcısını düşünelim. Bu yazılım, bir şüphelinin tarama geçmişinin yanı sıra indirmelerine ilişkin ayrıntıları, form girdilerini, çerezlerini (tanımlama bilgilerini) vb. saklayacaktır, fakat şüpheli tarafından devre dışı bırakılabilir veya silinebilir. Diğer bir örnek, "Başlat" menüsü ve şüphelinin yakın zamanda hangi dosyaları açtığını "hatır-

layan" Office programları olabilir. Bu şekilde (aşağıdaki tabloda gösterildiği gibi) sabit diskte otomatik olarak depolanan çeşitli türde 'önlenebilir' izler vardır. Ancak, nasıl yapılacağını bilen biri tarafından bu izler önlenebilir.

Kaçınılmaz izler: Buna karşılık elbette devre dışı bırakılamayan veya geçici olarak durdurulması büyük çaba gerektiren kaçınılmaz izler de vardır. Buna bağlı olarak, bir şüpheli izlerini kapatmaya çalışsa bile, bu tür izleri bulma olasılığı da yüksektir.

Aşağıdaki tabloda, önlenebilir ve kaçınılamaz izlere ilişkin bazı örnekler listelenmektedir:

Önlenebilir İzler	Kaçınılmaz İzler
Küçük Resim Önbellekleri	Bellek Boşluğu
En Son Kullanılan (MRU) Listeleri	Ayrılmamış Alan
Günlük dosyaları	Kullanılmayan Disk Alanı
Tarayıcı Geçmişleri	MFT (Yönetilen Dosya Transferi) Kayıtları
Tarayıcı Önbellekleri	RAM
En Sık Kullanılan Programlar	Bazı uygulama izleri
Form Verileri	
Pagefile.sys	
Hiberfil.sys	
Birim Gölge Kopyaları	
…	

6.5 Adli Analiz Türleri

Bu bölümde adli analiz türlerine örnekler verilecektir. İlgili zorluklar hakkında içgörü sağlanacak, ama aynı zamanda adli analizin sahip olabileceği delil değeri de gösterilecektir.

6.5.1 Dosya Sistemi Analizi

Veri depolama aygıtları, bilgileri ikili[121] biçimde saklamaktadır, yani bilgisayar belleğini oluşturan küçük yapı taşları sıfırlar veya birler biçiminde saklanır (bazen açık veya kapalı veya [+] veya [-] olarak da ifade edilir). Bu en küçük bilgi işleme durumlarına "bit" denir, bunlar "baytlar" içinde gruplandırılır ve bu nedenle kilobayt, megabayt, gigabayt vb. şeklinde bir terminoloji ile karşılaşırız. Bilgisayar sisteminin hangisinin hangisi ile gittiğini bilmesi için, bitleri/baytları/kilobaytları bir metodla yapılandırmak amacıyla bilgisayar mühendisleri 'dosya sistemleri' geliştirmişlerdir. Dosya sistemi, (kitapların olduğu) bir analog kütüphanede bulunan eski moda basılı kopya dizin kartlarının bulunduğu çekmeceler olarak düşünülebilir. Kartlar, "indekslenir" veya (belki yazara, başlığa veya konuya göre) sıralanır ve bina içindeki konumlar ile çapraz referanslandırılır. Her kart, ilgili olduğu kitabın hangi koridorda, hangi kitaplığa ve rafa yerleştirildiğini gösterir. Aynı şekilde bir dosya sistemi de bilgisayar dosyalarının bir cihazda depolanmasına ve geri çağırılmasına imkan tanır.

[121] Yaygın olarak kullandığımız sayısal sistem onluk temeldedir. İkili sistemler ise ikilik temeldedir.

Veri depolama aygıtları, "bölümler" adı verilen alanlara bölünebilir ve veri depolamak için kullanılacaksa, her bölümün kendisi için geçerli bir dosya sistemine sahip olması gerekir. Bir sabit diskin bölümlendirilmesi, kütüphane binasının daha küçük iki ayrı kütüphane oluşturmak üzere yeni bir iç duvarla bölünmesine benzer. Her mini kütüphanenin kendi dizin kartı sistemi olacaktır. Bir sabit disk iki bölüme ayrıldığında, bunlar iki farklı sürücü olarak görüntülenecektir. Windows içinde farklı sürücüler, C:\ sürücüsü ve D:\ sürücüsü gibi farklı alfabetik etiketler almaktadır.

Bir veri bölümünün birden fazla fiziksel sabit diski kapsaması da mümkündür (genellikle Bölüm 2.2'de açıklanan RAID[122] sistemi ile). Bu durumda, bilgisayar kullanıcısı yazılım arayüzünde sadece bir veri sürücüsü görür (örneğin C:\ sürücüsü), ancak gerçekte C sürücüsü iki veya daha fazla fiziksel sabit sürücüyü kapsamaktadır. Hepsini birbirine bağlayan şey, RAID denetleyicisidir (bu, RAID donanımı veya yazılımı olabilir) ve bir sabit diskin veya birden çok sabit diskin bir parçasını oluşturan dosya sistemi, işletim sistemine tek bir birim olarak görünür.

En yaygın dosya sistemleri NTFS (Yeni Teknoloji Dosya Sistemi) ve FAT'dir (Dosya Tahsis Tablosu). FAT sistemi 1980 yılında oluşturulmuş ve ilk kişisel bilgisayarlarda kullanılmıştır. Sağlam ve geniş ölçüde uyumlu olduğu için bugün hala kullanılmaktadır. Apple bilgisayarlar, Windows PC'ler, Linux ve diğer birçok yazılım FAT bölümlerini okuyabilmektedir.

Microsoft Windows NTFS dosya sistemini, mevcut Apple bilgisayarları APFS sistemini, Linux ise EXT, BTRFS, XFS veya ReiserFS gibi birkaç farklı dosya sistemini kullanmaktadır. Bir cihazı kopyalamak ve analiz etmek için, adli inceleme uzmanının o cihazda kaç bölüm olduğunu ve hangi dosya sisteminin kullanıldığını belirlemesi gerekir. İşletim sisteminin hemen tanımadığı, ancak bilgisayar kullanıcısının içeriğe erişmek için istediği zaman yükleyebileceği veya ekleyebileceği gizli bölümler de olabilir. HPA (Ana Makina Korunmuş Alanları) ve DCO (Cihaz Konfigürasyon Yaması) gibi sadece özel ATA[123] komutları ile açılabilen diğer gizli alanların mevcut olabileceği de göz önüne alınmalıdır.

6.5.2 Dosya Kurtarma

Kullanıcının dosyaları silip silmediğini görmek için Geri Dönüşüm Kutusu her zaman kontrol edilmeye değer. Bu klasördeki yasa dışı içerik, silindiği dizini gösterecek ve daha sonra orada başka deliller de aranabilecektir.

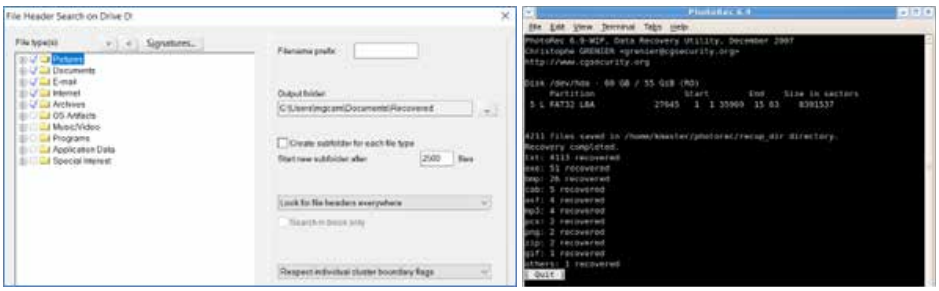
Silinmiş dosyalar klasörü boşaltılmış olsa bile, silinen dosyaları kurtarmak yine de mümkün olabilir. Bir bilgisayar kullanıcısı sil düğmesine bastığında, dosya veri depolama aygıtından fiziksel olarak silinmez, ancak dosyanın saklandığı alan artık kullanılmaz olarak işaretlenir ve dosyanın konumuna yapılan referanslar çoğunlukla dosya sisteminin dizininden silinir. Veriler, diskin bulunduğu bölüm başka bir dosya için gerekli olana veya başka bir kasıtlı eylem yapılana kadar potansiyel olarak sabit diskte veya depolama ortamında kalacaktır. Bu, dosya sistemi artık herhangi bir referansa sahip olmadığında bile silinen dosyaları kurtarmanın mümkün olduğu anlamına gelir.

---

[122] Yedekli Bağımsız Diskler Dizisi – verileri birden çok disk üzerinde depolamaya yönelik bir mekanizmadır.

[123] Gelişmiş Teknoloji Eklentisi, bilgisayar sürücülerini bağlamaya yönelik bir mekanizmadır.

Winhex[124] ve TestDisk & PhotoRec gibi araçlar da dahil olmak üzere silinen dosyaların geri alınması için bir takım araçlar mevcuttur.[125] Tüm ticari adli yazılım uygulamaları, işleme aşamasının bir parçası olarak dosyaları kazıyacaktır.



Üstteki resim, kurtarma için kurulum seçenekleriyle Winhex programını gösterirken, alttaki resim Photorec›in bir kurtarma işlemini başarıyla yürüttüğünü göstermektedir. Silinen verilerin kurtarılması, bir dosyanın dahili formatını bilen ve depolama ortamı genelinde sektörlerin açılış baytları içindeki dosya imzalarını bulabilen bir yazılım programına bel bağlamaktadır. Yazılım, Winhex ekran görüntüsünde görülebileceği gibi farklı türde dosyalara ait «profillere» sahip olacaktır. Bu noktada, söz konusu yazılım dosyayı ortamdan ‹kazıyacak› ve önceden belirlenmiş bir alanda saklayacaktır. Kazıma işlemi, gerçek ortamda canlı olarak da yapılabilir, ancak adli laboratuvarda, adli anlık görüntü genelinde yapılacaktır.

Kazıma işleminin, dosya sistemi düzeyinde değil, disk düzeyinde çalıştırıldığı için canlı ve silinmiş dosyaları kurtaracağı akılda tutulmalıdır. Aynı zamanda aynı dosyanın birden fazla kez depolandığı veya dosya ile ilgili küçük resimlerin bulunduğu birçok dosya kopyasını da kurtaracaktır. Son olarak, kazıma işlemi gerçekleştiğinde de bazen analistin veya müfettişin dosya sistemi konumu, tarihi, saati veya adı gibi bir dosyanın kaynağını tespit etmesine izin verecek hiçbir şey bulunamaz. Dosyaların kazınması artık bir sabit sürücü, USB sürücü veya akıllı telefon gibi bir depolama ortamından yüz binlerce dosyayı rutin olarak geri döndürmektedir - günümüzde internet etkinliğinin grafik yapısı budur.

Dosyaların veya verilerin sabit disklerden kalıcı olarak silinebileceği yazılım araçları geliştirilmiştir. Bu teknik daha yaygın olarak 'kalıcı olarak silme' olarak da bilinmektedir. Bu işlem, silinen dosyanın izi kalmayana kadar dosya veya dosyaların bulunduğu diskteki alanın üzerine veri yazarak yapılır. Kullanılan veriler, diskin geneline sürekli olarak 0'lar veya 1'ler veya bunların rastgele kalıplarını yazmak olacaktır. Bazı ticari araçlar, ek güvenlik sağlayarak birkaç kez üzerine yazacaktır, ancak kalıcı olarak silme aracının bir kez bile kullanılması çoğu kurtarma tekniğini boşa çıkaracaktır.

Bu, yerleşik Windows komutlarıyla (tam format) veya bu amaç için tasarlanmış diğer yazılım araçlarıyla kullanımı nispeten daha kolay olan basit bir delil karartma tekniğidir. Nitekim, delil karartma araçları bulunduğunda, bunların kullanımı bile şüphe uyandırmalıdır.

Sabit disk fiziksel olarak hasar görmüşse, diskleri sökerek ve kalan manyetik bilgileri dikkatlice okuyarak bazı dosyaları kurtarmak yine de mümkün olabilir. Manyetik disk-

---

[124] https://www.x-ways.net/winhex/

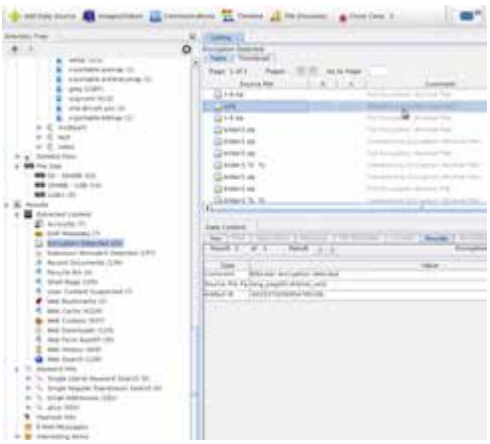
[125] https://www.cgsecurity.org/wiki/TestDisk_Download

lerden önemli ölçüde daha sağlam olan anlık bellek depolama aygıtları (SSD sürücüleri gibi) durumunda, diski oluşturan münferit anlık hücreler, verilerin alınabileceği hala işleyen hücreler bakımından da incelenebilirler. Bu, uzman araçlar ve bilgi gerektiren ve disklerin parçalarına ayırıldığı, disklerdeki mevcut toleranslar göz önüne alındığında temiz oda ortamında gerçekleştirilmesi gereken, yüksek düzeyde uzmanlık gerektiren bir görevdir.

6.5.3 Dosya Sisteminde Arama Yapılması

Veri depolama cihazlarının kapasiteleri, saklanan her dosyaya ayrı ayrı bakmayı neredeyse imkansız hale getirmektedir. Temel Windows 10 kurulumu, herhangi bir kullanıcı etkileşimi ve depolama olmadan önce belki 150.000 dosya üretmektedir. Analizi hızlandırmak amacıyla çoğu adli analist, ilgili dosyalar ve dizinler için önce ortak veri depolama dizinlerinin içine bakmaktadır. Bu teknik elbette birkaç terabayt veriye sahip yüzlerce bilgisayar sistemini analiz ederken yeterli olmayacaktır. Ardından, ilgili delil niteliğindeki içeriğin belirlenmesine yardımcı olmak için ticari yazılım araçlarına bel bağlanmaktadır.

Adli laboratuvara delille birlikte gönderilen teslim formu, müfettişin analistten ne talep ettiği konusunda da bir takım yönlendirmeler içermelidir. Uzun yıllar boyunca, depolama boyutlarındaki ilerlemeyle birlikte, basitçe sadece "her şeyin" elde edilmesini istemek mümkün değildir veya bu şekilde analistin zamanı ve kaynakları iyi kullanılmış olmaz.



İkinci bir analiz yöntemi, soruşturmayla ilgili anahtar kelimeleri dosya sisteminde aramak için ticari ürünler içindeki arama imkanlarını kullanmaktır. Bazı araçlar ayrıca (görüntü tanıma ve ten rengi algılama gibi işlevler gerçekleştirerek) görüntü arama olanağı da sunmaktadırlar. Resimlerdeki benzerlikleri tanımaya yönelik bir araç, Microsoft›un kolluk kuvvetleri için ücretsiz olarak sunduğu PhotoDNA[126] uygulamasıdır. Bu teknolojinin kullanılmasının, çocuk istismarına ilişkin bilinen görüntülerin bulunmasına ve kaldırılmasına yardımcı oması mümkünken, aynı şekilde bilinen ve dikkate değer dosyalara ait "adres kümelerinin" kullanılması da, materyal tanımlama sürecini hızlandırabilir.

[126] https://www.microsoft.com/en-us/photodna

6.5.4 Dosya Şifreleme ile Başa Çıkma

Dosyalarını korumak amacıyla suçlular, dosyalarını ve hatta tüm sabit disklerini okunamayan bir koda dönüştürmek için şifreleme teknolojisi kullanabilmektedir. Şifreleme teknolojisi birçok modern işletim sisteminde yerleşik olarak bulunmaktadır: Windows 7/8/10/11'de BitLocker, macOS'te FileVault ve birçok Linux dağıtımında dmCrypt/eCryptFS. PGP[127], TrueCrypt[128], VeraCrypt gibi dosya şifreleme teknolojileri, bağımsız olarak da kurulabilir. Modern bilgisayar sistemleri ve mobil sistemler, şifreleme mekanizmalarını donanım şifreleme işlemcilerine bile paketlemektedir. Örneğin BitLocker, bilgisayarın ana kartının Güvenilir Platform Modülü (TPM) yongasını kullanabilirken, macOS FileVault şifrelemesi, Apple Dosya Sistemini (APFS) şifrelemek/şifresini çözmek için Apple T2 güvenlik yongasını kullanabilmektedir.

Şifreleme, içeriği anlaşılmaz hale getiren bir matematiksel işlemin uygulanması yoluyla verileri disk düzeyinde değiştirerek dijital içeriği değiştirmektedir. İçeriği orijinal haline geri döndürmenin tek yolu, tersine bir matematiksel işlem uygulamaktır. Buna ‹simetrik› şifreleme denir. Bilgisayar dünyası sıklıkla simetrik şifreleme kullanmakta, ancak aynı zamanda genel ve özel anahtarlar kavramının olduğu «asimetrik» şifrelemeyi de kullanmaktadır. Asimetrik şifrelemenin işleyişine ilişkin bir açıklama sağlamaya çalışmak kesinlikle bu kılavuzun kapsamı dışına çıkar.

Doğru şifreyi veya "anahtarı" bilmeyen veya buna erişimi olmayan bir adli inceleme uzmanı, şifrelenmiş verilere erişmenin neredeyse imkansız olduğunu görecektir. Çeşitli farklı şifre çözme anahtarı kombinasyonlarını tek tek denemek mümkündür, ancak pratikte verilerin şifresini çözmek dünyadaki en güçlü bilgisayarların yardımıyla bile birkaç yıl sürecektir.

Şüpheli, şifre çözme anahtarını gönüllü olarak vermedikçe, adli inceleme uzmanının seçenekleri sınırlıdır. Şüphelinin kullandığı bilinen herhangi bir şifre denenebilir; makinenin yakınında veya şüphelinin elinde parola gibi görünen sözcük veya sayı kombinasyonları aranır veya ortak kullanılan parola listeleri (genellikle sözlükten sözcükler veya sabit disk içeriğinden oluşturulmuş bir sözlük) denenir.

Bazı araştırmalar, birçok kullanıcının 123456, parola, qwerty, süpermen veya futbol gibi kolay hatırlanan şifreler kullandığını göstermiştir. En sık kullanılan şifrelerin listesi internette arama yapılarak kolayca elde edilebilir.

Şifreleme anahtarlarının bilgisayar ağı tarafından sağlandığı durumlarda, ağ yöneticisi şifre çözme anahtarının bir kopyasına sahip olur ve sürücünün şifresini çözebilir. Bir Windows Aktif Dizini içindeki bilgisayarların BitLocker şifrelemesi için bu durum geçerlidir. Canlı veri adli incelemesi bölümünde açıklandığı gibi3.5, dosya ve birim şifrelemesini çözmeye çalışmanın bir yolu, bilgisayarın verilerini ve belleğini, cihaz çalışırken ve şifreli birim takılıyken almaktır. Yazılım geliştiriciler ve işletim sistemi üreticileri, sistemlerini daha güvenli hale getirmeye çalıştıkça, parolaların bellek içinde kolayca bulunabildiği günler artık geçmişte kalmıştır.

---

[127] 'Oldukça İyi Gizlilik' anlamına gelir

[128] TrueCrypt önde gelen bir dosya şifreleme yazılımıydı, ancak 2014 yılında kullanımdan kaldırıldı. Belki hala bulunabilir. Ancak Veracrypt, onun resmi olmayan bir halefidir.

Bu böyle bir sorun olduğu için, bazı ülkelerde kolluk kuvvetlerinin belirli koşullar altında bilgisayar sahibini şifreli depolama cihazının parolasını açıklamaya zorlamak için bir mahkeme emri almasına olanak tanıyan mevzuatlar vardır.[129]

6.5.5 Belge Adli Analizi

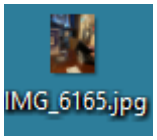
Elektronik belge adli incelemesi (basılı belge adli incelemesinin aksine), bilgisayarda bulunan bir dosya hakkında mümkün olduğunca fazla bilgi elde etmeye odaklanması bakımından veri dosyası adli incelemesinden farklıdır.

Belge adli incelemesi, belirli bir bilgisayar dosyasını kimin oluşturduğunu, dosyanın değiştirilip değiştirilmediğini ve dosyanın içinde herhangi bir bilginin gizlenip gizlenmediğini gösterebilir.

6.5.6 Meta (Tanımlayıcı) Veriler

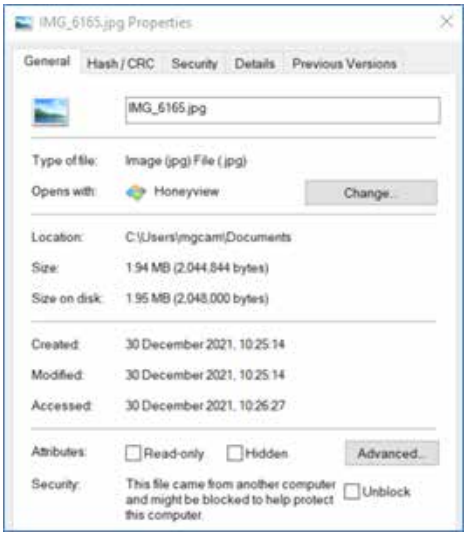
Meta veriler (veya veriler hakkındaki veriler), bir dosya hakkındaki bilgilerden oluşur. Esasen iki tür meta veri vardır - dosya sisteminin dosya hakkında tuttuğu ayrıntılar ve fiilen dosyanın içinde tutulan veriler. Dosya sisteminin ikinci tür verileri çıkardığı ve bilgisayar kullanıcısına sağladığı durumlarda bazen bunlar birbirinin yerine kullanılabilir.

Dosya "özellikleri", belgenin oluşturulduğu tarih ve saati, en son ne zaman değiştirildiğini ve en son ne zaman ve kim tarafından erişildiğini içerebilir. Bu veriler, dosyalarla bireyler arasında bağlantı kurmak bakımından son derece yararlı olabilir. Örneğin dünya genelinde milyonlarca bilgisayarı etkileyen Melissa bilgisayar virüsünün yaratıcısı, bu makro virüsün kaynak kodunda bulunan meta veriler sayesinde tespit edilmiştir.

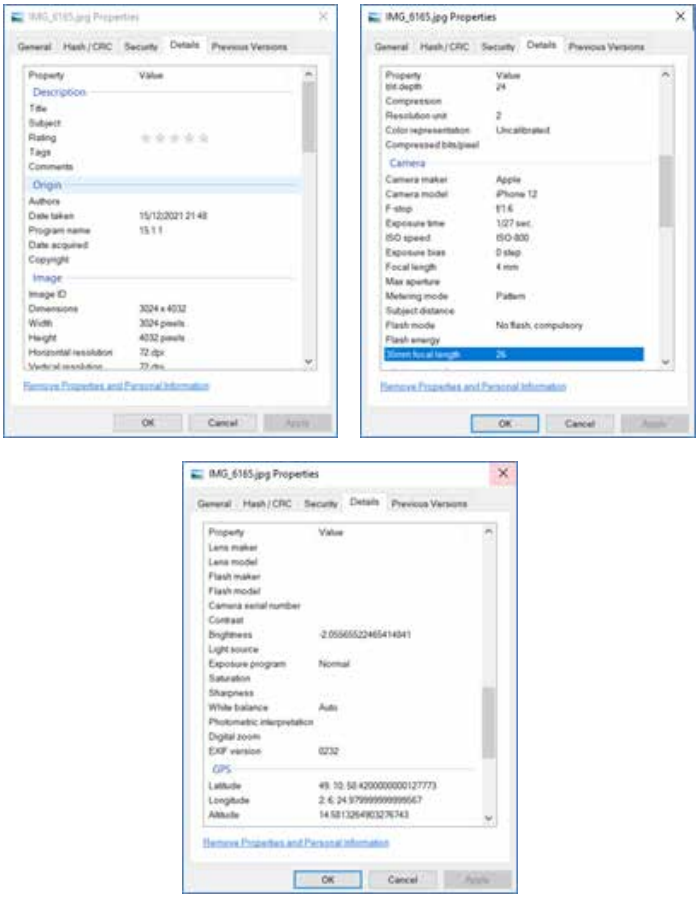


Örnek olarak, soldaki görüntü, masaüstünde bulunan bir JPG resim dosyasına aittir. Bu dosya hakkında bu ekran görüntüsündeki meta veriler, ‹IMG_6165.JPG› olan dosya adıdır. Araştırma, bunun Apple cihazlar (ve diğerleri) tarafından kullanılan adlandırma kuralına ve biçimine uyduğunu, bu fotoğrafın bir Apple cihazla çekilen 6165. resim olduğunu söyleyebilir.

[129] Örnekler; Birleşik Krallık (2000 tarihli Soruşturma Yetkilerinin Düzenlenmesi Yasasının III. Bölümü) ve Fransa'dır (Fransız Ceza Kanununun L 434-15-2. Maddesi)

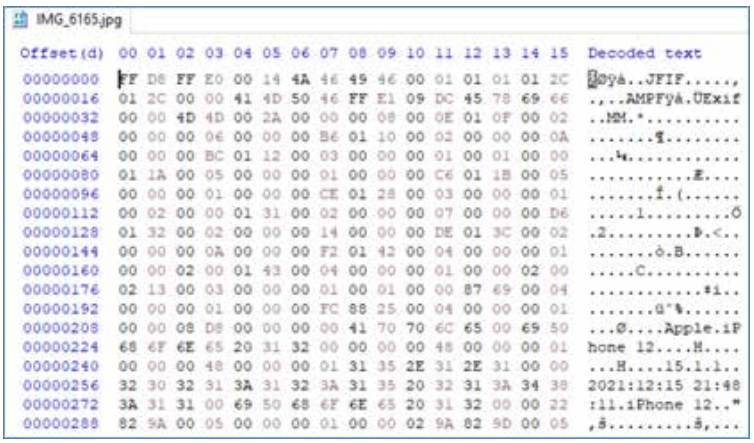


Dosyaya sağ tıklayarak özellikler seçeneğini seçip, 'genel' sekmesini görüntüleyerek, dosyanın depolandığı konum, dosyanın boyutu ve dosyayla ilgili bazı tarihler de dahil olmak üzere dosya hakkında daha fazla bilgi erişilebilir hale gelmektedir. Bu, 'veriler hakkındaki verilerin' başlangıcıdır - içeriğine bakmak için daha açmadan önce bile bir resim hakkında alınan bilgiler.



"Ayrıntılar" sekmesine tıklandığında dosya hakkında daha fazla bilgiye ulaşılır. Bu sefer işletim sistemi dosyanın kendisinin içinden çıkardığı bilgilerle genel bilgilere

ekleme yapmıştır. Daha önce Bölüm 4.3.3 içinde bahsedildiği gibi, bir dijital fotoğraf dosyası genellikle dosyanın EXIF[130] bölümü adı verilen bir kısmı içinde meta veriler içermektedir. EXIF verileri, fotoğrafın çekildiği tarih ve saati, pozlama süresini, odak uzaklığını, kameranın seri numarasını ve potansiyel olarak resmin çekildiği yerin coğrafi koordinatlarını içerecektir.



Yukarıdaki resimde HxD isimli hex editör programında görüntünün açılış baytları gösterilmektedir ve sağ tarafta cihaz bilgilerinin başlangıç kısmının yanı sıra tarih/saat bilgisi de görülebilmektedir. Daha önce bir 'dosya imzası'ndan bahsetmiştik, açılıştaki üç baytından bu dosyanın dosya imzasının 'FF D8 FF' olduğu görülebilir - bir kazıma uygulamasının işini yaparken aradığı şey budur.

Bir fotoğrafı çeken kişinin kimliği tespit edilmeye çalışılırken, eğer bir şüphelinin üzerinde bulunan bir kamera, resim içinde kaydedilen ile aynı seri numarasını taşıyorsa, bu güçlü bir delildir. EXIF verileri değiştirilebilir, ancak EXIF bölümündeki resme ait teknik verilerinin çoğu birbirine kenetli olduğundan genellikle herhangi bir değişiklik tespit edilebilir.

Günümüzde pek çok cep telefonunda ayrıca bir kamera işlevi vardır ve çoğu akıllı telefon, GPS koordinatlarını ya (10 metreye kadar ayrıntı düzeyi ile) hassas modda ya da yakındaki cep telefonu kulelerine olan mesafeleri bir kaç kilometre doğrulukla nirengileyerek kaba modda saklayabilir.

Bu bilgiyi üretmenin daha "görüntülenebilir" yollarını sağlayacak bir dizi çevrimiçi ve çevrimdışı meta veri görüntüleyici vardır. Yukarıdaki resim, çevrimiçi Pic2Map uygu-

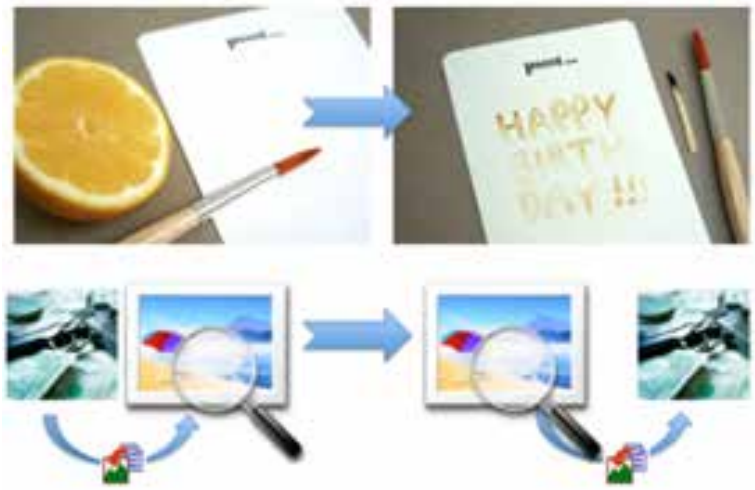
[130] Paylaşılabilir Görüntü Dosyası Formatı

lamasının EXIF bilgilerini nasıl aldığını ve görüntülediğini göstermektedir - resim ve konumu gösterilir ve ardından bir haritayla birlikte konumun havadan çekilmiş bir fotoğrafı eklenir.

Metin belgeleri de dahil olmak üzere çoğu düzenlenebilir belgede, meta veriler dosya içinde depolanır. Belge özellikleri, belgeyi değiştiren kullanıcıların adları ve belgeyi yazdırmak için kullanılan herhangi bir yazıcının adı da dahil olmak üzere belgenin revizyon geçmişini içerebilir.

6.5.7 Steganografi

Steganografi, bir mesajı veya başka bilgileri bir dosyanın içinde gizlemek için kullanılan bir tekniktir. En iyi dijital kullanımı, büyük boyutları dolayısı ile medya veya video tipi dosyaların içindedir. Kuruyunca kaybolan sihirli mürekkep ile veya limon suyuyla boş bir kağıda mesaj yazmaya benzetilebilir. Tıpkı kağıt üzerindeki sihirli mürekkep gibi, gizli dosya da fotoğraf, pdf ya da video gibi zararsız bir dosyanın içine gizlendiği için gözden kaçmaktadır.



Bir adli analist, resimdeki olağandışı bir ışık dağılımını (histogram) saptayarak veya resim dosyaları olağandışı özellikler sergiliyorsa, onu görmeye yönelik bir istatistiksel analiz yoluyla bu şekilde gizlenmiş bir dosyayı tespit edebilir. Özellikle bir vakada binlerce resim olduğunda ve her biri bu düzeyde değerlendirilemediğinde bunu yapmak inanılmaz derecede zordur. Tespit edildiğinde, gizli dosyayı çıkarmaya çalışmak için steganografi yazılımı kullanılabilir. Şüphelinin bilgisayar sisteminde bilinen bir steganografi yazılımının kurulu olduğu tespit edilirse, adli inceleme uzmanı gizli dosyaların bulunması olasılığı konusunda tetikte olabilir.

6.5.8 Günlük Dosyası Adli Analizi

Günlük dosyası adli incelemesi, bir bilgisayar sisteminin ve işletim sisteminin nasıl kullanıldığını belirlemeyi amaçlar.

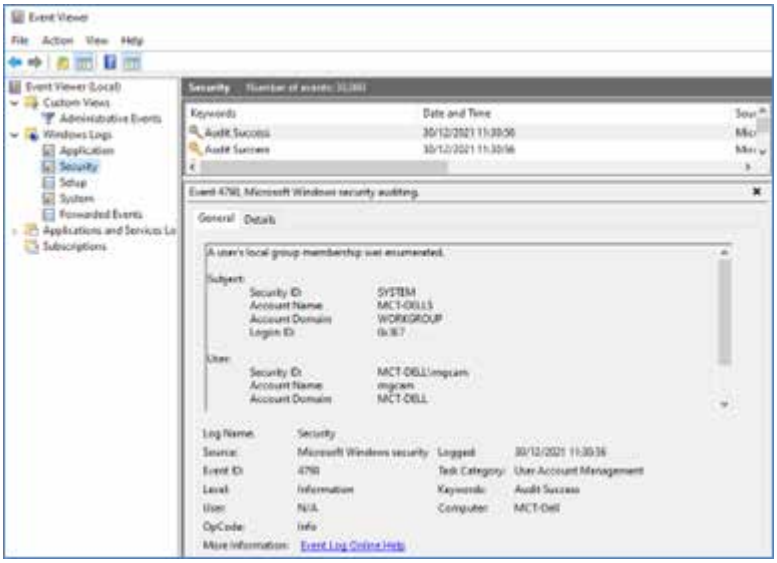
Dosya sistemi adli incelemesi ile, (bilgisayar virüsü gibi) yasa dışı bir dosya tespit edile-

bilir. Belge adli incelemesi ile, dosyanın şüphelinin makinesinde oluşturulduğu belirlenebilir. Sonraki adım, şüphelinin bunları oluşturan kişi olduğunu göstermektir.

Günlük dosyası adli incelemesi, bir makinede hangi yazılımların, süreçlerin ve hizmetlerin çalıştığına ve sistemde hangi kullanıcıların ve ne zaman oturum açtığına dair deliller sağlayabilir. Bu adli incelemeler, özellikle de üçüncü bir tarafın sisteme yasa dışı olarak eriştiğine dair deliller ararken değerli olabilir.

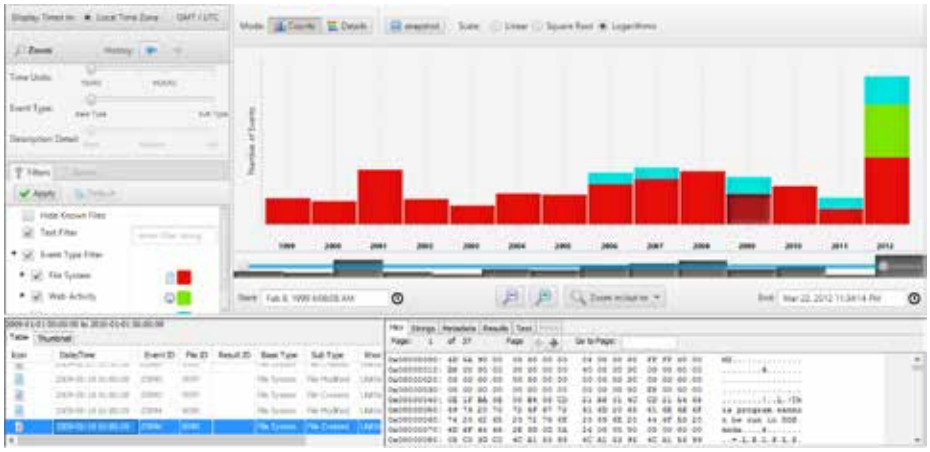
Günlük dosyası adli incelemesi, sistemde neler olduğunu tarihsel bir bağlamda analiz ederken, (bölüm 3.5 içinde açıklanan) canlı adli analiz, orada ve o anda çalışan bir bilgisayar sisteminde neler olduğunu sorgular.

Günlük dosyaları bir işletim sisteminin veya yazılım uygulamasının parçası olup, Windows, macOS ve Linux içinde bulunurlar. Bilgisayarın ne yapmakta olduğu veya yaptığı ile ilgili bilgileri kaydetmek ve bir kronolojik olay kaydı oluşturmak için kullanılırlar. Bir günlük dosyasının asıl amacı, yazılım geliştiricilerin yazılımı düzeltmesine yardımcı olmak için çökmelerin nedenlerini belirlemekti, ancak günlük dosyaları ayrıca, bir kullanıcının ne zaman oturum açtığı ve sisteme erişme girişimlerinin ne zaman yapıldığı gibi güvenlik uzmanları açısından ilgi çekici kayıtları da içerir.



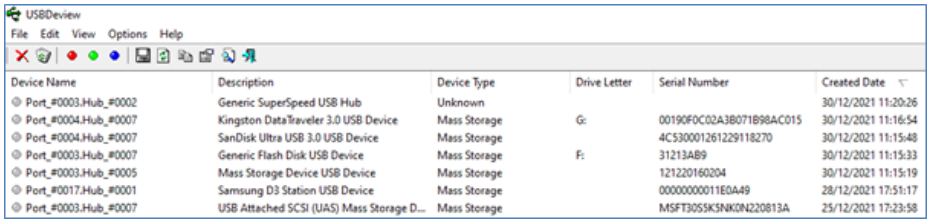
Yukarıdaki ekran görüntüsü, Windows içindeki Olay Görüntüleyici uygulamasını ve bir işletim sistemi içinde günlük kaydının gerçekleştiği ayrıntı düzeyini göstermektedir. Bu olguların derinlemesine incelenmesi, gerektiğinde bir soruşturmaya büyük ölçüde yardımcı olabilir.

Kronolojik kaydı analiz edebilmek ve kimin giriş yaptığını, ne zaman giriş yaptığını ve hangi yazılımın veya hizmetin ne zaman başlatıldığını görebilmek, üçüncü bir tarafın sisteme erişip erişmediğini göstermeye yardımcı olabilir ve bir bilgisayar sistemine yetkisiz erişime sağlandığına dair çok güçlü bir delil olabilir.



Günlük dosyaları[131], örneğin muhasebe yazılımı gibi bir uygulama düzeyinde de bulunabilirler. Burada yazılım günlüğü, hangi kullanıcının deftere bir işlem girdiğini kaydedebilir ve bir muhasebe yazılımı günlüğünün analizi, sahte kayıtların ortaya çıkarılmasına yardımcı olabilir.

Microsoft Windows, günlük dosyasına paralel olarak, kayıt defteri veri tabanı adı verilen bir dizin de sağlamıştır. Bilgisayar sisteminin yapılandırmalarının kaydedilmesi bakımından amacı biraz farklıdır ancak kayıt defteri adli inceleme amacıyla da kullanılabilir. USB çubukları gibi hangi harici cihazların makineye bağlanmak üzere önceden yapılandırıldığı, bir bilgisayarın hangi ağ için yapılandırıldığı vb. ile ilgili bilgiler içerir. Ayrıca, söz konusu bilgisayar sisteminin bağlı olduğu WiFi ağları da dahil olmak üzere çeşitli ağları depolar. Windows Kayıt Defteri, bir sistemin belirli bir yerde kullanılıp kullanılmadığını veya sisteme bir USB anahtarının bağlanmış olup olmadığını kanıtlamak bakımından yararlı olma potansiyeline sahiptir.



Device Name	Description	Device Type	Drive Letter	Serial Number	Created Date
Port_#0003.Hub_#0002	Generic SuperSpeed USB Hub	Unknown			30/12/2021 11:20:26
Port_#0004.Hub_#0007	Kingston DataTraveler 3.0 USB Device	Mass Storage	G:	00190F0C02A3B071B98AC015	30/12/2021 11:16:54
Port_#0004.Hub_#0007	SanDisk Ultra USB 3.0 USB Device	Mass Storage		4C53000126122911827O	30/12/2021 11:15:48
Port_#0003.Hub_#0007	Generic Flash Disk USB Device	Mass Storage	F:	31213AB9	30/12/2021 11:15:33
Port_#0003.Hub_#0005	Mass Storage Device USB Device	Mass Storage		121220160204	30/12/2021 11:15:19
Port_#0017.Hub_#0001	Samsung D3 Station USB Device	Mass Storage		00000000011E0A49	28/12/2021 17:51:17
Port_#0003.Hub_#0007	USB Attached SCSI (UAS) Mass Storage D...	Mass Storage		MSFT30S5K5NK0N220813A	25/12/2021 17:23:58

Yukarıdaki resimde, kayıt defteri girdilerinden bir sisteme takılan USB cihazlarını tanımlayan USBDeview adlı bir yazılım programı kullanılarak alınan bir çıktının yanı sıra daha fazla analiz veya kurtarma için her cihaz hakkında da önemli miktarda bilgi gösterilmektedir.

6.5.9 Ağ Adli Analizi

Ağ trafiğinin analiz edilmesinin amacı, bir iletişimin kaynağını veya internet üzerinden yapılan bir saldırının kaynağını tespit etmektir. Çoğu zaman adli analistin elinde, ya bilgisayara gönderilen kötü niyetli iletişimin IP adresini içeren günlük dosyası veya yasadışı içeriğe sahip bir web sitesinin alan adı ve IP adresi ya da muhtemelen suç

[131] https://www.sleuthkit.org/autopsy/images/v3/tl_counts.png

içerikli bir e-posta tarafından izlenen yolu da içeren başlık aracılığı ile halihazırda bir başlangıç noktası bulunmaktadır.

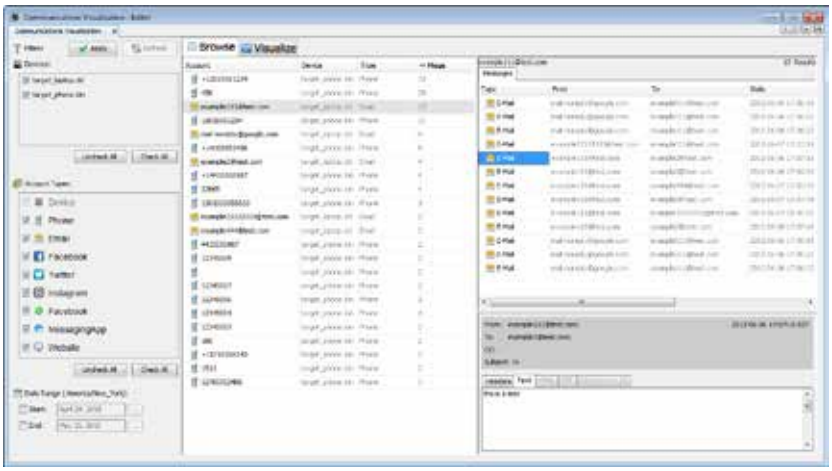
İnceleme uzmanı, hem faili belirlemeye yardımcı olması için, hem de ilgili bağlantılar gelişmeye ve daha fazla suç davranışı ortaya koymaya başladığı için, bu başlangıç noktasından diğer internet kaynaklarıyla olan bağlantılara ve ilişkilere bakacaktır. Başka kötü niyetli internet kaynakları bulunursa, kolluk kuvvetleri bunların kapatılmasını talep edebilir.

6.5.10 İnternet İzleri

Bölüm 4.2, IP adreslerinin yapısına ve alan adı hizmetine ilişkin bir teknik özet sağlamaktadır. Adli analistin, (aynı internet sunucusu üzerinde barındırılan diğer alan adları gibi) bağlantılı internet kaynaklarını ve Sınıfsız Alanlar Arası Yönlendirme (CIDR) gösterimini ve IP adresinin ait olduğu Otonom Sistemi tespit etmek için hem fail tarafından kullanılan IP adreslerine hem de fail tarafından kullanılan alan adlarına daha yakından bakması gerekmektedir. Fail tarafından kullanılan diğer alan adlarının ve IP adreslerinin belirlenmesi, şüphelinin tüm potansiyel yasa dışı faaliyetlerine ilişkin daha iyi bir genel bakış sağlar ve ayrıca şüphelinin kimliğinin tespit edilmesi için ek bilgiler sağlanması konusunda yardımcı olabilir.

Aşağıdaki alt bölümlerde, e-posta ve internet aramalarına ilişkin adli analize bakılacaktır.

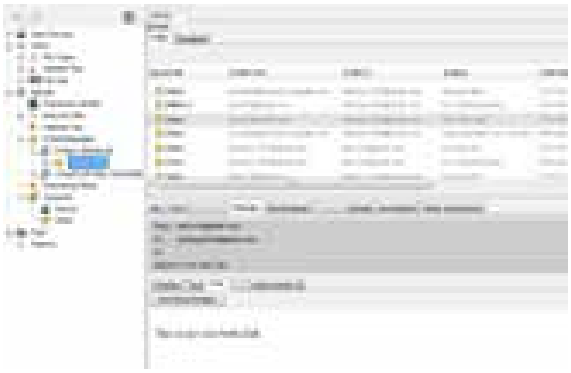
6.5.10.1 *E-posta adli analizi*[132]



E-posta adli incelemeleri, e-posta mesajının nereden gönderildiğini belirlemek için e-posta kaynak metnini inceler. E-posta yazılımı normalde e-posta mesajının içindeki teknik bilgileri okuyucudan gizler. Bu tür bilgilere e-posta başlığı (veya bazen de genişletilmiş başlık) denir. E-posta başlığı, ortak bir standartlaştırılmış İnternet biçiminde (RFC 2822) olacaktır, ancak başlık bilgilerini ortaya çıkarma yöntemi, hangi e-posta istemcisinin kullanıldığına bağlı olarak değişmektedir.

[132] https://sleuthkit.org/autopsy/docs/user-docs/4.7.0/communications_page.html

Ne zaman Posta Aktarım Aracısı (MTA) olarak da bilinen bir e-posta sunucusu bir e-posta iletisi alsa ve bunu alıcıya giden yolculukta bir sonraki MTA'ya iletse, sunucu damgası e-posta başlığına e-postanın alındığı IP adresini ve alındığı zamanı da gösteren bir satır ekler.



E-posta başlığı okunarak, e-postanın alıcının gelen kutusuna giderken izlediği yolun takip edilmesi mümkündür. Geçilen sunucular tarafından eklenen yeni satırlar en üste eklendiğinden, e-posta başlıkları her zaman aşağıdan yukarıya doğru okunmalıdır - dolayısıyla ilk sunucu en altta kaydedilen olacaktır.

Konusu "E-posta başlığı" ve gövde metni "Bu, gövde metnidir" olan bir e-posta mesajına ait bir e-posta başlığı örneği aşağıdadır:

```
Teslim Edilen: forensics@forensics.com
Alındı: jz15csp53304qcb SMTP kimliği ile 10.229.233.207 tarafından;
        Çarşamba, 30 Mart 2022 00:37:09 -0700 (PDT)
Alındı: oa9mr46792071pbb.95.1338363429020 SMTP kimliği ile
10.68.130.9 tarafından;
        Çarşamba, 30 Mart 2022 00:37:09 -0700 (PDT)
İade Adresi: <forensics@hotmail.com>
Alındı: bay0-omc2-s16.bay0.hotmail.com [65.54.190.91] tarafından
        rg2si17612042pbc.261. 2022.03.30.00.37.08 ESMTP kimliği ile
mx.google.com tarafından;
        Çarşamba, 30 Mart 2022 00:37:08 -0700 (PDT)
Alındı: Microsoft SMTPSVC(6.0.3790.4675) ile BAY157-W32
([65.54.190.123]) tarafından;
       Çarşamba, 30 Mart 2022 00:36:32 -0700
Mesaj Kimlik No: <BAY157-W32F746CCEC9B74654CC7C0A40A0@phx.gbl>
İade Adresi: forensics@hotmail.com
X-Kaynak-IP: [84.169.25.82]
Kimden: Forensics <forensics@hotmail.com>
Gönderen: <forensics@hotmail.com>
Alıcı: <forensics@forensics.com>
Konu: E-posta başlığı
Tarih: Çarşamba, 30 Mart 2022 07:36:51 +0000
Önem derecesi: Normal
MIME-Version: 1.0

Bu, gövde metnidir.
```

Başlık, potansiyel olarak iletişim hakkında bilgi verecektir. Bu durumda, e-postanın gönderildiği görünen IP adresi 84.169.25.82'dir ve tarih, saat ve saat dilimi göndericinin tanımlanmasına yardımcı olacaktır.

Gönderici, örneğin e-postayı bir botnet kullanarak göndermek için birinin bilgisayarını ele geçirdiyse, e-posta iletisinin göndericisini belirlemek yine de zor olabilir. Gönderici, internet kafe gibi halka açık bir yere giderek de izlerini gizleyebilir. Göndericinin IP adresi kafeye ait olacak ve ona yönlendirmeyecektir.

Analizin, gönderen makinenin muhtemelen ele geçirildiğini ortaya çıkardığı durumlarda, saldırının kaynağını belirlemek için canlı adli incelemelerin ve günlük dosyası adli incelemelerinin yapılması gerekecektir. E-posta, otel lobisi veya internet kafe gibi halka açık bir yerden gönderilmişse, e-postanın gönderildiği sırada halka açık bilgisayarı kullanan müşteriyi tespit etmeye yardımcı olması için eski moda dedektiflik yapılabilir. Ayrıca, bir e-posta başlığındaki bilgilerin çoğu güvenilir olmayabilecek farklı e-posta sunucuları tarafından eklendikleri için, bunların değiştirilebileceğini de belirtmek gerekir. Temel olarak bu husus, bir e-posta başlığının altındaki tüm bilgiler için geçerlidir, çünkü bunlar doğrudan gönderenin (şüphelinin kontrolü altında olması muhtemel) posta sunucusundan gelmektedir. Başlığın daha yukarı tarafında yer alan bilgiler, internet sağlayıcısının posta sunucusu ve ardından diğer uzak cihazlar tarafından eklendiğinden daha güvenilirdir.

6.5.10.2 *İnternet aramaları*

Bir kullanıcının internet aramaları onun hakkında çok şey ortaya çıkarabilir. Örneğin, bir adamın eşinin kayıp olduğunu bildirdiği bir vakada polis, kayıp eşin nereye gitmiş olabileceğine dair ipuçları bırakıp bırakmadığını görmek için ev bilgisayarını araştırmıştır. Bir seyahate hazırlanırken, bilgisayar kullanıcısı çoğunlukla internette seyahat edeceği yer hakkında bilgi veya bir otel odası arayacaktır. Bu vakada polis, ev bilgisayarındaki arama geçmişine bakmış ve bilgisayarın, internette "Birini nasıl öldürür de yakalanmazsın" ve "birini sessizce öldürmek" aramaları yapmak için kullanıldığını keşfetmiştir. Bu keşif polisin düşüncesini değiştirmiştir.

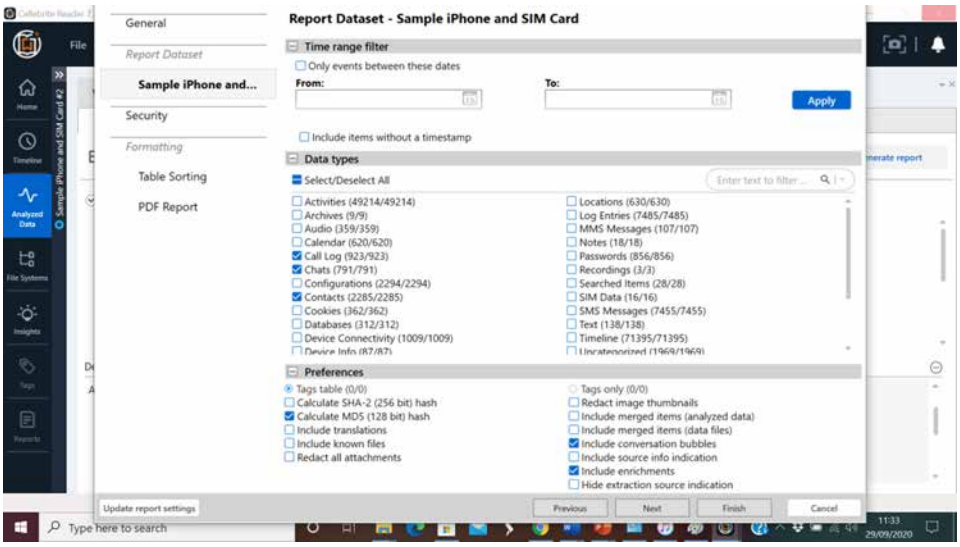
https://www.google.com/search?q=killing+someone+quietly&rlz=1C1FKPE_en-GBGB966GB966&oq=killing+someone+quietly&aqs=chrome..69i57j0i22i30.6177j0j4&sourceid=chrome&ie=UTF-8

Yukarıdaki kayıt, Google'ın bir aramayı nasıl biçimlendirdiğine ilişkin bir örnektir. Daha önce görülen örnekte, aranan kelime dizisi açıkça görülebilmektedir.

Tüm aramalar ve web sayfası görünümleri, Internet Explorer, Edge, Mozilla Firefox, Opera, Safari veya Google Chrome tarayıcılarının geçmiş bölümünde mevcuttur ve bu bölüm Windows ve Linux içinde Ctrl+H ve macOs içinde Command+H tuşlarına basılarak açılabilir. Google ve Bing arama motorları, arama geçmişini sunucularında birkaç yıl boyunca tutmaktadır. Google, kullanıcının arama geçmişini ve etkinliklerini https://myactivity.google.com adresinde tutar ve Windows Live (Bing), arama geçmişini https://www.bing.com/profile/history adresinde görüntüler. Giriş yapıldığında, belirli bir kullanıcı hesabının arama geçmişi, bu motorlar kullanılarak bir kullanıcının cep telefonundan, ofis bilgisayarından ve ev bilgisayarından yapılan aramaların tümünü tek bir merkezde depolanmış olarak gösterecektir. Kullanıcılar, burada tutulanları kısıtlayabilir ve bu geçmişleri temizleyebilir, ancak yukarıda görüldüğü gibi kalıntılar, şüphelinin sildiğini düşündüğü zamandan uzun bir süre sonra sabit disklerden geri alınabilir.

6.6 Elkonulan Cihazlar Üzerinde Bağlı Hizmetler

Elkonulan bir cihaz, soruşturma ile ilgili daha fazla bilgi içeren bir dizi çevrimiçi hizmete bağlı olabilir. Örneğin bir cihaz, bir sosyal ağ hesabında, bir VoIP hesabında veya bir e-posta hesabında vb. otomatik olarak oturum açacak ve bir dizi web sitesi için tarayıcıda önceden kaydedilmiş parolalar olacak şekilde yapılandırılabilir. Bu bilgilere erişim, müfettiş için çok değerli olabilir.



Cihaz, kullanıcı tarafından internet üzerinde depolanan ve cihazda yerel olarak depolanmayan dosyalara erişim sağlayan bir bulut veri depolama hesabına açık olan bir bağlantıya sahip olabilir. Cihazın tarayıcısına erişim, cihaz sahibi tarafından kullanılan diğer çevrimiçi hizmetler ile ilgili olarak denenecek bir dizi ortak şifreyi de ortaya çıkarabilir. Firefox Seçenekleri iletişim kutusunda, güvenlik bölümünün altındaki bir butona tıklayarak, kullanıcılardan herhangi birinin tarayıcı tarafından saklanan şifresini görüntülemek mümkündür.

Cihazı inceleyen bir uzmanın, özellikle de uzmanın yetki alanı dışında depolanan veriler başta olmak üzere, uzakta depolanan verilere erişmesine ne ölçüde izin verildiği, geçerli ulusal mevzuata bağlı olacaktır ve bu Kılavuzun içinde yanıtlanamaz.

Benzer şekilde, IMAP, Microsoft Exchange Server veya Gmail hizmetlerini kullanan herhangi bir e-posta hesabı, bir kullanıcının e-posta hesabının içeriğini çevrimdışı kullanım için cihazda yerel olarak depolayabilir. Ancak, uzmanın e-postalara yerel olarak cihaz üzerinde mi yoksa uzaktan bir sunucu üzerinde mi erişmekte olduğunu anlamak, buna kesin olarak yanıt vermek zor olabilir. Adli inceleme uzmanlarının, yargı bölgesine ilişkin uluslararası hukuk kurallarını istemeden de olsa ihlal etme olasılığına karşı dikkatli olmaları gerekir.

7 Delillerin Hazırlanması ve Sunulması

7.1 Elektronik Delillerin Yargılama İşlemlerinde Kullanılması

Bu bölüm, elektronik delillere ilişkin ilkelerin açıklandığı bölüm 1.6'yı tamamlamaktadır.

Hepsi dijital veriler oluşturan e-postalar, dijital fotoğraflar, ATM işlem günlükleri, kelime işlem belgeleri, anlık mesajlar, elektronik tablolar, internet tarayıcısı geçmişi, veri tabanları, bilgisayar belleğinin içeriği, bilgisayar yedekleri, bilgisayar çıktıları ve dijital video ve ses dosyaları biçimindeki elektronik delilleri, mahkemelerin kabul etmek ve göz önüne almak zorunda kalması sebebiyle geçtiğimiz birkaç yıl içinde elektronik delillerin kullanımı artmıştır.

Suç mahallinde bulunan diğer fiziksel delil türlerinde yapılacağı gibi, suçta kullanılan bir dijital cihaz da güvence altına alınmalıdır, çünkü bu tür tüm cihazlar fiziksel delil olarak kalmaktadır. Parmak izi ve DNA delillerinde olduğu gibi, dijital deliller de hassastır ve uygun önlemler alınmazsa kolayca kaybolabilir veya değişebilir. Dijital delillerin ele alındığı erken dönemlerde, kolluk kuvvetlerinin eğitimsiz mensupları, bir adli incelemeye göndermeden önce delil aramak için bilgisayarları açmış veya açık cihazları kapatarak RAM içindeki verileri ve potansiyel delilleri kaybetmişlerdir.

Dijital cihazın nerede bulunduğunu ve ele geçirildiğini kaydetmek önemlidir, çünkü bu bilgi, şüphelenilen suçlunun niyeti hakkındaki birçok şeyi ortaya çıkarabilir. Arama ve elkoymayı videoya kaydetmek iyi uygulamadır. Bu uygulama, dijital cihazların konumunu gösterecek, böylece örneğin kablosuz cihazın oturma odasındaki açık alanda değil de çatı katında gizlenmiş olarak bulunduğuna dair bir tartışma kalmayacaktır.

Elektronik delillerin kullanımı ile ilgili zorluklar artık sadece delilin kalitesi ve güvence altına alınması ile ilgili değildir, aynı zamanda giderek artan bir şekilde elektronik delillerin miktarıyla da ilgilidir. Nitekim, elkonulan veya ele geçirilen elektronik delillerin hacmi katlanarak artmaktadır. Büyük verilerin işlenmesi de mahkemelerde bir sorun haline gelmektedir. Bir fikir vermesi açısından, Encrochat[133] davası veya SKY ECC davası[134] gibi davalarda, Fransa, Hollanda ve Belçika'nın toplam ulusal polis kapasitesinin makul bir süre içinde okuyabileceğinden daha çok terabaytlık elektronik delil toplanmıştır.

Elektronik delillerin miktarı, kovuşturma ve yargılama açısından olduğu kadar, aynı zamanda savunmanın hakları ışığında da giderek en büyük zorluklardan biri haline gelmektedir. Hiçbir savcı, hâkim veya savunma avukatı, yargılama işlemleri boyunca büyük veri paketlerinin eksiksiz bir değerlendirmesini, incelemesini ve analizini yapamaz. Bu, delilin nasıl toplandığını, nasıl işlendiğini ve analiz edildiğini, verilerin analizi ve kullanılması sırasında hangi parametrelerin ve adli metodolojinin kullanıldığını,

[133] https://www.europol.europa.eu/media-press/newsroom/news/dismantling-of-encrypted-network-sends-shockwaves-through-organised-crime-groups-across-europe

[134] https://www.europol.europa.eu/media-press/newsroom/news/new-major-interventions-to-block-encrypted-communications-of-criminal-networks

(örneğin özel yazılım ve donanım, yapay istihbarat, arama robotları, anahtar kelimeler içeren çok dilli kütüphaneler vb.) hangi teknik araçların kullanıldığı ve ayrıca belirli veriler elektronik delil olarak seçilip, diğer veriler seçilmezken hangi seçim kriterlerinin kullanıldığını bilmeyi daha da elzem hale getirmektedir. Bütün bunlar, hem yargıçlar (ve varsa jüri) hem de savunma için şeffaf ve anlaşılır hale getirilmelidir. Ayrıca, savunmanın etkili argüman üretme sürecine girebilmesi de sağlanmalıdır.

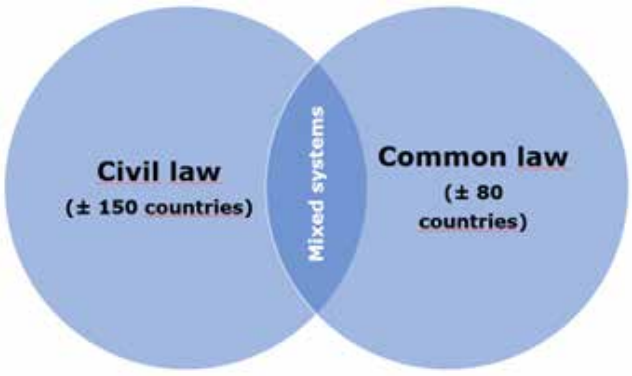
Ayrıca, tipik olarak savcıların, hâkimlerin (ve varsa jürinin) ve savunma avukatlarının bilgisayar adli incelemesi veya veri analizi konularında teknik olarak uzman düzeyinde eğitim almadıkları dikkate alınmalıdır. Bu yüzden, elektronik deliller kullanılırken, gösterilmelerinin ve mahkemeye sunulmalarının anlaşılır bir şekilde aktarılması gerektiğine dikkat edilmelidir.

7.2 Farklı Yasal Sistemler

Mahkemede (elektronik) delillerin kullanımını tartışırken, her şeyden önce, mahkemeler tarafından (elektronik) delillerin alınma şeklinin, kullanıldıkları ilgili ülkenin hukuk sistemine bağlı olarak bütünüyle farklı olabileceğini belirtmeliyiz. Genel hukuk ve medeni hukuk yasal kültürleri arasında önemli bir fark vardır ve bu hususa gereken ilgi gösterilmelidir.

Bir Medeni Hukuk sistemi, özünde soruşturma ile ilgilidir ve kodlanmış tüzükler ve çoğu durumda jürinin olmadığı ve hâkimin yargılamayı yönettiği bir mahkeme sistemi ile karakterize edilir. Delil toplamanın odak noktası, savcının (veya bir soruşturma hâkiminin) başını çektiği, yargılama öncesi kapsamlı soruşturma aşamasıdır. Mahkeme duruşması boyunca yürütülen soruşturma çok daha sınırlıdır (hâkimler çoğunlukla bildirilen iddialara ve duruşma öncesi soruşturma sonuçlarına güvenir).

Genel Hukuk sistemi ise çekişmelidir ve daha çok içtihata dayalıdır. Jüri sistemi, hâkimin büyük ölçüde bir hakem rolünü üstlendiği yaygın bir uygulamadır. Duruşma çok önemlidir ve her delil ilkesel olarak jüri huzurunda sunulmalı ve savunulmalıdır. Bilirkişilerin ve tanıkların çapraz sorgusu, standart yargı sürecinin bir parçasıdır.



Ülkelerin farklı yasal aileler içinde kabaca sınıflandırılması

7.3 Yargılama İşlemleri İçinde Delil

Ayrıntılar yargı bölgesinden yargı bölgesine farklılık gösterebilse de, yargılama için elektronik delillerin (kabul edilebilirliği) değerlendirilirken genellikle aşağıdaki kriterler dikkate alınmalıdır:

- Gerçeklik: Delil, gerçekleri tartışılmayacak bir şekilde ve orijinal durumunu temsil eden bir şekilde tespit etmelidir.
- Tamlık: Delilin analizi veya delile dayalı herhangi bir görüş, hikayenin tamamını anlatmalı ve daha olumlu veya arzu edilen bir bakış açısına uyacak şekilde uyarlanmamalıdır.
- Güvenilirlik: Delilin toplanma ve daha sonra ele alınma şekli hakkında, gerçekliği veya doğruluğu konusunda şüphe uyandırabilecek hiçbir şey olmamalıdır.
- İnanılırlık: Delil, temsil ettiği gerçekler konusunda ikna edici olmalı ve mahkeme sürecinde mahkeme heyeti ona gerçek olarak güvenebilmelidir.
- Orantılılık: Delilleri toplamak için kullanılan yöntemler adil ve adaletin çıkarları ile orantılı olmalıdır; herhangi bir tarafın haklarına yönelik önyargı (yani haksız müdahale veya zorlama düzeyi), delilin "ispat değerinden" (yani delil olarak değerinden) daha ağır basmamalıdır.

7.3.1 Kabul Edilebilirlik

Bilgisayar Delili, mahkeme tarafından kabul edilebilir olmasını sağlayan bir dizi yasaya ve kurala uyuyorsa kabul edilebilirdir. Delil elde edilirken uygun prosedürler izlenmelidir. Bunlar önceki bölümlerde açıklanmıştır.

7.3.2 Gerçeklik

Verilerin gerçekliğine ilişkin delilleri hazırlamak ve sunmak, kabul edilecek delilleri arayan tarafın sorumluluğundadır.

Elektronik delil, bir kağıt parçası üzerinde kaydedilmiş bir belge gibi, fiziksel delilden farklı değildir. Delilin gerçek olduğundan emin olmak gerekmektedir. Elektronik delil ile fiziksel delil arasındaki fark, genellikle elektronik delilin değişebilme ve kasıtlı veya kasıtsız olarak değiştirilebilme kolaylığıdır.

7.3.3 Tamlık

Delilin analizi veya delile dayalı herhangi bir görüş, hikayenin tamamını anlatmalı ve daha olumlu veya arzu edilen bir bakış açısına uyacak şekilde uyarlanmamalıdır. Delili arama ve sunma görevi (ispat yükümlülüğü) tamamen tüketilmiş olmalıdır.

Tamlık, sanık lehindeki ve aleyhindeki tüm delilleri toplamak için yeterli düzeyde bir çabanın gösterilmiş olması gerektiği anlamına gelmektedir. Ancak tamlık, elkonulan veri taşıyıcılarda bulunan verilerden hiçbir seçim yapılamayacağı veya belirli veri ana-

lizlerinin yapılmadığı veya belirli soruşturma eylemlerinin gerçekleştirilmediği anlamına gelmez. Bununla birlikte, bazı unsurlar araştırılmazsa, bunun neden yapılmadığına ilişkin olarak yeterince gerekçelendirilme yapılmalı ve bu husus belgelenmelidir.

7.3.4 Güvenilirlik

Delilin toplandığı andan mahkemeye sunulduğu ana kadar, nerede olduğu, onu kimin elinde tuttuğu ve herhangi bir şey olduysa, ona ne olduğu her zaman net olmalıdır. Buna *delil zinciri* denir.

Delil Zinciri, esas olarak elektronik delillerin - soruşturma için elde edilen öğelerin - uygun bir şekilde nasıl toplandığını, tutulduğunu, nakledildiğini ve güvence altına alındığını belgelemektir. Delil zinciri, veri ortamının kurcalanmadığına "güven" duyulduğunu mahkemelere gösterir. Belirli bir delile "kimin ne yaptığını" ve "bunun ne zaman gerçekleştiğini" gösteren bir denetim izidir.

7.3.5 İnanılırlık

Delil olarak sunulan elektronik veriler hakkında bir şüphe olması durumunda, kabul edilebilirliklerine itiraz etmek savunmaya düşer. Bu husus ileri sürüldükten sonra, savcılık genellikle verilerin bütünlüğünün güven telkin ettiğine ve bu nedenle güvenilir kabul edildiğine dair yeterli delil sunarak bu hususla ilgilenmek zorundadır.

Delilin bir diğer önemli yönü, söz konusu delilin nasıl elde edildiği ve bu delilin oluşturulduğu metodolojinin nesnel, bilimsel doğrulama ve gözden geçirmeye tabi olup olmadığıdır. Örneğin, iddia makamı tarafından, davalının günün belirli bir saatinde kendi ISP'sine bağlandığını gösteren bir telefon faturası ibraz edilirse, bu genellikle kabul edilecektir. Tersine, iddia makamı tarafından "*Davalı sabit diskindeki tüm dosyaları silmiş, diski yeniden biçimlendirmiş, ardından 10. katın penceresinden dışarı atmış, ama biz bir veri kurtarma firmasına giderek dosyaları yeniden oluşturabildik*" iddiasında bulunulursa, o durumda savunma, delillerin geri kazanılmasına yönelik bu yöntemin geçerliliğini sorgulayabilir. Delilleri elde etmek için kullanılan yöntemlerin geçerli olduğunu kanıtlamak ve mahkemeyi delillerin kabul edilmesi gerektiğine ikna etmek iddia makamının görevidir.

Doğru dengeyi kurmak gereklidir. Bir yandan, karar vericilerin (gerek jüri üyeleri olsun, gerekse tek bir hâkim olsun) teknik ayrıntıları anlamalarını beklemek makul değildir. Öte yandan, veri kurtarma tekniklerini "sihir" olarak kabul etmelerini beklemek de doğru değildir. Bazı ülkelerde çözüm meslektaş incelemesidir - eğer söz konusu alanda çalışan diğer uzmanlar tekniği incelemiş, test etmiş ve sonuçları doğrulamışsa, mahkeme de delilleri kabul edecektir.

Ancak, hâkim(ler)in veya jürinin elektronik delili ve toplanmasını basit anlamda "sihir" olarak kabul etmemesi gerektiği gerçeği, polis tekniklerinin korunmasına yer olmadığı anlamına gelmez. Söz konusu koruma, belirli polis tekniklerinin gelecekte de kullanılmaya devam etmesini sağlamak için gerekli olabilir. Bu koruma olasılığı, esas olarak elektronik delillerin toplanması ve bunun için kullanılan polis yöntemleri düzeyinde gerçekleşmektedir. Başka bir deyişle: kolluk kuvvetlerinin verileri elde etmesini ve

bilgisayar sistemine girmesini mümkün kılan yöntem, gerektiğinde uygun mahkeme emri kapsamında olduğu sürece korunabilir (örneğin bir mahkeme emri, bu sonuca ulaşmak için kullanılan teknik polis yöntemlerini ifşa etmeden de "iletişimin, okunabilir bir formatta dinlenmesi emrinin verilmiş" olduğunu belirtebilir - ancak hukuk sistemine ve ülke mevzuatına bağlı olarak, kullanılan yöntemleri açıklama zorunluluğu düzeyinin değişeceği belirtilmelidir) . Adli analiz söz konusu olduğunda, bu fark ilke olarak mevcut değildir; zaten adli analizin kendisi her zaman şeffaf ve bilimsel olarak doğrulanabilir olmalıdır.

Tekrar etmekte fayda var, elektronik deliller mahkemede diğer deliller ile aynı şekilde ele alınır. İddia makamının belgenin gerçek olduğunu ve içeriğinin kabul edilebilir olduğunu kanıtlaması gerekecektir. Elektronik deliller ile ilgili tüm işlemler, bu Kılavuzda belirtilen elektronik delil ilkelerine uygun olmalıdır.

7.3.6 Orantılılık

Orantılılık ilkesi, hem suçun niteliğini ve koşullarını, hem de etkilenen temel hakların niteliğini ve meşruiyetini dikkate alarak, daha az müdahaleci olan başka bir yetki veya prosedürün, bu yetki veya prosedürün amacına yeterli düzeyde ulaşılmasına olanak tanıyamayacağından emin olmaktır.

Başka bir deyişle, hukuk devleti bakış açısı ile konu, "Araçlar, amaçları haklı çıkarır mı, yoksa çıkarmaz mı?" sorusuna gelir.

Orantılılık aslında somut koşullarda ne anlama gelmektedir? Budapeşte Sözleşmesi'nin içindeki elektronik delillerin toplanmasına ilişkin prosedürel yetkilere atıfta bulunularak birkaç örnek verilebilir:

- Bir ibraz talimatı aynı sonucu verecekse, şüpheliyi belirlemek için telefonunu dinlemeyin;
- İyi tanımlanmış bir disk bölümü kesinlikle yeterliyse, tüm sunucuya elkoymayın;
- Eğer yasa dışı içeriğe ek olarak %80 yasal içerik barındırıyorsa, bir sunucuya (internet) erişimini (IP) engellemeyin;
- Bir şüpheliyi sınırsız bir süre boyunca gizlice dinlemeyin;
- İyi tanımlanmış bir şehir veya bölgeden gelen, önceki aya ait ANPR (Otomatik Plaka Tanıma) verilerinin yeterli olabileceği durumlarda, önceki yıl için ülkenin tamamından gelen tüm ANPR verilerini muhafaza etme talimatı vermeyin;
- Eğer kendisinin ceza gerektiren suçlara karıştığından şüphelenmek için bir neden yoksa, kaynaklarını öğrenmek için bir gazeteciyi dinlemeyin.

7.4 İlkelerin Açıklanması

Ceza kovuşturmalarında deliller değerlendirilirken, elektronik delillerin belgesel deliller için geçerli olanlar ile aynı kural ve kanunlara tabi olduğu unutulmamalıdır. Belgesel delil doktrini şu şekilde açıklanabilir: İbraz edilen delilin, o anda, kolluk kuvvetlerinin eline ilk geçtiği zamandan daha fazla ve daha az olmadığını mahkemeye

gösterme sorumluluğu iddia makamına aittir. İşletim sistemleri ve diğer programlar sıklıkla elektronik depolamanın içeriğini değiştirir ve ona eklemeler yapar. Bu, illa kullanıcının verilerin değişmiş olduğunun farkında olması gerekmeksizin otomatik olarak gerçekleşebilir.

Daha önce Bölüm 6.2 içinde de açıklandığı gibi, mümkün olan her durumda, tüm hedef cihazın bir anlık görüntüsü (kopyası) alınmalıdır. Örneğin anlık görüntüsü alınacak veri miktarı (örneğin büyük veri, …) bunu uygulanamaz hale getirdiğinde, belirli durumlarda kısmi veya seçici dosya kopyalama bir alternatif olarak düşünülebilir. Ancak, bu yaklaşımın benimsenmesi halinde, müfettişler ilgili tüm delillerin ele geçirildiğini gösterebilmelidirler. Bu bağlamda bir seçim yapılacaksa, mahkemede bu konuda ortaya çıkabilecek sorunları öngörebilmek amacıyla iddia makamı (veya hukuk sisteminde varsa soruşturma hâkimi) ile erkenden bir istişare yapılması tavsiye edilir.

Az sayıda vakada, kabul edilen bir anlık görüntü alma cihazı kullanarak bir anlık görüntü elde etmek mümkün olmayabilir. Bu koşullarda, delilleri kurtarmak için orijinal makineye erişim sağlamak gerekli hale gelebilir. Bunu akılda tutarak, mahkemede delil sunmaya yetkili, uygun niteliklere sahip bir dijital delil uzmanının delilleri elde etmesi esastır.

Duruşmada, delilin nesnelliğin yanı sıra sürekliliğin ve bütünlüğünün de gösterilmesi esastır. Ayrıca, delilin elde edilmesini sağlayan her bir süreci göstererek delilin nasıl elde edildiğini göstermek de gereklidir. Deliller, üçüncü bir tarafın aynı süreci tekrarlayabileceği ve mahkemeye sunulan sonuçla aynı sonuca varabileceği şekilde muhafaza edilmelidir. Başka bir deyişle, delil zinciri esastır.

7.5 Açıklama

Her yargı bölgesinin, delillerin savunmaya açıklanmasına ilişkin farklı kuralları ve prosedürleri vardır. Genellikle müfettişin, şüpheliyi veya başka tarafı işaret edip etmediğine bakmaksızın tüm makul soruşturma hatlarını takip etme yükümlülüğü vardır. Kolluk kuvvetleri tarafından ibraz edilen herhangi bir materyalin veya kolluk kuvvetlerinin elinde bulunan üçüncü taraf materyallerinin ilgili saklama süreleri dolmadan silinmesi, açıklanmaya hazır olmamaları halinde, kovuşturma davası için çok kötü sonuçlar doğuracak şekilde usulün ihlali anlamına gelebilir. Uygulamada bu, kolluk kuvvetleri tarafından hazırlanan delillerin, ele geçirilmesinden kovuşturmaya iletilmesine kadar ve tüm yönetim süreci boyunca her zaman eksiksiz bir denetim izi eşliğinde tutulması gerektiği anlamına gelir.

7.6 Kulanılmayan Materyaller

Bazı yargı bölgelerinde, kullanılmayan materyaller, soruşturma ile ilgili olabilecek ve alıkonulmuş ancak sanık aleyhindeki kovuşturma davasının bir parçası olmayan materyallerdir. Açıklama ilkeleri, bir soruşturma sırasında elde edilen diğer materyaller ile aynı şekilde elektronik deliller için de geçerlidir. Hangi materyali ve ne şekilde sorgulamanın makul olduğuna karar vermek müfettişe (veya medeni hukuk sistemlerinde savcı veya soruşturma hâkime) kalmış bir meseledir.

İncelenmemiş herhangi bir materyal, kayıt altına alınan herhangi bir materyale dair muayenenin veya incelemenin kapsamı ve şekli ile ve soruşturmanın bir parçası olarak incelenmemiş olmasına ilişkin bir gerekçe ile birlikte, genel kategoriye göre tanımlanmalıdır. Kullanılması gerektiğine inandığınız verilerden oluşan bir seçim yaparsanız, bu seçimin, söz konusu seçim ile ilgili olarak dahi savunmanın kontrol ve itiraz etme hakkına tabi olduğunu unutmayın. Bu, hukukun üstünlüğünün bir parçasıdır.

Mümkün olduğu durumlarda bilgi veya verilerin iddia makamına orijinal formatında sunulması tercih edilir, çünkü bunların farklı bir formata veya ortama aktarılması birebir kopya oluşturmayacak ve orijinal kalitede bir miktar kayıp meydana gelecektir. Orijinal formattan farklı bir formata yapılacak herhangi bir dönüştürme, kopyanın kalitesinin dikkate alınmasını ve değerlendirilmesini içermelidir. İddia makamı ve mahkeme sisteminin kolayca erişebileceği standart formatlarda delillerin elde edilmesine ve depolanmasına çaba gösterilmelidir. Yerel savcının materyali orijinal veya yerli formatında kolayca görüntüleyemediği durumlarda, incelemeyi kolaylaştırmak veya başka bir formata dönüştürmek için düzenlemeler yapılmalıdır. Savcıların zamanında kararlar alabilmek için delilleri hızlı bir şekilde görebilmelerini sağlamak amacıyla servis anlaşmaları da dahil olmak üzere yerel protokoller geliştirilmelidir.

7.7 Mağdurların ve Tanıkların Himaye Edilmesi

Avrupa İnsan Hakları Sözleşmesi, kamu makamlarının, mağdurların ve tanıkların insan haklarına uyumlu şekilde hareket etmesini gerektirmektedir. Ancak bir yandan bu haklara saygı gösterilmeli, bir yandan da davalının hakları ile dengelenmelidir.

Davadaki deliller bir kovuşturma için gerekçe olarak yeterliyse, mağdurun menfaatleri düşünülmesi gereken önemli bir husustur. Suçun mağdur üzerindeki etkisi dikkate alınmalıdır. Bu, özellikle çocukların istismar edilmesini ve bu tür istismarın dijital görüntüleri ile ilgili kovuşturma olasılığını içeren davalarda önemlidir.

Suça tanık olan birçok kişi, bir suçun soruşturulması sırasında ve sonrasında mahkemeye gidip ifade verirken stres ve korku hissedebilir. Stres, her yaştan tanığın ifadesinin niceliğini ve niteliğini etkileyebilir. Bazı tanıklar; yaşları, kişisel koşulları, tehdit edilme korkusu veya özel ihtiyaçları nedeniyle mahkemeye katılmak ve ifade vermek konusunda belirli zorluklar yaşayabilir. Savunmasız ve gözü korkmuş tanıkların mahkemede en iyi ifadelerini vermelerine yardımcı olmak ve ifade vermekle ilgili stresin bir kısmını hafifletmek için ilave imkanlar sağlanmalıdır.

7.8 Mahkemeye İbraz

7.8.1 Genel Hususlar

Deliller ve elde edilme şekli sorgulanabilir; hazırlıklı olun. Savcılar, delillerin doğru şekilde elde edildiğini, güvenilir olduğunu ve dikkate alınmamaları için yasal bir gerekçe olmadığını mahkemede kanıtlamak zorunda kalabileceklerini unutmamalıdır. Bu nedenle mahkemeye gitmeye hazırlıklı olmak ve delillerin nasıl elde edildiğine

ilişkin olayların mantığını ve yasallığını gösterebilmek önemlidir. Daha da önemlisi, dava mahkemeye sunulmadan önce bile, savunma avukatlarının tartışmalarda çıkarabilecekleri tüm zorluklarla karşılaşmaya hazır olunmalıdır. Tanık olarak çağrılan polis memurlarının ve uzmanların savunma makamının tüm sorularını yanıtlamaya hazır olduğundan emin olun. Delilin kendisine itiraz edilemiyorsa, onu toplayan kişiye ve toplanma şekline itiraz edilebileceğini unutmayın:

- uzman-polis memuru;
- adli bilişim uzmanı.

Savcının sunulan deliller ile ilgili herhangi bir zaaftan veya sınırlamadan haberdar olması çok önemlidir. Savcının deliller ile ilgili her türlü alternatif açıklamayı biliyor olması gerekir.

Savcılar ve hâkimler, savunma avukatları tarafından gündeme getirilen hususlarla başa çıkabilmek için, en azından adli incelemeye ve teknik hususlara ilişkin esasları anlayabilmelidirler. Müfettişlerin, savcıların, savunma avukatlarının, hâkimlerin ve jüri üyelerinin tümünün bilgileri ve teknolojiyi anlaması gerekir. Savcı, bir davada karara bağlanması gereken hususları belirleyemezse ve özellikle de ilgili teknik yönler söz konusu olduğunda davayı basit ve özlü bir şekilde mahkemeye sunamazsa, davalar başarısız olabilir. Savcılar ve müfettişler, özellikle yeni teknolojiler söz konusu olduğunda, soruşturma ve kovuşturma yapmak için eğitimli ve uzman becerileri ve bilgileri ile donatılmış olmalıdır. Savcılar, bilgisayarların ve internet hizmetlerinin nasıl çalıştığını bilmeli, bilirkişi raporlarını anlayabilmeli ve soruşturma konusunda polise tavsiyede bulunabilmeli (ve bazı yargı bölgelerinde yönlendirmeli) ve yetki bölgesinin hem içinde hem de dışında dijital delillerin toplanmasını ve bütünlüğünü, dijital delillere elkonulmasına ilişkin ilkeler uyarınca denetlemelidir.

İyi hazırlanmış bir davanın bazı faydaları vardır; hem savcının hem de müfettişin, baktıkları davanın gerçekte ne olduğunu anlamaları çok önemlidir. Ancak o zaman savcı, mahkemede itiraz edildiğinde delilleri savunabilecektir.

7.8.2 AİHS Madde 6 – Adil Yargılanma Hakkı

Avrupa İnsan Hakları Sözleşmesi'nin 6. maddesi, herkesin adil yargılanma hakkına sahip olması gerektiğini belirlemekte ve bunun ne anlama geldiğini sıralamaktadır.

AİHS MADDE 6: Adil yargılanma hakkı:

1. Herkes davasının, medeni hak ve yükümlülükleriyle ilgili uyuşmazlıklar ya da cezai alanda kendisine yöneltilen suçlamaların esası konusunda karar verecek olan, yasayla kurulmuş, bağımsız ve tarafsız bir mahkeme tarafından, kamuya açık olarak ve makul bir süre içinde görülmesini isteme hakkına sahiptir. Karar alenî olarak verilir. Ancak, demokratik bir toplum içinde ahlak, kamu düzeni veya ulusal güvenlik yararına, küçüklerin çıkarları veya bir davaya taraf olanların özel hayatlarının gizliliği gerektirdiğinde veyahut, aleniyetin adil yargılamaya zarar verebileceği kimi özel durumlarda ve mahkemece bunun kaçınılmaz olarak değerlendirildiği ölçüde, duruşma salonu tüm dava süresince veya kısmen basına ve dinleyicilere kapatılabilir.

2. Bir suç ile itham edilen herkes, suçluluğu yasal olarak sabit oluncaya kadar masum sayılır.

3. Bir suç ile itham edilen herkes aşağıdaki asgari haklara sahiptir:

   a) Kendisine karşı yöneltilen suçlamanın niteliği ve sebebinden en kısa sürede, anladığı bir dilde ve ayrıntılı olarak haberdar edilmek;

   b) Savunmasını hazırlamak için gerekli zaman ve kolaylıklara sahip olmak;

   c) Kendisini bizzat savunmak veya seçeceği bir müdafinin yardımından yararlanmak; eğer avukat tutmak için gerekli maddi olanaklardan yoksun ise ve adaletin yerine gelmesi için gerekli görüldüğünde, resen atanacak bir avukatın yardımından ücretsiz olarak yararlanabilmek;

   d) İddia tanıklarını sorguya çekmek veya çektirmek, savunma tanıklarının da iddia tanıklarıyla aynı koşullar altında davet edilmelerinin ve dinlenmelerinin sağlanmasını istemek;

   e) Mahkemede kullanılan dili anlamadığı veya konuşamadığı takdirde bir tercümanın yardımından ücretsiz olarak yararlanmak.

Kısacası bu, bir kişi hakkında kovuşturma yapıldığında ve bu kişi mahkemede bir hükümle karşı karşıya kaldığında, iddia makamının argümanlarını neye dayandırdığını anlama fırsatına sahip olması ve sunulan delilleri tartışma imkanına sahip olması gerektiği anlamına gelir. Kişi bilgilendirilmeli, savunmasını hazırlamak ve sadece tanıklara değil, aleyhindeki tüm delillere de itiraz etmek için gereken zamana ve olanaklara sahip olmalıdır.

7.8.3 Mahkemede Deliller Nasıl Sunulmalı

Duruşma stratejisine ilişkin esasları izlediğiniz zaman bile, hala mahkeme salonundaki herkesin aynı teknolojik uzmanlık düzeyini paylaşmadığını aklınızda bulundurmalısınız.

Davaya ve (elektronik) delillere ilişkin "bir resim çizin" ve aşağıdakileri yapmayı dikkate alın:

- Adım adım ilerlemek;
- Herkesin bilişim uzmanı olmadığını hatırlamak;
- Seviyeyi yükseltmek; aptallar için internetten yüksek teknolojiye;
- Her adımı kanıtlamak;
- Olayların mantığını göstermek.

Davanızı sunmaya başladığınızda, delillerinizi oluşturmalısınız; delilleri hâkime veya jüriye göstermeden önce her adımı belgelediğinizden ve olayların mantığını gösterdiğinizden emin olun. Adli bilimi basit dile tercüme edebilecek uzman tanıklar çağırmayı düşünün. Önce temel bilgileri açıklayın (belki bir PowerPoint sunumu veya bir sözlük kullanın) ve sonra zor adli konulara girin (hâkim bir IP adresinin ne anlama geldiğini bilmediğinde, onu ileri teknoloji deliller konusunda ikna etmeye çalışmanın hiçbir faydası yoktur).

7.8.4 Sunum Yöntemleri

Sunum; avukatların, hâkimlerin ve sistemde varsa jürinin, uzman delillere hak ettiği önemi vermesi bakımından önemlidir. Elektronik delillerin mahkemeye sunulması; bilgisayar gösterimleri, video gösterimi, bilgisayar grafikleri, çizelgeler ve tablolar kullanılarak görsel olarak yapılırsa daha etkili olur. Ancak savcılar, bu tür teknoloji kullanımının neden olabileceği önyargının farkında olmalı ve savunmanın bu tür teknoloji kullanılmasına itiraz etmesi halinde bu hususları yetkin bir şekilde tartışmaya hazır olmalıdır.

Araştırmalarla, birçok insanın duyduklarından ziyade gördüklerine dikkat ettiği bulunmuştur. Bir savcının görevi, savcılığın iddiasını mümkün olan en iyi şekilde ortaya koymak olduğundan, özellikle karmaşık davalarda delillerin görsel olarak sunulması tavsiye edilir.

Vakayı "hazır lokma" hale getirmek için bir PowerPoint sunumu yapmayı düşünün, tüm teknik ve özel terimlerin tanımlandığı bir kelime dağarcığı veya sözlük sunun, hikayeyi okunabilir kılmak için vakanın bir özetini sunun ve nihai olarak delilleri gösterin. Ayrıca, mahkemedeki herkes için bir temel standart oluşturmak adına davayla ilgili elektronik delil/teknoloji hakkında kısa bir açıklama yapmayı da düşünün.

Bu sunum araçlarının çoğu ilk başta zaman açısından çok büyük bir yatırım gibi görünebilir ancak farklı yargılamalarda yeniden kullanılmaları mümkün olacaktır. Örneğin, bir kelime dağarcığı birçok bilişim suçu vakasında ve davasında hizmet edebilir. Ayrıca, kimlik avı, tuş kaydediciler veya botnetler gibi bilişim suçlarının en yaygın yönleri hakkında bir PowerPoint sunumuna veya hazır bir elektronik delil açıklamasına sahip olmak her zaman yararlı olacaktır.

Elektronik delillere nasıl elkonulduğuna ve nasıl analiz edildiklerine ilişkin görsel sunumlar da çeşitli durumlarda kullanışlı olacaktır. Bu tür sunum tekniklerini geliştirmenin temsil ettiği uzun vadeli yatırımı anlamak önemlidir.

8 Yetki Bölgesi ve Sınır Ötesi Elektronik Delil Toplama

8.1 Bilişim Suçlarının Uluslararası Boyutu

Ağ ile bağlı dünyada, ulusal sınırların bilişim suçluları için kolaylık sağladığı, ancak ceza yargılamasını kısıtladığı söylenebilir. İnternet üzerinde suçlular "sanal olarak" kıtalar arasında istedikleri gibi gezebilmektedir. Her ne kadar bir bilişim suçu müfettişi için birden fazla yasal yargı bölgesi ile ilişki içinde olması kural olmasına rağmen, bir suça dair delileri ararken kendisi aynı hareket özgürlüğünden yararlanamamaktadır. Bir kolluk görevlisinin kendi ülkesi dışında yasal olarak soruşturma yürütebileceği durumlar ("bulutta" depolanan deliller de dahil olmak üzere) ulusal hukuka ve müfettişin mensubu olduğu devletin katıldığı Karşılıklı Adli Yardım çerçevelerine bağlı olarak çok farklı olabilir.

Fiziksel olarak yargı bölgesi içerisinde olmayan elektronik deliller ile uğraşılırken ayırt edilmesi önemli olan iki grup koşul vardır:

1. Bir müfettişin internete bağlı bir bilgisayarın kontrolünü ele geçirdiği durumlar. Bu gibi durumlarda, müfettişin web sitelerine tıklama veya diğer yargı bölgelerinde bulunan bilgisayarlara girme yetkisi olabilir. Bunu yapma yetkisi, iç hukuk veya iç hukuk ile Budapeşte Bilişim Suçları Sözleşmesi'nin 32. Maddesi hükümlerinin bir birleşimine istinaden müfettişe verilebilir. (Ancak, gerçek sunucuların veya bilgisayarların fiziksel olarak bulunduğu ülke başka bir görüş benimseyebilir).

2. Elektronik delilin "bulut" içinde bulunduğu, yani örneğin bir şüphelinin e-postalarının evindeki bilgisayarında saklanmadığı, ancak yabancı bir yargı bölgesinde bulunan ayrı bir sabit disk üzerinde başka bir yerde saklandığı durumlar.

Bu iki gruba ayrılmış koşullar arasındaki farkı anlamak önemlidir çünkü soruşturma makamlarının geçerli olan yasalara bağlı olarak her bir durumda farklı adımlar atmaları gerekecektir.

8.2 Uluslararası Adli İşbirliği Ağları

Bilişim suçlarına karşı uluslararası alanda çeşitli önlemler alınmıştır. Bunların en önemli olanları arasında; Interpol, Avrupa Konseyi ve Avrupa Birliği tarafından sağlanan gelişmeler (7/24 İrtibat Noktası Ağı, Europol, Eurojust, EJCN (Avrupa Adli Bilişim Suçları Ağı)[135]

[135] EJCN, 9 Haziran 2016 tarihli ve 10025/16 sayılı Konsey Kararı ile uzmanlık ve en iyi uygulama paylaşımını kolaylaştırmak, bilişim suçları, bilişim destekli suçlar ve siber uzaydaki soruşturmalar ile uğraşırlarken yetkili adli makamlar arasındaki işbirliğini geliştirmek ve siber uzayda hukukun üstünlüğünü sağlamaya yönelik diyaloğu teşvik etmek amacıyla kurulmuştur. EJCN yılda iki kez Lahey'deki Eurojust tesislerinde toplanmaktadır. EJCN üyeleri, mesleki uzmanlık ve deneyimlerine dayalı olarak ağın toplantılarına ve diğer faaliyetlerine katkıda bulunmaktadır. Avrupa Birliği Konseyi, Avrupa Komisyonu, Eurojust, Europol'ün Avrupa Bilişim Suçları Merkezi ve Avrupa Yargı Ağı, EJCN'nin gözlemcileridir.

Eurojust, toplantılar düzenlemeyi, ağın kısıtlı erişimli web sitesini korumak, Kurulun günlük faaliyetlerini kolaylaştırmak ve EJCN'nin çalışma programının uygulanmasına yardımcı olmak da dahil olmak üzere ağa destek sağlamakla görevlendirilmiştir. Faaliyetlerin sürekliliği gayri resmi bir Başkanlık Kurulu tarafından izlenir. EJCN ile

ve EJN (Cezai Konularda Avrupa Adli Ağı)) yer almaktadır. Bu grupların kaynakları, ceza hukuku sistemindeki farklı oyunculara soruşturma veya kovuşturmalarda yardımcı olmak için kullanılabilir.

8.3 Karşılıklı Adli Yardımlaşma ve Sınır Ötesi Elektronik Delil Toplama

8.3.1 Karşılıklı Adli Yardımlaşma

Uzun bir zamandır, bir egemen devletin başka bir egemen devletten yasal konularda yardım isteyebildiği resmi bir çerçeve bulunmaktadır. Bu işbirliğinin en bilinen yasal dayanağı, karşılıklı yardımlaşmayı sağlayan Karşılıklı Adli Yardımlaşma (MLA) Antlaşmaları ve çok taraflı Sözleşmelerdir (örneğin ceza meselelerinde karşılıklı adli yardımlaşmaya ilişkin Avrupa Sözleşmesi, Birleşmiş Milletler Sınıraşan Örgütlü Suçlar Sözleşmesi gibi).

Sınır ötesi yardım talepleri, internet hizmetlerinin uluslararası niteliği nedeniyle elektronik deliller içeren davalarda özellikle önemlidir. Bu davalardaki asıl zorluk, delillerin değiştirilmesini veya silinmesini önlemek için yeterince hızlı hareket edebilmektir, ancak geleneksel uluslararası işbirliği biçimleri yavaş ve hantaldır ve böyle bir talebin başarısı genellikle hem talep eden hem de talepte bulunulan makamların iyi niyetine ve uzmanlık düzeyine bağlıdır. Delillerin zaman açısından kritik durumlarda değiştirilmesinin veya silinmesinin önlenmesi hususunu çözmenin bir yolu, Budapeşte Sözleşmesinin 29 ve 30. maddelerinde ortaya koyulan verilerin ivedilikle korunmasıdır. Sözleşme Tarafları, başka bir taraftan verilerin ivedilikle korunmasını istemek için 7/24 irtibat noktalarını kullanabilmektedirler (Madde 35).

Kabul edilmelidir ki, elektronik delillerin ivedilikle korunmasını veya bunlara elkonulmasını gerektiren çoğu durumda, MLA oldukça hantal ve zaman alıcı olarak algılanmaktadır.

Bununla birlikte, Budapeşte Sözleşmesi ve 17 Kasım 2021 tarihinde kabul edilen İkinci Ek Protokolü, elektronik delillerin hızlı, yaratıcı ve verimli bir şekilde sınır ötesi elde edilmesini sağlayan çok sayıda yasal araç içermektedir.

Elektronik delil kılavuzunun öncelikle teknik ve adli bir açısı olmasına rağmen, elektronik delillerin sınır ötesi toplanmasına ilişkin Budapeşte Sözleşmesi araç kutusunun temel araçlarını listelemek ve kısaca açıklamak yerinde olacaktır. Bu bağlamda, aşağıdaki başlıklara bakınız.

8.3.2 MLA ve Elektronik Delillerin Sınır Ötesi Toplanmasına İlişkin Yasal Çerçeve

Bir dava birden fazla yargı bölgesi içerdiğinde, her bir yargı bölgesinin maddi hukuku dikkate alınmalıdır. Bu karmaşık bir alan olabilir ve bazen tek bir yargı alanındaki

yazışmalar için e-posta adresi ejcn@eurojust.europa.eu'dur.
https://www.ejn-crimjust.europa.eu/ejn/PartnersDetail/EN/24

tek bir soruşturma ekibinin öncülük etmesine izin verilmesine karar verilir. Diğer yargı bölgelerindeki ilgili kurumlar, lider soruşturma kurumu ile işbirliği yapmayı ve kendi yargı bölgelerinde ilgili delilleri güvence altına almayı kabul edeceklerdir.

8.3.2.1 Budapeşte Sözleşmesi

8.3.2.1.1 Budapeşte Sözleşmesi'nin benzersizliği

Budapeşte Sözleşmesi bir takım uluslararası işbirliği araçları içermektedir. Bunlardan bazıları diğer uluslararası sözleşmelerle ortaktır. Ancak diğer hükümler çok yenilikçidir ve bu tür hükümler başka hiçbir küresel anlaşmada yer almadığından fark yaratmaktadır. Bunlar, örneğin depolanan bilgisayar verilerinin ivedilikle korunması, korunan trafik verilerinin ivedilikle açıklanması, depolanan bilgisayar verilerine erişim ile ilgili karşılıklı yardım veya trafik verilerinin ve içerik verilerinin gerçek zamanlı toplanmasında karşılıklı yardım ile ilgili özel hükümleri içermektedir.

Diğer uluslararası anlaşmalarla ortak olan hükümlerin kapsamı, aralarında belirli bir uluslararası işbirliği anlaşması olmayan Devletler arasındaki işbirliğini kolaylaştırmaktır.

Sözleşme, genel bir MLA anlaşması olmasa da, ülkelerin işbirliği yapmasına imkan tanımak amacıyla, karşılıklı adli yardımlaşmaya ilişkin genel kurallar öngörmektedir. Tarafların, bilgisayar sistemleri ve verileri ile ilgili ceza gerektiren suçlara ilişkin soruşturma veya kovuşturma amacıyla veya ceza gerektiren bir suça dair delillerin elektronik ortamda toplanması amacıyla mümkün olan en geniş ölçüde işbirliği yapacaklarını ifade eden uluslararası işbirliğine ilişkin genel ilkeler, Sözleşme›nin 23. maddesi içinde düzenlenmiştir. Ayrıca, geçerli uluslararası anlaşmaların olmadığı durumlarda, karşılıklı yardımlaşma isteklerine ilişkin eksiksiz bir dizi prosedür, Sözleşme›nin 27. maddesinde tanımlanmıştır. Beş kıtadan çok çeşitli hukuk kültürlerine mensup Tarafları bir araya getiren Budapeşte Sözleşmesi gibi küresel bir belgede bu özellikle önemlidir.

Sözleşme'nin 27. maddesinde öngörülen bir dizi kurala rağmen, bu hüküm ilke olarak uygulanmayacaktır. Sadece Sözleşme'nin 25. maddesine göre, istekte bulunulan Tarafın hukukunda veya geçerli karşılıklı yardım anlaşmalarında diğer hükümlerin olmaması durumunda geçerlidir. Aslında Budapeşte Sözleşmesi'nin karşılıklı adli yardıma ilişkin genel kurallarının amacı, diğer antlaşmalarla rekabet içinde evrensel düzeyde uygulanmak değildir. Sözleşme'nin 27. maddesinde yer alan bu kurallar, yalnızca diğer bağlayıcı uluslararası belgelerin eksikliklerini ve hatta yokluklarını gidermek için uygulanacaktır. Bu nedenle, sadece önceden var olan diğer belgeler için tamamlayıcı niteliktedirler.

Bununla birlikte, Budapeşte Sözleşmesi'nin özellikle bilişim suçlarına ek olarak elektronik delilleri de kapsayan tek anlaşma olduğunu unutmamalıyız. Bu, Budapeşte Sözleşmesi'nin belirli araçlarının, elektronik delillerin sınır ötesi de dahil olmak üzere toplanmasına özel olarak uyarlandığı anlamına gelir. Dolayısıyla, ülkelerin sınır ötesinde elektronik delil toplamak için bu özel araçlara ne ölçüde sahip olduklarının değerlendirilmesi çok önemlidir. Ve bu nedenle, elektronik delillerin toplanması ile ilgili oldukları için bu belirli araçlara özellikle odaklanılacaktır.

8.3.2.1.2 *Budapeşte Sözleşmesi uluslararası işbirliği ve sınır ötesi elektronik delil toplama araç kutusu*

Budapeşte Sözleşmesinin 3. Bölümü uluslararası işbirliğine ayrılmıştır. İadeye ilişkin 24. madde, elektronik delillerin (sınır ötesi) toplanmasının ve MLA işlemlerinin odak noktasının dışında kaldığı için bu raporda dikkate alınmamıştır.

Bölüm 3 kapsamında sağlanan araçların bir kısmı, kaçınılmaz olarak klasik karşılıklı adli yardımlaşmanın konusudur ve ilke olarak, istekte bulunan devletten, delillerin alınması gereken, istekte bulunulan devlete klasik bir karşılıklı adli yardımlaşma isteği haricinde sınır ötesi uygulanamaz. Bununla birlikte Budapeşte Sözleşmesi, MLA sürecinden geçmek zorunda kalmadan hızlı bir şekilde sınır ötesi delil toplanmasını sağlayabilecek araçlar da sunmaktadır. Ayrıca, Budapeşte Sözleşmesi'nin 2. Bölümünün 2. Kısmında (ulusal usul hukuku) ortaya koyulan ve yerel tedbirler olmalarına rağmen, tartışılmaz bir bölge dışı etkileri ve erişimleri olan veya olabilecek usule ilişkin yetkiler de vardır. Bunları aşağıda açıklayacağız.

İlke olarak bir MLA isteği yoluyla kullanılması gereken usule ilişkin yetkiler, 31. madde (Depolanmış bilgisayar verilerine erişim konusunda karşılıklı yardımlaşma), 33. madde (Gerçek zamanlı trafik verilerinin toplanmasına ilişkin karşılıklı yardımlaşma) ve 34. madde (İçerik verilerinin ele geçirilmesine ilişkin karşılıklı yardımlaşma) içinde ortaya koyulan yetkilerdir.

Ancak, depolanan bilgisayar verilerine erişimle ilgili olarak (Madde 31), bu depolanan bilgisayar verileri, içerik verilerini değil de, temel abone bilgilerini veya trafik verilerini ilgilendirdiği ölçüde, hizmet sağlayıcılarla kamu-özel işbirliği, MLA prosedüründen geçmek zorunda kalınmadan da bu verilerin sınır ötesi elde edilmesini mümkün kılabilir. Yabancı hizmet sağlayıcılarla bu kamu-özel doğrudan işbirliği kanalları en iyi haline getirildiği ölçüde, bu durumun sınır ötesi delil toplama hızı üzerinde katlanarak artan olumlu bir etkisi olduğunu söylemeye bile gerek olmadığı açıktır.

Bununla birlikte, trafik verilerinin gerçek zamanlı toplanması ve içerik verilerinin ele geçirilmesi, MLA durumu dışında neredeyse hiçbir zaman açıklamaya tabi olmayacaktır. Göz önünde bulundurulabilecek bir istisna, yakın tehdit acil durum prosedürlerine ilişkin istisnadır.

Özellikle dikkatimizi çeken şey, *tüm MLA sürecinden geçmek zorunda kalmadan sınır ötesi elektronik delil elde etmeyi mümkün kılan araçlardır*. Doğru kullanıldığında, bunun sınır ötesi delil toplama hızını en üst düzeye çıkardığını söylemeye bile gerek olmadığı açıktır.

- **Madde 26 - Talep olmadan (kendiliğinden) sunulan bilgi**

Madde 26, "karşılıklı yardımlaşmaya ilişkin genel ilkeler" hakkındaki Başlık 3 çerçevesinde yapılandırılmıştır, ancak elektronik delillerin sınır ötesi elde edilmesi için son derece güçlü bir araç ve yasal temel olabileceği için ve bu nispeten gayri resmi bir şekilde olabileceği için özel olarak ilgi gösterilmeyi hak etmektedir. Burada gayri resmi ile, idari iş yükünün az olması ve neredeyse yerine getirilmesi gereken hiçbir resmi koşul olmaması kastedilmektedir.

Bir Tarafın yetkili makamları, bir iç soruşturma kapsamında, elde ettikleri bilgilerin bir kısmının başka bir Tarafın yetkili makamlarına iletilmesi gerektiğini keşfettikleri za-

man, herhangi bir resmi karşılıklı yasal yardım talebi olmaksızın, elektronik delilleri göndermek için mükemmel bir araç olan 26. madde uygulanabilir. Gönderilen bilgiler mahkemede kabul edilebilir deliller olarak kullanılabilir.

Söz konusu bilgiler, Sözleşme uyarınca belirlenen veya ((başka) herhangi bir Devletten) uluslararası işbirliği talebine yol açabilecek ceza gerektiren suçlara ilişkin *bir soruşturmanın başlatılması veya geliştirilmesi için* faydalı veya gerekli görülürse, bu kendiliğinden bilgi paylaşımı yapılabilir.

Madde 26.2'ye göre, bu bilgi paylaşımı, gizliliğe ve bu bilgilerin üçüncü taraflarca kullanımına ilişkin belirli koşullara tabi olmak kaydıyla yapılabilir.

Madde 26'nın sınır ötesi elektronik delillerin aktif olarak alınmasına veya paylaşılmasına yönelik bir araç olması konusunda algılanan bir farkındalık ve kullanım eksikliği söz konusudur. Ülkeler arasında yapılan istişareler, şu ana kadar 26. maddenin, resmi MLA talepleri olmaksızın bir aktif karşılıklı adli yardım başlatma imkanı olarak esaslı bir şekilde araştırılmadığını göstermektedir. Daha ziyade, başka bir ülke için önemli olabilecek eldeki bilgileri aktarmak için proaktif olmayan bir araç olarak kullanılmış ve öyle kabul edilmiştir.

Ancak, 26. maddenin ustaca kullanılması sayısız MLA talebini önleyebilir. Örneğin, ulusal (bu durumda genellikle uluslararası bir boyuta da sahip olan) soruşturmalarında benzer menfaatleri olan ülkeler ile elektronik delillerin paylaşılmasına ilişkin bir yasal dayanak olarak 26. madde önemli bir rol oynayabilir. Bu durumda, A ülkesinin adli makamı, soruşturmasından elde edilen bilgiyi, bu bilginin B ülkesiyle ilgili olduğu ölçüde B ülkesiyle paylaşabilir ve B ülkesi de A ülkesi için aynısını yapabilir. Yetkili adli makamın söz konusu bilgiyi Budapeşte Sözleşmesinin 26. maddesi uyarınca paylaşmak istediğini belirtmesiyle, bu bilgi basitçe herhangi bir yolla (posta, posta, faks, vb.) aktarılabilir veya paylaşılabilir. Bunu yaparken A ve B ülkeleri, 26. maddenin 2. paragrafını uygulayabilir veya uygulamayabilir ve örneğin önceden istişare edilmeden veya izin alınmadan bilgilerin (henüz) adli amaçlarla kullanılmaması veya önceden izin alınmadan bilgilerin üçüncü bir ülkeye aktarılmaması gibi belirli koşullar getirebilir. Bu sınırlar içinde, aktarılan bilgiler ilke olarak mahkemeler huzurunda kabul edilebilir elektronik deliller olarak kullanılabilir. Söz konusu bilgilerin adli bakımdan kabul edilebilirliğinin, bilgileri alan ülkenin ulusal delil rejimine ve mevzuatına bağlı olacağını söylemeye bile gerek olmadığı açıktır. Nispeten serbest bir delil rejimine sahip ülkelerde, bilgiler genellikle MLA taleplerine veya yetkilendirmelerine gerek kalmadan kabul edilebilir deliller olarak kullanılabilir. Bu fırsatlar her ülke tarafından araştırılabilir ve değerlendirilebilir.

Hatta bazı koşullarda ve hukuken gerekçelendirilmesi durumunda, A ülkesinin B ülkesinde ve *B ülkesinin A ülkesinde* yapılmasını istediği her soruşturma işlemi için resmi bir MLA talebi gerektirmeden, A ülkesindeki ve B ülkesindeki ikiz soruşturmalardan kendiliğinden bilgi alışverişine olanak tanıyan adli çerçeveyi oluşturmak için ikiz soruşturmalar açılması bile düşünülebilir. A ülkesinin adli makamı ile B ülkesinin adli makamı arasında iyi bir doğrudan temas, işbirliği ve bilgi alışverişi elbette bu durumda çok önemlidir, fakat aynı zamanda da yeterlidir. Bu durumda, sürekli gelen ve giden MLA taleplerinden kaçınmak mümkün olabilir.

Yukarıda da belirtildiği gibi, Budapeşte Sözleşmesi'nin 26. maddesi kapsamındaki bilgi paylaşımı katı resmi koşullara tabi değildir. Uygulamada bu, A ülkesinin adli maka-

mının B ülkesinin adli makamına "ekli bilgilerin Budapeşte Sözleşmesinin 26. maddesi uyarınca iletildiğini" teyit ettiği bir e-posta şeklini bile alabilir. Ancak, iki ülke arasında iki farklı soruşturmada 26. maddenin uygulanmasını bir belge içinde teyit etmek de bazen faydalı olabilir veya istenebilir ve bu belge daha sonra her iki ulusal soruşturmaya da eklenebilir. Bilgilerin aynı soruşturmalar içinde birden çok kez ve sıklıkla paylaşılması gerektiğinde bu husus özellikle yararlı olacaktır; o durumda 26. madde uyarınca her paylaşım yapıldığında bu işlemin tekrar edilmesi gerekmeyecektir.

26. maddenin bu şekilde kullanılmasının büyük ölçüde ulusal mevzuata ve ulusal delil rejimine bağlı olacağı açıkça tekrarlanmalıdır, ancak kendiliğinden paylaşılan bilgilerin ardından karşılıklı yardım taleplerinin gelmesi gerekliliği hiçbir şekilde olağan durum olmamalıdır. Ulusal hukuk, 26. madde uyarınca kendiliğinden alınan bilgilerin adli kullanımına açık bir şekilde karşı çıkmıyorsa, ilke olarak bu bilgiler bir MLA olmaksızın kabul edilebilir şekilde kullanılabilir.

- **Madde 29 ve 30 – Hızlandırılmış muhafaza ve açıklama**

Elektronik deliller ve veriler ile ilgili sorunlardan biri oldukça değişken olmalarıdır. Bir düğmeye basılarak silinebilirler. Açıkçası, başka bir ülkede bulunan verilere ihtiyaç duyulursa, verileri almak için bir karşılıklı adli yardım talebi gönderilmeden önce veriler halihazırda kaybolmuş olabilir. Budapeşte Sözleşmesi, resmi bir adli yardım talebi beklentisiyle, her türlü verinin çok hızlı ve nispeten gayri resmi bir şekilde sınır ötesi dondurulmasına olanak tanıyan bir araç sağlamaktadır. Bu aynı zamanda "hızlı dondurma" olarak da anılır ve Madde 29'da (depolanan bilgisayar verilerinin hızlandırılmış muhafazası) yer alır.

Talepte bulunulan taraf, talep edilen verileri kendi ulusal kanunlarına göre muhafaza etmek için gereken tüm özeni göstererek hareket etmelidir. Hızlı dondurma talebi, esas olarak ilgili ülkelerin 7/24 irtibat noktaları (POC'ler) aracılığıyla yapılır. Bu 7/24 POC'ler, gerekli verilerin standart bir şekilde ve asgari düzeyde formalite ile dondurulmasına ilişkin talepler için genellikle standart formlara sahiptir.

Verilerin dondurulmasının, otomatik olarak verilerin açıklanmasının sağlanacağı anlamına gelmediğini anlamak çok önemlidir. Bu, müdahaleci olmayan, düşük bir eşiğe sahip geçici bir önlemdir. Buna göre veriler, söz konusu verilerin aktarılmasının istendiği bir adli yardım talebi alınıncaya kadar en az 90 günlük (yenilenebilir) bir süre boyunca saklanacaktır. Dolayısıyla Madde 29, karşılıklı yardımlaşma önlemleri uygulanırken verilere varlığını güvence altına almaya yönelik bir mekanizma sağlamaktadır.

Yani Madde 29 kendi içinde elektronik delillerin doğrudan toplanmasına yönelik bir araç değil, sadece elektronik delillerin muhafaza edilmesine yönelik bir araçtır. Bu nedenle, 29. maddenin uygulanmasının ardından ilke olarak bir MLA (veya mümkünse doğrudan kamu-özel işbirliği) talep edilmelidir. Ancak, trafik verilerinin dondurulması istendiğinde, 30. maddenin (korunan trafik verilerinin hızlandırılmış olarak açıklanması) koşulları karşılanıyorsa, MLA talebinde bulunmaya gerek kalmadan hızlandırılmış açıklama elde etmek mümkündür. Bir Devlet bir hızlı dondurma talebi aldığında ve talep edilen Devlet, korunan trafik verilerinin, iletişimin iletiminin üçüncü bir Devlet içindeki bir hizmet sağlayıcı veya talep eden Devletin kendisi aracılığıyla yönlendirildiğini ortaya çıkardığını gördüğünde, muhafaza edilen bu tür trafik verilerini hızlı bir şekilde açıklamalıdır. Açıklama çok dar ve sınırlıdır, ancak ilgili hizmet sağlayıcıyı/sağlayıcıları ve iletişim yolunu belirlemek için yeterli miktarda veri içermelidir.

Temel olarak, aşağıdaki sonuça varılacaktır: Talep edilen Devlet bir dondurma işlemi yaparsa ve bunu yaparken dondurulan verilerin, talep eden Devletin dondurma işlemini yapan ülkeden başka bir ülkeye adli yardım talebi göndermesinin daha iyi olacağını gösterdiğini tespit ederse, dondurma işlemini yapan ülke, talepte bulunan ülkenin aranan bilgileri başka bir ülkeden doğrudan (adli yardım yoluyla) talep etmesine olanak tanıyacak gerekli verileri derhal açıklayacaktır. Bu, kritik bir zaman ve çaba tasarrufu sağlar.

- **Madde 32 – İzin ile veya kamuya açık olduğu durumlarda depolanmış bilgisayar verilerine sınır ötesi erişim**[136]

Polisin ve yargının, diğer bir ülkedeki sunucularda saklanan verileri, söz konusu diğer ülkeye adli yardım talebinde bulunmaksızın elde etme ve kullanma yetkisinin olup olmadığı da sorulabilir.

Budapeşte Sözleşmesi'nin 32. maddesi, ceza hukuku makamlarına, fiziksel olarak başka bir Tarafın topraklarında bulunan bir bilgisayarda saklanan delilleri elde etme imkanı vermektedir. Bu prosedür, uluslararası işbirliğine ilişkin herhangi bir resmi talep gerektirmemektedir. Ancak bu, açık kaynak bilgilerle veya açık kaynak değilse, yasal olarak bu verilere erişim sağlamaya yetkili kişinin yasal ve gönüllü izni ile elde edilen veriler ile sınırlıdır.

Yurtdışında depolanan verilere erişim, bu durumlarda verilerin depolandığı ülkenin izni olmadan gerçekleştirilebilir; bu da, Taraflar arasında karşılıklı yardım talebi gerektirmediği ve diğer tarafa bildirimde bulunulmasını gerektirmediği (Tabii ki bu, Tarafın gerekli gördüğü herhangi bir bildirimi içermez) anlamına gelir.

Madde 32.a'da da bahsedildiği gibi, "kamuya açık" ifadesi esasen açık kaynaklı araştırma/istihbarat (OSINT) anlamına gelir ve www (dünya çapında web) üzerinden edinebileceğiniz her şeyin, internetteki belirli alanları özel veya yarı özel kılan erişim engellerini aşmanıza gerek kalmadan, kabul edilebilir delil olarak internetten çekilip alınabilmesinin mümkün olduğu gerçeğine indirgenir. Web sitesinin belirli bir bölümü kamuya kapalıysa, o zaman kamuya açık değildir. Bu bağlamda, verilerin coğrafi konumu (biliniyor veya tespit edilebiliyor ise) önemli değildir.

Madde 32.b, ceza hukuku makamlarına, fiziksel olarak başka bir Tarafın topraklarında bulunan bir bilgisayarda depolanan delilleri elde etme imkanını vermekle birlikte, bu husus, bu verilere erişim vermeye yasal olarak yetkili kişinin yasal ve gönüllü izni ile elde edilen verilerle sınırlıdır. Ancak, istenen veriler Budapeşte Sözleşmesine Tarafı başka bir ülkenin topraklarında depolanmıyorsa, Madde 32.b'nin kullanılamayacağı belirtilmelidir. Aynı durum, verilerin saklandığı yer belirsizse veya bilinmiyorsa da meydana gelebilir.[137]

---

[136] Verilere sınır ötesi erişime ilişkin 3 Nolu T-CY Yönlendirme Notuna bakın (Madde 32): https://www.coe.int/en/web/cybercrime/guidance-notes

[137] Bununla birlikte, "konumun kaybedilmesinin" benimsenmesi ve bulut verilerinin ve bulut bilişimin katlanarak artan kullanımı ışığında bu artık konum olarak inandırıcı değildir. Verilere sınır ötesi erişime ilişkin 3 Nolu T-CY Yönlendirme Notu (Madde 32), verilerin başka bir Tarafta depolanıp depolanmadığının bilinmediği veya kesin olmadığı durumlarda, bir aramanın veya diğer erişim türlerinin meşruiyetini, iç hukuk, ilgili uluslararası hukuk ilkeleri veya uluslararası ilişkiler mülahazaları ışığında Tarafların kendilerinin değerlendirmesi gerekebileceğini açıklamaktadır:

https://www.coe.int/en/web/cybercrime/guidance-notes

Gereken izin ile ilgili olarak, izin veren kişi zorlanmamalı veya aldatılmamalıdır. İzin verme ehliyeti ulusal yasalara bağlıdır. Ancak genel olarak reşit olmayanlar veya ruh sağlığı bozuk olan kişiler izin veremezler. Ayrıca, genellikle (yazılı olarak ve veriye erişmeden önce) açık bir iznin gerekli olduğu da dikkate alınmalıdır. Ayrıca, çevrimiçi hizmet sağlayıcıların genel hüküm ve koşullarına ilişkin bir mutabakatın, kolluk kuvvetleri tarafından bir veriye elkonulmasının kabul edildiğini varsaymak için yeterli olmayabileceği de belirtilmelidir. Bu husus büyük ölçüde, verileri açıklamak için yasal yetkiye sahip kişi olarak kabul edilebilecek olan Tarafın koşullarına, kanunlarına ve düzenlemelerine bağlıdır. Bu arada, hizmet sağlayıcılar genellikle kullanıcı verilerini tutarlar, ancak onlara sahip değillerdir/onları kontrol etmezler ve bu nedenle, kullanıcı verilerinin açıklanması bakımından geçerli bir izin verebilecekleri düşünülmemelidir.

Madde 32'nin amaçları açısından, elektronik delilin başka bir ülkede bulunup bulunmadığının bir önemi yoktur, bu durumda, Madde 32.b istisna olmak kaydıyla, ilke olarak verilerin en azından Budapeşte Sözleşmesine Taraf olan ülkelerden birinde bulunabileceğinin tespit edilmesi mümkün olmalıdır.

Ancak bu noktada, verilerin kamuya açık olmaması ve şüphelinin verilere erişim konusunda gönüllü olarak izin vermemesi durumunda, bununla nasıl başa çıkılacağı sorulabilir. Eğer verilerin başka bir konumda olduğu, ancak yine de kendi topraklarında bulunduğu belirlenebilirse herhangi bir sorun kalmaz çünkü o zaman bu özel durumun ele alındığı Madde 19.2 kapsamına girer.

- **Madde 19.2 – Depolanan bilgisayar verilerine ilişkin genişletilmiş arama ve elkoyma**

Madde 19.2 esasen bir arama sırasında bir bilgisayar sisteminde arama yapılır ve aranan verinin *kendi topraklarında bulunan* başka bir bilgisayar sisteminde veya bir parçasında depolandığına ve bu verilerin ilk sistemden yasal olarak erişilebilir veya kullanılabilir olduğuna inanmak için sebepler olursa, arama veya benzeri erişim diğer sisteme hızlı bir şekilde genişletilebilmelidir.

Temel soru, diğer bilgisayar sistemindeki verilerin nerede depolandığının bilinmediği (ve kamuya açık olmadığı ve verilere erişmek için yasal ve gönüllü iznin olmadığı) durumla nasıl başa çıkılacağıdır. Gerçek hayattan çok pratik ama çok çarpıcı bir örnek: Terör olayında arama yapıldığında bir bilgisayar açık bulunsa ve ekranda bir bulut depolama uygulamasının açık olduğu görülse, ilk bakışta halihazırda gerçekleştirilmiş veya belki de henüz gerçekleştirilmemiş saldırılarla ilgili önemli deliller mevcut gibi görünse, aramayı yapan bu verilerin kendi bölgesindeki bir sunucuda depolandığından emin değilse, aramayı durdurmasının gerekip gerekmedi sorusu ortaya çıkmaktadır.

Budapeşte Siber Suçlar Sözleşmesi'nin açıklayıcı raporu, 32. maddenin yorumlanması hakkında yorum yaparken, 293. paragrafında bu duruma ışık tutmaktadır: *"Bir Tarafın, karşılıklı yardımlaşma istemeden tek taraflı olarak başka bir Tarafta depolanan bilgisayar verilerine erişimine ne zaman izin verileceği, Sözleşme taslağını hazırlayanların uzun uzadıya tartıştığı bir konuydu. Devletlerin tek taraflı olarak hareket etmesinin kabul edilebilir olacağı ve olamayacağı durumlar ayrıntılı olarak ele alındı. Taslağı hazırlayanlar sonunda, bu alanı düzenleyen kapsamlı, yasal olarak bağlayıcı bir rejim hazırlamanın henüz mümkün olmadığına karar verdiler. (…) Daha fazla deneyim elde edilinceye ve bunların ışığında daha fazla tartışma yapılabilene kadar diğer durumları düzenlememeyi kabul*

ettiler. Bu bağlamda, 39. maddenin, 3. paragrafı, söz konusu diğer durumlara ne izin verileceğini ne de bunların engelleneceğini öngörmektedir."

Bu, Budapeşte Sözleşmesi'nin hüküm ve ilkelerinin, bu duruma ilişkin yerel çözümlere veya mevzuata ilke olarak karşı olmadığı anlamına gelir. Belçika ve Portekiz dışında, bu tek taraflı sınır ötesi elektronik delil toplanması olasılığını yasal olarak teminat altına alan pek fazla ülke yoktur. Bununla birlikte bu durum, birçok ülkenin buna çok pragmatik yaklaştığı ve *konumun kaybedilmesi* veya *konumun belirsizliği* olgusunu egemenlikleri lehine yorumladığı gerçeğini değiştirmez.

- **Madde 35 – 7/24 Ağı**

35. madde, Budapeşte Sözleşmesi'nin en önemli maddelerinden biridir. Bu madde, Tarafların her biri için, hızlı bir şekilde sınır ötesi delil toplanmasını sağlamak üzere 7/24 İrtibat Noktası (POC) oluşturma yükümlülüğü yaratmaktadır.

Bu irtibat noktalarının genel amaçları, uluslararası işbirliğini kolaylaştırmak, diğer irtibat noktalarına teknik danışmanlık vermek, verilerin hızlı bir şekilde muhafaza edilmesi için uygun mekanizmayı harekete geçirmek, delilleri acilen toplamak veya dondurmak ve şüphelileri tespit etmek ve bulmaktır. POC'nin temel olarak dünya genelinde depolanan trafik verilerini ve diğer verileri anında muhafaza etme imkanı sağlaması planlanmaktadır. Fakat aynı zamanda, uluslararası işbirliği veya elektronik delil elde etme ışığında bir ülkenin yasal çerçevesinin veya yeteneklerinin özgünlüğüne ilişkin ülkeye özgü bilgileri çekmek için de kullanılabilir. Ülkenizin 7/24 POC'si bu durumda o bilgileri almak için o spesifik ülkedeki POC ile iletişime geçebilir. POC ayrıca, temel abone bilgilerinin veya trafik verilerinin doğrudan (MLA olmadan) nasıl elde edilebileceğini incelemek için yabancı hizmet sağlayıcılarla temaslarda da bir dünya fark yaratabilir. Doğrudan bir işbirliği kurmak isteyen çoğu yabancı hizmet sağlayıcı, genellikle bir ülke içinde tek bir irtibat noktası (SPOC) olmasını şart koşar; çoğu durumda da bu 7/24 POC'dir.

İrtibat noktalarının çoğu polis merkezli irtibat noktalarıdır, ancak bazıları Savcılık Servislerinin irtibat noktalarıdır ve bazı ülkelerde de polis ve yargı irtibat noktaları bulunmaktadır. Budapeşte Sözleşmesi'nin en iyi tarafı, uluslararası işbirliğine ilişkin en faydalı araçlardan biri olarak kabul edilen 7/24 irtibat noktaları ağı için bir yasal dayanak sağlamış olmasıdır.

- **Madde 18.1.b - Yabancı bir hizmet sağlayıcıya verilen ibraz talimatı**[138]

Madde 18.1.b, Tarafların her birinin, yetkili makamlarını, *Tarafın ülkesinde hizmetlerini sunan* bir hizmet sağlayıcıya, o hizmet sağlayıcının sahip olduğu veya kontrol ettiği söz konusu hizmetlerle ilgili *abone bilgilerini* ibraz etmesi talimatını vermek üzere yetkilendirmek için gerekli olabilecek yasal ve diğer önlemleri alacağını ifade etmektedir.

18. Madde kapsamındaki bir "ibraz talimatı" yerel bir tedbirdir ve ulusal ceza hukuku kapsamında öngörülmelidir. Bir "ibraz talimatı", söz konusu talimatın ülkesi içinde verildiği Tarafın yargı ve icra yetkisi alanı ile sınırlıdır. Ancak Taraflar bu hükmü, söz konusu Tarafın ülkesi içinde hizmet sunan hizmet sağlayıcının o ülkede ne yasal ne de fiziksel olarak bulunmadığı koşullarda da uygulayabilirler. Bu nedenle, tedbirin yerel

---

[138] Abone bilgileri için İbraz talimatlarına ilişkin 10 Numaralı T-CY Yönelendirme Notuna bakın (Budapeşte Sözleşmesi Madde 18): https://www.coe.int/en/web/cybercrime/guidance-notes https://www.coe.int/en/web/cybercrime/guidance-notes

niteliğine bakılmaksızın, ülke dışında bir *yargı yetkisinin* uygulanması ima edilmeksizin, bölge dışı bir *etkinin* de olabileceği görülmektedir. Hizmet sağlayıcı, söz konusu Tarafın topraklarında hizmet sunduğu için, bu hizmetleri topraklarında sunduğu Devletin adli amaçlarla temel abone bilgilerine ilişkin yasal talebi ile ilgili yargı yetkisini kabul etmiş sayılabilir.

Dolayısıyla, abone bilgilerinin başka bir yargı bölgesinde depolanması, söz konusu veriler hizmet sağlayıcının elinde veya kontrolünde olduğu sürece Budapeşte Sözleşmesi'nin 18. maddesinin uygulanmasına engel teşkil etmez. Madde 18.1.b ile ilgili olarak, bir durum, genel merkezi bir yargı bölgesinde bulunan ancak verileri başka bir yargı bölgesi içinde depolayan bir hizmet sağlayıcıyı içerebilir. Veriler ayrıca, hizmet sağlayıcının takdirine bağlı olarak ve abonenin bilgisi veya kontrolü olmaksızın, birden fazla yargı bölgesinde yansıtılabilir veya yargı bölgeleri arasında taşınabilir. Yasal rejimler, hem ceza hukuku alanında hem de mahremiyet ve veri koruma alanında, yargı yetkisini tesis etmek için verilerin konumunun belirleyici faktör olmadığını giderek daha fazla kabul etmektedir.

Madde 18.1.b'yi ulusal mevzuatlarında açıkça ve yasal olarak uygulatılabilir bir şekilde uygulayan ülkelerin, kamu-özel işbirliği ve (Facebook, Microsoft, Google, Instagram, Twitter, Apple vb. gibi) ana hizmet sağlayıcılarla işbirliği modellerinin tesis edilmesi bakımından daha güçlü bir konuma sahip olduğunu söylemeye bile gerek olmadığı açıktır.

8.3.2.2 *İkinci Ek Protokol araç kutusu*

Budapeşte Sözleşmesi'nin İkinci Ek Protokolü, özellikle uluslararası işbirliğine ayrılmıştır. Delillerin, yabancı, çoklu, değişken veya bilinmeyen yargı bölgelerinde depolandığı her durumda, kamu-özel işbirliği ve hukukun üstünlüğünün, karşılıklı adli yardım talebi hazırlamak zorunda kalmadan siber uzayda genişletilmesi konusunda ileriye dönük önemli bir adımdır.

- **Madde 10 – Acil durumda karşılıklı adli yardımlaşma (MLA)**

2. Bölümün 4. Kısmı kapsamında öngörülen araçlardan biri, acil bir durumda yapılan MLA talepleri için azami düzeyde hızlandırılmış bir prosedür sağlamak amacıyla zorunlu olarak karşılıklı adli yardım konusudur. 10. Maddede belirtilmiştir ve *Acil Durum MLA* ile ilgilidir.

Bu özellik, gerçek bir kişinin hayatı ve güvenliği için önemli ve yakın bir riskin bulunduğu acil durumlar ile sınırlıdır. Bu makalenin önemli bir unsuru, talebin içeriğinin zorunlu olmasıdır. MLA için gerekli olan klasik içeriğin yanı sıra, acil bir durum olduğunu gösteren olgulara ve istenen yardımın bununla ne şekilde ilişkili olduğuna ilişkin bilgilerin açıklanması zorunludur. Söz konusu Taraf ayrıca, bu tür bir acil durum MLA talebinin yerine getirilmesinin değerlendirilmesi için bu bilgilerin gerekli olması halinde ek bilgiler sunmakla da yükümlüdür.

Ayrıca taraflar için bu madde kapsamındaki herhangi bir talebe cevap verebilmek için 7/24 ulaşılabilir olma yükümlülüğü de getirmektedir. 10. Madde, bu tür bir talebin iletildiği ve yanıt verilmesi için kullanılacak kanal konusunda esneklik sağlamaktadır. Ülkeler, bu tür bir işbirliği kabul edildiğinde doğrudan işbirliğini kullanma ya da 7/24

POC kanalları veya Interpol irtibat noktası ve merkezi otoriteler gibi diğer kanalları da kullanma olanağına sahiptir.

- **Madde 11 – Video konferans**

2. Ek Protokol kapsamında sağlanan bir diğer güçlü yeni araç, Madde 11.2.a'ya göre talepte bulunulan ve talepte bulunan Tarafların merkezi otoriteleri arasında doğrudan iletişimi sağlayan *Video konferans* ile ilgilidir.

Madde 11.1'de, talepte bulunan Tarafın video konferans yoluyla bir tanık veya bilirkişiden tanık beyanlarının veya ifadelerinin alınmasını talep edebileceği ve talepte bulunulan Tarafın da buna izin verebileceği belirtilmektedir. Talepte bulunan Taraf ve talepte bulunulan Taraf, uygun olduğu şekilde; hangi Tarafın başkanlık edeceği, hazır bulunacak makamlar ve kişiler, Taraflardan birinin veya her ikisinin belirli yeminler edip etmeyeceği, tanık veya bilirkişiye uyarı veya talimat verip vermeyeceği, tanığın veya bilirkişinin sorgulanma şekli, tanık veya bilirkişi haklarının usulüne uygun olarak sağlanma şekli, imtiyaz veya dokunulmazlık iddialarının ele alınması, sorulara veya yanıtlara yapılan itirazların ele alınması ve Taraflardan birinin veya her ikisinin yazılı tercüme, sözlü tercüme ve deşifre hizmetleri sunup sunmayacağı da dahil olmak üzere talebin yerine getirilmesi ile ilgili olarak ortaya çıkabilecek herhangi bir sorunun çözümünü kolaylaştırmak için birbirleriyle istişare edeceklerdir.

Ne yazık ki uygulamada, talepte bulunulan ülkede gerekli olan belirli prosedürler dikkate alınmadan talepte bulunan tarafın ulusal hukukunun uygulanması nedeniyle başka bir taraftan toplanan bazı tanık beyanlarının veya ifadelerin delil olarak geçerli olmadığı ortaya çıkmıştır.

Bununla birlikte, tüm ülkeler, talepte bulunan Tarafa, soruşturmalarda veya mahkeme işlemlerinde delil olarak kullanılmasına izin verecek bir biçimde tanık beyanları veya ifadeler sağlamanın önemini kabul etmektedir. Bu nedenle, video konferans önemli bir özelliktir ve yeni protokolün içindeki yeni bir unsurdur. Bu hükmün, ülkelerin güvenebilecekleri başka ikili veya çok taraflı anlaşmalara sahip olmadığı durumlarda ikincil bir yasal dayanak olarak kullanılması amaçlanmıştır.

* Acil Durum MLA ve video konferansın yanı sıra, Budapeşte Sözleşmesi'nin İkinci Ek Protokolü, MLA sürecinden geçmek zorunda kalmadan ivedilikle sınır ötesi delil toplanmasını sağlayabilecek araçlar sunmaktadır. Bu prosedürler Bölüm 2, Kısım 1, 2, 3 ve 5'te belirtilmiştir.

- **Madde 6 ve 7 - Diğer taraflardaki hizmet sağlayıcılar ve kuruluşlar ile doğrudan işbirliğini artıran prosedürler**

6. Madde, Alan Adı Tescil Bilgisi Talebi (WHOIS) ile ilgilidir ve aşağıdakileri ifade etmektedir:

1. Tarafların her biri, yetkili makamlarına, belirli cezai soruşturmalar veya kovuşturmalar amacıyla, başka bir Tarafın ülkesinde alan adı tescil hizmetleri sağlayan bir kuruluşa, bir alan adını tescil ettiren kişinin belirlenmesi veya onunla iletişim kurulması için işletmenin mülkiyetinde veya kontrolünde bulunan bilgilere ilişkin bir talep sunma yetkisi vermek üzere gerekli olabilecek yasal tedbirleri ve diğer önlemleri alacaktır.

2. Tarafların her biri, kendi ülkesindeki bir kuruluşun, iç hukuk tarafından sağlanan makul koşullara tabi olarak, 1. paragraf kapsamındaki bir talebe yanıt olarak bu tür

bilgileri açıklamasına izin vermek için gerekli olabilecek yasal tedbirleri ve diğer önlemleri alacaktır.

Abone bilgilerinin açıklanması ile ilgili 7. Madde'de aşağıdakiler ifade edilmektedir:

1. Tarafların her biri, yetkili makamlarına, abone bilgilerinin talepte bulunan Tarafın belirli cezai soruşturmaları veya kovuşturmaları için gerekli olduğu durumlarda, başka bir Tarafın ülkesindeki bir hizmet sağlayıcıya doğrudan sunulmak üzere, o hizmet sağlayıcının mülkiyetindeki veya kontrolündeki belirtilen kayıtlı abone bilgilerinin alınmasına ilişkin bir talepte bulunma yetkisi vermek üzere gerekli olabilecek yasal tedbirleri ve diğer önlemleri alacaktır.

2. a. Tarafların her biri, kendi ülkesi içindeki bir hizmet sağlayıcının, 1. paragraf kapsamındaki bir talebe yanıt olarak abone bilgilerini açıklaması için gerekli olabilecek yasal tedbirleri ve diğer önlemleri alacaktır.

Bu iki prosedür, bir ülkenin yetkili makamı ile başka bir Ülke topraklarında yerleşik bir kuruluş veya hizmet sağlayıcı arasında temel abone bilgilerinin alınmasına yönelik doğrudan işbirliğini geliştirmek amacı ile İkinci Ek Protokol'e dahil edilmiştir.

Bir MLA talebi veya hizmet sağlayıcının bulunduğu ülkenin yardımını bile gerektirmemektedir. Yalnızca, başka bir Tarafın topraklarında alan adı tescil hizmetleri sağlayan kuruluşun, bir alan adını tescil ettireni belirlemek veya onunla iletişime geçmek için gerekli bilgileri açıklayarak doğrudan talebi yerine getirmemesi durumunda, bilgileri almaya yönelik uygun tedbirleri belirlemek amacıyla ülkelerin ilgili makamları arasında istişare gerekebilir.

Buna ek olarak hizmet sağlayıcının, istenen abone bilgilerini açıklamayacağını veya doğrudan talebi yerine getirmeyeceğini ve talep edilen abone bilgilerini vermeyeceğini, talebin kendisine ulaştığı tarihten itibaren otuz gün içinde ülkesindeki yetkili makamlara bildirmesi halinde, talepte bulunan ülke, 8. madde aracılığıyla (MLA prosedürü olmaksızın) talebin uygulatılmasını isteyebilir.

- **Madde 8 - Abone bilgilerinin ve trafik verilerinin ivedilikle sunulması için başka bir taraftan gelen taleplerin yürürlüğe sokulması**

Madde 8.1. Tarafların her birinin, yetkili makamlarını, talepte bulunulan Tarafın ülkesindeki bir hizmet sağlayıcıyı, söz konusu hizmet sağlayıcının mülkiyetinde veya kontrolünde bulunan, ilgili Tarafın ceza soruşturmalarında veya kovuşturmalarında gereken, belirtilen ve kayıtlı

a. abone bilgilerini, ve

b. trafik verilerini

sunmaya zorlamak amacıyla, bir talebin parçası olarak başka bir Tarafa sunulmak üzere bir talepte bulunmak üzere yetkilendirmek için gerekli olabilecek yasal tedbirleri ve diğer önlemleri alacağını ifade etmektedir

Madde 8.2, Tarafların her birinin, 1. paragraf kapsamındaki bir talebin, talepte bulunan bir Tarafça yürürlüğe koyulması için gerekli olabilecek yasal tedbirleri ve diğer önlemleri alacağını ifade etmektedir.

Bu prosedür, abone bilgilerinin açıklanmasına yönelik bir yaptırım mekanizmasıdır ve başka bir ülkenin topraklarında bulunan bir hizmet sağlayıcıya bir talep gönderilmesi-

ni öngörmektedir ve başka bir ülkede bulunan bir hizmet sağlayıcıdan trafik verilerini almak için bağımsız bir mekanizma olarak düşünülmelidir. Bir MLA talebi göndermeye veya almaya gerek kalmadan, ülkeler ve hizmet sağlayıcılar arasındaki tek taraflı yaptırım mekanizmalarının yerini alır.

Bu 8. maddenin temel bir unsuru, Tarafların, başka bir Tarafça sunulan bir talebi yürürlüğe koymak için gerekli tedbirleri alma yükümlülüğüdür. Bu, ilgili tarafın böyle bir talebi nasıl yürürlüğe koyacağını yerel tedbirlerle seçebilmesi anlamına gelir. Bazı taraflar içinde bu, başka bir taraftan bir talep kabul edebilecekleri anlamına gelir. Diğer taraflar içinde, bu talebi başka tedbirlerle onaylayabilirler veya hizmet sağlayıcıyı ilgili verileri sunmaya zorlayan bir talepte bulunabilirler.

Uygulama için de sınırlı bir zaman dilimi verilmiştir (Madde 8.6). Talepte bulunulan Taraf, gerekli tüm bilgilerin alındığı tarihten itibaren, daha erken değilse de en geç kırk beş gün içinde hizmet sağlayıcıya sunulması için makul her çabayı gösterecek ve talep edilen bilgi veya verilerin en geç:

i. abone bilgileri için yirmi gün; ve

ii. trafik verileri için kırk beş gün içinde iadesi için talepte bulunacaktır.

- **Madde 9 – Acil bir durumda depolanan bilgisayar verilerinin ivedilikle açıklanması**

Madde 9.1.a. Tarafların her birinin, acil bir durumda, Sözleşmenin 35. maddesinde atıfta bulunulan 7/24 Ağına (7/24 POC) ilişkin irtibat noktası için ve o Tarafın topraklarındaki bir hizmet sağlayıcıdan, o hizmet sağlayıcının mülkiyetinde veya kontrolünde olan, belirtilen kayıtlı bilgisayar verilerinin, karşılıklı yardım talebi olmaksızın hızlı bir şekilde açıklanmasını sağlamak için derhal yardım isteyen başka bir Taraftaki bir irtibat noktasına bir talep iletmek ve o irtibat noktasından bir talep almak için gerekli olabilecek yasal tedbirleri ve diğer önlemleri alacağını ifade etmektedir.

Bu yetkinin temel unsuru, bir Tarafta bulunan yetkili makamın, tanımlandığı şekilde acil bir durumda verilerin sunulmasına ilişkin taleplerde bulunması ve talepler almasıdır. Bu madde ile, karşılıklı adli yardım talebi olmaksızın belirli bilgisayar verilerinin hızlı bir şekilde açıklanması için acil yardım almaya ilişkin yasal dayanağın belirlenmesi amaçlanmaktadır. Hizmet sağlayıcının kontrol ettiği içerik verilerini, trafik verilerini veya diğer bilgi türlerini içerir. Burada abone bilgilerinden bahsetmiyoruz.

9. madde, hizmet sağlayıcı ile doğrudan işbirliğine izin vermemektedir. Acil bir durumda, hizmet sağlayıcı istenen verileri doğrudan talepte bulunan ülkeye göndermeyecektir. Bunun yerine verileri kendi yetkililerine açıklayacak, onlar da talepte bulunan tarafa verecektir.

Bu açıklama için iletim Kanalı belirtilmiştir. Her iki Tarafta da 7/24 iletişim noktasıdır.

- **Madde 12 – Ortak Soruşturma(lar) (Ekipler)**

Madde 12.1 ile, karşılıklı mutabakatla, iki veya daha fazla Tarafın yetkili makamlarının, gelişmiş koordinasyonun özellikle yararlı olduğu düşünülen cezai soruşturmaları veya kovuşturmaları kolaylaştırmak için kendi topraklarında ortak bir soruşturma ekibi kurabileceği ve çalıştırabileceği ifade edilmektedir.

12.2 içinde buna ek olarak, özel amaçları, oluşumları, işlevleri, süreleri ve her türlü uzatma süreleri, konum, organizasyon, bilgi veya delil toplama, iletme ve kullanma koşulları, gizlilik koşulları ve bir Tarafın katılımcı makamlarının diğer bir Tarafın topraklarında gerçekleşen soruşturma faaliyetlerine katılımına ilişkin koşullar gibi ortak soruşturma ekiplerinin işleyişini düzenleyen prosedürlerin ve koşulların bu yetkili makamlar arasında kararlaştırıldığı gibi olacağı da ifade edilmektedir.

Bu maddenin amacı, temel unsurların (prosedürlerin ve koşulların) ilgili tarafların bir mutabakatı ile belirlendiği durumlarda, bir ortak soruşturma ekiplerinin etkin bir şekilde ve operasyonel işbirliği veya koordinasyon için bir araç olarak kurulmasına izin verecek prosedürleri uyumlu hale getirmektir. Esnek bir maddedir çünkü Ortak Soruşturma Ekibinin zamanının, amacının ve üyeliğinin Taraflarca belirlenmesi için alan açmaktadır.

Daha da önemlisi, soruşturmaya ilişkin bu tedbirin, bir MLA talebi olmadan uygulanması için bir yasal dayanak sağlamaktadır. İstisnai durumların daha fazla merkezi koordinasyon gerektirdiği durumlarda, Tarafların diğer uygun iletişim kanallarını karşılıklı olarak belirleyebilmeleri dışında, yetkili ve katılımcı makamlar doğrudan iletişim kuracaktır. Bir Tarafın katılımcı makamları, diğer Tarafların bir MLA talebi göndermesine gerek kalmadan kendi makamlarından bu tedbirlerin alınmasını talep edebilir. Bu tedbirler, ulusal bir soruşturmada iç hukuk kapsamında geçerli olan koşullar altında, söz konusu Tarafın kendi topraklarındaki makamları tarafından yürütülecektir.

8.4 Uluslararası Delil Toplamanın Yasallığını Belgeleme Zorunluluğu

Yurt dışında elde edilen delillerin kullanılması, ulusal ve uluslararası yasal belgelere uygun olarak yapılmış olması halinde ilke olarak kabul edilmektedir. Bu bakımdan önemli olan, elektronik delillerin yurt dışında yasal ve meşru bir şekilde toplandığının gösterilmesidir. Çoğu hukuk sisteminde, yurtdışında toplanan ve daha sonra mahkemede delil olarak kullanılmak üzere başka bir ülkeye aktarılan deliller için bir yasallık karinesi vardır. Yine de, elektronik delil toplamanın kabul edilebilirliğini ve yasallığını mahkemenin ve savunmanın teyit etmesini sağlamaya yönelik tüm unsurlar dava dosyasına eklenmelidir. Başka bir deyişle, savunmanın delillerin (sınır ötesi) toplanmasına itiraz edebilmesi sağlanmalıdır.

Bu, çok belirgin bir şekilde, ilke olarak, savcının mahkemeye diğer şeylerin yanı sıra aşağıdaki belgeleri sunması gerektiği anlamına gelir:

- elektronik delillerin toplanmasına izin vermiş olan yetkili ulusal ve yabancı makamlara ait tutanaklar ve ibraz talimatları;
- adli yardım talepleri ve bunlara ait uygulama belgeleri;
- söz konusu bilgilerin - şartlı olarak veya başka bir şekilde (Madde 26.2) - delil olarak kullanılabilmesine dair onay ile birlikte, Budapeşte Sözleşmesi'nin 26. maddesi uyarınca kendiliğinden bilgi paylaşımına yönelik alınan her karar;

- yurtdışında delil toplanmasına ilişkin olarak yurtdışında müdahalede bulunmuş her mahkeme kararı;
- yabancı delil toplamanın kabul edilebilirliği ve kanuna uygunluğunun değerlendirilmesi ile ilgili diğer herhangi bir belge veya kayıt.

Ancak bu, mevcut yabancı (ikiz) dava dosyalarının tamamının eklenmesi gerektiği anlamına gelmez. Genel olarak, yabancı delil toplamanın kabul edilebilirliği ve kanuna uygunluğunun değerlendirilmesi ile ilgili belge veya yazıların sunulması yeterlidir.

9 Role Özgü Hususlar

Elektronik deliller içeren davalardaki çeşitli rollere özgü bir takım hususlar söz konusudur:

- Soruşturma yönetimi
- Delil Zinciri
- Delillerin incelenmesi (laboratuvar işlemleri)
- Aramaların failler (örneğin şirket ağları) üzerindeki etkisi
- Tedbirler, mahremiyetle ilgili hususlar, orantılılık, teminat ihlali

9.1 Kolluk Kuvvetleri, Muhtemelen Tüm Soruşturma Makamları

Bu bölümde ele alınan tüm hususlar önceki bölümlerde zaten ele alındığından, kolluk kuvvetleri için role özgü bilgiler sağlamaya gerek yoktur.

9.2 Savcılar

9.2.1 Soruşturmaların Yönetilmesi

Müfettişlerin, savcıların, savunma temsilcilerinin ve hâkimlerin hepsinin bilgileri ve teknolojiyi anlaması gerekmektedir. Savcı bir davada karara bağlanması gereken tüm hususları tespit edemez ve bunları basit ve özlü bir şekilde mahkemeye sunmazsa, özellikle de teknik hususlar söz konusuysa, davalar başarısız olabilir. Savcılar ve müfettişler, özellikle yeni teknolojiler söz konusu olduğunda, soruşturma ve kovuşturma yapmak için eğitimli ve uzman becerileri ve bilgileri ile donatılmış olmalıdır.

Savcıların sınır ötesi suç meselelerinde bir kovuşturma için en uygun yargı bölgesini belirleyebilmesi ve söz konusu delilleri mahkemede sunmak için en son teknolojiyi kullanabilmesi gerekir. Bu, mahkeme duruşmalarının delilin sunumunu kolaylaştırmaya yönelik ilave teknolojiler ile donatılması gerektiği anlamına gelebilir.

Ülkeye bağlı olarak, savcılar, kolluk kuvvetleri ile yan yana çalışmalı veya yasal tuzakları önlemeye, delil fırsatlarını en üst düzeye çıkarmaya ve mahkemede güçlü, sağlam ve iyi sunulmuş iddialar geliştirmeye yönelik tedbirler konusunda tavsiyelerde bulunmaya hazır olmalıdır. Savcılar, yaptıkları her şeyde bağımsızlık, tarafsızlık ve adalet gibi temel değerleri savunmalıdır.

9.2.2 Kovuşturmaların Yönetilmesi

Adil yargılanma hakkı kutsaldır ve savcılık ekibinin, elektronik delillerin toplanmasına, saklanmasına ve mahkemeye adil ve tarafsız bir şekilde sunulmasına ilişkin sorumlu-

luğu herşeyin üstünde olmaya devam eder. Savcılık ekibinin her bir üyesinin, oynayacağı, açıkça tanımlanmış bir rolü olacaktır. Dava süresi boyunca savcı ile müfettişler ve ilgili diğer personel arasında düzenli dava toplantıları yapılmalıdır. Kovuşturmadan sonra, çıkarılacak derslerin belirlenmesine ve yaygınlaştırılmasına yardımcı olmak için tüm katılımcıları içeren resmi bilgilendirme oturumları yapılmalıdır.

Bilişim suçları coğrafi sınır tanımadığından, savcıların sınır ötesi irtibatı kolaylaştırmak ve karşılıklı adli yardım yoluyla elektronik delil elde etmek konusunda giderek artan bir rolü vardır.

Savcıların, elektronik delillerdeki eksiklikleri tespit etmek ve mümkün olduğunda düzeltmek konusunda proaktif olmaları ve daha fazla soruşturma ile güçlendirilemeyecek davaları erkenden bir sonuca götürmeleri gerekir.

Her davanın benzersiz olduğunu ve soruşturmanın sonucundan emin olmak için hangi tedbirlerin gerektiğini doğru bir şekilde belirleyebilmek için kendine has olgular ve esaslar üzerinden (ve geçerli ulusal hukuk bağlamı içinde) değerlendirilmesi gerektiğini akılda tutmak önemlidir.

Soruşturma sırasında ortaya çıkarılmış olan delillerin ve suç miktarının etkili ve verimli bir kovuşturma açısından değerlendirilmesi büyük önem taşımaktadır. Bir savcının yapabileceği en büyük hatalardan biri, kovuşturmayı/iddianameyi ayrıntılarla ve önemsiz olgularla aşırı doldurmaktır. Şu ünlü sözün değerini bilin: "*De minimis non curat praetor*"[139].

Kovuşturma yönetimi aynı zamanda delil ve bulguların sadece miktarının değil, niteliğinin de değerlendirilmesi gerektiği anlamına gelir. Savunmanın hangi argümanları tercih ettiğini ve bunları dava öncesi duruşmada nasıl sunacağını da seçmesi gerekecektir. Klasik olarak savunma küçük bir avantaja sahiptir: Savunma, çoğunlukla delilin herhangi bir yönüne karşı bir saldırıyı göze alabilir. Savunma şüphe tohumları ekmelidir ve bunu yaparken çok ileri gidebilir. Başka bir deyişle, savunma bazen yıkıcı olma lüksüne sahiptir. Öte yandan, savcının ise delilleri her zaman yapıcı bir şekilde biriktirme görevi vardır.

9.2.3 Savunmaya Açıklama

Bölüm 7.6'da da açıklandığı gibi, herhangi bir soruşturma mahkemede dayanak oluşturmayacak materyaller üretecektir. Bir davalının adil yargılanma hakkı, Avrupa İnsan Hakları Sözleşmesi'nin (AİHS) 6. maddesinde yer almaktadır ve bir müfettişin, kovuşturma davasını baltalayabilecek veya savunma davasına yardımcı olabilecek herhangi bir materyali tespit etmesi önemlidir. Mahkeme uygulamasının, savcılığın savunma için kovuşturma delilleri takvimi hazırlamasını gerektirdiği durumlarda, müfettiş bu tür kullanılmayan materyalin uygun şekilde vurgulanmasını sağlamalıdır.

Savcılar, adaletin yararına ve yasalara uygun olarak adil ve tarafsız davranma konusundaki genel ve mesleki sorumluluklarının bir parçası olarak, ilgili mevzuat uyarınca uygun şekilde açıklamayı kolaylaştırmak için ellerinden gelen her şeyi yapmalıdır. Savcılar ayrıca, açıklama yükümlülüklerinin yerine getirildiğinden emin olmak için

[139] Otorite veya kral ya da kanun önemsiz şeylerle ilgilenmez

müfettişlere tavsiyelerde bulunma ihtiyacı konusunda tetikte olmalı ve gerektiğinde attıkları adımları irdelemelidir.

9.2.4 Delilin Kabul Edilebilirliği

Yukarıda Bölüm 7 içinde de açıklandığı gibi, ceza davalarındaki dijital deliller; kabul edilebilir, gerçek, doğru ve eksiksiz olmalıdır. Geçerli kanunlara ve kurallara uygun olmalı ve mahkeme için kabul edilebilir olmalıdır.

Davayı incelerken savcı, bariz bir şekilde dosyalar (belirli kişilere ve olaylara ait veriler) bağlamanın ve delil sürekliliğini göstererek bir ibrazın nasıl ortaya çıktığını açıklamanın mümkün olup olmadığını değerlendirecektir.

Ceza davaları sırasında savcı, davayı ceza standardına göre kanıtlamak için delilleri kullanmalıdır (birçok ülkede bu, "makul şüphenin ötesinde" anlamına gelir). Delil kurallarının bir parçası olarak, mahkeme her zaman kendisine en iyi delilin sunulması hakkına sahiptir. Geleneksel olarak en iyi delil orijinal belgedir, ancak belirli koşullar altında ikincil deliller de kabul edilebilir. Tipik olarak ikincil deliller, en iyi delillerin kopyalarından veya alıntılarından oluşur.

Bir davada, delillerin yeterli olup olmadığını, zaafların olduğu ve daha fazla elektronik delilin gerekli olduğu yerleri belirlemeye yardımcı olmak üzere savcı tarafından elektronik delilin erken bir incelemesinin yapılması gereklidir. Bu inceleme erken bir aşamada yapılırsa, dava mahkeme huzuruna gitmeden önce hala diğer yargı bölgelerinden ilave delil elde etme fırsatı olabilir. Bu, polis özerkliğinin soruşturmanın sonuna kadar büyük ölçüde mevcut olduğu Genel Hukuk sistemlerinde kesinlikle bir meseledir. Medeni Hukuk sistemlerinde, tipik olarak savcı (veya varsa soruşturma hâkimi) soruşturmanın öncülüğünü ve kontrolünü üstlenecektir.

Adli tanık rolünün özünde, elde edilen elektronik deliller, ifadeler ile ilgili raporların ve uygun olduğu durumlarda itirazın yanlışlığını kanıtlamaya yönelik raporların ibraz edilmesi yatmaktadır. Savcı, tanığın düşünce süreçleri ve bulguları hakkında netlik sağlayabilmek için olgu ve görüş biçiminde açıkça ayrılmış kısa ifadeler verilmesini teşvik etmelidir. Savcı, gereksiz düzeyde hacimli bir belge sunulmasından ziyade gerekirse ekler biçiminde destekleyici belgeler sunulmasını talep etmelidir.

Kısa bir rapor iyi bir rapor olabilir; hiç kimse baştan sona okuyamıyorsa, uzun bir rapor gereksizdir.

Raporu/raporları inceledikten sonra (ve ulusal ceza muhakemesi usulü uyarınca uygun olduğu durumlarda) tanıktan, savunmanın ileri sürmesi muhtemel hususlar hakkında - özellikle de karşı taraf tanıklarının beyanlarında yer alan çelişkilerle ilgili olarak - özel bilgi ve açıklamalar istenmelidir. Tanığın, davada kullanılmak üzere, bir kararlaştırılan terimler sözlüğü hazırlaması da çok yararlı olabilir.

Duruşma öncesi dönemde (ve gerekirse asıl yargılama sırasında) savcılık, delil durumunu netleştirmek için elektronik delilin kapsamını ve mevcudiyetini/içeriğini tartışmak üzere savunmayla görüşmeyi yararlı bulabilir (bu, Genel Hukuk sistemlerinde öncelikli olarak, Medeni Hukuk sistemlerinde ise daha seyrek başvurulan bir uygulama olabilir).

Adli tanık tarafından sunulan deliller şu özellikleri haiz olmalıdır:

- Güvenilir
- Tarafsız
- Net

9.3 Hâkimler

9.3.1 Hâkimin Soruşturmadaki Rolü

Geçerli hukuk sistemine ve ulusal mevzuata bağlı olarak, farklı türde hâkimler birbirinden ayırt edilmelidir:

1. Belirli medeni hukuk sistemlerinde (örneğin Belçika, Fransa, İspanya vb.), savcı tarafından talep edildiği takdirde bağımsız ve tarafsız bir hâkim olarak adli soruşturmayı yürüten, "soruşturma hâkimliği" adı verilen bir makam vardır.
2. Ayrıca, müdahaleci soruşturma tedbirleri uygulanmasına izin vermek amacıyla bağımsız ve tarafsız bir hâkim olarak gecikmeksizin müdahale etmesi istenen "soruşturma hâkimi" veya "izin hâkimi" adı verilen hâkimler vardır;
3. Son olarak, bir adil yargılamada, savcı tarafından açılan ceza davasının kabul edilebilirliği ve esası hakkında karar vermek üzere davet edilen duruşma hâkimleri vardır.

Hâkimlerin mahkemede çok önemli bir rol oynadığı durumlarda, elektronik delilin teknik yönlerinin yanı sıra delilin nerede ve nasıl bulunabileceğini de anlamaları gerekmektedir. Ayrıca, dijital delillerin kabul edilebilirliği konusunda sağlam ve uygun kararlar alabilmek için elde edildikleri teknoloji ve uygulamalara ilişkin bir kavrayışa da sahip olmaları gerekir.

Diğer delil türlerinde olduğu gibi, dijital delillerin de doğrulanması gerekmektedir. Hâkimler, hukuk veya ceza davalarında elektronik delilleri diğer deliller ile aynı şekilde ele almalı ve bunların üç genel ilkeye uygun olmasını sağlamalıdır:

- Kabul edilebilir;
- Gerçek (doğruluk ve tamlık da dahil olmak üzere);
- İkna edici.

Hâkimler, bir davada hangi delillerin kabul edileceğini belirler ve uzman ve bilirkişi tanıklığına göre hüküm kurarlar. Pek çok yargı bölgesinde hâkimler, yasaların yanı sıra olgular hakkında da karar verirler. Bu tür kararlar bilinçli bir bakış açısıyla alınmalıdır. Herhangi bir yüksek teknoloji vakasında, çoğu karmaşık ve teknik nitelikte olan muazzam miktarda materyal görülebilir. Hâkimlerin bu tür davaları yönetebilmeleri ve sağlam temele dayalı olan başvurularla sağlam temele dayalı olmayanları ayırt edebilmeleri gerekmektedir.

9.3.2 Bilirkişinin Rolü

Yasal işlemlerde, mahkemenin bilgisinin ötesinde, belirli bir konudan daha iyi anlayan

ve daha fazla deneyime sahip biri tarafından açıklanması gereken hususlar olabileceği kabul edilmektedir. Bu kişi "uzman" tanıktır ve bu rolü ile ayırt edilmektedir çünkü sadece kendisi tarafından bilinen olguları değil, aynı zamanda görüşleri de tartışabilir. Bir hâkim, bir bilirkişinin davaya kattığı bilgi birikimin niteliklerini ve düzeyini değerlendirebilmelidir.

Kimin bilirkişi olabileceğine ve kimin olamayacağına ilişkin kurallar ülkeden ülkeye değişmektedir. Bazı ülkelerde oturmuş şartlar varken[140]; diğerlerinde durum daha az kuralcıdır.

Bilirkişi bağımsız ve tarafsız olmalıdır. Mahkemeye karşı bir görevi vardır ve sunulan delillerle ilgili herhangi bir zaafı veya sınırlamayı mahkemenin dikkatine sunmalıdır.

"Bağımsız danışman tanığa" ilişkin bazı kriterler Bölüm 2.6 içinde açıklanmıştır. Çoğu durumda bu kriterler bilirkişi için de geçerli olacaktır.

9.3.3 Kullanılmayan Materyallerin Ele Alınması

Her soruşturmada, delil olarak kullanılmayacak materyaller olacaktır. Bir davalının adil yargılanmasını sağlamak için hâkim, savcılığın açıklama sorumluluklarını gerektiği gibi yerine getirdiğinden emin olmalıdır.

9.3.4 Yargı Yetkisi

Mahkemenin, belirli bir davayı karara bağlamak için yargı yetkisi iddiasında bulunup bulunamayacağına ve yargı yetkisini kullanmak için davanın gerekli ülke bağlantısı faktörlerini içerip içermediğine karar vermesi gerekecektir. Bilişim suçu vakalarının kendine özgülüğü ve genellikle ilgili "konum kaybedilmesi" sorunları göz önüne alındığında, bu kolay bir iş değildir. Bu nedenle, elektronik delil toplama konusunda karar vermek zorunda olan hâkimlerin, dijital suç mahalline ve siber uzayda yargı yetkisi ve ülkesellik kavramlarına aşina olmaları daha da önemlidir.

Hâkimlerin ayrıca, Bölüm 8 içinde ana hatlarıyla belirtildiği ve tanımlandığı gibi, (sınır ötesi) elektronik delil toplama araçları ve mekanizmaları hakkında derinlemesine bir bilgiye sahip olmaları da gerekecektir.

Bu Kılavuz boyunca tekrarlandığı gibi, elektronik delillerin teknik yönlerinin anlaşılması ve değerlendirilmesi, bu tür kararları ilgili taraflar açısından kolaylaştıracaktır ve buna hâkim de dahildir.

[140] Bkz. örneğin ABD'deki 702 Nolu Federal Delil Kuralı.

10 İlgili İçtihat ve Dava Örnekleri

Teoriyi pratiğe dönüştürmek genellikle zor bir iştir. Bu bölümde özellikle, bir yanda elektronik delillerin toplanması ve kullanılması ile diğer yanda temel hak ve özgürlükler ve hukukun üstünlüğü arasındaki ilişkiye ilişkin önemli mahkeme kararlarından oluşan bir seçkiye dair bir genel bakış sunuyoruz.

Bu arada her şeyin daima siyah veya beyaz olmadığını da akıldan çıkarmayalım; belirli bir bireyin temel haklarının genellikle başka bir bireyin temel haklarına veya aynı zamanda toplumsaL menfaatlere veya kamu düzenine de karşı olması gibi basit bir nedenden dolayı çok sayıda gri alan bulunmaktadır. Bu nedenle içtihat hukuku çok kapsamlıdır. Bu bölümde, elektronik deliller ile ilgili olarak mihenk taşı olmuş bazı AİHM içtihatlarından ve üzerinde düşünülmesi gereken bazı somut davalardan ve ikilemlerden oluşan bir seçki sunacağız.

Hem ulusal hem de uluslararası bazı önemli yargı kararları da dahil olmak üzere, "siber alemde" olup bitenlerden daha küresel bir şekilde haberdar olmak için, diğerlerinin yanı sıra, CoE ve EJCN (Avrupa Adli Bilişim Suçları Ağı) tarafından yayınlanan ve halkın erişimine açık olan periyodik haber bültenlerine/izleme raporlarına atıfta bulunulabilir:

- CoE'nin **Bilişim Suçları Haber Özeti**, Avrupa Konseyi Bilişim Suçları Program Ofisi'nin (C-PROC) güncel ilgi alanlarıyla ilgili iki haftada bir çıkan bir haber seçkisidir. Haber özeti, okuyucularına bilişim suçları hakkında küresel ve güncel bir bakış açısı sunmayı amaçlamaktadır.[141]
- Avrupa Birliği Ceza Hukuku İşbirliği Ajansı (Eurojust), **Bilişim Suçları Adli İzleme Raporu (CJM)** yayınlamaktadır. CJM yılda bir kez yayınlanır ve bilişim suçları ve bilişim destekli suçlar ile mücadele alanında faaliyet gösteren adli makamlara ve kolluk kuvvetlerine dağıtılır. Avrupa Adli Bilişim Suçları Ağı'nın (EJCN) üyeleri tarafından sağlanan bilgiler esasında hazırlanmaktadır. Tüm CJM sayıları Eurojust web sitesinde bulunabilir. CJM dört ana bölümden oluşmaktadır. İlk bölümde, 2020 yılı içinde, bilişim suçları, bilişim destekli suçlar ve elektronik deliller veya e-deliller alanındaki yasal gelişmeler anlatılır. Adli analiz bölümünde, Üye Devletlerdeki ve AB dışı ülkelerdeki mahkemeler tarafından ve Avrupa mahkemeleri tarafından verilen kararlara ilişkin yasal analizler sunulur.[142]

Bu bölümde, hukukun üstünlüğüne göre somut davalarda elektronik delile hukuki yaklaşımın ne olması gerektiğini takdir etme perspektifi ile çok ilgili olan bir dizi konu açıklanacak ve vurgulanacaktır. Bu açıklama hiçbir şekilde eksiksiz değildir, ancak belirli bir ülkenin hangi yasal aileye ait olduğuna bakılmaksızın uyulması gereken ilkeler hakkında iyi bir temel fikir vermektedir.

---

[141] https://www.coe.int/en/web/cybercrime/cyber-digests-and-updates.

[142] https://www.eurojust.europa.eu/publications?search=Cybercrime%20Judicial%20Monitor&criteria=publication&order=DESC

10.1 İnternette Özel Hayatı Koruma Yükümlülüğüne İlişkin Davalar

AİHM, Finlandiya'ya karşı K.U. - 2872/02

Karar tarihi: 2 Aralık 2008

Madde 8 - Özel hayata saygı

Finlandiya'ya karşı K.U. davasındaki AİHM kararı, bu kursun amacı açısından, Devletin ilgili bağlamdaki koruma görevini gösteren en önemli dava olmaya devam etmektedir.

- Bir çevrimiçi çöpçatanlık sitesinde, 12 yaşında bir erkek çocuğu olan başvuru sahibinin, iddiaya göre müsait olduğu hakkında bir mesaj, isimsiz olarak yayınlanmıştır. ISP, iletişimin gizliliğine ilişkin kanun nedeniyle, mesaj sahibinin kimliğini, suçlamada bulunulmasına imkan tanıyacak şekilde açıklamamaktadır. Finlandiya mahkemeleri bunu kabul etmiştir.

- AİHM, çocuğun özel yaşam hakkının ihlal edildiğine karar vermiştir. İfade özgürlüğü ve iletişimin gizliliği üzerinde durulan temel hususlardır. İnternet hizmetlerinin kullanıcıları, kendi mahremiyetlerine ve ifade özgürlüklerine saygı duyulacağına dair bir garantiye sahip olmalıdır. Ancak bu garanti mutlak olamaz ve bazen başkalarının hak ve özgürlüklerinin korunması da dahil olmak üzere başka meşru kaygılara yol açması gerekir.

Olgular: 1999 yılında kimliği belirsiz bir kişi, on iki yaşındaki başvuru sahibi adına, bilgisi dışında, bir internet çöpçatanlık sitesinde cinsel nitelikli bir ilan yayınlamıştır. İlanda; başvuru sahibinin yaşı, doğum yılı ve fiziksel özellikleri hakkında ayrıntılı bilgi verilmiş ve bir erkekle yakın bir ilişki istediği belirtilmiştir. Ayrıca, resminin ve telefon numarasının bulunabileceği web sayfasına giden bir bağlantı da eklenmiştir. Başvuru sahibi, ilandan, kendisiyle buluşmayı teklif eden bir adamdan e-posta aldığında haberdar olmuştur. Polise şikayette bulunulmuş, ancak hizmet sağlayıcı, kendisini gizlilik kuralları ile bağlı olarak değerlendirdiği için ilanı veren kişinin kimliğini açıklamayı reddetmiştir. Daha sonra bir bölge mahkemesi, polisin Ceza Soruşturmaları Yasası uyarınca hizmet sağlayıcının ilanı verenin kimliğini ifşa etmesini gerektiren bir talebini, bir hizmet sağlayıcıyı mesleki gizliliği göz ardı etmeye ve bu bilgileri açıklamaya zorlamak için kullanılabilecek olan iftira gibi daha önemsiz suçlarla ilgili davalarda açık bir yasal hüküm bulunmadığını tespit ettikten sonra reddetmiştir. Temyiz mahkemesi bu kararı onamış ve Yargıtay da görülebilirlik iznini reddetmiştir.

Hukuk: İç hukuk, başvuru sahibinin davasını iftira olarak görse de, Mahkeme, başvuru sahibinin fiziksel ve zihinsel sağlığına yönelik potansiyel tehdit ve savunmasız yaşını göz önüne alarak, başvuru sahibinin özel hayatı üzerindeki etkileri vurgulamayı tercih etmiştir. Başvuru sahibi hakkındaki internet ilanının yayınlanması, reşit olmayan bir kişinin sübyancıların hedefi olmasına yol açan bir suç eylemidir. Bu davranış, ceza hukuku müdahalesinin ve etkili caydırıcılığın, yeterli soruşturma ve kovuşturma yoluyla güçlendirilmesini gerektirmektedir. Çocuklar ve diğer savunmasız bireyler, özel hayatlarına yapılan bu tür ciddi saldırılardan Devlet tarafından korunma hakkına sahiptir. Üçüncü bir taraftan, bu durumda hizmet sağlayıcıdan tazminat alma olasılığı, ye-

terli bir çözüm değildir. Burada gerekli olan, asıl failin - bu durumda, ilanı veren kişinin - tespit edilip adalete teslim edilmesini ve mağdurun da ondan maddi tazminat almasını sağlayan bir hukuk yolunun bulunabilmesidir. Olayın gerçekleştiği tarihte yaygın olan çocuğa yönelik cinsel istismar sorunu ve internetin suç amacıyla kullanılması tehlikesi gayet iyi bilindiği için Devlet, sübyancıların internet üzerinden çocukları hedef almasını önlemeye yönelik bir sistemi uygulamaya koyma fırsatına sahip olmadığını iddia edememiştir. İfade özgürlüğü ve iletişimin gizliliği en önemli hususlar olmasına ve telekomünikasyon ve internet hizmetlerinin kullanıcılarının kendi mahremiyetlerine ve ifade özgürlüklerine saygı duyulacağına dair bir garantiye sahip olmaları gerekmesine rağmen, bu garanti mutlak olamazdı ve zaman zaman düzensizliğin veya suçun önlenmesi veya başkalarının hak ve özgürlüklerinin korunması gibi başka meşru zorunluluklara boyun eğmek zorunda kalıyordu. Bu nedenle, yasama organı, rekabet içindeki bu menfaatleri uzlaştırmaya yönelik bir çerçeve sağlamalıydı. Böyle bir çerçeve daha sonra Kitle İletişiminde İfade Özgürlüğünün Kullanılması Kanunu yoluyla getirilmiş olsa da, o zamanlar mevcut değildi. Devlet, gizlilik şartına, başvuru sahibinin fiziksel ve manevi sağlığından daha büyük bir öncelik vererek, başvuru sahibinin özel hayatına saygı duyulması hakkını korumamıştır.

Sonuç: İhlal (oybirliğiyle).

10.2 Önceden Yargı İzni Olmaksızın Orantısız Arama ve Elkoyma

AİHS, İspanya'ya karşı TTrabajo Rueda, 32600/12

Karar tarihi: 30 Mayıs 2017

Madde 8 Özel hayata saygı

Bu dava, çocuk istismarına yönelik materyal içerdiği gerekçesiyle başvuru sahibinin bilgisayarına elkonulması ile ilgilidir. Başvuru sahibi, polisin bilgisayarına elkoymasının ve incelemesinin, özel hayatına ve yazışmalarına saygı duyulması hakkına müdahale teşkil ettiğinden şikayetçi olmuştur.

Mahkeme, Sözleşme'nin 8. maddesinin (özel hayata saygı hakkı) ihlal edildiğine karar vermiştir. İlk olarak, polisin başvuru sahibinin kişisel bilgisayarındaki dosyalara erişiminin ve mahkumiyetinin, başvuru sahibinin özel hayatına saygı duyulması hakkına müdahale teşkil ettiği kaydedilmiştir. Bu müdahale iç hukuk tarafından öngörülmüştür. Ayrıca "suçun önlenmesi" ve "başkalarının haklarının korunması" meşru amacı da izlenmiştir. Bu bağlamda Mahkeme, özellikle "cinsel istismarın, şüphesiz, mağdurları üzerinde güçten düşürücü etkileri olan, tiksindirici bir suç türü olduğunu" ve "çocukların ve diğer savunmasız kişilerin, özel hayatlarının temel yönlerine bu tür ciddi müdahale türlerine karşı etkili bir caydırıcılık şeklinde Devlet tarafından korunma hakları olduğunu" vurgulamıştır. Ancak Mahkeme, önceden adli izin olmaksızın polisin bilgisayara elkoymasının ve içerdiği dosyaları incelemesinin, izlenen meşru amaçlarla orantılı olmadığına ve "demokratik bir toplumda gerekli" olmadığına karar vermiştir. Mahkeme, aslında söz konusu bilgisayar zaten polisin elindeyken ve öncesinde polis soruşturmalarını engellemeden oldukça hızlı bir şekilde izin alınabilmesi mümkünken, polisin, önceden adli izin alınmasına ilişkin normal gerekliliği atlayarak, başvuru sahibinin kişisel bilgisayarındaki dosyalara elkoymasını ve içeriğine erişmesini gerektiren durumun aciliyetini değerlendirmenin zor olduğunu tespit etmiştir.

10.3 Mahkeme Emri ve Bağımsız Denetim Olmaksızın Dinamik IP Adresleri

AİHM, Slovenya'ya karşı Benedik, 62357/14

Karar tarihi: 24 Nisan 2018

Madde 8 Özel hayata saygı

Slovenya'ya karşı Benedik davasında (başvuru no. 62357/14), Avrupa İnsan Hakları Mahkemesi bire karşı altı oyla, Avrupa İnsan Hakları Sözleşmesi'nin 8. Maddesinin (özel hayata ve aile hayatına saygı hakkı) ihlal edildiğine karar vermiştir.

Dava, Sloven polisinin, belirli bir dosya paylaşım ağının kullanıcılarını izlemeleri sırasında, İsviçre kolluk kuvvetleri tarafından kaydedilen bir dinamik IP adresi ile bağlantılı abone bilgilerine erişmek için mahkeme emri alamaması ile ilgilidir. Bu, başvuru sahibinin, çocuk pornografisi de dahil olmak üzere ağ üzerinden dosya paylaştıktan sonra kimliğinin tespit edilmesine yol açmıştır. Mahkeme özellikle, dinamik IP adresi ile bağlantılı abone bilgilerini elde etmek için polis tarafından kullanılan yasal hükmün Sözleşme'nin "yasaya uygun" olma standardını karşılamadığını tespit etmiştir. Söz konusu hüküm netlikten yoksundu, keyfi müdahaleye karşı neredeyse hiçbir koruma sağlamamaktaydı, kötüye kullanıma karşı hiçbir güvenceye sahip değildi ve ilgili kolluk kuvvetlerinin bağımsız denetimine tabi değildi. Bay Benedik'in Sözleşme kapsamındaki haklarının ihlal edildiğine dair bir tespitin, herhangi bir manevi zarar için yeterince adil bir tazminat olduğu belirtilmiştir.

Temel gerçekler: Başvuru sahibi Igor Benedik, 1977 doğumlu ve Kranj'da (Slovenya) yaşayan bir Sloven vatandaşıdır. 2006 yılında İsviçre polisi, çocuk pornografisi resimlerinin veya videolarının paylaşılmasını içeren, bir eşler arası dosya paylaşımı ağında kullanılan bir dinamik IP adresi hakkında Slovenya'daki meslektaşlarını bilgilendirmiştir. Ağustos 2006'da Sloven polisi, yerel İnternet servis sağlayıcısından, şirketin devrettiği IP adresinin tahsis edildiği kullanıcı hakkında bilgi istemiştir. Polis, Ceza Muhakemesi Usul Kanunu'nun bir elektronik iletişim sağlayıcısından, ayrıntıları ilgili rehberde bulunmayan belirli bir elektronik iletişim aracının kullanıcısı hakkında bilgi talep etmelerine imkan tanıyan bir hükmünü kullanmıştır. Polis bir mahkeme emri çıkartmamıştır. Aynı yılın Aralık ayında polis, söz konusu kullanıcının trafik verileri hakkında bilgi almak için bir mahkeme emri almıştır. IP adresi başta Bay Benedik'in babasını söz konusu İnternet hizmetinin abonesi olarak tanımlasa da, hizmeti kullananın ve çocuk pornografisi içeren dosyaları indirenin Bay Bendik'in kendisi olduğu ortaya çıkmıştır. Kasım 2007'de resmen soruşturma altına alınmıştır. Herhangi bir suç işlediğini reddetmiş ve müfettişlere dosyalarda ne olduğunu bilmediğini söylemiştir. Aralık 2008'de çocuk pornografisi sergileme, imal etme, bulundurma veya dağıtma suçundan mahkum edilmiştir. Ljubljana Yüksek Mahkemesi'ne, Yargıtay'a ve Anayasa Mahkemesi'ne yaptığı başvurular başarısız olmuştur. Yerel yargılamalar boyunca, yetkililerin söz konusu dinamik IP adresi ile bağlantılı abone bilgilerini elde etmek için ellerinde bir mahkeme emri olmaması nedeniyle kimliğine ilişkin delillerin kanuna aykırı olarak elde edildiğini iddia etmiştir. Özellikle Anayasa Mahkemesi, bu tür bilgilerin prensipte anayasal veri gizliliği güvenceleri tarafından korunduğuna ancak Bay Benedik'in dosya paylaşım ağında IP adresini ve iletişimlerinin içeriğini ifşa ederek korunma hakkından feragat ettiğine karar vermiştir.

Mahkemenin şikayetleri, usulü ve bileşimi: Başvuru sahibi, 8. maddeye (özel hayata ve aile hayatına saygı duyulması hakkı) dayanarak, polisin dinamik IP adresine bağlı verilere, mahkeme emri almadan keyfi bir şekilde erişmek suretiyle kendisi hakkında bilgi edindiğinden şikayet etmiştir.

Mahkemenin Kararı: Madde 8. Mahkeme ilk olarak, Bay Benedik'in çevrimiçi etkinliğiyle ilgili olarak kimliğinin korunmasına ilişkin menfaatinin Sözleşme kapsamındaki "özel hayat" kavramı kapsamına girdiğine karar vermiştir. Mahkeme, özellikle polisin başvuru sahibinin haklarına müdahalesinin "hukuka uygun" olup olmadığını değerlendirerek devam etmiştir. Bu; söz konusu tedbirin iç hukukta bir dayanağı olmasının, yasanın erişilebilir olmasının; etkilenen kişinin, eylemlerinin sonuçlarını öngörebilmesinin ve hükmün hukukun üstünlüğü ile uyumlu olmasının gerekmesi anlamına geliyordu. Mahkeme, polisin abone bilgilerine erişmek için kullandığı Ceza Muhakemesi Usul Kanunu hükmünün, bilgilerin erişilebilirliği konusunu hiç gündeme getirmediğini, ama ayrıca kötüye kullanmaya karşı yeterli güvencelerin olduğuna da tatmin olmuş olması gerektiğini tespit etmiştir. Söz konusu hüküm, bir elektronik iletişim aracının sahibi veya kullanıcısı hakkındaki bir bilgi talebi ile ilgilidir, ancak dinamik bir IP adresi ile abone bilgileri arasındaki bağlantıya yönelik herhangi bir kurala sahip değildir. Buna karşılık, diğer mevzuat elektronik iletişimin gizliliğine ve mahremiyetine ilişkin kurallar koymaktadır. Örneğin, Anayasa'nın 37. maddesi, iletişimin gizliliğine herhangi bir müdahale için mahkeme emri alınması gerektirmektedir. Hangi mevzuat hükmünün geçerli olduğunu söylemek Mahkeme'nin görevi değildir, ancak yerel kararları incelerken, Bay Benedik hakkındaki anayasal tespitin altını çizmiştir: IP adresine dayalı olarak abone bilgilerine erişim ilke olarak bir mahkeme emri gerektirmektedir, ancak Anayasa Mahkemesi nihai olarak, Bay Benedik'in IP adresini ve iletişiminin içeriğini dosya paylaşım ağında ifşa ederek gizlilik hakkından fiilen feragat ettiği için böyle bir mahkeme emri alınmasına gerek olmadığına karar vermiştir. Ancak Mahkeme bu kararı, Sözleşme kapsamındaki özel hayatın gizliliği hakkının kapsamıyla uzlaştırılabilir bulmamıştır. Mahkemenin görüşüne göre, polisin bir mahkeme emri almış olması gerekirdi ve kanunda almalarını önleyecek hiçbir şey yoktu. Aslında, daha sonra benzer bilgileri elde etmek için bir mahkeme emri almışlardır. Ayrıca, o tarihte ilgili verilerin saklanmasına ilişkin herhangi bir düzenleme ve bunlara erişime ve bunların aktarılmasına ilişkin prosedürde Devlet görevlilerinin yetkiyi kötüye kullanmasına karşı hiçbir güvence yoktu. Mahkeme, Slovenya'nın daha sonra bu tür konuları düzenlemek için bir yasa çıkardığını not etmesine rağmen, o sırada ISP'lerden bilgi almayla ilgili olarak polisin yetkilerini kullanımına ilişkin bağımsız bir denetim mevcut değildi. Genel olarak Mahkeme, polisin dinamik IP adresiyle ilgili abone bilgilerini elde etmek için kullandığı kanunun netlikten yoksun olduğunu ve başvuru sahibinin 8. madde haklarına keyfi müdahaleye karşı yeterli koruma sağlamadığını tespit etmiştir. Bu nedenle Bay Benedik'in haklarına yapılan müdahale "hukuka uygun" olmamış ve Sözleşme'nin ihlal edilmesine yol açmıştır.

Mahkeme, ihlal tespitinin, Bay Benedik'in maruz kalabileceği herhangi bir manevi zarar için yeterli adil tazminat sağladığına karar vermiştir. Mahkeme, başvuru sahibine, hem yerel yargılamalara hem de Mahkeme huzurundaki yargılamalara ilişkin masraf ve giderler ile ilgili olarak 3.522 Euro ödenmesine karar vermiştir.

Ayrı görüşler: Yargıç Yudkivska, Yargıç Bošnjak'ın da mutabık kaldığı bir müşterek görüş bildirirken, Yargıç Vehabović bir karşı görüş bildirmiştir. Görüşler, karara eklidir. Kararın sadece İngilizcesi mevcuttur.

10.4 Elektronik Delilin Aranmasına ve Elkonulmasına Haksız ve Sebepsiz Yere İzin Verilmesi

AİHM, Avusturya'ya karşı Robathin - 30457/06

Karar tarihi: 3 Temmuz 2012

Madde 8 Yazışmaya saygı

Dava, bir hukuk bürosundaki tüm elektronik verilerin aranmasına ve elkonulmasına ilişkin bir açıklamanın ve uygun gerekçelerin bulunmamasına ilişkindir. Soruşturma hâkiminin emri, başvuru sahibi lehine belgelerin, kişisel bilgisayarların ve disklerin, hesap defterlerinin, banka belgelerinin ve hibe senetlerinin ve vasiyetnamelerin aranmasına ve bunlara elkonulmasına genel ve sınırsız bir şekilde izin verdiği için çok genel terimlerle ifade edilmiştir. Tüm verilere elkonulması ve bunların incelenmesi, meşru amaca ulaşmak için gerekenin ötesine geçmiştir.

Olgular: 2006 yılında bir soruşturma hâkimi, bir dizi hırsızlık ve dolandırıcılık suçuyla bağlantılı olarak aranan bir avukat olan başvuru sahibinin mülkleri ile ilgili olarak bir arama emri çıkarmıştır. Arama emri, iddia edilen suçlarla ilgili olması muhtemel verilerle sınırlı olmayıp, ofisteki tüm verileri kapsayacak şekilde genişletilmiştir. Aramanın ardından, bir inceleme kurulu, verilere ön soruşturma kapsamında elkonulduğunu ve bir avukatın kendisi şüpheliyken mesleki sır saklama görevinin onun için dayanak teşkil edemeyeceğini belirterek tüm materyallerin incelenmesine izin vermiştir. Başvuru sahibi nihayetinde söz konusu suçlardan beraat etmiştir.

Hukuk: Madde 8: Elektronik verilerin aranması ve bunlara elkonulması, başvuru sahibinin "yazışmalarına" saygı gösterilmesi hakkına bir müdahale teşkil etmiş ve suçun önlenmesine ilişkin meşru amaç gözetilmiştir. Başvuru sahibinin ileri sürdüğü gibi, arama emrinin yasaya uygun olamayacak kadar belirsiz olup olmadığı konusu orantılılık sorunlarına yol açmıştır ve bu bağlamda incelenecektir. Arama emri, başvuru sahibi aleyhindeki cezai kovuşturma bağlamında bir soruşturma hâkimi tarafından verilmiş ve iddia edilen suçlar, işlendikleri zaman ve iddia edilen zarar hakkında ayrıntılı bilgi vermiştir. Başvuru sahibinin nihai olarak beraat etmiş olması, dava açıldığında şüphelenmek için makul gerekçelerin olmadığı anlamına gelmemektedir. Ancak, arama izni, başvuru sahibi lehine belgeler, kişisel bilgisayarlar ve diskler, hesap defterleri, banka belgeleri ve hibe senetleri ve vasiyetnamelerin aranmasına ve bunlara elkonulmasına genel ve sınırsız bir şekilde izin verdiği için çok genel terimlerle ifade edilmiştir. Başvuru sahibi bir dizi prosedürel önlemlerden yararlanmış olsa da, davayı sevk ettirdiği inceleme dairesi, sadece başvuru sahibi ile iddia edilen suçlarının mağdurları arasındaki ilişki ile ilgili verilerden ziyade, başvuru sahibinin hukuk bürosundaki tüm elektronik verilerin aranmasına izin verirken, yalnızca kısa ve oldukça genel gerekçeler sunmuştur. Bir hukuk bürosunda hâkim olan özel koşullar göz önüne alındığında, böylesi kapsamlı bir aramaya izin verilmesi için istisnai sebepler sunulmuş olmalıdır. Bu tür sebepler olmadığında, tüm verilere elkonulması ve bunların incelenmesi meşru amaca ulaşmak için gerekenin ötesine geçmiştir.

Sonuç: İhlal (ikiye karşı beş oyla).

10.5 Uygun Prosedürel Önlemler Olmaksızın Toplu Gözetim ve Elektronik Verilerin Ele Geçirilmesi

AİHM, Macaristan'a karşı Szabó ve Vissy - 37138/14

Karar tarihi: 12 Ocak 2016

Madde 8 Yazışmaya saygı - Konuta saygı - Özel hayata saygı

Olgular: 2011 yılında Macar polisinin bir kolu olarak Terörle Mücadele Görev Gücü ("TEK") kurulmuştur. Yetkileri, 2011 yılında değiştirilen Polis Kanunu'nun 7/E bölümünde ve Ulusal Güvenlik Kanunu'nda tanımlanmıştır. Başvuru sahipleri, Avrupa Mahkemesi'ne yaptıkları başvuruda, mevzuatın ve özellikle Polis Kanunu'nun "7/E (3) gözetim bölümünün", yeterince ayrıntılı ve kesin olmadığı ve suistimal ve keyfiliğe karşı yeterli güvence sağlamadığı için Sözleşme'nin 8. maddesini ihlal ettiğinden şikayet etmişlerdir.

Hukuk – Madde 8: Mevzuat uyarınca, iki durum TEK tarafından gizli gözetim gerektirir: Macaristan'daki terör eylemlerinin önlenmesi, izlenmesi ve püskürtülmesi ve yurtdışında tehlikede olan Macar vatandaşlarının kurtarılması için gerekli istihbaratın toplanması. TEK'e, evleri gizlice arama ve gözetim altında tutma, posta ve kolileri kontrol etme, elektronik haberleşmeleri ve bilgisayar verisi aktarımlarını izleme ve bu yöntemler vasıtasıyla elde edilen tüm verilerin kayıtlarını alma yetkileri verilmiştir. Mahkeme, bu tedbirlerin, bir kamu makamının başvuru sahiplerinin özel hayatlarına, konutlarına ve yazışmalarına saygı hakkının kullanılmasına müdahale teşkil ettiğini tespit etmiştir.

Gizli gözetim tedbirleri bağlamında öngörülebilirlik gerekliliği, Devletleri gizli gözetim operasyonlarını başlatma kararı vermelerine gerektirebilecek tüm durumları ayrıntılı olarak listelemeye zorlamamıştır. Halbuki, temel hakları etkileyen konularda, ulusal güvenlik alanında yürütmeye takdir yetkisi tanıyan mevzuatın, keyfi müdahaleler yapılmasına karşı bireye yeterli koruma sağlamak için bu takdir yetkisinin kapsamını ve kullanılma şeklini yeterli netlikle belirtmesi gerekmektedir. Macaristan mevzuatı uyarınca, sadece adı verilen kişiler için değil, aynı zamanda "bir dizi kişi" ile ilgili olarak da dinleme izni verilebilmektedir; bu izin, aşırı geniş ve çok sayıda vatandaşın sınırsız gözetiminin önünü açabilecek bir kavramdır. Mevzuat, bu kavramın pratikte nasıl uygulanacağını açıklamamaktadır ve yetkililerin, ilgili kişiler veya bir dizi kişi ile herhangi bir terör tehdidinin önlenmesi arasındaki fiili veya varsayılan ilişkiyi göstermesi gerekmemektedir. Mahkeme'nin görüşüne göre, eğer terör tehdidi çelişkili bir biçimde, kontrolsüz ancak geniş kapsamlı gözetim teknikleri sayesinde vatandaşların özel alanlarına giren dizginlenemez bir yürütme gücü olarak algılanan bir tehdit ile yer değiştirirse, bu durum hükümetin terörizmi uzak tutma ve bu sayede vatandaşların kamu güvenliğini sağlama becerilerine olan güvenini yeniden kazanma çabalarının amacına ulaşmasını engelleyecektir. Mevcut davada, yerel hükümlerin stratejik, büyük ölçekli müdahaleyi mümkün kılacak şekilde yorumlanabileceği göz ardı edilemez. Bu husus ciddi bir endişe yaratmıştır.

Gizli izleme bağlamında, müdahale ihtiyacının "demokratik bir toplumda gerekli" olması, alınan her türlü tedbirin, hem genel bir kaygı olarak demokratik kurumları korumak için, hem de özel bir kaygı içinde münferit bir operasyonda gerekli istihbaratı elde etmek amacıyla kesinlikle gerekli olması gerektiği şeklinde yorumlanmalıdır. Kesin gereklilik kriterini karşılamayan herhangi bir gizli izleme tedbiri, yetkililer

tarafından kötüye kullanılmaya müsait olacaktır. Bu bağlamda Mahkeme, dinlemeler için önceden mahkeme emri alınması gerekliliği veya gözetim emirlerinin yenilenme sıklığını düzenleyen açık hükümler gibi güvencelerin mevzuatta bulunmadığına dikkat çekmiştir. Her ne kadar gözetim tedbirleri Adalet Bakanı'nın önceden izninin alınmasına tabi olsa da, bu tür bir denetim fazlasıyla siyasidir ve doğası gereği kesin gerekliliğe ilişkin önkoşul değerlendirmesini sağlamaktan da acizdir. Mahkemeye göre, yürütme organının siyasi bakımdan sorumlu bir üyesinin denetimi, gerekli garantileri sağlamamaktadır.

Mahkeme, önceden adli kontrol şartının, kıymetli zamanın kaybedilmesi riskini doğuracağı aşırı derecede acil durumların ortaya çıkabileceğini de kabul etmiştir. Bununla birlikte, bu tür durumlarda, yargı dışı bir makam tarafından önceden izin verilen herhangi bir gözetim tedbirinin, olay sonrası bir yargı denetimine tabi olması gerektiğini vurgulamıştır. Mahkeme, Macaristan sistemi uyarınca yürütmenin bu tür operasyonlar hakkında genel olarak bir meclis komisyonuna hesap vermesi gerektiğine dikkat çekmiştir. Ancak, kamuya açık görünmeyen bu raporlama prosedürünün, gizli gözetimin neden olduğu herhangi bir bireysel şikayetle ilgili olarak telafi mekanizması sağlayabileceğine veya gözetim organlarının günlük işleyişini etkin bir şekilde kontrol edebileceğine ikna olmamıştır. Dahası, söz konusu şikayet usulü, gözetim tedbirlerinin, onlara tabi olan vatandaşlara daha sonra herhangi bir şekilde bildirilmesini öngörmediği için, iç hukuk, gizli gözetime tabi olanlar tarafından harekete geçirilebilecek bir adli kontrol mekanizması sağlamamaktadır. Buna ek olarak şikayetler, yeterince bağımsız görünmeyen İçişleri Bakanı tarafından soruşturulacaktır.

Yukarıdaki değerlendirmelerden, gözetim tedbirlerinin yetkilendirmesi, uygulanması ve potansiyel olarak telafi edilmesi konusunda mevzuatın yeterince kesin, etkili ve kapsamlı güvenceler sağlamadığı sonucuna varılmıştır.

Sonuç: İhlal (oybirliğiyle).

Mahkeme, 13. maddenin iç hukuka karşı bir çözüm yolu gerektirdiği şeklinde yorumlanmaması nedeniyle, Sözleşme'nin 8. maddesiyle birlikte ele alındığında 13. maddesinin ihlal edilmediğine hükmetmiştir.

10.6 İletişimlerin, Öngörülebilirlik Şartları Yerine Getirilmeden Umumi Olarak Dinlenmesi

AİHM, Rusya'ya karşı Roman Zakharov
Karar tarihi: 4 Aralık 2015 (Büyük Daire)
Madde 8

Bu dava, Rusya'daki cep telefonu iletişimini gizli olarak dinleme sistemi ile ilgilidir. Bir yayıncılık şirketinin genel yayın yönetmeni olan başvuru sahibi, özellikle Rusya'daki mobil ağ operatörlerinin kanunen kolluk kuvvetlerinin operasyonel arama faaliyetlerini yürütmesine olanak sağlayan teçhizatı kurmak zorunda olduğundan ve Rus hukuku uyarınca yeterli güvenceler olmaksızın iletişimlerin umumi olarak dinlenmesine izin verilmesinden şikayetçi olmuştur.

Mahkeme, iletişimlerin dinlenmesini düzenleyen Rus mevzuatı hükümlerinin herhangi bir gizli izleme sisteminin özünde var olan güvenceleri sağlamadığını ve gizli servislerin ve polisin teknik yollarla tüm cep telefonu iletişimlerine doğrudan erişiminin olduğu Rusya'daki gibi bir sistemde bu durumun özellikle yüksek olduğunu tespit ederek, Sözleşme'nin 8. maddesinin ihlal edildiğine karar vermiştir. Mahkeme özellikle aşağıdaki alanlardaki yasal çerçevede eksiklikler tespit etmiştir: Rusya'daki kamu makamlarının gizli gözetim tedbirlerine başvurmak üzere yetkilendirildiği koşullar; bu tür tedbirlerin süresi, özellikle de devam ettirilmemeleri gereken koşullar; dinlemeye izin verilmesinin yanı sıra ele geçirilen verilerin saklanmasına ve yok edilmesine ilişkin prosedürler; dinlemeye ilişkin denetim. Ayrıca, iletişimlerin dinlenmesine itiraz etmek için kullanılabilecek hukuk yollarının etkililiği, söz konusu hukuk yollarının sadece dinlemeye dair deliller sunabilecek kişilere açık olması gerçeği ve herhangi bir bildirim sistemi veya dinleme ile ilgili bilgilere erişim olasılığı olmadığında bu tür delilerin elde edilmesinin imkansız olması dolayısıyla baltalanmaktadır.

Cezai kovuşturmalar bağlamında gizli izleme tedbirlerine ilişkin olarak ayrıca bkz.: Rusya'ya karşı Akhlyustin, Rusya'ya karşı Zubkov ve Diğerleri, Rusya'ya karşı Moskalev ve Rusya'ya karşı Konstantin Moskalev, 7 Kasım 2017 tarihli kararlar.

10.7 Adil Yargılama ve Elektronik Delil

10.7.1 Delillerin Açıklanmaması ve Uygun Karşı Dengeleme Prosedürleri

- Birleşik Krallık'a karşı Rowe ve Davis [Büyük Daire], no. 28901/95, 16 Şubat 2000
- Rusya'ya karşı Mirilashvili, no. 6293/04, 11 Aralık 2008 (özellikle, §§ 195-200)
- Hırvatistan'a karşı Matanović, no. 2742/12, 4 Nisan 2017 (özellikle, §§ 147-188)

10.7.2 Orijinal Belgelere ve Bilgisayar Dosyalarına Erişim Eksikliği

- Yunanistan'a karşı Georgios Papageorgiou, no. 59506/00, 9 Mayıs 2003

10.7.3 Elkonulan Elektronik Verilerin Duruşmada Kullanılması

- Rusya'ya karşı Khodorkovskiy ve Lebedev, no. 11082/06 ve 13772/05, 25 Temmuz 2013 (özellikle §§ 700-702)

10.7.4 Gizli Gözetim Tedbirleri ile Elde Edilen Delillerin Duruşmada Kullanılması

- Rusya'ya karşı Bykov [Büyük Daire], no. 4378/02, 10 Mart 2009
- Hırvatistan'a karşı Dragojević, no. 68955/11, 15 Ocak 2015

10.7.5 Delillerin Kabulündeki ve İncelenmesindeki Ciddi Kusurlar

- Azerbaycan'a karşı Ilgar Mammadov (no. 2), no. 919/15, 16 Kasım 2017

10.8 Bir Kişiyi Parolayı veya Şifreleme Anahtarını Vermeye Zorlama - Parmak İzi ve Yüz Tanımanın Zorla Kullanılması

10.8.1 Parola Açıklama Emri

Soru: Bir hâkimin bir şüpheliye bir parolayı (veya şifreleme anahtarını) açıklamasını emretmesine izin veren mevzuatın olduğu ve şüphelinin daha sonra söz konusu şifreyi (veya şifreleme anahtarını) vermeyi reddetmesi halinde ceza alacağı birkaç ülke vardır (Belçika, Fransa, BK....). Bu konuda siz ne düşünüyorsunuz? Bu, sessiz kalma hakkına mı yoksa kendini suçlu duruma düşürmeme hakkına mı aykırı? Hâkim siz olsaydınız, o emri verir miydiniz?

Bu, AİHM'nin de henüz yanıtlamadığı bir sorudur. Bu arada, her görüş savunulabilir.

Fransız Anayasa Mahkemesi 30 Mart 2018[143] tarihinde bunun kendini suçlu duruma düşürmeme hakkını ve adil yargılanma hakkını ihlal etmediğine karar vermiştir. Belçika'da Yargıtay 4 Şubat 2020[144] tarihinde aynı ilkeler doğrultusunda karar vermiştir. Belçika Anayasa Mahkemesi de 20 Şubat 2020[145] tarihinde aynı doğrultuda karar vermiştir.

Bunun arkasındaki mantık, Birleşik Krallık'a karşı Saunders[146] davasındaki AİHM içtihadına dayanmaktadır ve parolanın veya şifreleme anahtarının şüphelinin iradesinden bağımsız olarak var olduğunu ima etmektedir. Bununla birlikte, kendini suçlu duruma düşürmeme hakkı öncelikle suçlanan kişinin sessiz kalma iradesine saygı gösterilmesiyle ilgilidir. AİHS akit taraflarının hukuk sistemlerinde ve başka yerlerde yaygın olarak anlaşıldığı gibi, güç kullanılarak sanıktan zorla elde edilebilecek materyallerin değil, ama örneğin bir mahkeme emri uyarınca elde edilen belgeler, DNA testi yapmak amacıyla kullanılacak nefes, kan ve idrar örnekleri ve vücut dokusu gibi şüphelinin iradesinden bağımsız olarak var olan materyallerin ceza yargılamasında kullanılmasını kapsamaktadır. Bir parolanın veya bir şifreleme anahtarının da bu akıl yürütme kapsamına girip girmediğinin düşünülmesi gerekir. Kesin olan şey, şüpheli unutmuş olsa veya unutmak istese bile bir parolanın veya şifreleme anahtarının var olduğudur. Bu anahtarı 'tahmin etmek' veya kırmaya çalışmak da mümkündür. Yani anahtar vardır.

Birleşik Krallık'a karşı Saunders davasında AİHM, Sözleşme'nin 6. maddesinde özel olarak bahsedilmese de, sessiz kalma hakkının ve kendini suçlu durumuna düşürmeme hakkının, genel olarak kabul görmüş uluslararası standartlar olduğunu ve bu hakların

---

143 https://www.conseil-constitutionnel.fr/decision/2018/2018696QPC.htm

144 https://juportal.be/content/ECLI:BE:CASS:2020:ARR.20200204.2N.6/NL?HiLi=eNpLtDKwqq4FAAZPAf4=

145 https://www.const-court.be/public/f/2020/2020-028f.pdf

146 AİHM 17 Aralık 1996, No 19187/91, Saunders/Birleşik Krallık.

6. madde kapsamındaki bir adil yargılanma kavramının özünde yer aldığını hatırlatır. Gerekçeleri, diğerlerinin yanı sıra, sanığın yetkililer tarafından yersiz zorlamaya karşı korunmasında yatmaktadır; bu suretle adli hataların önlenmesine ve 6. maddenin amaçlarının yerine getirilmesine katkıda bulunulmaktadır. Yani sessiz kalma hakkının ve kendini suçlu duruma düşürme yasağının *yasal gerekçesi* ve kökeni, gerçeğin tahrif edilmesine neden olmama kaygısıdır. Yeterince zorlanan biri sonunda yalan veya her şeyi söyleyebilir. Fakat bir parola veya bir şifreleme anahtarı yalan söyleyemez: Ya doğrudur ya da yanlıştır. Dolayısıyla, bu durumda zor kullanılarak gerçek bozulamaz. Bu nedenle, bu gibi durumlarda, bir şüphelinin anahtarı bildiği gösterildikten sonra (ki bunu ispat etmek oldukça külfetli olabilir) sessiz kalma hakkının ve kendini suçlu duruma düşürmeme hakkının kullanılıp kullanılamayacağı sorusu gündeme getirilebilir.

Bu bağlamda ilginç olan da, Mahkemenin - trafik kanunu bağlamında da olsa - bir kişiyi cezalandırma tehdidi altında aracı kimin sürdüğünü söylemeye zorlamanın sessiz kalma hakkını ihlal etmediğine karar verdiği O'Halloran ve Francis/Birleşik Krallık[147] davasındaki AİHM kararıdır. Parolalar ve şifreleme anahtarları söz konusu olduğunda AİHM'nin nihai olarak ne karar vereceğini göreceğiz.

10.8.2 Zorla Parmak İzi Alma ve Yüz Tanıma

Soru: Çoğu durumda, parola sadece akılda değil, aynı zamanda parmaklarda veya yüzde de bulunur. Biyometrik anahtarları ne şekilde kullanıyorsunuz? Şu somut durumu hayal edin: Bir hâkimsiniz ve yakın zamanda tutuklanmış bir çocuk kaçırma şüphelisine karşı parmak izi veya yüz tanıma ile akıllı telefonunu açmak için, kaçırılan reşit olmayan çocuğu aramak için çok önemli olan zamanı kaybetmemek için sınırlı orantılı fiziksel güç kullanımına katılıp katılmadığınız soruluyor.

Bu, aynı zamanda AİHM'nin de henüz yanıtlamadığı bir sorudur. Bu arada, her görüş savunulabilir.

Daha önce de açıklandığı gibi, Birleşik Krallık'a karşı Saunders[148] davasından, öncelikle kişinin kendini suçlu göstereme hakkı ile ilgili olduğunu, ancak bu hakkın, güç kullanılarak sanıktan zorla elde edilebilecek materyallerin değil, ama örneğin bir mahkeme emri uyarınca elde edilen belgeler, DNA testi yapmak amacıyla kullanılacak nefes, kan ve idrar örnekleri ve vücut dokusu gibi şüphelinin iradesinden bağımsız olarak var olan materyallerin ceza yargılamasında kullanılmasını kapsadığını öğrendik. AİHM'nin benzer şekilde parmak izlerinin ve yüz özelliklerinin de iradeden bağımsız olarak var olduğunu varsayması makul görünmektedir.

Hatta bunun bir elektronik delile el koyma biçimi, yani bir bilgisayar sistemine erişim sağlayan elektronik olarak ilgili verileri temsil eden biyometrik anahtarlara el konulması olarak görülebileceğini düşünmeye kadar ileri gidilebilir. Üzerinde düşünülmeye değer mi?

Zor kullanma söz konusu olduğunda, AİHM, belirli koşullarda orantılı fiziksel güç kullanılmasına kesinlikle karşı çıkmıyor görünmektedir. Bu arada DNA da, orantılı fiziksel

---

147 AİHM 29 Haziran 2007, no. 15809/02 ve 25624/02, O'Halloran ve Francis/Birleşik Krallık.

148 AİHM 17 Aralık 1996, No 19187/91, Saunders/Birleşik Krallık.

güç kullanılarak alınabilir. Fakat AİHM, uyuşturucuların iradeden bağımsız olarak var olduğuna karar vermiş olmasına rağmen, Almanya'ya karşı Jalloh[149] davasında şüphelinin yuttuğu uyuşturucu "topaklarını" kusmasını sağlamak için bir kusturucu ilaç uygulanmasının orantılı olmadığına ve hatta AİHS'nin 3. maddesini (işkence yasağı) ihlal ettiğine karar vermiştir. Bu nedenle, tüm temel hak ve özgürlüklerin orantılılık ilkesiyle bağlantılı olarak birbirleri karşısında tartılmaları gerekmektedir.

10.8.3 Şüpheliyi Elektronik Delilleri Açıklamaya Zorlama Konusundaki AİHM İçtihadının Analizi[150]

AİHM bugüne kadar bu konuyla ilgili henüz bir karar vermemiştir, bu da ulusal mahkemelerin bu konuda net bir uluslar üstü yönlendirmeye sahip olmadığı anlamına gelmektedir. Avrupa Adalet Divanı içtihatlarına dair kapsamlı bir inceleme, Divan'ın sessiz kalma hakkı ve kendini suçlu durumuna düşürmeme ilkesi ile ilgili soruları klasik olarak nasıl yanıtladığını bize öğretmektedir. Dolayısıyla hukuk, bize bir şifre çözme zorunluluğu ile nasıl başa çıkılacağı konusunda bir fikir verebilir. Bununla birlikte, şifre çözme sorununun acayipliği (sadece anahtar zorlama yoluyla elde edilir, ancak potansiyel olarak birçok bilginin erişilebilir/okunabilir hale gelmesini sağlar), mevcut durumlarla karşılaştırma yapmayı ve Mahkeme'nin yaklaşımına dair bir tahminde bulunmayı zorlaştırmaktadır.

AİHM'nin kendini suçlu durumuna düşürmeme ilkesine ilişkin kararları da genellikle aynı yaklaşımı izlemektedir, söz konusu kararların okunmasından en azından AİHM'nin yaklaşımı çıkarılabilir.[151] Şüpheliyi parolasını vermeye zorlamak temel insan haklarıyla bağdaştırılabiliyorsa, bu soru analiz edilirken aşağıdaki üç soru sorulmalı ve yanıtlanmalıdır:

1. *Suçlu duruma düşürmeme* ilkesinden taviz verilecek mi?
2. Söz konusu ilke özünde etkilenmekte midir?
3. İhlal haklı gerekçelere dayandırılabilir mi?

1. Suçlu duruma düşürmeme ilkesinden taviz verilecek mi?

Mahkeme öncelikle *suçlu duruma düşürmeme* ilkesinin ihlal edilip edilmediğini soruşturur. Bu soruşturma iki alt soruya ayrılmaktadır.

---

[149] AİHM 11 Temmuz 2006, no. 54810/00, Jalloh/Almanya, §110-113.

[150] Bu, Belçika kılavuzu *Cybercrime* 3.0, J. KERKHOFS ve P. VAN LINTHOUT, Politeia, Brüksel, 2019, sayfa 541-568 içinde savunma avukatı Dr. Charlotte CONINGS ve federal hâkim Jan KERKHOFS tarafından yapılan analizin bir uyarlaması ve çevirisidir.

[151] Aynı zamanda ilham kaynağı olarak da hizmet eden, konuyla ilgili ayrıntılı bir analiz için bkz.: C. Conings, *Suç delilleri için klasik ve dijital arama,* Antwerp, Intersentia, 554-556.

(1) Zorlama hükümet tarafından mı yapılıyor? Mahkeme, bir cezai yaptırım tehdidini zorlama olarak dikkate almaktadır.[152] Aynı husus, örneğin, işbirliği yapmayı reddetmekten kaynaklanan olumsuz bir çıkarım için de geçerlidir.[153]

(2) Zorlama, doğrudan veya dolaylı olarak davalıdan potansiyel olarak kendini suçlayıcı deliller elde etmek için mi yapılıyor?

Bununla birlikte, potansiyel olarak kendini suçlayıcı deliller elde etmek amacıyla sanığa yapılan her zorlama, kendini *suçlu duruma düşürmeme* ilkesine ilişkin bir ihlal teşkil etmez; örneğin Mahkeme uzun süredir DNA materyalinin zorlama ile alınmasının söz konusu ilkeye aykırı olmadığını kabul etmektedir[154]. Bu nedenle, bu hususta daha fazla analiz yapılması gerekmektedir.

a. İlke

AİHM, suçlu duruma düşürmeme ilkesinin ve sessiz kalma hakkının, yargı hatalarını önlemek ve AİHS'nin 6. maddesinin (adil yargılanma hakkı) amacına ulaşmak için sanığı hükümetin hukuka aykırı baskısına karşı korumayı amaçladığına içtihatlarında sürekli olarak işaret etmektedir.[155] Mahkeme'ye göre bu hak, özellikle sanığın bir sorgulama bağlamında sessiz kalma özgürlüğünü güvence altına almakta ve bir kişinin ifade vermeye zorlanmasına ilişkin yasağı içermektedir[156]. Bu nedenle, *suçlu duruma düşürmeme* ilkesi, öncelikle zorla alınan kendini suçlayıcı ifadelere karşı koruma sağlar. Mahkeme haklı olarak bu konuda duyarlı olduğunu göstermektedir. Zorlama uygulaması gerçekten de yanlış ifadelere yol açabilir. İşkence altında alınan bir itiraf bunun tipik bir örneğidir. İtirafın içeriği tamamen ifadeleri veren kişinin iradesine bağlıdır. Zorlama, söz konusu içeriği ve dolayısıyla da "delili" etkileyebilir. Dolayısıyla bu durumda delilin güvenilirliğinin ve adil yargılanma hakkının etkilenmesi riski yüksektir. Zorla alınan ifadelere karşı yeterli bir koruma sağlanması bu yüzden önemlidir. Ancak, bu sorun bir anahtarın zorla elde edilebilirliğinde bir rol oynamamaktadır. Söz konusu anahtar ister bir dizi harften ve rakamdan, ister biyometrik verilerden oluşsun, soruşturma altındaki suçla ilgili yanlış, suçlayıcı beyanlarda bulunulması riski yoktur.[157]

---

152 AİHM 25 Şubat 1993, No 10828/84, Funke/Fransa; AİHM 17 Aralık 1996, No 19187/91, Saunders/Birleşik Krallık; AİHM 21 Aralık 2000, No 34720/97, Heaney ve McGuinness/İrlanda; AİHM 21 Aralık 2000, No 36887/97, Quinn/İrlanda; AİHM 3 Mayıs 2001, No 31827/96, J.B./İsviçre; AİHM 8 Nisan 2004, No 36887/97, Quinn/İrlanda; AİHM 3 Mayıs 2001, No 31827/96, J.B./İsviçre; AİHM 8 Nisan 2004, No 31827/96, J.B./İsviçre. 38544/97, Weh/Avusturya; AİHM 4 Ekim 2005, no. 6563/03, Shannon/Birleşik Krallık; AİHM 29 Haziran 2007, no. 15809/02 ve 25624/02, O'Halloran ve Francis/Birleşik Krallık; AİHM 14 Ekim 2010, no. 1466/07, Brusco/Fransa; AİHM 5 Nisan 2012, no. 11663/04, Chambaz/İsviçre.

153 AİHM 8 Şubat 1996, no. 18731/91, John Murray/Birleşik Krallık; AİHM 18 Mart 2010, no. 13201/05, Krumpholz/Avusturya.

154 AİHM 17 Aralık 1996, no. 19187/91, Saunders/Birleşik Krallık.

155 AİHM 25 Şubat 1993, No 10828/84, Funke/Fransa; AİHM 8 Şubat 1996, No 18731/91, John Murray/Birleşik Krallık; AİHM 17 Aralık 1996, No 19187/91, Saunders/Birleşik Krallık; AİHM 21 Aralık 2000, No 34720/97, Heaney ve McGuinness/İrlanda; AİHM 21 Aralık 2000, No 34720/97, Heaney ve McGuinness/İrlanda. 36887/97, Quinn/İrlanda; AİHM 3 Mayıs 2001, No 31827/96, J.B./İsviçre; AİHM 10 Eylül 2002, No 76574/01, Allen/Birleşik Krallık; AİHM 5 Kasım 2002, No 48539/99, Allan/Birleşik Krallık; AİHM 8 Nisan 2004, No 76574/01, Allan/Birleşik Krallık. 42371/02, Pavlenko/Rusya; AİHM 14 Ekim 2010, no 1466/07, Brusco/Fransa; AİHM 5 Nisan 2012, no 11663/04, Chambaz/İsviçre; AİHM 31 Ekim 2013, no 17416/03, Tarasov/Ukrayna; AİHM 31 Ocak 2017, no 40233/07, Kalnéniené/Belçika.

156 AİHM 11 Temmuz 2006, no. 54810/00, Jalloh/Duitsland: *"Kendini suçlamama ayrıcalığı, Taraf Devletlerde ve başka yerlerde genel olarak, esasen davalının sorgulama karşısında sessiz kalma iradesine saygı göstermek ve ifade vermeye zorlanmaması ile ilgili olarak anlaşılmaktadır."*

157 Bu bağlamda bkz.: AİHM 17 Aralık 1996, no. 19187/91, Saunders/Birleşik Krallık; AİHM 21 Aralık 2000, no. 34720/97, Heaney ve McGuinness/İrlanda; AİHM 21 Aralık 2000, no. 34720/97, Heaney ve McGuinness/İrlanda. 36887/97, Quinn/İrlanda; AİHM 29 Haziran 2007, No. 15809/02 ve 25624/02, O'Halloran ve Francis/Birleşik

Mahkeme, *suçlu duruma düşürmeme* ilkesinin ihlal edilip edilmediği sorusunu değerlendirirken, *suçlu duruma düşürmeme* ilkesinin uygulanmadığı, *davalının iradesinden bağımsız olarak var olan materyal* ile *davalının iradesine bağlı olarak var olan materyal arasında bir ayrım yapmaktadır*[158]. Bu ayrım, diğer hususların yanı sıra, ifade özgürlüğü bağlamında görülmelidir. Bu nedenle, materyalin varlığının iradeye bağımlı olup olmadığına, zorlamanın uygulandığı andaki duruma göre karar verilmelidir. Delilin yine de tam o anda vücut *bulması* gerekir ve varlığı (ve dolayısıyla içeriği de) sanığın iradesine bağlı olmalıdır[159], bunun bir sonucu olarak, zorlamanın uygulanması *yoluyla* yukarıda bahsedilen gerçekliğin çarpıtılmış bir şekilde temsil edilmesi riski ortaya çıkmaktadır. Zorla elde edilen anahtar, bir şifre çözme zorunluluğu dolayısıyla zorla alındığı anda zaten mevcut olduğu için, diğer şeylerin yanı sıra anahtarın varlığı da iradeden bağımsızdır. Anahtar - yukarıda da belirtildiği gibi - şüphelinin iradesinden bağımsız olarak mevcuttur ve söylenen anahtarın doğruluğu hemen kontrol edilebilir. Gerçeğin değiştirilmesi riski yoktur.

Mahkeme'nin kendisi, davalının iradesinden bağımsız olarak var olan birkaç materyal örneğinden alıntı yapmaktadır. Suçlu duruma düşürmeme yasasının bu tür delillere uygulanmadığını açıkça belirtmektedir:

"*Kendini suçlu duruma düşürmeme hakkı, öncelikle suçlanan kişinin sessiz kalma iradesine saygı gösterilmesi ile ilgilidir. Sözleşmeyi İmzalayan Taraflarının hukuk sistemlerinde ve başka yerlerde yaygın olarak anlaşıldığı üzere, bu husus, diğerlerinin yanı sıra,* ***bir mahkeme emri uyarınca edinilen belgeler, DNA testi amacıyla izin belgesi, nefes, kan ve idrar örnekleri ve vücut dokusu*** *gibi şüphelinin iradesinden bağımsız olarak var olan materyallerin cezai kovuşturmada kullanılmasını kapsamamaktadır.*"[160]

Birleşik Krallık'taki P.G. ve J.H. davasında Mahkeme bu listeye ses kaydını da eklemektedir. Mahkeme basitçe, kendini suçlu duruma düşürmeme hakkının bu tür materyaller için geçerli olmadığını ifade etmektedir. Bu ses kaydı izinin nasıl elde edildiği (*bu davada* gizli kayıtlar yoluyla elde edilmiştir) bu bakımdan önemsizdir:

"*Başvuru sahipleri, karşılaştırma için ses örneklerinin gizlice elde edilmesinden ve bunun kendini suçlu duruma düşürmeme ayrıcalıklarını ihlal ettiğinden şikayet ettikleri için Mahkeme, herhangi bir suçlayıcı ifade içermeyen ses örneklerinin adli analizde kullanılan kan, saç veya diğer fiziksel veya nesnel numunelere benzer kabul edilebileceği ve kendini*

Krallık; AİHM 18 Mart 2010, No. 13201/05, Krumpholz/Avusturya; AİHM 31 Ekim 2013, No. 17416/03, Tarasov/Ukrayna.

158 AİHM 17 Aralık 1996, no. 19187/91, Saunders/Birleşik Krallık, §92. Söz konusu kriter yakın zamanda onaylanmıştır: AİHM 31 Ocak 2017 , no. 40233/07, § 52: *"Son olarak, sessiz kalma ve kendini suçlu durumuna düşürmeme hakkına ilişkin olarak, Birleşik Krallık'a karşı Allan (yukarıda anılan, §§ 50-53) davasının aksine, başvuru sahibinden itiraf ve kendini suçlayıcı ifadeler almak için zorlama veya baskı, hatta aldatmaca bile yapılmamış gibi görünmektedir. Aksine, elkoyma sırasında yapılan edinimler, başvuru sahibinin iradesinden bağımsız olarak var olan maddi unsurlardır. Aynı kriter, masumiyet karinesine ilişkin AB Direktifinde de bulunmaktadır (Masumiyet karinesinin belirli yönlerinin güçlendirilmesine ve ceza yargılamasında duruşmada hazır bulunmaya ilişkin 9 Mart 2016 tarihli (EU) 2016/343 sayılı Avrupa Parlamentosu ve Konsey Direktifi, R.G. L. 11 Mart 2016, no. 65, Madde 7.3'e göre: "Kendini suçlu duruma düşürmeme hakkının kullanılması, yetkili makamların, yasal zorlama kullanılarak hukuka uygun olarak elde edilen ve şüpheli veya sanıkların iradesinden bağımsız olarak var olan bu tür delilleri toplamasını engellemez").*

159 Mahkeme'nin kendisinin soruşturma emri ile elkonulabilecek belgelere, sanığın iradesinden bağımsız olarak var olan materyal olarak atıfta bulunması olgusu bunu doğrulamaktadır. Bu belgelerin geçmişte sanığın iradesiyle oluşturulmuş olması ve dolayısıyla varlıklarının bir zamanlar sanığın iradesine bağlı olması mümkünse de, infaz anında bunlar sanığın iradesinden bağımsız olarak var olan materyaller teşkil etmektedir. Belgeler mevcuttur ve şüphelinin iradesi temelindeki hiçbir şey bunu değiştiremez.

160 AİHM 17 Aralık 1996, no. 19187/91, Saunders/Birleşik Krallık, §92.

suçlu duruma düşürmeme ayrıcalığının bu durum için geçerli olmadığı değerlendirmesini yapmıştır."[161]

Bu içtihada dayanarak, diğer şeylerin yanı sıra, potansiyel delillerin anahtarı olabilecek biyometrik verileri (örneğin, bir iris taraması, yüz taraması, parmak izi veya muhtemelen bir bilişim sisteminin veya dosyaların şifresinin çözülmesine imkan tanıyan sesi) baskı altında elde etmenin *suçlu duruma düşürmeme* ilkesi ışığında sorunlu olmadığı savunulabilir.

Örneğin sayı ve harflerden oluşan bir anahtarın elde edilmesine ilişkin analizin bundan farklı olması için bir sebep görmüyoruz. Bu durumda anahtar bir ifade gibi görünebilir, ancak bir ifade ile denk kabul edilemez. Sabit bir gerçektir. İfade özgürlüğünün korunmasını elzem kılan delillerin güvenilirliğini zedeleme riski, zorla alınan anahtar düzeyinde bir rol oynamamaktadır.

İki tür anahtar arasında da, kişinin biyometrik verilerinin elde edilmesinin mutlaka ilgili kişinin işbirliğine bağlı olmadığı, oysa harf ve sayıların kombinasyonu için işbirliğinin gerekli olduğu gerekçeleriyle haklı görülebilecek bir ayrım yoktur. Her şeyden önce, örneğin bir iris taraması alınabilmesi için, (hızlı bir şekilde aşağılayıcı ve insanlık dışı hale gelecek ve bu nedenle de AİHS›nin 3. maddesinin ihlali anlamına gelecek kadar ciddi bir zorlama olmaması amacıyla) bize göre ilgili kişinin de fiziksel olarak işbirliği yapması gereklidir. Aynı durum; idrar, verilen nefes ve ses çıktılarının alınması için de geçerlidir. Jalloh/Almanya davasında Mahkeme, *suçlu duruma düşürmeme* ilkesinin sanığın vücut materyalinin elde edilmesi için sınırlı aktif işbirliği durumunda da geçerli olmadığını açıkça kabul etmektedir (*bkz. aşağıda*).[162] Sonuç olarak, bu da farklı şifreleme türleri arasında bir ayrımı haklı çıkaramaz.

b. İstisna

Sessiz kalma hakkı ve *suçlu duruma düşürmeme* ilkesi, sanığın iradesinden bağımsız olarak var olan deliller için ilke olarak geçerli olmayabilir, ancak bunun istisnaları vardır. Her şeye rağmen, Mahkemenin ilgili kişinin iradesinden bağımsız olarak var olan delillerin zorla alınmasının *suçlu duruma düşürmeme* ilkesine ilişkin bir ihlal teşkil ettiğine karar verdiği içtihatlar da mevcuttur. Bu, sürekli olarak, hükümetin talebi üzerine sanığın "maddi delil" sağlama görevi ile ilgilidir.[163] Ancak Mahkeme, *suçlu duruma düşürmeme* ilkesinin neden geçerli olduğuna dair net kriterler ve hepsinden önemlisi net bir *gerekçe* sunmamaktadır.

Daha belirgin bir anlatımla, Funke/Fransa davası, kamu makamlarının varlığından emin olmasalar da var olduğuna inandıkları belgelerin davalı tarafından teslim edilmesi yükümlülüğünü içeriyordu. Bu belgeleri kendileri almayı başaramadıkları zaman, sanığı belgeleri teslim etmesi için zor kullanarak ikna etmeye çalışmışlardır. Mahkemeye göre bu, sessiz kalma hakkına ve kendini suçlu duruma düşürmeme ilkesine ilişkin bir ihlal teşkil etmektedir[164]. J.B./İsviçre davasında da Mahkeme, belgelerin teslim

---

161 AİHM 25 Eylül 2001, no. 44787/98, P.G. ve J.H/B.K., § 80.

162 AİHM 11 Temmuz 2006, no. 54810/00, Jalloh/Almanya.

163 Bkz. AİHM 25 Şubat 1993, no. 10828/84, Funke/Fransa; AİHM 3 Mayıs 2001, no. 31827/96, J.B./İsviçre; AİHM 11 Temmuz 2006, no. 54810/00, Jalloh/Almanya.

164 AİHM 25 Şubat 1993, no. 10828/84, Funke/Fransa: *"Mahkeme, gümrük görevlilerinin, gerçekten emin olmamalarına karşın, var olması gerektiğine inandıkları bazı belgeleri elde etmek için Bay Funke'nin suçluluğuna kesin gözüyle baktıklarına dikkat çekmektedir. Başka yollarla elde edemedikleri veya elde etmek istemedikleri için, başvuru sahibini, işlediği iddia edilen suçlara dair delilleri kendisinin sunması için zorlamaya çalışmışlardır. Gümrük hukukunun ken-*

edilmesi için bir emir vermeyi düşünmüştür. Burada da Mahkeme, kamu makamlarının iletilecek bilgilerin varlığından henüz haberdarmış gibi görünmedikleri gerçeğine önem veriyor gibi görünmektedir. Söz konusu davada da Temyiz Mahkemesi, kapsamlı bir inceleme yapmadan suç duyurusunda bulunmama ilkesini ihlal etmeye karar vermiştir. Şifrenin çözülmesi emrine aktarıldığında, bu durum her şeyden önce şifrelenmiş verilerin ve anahtarın mevcut olduğunun ve davalının bu anahtara ilişkin bilgiye sahip olduğunun ciddi bir şekilde ispatlanması gerekliliğine dönüşebilir (*altta*).

Funke/Fransa ve J.B./İsviçre davalarında Mahkeme'nin, istenen belgelerin var olduğunun belirsiz olduğuna açıkça atıfta bulunduğu gerçeğini göz önüne alarak, Mahkeme'nin burada ispat yükünün tersine çevrilemeyeceğini önemli bulduğuna inanıyoruz.[165] Bu bağlamda bazen delilin sanığın iradesinden bağımsız olarak *elde edilmiş* olup olmadığı kriterine atıfta bulunulmaktadır.[166] Suç delillerinin izini sürmek, her şeyden önce soruşturma makamlarının görevidir ve öyle olmaya devam edecektir ve söz konusu görev, bir işbirliği görevi aracılığıyla sanığa devredilemez. Gerçekten de Mahkeme, genellikle sessiz kalma hakkını masumiyet karinesine bağlamaktadır.[167] İspat yükünün devredilmesi ile, işbirliği yapmak isteyen fakat (gerekli bilgiye sahip olmadığı için) işbirliği yapamayan bir kişinin yine de işbirliği yapmaması dolayısıyla hüküm giymesi riski vardır. Bu nedenle, bu durumlarda masumiyet karinesinin baltalanması riski yüksektir.

Funke ve J.B. içtihatlarını şifre çözme yükümlülüğüne uyguladığımızda, hükümet bir bilgisayar sisteminin şifresini çözmek için şüpheliye zorla iris taraması yaptığında, parmak izi aldığında veya yüz veya ses tanıma uyguladığında, ilk olarak ispat yükünün hiçbir durumda tersine çevrilmediğini tespit ederiz. Soruşturma makamlarının kendileri, delil zincirindeki her unsuru, yani bilgisayar sistemini, anahtarı, şifreli materyalleri ararlar. Funke ve J.B. mahkemeleri bu nedenle biyometrik verilerin zorla elde edilmesine karşı değildir.

O zaman da, anahtar türüne göre bir ayrımın koruma konusundaki bir farklılığı haklı gösterip gösteremeyeceği sorusu ortaya çıkmaktadır. Örneğin, biyometrik verilerin kullanıldığı şifreleme durumunda, veri öznesinin söz konusu koda sahip olup olmadığına ilişkin ifadenin doğruluğu hemen kontrol edilebileceği için, ilke olarak bir ayrım aslında gerekçelendirilebilir. Bu bağlamda, "anahtarı" teslim etmenin reddedilmesine dayalı bir mahkumiyet kararının masumiyet karinesini etkileme riski bulunmamaktadır. Bu reddetmenin sadece iki nedeni olabilir. Ya şüpheli anahtarı (biyometrik verileri) teslim etmek istemiyordur, bu durumda kamu yararı gerekçelerinin onu şifreyi çöz-

---

dine özgü özellikleri (bkz. yukarıdaki 30-31. paragraflar), bu ifadenin 6. maddedeki müstakil anlamı çerçevesinde, "bir suç isnat edilen" herhangi birinin, sessiz kalma ve kendini suçlu duruma düşürmeye katkıda bulunmama hakkının bu şekilde ihlal edilmesini haklı çıkaramaz."

Bu nedenle yasa koyucu haklı olarak madde 88 §2 içindeki "belirli verileri arama" görevinin, sanığa dayatıldığı zaman kendini suçlu duruma düşürmeme ilkesine aykırı olduğunu belirtmektedir.

165 Bu nedenle yasa koyucu haklı olarak madde 88 §2 içindeki "belirli verileri arama" görevinin, sanığa dayatıldığı zaman kendini suçlu duruma düşürmeme ilkesine aykırı olduğunu belirtmektedir.

166 Bkz. örneğin Corr. Dendermonde 17 Kasım 2014, NJW 2016, afl. 336, 132, not C. Conings; D. Dewandeleer, R. Verstraeten ve F. Verbruggen, Ceza ve Ceza Usul Hukuku içinde "Bilişim bağlamında suçlar ve ceza soruşturmaları", Bruges, die Keure, 2009-10, (125) 159-160, dipnot no. 126.

167 AİHM 25 Şubat 1993, No 10828/84, Funke/Fransa; AİHM 8 Şubat 1996, No 18731/91, John Murray/Birleşik Krallık; AİHM 17 Aralık 1996, No 19187/91, Saunders/Birleşik Krallık; AİHM 20 Ekim 1997, No 20225/92, Serves/Fransa; AİHM 21 Aralık 2000, No 34720/97, Heaney ve McGuinness/İrlanda; AİHM 21 Aralık 2000, No 34720/97, Heaney ve McGuinness/İrlanda. 36887/97, Quinn/İrlanda; AİHM 3 Mayıs 2001, No 31827/96, J.B./İsviçre; AİHM 10 Eylül 2002, No 76574/01, Allen/Birleşik Krallık; AİHM 8 Nisan 2004, No 38544/97, Weh/Ukrayna; AİHM 19 Şubat 2009, No 16404/03, Shabelnik/Ukrayna; AİHM 31 Ekim 2013, No 17416/03, Tarasov/Ukrayna.

meye zorlaması halinde haklı olarak cezalandırılabilir. Ya da şüpheli anahtarı teslim edemiyordur, çünkü anahtar onun biyometrik verileri değildir. Bu durumda şüpheli, bilgisayar sisteminin veya şifrelenmiş verilerin şifresinin çözülmediğini parmak iziyle, yüzüyle, sesiyle veya gözüyle mükemmel bir şekilde ispat edebilir. Şifreleme rakam ve harflerden oluşuyorsa, ilgili kişinin kodu bilmediğine ilişkin ifadesinin doğru olup olmadığının kontrol edilmesi mümkün değildir. Bu nedenle, sadece ikinci durumda, bir kişinin kodu gerçekten bilmediği halde işbirliği yapmamaktan mahkum edilmesi riski söz konusudur. Bu bağlamda, Belçika savcılığının ilgili kişinin anahtarı (*yukarıdaki*) bildiğine dair yeterli delil sunma görevi bu nedenle büyük önem taşımaktadır. Bu görev, anahtarın türüne göre farklı muamele görmeye ilişkin sebebi ortadan kaldırır. Dahası, savcının, potansiyel olarak suç unsuru olan "anahtar bilgisi" (çocuk pornografisi bulundurma ile ilgili olarak *yukarıdaki* - İngiltere'de mücadele edilen husus) bakımından ispat yükünün güvence altına alınmasını sağlayan bu ispat ilkesi görevi de tersine çevrilmemiştir. Ayrıca Funke ve J.B. içtihatlarına dayanarak, sonucunda Savcılığın şüphelinin anahtar hakkında bilgi sahibi olduğunu yeterli şekilde ispatlamak zorunda olduğu, bu nedenle anahtarın şifresini çözme zorunluluğunun, *kendini suçlu duruma düşürmeme* ilkesini ihlal etmediği sonucuna varma cüretini gösteriyoruz.

Son olarak, Jalloh/Almanya davası, söz konusu kişinin yutmuş olduğu uyuşturucu dozlarının elde edilmesi için bir kişiye fiziksel cebir uygulanması (kusturucu ilaç verilmesi) ile ilgilidir. Bu davada Mahkeme *kendini suçlu duruma düşürmeme* ilkesinin kapsamını netleştirmeye çalışır:

"[Mahkeme], kendini suçlu duruma düşürmeme ayrıcalığının, Sözleşmeyi İmzalayan Devletlerde ve başka yerlerde genel olarak, öncelikle *davalının sorgulama karşısında* ***sessiz*** *kalma ve bir* ***ifade*** *vermeye* ***zorlanmama*** *iradesine saygı göstermekle ilgili olarak anlaşıldığını kaydetmektedir. Ancak Mahkeme zaman zaman 6. madde § 1 kapsamında korunan kendini suçlu durumuna düşürmeme ilkesine, yetkililere* ***gerçek delillerin teslim edilmesi için zor kullanımı*** söz konusu olan davaları kapsayacak şekilde daha ***geniş bir anlam*** *vermiştir* [Funke/Fransa ve JB/İsviçre davaları referans alınarak]. *Saunders davasında Mahkeme, kendini suçlu duruma düşürmeme ilkesinin, "cebri güç kullanılması yoluyla sanıktan elde edilebilecek ancak diğerlerinin yanı sıra bir mahkeme emri gereğince elde edilen belgeler, DNA testi amacıyla nefes, kan ve idrar numuneleri ve vücut dokuları gibi şüphelinin* ***iradesinden bağımsız*** *olarak var olan materyalleri"* ***kapsamadığı*** *kanaatine varmıştır. Mahkeme'ye göre, mevcut davada söz konusu deliller, yani başvuru sahibinin vücudunda saklanan, zorla kusturucu ilaç verilmek suretiyle elde edilen uyuşturucular, kullanımı genellikle cezai kovuşturmalar içinde yasaklanmayan, şüphelinin iradesinden bağımsız bir varlığı olan materyaller kategorisine girdikleri düşünülebilir."*[168]

Mahkeme, davalının iradesinden bağımsız olarak var olan delillerle ilgili olmasına rağmen, bu davada neden kendini suçlu duruma düşürmeme ilkesinin geçerli olduğunu düşündüğünü açıklamaya devam etmektedir. Gerçekten de, Mahkeme'nin gözünde davanın Saunders davasında sıralanan örneklerden farklı olmasının birkaç nedeni vardır:

1. *Funke* ve *J.B.* davalarında olduğu gibi, maddi delil elde etmek için kişiye cebir uygulanmıştır. Saunders davasında listelenen vücut materyalleri ise, örneğin alkol veya uyuşturucu varlığının belirlenmesi amacıyla daha ileri adli inceleme için

---

[168] AİHM 11 Temmuz 2006, no. 54810/00, Jalloh/Almanya, §110-113.

baskı altında elde edilen materyallerdir. Bu noktada, şifre çözme görevini, kendi başına maddi delil teşkil etmeyen bir anahtarı zorla teslim etme görevi olarak anlamamız gerekip gerekmediği veya şifre çözme görevi ile, açıkça potansiyel olarak sağlam delil teşkil eden tüm temel verilerin de esasen şüpheli tarafından baskı altında sağlanıp sağlanmadığı sorusu ortaya çıkmaktadır. Bu ikinci yorumda, anahtarın şifresini çözme zorunluluğu, sessiz kalma hakkına ilişkin bir ihlale yol açmaktadır. Bu, anahtarın türünden kesinlikle bağımsızdır. Bu yorumda, bir sayı ve harf kodunu zorla vererek veya parmak izini veya diğer biyometrik verileri zorla alınarak şüpheli, zorlama sonucunda her zaman için tüm temel verileri teslim edecektir. Ancak biz bu yorumu desteklemiyoruz. Kan, nefes veya idrar, aynı zamanda kan alındığında veya şüphelinin üzerinde cebir uygulanarak yapılan bir nefes analizi veya idrar testi bağlamında da elde edilir. Fakat, müfettişler kan, nefes veya idrarla birlikte, aynı zamanda bir suça dair sağlam delil de olabilen, alkol veya uyuşturucu yüzdesini de baskı altında elde ederler. Bu nedenle, buradaki daha katı olan yorumun doğru yorum olduğunu iddia etme cüretini gösteriyoruz. Zorlama yoluyla, müfettişlerin kendilerinin tespit ettiği ancak okuyamadıkları potansiyel delillere ilişkin anahtar elde edilir. Bu nedenle müfettişler, kişi üzerinde herhangi bir baskı olmaksızın bilgisayar sistemini veya ilgili verileri zaten saptamışlardır. Dolayısıyla ne bilgisayar sistemi, ne de dosyalar ve veriler kişiye baskı yapılarak elde edilmemiştir. Delillerin keşfedilmesi her zaman şifre çözme emrinden önce olur ve gerekirse ondan sonra da devam eder. Sadece potansiyel olarak ilginç bir bilgisayar sistemi veya veri tespit edildiğinde, bulunduğunda ve izole edildiğinde, bulunan verilerin okunabilir hale getirilmesi için bir emir çıkarılır. Bu emir doğrudan, tespit edilen ancak şifrelenmiş haldeki bilgiler ile ilgilidir. Şifrelenmiş bilgiler belirli bir boyuttaysa, şifresi çözüldükten sonra bilgileri taramaya devam edecek olan da yine soruşturma makamları olacaktır. Aynı şekilde, aramanın bir parçası olarak bir konutun açılması emri, delillerin nereye saklandığının söylenmesine ilişkin bir emirden farklı olacaktır. Şifre çözme emri, dijital çilingirlikten daha fazlası veya daha azı değildir.

2. Uygulanan baskının derecesi de Saunders davasında listelenen materyalleri elde etmek için gereken zorlamadan açık bir şekilde farklıdır. Sonuçta, ikincisi sadece şüphelinin pasif olarak fiziksel bütünlüğüne sınırlı müdahaleye maruz kalmasını veya vücudun normal işleyişinden dolayı materyal temini konusunda aktif olarak işbirliği yapmasını gerektirir. İkincisi için Mahkeme açıkça nefes, idrar ve ses çıktılarına atıfta bulunur. Öte yandan, Jalloh davasında uygulanan baskı düzeyi, AİHS'nin 3. maddesinde öngörüldüğü şekilde işkence, insanlık dışı ve aşağılayıcı muamele yasağına ilişkin bir ihlal bile teşkil edecek kadar olmuştur. Bu anlamda Jalloh davası oldukça uyumsuz bir davadır, çünkü Mahkemenin özellikle baskının uygulanma şekline karşı hassas olduğu görülmektedir. Klasik olarak, baskının niteliği ve derecesi, yalnızca sessiz kalma hakkına ilişkin bir ihlalin olası bir gerekçesi düzeyinde bir rol oynar (*aşağıda*). Söz konusu zorlamanın özel yanı, reddetme iradesini ve kabiliyetini ortadan kaldırmış olmasıdır. Zorla DNA, kan veya idrar alındığında, bu zorlama, şüphelinin özgürlüğüne ve mutabık olmama iradesine saygı gösterilerek maddi delillerin doğrudan alınması ile ilgilidir. Jalloh/Almanya davasında, bir (kusturucu) ilacın verilmesini ve böylece zorlama yoluyla şüphelinin irade özgürlüğünün kırılmasını içeren bir tür *sektirme zorlaması* uygulanmış, bunun sonucunda artık vücudunun delili kendiliğinden teslim etmesini (boşaltmasını) engelleyememiştir. Başka bir deyişle, vücut kendiliğinden ve dahası doğal olmayan bir şekilde

işbirliği yapmaya zorlanmıştır. Bu, itiraf ettirmek için bir şüphelinin hipnoz altında sorguya çekilmesine benzemektedir.

c. Şifre çözme zorunluluğuna ilişkin sonuç

Yukarıdakiler ışığında, AİHM içtihadı esasında, bir bilişim sistemi anahtarının iletilmesine ilişkin cezai görevin, hangi biçimde olursa olsun, söz konusu ilkeyi ve dolayısıyla da AİHS'nin 6. maddesini etkilemediği görüşündeyiz. Aynı husus, diğerlerinin yanı sıra, esasen aynı anlama geldiğinden, anahtarın kendisini sağlamaya ilişkin cezai görev için de geçerlidir. Anahtarı, sanığın kendisinin vermesi görevi, bu bağlamda mahremiyet hakkına daha sınırlı müdahale ve daha sınırlı istismar riski göz önüne alındığında, anahtarı iletme görevine göre bile daha tercih edilir bir görevdir. Sonuçta, parola birkaç dosya veya sistem için aynı olabilir.[169]

Denetimi azaltma yükümlülüğüne ilişkin bu ilk sorunun cevabına ilişkin tartışma, sorunun kendine has özellikleri göz önüne alındığında olası olduğu için, eksiksiz olması adına, denetimi azaltma yükümlülüğüne ilişkin analizi *kendini suçlu duruma düşürmeme* ilkesi ışığında aşağıda daha ayrıntılı olarak tartışacağız. Bununla birlikte, aşağıda tartışılan soruların, sadece şifre çözme görevinin *kendini suçlu duruma düşürmeme* ilkesine ilişkin bir ihlal olarak hesaba katıldığı ölçüde cevaplanması gerekir.

2. Söz konusu ilke özünde etkilenmekte midir?

Mahkeme, *kendini suçlu duruma düşürmeme* ilkesinin ihlal edildiğini tespit ettiğinde, ilkenin esastan ihlal edilip edilmediğini inceler. İlkenin esastan ihlal edilmesi hiçbir koşulda haklı görülemez (*aşağıda*). İlkenin özünde bir ihlal olup olmadığını Mahkeme aşağıdaki kriterler esasında değerlendirir:[170] (1) zorlamanın ve sorgulamanın niteliği ve derecesi, (2) ilgili usule ilişkin güvencelerin var olması ve (3) zorla elde edilen materyalin ne ölçüde kullanıldığı. Aşağıda bu üç kriteri inceleyip, bunları hemen Belçika şifre çözme zorunluluğuna uyguluyoruz. Yine, mevcut içtihat temelinde, AİHM'nin, *kendini suçlu duruma düşürmeme* ilkesinin şifre çözme zorunluluğunu baltaladığını değerlendirmesi halinde, bunu bir esastan ihlal olarak görüp görmeyeceğini tahmin etmenin zor olduğu ortaya çıkacaktır.

1. Bu davada ağır hapis cezaları tehdidinde bulunulması gibi ciddi zorlama biçimleri, hızla ilkenin esastan ihlaline yol açmaktadır. Aynı durum, açıklama özgürlüğü üzerinde büyük bir kısıtlama[171] veya potansiyel delillerin teslimine ilişkin kapsamlı bir emir[172] teşkil eden kapsamlı aramalar için de geçerlidir. Öte yandan, sınırlı ara-

---

169 23 Kasım 2001 tarihli Bilişim Suçları Sözleşmesi'ne ilişkin açıklayıcı rapor, http://conventions.coe.int/Treaty/EN/Reports/html/185.htm, § 202; Komisyon adına rapor, Parl.St. Senato 1999-2000, no. 2-392/3, 69-70.

170 AİHM 5 Kasım 2002, No 48539/99, Allan/Birleşik Krallık; AİHM 11 Temmuz 2006, No 54810/00, Jalloh/Almanya; AİHM 29 Haziran 2007, No 15809/02 ve No 25624/02, O'Halloran ve Francis/Birleşik Krallık; AİHM 10 Ocak 2008, No 54810/00, Jalloh/Almanya; AİHM 29 Haziran 2007, No 15809/02 ve No 25624/02, O'Halloran ve Francis/Birleşik Krallık; AİHM 10 Ocak 2008, No 54810/00, Jalloh/Almanya. 58452/00 ve 61920/00, Lückhof ve Spanner/Avusturya; AİHM 10 Mart 2009, no. 4378/02, Bykov/Rusya; AİHM 1 Nisan 2010, no. 42371/02, Pavlenko/Rusya; J. Meese, *"Sessizliğin sesi. Ceza davalarında sessiz kalma hakkı ve kendini suçlu duruma düşürmeme ilkesi. Tarihsel ve karşılaştırmalı bir genel bakış"*, J. Rozie, S. Rutten, A. Van Oevelen (ed.), Sessiz kalma hakkı ile konuşma zorunluluğu karşılaştırması, Antwerp, Intersentia, 2013, (37) 41.

171 AİHM 17 Aralık 1996, No 19187/91, Saunders/Birleşik Krallık; AİHM 21 Aralık 2000, No 34720/97, Heaney ve McGuinness/İrlanda; AİHM 4 Ekim 2005, No 6563/03, Shannon/Birleşik Krallık.

172 Örneğin bkz. AİHM 25 Şubat 1993, no. 10828/84, Funke/Frankrijk, mütalaa no 30: *"departmanları açısından şüpheli işlemlerle ilgili her türlü evrak ve belgenin sunulması"*; AİHM 3 Mayıs 2001, no. 31827/96, J.B./İsviçre, mütalaa 39: *"vergilerin değerlendirilmesi ile ilgili olabilecek belgeler vb."*; *AİHM 5 Nisan 2012, no. 11663/04, Chambaz/İsviçre: "ellerindeki defterler, belgeler ve fişler ve vergilendirme açısından önem arz eden [...] sertifikalar ve beyanlar."*.

maların sessiz kalma hakkının esasını etkileme olasılığı daha düşüktür.[173] Zorunlu şifre çözme durumunda, baskı altında sadece çok sınırlı bilgi, yani sadece anahtar (örneğin kod, şifre, oturum açma bilgisi) istenmektedir. Diğer yandan, bu anahtar çok sayıda potansiyel delilin şifresini çözmek için kullanılabilir.

2. Zorlamayı azaltan, usule ilişkin ilgili güvencelerin olması da Mahkeme tarafından dikkate alınmaktadır. Bu, örneğin, davalının neden belirli bilgileri vermediğini veya veremeyeceğini açıklamaya dönük bir fırsatının olması[174] ve yetkililerin inisiyatifi ile bu konuda söyleyeceklerinin dinlenmesi ile ilgilidir.[175] Belçika hukuku uyarınca savcılığın ilgili kişinin anahtarı bildiğine ilişkin delil sunması gerektiği gerçeği, diğer hususların yanı sıra bu açıdan da önemlidir. Bu itibarla Savcılık makamı, sanığın anahtara dair bilgisine ilişkin ileri sürdüğü savunmayı da göz önünde bulundurarak, ilgili kişinin koda aşina olduğunu yeterli şekilde kanıtlamalıdır.

3. Son olarak, Mahkeme, zorla alınan materyalin ne ölçüde kullanıldığını dikkate almaktadır. Asıl soru, elde edilen delillerin, delil toplama bakımından önemli bir rol mü yoksa sınırlı bir rol mü oynadığıdır. Bilgi verme veya işbirliği yapma yükümlülüğü sınırlıysa ve örneğin, temel teşkil eden suçun sadece bir unsuru ile ilgiliyse, o durumda kullanım sınırlıdır ve Mahkeme bunun yerine ilkenin esastan etkilenmediği sonucuna varacaktır. Şifre çözme zorunluluğu bağlamında, terazinin kefelerine tam olarak ne konması gerektiği sorusu tekrar ortaya çıkmaktadır. İlke olarak, soruşturma makamları sadece anahtarın elde edilmesini zorunlu kılmaktadır. Özellikle de Belçika hukuku uyarınca yetkililerin önce şüphelinin anahtara sahip olduğunu ve dolayısıyla anahtarın arkasındaki bilgilere erişimi olduğunu kanıtlamaları gerektiği için[176], anahtarın kendisi delil toplama bakımından bir rol oynamaz. Bu nedenle anahtarın iletilmesi, (sadece) şüphelinin şifrelenmiş bilgilere erişimi olduğuna dair potansiyel olarak suçlayıcı ifadeyi beraberinde getirmez. Bu ifade gerçekten de kendi içinde suçlayıcı olabilir. Örneğin, yukarıda da belirtildiği gibi, anahtarın paylaşılması, şüphelinin çocuk pornografisi materyaline erişimi olduğu ifadesini üstü kapalı olarak ima edebilir. Bu "erişim beyanı", çocuk pornografisi *bulundurma* suçunun nesnel bir unsuruna ilişkin delil sağlar. Ancak bir kez daha, anahtarın zorla alınmasının büyük miktarda bilgiyi erişilebilir ve okunabilir hale getirebileceği düşünülebilir. O zaman asıl soru, bu bilgilerin de "zorla alınmış" olarak kabul edilip edilmeyeceğidir. Bu soruya olumlu yanıt verilmesi halinde, zorla alınan materyal delillerin üretilmesinde kesinlikle potansiyel olarak önemli bir rol oynar. Neden temel delillerin değil de sadece anahtarın zorla alındığına inandığımızı zaten tartışmıştık (*yukarıda*).

---

173 AİHM 29 Haziran 2007, no. 15809/02 ve 25624/02, O'Halloran ve Francis/Birleşik Krallık; AİHM 10 Ocak 2008, no. 58452/00 ve 61920/00, Lückhof ve Spanner/Avusturya.

174 AİHM 29 Haziran 2007, no. 15809/02 ve 25624/02, O'Halloran ve Francis/Birleşik Krallık; AİHM 10 Ocak 2008, no. 58452/00 ve 61920/00, Lückhof ve Spanner/Avusturya.

175 AİHM 18 Mart 2010, no. 13201/05, Krumpholz/Avusturya.

176 AİHM 29 Haziran 2007, no. 15809/02 ve 25624/02, O'Halloran ve Francis/Birleşik Krallık: Bu dava ile bağlantılı olarak işlenen bir trafik suçu sırasında aracı kullanan kişinin kimliğinin belirlenmesi görevi: *"Sürücünün kimliği, hız suçunun yalnızca bir unsurudur ve sadece bölüm 172(2)(a)'nın bir sonucu olarak elde edilen bilgilerle ilgili olarak temel yargılamada ortaya çıkan bir mahkumiyet söz konusu değildir".* Aynı cümlede bkz.: AİHM 10 Mart 2009, no. 4378/02, Bykov/Rusya, gerekçe 103: *"mahkeme tarafından değerlendirilen karmaşık bir deliller bütününde sınırlı bir rol oynamıştır".*

3. İhlal haklı gerekçelere dayandırılabilir mi?

Son olarak, *kendini suçlu duruma düşürmeme* ilkesinin özünde bir ihlal olup olmadığı, AİHM testindeki üçüncü sorunun cevabı için önemlidir: İhlal, bir kamu yararı dolayısıyla haklı görülebilir mi? Her şeye rağmen, ilkenin özünde bir ihlal, en ciddi suç biçimlerine karşı mücadele bağlamında bile asla haklı görülemez.[177]

Bu bağlamda ilginç olan, O'Hallaron ve Francis davasında, trafik suçlarında kimlik tespiti görevi ile ilgili kararıdır. Uygulanan - sınırlı - baskıyı haklı çıkarmak için Mahkeme şu şekilde karar vermiştir: *"Motorlu araç sahibi olan veya kullanan herkes, bunu yaparak kendilerini bir düzenleyici rejime tabi kıldıklarını bilmektedir. Bu rejim, araba sahibi olmak veya kullanmak Devlet tarafından verilen bir ayrıcalık veya hoşgörü olduğu için değil, (örneğin pompalı tüfekler vb. gibi) arabalara sahip olmanın ve kullanmanın ciddi yaralanmalara yol açma potansiyeline sahip olduğu kabul edildiğinden dayatılır". Motorlu araç bulundurmayı ve sürmeyi seçenler, motorlu araçlarla ilgili düzenleyici rejimin bir parçası olarak belirli sorumlulukları ve yükümlülükleri kabul etmiş kabul edilebilirler ve karayolu trafik suçlarının işlendiğinden şüphelenilmesi durumunda, Birleşik Krallık'ın yasal çerçevesi içinde bu sorumluluk, bu durumda sürücünün kimliğinin yetkililere bildirilmesi yükümlülüğünü içerir."*[178] Bir şifre çözme yükümlülüğü bağlamında da benzer bir gerekçelendirme düşünülebilir. Öte yandan, toplum olarak, azami veri güvenliğini sağlamak için herkesin kullanımına açık olması gereken ağır şifreleme biçimlerini genel bir fayda olarak görüyorsak, kullanıcıların bilgisayar kullanımlarıyla ilgili olarak, somut, ciddi bir suç şüphesi durumunda, emir verildiğinde şifreleme anahtarını teslim etme yükümlülüğü de dahil olmak üzere belirli sorumluluklar ve yükümlülükler üstlenmesi gerekmektedir.

4. Uygulamaya ilişkin hususlar

Son olarak, bir şifre çözme emrinin etkililiği hakkında bir soru söz konusu olabilir. Yoksa bu pratik sorunun yanıtlanması yasal sorunun yanıtlanmasından bile daha zordur.

Parmak izi, *damar tanıma*[179], yüz tanıma ve iris taraması gibi biyometrik anahtarlar tipik olarak artan bir güvenli şifreleme hissi sağlarken, bu durum ne yasal ne de pratik sorunlar doğurmamaktadır. Şüpheli yakalanırsa, kullanılan biyometrik anahtarları görmek için (hukuk sisteminize bağlı olarak) kabul edilebilir fiziksel cebir uygulanabilir. Bu, örneğin parmak izinin *kolluk kuvveti marifetiyle* alınması veya bir akıllı telefonun şüphelinin yüzünün önünde tutulması şeklinde olabilir. Ayrıca, belirli durumlarda, örneğin elde edilen parmak izlerinden protezler veya kopyalar yapılabilir. Bu arada, büyük akıllı telefon geliştiricilerinin kademeli olarak *damar tanımaya* geçmelerinin nedenlerinden biri de budur, çünkü bunun bir protez ile kopyalanması çok zordur.

---

177 AİHM 17 Aralık 1996, No 19187/91, Saunders/Birleşik Krallık; AİHM 21 Aralık 2000, No 34720/97, Heaney ve McGuinness/İrlanda; AİHM 21 Aralık 2000, No 36887/97, Quinn/İrlanda; AİHM 10 Mart 2009, No 4378/02, Bykov/Rusya, alıntı 93: *"6. maddede yer alan genel adil yargılama gereklilikleri, söz konusu suçun türüne bakılmaksızın tüm ceza yargılamaları için geçerlidir. Kamu yararı kaygıları, Sözleşme'nin 6. maddesi ile güvence altına alınan kendini suçlu duruma düşürmeme ayrıcalığı da dahil olmak üzere, başvuru sahibinin savunma haklarının esasını ortadan kaldıran tedbirleri haklı çıkaramaz.". Her ne kadar Temyiz Mahkemesi üç farklı soru arasında her zaman net bir ayrım yapmasa da, olası bir gerekçe değerlendirmesi ancak kendini suçlu duruma düşürmeme ilkesinin özünde ihlal edilmediğinin tespit edilmesinden sonra yapılabilir. İkinci adımda kamu yararını göz önünde bulundurmak, kendini suçlu duruma düşürmeme ilkesini* tamamen baltalayacaktır çünkü büyük bir kamu yararı, ciddi baskı biçimlerini bile haklı kılabilir. Ayrıca bkz. Yargıç Pavlovschi ve Yargıç Myjer'in AİHM 29 Haziran 2007, no. 15809/02 ve 25624/02, O'Halloran ve Francis/Birleşik Krallık davalarındaki muhalefet şerhleri; C. Conings, Suç delilleri için klasik ve dijital arama, Antwerp, Intersentia, 549-550.

178 AİHM 29 Haziran 2007, no. 15809/02 ve 25624/02, O'Halloran ve Francis/Birleşik Krallık, §57.

179 Bkz. https://www.bayometric.com/fingerprint-vs-finger-vein-biometric-authentication/

Fakat, sadece akıllı anahtarlar kullanıldığında iş gerçekten zorlaşmaktadır. Böylece, şifreleme sektörü, *makul inkar edilebilirlik* argümanı üzerinde gelişmektedir. Örneğin, VeraCrypt, şifreleme yazılımının her kullanıcısına şu mesajla güvence vermektedir: "*Bir düşmanın sizi parolanızı açıklamaya zorlaması durumunda, VeraCrypt iki tür makul inkar edilebilirlik imkanı sağlar ve destekler*: (...)"[180]. Gizli birimler *olarak adlandırılan dijital kasalar oluşturma olasılığı yazılımın içine yerleştirilmiştir*. Örneğin, sübyancı olduğundan şüphelenilen bir kişi bir şifre çözme emriyle karşı karşıya kalırsa, basitçe sadece ayçiçeklerinin ve yetişkin erkeklerin fotoğraflarını içeren bir disk bölümüne erişim sağlayan bir 'kod' vermektedir. *Gizli işletim sistemleri* de sunulmaktadır: "*Birisi tarafından işletim sisteminin şifresini çözmeye zorlanabilirsiniz. Bunu yapmayı reddedemeyeceğiniz birçok durum vardır (örneğin gasp nedeniyle). VeraCrypt, (belirli yönergelere uyulması koşuluyla) varlığının kanıtlanmasının imkansız olması gereken gizli bir işletim sistemi oluşturmanıza olanak tanımaktadır. Böylece, gizli işletim sistemi için şifreyi çözmek veya şifreyi açıklamak zorunda kalmazsınız*"[181]. İlke olarak, hatta böyle bir gizli işletim *sistemi* asla keşfedilmeyecektir.

Soruşturma uygulamasını ciddi şekilde karmaşıklaştıran bir diğer sorun da, şüpheli tarafından verilen kodu denemenin pekala kötü bir fikir olması ihtimalidir. Belirli uygulamalar, yazılımlar ve cihazlar, girildiğinde veri taşıyıcısını tamamen silen ve bloke eden alternatif - öldürme kodu adı verilen - bir kodun programlanmasına izin vermektedir. Bu nedenle, şüphe edilmesi durumunda, kodun elde edilmesi ve denenmesi amacıyla bir şifre çözme emri verilmesi ve gönüllü olarak verilen bir kod bazında herhangi bir işlem yapılmaması uygun görünmektedir. Daha sonra yukarıda belirtilen emir esasında bir öldürme kodu verildiğinde, en azından bilgisayar aramasını 'engellemek' ulusal hukuka göre ceza gerektiren bir suç olarak kabul edilebiliyorsa, hala bir önlem alınabilir. Sanık tarafından gönüllü olarak verilen bir kodu denemek, günümüzde sadece son çare veya *nihai çözüm* olmalıdır.

Bu, birçok durumda, bir şifre çözme emrinin etkililiğinin, şifre çözme emrinin verildiği soruşturmadaki nesnel gerçeği ortaya çıkarmaya hizmet ettiği sürece yetersiz olabileceğini açıkça göstermektedir. Öte yandan bu, şifreleme özgürlüğünün olumsuz sonuçlarına karşı bir denge sunmaktadır. Bir veri taşıyıcısına erişim izni vermeyi reddetmek, haklı olarak kamu güvenliği ve toplum için doğal bir tehlike barındırdığı için günümüz toplumunda gerçekten cezalandırılabilir. Kendiliğinden suçluluk ayrıca, örneğin bir Çocuğun Cinsel İstismarı Materyali kitaplığının şifrelemenin arkasına gizlendiğine dair ciddi göstergeler olsa bile, aksi takdirde geri dönülmesi gereken veri taşıyıcılarından mahrum kalma olasılığını da yaratmaktadır.

5. Şifre çözme zorunluluğuna ilişkin sonuç

Yargı, dijital çağın kendine özgü niteliğine göre klasik kavramları yeniden düşünme zorluğuyla karşı karşıyadır. Birçok ülkede ilk Ceza (Usul) Kanunları tasarlandığında, bir arama emrinin ve bir çilingirin başa çıkamayacağı yerlerin veya (depolama) alanlarının olabileceği belki de henüz düşünülmemiştir. Şimdi, VeraCrypt[182] gibi bir ücretsiz şifreleme yazılımının, dosyaların sadece 256 bitlik bir şifreleme anahtarı ile açılabilen sanal bir kasaya yerleştirilmesine izin vermesi gibi bir zorlukla karşı karşıya kalıyoruz. Bu

---

180 https://www.veracrypt.fr/en/Plausible%20Deniability.html

181 https://www.veracrypt.fr/en/Hidden%20Operating%20System.html

182 www.veracrypt.fr

yazılım çok yaygındır, yasaldır ve kullanımı da çok kolaydır. Her biri 3 GHz işlemcili ve saniyede 3 milyar işlem yapma gücüne sahip[183] 1.000.000 bilgisayarın işlem gücü ile 256 bitlik bir kodu kırmaya kalksak, yine de kodu kırmanın 1.223.914.354.360.000.000 .000.000.000.000.000.000.000.000.000 yıl sürebileceği gerçeğiyle karşı karşıya kalırız. Birçok durumda bunun dijital deliller için bir *güvenli sığınak* olduğunu söylemek bile yetersiz kalır. Unutulmamalıdır ki, insan hakları aynı zamanda hukukun üstünlüğünün hâkim olduğu devletler için vatandaşlarını ciddi insan hakları ihlallerine karşı korumak konusunda olumlu bir görev oluşturmaktadır. Mevcut koşullarda, yasal olarak güvence altına alınan şifreleme özgürlüğünü, yaşam hakkı (AİHS Madde 2), işkence yasağı (AİHS Madde 3), özgürlük ve güvenlik hakkı (AİHS Madde 5) ve aynı zamanda mahremiyet hakkı (AİHS Madde 8) gibi diğer temel haklarla dengelemek anlamsız değildir. Bu nedenle, şifreleme özgürlüğünün suistimal edildiğine dair ciddi göstergeler olduğunda, şifre çözme yükümlülüğü de dahil olmak üzere, şifreleme kullanıcısının, bu özgürlükle beraber, kanuni yaptırımı sağlamaya yönelik belirli sorumluluk ve yükümlülükleri olması gerektiğine dair bir "*O'Hallaron muhakemesi*" durumu bulunmaktadır.

Ayrıca, AİHS'nin 17. maddesi, AİHS hükümlerinin bir Devlet, bir grup veya bir kişi için AİHS'de belirtilen hak veya özgürlükleri ortadan kaldırmak amacıyla bir faaliyette bulunma veya bir eylem yapma hakkını ima ettiği şeklinde yorumlanmasını da yasaklamaktadır.[184] Kuşkusuz, potansiyel olarak pratikte şifresi kırılamaz kodların kırılmasına ek bir engel olarak sessiz kalma hakkı, bu sağlam şifreleme duvarının arkasında diğer insanların haklarını veya özgürlüklerini yok etme niyetiyle herhangi bir faaliyette bulunma hakkını ima etmez. Yine de, savcının (1) bir veri taşıyıcısının (mağdurların veya faillerin tespit edilmesine ve hatta muhtemelen bir suçun durdurulmasına imkan tanıyacak) suç delilleri barındırdığına ve (2) ilgili kişinin şifre çözme anahtarını bildiğine, bir şekilde bir hakkın, *bu davada* sessiz kalma hakkının ve kendini suçlu durumuna düşürmeme hakkının, kendi özgün bağlamı dışında ve hizmet etmesi amaçlanan amaca, yani adli hatalara ve ispat yükünün tersine çevrilmesine ve bununla bağlantılı olarak masumların mahkum edilmesi riskine karşı koruma amacına hizmet etmeden kötüye kullanılmasına itibar etmeye pek yaklaşmadığına dair ciddi göstergeler olduğunu gösterdiğinde, sessiz kalma hakkının şifreyi çözmek zorunda kalmamak için bir gerekçe olarak kabul edilip edilmeyeceği sorusunu kendimize sorma cüretini gösteriyoruz.

---

183 Kaba kuvvet genellikle parolaları kırmak veya güçlü şifreleme ile şifrelenmiş kayıp veya unutulmuş parolaları geri almak için kullanılmaktadır. Mevcut karakterlerin tüm olası kombinasyonlarını denemektedir. (https://nl.wikipedia.org/wiki/Brute_force_(method))

184 Örneğin, çok yakın bir zamanda - 24 Mayıs 2018 tarihinde - ROJ TV t/Danimarka davasında AİHM, ROJ TV'nin AİHS'nin 17. maddesi çerçevesindeki hakları kötüye kullanmasından dolayı şikayetin AİHS'nin 10. maddesi (ifade özgürlüğü) gerekçesiyle kabul edilemez olduğu için reddedilmesine oybirliğiyle karar vermiştir. Dolayısıyla AİHM, terör faaliyetlerini desteklemek ve terör propagandası yapmak için ifade özgürlüğünü kötüye kullanamaz. Temyiz Mahkemesi aşağıdaki değerlendirmeleri yapmıştır (AİHM 24 Mayıs 2018, no. 24683/14, ROJ TV/Danimarka):

"47. Sonuç olarak Mahkeme, öncelikle ulusal mahkemeler tarafından kapsamlı bir şekilde incelenen unsurlar olan, şiddete teşvik ve terör faaliyetlerine destek içeren ihtilaflı programların niteliğini, ikinci olarak, orada ifade edilen görüşlerin, televizyon yayıncılığı aracılığıyla geniş bir kitleye hitap ettiği gerçeğini ve üçüncü olarak da, modern Avrupa toplumunda en önemli mesele olan terörün önlenmesi ve şiddet kullanılmasını savunan teröristler ile ilgili ifadelerle doğrudan ilgili olduklarını göz önünde bulundurarak, başvuru sahibi şirketin şikayetinin, Sözleşmenin 17. maddesi gereğince, 10. madde tarafından sağlanan korumadan yararlanamayacağını tespit etmiştir.

48. Mahkeme, bunları göz önünde bulundurarak, başvuru sahibi şirketin, bu hakkı Sözleşme'nin değerlerine açıkça aykırı amaçlar için kullanarak Sözleşme'nin 10. maddesini gerçek amacından saptırmaya çalıştığı kanaatine varmıştır. Sonuç olarak Mahkeme, Sözleşme'nin 17. maddesi nedeniyle başvuru sahibi şirketin Sözleşme'nin 10. maddesinin sağladığı korumadan yararlanamayacağını tespit etmiştir."

11 Sözlük[185]

24/7 RealMedia: Merkezi New York'ta bulunan ve Dijital Pazarlama konusunda uzmanlaşmış bir teknoloji şirketidir. Küresel ölçekte yayıncılar, reklamcılar ve ajanslar için dijital pazarlama çözümleri sunmaktadır. Daha önce NASDAQ borsasında "TFSM" olarak listelenmiştir.

3G ağları: **3G** veya **3. nesil mobil telekomünikasyon**, Uluslararası Telekomünikasyon Birliği tarafından **Uluslararası Mobil Telekomünikasyon-2000 (IMT-2000)** özelliklerini sağlayan cep telefonları ve mobil telekomünikasyon hizmetleri için bir standartlar neslidir. Uygulama hizmetleri, tümü mobil bir ortamda olmak üzere geniş alan kablosuz sesli telefon, mobil internet erişimi, görüntülü aramalar ve mobil TV'yi içermektedir.

Erişim Kontrol Listeleri (ACL'ler): Bir nesneye eklenen izinlere dair bir listedir. Bir ACL, hangi kullanıcılara veya sistem süreçlerine nesnelere erişim izni verildiğini ve ayrıca belirli nesneler üzerinde hangi işlemlere izin verildiğini belirtir. Tipik bir ACL içindeki her kayıt, bir konuyu ve bir işlemi belirtir.

Erişim belirteci: Bir sürecin güvenlik tanımlayıcısını içinde barındıran bir nesnedir. Bir sürece eklenmiş bir güvenlik tanımlayıcısı, nesnenin (bu durumda, sürecin) sahibini ve nesnenin sahibine verilen veya verilmeyen erişim haklarını belirten ACL'leri tanımlar. Bir belirteç sadece güvenlik bilgilerini temsil etmek için kullanılsa da, teknik olarak serbest biçimlidir ve herhangi bir veriyi kapsayabilir. Erişim belirteci, Windows tarafından, süreç veya iş parçacığı, güvenlik tanımlayıcıları erişim kontrolünü zorunlu kılan nesneler (*güvenli nesneler*) ile etkileşime girmeye çalıştığında kullanılır.

Elde etme: Anlık görüntü alma olarak adlandırılan bir süreçtir. Söz konusu kopya, bir sabit sürücü çoğaltıcı veya DCFLdd, ddrescue, ewfacquire, Guymager, EnCase, FTK Imager veya X-Ways gibi yazılım görüntüsü alma araçları kullanılarak oluşturulur. Orijinal sürücü daha sonra kurcalamayı önlemek için güvenli depolamaya geri döndürülür. Alınan anlık görüntü, SHA-1 veya MD5 adres işlevleri kullanılarak doğrulanır. Analiz boyunca kritik noktalarda, delilin hala orijinal durumunda olduğundan emin olmak için "adresleme" olarak bilinen işlemle ortam yeniden doğrulanır. Medeni veya dahili isnatlar gerektiren kurumsal ortamlarda, bu tür adımlar, bunları gerçekleştirmek için gereken süre nedeniyle genellikle göz ardı edilmektedir.

Canlı veriler: Bilişim sistemi depolama birimlerinde bulunan, işletim sisteminin araçları aracılığıyla kullanıcılar tarafından anında ve doğrudan erişilebilen ve görülebilen dosya ve klasörlerdir.

AdBrite: 2002 yılında Philip J. Kaplan ve Gidon Wise tarafından kurulan San Francisco, California merkezli bir çevrimiçi reklamcılık ağıdır. Aslen Marketbanker.com olarak kurulan site, 2004 yılında AdBrite olarak yeniden hizmete girmiştir ve yayınlanan istatistiklerine göre günümüzde yüz binlerce sitede reklamlar sunmaktadır.

AdCenter: **Microsoft adCenter** (eski adıyla **MSN adCenter**), MSN'nin reklam hizmetlerinden sorumlu Microsoft Network (MSN) bölümüdür. Microsoft adCenter, tıklama başına ödemeli reklamlar sağlamaktadır. Bu, bir ürünün reklamını yapmak isteyen ki-

[185] Kaynaklar: Kendi tanımlarımız ve Wikipedia.org'dan alıntılar

şilere yönelik bir hizmettir. Microsoft ayrıca, sitelerinde para kazanmak isteyen web yöneticileri için (hala beta sürümünde olan) bir hizmete sahiptir: Microsoft pubCenter.

AfriNIC (Afrika Ağı Bilgi Merkezi): Afrika için bölgesel internet tescil merkezidir (RIR).

Amazon S3 (Basit Depolama Hizmeti): Amazon Web Hizmetleri tarafından sunulan bir çevrimiçi depolama web hizmetidir. Amazon S3, web hizmetleri arabirimleri (REST, SOAP ve BitTorrent) aracılığıyla depolama imkanı sağlamaktadır. Amazon, halka açık ilk web hizmeti olan S3'ü Mart 2006'da Amerika Birleşik Devletleri'nde ve Kasım 2007'de Avrupa'da piyasaya sürmüştür.

API: Bir **uygulama programlama arabirimi**, yazılım bileşenleri tarafından birbirleriyle iletişim kurmak için bir arabirim olarak kullanılması amaçlanan bir belirtimdir. Bir API; yordamlar, veri yapıları, nesne sınıfları ve değişkenlere ilişkin belirtimler içerebilir. Bir API belirtimi, POSIX gibi bir Uluslararası Standart veya Microsoft Windows API gibi satıcı belgeleri veya örneğin C++ veya Java API'de Standart Şablon Kitaplığı gibi bir programlama dilinin kitaplıkları da dahil olmak üzere birçok biçimde olabilir.

APNIC (Asya Pasifik Ağı Bilgi Merkezi): Asya Pasifik bölgesi için bölgesel internet tescil merkezidir. APNIC, internetin küresel işleyişini destekleyen numara kaynak tahsisi ve tescil hizmetleri sağlamaktadır. Üyeleri İnternet Servis Sağlayıcıları, Ulusal İnternet Sicilleri ve benzer organizasyonları içeren, kar amacı gütmeyen, üyeliğe dayalı bir organizasyondur.

ARIN (Amerikan İnternet Numaraları Sicili): Kanada, birçok Karayip ve Kuzey Atlantik adası ve Amerika Birleşik Devletleri için Bölgesel İnternet Tescil Merkezidir (RIR). ARIN, IPv4 ve IPv6 adres alanı ve AS numaraları da dahil olmak üzere internet numarası kaynaklarının dağıtımını yönetmektedir.

Asistan (PDA): Birçok biçimde ve boyutta olanları vardır ve genellikle sabit diskler veya anlık (flash) bellek biçiminde yerleşik depolama yeteneklerine sahiptirler. Son yıllarda çok popüler hale gelmişlerdir ve kendi işletim sistemleri olduğu için ve çoğunlukla **WLAN**, **3G** veya **LTE** ağları üzerinden internete bağlandıkları için faydalı elektronik delil kaynakları olabilirler.

ATM: Otomatik vezne makinesi (ATM), bir finans kuruluşunun müşterilerinin, bir kasiyere, insan memura veya banka memuruna ihtiyaç duymadan kamusal alanda finansal işlemlere erişmelerini sağlayan bir bilgisayarlı telekomünikasyon cihazıdır (Wikipedia'dan).

Otonom Sistem: İnternete ortak, açıkça tanımlanmış bir yönlendirme politikası sunan bir veya daha fazla ağ operatörünün kontrolü altında bağlı haldeki İnternet Protokolü (IP) yönlendirme önekleri topluluğudur.

Azure: Microsoft Windows Azure Platformu, Microsoft veri merkezleri aracılığıyla web uygulamaları oluşturmak, barındırmak ve ölçeklendirmek için kullanılan bir Microsoft bulut bilişim platformudur. Azure, hizmet olarak platform biçiminde sınıflandırılmaktadır ve Microsoft'un bulut bilişim stratejisinin bir parçasını ve hizmet olarak yazılım ürünü olan Microsoft Çevrimiçi Hizmetleri'nin bir parçasını oluşturmaktadır. Platform, Microsoft veri merkezlerinde barındırılan ve üç ürün markası aracılığıyla metalaştırılan çeşitli talebe bağlı hizmetlerden oluşmaktadır. Bunlar; Windows Azure (ölçeklenebilir bilişim ve depolama olanakları sağlayan bir işletim sistemi), SQL Azure (SQL Server'ın

bulut tabanlı, ölçeklenebilir bir sürümü) ve Windows Azure AppFabric'dir (hem buluttaki hem de şirket içindeki uygulamaları destekleyen bir servis koleksiyonu). Microsoft, 1 Temmuz 2011 tarihinden itibaren tüm Azure müşterileri için ücretsiz Giriş duyurusu yapmıştır.

Yedekleme: Orijinal kopya ile ilgili bir sorun olması durumunda başvurulmak üzere bilgisayarda tutulan tüm bilgilerin bir kopyası.

Biyometrik tarayıcılar: Bir bireyin fiziksel özelliklerini (örneğin parmak izi, ses, retina) tanıyan bir bilgisayar sistemine bağlı cihazlar.

BIOS: Temel Giriş Çıkış Sistemi. Bir bilgisayarın işletim sistemini başlatmasını ve sistemdeki disk sürücüleri, klavye, monitör, yazıcı ve iletişim bağlantı noktaları gibi çeşitli cihazlarla iletişim kurmasını sağlayan, salt okunur bellekte depolanan yordamlar kümesidir.

Bit: Bir **bit** (**ikili sayı** ifadesinin bir kısaltması), bilişimdeki ve telekomünikasyondaki temel bilgi kapasitesi olup, bir bit sadece ya 1'i veya 0'ı (biri veya sıfırı) temsil eder. Bu temsil, iki durumlu bir cihaz vasıtasıyla çeşitli sistemlerde uygulanabilir. Bilişimde, bir bit, sadece iki olası değere sahip olabilen bir değişken veya bir hesaplanmış miktar olarak da tanımlanabilir. Bu iki değer genellikle ikili sayılar olarak yorumlanır ve genellikle 0 ve 1 sayıları ile gösterilir. İki değer ayrıca; mantıksal değerler (*doğru*/*yanlış*, *evet*/*hayır*), cebirsel işaretler (+/–), etkinleştirme durumları (*açık*/*kapalı*) veya iki değerli başka her nitelik olarak da yorumlanabilir. Bu değerler ile temel depolama biriminin veya cihazın fiziksel durumları arasındaki uyuşma bir uzlaşma meselesidir ve aynı cihaz veya program içinde bile farklı değerler kullanılabilir. Bir ikili sayının uzunluğu, onun "bit uzunluğu" olarak adlandırılabilir.

Bluetooth: Cep telefonlarının, bilgisayarların ve PDA'ların kısa menzilli bir kablosuz bağlantı kullanarak birbirleri ile ve ev ve iş telefonları ve bilgisayarları ile nasıl kolayca bağlantı kurabileceğini açıklayan bir telekomünikasyon endüstrisi özelliğidir. Bluetooth, her cihaza düşük maliyetli bir alıcı-verici yonganın (çipin) dahil edilmesini gerektirmektedir.

Blu-ray Disk (BD): DVD formatının yerini almak üzere tasarlanmış bir optik disk depolama ortamıdır. Plastik disk 120 mm çapında ve 1,2 mm kalınlığında olup DVD'ler ve CD'ler ile aynı boyuttadır. Blu-ray Diskler, katman başına 25 GB içerir ve çift katmanlı diskler (50 GB) uzun metrajlı video diskleri için normdur. *BD-XL* yeniden yazma sürücüleri için üç katmanlı (100 GB) ve dört katmanlı (128 GB) diskler mevcuttur.

Veri yakalama: Veri yakalama, verileri bir bilgisayar sisteminden veya elektronik ortamdan kopyalamak ve mümkün olduğunda (örneğin RAM yakalama için mümkün değildir) verilerin bütünlüğünü doğrulamadan önce bir harici depolama ortamı üzerinde depolamaktır. Veri yakalama aynı zamanda ağ verileri için de mümkün olabilir. Bu bağlamda ağ paketlerini yakalamak ve bilgilerini bir dosyaya (örneğin PCAP formatında) depolamak için ağdaki bir makine kullanılır.

CentralOps: CentralOps; alan dosyası, e-posta dosyası, whois aramaları vb. gibi soruşturmaya yönelik arama fırsatları sunan bir web sitesidir. Bu hizmetler IP adresleri, etki alanları ve e-posta adresleri hakkında bilgi sağlayabilir. Web sitesi, ABD merkezli özel bir şirket olan Hexillion tarafından yönetilmektedir. Adresi: http://centralops.net

Sohbet günlükleri: çevrimiçi sohbet ve anlık mesajlaşma konuşmalarından oluşan bir arşividir. Birçok sohbet veya IM (anlık mesajlaşma) uygulaması, çevrimiçi sohbet konuşmalarının istemci tarafında arşivlenmesine izin verirken, sohbet veya IM istemcilerinin bir alt kümesi (yani, Google Talk ve Yahoo! Messenger 11 Beta), sohbet arşivlerinin gelecekte geri alınmak üzere bir sunucuda kaydedilmesine olanak tanır. Web sunucusu sabit disk alanının maliyetini düşürmesi nedeniyle uygulama satıcıları tarafından bu ikinci trend benimsenmiştir.

CIDR gösterimi: bir İnternet Protokolü adresinin ve bununla ilişkili yönlendirme önekinin küçük bir belirtimidir. Sınıfsız Alanlar Arası Yönlendirme (CIDR), IP adres alanının IPv4 sınıflı ağ organizasyonunun yerini alan İnternet adresleme mimarisinde kullanılan bir İnternet Protokolü (IP) adres tahsisi ve yol birleştirme metodolojisidir [1]. Aynı zamanda yeni nesil IP adresleme mimarisi olan IPv6 ağ iletişimi için de kullanılmaktadır.

Devre kartları: Üzerinde takılı yongaların, cihazların ve diğer elektronik bileşenlerin bulunduğu ince bir plakadır (baskılı devre kartı olarak da anılır).

Kapalı Devre Televizyon (CCTV): Şirketler, hükümetler ve bireyler tarafından güvenlik amacıyla kullanılırlar ve belirli faaliyetlerin gerçekleşip gerçekleşmediğine dair delil sağlayabilirler.

Bulut: Bulut bilişim, asgari yönetim gayreti veya hizmet sağlayıcı etkileşimi ile hızla hazırlanabilen ve yayınlanabilen, ortak bir yapılandırılabilir bilişim kaynakları havuzuna (örneğin ağlara, sunuculara, depolamaya, uygulamalara ve hizmetlere) talep esasında ağ erişimine imkan tanıyan, konum bağımsız, elverişli bir modeldir […]

CMOS: Tamamlayıcı metal oksit yarı iletken. Günümüzün bilgisayar mikroçiplerinin çoğunun içinde imal edilen transistörlerde kullanılan yarı iletken teknolojisi. Genellikle bilgisayarın BIOS tercihlerini, bilgisayarın kapalı olduğu süre boyunca bir pil yardımıyla (ona bağlı olarak) tutar.

Kompakt Disk (CD): İkili bilgileri depolamak için kullanılan 12 cm çapındaki optik disktir. Biçimlendirilmiş kapasitesi 640-700 Mb arasındadır ve başlangıçta ses depolamak için kullanılmıştır. Genel verileri depolamak için kullanıldığında CD-ROM olarak adlandırılır.

Bilgisayar Belleği: Bellek, bir bilgisayarın mikroişlemcisinin hızlı bir şekilde ulaşabileceği komutların ve verilerin elektronik olarak tutulduğu yerdir. RAM, bir bilgisayara takılı olan bir veya daha fazla mikroçip üzerinde bulunur.

Bilgisayar Ağları: Veri kabloları veya kablosuz bağlantı ile birbirine bağlanan iki veya daha fazla bilgisayar arasındaki bağlantılardan oluşur. Bu bilgisayarlar, kendi aralarında verileri ve diğer kaynakları paylaşabilir. Ağın gerektirdiği kapsamdaki etkinlikleri sağlamak için genellikle başka donanım bileşenlerine sahiptirler.

Çerez: Çerezler, internet sunucusunun kullanıcının bilgisayarının sabit diskine indirdiği küçük dosyalardır. Bu dosyalar, (örneğin şifreler ve ziyaret edilen web sitelerinin bulunduğu listeler aracılığıyla) kullanıcıyı tanımlayan belirli bilgileri içermektedir.

CPU: Merkezi işlem birimi. Bir bilgisayarın hesaplama ve kontrol birimidir. Bir bilgisayarın içinde yer alan, bilgisayardaki tüm aritmetik, mantık ve kontrol işlevlerini yerine getiren "beyin"dir.

Sistem Kırıcı: Sistem Kırıcı, bir sistemin içine, herhangi bir şekilde zarar vermek veya çıkar sağlamak amacıyla izinsiz olarak giren kişidir.

Bilişim suçu: Bir bilgisayarın ve bir ağın dahil olduğu herhangi bir suçu ifade eder. Bilgisayar, bir suçun işlenmesinde kullanılmış olabilir veya suçun hedefi olabilir.

Siber İşgalci: Siber İşgalci, gelecekte ilgilenen şirketlere satmak amacıyla alan adlarını ayırtan (rezerve eden) veya satın alan kişidir.

DAT (Dijital Ses Bandı): *Yedekleme* sistemlerinde depolama için kullanılan dijital ses bandıdır.

Veri depolama cihazları: Bir **veri depolama cihazı**, bilgileri (verileri) kaydetmeye (depolamaya) yönelik bir cihazdır. El yazısındaki manuel kas gücünden fonografik kayıttaki akustik titreşimlere, elektromanyetik enerji modülasyonlu manyetik bant ve optik disklere kadar uzanan bir yelpazede neredeyse her enerji türü kullanılarak kayıt yapılabilir.

VERİTABANI: Birçok şekilde erişilebilen yapılandırılmış veri koleksiyonudur. Yaygın veritabanı programları şunlardır: Dbase, Paradox, Access. Kullanım Alanları: Adres bağlantıları, fatura bilgileri, vb. de dahil olmak üzere çeşitlidir.

Kapalı kutu adli incelemesi: Kapalı kutu adli incelemesi, adli bilişim biliminin bir dalı olan bilgisayar adli incelemesinin bilgisayarlarda bulunan yasal deliller ile ilgili bir kısmıdır. Bilgisayar adli incelemesi, bir davada delil haline gelebilecek olguların belirlenmesi, korunması, kurtarılması, analiz edilmesi ve sunulması amacıyla bilgisayar sistemlerinin adli bakımdan sağlıklı bir şekilde incelenmesiyle ilgilenir. Kapalı kutu adli incelemesi de bu amacı gütmekte, fakat sadece kapalı durumdaki bilgisayar sistemlerinin içindeki depolama ortamına odaklanmaktadır.

Silinmiş veriler: Daha önce bilgisayarda etkin veri olarak bulunan ancak o zamandan beri işletim sistemi veya son kullanıcı tarafından silinen dosyalar ve klasörlerdir. Silinen veriler, başka bir dosya tarafından üzerine yazılana kadar depolama biriminin içinde kalacaktır.

Masaüstü Cihazlar: Bir masanın üzerine yerleştirilebilen ofis araçlarını (fotokopi makinesi ve yazıcı gibi), zemin üzerinde kendi alanını kaplayan daha büyük ekipmanlardan ayırt etmek için kullanılan bir sıfat olarak benimsenen bir terimdir. Masaüstü terimi aynı zamanda, bir masanın üstüne sığacak şekilde tasarlanmış bir kişisel bilgisayar olan Masaüstü bilgisayarı da ifade edebilir.

Adli Bilişim: Adli Bilişim, adli inceleme biliminin, bilgisayar sistemlerinde, dijital cihazlarda ve diğer depolama ortamlarında saklanan delillerin mahkemede kabul edilebilirlik amacıyla elde edilmesi, işlenmesi, analizi ve raporlanması ile ilgili bir dalıdır.

Dijital ortam: Verilerin (analog yerine) dijital biçimde depolandığı bir elektronik ortam biçimidir. Bilgilerin depolanmasına ve iletilmesine ilişkin teknik bileşeni (örneğin sabit disk sürücülerini veya bilgisayar ağını) veya dijital video, artırılmış gerçeklik veya dijital sanat gibi "son ürünü" ifade edebilir.

Dijital fotoğrafçılık: Dijital fotoğrafçılık, lens tarafından odaklanan görüntüyü kaydetmek için bir dizi ışığa duyarlı sensör kullanan bir fotoğrafçılık biçimidir (Wikipedia'dan alıntı).

Dijital Video Diski (DVD): Dijital Çok Yönlü (video) Disk. Günümüzde, CD'nin doğal halefi olup, kaliteli ses ve görüntünün yeniden üretimi için kullanılmaktadır.

Dijital Video: Dijital bir biçimlendirme ile kaydedilen, değiştirilen ve saklanan videodur.

Dijitalleştirme (Sayısallaştırma): Elektronik bilgileri "birlerden" ve "sıfırlardan" oluşan bir zincir biçiminde saklamaktır. Elektronik ortamda istenilen sayıda "birin" ve "sıfırın" 2 voltaik seviye ile kolaylıkla temsil edilebilmesi dolayısıyla, ikili sayı sistemi dijital bilişim teknolojileri dünyasında yaygın olarak kullanılmaktadır.

Diskette Tescilli araçlar: **Açıkça bu uygulamaları kullanan şirketin işlevlerine ve işleyişine uygun olarak geliştirilmiş olan ve genellikle satın alınmaları için serbest piyasaya sürülmeyen bilişim uygulamalarıdır.**

Disket: Plastik bir kasa/kaplama içinde dairesel bir manyetik malzeme parçasından oluşan, giderek daha az kullanılan medya depolama türüdür.

DNS: Alan Adı Sistemi (DNS). Örneğin www.cybex.es gibi bir alan adını, aradığınız sunucunun bulunduğu IP adresine dönüştürür.

Bağlantı terminalleri: Bir taşınabilir bilgisayarın (örneğin dizüstü bilgisayarın), masaüstü bilgisayar olarak kullanılmak üzere bağlanabileceği, genellikle sabit sürücüler, tarayıcılar, klavyeler, monitörler ve yazıcılar gibi harici olarak bağlanan cihazlar için bir konektöre sahip cihazlardır.

Alan Adı: **Alan Adı Sistemi** (**DNS**), bilgisayarlar, hizmetler veya internete veya özel bir ağa bağlı herhangi bir kaynak için hiyerarşik olarak dağıtılmış bir adlandırma sistemidir. Çeşitli bilgileri, kendisine katılan varlıkların her birine tahsis edilen alan adları ile ilişkilendirir. Bir **Alan Adı Hizmeti**, dünya genelindeki bilgisayar hizmetlerinin ve cihazların konumunu bulmak amacıyla (internete erişirken anlaşılması ve kullanılması daha kolay olan) alan adlarına yönelik sorguları IP adreslerine çözümler. Alan Adı Sistemini açıklamak için sıklıkla kullanılan bir benzetme, kullanımı kolay ana bilgisayar adlarını IP adreslerine çevirerek internet için telefon rehberi görevi görmesidir. Örneğin www.example.com alan adı, 192.0.43.10 (IPv4) ve 2620:0:2d0:200::10 (IPv6) adreslerine çevrilir.

DomainTools: DomainTools, LLC şirketi, on yıldan uzun internet geçmişini kapsayan geçmiş ve mevcut alan adı kaydının ve sahiplik kayıtlarının kapsamlı bir anlık görüntüsü olarak hizmet veren bir alan adı sahiplik kayıtları (Whois) dizini sağlamaktadır. Whois verilerine ek olarak DomainTools, bireylerin ve kuruluşların bir alan adı ile ilgili her şeyi keşfetmesine ve izlemesine yardımcı olan bir dizi araştırma aracı da sunmaktadır. DomainTools ayrıca, gelişmiş semantik isim önerme teknolojisi, patentli Ters IP teknolojisi ve bir web sitesinin şimdi nasıl göründüğüne ve geçmişte nasıl göründüğüne dair milyonlarca anlık ekran görüntüsünü birleşik bir anlık ekran görüntüsü geçmişi görünümüne dahil etmesiyle de bilinmektedir.

Dongle: Bir bilgisayar üzerindeki bir elektrik konektörüne takılan ve bir yazılım parçası için elektronik bir "anahtar" görevi gören küçük bir donanım parçasıdır; söz konusu program yalnızca dongle takılıyken çalışacaktır. "Dongle" terimi başta sadece yazılım koruma kilitlerini ifade etmek için kullanılmıştır; ancak günümüzde "dongle" genellikle bir bilgisayara takılan herhangi bir küçük donanım parçasını belirtmek için kulla-

nılmaktadır. Bu yazının kapsamı, bir sistemde kullanılacak yazılımın kopya koruması veya kimlik doğrulaması amacıyla kullanılan dongle'larla sınırlıdır.

Sürücü çoğaltıcılar: Farklı depolama ortamlarının, örneğin sabit disklerin veya CD'lerin hızlıca kopyalanmasına (çoğaltılmasına) yönelik cihazlardır.

DropBox: Dropbox, Inc. şirketi tarafından işletilen ve bulut depolama, dosya senkronizasyonu ve istemci yazılımı sunan bir dosya barındırma hizmetidir.

Dinamik Ana Bilgisayar Yapılandırma Protokolü (DHCP): Bir grup cihaza otomatik olarak bir IP adresi havuzu tahsis etmek için kullanılan bir protokoldür.

Elektronik delil: Elektronik delil, mahkemede delil olarak kullanılabilecek, elektronik cihazlar kullanılarak üretilen, saklanan veya iletilen bilgilerdir. Delillerin mahkemede kabul edilmesinin garanti altına alınması için, bilgilerin, uzman personel kullanılan çok iyi tanımlanmış süreçler izlenerek ve yeterli düzeyde bir yasal çerçeve içerisinde faaliyet göstererek elde edilmesi gerekmektedir.

E-posta virüsü: E-posta iletileri, metin aktarmak için sadece 7-bit bir format kullandıkları için virüsler bunların içinde seyahat edemezler. Seyahat edebilmelerinin yegane yolu, metin iletisinin eki olarak gönderilen ikili dosyalar vasıtasıyladır. Bu dosyaların açılmadan önce bir anti-virüs programı ile kontrol edilmesi önerilir.

E-posta: Bilgisayarda depolanan iletilerin telekomünikasyon yoluyla alınıp gönderilmesidir.

Şifreleme: Verileri karıştırma ve kodlama yöntemidir. Amaçlanan alıcı dışında herhangi birinin ilgili verileri okumasını önlemek amacıyla (kriptografik anahtar adı verilen matematiksel bir parametre kullanılarak) düz metni şifreli metne dönüştürmek için kullanılır.

Çevresel veriler: Bir bütün olarak bilişim sistemi üzerinde aktif olmayan verileri ifade eder. Çevresel veriler şunları içerir: Kullanılmayan veya tahsis edilmemiş alanlarda bulunan veriler, "Boş" dosya alanında bulunan veriler ve işletim sistemi araçları kullanılarak görülemeyen silinmiş Dosya verileri.

Olay günlükleri: Olay Günlükleri, Windows işletim sistemleri tarafından kaydedilen günlük dosyalarıdır. Genellikle Windows'un farklı hizmetlerinden kaynaklanan çeşitli olayları denetleyen birkaç Olay Günlüğü vardır. Belirli Olay Günlüklerinin oluşturulması varsayılan olarak açıktır ancak kullanıcı tarafından devre dışı bırakılabilir. Windows XP makineler için varsayılan depolama konumu: C:\Windows\system32\config*.evt, Windows Vista/7 makineler için varsayılan depolama konumu: C:\Windows\system32\Winevt*.evtx

EXIF meta veriler: Değiştirilebilir görüntü dosyası formatı (Exif), (akıllı telefonlar da dahil olmak üzere) dijital kameralar, tarayıcılar ve dijital kameralar tarafından kaydedilen görüntü ve ses dosyalarını işleyen diğer sistemler tarafından kullanılan görüntüler, ses ve yardımcı etiketlere ilişkin formatları belirten bir standarttır. Tipik olarak, EXIF meta veriler içinde, örneğin fotoğrafın ne zaman ve nerede ve hangi kamera modeli ile hangi konfigürasyon kullanılarak çekildiğini gösteren saat, tarih ve yer gibi pek çok bilgi bulunmaktadır.

EXT4: veya **dördüncü genişletilmiş dosya sistemi**, EXT3'ün halefi olarak Linux için geliştirilen bir günlük kaydı dosya sistemidir.

Harici sabit disk sürücüler: Harici sabit disk sürücü, bir tür harici depolama ortamıdır. Modern harici sabit disk sürücüler, USB, Firewire, eSATA ve/veya Thunderbolt aracılığıyla bağlantı sunan bir kasa ve kasanın içinde bulunan normal bir 2,5" veya 3,5" sabit disk veya SSD'den oluşmaktadır. Tipik olarak, harici sabit disk sürücüler, USB bellek çubuklarına veya SD kartlara kıyasla daha büyük miktarda veri depolayabilirler.

Faraday izolasyon torbaları: Yaklaşık 6.02 x 10^23 elektrik yükü taşıyıcısına eşit, boyutsuz bir elektrik yükü miktarı birimidir. Bu, Avogadro sabiti (sayısı) olarak da bilinen bir mol eşdeğeridir. Faraday izolasyon torbaları, cep telefonlarının ve cihazların iletişim sinyallerine bağlanmasını önlemek için kullanılır.

FAT (Dosya Tahsis Tablosu): bir bilgisayar dosya sistemi mimarisinin ve o mimariyi kullanan endüstri standardı dosya sistemleri ailesinin adıdır. FAT dosya sistemi teknik olarak nispeten basit ama sağlamdır. Hafif uygulamalarda bile oldukça iyi bir performans sunar ve bu nedenle kişisel bilgisayarlar için neredeyse tüm mevcut işletim sistemleri tarafından geniş ölçekte benimsenmekte ve desteklenmektedir. Bu durum onu 1980'lerin başından günümüze kadar neredeyse her tür ve yaştaki bilgisayarlar ve cihazlar arasında veri alışverişi bakımından çok uygun bir format haline getirmektedir.

Dosya uzantısı: Dosya etiketi, genellikle 3 karakter uzunluğundadır, önünde bir nokta bulunur, veri dosyasının biçimini veya onu değiştirmek için kullanılan uygulamayı tanımlar.

FireBug: İnternette gezinme sırasında bol miktarda geliştirme aracı ile Firefox tarayıcısına entegre olur. Kullanıcının herhangi bir web sayfasında canlı olarak CSS, HTML ve JavaScript düzenlemesine, hata ayıklamasına ve izlemesine olanak tanır.

FireWire: 63 cihaza kadar bağlantıya izin veren yüksek hızlı bir seri bağlantılı veri yoludur. Dijital kameralardan bilgisayara video indirmek için yaygın olarak kullanılır.

Flash (anlık) bellek kartları: Dijital bilgileri depolamak için kullanılan cihazlardır. Genellikle dijital kameralar, cep telefonları, dizüstü bilgisayarlar, müzik çalarlar ve oyun konsolları gibi birçok elektronik cihazda kullanılırlar. Elektriğe bağlı olmadan verileri saklayabilirler ve çeşitli kapasitelerde olanları vardır, yani büyük miktarlarda veri depolayabilir ama kolayca da gözden kaçırılabilirler.

Adli İnceleme Önyükleme DVD'leri: Adli İnceleme Önyükleme DVD'leri, önyüklenebilir ve adli bilişim görevlerini gerçekleştirmeye yönelik yazılımlar içeren, bir işletim sistemine sahip DVD'lerdir. Bu Önyükleme DVD'leri, sadece adli araçlar sunmanın yanı sıra, takılı depolama ortamlarından herhangi birine istenmeyen yazma işlemlerini önlemek için de önlemler alırlar.

FQDN (Tam Nitelikli Alan Adı): Bazen *mutlak alan adı* olarak da adlandırılır, Alan Adı Sisteminin (DNS) ağaç hiyerarşisindeki tam konumunu belirten bir alan adıdır. Üst düzey alan ve kök bölge de dahil olmak üzere tüm alan düzeylerini belirtir. Bir tam nitelikli alan adı, belirsiz olmaması ile ayırt edilir; sadece tek bir şekilde yorumlanabilir.

Parçalanmış veriler: Parçalanmış veriler, bölünmüş ve sabit disk üzerinde farklı fiziksel konumlarda depolanmış aktif verilerdir.

FTK Imager: FTK Imager, Access Data Inc. şirketi tarafından sağlanan çok amaçlı bir yazılımdır. Ücretsizdir ve sabit disklerin anlık görüntüsünü alma, sabit diskleri ve anlık

görüntü dosyalarını doğrulama, dönüştürme, kurma yeteneğine sahiptir. FTK Imager şu web sitesinden indirilebilir: http://accessdata.com/support/adownloads

FTP (Dosya Aktarım Protokolü): İnternet üzerinden bağlı bilgisayarlar arasında dosya/veri aktarımına olanak tanıyan internet protokolüdür.

Google AdSense: Google Inc. şirketi tarafından yürütülen ve içerik sitelerinin Google Ağındaki yayıncıların, site içeriğini ve hedef kitleyi hedefleyen otomatik metin, resim, video ve zengin medya reklamları sunmasına olanak tanıyan bir programdır. Bu reklamlar Google tarafından yönetilir, sıralanır ve sürdürülür ve tıklama başına veya gösterim başına gelir üretebilirler.

GPS: GPS (Küresel Konumlandırma Sistemi), Dünya'nın yörüngesinde dönen ve yer alıcılarına sahip kişilerin coğrafi konumlarını tam olarak belirlemelerini mümkün kılan, iyi aralıklandırılmış 24 uydudan oluşan bir "takımuydudur". Çoğu ekipman için konum doğruluğu 100m ila 10m arasındadır. GPS cihazları, hedef bilgileri, yol noktaları ve rotalar aracılığıyla geçmiş seyahatler hakkında bilgi sağlayabilir.

Bilgisayar Korsanı (Hacker): Söz konusu sistemlerin güvenliğindeki hatalardan ve arızalardan yararlanmalarını olanak tanıyan bilgisayarların ve ağların işlevselliği hakkında kapsamlı bilgiye sahip kişidir.

Sabit disk: Ferromanyetik bir yanma (kayıt) tabakası ile kaplanmış metal disktir. Vinil disk (plak) ile benzetme yaparsak, diskin düz tarafları yanma (kayıt) tabakası, plak çaların döner tablasının kolu lazer kolu ve döner tabla kolundaki iğne bilgiyi okuyan/yazan lazer ışınıdır. Bir kullanıcı, ses bandında olduğu gibi manyetik disklere de yazabilir, silebilir veya üzerine yeniden yazabilir.

Sabit sürücüler: Sabit sürücüler, bilgisayar sistemlerindeki ana depolama cihazlarıdır. Bir devre kartı, veri ve güç bağlantıları ile birlikte verileri depolayan manyetik olarak yüklü, seramik, metal veya cam plakalardan oluşurlar. Bir bilgisayar sistemine bağlı olmayan veya içine takılmamış sabit sürücüler keşfedilmesi olağandışı bir durum değildir.

Donanım: Klavye, monitör ve fare gibi bir bilgisayar sistemini oluşturan fiziksel bileşenlerdir.

Asılsız Uyarı: Özellikle ağ üzerinden yayılan var olmayan virüsler hakkında yanlış söylentileri tanımlamak için kullanılan terim. Bazen çok başarılı olur ve gerçek bir virüs kadar zarar verirler.

Barındırma sağlayıcıları: Bir **internet barındırma hizmeti**, internet sunucularını çalıştıran ve kuruluşların ve bireylerin internete içerik sunmasına olanak tanıyan bir hizmettir. Çeşitli hizmet seviyeleri ve sunulan çeşitli hizmetler vardır. Yaygın bir barındırma türü web barındırmadır. Çoğu barındırma sağlayıcısı, birleştirilmiş çeşitli hizmetler de sunarlar. Web barındırma hizmetleri aynı zamanda örneğin e-posta barındırma hizmeti de sunarlar. DNS barındırma hizmeti genellikle alan adı kaydı ile birlikte gelmektedir.

HTML kodu (Köprü Metni İşaretleme Dili): Web sunucularına yönelik dokümanları yazmak için kullanılan dildir. HTML, ISO 8879:1986 Standardından bir uygulamadır.

HTTP (Köprü Metni Aktarım Protokolü): HTTP, multimedya bilgi sistemlerini internet üzerinden dağıtmak ve yönetmek için gerekli çevikliğe ve hıza sahip bir protokoldür.

HTTP'nin karakteristik bir özelliği, verilerin görselleştirilmesindeki ve sunulmasındaki bağımsızlık olup, sistemlerin, verinin sunumundaki yeni gelişmelerin geliştirilmesinden bağımsız olarak oluşturulmasına izin verir.

HTTPS: Güvenli HTTP protokolüdür. 2 temel özelliği, kodlama ve kimlik doğrulamadır. Kodlama sayesinde sunucunun üçüncü şahıslara yönelik iletişiminin içeriği gizlenmektedir. Kimlik doğrulama, Yetki Belgesi ile belgelendirilmiş imzaların kullanılması suretiyle sunucunun iyi niyetli olduğunu kullanıcıların bilmesini sağlar.

Adli kopya: Bir adli soruşturmada kullanılan bir bilişim sistemine ait depolama biriminin tam (bire bir) bir kopyasıdır.

Hub'lar (Dağıtıcılar): Bir ağdaki verilerin, bir veya daha fazla yönden geldiği ve bir veya daha fazla yöne iletildiği birleşme noktalarıdır. Genellikle, tek bir girişten (çıkış=-giriş) birbirinin aynısı bir dizi çıkış üreterek çok kapılı bir tekrarlayıcı biçiminde çalışırlar. Bir hub, bir tür (uyarlanmış) anahtar içerebilir.

I ROM belleği: ROM, *Salt Okunur Bellek* anlamına gelir. Üzerine tekrar yazılamayan ve güç kaynağı kaybı da dahil olmak üzere her durumda saklanan bilgileri bozulmadan koruyan yarı iletken bellektir. ROM, sistem yapılandırmasını veya programı bilgisayarın önyüklemesinde depolamak için kullanılır.

ICQ: İlk olarak İsrailli Mirabilis şirketi tarafından geliştirilen ve popüler hale getirilen, daha sonra America Online tarafından satın alınan ve Nisan 2010'dan bu yana da Mail.ru Group'a ait olan bir anlık mesajlaşma programıdır. *ICQ* adı, "Seni arıyorum" ifadesi ile eş seslidir. Bu, "herhangi bir istasyonu aramak" anlamına gelen Mors kodu ifadesi "CQ"nun bir uyarlamasıdır.

IMAP: İnternet Mesaj Erişim Protokolü. Posta sunucusundan (yani IMAP sunucusundan) e-posta mesajlarını almak ve/veya bunlara erişmek için standart bir protokole dayalı bir internet hizmetidir.

Kızılötesi: Kızılötesi kablosuz teknolojisi, (örneğin kablosuz yerel alan ağları, dizüstü bilgisayarlar ve masaüstü bilgisayarlar arasındaki bağlantılar, kablosuz modemler, izinsiz giriş detektörleri gibi) çeşitli uygulamalarda kısa ve orta menzilli iletişim ve kontrol için kullanılmaktadır. Kızılötesi, elektromanyetik radyasyon tayfı bölgesi içindeki, görünür ışıktan daha uzun, ancak radyo dalgalarından daha kısa dalga boylarındaki enerjiyi ifade etmektedir.

Katılım Öncesi Araç: Katılım Öncesi Yardım Aracı (IPA), 2007-2013 dönemi için Avrupa Birliği'ne (AB) katılım öncesi sürece yönelik mali araçtır. Yardım, potansiyel adayların Avrupa Ortaklıkları ve aday ülkelerin, yani Batı Balkan ülkelerinin, Türkiye'nin ve İzlanda'nın Katılım Ortaklıkları temelinde sağlanmaktadır. IPA, esnek bir araç olarak tasarlanmıştır ve bu nedenle, yararlanıcı ülkelerin kaydettiği ilerlemeye ve Komisyonun değerlendirmelerinde ve strateji belgelerinde gösterilen ihtiyaçlarına bağlı olarak yardım sağlar.

"Gnome" Arayüzü: Bir yelpazede farklı Linux dağıtımları tarafından kullanılan GNOME masaüstü ortamının temel kullanıcı arayüzüdür. Pencereler arasında geçiş yapma ve uygulamaları başlatma gibi temel işlevler sağlamaktadır. GNOME'un önceki sürümlerinde kullanılan masaüstü metaforunun önceki modelinden ayrılan bir kullanıcı deneyimi sunmak için GNOME Panel'in ve GNOME 2'deki diğer yazılım bileşenlerinin yerini almıştır.

İnternet erişimi: Münferit terminallerin, bilgisayarların, mobil cihazların ve yerel ağların küresel internete bağlanma yöntemidir. İnternet erişimi genellikle son kullanıcıya çok çeşitli veri hızları sunan birçok farklı teknolojiyi kullanan İnternet Servis Sağlayıcıları (ISP›ler) tarafından satılmaktadır.

İnternet Tahsisli Sayılar Kurumu (IANA): Küresel IP adresi tahsisini, otonom sistem numarası tahsisini, Alanı Adı Sistemi (DNS) içinde kök bölge yönetimini, medya türlerini ve İnternet Protokolü ile ilgili diğer sembolleri ve sayıları denetleyen kuruluştur. IANA, ICANN olarak da bilinen Tahsis Edilen Adlar ve Numaralar için İnternet Kurumu tarafından işletilen bir departmandır.

İnternet tarama geçmişi: Apple Safari, Google Chrome, Microsoft Internet Explorer, Mozilla Firefox, vb. gibi web sitelerini taramak için tasarlanmış yazılımlar, genellikle bir bilgisayar sisteminin kullanıcılarının yaptığı web sitesi ziyaretlerine dair geçmişi kaydeder. Bu geçmiş günlük dosyalarının veya veritabanlarının temel amacı, kullanıcının yakında veya çok sık ziyaret edilen web sitelerini kolayca seçmesini sağlamaktır. Adli inceleme uzmanları için, tarayıcılar tarafından kaydedilen internet tarama geçmişi, delil bulmak için değerli bir kaynak olabilir.

İnternet Servis Sağlayıcı (ISP): İnternete erişim sağlayan bir kuruluştur. İnternet servis sağlayıcıları ya topluluğa aittir ve kar amacı gütmez veya özel sektöre aittir ve kar amacı güder.

İnternet: Bilgisayarları birbirine bağlamak ve dolayısıyla en popülerleri e-posta, web ve FTP hizmetleri olmak üzere çeşitli hizmetlerin taşınması için kullanılan TCP/IP protokolüne dayalı küresel veri ağıdır.

IP adresi: İnternette bir bilgisayarı temsil etmek ve tanımlamak için kullanılan, noktalarla ayrılmış 4 sayıdan oluşan sayı zinciridir. İnternete bağlandığımızda ISP'ler IP adreslerini otomatik olarak tahsis etmektedir.

ISP (İnternet Servis Sağlayıcı): Özel hatlar veya anahtarlar olan bilgisayarlar için internete bağlantı sağlayan kuruluştur. Özel ve/veya tüzel kişiler için internete erişim sağlamanın yanı sıra web barındırma, web tasarım danışmanlığı, web sitesi ve intranet entegrasyonu gibi hizmetler de sunabilen kar amacı güden bir kuruluştur.

Bilişim sistemi: Bir bilişim sistemi - veya uygulama ortamı - operasyonları, yönetimi ve karar vermeyi destekleyen bilişim teknolojisinin ve insan faaliyetlerinin herhangi bir birleşimidir. Çok geniş bir anlamda bilişim sistemi terimi, insanlar, süreçler, veriler ve teknoloji arasındaki etkileşimi ifade etmek için sıklıkla kullanılmaktadır. Bu anlamda, bu terim yalnızca bir organizasyonun kullandığı bilgi ve iletişim teknolojisini (BİT) değil, aynı zamanda iş süreçlerini desteklemek için insanların bu teknolojiyle etkileşim kurma şeklini de ifade etmek için kullanılmaktadır.

JAVA: Java, nesne tabanlı ve Sun Microsystems tarafından geliştirilen bir dildir. C, C++ ve Objective C dilleri ile benzerlikler taşır. Diğer nesne tabanlı dilleri temel alan Java, diğerlerinin en iyi kısımlarını kullanır ve en az etkili olan noktaları ortadan kaldırır. Java'nın temel amacı, (kod kötü niyetle yazılmış olsa dahi) internet üzerinden güvenli bir şekilde işletilebilecek kapasiteye sahip bir dil oluşturmaktı. Bu özellik, birçok C ve C++ kullanımının ve yapısının ortadan kaldırılmasını gerektirmektedir. En önemlisi, hiçbir işaretçinin olmamasıdır. Java'da program, bellek adreslerine keyfi olarak erişemez.

LACNIC (Latin Amerika ve Karayipler Ağı Bilgi Merkezi): Latin Amerika ve Karayip adaları bölgeleri için Bölgesel İnternet Tescil Merkezidir. LACNIC, internetin küresel işleyişini destekleyen numara kaynak tahsisi ve tescil hizmetleri sağlamaktadır. Üyeleri İnternet Servis Sağlayıcıları ve benzer organizasyonları içeren, kar amacı gütmeyen, üyeliğe dayalı bir organizasyondur.

LAN: Yerel Alan Ağı (Yerel Ağ). IEEE (Elektrik ve Elektronik Mühendisleri Enstitüsü) tarafından standartlaştırılmış ağ teknolojileri için ortak bir isimdir.

LAN YAPILANDIRMASI: Ethernet veya simgeli halka gibi LAN topolojisi veya Ethernet adresi gibi MAC adresleridir (MAC: Orta Erişim Kontrolü, OSI yedi katmanlı modeldeki veri bağlantı katmanının bir parçasıdır).

Linux: Ücretsiz ve açık kaynaklı yazılım geliştirme ve dağıtımı modeli altında toplanmış Unix benzeri bir bilgisayar işletim sistemidir. Linux'un tanımlayıcı bileşeni, ilk olarak 5 Ekim 1991 tarihinde Linus Torvalds tarafından piyasaya sürülen bir işletim sistemi çekirdeği olan Linux çekirdeğidir.

Canlı bilgisayar sistemi: Canlı bilgisayar sistemi, açık durumda olan bir bilgisayar sistemidir.

Canlı veri adli incelemesi: Canlı veri adli incelemesi, bilgisayarlar içinde bulunan yasal deliller ile ilgili adli bilişim biliminin bir dalı olan bilgisayar adli incelemesinin bir parçasıdır. Bilgisayar adli incelemesi, bir davada delil haline gelebilecek olguların belirlenmesi, korunması, kurtarılması, analiz edilmesi ve sunulması amacıyla bilgisayar sistemlerinin adli bakımdan sağlıklı bir şekilde incelenmesiyle ilgilenir. Canlı veri adli incelemesi de bu amacı güder, ancak sadece açık durumda olan bilgisayar sistemlerine odaklanır. Temel amaç, bilgisayar sistemi kapatıldığında kaybolacak veya bilgisayar sistemi daha uzun süre açık kalacaksa üzerine yazılacak geçici verileri elde etmektir.

Günlük: Belirli bir süre boyunca işletim sistemi veya uygulama tarafından oluşturulan belirlenmiş olayların kaydıdır. Günlükler, harici denetçiler tarafından bilgisayar veya uygulamanın kullanımını kaydetmek/yeniden yapılandırmak için kullanılabilir.

LTE ağları: LTE Advanced, 2009 yılı sonlarında ITU-T'ye 4G sistemi adayı olarak resmen sunulan, ITU, Uluslararası Telekomünikasyon Birliği, IMT-Advanced tarafından onaylanmış ve Mart 2011'de 3GPP tarafından nihai hale getirilmiş bir mobil iletişim standardıdır. 3. Nesil Ortaklık Projesi (3GPP) tarafından Uzun Vadeli Evrim (LTE) standardına ilişkin önemli bir geliştirme olarak standartlaştırılmıştır.

MAC adresi (Medya Erişim Kontrolü): Donanım adresi veya Ethernet adresi olarak da bilinir. Bir bilgisayarın içindeki ağ kartına özgü benzersiz bir tanımlayıcıdır. DHCP sunucusunun, bilgisayarın ağa erişmesine izin verildiğini onaylamasına olanak tanır. MAC adresleri XX-XX-XX-XX-XX-XX biçiminde yazılır; burada X'ler rakamları veya A'dan F'ye kadar olan harfleri temsil etmektedir.

macOS: Apple Inc. (eski adıyla Apple Computer, Inc.) şirketi tarafından Macintosh bilgisayar sistemleri serisi için geliştirilen bir dizi grafik kullanıcı arabirimi tabanlı işletim sistemidir. Macintosh kullanıcı deneyimi, grafik kullanıcı arabirimini popüler hale getirmesiyle tanınır. Apple'ın daha sonra "MacOS" olarak adlandıracağı sistemin ilk hali, ilk olarak 1984'te orijinal Macintosh ile tanıtılan ve genellikle basitçe Sistem yazılımı olarak adlandırılan tümleşik ve adsız sistem yazılımıydı.

Makro virüs: Virüsün nihai halidir. Uygulama dosyalarında (Word, Excel, vb.) taşınırlar ve (geleneksel virüsler gibi) ikili dosyalarda taşınmazlar. Kendilerini içeren veri dosyası açıldığında çalıştırılmış olurlar.

Ana sistem bilgisayarları: Tipik olarak IBM gibi büyük bir şirket tarafından ticari uygulamalar ve diğer büyük ölçekli bilgi işlem amaçları için üretilen büyük bilgisayarlar için kullanılan endüstri terimidir.

Malware: **Kötü amaçlı yazılım. Amacı; bilgisayarlara, sistemlere veya ağlara ve bunun sonucunda da kullanıcılarına zarar vermek olan bir programdır.**

Hafıza önbelleği: Bu verilere hızlı erişim sağlamak için sık kullanılan bilgileri geçici olarak saklayan bir bellek türüdür.

Hafıza kartları: Dijital bilgileri depolamak için kullanılan cihazlardır. Genellikle dijital kameralar, cep telefonları, dizüstü bilgisayarlar, müzik çalarlar ve oyun konsolları gibi birçok elektronik cihazda kullanılırlar. Elektriğe bağlı olmadan verileri saklayabilirler ve çeşitli kapasitelerde olanları vardır, yani büyük miktarlarda veri depolayabilir ama kolayca da gözden kaçırılabilirler.

Bellek cihazları: Bir bellek cihazı, verileri ya kalıcı olarak veya kalıcı olmaksızın depolayabilen bir cihazdır.

Meta veri: Meta veriler, bir dosya ve/veya klasör kombinasyonu hakkında örneğin nasıl ve ne zaman oluşturulduğunu, alındığını, erişildiğini ve değiştirildiğini ve bunların kimin tarafından yapıldığını açıklayabilen bilgilerdir. Bu veriler, Bilgisayar Adli İncelemesinde analiz edilen dosyayla ilişkili olaylar zincirini yeniden oluşturmak için kullanılır. Terimin kullanıldığı bağlama bağlı olarak, veri parçalarının birini veya diğerini ifade edebilir.

Mikroişlemciler: Bir bilgisayarın merkezi işlem biriminin (CPU) işlevlerini tek bir tümleşik devre (IC) veya en fazla birkaç tümleşik devre üzerinde birleştirirler. Sayısal verileri girdi olarak kabul eden, hafızasında kayıtlı talimatlara göre işleyen ve çıktı olarak sonuçlar sunan çok amaçlı, programlanabilir bir cihazdır. Dahili belleğe sahip olduğu için bir sıralı dijital mantık örneğidir. Mikroişlemciler, ikili sayı sisteminde temsil edilen sayılar ve semboller üzerinde çalışırlar.

Microsoft COFEE: **Bilgisayar Çevrimiçi Adli Delil Çıkarıcı**, bilgisayar adli soruşturmacılarının bir Windows bilgisayarından delil çıkarmasına yardımcı olmak için Microsoft tarafından geliştirilen bir araç setidir. Bir USB anlık belleğe veya başka bir harici disk sürücüsüne yüklendiğinde, canlı analiz sırasında otomatik bir adli araç görevi görür. Microsoft, kanun uygulayıcı kurumlara COFEE cihazları ve çevrimiçi teknik desteği ücretsiz olarak sağlamaktadır.

Microsoft PubCenter, Microsoft adCenter'a ek olarak Microsoft tarafından geliştirilen ve reklam verenlerin arama motorlarına ve ayrıca belirli MSN web sitelerine veya uygulamalarına reklam yerleştirmesine olanak tanıyan bir yayıncı reklam sunma uygulamasıdır. Şu anda, beta (deneme) sürümündedir.

Microsoft Windows, Microsoft tarafından geliştirilen, pazarlanan ve satılan bir dizi grafik arayüzlü işletim sistemidir.

Mini bilgisayarlar: 1960'ların ortalarında gelişen ve IBM'in ve doğrudan rakiplerinin

ana sistem bilgisayarlarından ve orta ölçekli bilgisayarlardan çok daha ucuza satılan, daha küçük olan bilgisayar sınıfı için kullanılan bir terimdir.

Modem: Modülatör/DEModülatör. Bilgisayarlar tarafından, telefon hatları üzerinden iletişim kurmak için kullanılan bir cihazdır. Genellikle bir telefon hattına bağlı olması ile tanınır, ancak (örneğin kablolu modemler gibi) DSL teknolojisine dayalı kablolu modemler de vardır. Bir (uyarlanmış) PC kartı içerisinde bir faks işleviyle de birleştirilebilir.

Rafa monte edilen modüler sistemler: Rafa monte edilen modüler sistemler, bir rafın içine takılan bilgisayar sistemleridir ve çoğu zaman modüler bir şekilde oluşturulur ve her bir modülün tüm sistem üzerinde olumsuz bir etkisi olmadan anında değiştirilmesine imkan tanırlar. Bu raflar çoğunlukla 19" biçim katsayısına sahip birden fazla bilgisayar sistemi barındırabilirler.

Mozilla Firefox, Mozilla Corporation ve Mozilla Foundation tarafından koordine edilen Microsoft Windows, MacOS ve Linux için geliştirilmiş ücretsiz ve açık kaynaklı bir web tarayıcısıdır. Firefox, mevcut ve beklenen web standartlarını uygulayan web sayfalarını oluşturmak için Gecko tasarım motorunu kullanır.

Ağ arabirim kartları: Ağ bağlantısı sağlarlar (kablolu veya kablosuz). Genişletme kartı veya PC kartı şeklinde olabilirler.

NTFS (Yeni Teknoloji Dosya Sistemi): Windows NT 3.1 ve Windows 2000'den başlayarak, Windows XP, Windows Server 2003 ve bugüne kadarki tüm ardılları da dahil olmak üzere, Windows işletim sistemleri dizisi için Microsoft Corporation tarafından geliştirilen tescilli bir dosya sistemidir.

Çevrimiçi hizmet sağlayıcı: Örneğin bir internet hizmet sağlayıcısı, e-posta sağlayıcısı, haber sağlayıcısı (basın), eğlence sağlayıcısı (müzik, filmler), arama, e-ticaret sitesi (çevrimiçi mağazalar), e-finans veya e-bankacılık sitesi, e-sağlık sitesi, e-devlet sitesi, Wikipedia, Usenet olabilir. Orijinal daha sınırlı tanımında, sadece ücretli üyelerin bir bilgisayar modemi aracılığıyla hizmete ait özel bilgisayar ağını çevirebildiği ve bülten panoları, indirilebilir dosyalar ve programlar, haber makaleleri, sohbet odaları ve elektronik posta hizmetleri gibi çeşitli hizmetlere ve bilgi kaynaklarına erişebildiği ticari bir bilgisayar iletişim sistemini ifade etmekteydi.

P2P-Eşler Arası: Dosya alışverişi ve indirilmesi için interneti kullanan protokoldür. P2P terimi, *eşler arası* ifadesinin kısaltmasıdır ve bir eşitler ağını ifade eder; bu, her istemcinin durumunun aynı olduğu anlamına gelir. P2P ağlarının pratikteki uygulamasında sunucular olmasının sebebi, istemcilerinin sabit IP adreslerine sahip olmamasıdır. Sonuç olarak, bu sunucular sadece istemcilere ve dosya aramalarına ait birer liste sunmaktadır.

Çağrı cihazları: Çağrı cihazı, sayısal (örneğin telefon numaraları) ve alfanümerik (genellikle e-posta da dahil olmak üzere metin) elektronik mesajlar göndermek ve almak için kullanılabilen bir cihazdır.

Paralel bağlantı noktası teçhizat kilidi: Programlanabilir bellek, uzaktan güncelleme, kiralama kontrol algoritmaları veya sayaçları sağlayabilen paralel bağlantı noktası konektörüne sahip küçük bir cihazdır.

Bölümler: Bir fiziksel disk sürücüsünü birden çok disk gibi kullanmak için, bir sabit disk sürücüsünü *bölümler* olarak adlandırılan birden çok mantıksal depolama birimine bölme işlemidir. BSD, Solaris veya GNU Hurd tabanlı işletim sistemleri için bölümlere "dilimler" de denmektedir. Sabit diskte bu bölümleri oluşturmak, yeniden boyutlandırmak, silmek ve değiştirmek için bir bölüm düzenleyici yazılım programı kullanılabilir.

Çevresel Cihazlar: Bilgisayarın ayrılmaz bir parçası değildirler, ama yeteneklerini geliştirmek için bilgisayara bağlanırlar. Çevresel cihazlara örnek olarak; tarayıcılar, yazıcılar, bant sürücüleri, web kameraları, hoparlörler, mikrofonlar, faks, telesekreterler ve kart okuyucular verilebilir.

Kişisel Dijital Asistan (PDA): Hesaplama, telefon/faks, çağrı, ağ iletişimi ve başka özellikler de içerebilen küçük (yani cep boyutunda) bir cihazdır.

PGP: Oldukça İyi Gizlilik. Orijinal olarak 1991 yılında Philip R. Zimmermann tarafından geliştirilen ücretsiz şifreleme yazılımıdır (bkz., örn. www.pgpl.org). E-postaları şifrelemek/imzalamak veya bilgisayar dosyalarını şifrelemek için kullanılabilir. Düşük maliyetli bir ticari versiyonu da bulunmaktadır.

Pharming (Trafiği Yönlendirme): *Phishing (Kimlik Avı)* ile aynı amaca sahip, ancak kullanıcıyı değil, onun yerine Alan Adı Sistemini (DNS) yanıltmaya dayalı bir tekniktir. Bu yöntemde, kullanıcının ISP'si savunmasız DNS'ler kullanıyorsa, "trafikçi (pharmer)" ilgili URL'lerin tüm trafiğini kontrolü altındaki sunuculara yönlendirir. Bunlar orijinalleri ile aynı görünüme sahiptir. Bu tür bir saldırıyı tespit etmenin tek yolu sertifikalı sunucular kullanmaktır; o durumda "trafikçi" bir Yetki Belgesine sahip olmayacaktır.

Kimlik Avı (Phishing): Bireysel bir kullanıcıdan kişisel bankacılık bilgilerini çalmak amacıyla sosyal mühendisliği belirli teknik numaralarla birleştiren aldatma tekniğidir. *Kimlik avı* saldırıları, akıllıca, banka bilgilerini veya kullanıcının şifrelerini isteyen güvenilir bir kuruluştan gelen e-postaların görünümünü almaktadır.

Phreaker veya Phreak: Diğer insanların sistemlerine erişmek için veya genellikle sadece telefon faturalarını ödememek için telefon ağlarını kullanma konusunda uzmanlaşmış bilişim korsanıdır. *Phreaker'lar* tarafından kullanılan teknikler genellikle *phreak'ler* olarak bilinir.

Program korsanlığı: Yazarlarını koruyan fikri mülkiyet haklarını yasal olarak ihlal ederek mevcut bilişim programlarını kopyalama, dağıtma veya kullanma faaliyetidir.

POP3: Postane Protokolü. Posta sunucusundan (yani POP sunucusundan) e-posta mesajlarını almak için standart bir protokole dayalı bir internet hizmetidir.

Bağlantı noktası çoğaltıcılar: Taşınabilir bir bilgisayara takılan seri, paralel ve ağ bağlantı noktaları gibi ortak PC bağlantı noktalarını içeren bir cihazdır. Bağlantı noktası çoğaltıcı, bağlantı terminallerine benzer, ancak bağlantı terminalleri normalde ek genişletme kartları kullanmak için de imkan sağlar.

Taşınabilir medya oynatıcılar: Müzik ve diğer ses, görüntü, video gibi dijital ortamların yanı sıra belgeler ve dijital olarak depolanabilen diğer alan türleri de dahil olmak üzere başka dosyaları da depolar ve yürütür.

Vekil sunucu (Proxy): Bilgisayar ağlarında, **vekil sunucu**, diğer sunuculardan kaynak arayan istemcilerden gelen istekler için aracı görevi gören bir sunucudur (bilgisayar

sistemi veya uygulama). Bir istemci; bir dosya, bağlantı, web sayfası veya farklı bir sunucudan kullanılabilen başka bir kaynak gibi bazı hizmetleri talep ederek vekil sunucuya bağlanır. Vekil sunucu, karmaşıklıklarını basitleştirmenin ve kontrol etmenin bir yolu olarak bu isteği değerlendirir. Günümüzde çoğu vekil sunucu, Dünya Çapında Ağ'daki içeriğe erişimi kolaylaştıran **web proxy'leridir**.

Qwerty: Günümüzün en yaygın klavye düzenidir.

RAM belleği: RAM, *Rastgele Erişim Belleği anlamına gelir*. RAM belleği, bilgisayarın üzerinde çalıştığı verileri geçici olarak depolar. Bu bellek, bir güç kaybı olması durumunda içerdiği verileri kaybeder.

Kurtarılan veriler: Etkin veri alanından silinmiş olan, kurtarılan veya yeniden oluşturulan dosyaları veya klasörleri tanımlayan terimdir. Bu dosyalar, bazen orijinal boyutunda ve formatında, bazen de adli bir yeniden yapılandırma işlemi gerektiren küçük parçalar halinde kurtarılabilir.

Hizmet reddi: Bir kullanıcının veya kuruluşun normalde kullanabileceği bir kaynağa erişiminin reddedilmesi durumu. Genellikle erişim kaybı, e-posta gibi belirli bir ağ hizmetinin kullanılır olmamasından veya tüm ağ bağlantılarının ve hizmetlerinin geçici olarak kaybedilmesinden kaynaklanır. En kötü durumda, örneğin milyonlarca insanın eriştiği bir web sitesi geçici olarak çalışmayı durdurmaya zorlanabilir. Her ne kadar normalde kasıtlı ve kötü niyetli olsalar da bu tür saldırılar bazen kazara gerçekleşir. Bu saldırılar her zaman bilgi hırsızlığıyla sonuçlanmasa da, etkilenen kişi veya kuruluş için neredeyse her zaman çok fazla zamana ve paraya mal olur.

Tersine mühendislik: Bir programın veya uygulamanın davranışını belirlemek için, ikili kodunun analiz edilmesini içerir.

RIPE Réseaux IP Européens (RIPE, "Avrupa IP Ağları" ifadesinin Fransızcasıdır): İnternetin teknik gelişimine ilgi duyan tüm taraflara açık bir forumdur. RIPE topluluğunun amacı, interneti sürdürmek ve geliştirmek için gerekli idari ve teknik koordinasyonun devam etmesini sağlamaktır. IETF gibi bir standardizasyon kuruluşu değildir ve ICANN gibi alan adlarıyla ilgilenmez.

Yönlendiriciler: Bir paketin hedefine doğru iletilmesi gereken bir sonraki ağ noktasını belirleyen bir cihazdır. En az 2 ağa bağlı olmalıdır. Akıllıdır ve yönlendirme tabloları üzerinde çalışır. Bir ağın ağ geçidinde bulunmasına rağmen, bunun mutlaka internete açılan bir ağ geçidi olması gerekmez.

Zamanlayıcı: iş parçacıklarının, süreçlerin veya veri akışlarının (örneğin işlemci zamanı, iletişim bant genişliği gibi) sistem kaynaklarına erişim sağlama yöntemidir. Bu genellikle bir sistemi etkili bir şekilde dengelemek veya hedeflenen hizmet kalitesine ulaşmak için yapılır. Bir zamanlayıcı algoritmasına duyulan ihtiyaç, çoğu modern sistemin çoklu görev (bir seferde birden fazla işlem yürütme) ve çoğullama (birden çok akışı aynı anda iletme) gerçekleştirme gereksiniminden kaynaklanmaktadır.

SHA-256 adresi: Ulusal Güvenlik Ajansı (NSA) tarafından tasarlanan ve 2001 yılında NIST tarafından ABD Federal Bilgi İşleme Standardı olarak yayınlanan bir dizi kriptografik adresleme işlevidir (**SHA-224, SHA-256, SHA-384, SHA-512**). SHA, Güvenli Adres Algoritması anlamına gelir. SHA-2, selefi SHA-1'e kıyasla belirgin sayıda değişiklik içermektedir. SHA-2; 224, 256, 384 veya 512 bitlik özetlere sahip bir dört adres işlevi dizisinden oluşmaktadır.

Boş alan verileri: Bilgisayarın sabit boyutlu disk alanı blokları tahsis etmesi gerekliliği nedeniyle, her dosyanın sonunda, dosyaya tahsis edilmiş olmasına rağmen, içerdiği diğer bilgilerle ilgili olmayan bilgileri içeren bir alan bulunmaktadır. Bu alan "boş" olarak adlandırılır ve yeni bir dosya tahsis edilmeden önce bu blok alanında bulunan içeriğin bilgilerini içerir.

Boş alan: Boş alan, bir depolama cihazı içinde belirli bir birime, örneğin bir dosya, bir bölüm, bir disk, bir MFT kaydına tahsis edilen, ancak bu birim tarafından kullanılmayan alandır. Çoğu zaman bir adli inceleme uzmanı, bu boş alanlarda daha önce depolanmış dosyalara ait verileri bulabilir. Örneğin, bir küme yeni oluşturulan bir dosyaya tahsis edilmişse ancak bu dosyanın verileri kümenin tamamını kullanmıyorsa, kümenin boş alanında önceden depolanmış bir dosyanın izlerini bulmak pekala mümkündür.

Sosyal Mühendislik: Bilgi açıklamak gibi normalde yapmayacağı eylemleri gönüllü olarak gerçekleştiren bir kişinin manipülasyonuna olanak tanıyan teknikler veya becerilerdir.

Yazılım: Kelime işlemci, muhasebe, ağ yönetimi, Web sitesi geliştirme, dosya yönetimi veya envanter yönetimi gibi belirli görevleri gerçekleştirmek için tasarlanmış bilgisayar programlarıdır.

Katı hal diskler: Geleneksel sabit disklerle aynı şekilde erişim sağlamayı amaçlamakla birlikte, bilgileri sabit disklerden farklı bir şekilde depolarlar. Sabit diskler verileri plakalar üzerinde depolarken, katı hal diskler verileri hareketli parçası olmayan mikroçipler kullanarak depolar. Bu nedenle, darbe ile zarar görme olasılıkları daha düşüktür ve verilere daha hızlı erişim sağlarlar. Bu cihazlar değerli deliller içerebilirler.

Hoparlör mıknatısları: Sıradan hoparlörler; bir mıknatıs, bir bobin ve konik bir parçadan oluşurlar. Hoparlör mıknatısı, hoparlör konisinin kağıdına gömülü olan hoparlör bobini için kalıcı bir manyetik alan sağlaması amacıyla oraya yerleştirilmiştir. Ses sinyali akışı hoparlör bobini içinden geçtiğinde, gücü ses sinyalinin gücüne göre değişen küçük bir manyetik alan oluşturur. Bu küçük manyetik alan, hoparlör mıknatısı tarafından üretilen kalıcı manyetik alan tarafından itilir veya çekilir.

Depolama cihazları: bilgileri (verileri) kaydetmeye (depolamaya) yönelik bir cihazdır. El yazısındaki manuel kas gücünden fonografik kayıttaki akustik titreşimlere, elektromanyetik enerji modülasyonlu manyetik bant ve optik disklere kadar uzanan bir yelpazede neredeyse her enerji türü kullanılarak kayıt yapılabilir.

Tablet Cihazlar: Tablet bilgisayarlar, klavye ya da fare yerine ekrana dokunarak işletilen cihazlardır. Normalde bir cep telefonundan veya **Kişisel Dijital Yardımcıdan** daha büyüktürler.

İzlenebilirlik: İzlenebilirlik, bir süreç zincirindeki her adım hakkındaki bilgilerin eksiksizliği anlamına gelmektedir. İzlenebilirliğin resmi tanımı, benzersiz bir şekilde tanımlanabilir olan varlıkları, doğrulanabilir bir şekilde kronolojik olarak birbiriyle ilişkilendirebilmektir. İzlenebilirlik; belgelenmiş, kayıtlı kimlik tespiti aracılığıyla bir öğenin geçmişinin, yerinin veya uygulanmasının doğrulanabilmesidir.

TrueCrypt: Anında şifreleme (OTFE) için kullanılan ücretsiz bir yazılım uygulamasıdır. Bir dosya içinde sanal şifreli bir disk oluşturabilir veya bir bölümü veya (Windows 2000 dışındaki Microsoft Windows sürümlerinde) tüm depolama cihazını şifreleyebilir (önyükleme öncesi kimlik doğrulaması).

Güvenilir Platform Modülü (TPM): En yaygın olarak TPM kavramı, TPM yongası olarak bilinen bir TPM şifreleme işlemcisi içinde uygulanır. TPM görevlerinin yerine getirilmesinden sorumlu olan bu çip, bir bilgisayar sisteminin ana kartına lehimlenmiştir. Bir TPM'nin birincil amacı, bir platformun bütünlüğünü sağlamaktır. Bu bağlamda "bütünlük", "amaçlandığı gibi davranma" anlamına gelir ve "platform" genel olarak herhangi bir bilgisayar platformudur: Açılışta önyükleme işlemini güvenilir bir durumdan başlatır ve bu güveni, işletim sistemi tamamen önyüklenene ve uygulamalar çalışana kadar sürdürür. TPM ayrıca çoğu zaman disk şifrelemesi, örneğin Truecrypt veya Bitlocker Tam Disk Şifrelemesi ile birlikte, bilgisayarın sabit disklerini şifrelemek için kullanılan anahtarları korumak ve güvenilir bir önyükleme yolu için bütünlük doğrulaması sağlamak amacıyla da kullanılır.

Ubuntu Linux: Debian Linux dağıtımına dayanan ve kendi masaüstü ortamını kullanarak ücretsiz ve açık kaynaklı yazılım olarak dağıtılan bir bilgisayar işletim sistemidir. Adını, Güney Afrika felsefesi olan ubuntu'dan ("başkalarına gösterilen insanlık") almıştır. Bir sunucu sürümü de mevcut olmasına rağmen, Ubuntu öncelikle kişisel bilgisayarlarda kullanılmak üzere tasarlanmıştır.

Evrensel Seri Veriyolu (USB): Bilgisayarlara bağlanacak cihazlar için iletişim, bağlantı ve güç kaynağı protokollerini tanımlayan bir standarttır. 1990'larda ortaya çıkmasından bu yana, artık bu protokolü kullanarak bağlanabilen cihazların sayısı artmıştır ve artık veri depolamak için her türlü şekil ve boyuta sahip olan yeni cihazlar kullanılmaktadır.

Unix: İlk olarak 1969'da geliştirilen çok görevli, çok kullanıcılı bir bilgisayar işletim sistemidir.

Güvenilmeyen ikili dosyalar: "Güvenilmeyen ikili dosya" terimi, çoğunlukla güvenilmeyen bir kaynaktan depolanan veya kopyalanan, çalıştırılabilir ikili dosyalar için kullanılır. Doğrulanamayan veya tanımlanmış yakın doğrulama prosedürlerinden geçmemiş herhangi bir kaynak, potansiyel olarak değiştirilmiş veya hatta zararlı kaynak kod içerebilir ve bu nedenle de güvenilmez olarak kabul edilmelidir. Güvenilmeyen ikili dosyaların tipik bir örneği, adli inceleme uzmanının doğrulanmış makinesinden başka bir sistemde depolanan çalıştırılabilir dosyalardır.

Kullanılmayan veya tahsis edilmemiş alan verileri: Şu anda bir dosyaya ait olmayan disk alanında bulunan veriler, silinen dijital belgelerden geriye kalan verilerdir.

URL (Tekdüzen Kaynak Konum Belirleyici): **Dünya Çapında Ağ›a ait belgelerin** (*haber, metin içerik*, vb.) her birine benzersiz bir adresin tahsis edildiği bir karakter zinciridir.

UTorrent: Artık BitTorrent, Inc. şirketine ait olan ücretsiz, kapalı kaynaklı bir BitTorrent istemcisidir. Çin dışında (orada Xunlei daha popülerdir) en yaygın kullanılan BitTorrent istemcisidir. Adındaki "µ" sembolünü, programın küçük bellek ayak izine atıfta bulunularak "micro-" metrik önekinden almaktadır: Program, Vuze veya BitComet gibi daha büyük BitTorrent istemcileriyle kıyaslanabilir işlevsellik sunarken asgari bilgisayar kaynağı kullanmak üzere tasarlanmıştır. Program; özellik seti, performansı, kararlılığı ve eski donanım ve Windows sürümleri için desteği ile sürekli olarak iyi eleştiriler almıştır.

Sanal ortam: Fiziksel konumlarından bağımsız olarak dijital bilgilere erişim imkanı tanıyan birden fazla bilgisayarın birbirine bağlanmasıyla oluşturulan bir çalışma ortamının bilişimsel simülasyonudur.

Virüs: Diğer programlara bulaşabilen ve onları kendisinin bir kopyasını içerecek şekilde değiştiren programdır. Virüsler temel olarak yayılma ve çoğalma işlevine sahiptir, ancak ayrıca basit bir şakadan sistemlere ciddi hasar vermeye kadar farklı amaçlara sahip zararlı içeriklere (*güvenlik yüklerine*) sahip olanları da vardır. Bu tür programlar çeşitli şekillerde çalışabilirler: Görünür bir hasara yol açmadan sadece kullanıcıya varlığını bildirmek, mümkün olan en fazla hasara neden olmak için fark edilmemeye çalışmak veya temel işlevleri ele geçirmek (dosyalama sistemine bulaşmak).

VoIP: İnternet Protokolü Üzerinden Ses. İnternet protokolünü kullanarak bir veri ağı üzerinden sesli konuşmaları iletmek için kullanılan teknolojidir. Veri ağı internet veya kurumsal ağ olabilir.

Geçici Veriler: Geçici Veriler, dijital olarak depolanan, insan etkileşimi veya otomatik işlemler ile kısa bir süre içinde içeriklerinin silinme, üzerine yazılma veya değiştirilme olasılığı çok yüksek olan verilerdir.

Warez: Programların korsan kopyalarıdır. Korumanın kaldırıldığı korumalı yazılım sürümleridir.

Web Tarayıcısı: Bir web tarayıcısı, kullanıcıların internetteki belgelere ve diğer kaynaklara erişmesini, bunları almasını ve görüntülemesini sağlamak için tasarlanmış bir uygulama yazılımı veya program olarak da tanımlanabilir.

Windows Gezgini: Microsoft Windows işletim sisteminin Windows 95'ten itibaren bütün sürümlerinde bulunan bir dosya yöneticisi uygulamasıdır. Dosya sistemlerine erişmek için bir grafik kullanıcı arayüzü sağlar. Aynı zamanda ekranda görev çubuğu ve masaüstü gibi birçok kullanıcı arayüzü öğesi sunan işletim sisteminin de bir bileşenidir. Bilgisayarı Windows Gezgini çalıştırmadan kontrol etmek mümkündür (örneğin, Windows'un NT türevi sürümlerinde Görev Yöneticisi'ndeki Dosya | Çalıştır komutu gibi komut istemi penceresine yazılan komutlar da Windows Gezgini olmadan çalışacaktır).

Kablosuz Modemler: Kablosuz modem, telefon veya kablolu televizyon hatları kullanmak yerine kablosuz bir ağa bağlanan bir modülatör-demodülatör türüdür. Mobil internet kullanıcısı, internet erişimi elde etmek için kablosuz İnternet Servis Sağlayıcısına (ISP) kablosuz bir modem kullanarak bağlanabilir.

WireShark: Ücretsiz ve açık kaynaklı bir paket analiz aracıdır. Ağ sorunlarını giderme, analiz, yazılım ve iletişim protokolü geliştirme ve eğitim amaçlarıyla kullanılmaktadır. Orijinal adı **Ethereal** olan proje, Mayıs 2006'da ticari marka sorunları nedeniyle Wireshark olarak yeniden adlandırılmıştır.

WLAN ağları: Kablosuz yerel alan ağı (WLAN), bazı kablosuz dağıtım yöntemlerini (tipik olarak yayılmış spektrum veya OFDM radyo) kullanarak iki veya daha fazla cihazı birbirine bağlar ve genellikle bir erişim noktası aracılığıyla internete bağlantı sağlar. Bu, kullanıcılara yerel bir kapsama alanı içinde hareket edebilme ve yine de ağa bağlı kalma hareketliliği sağlar. Çoğu modern WLAN, Wi-Fi markası altında pazarlanan IEEE 802.11 standartlarına dayanmaktadır.

Kelime İşlemci: Bilgisayarı; mektuplar, raporlar ve belgeler yazmak için bir daktiloya dönüştürmek için kullanılan bir yazılım programıdır. Yaygın Kelime İşleme programları: Wordstar, Wordperfect, MS-Word.

Solucan (Worm): Otomatik olarak çoğalan ve otomatik olarak yayılan bilgisayar programı. Virüslerin aksine solucanlar genellikle özel olarak ağlar için yazılmaktadır. Ağ solucanları ilk olarak Xerox'tan Shoch & Hupp tarafından *ACM Communications* dergisinde (Mart 1982) tanımlanmıştır. İlk ünlü internet solucanı Kasım 1988'de ortaya çıkmış ve kendisini internette 6.000'den fazla sistem geneline yaymıştır.

WWW (Dünya Çapında Ağ): Ağ üzerinden erişilebilir bilgi evreni, yani Köprü Metin Aktarım Protokolünü (HTTP) kullanan internetteki tüm kaynaklar ve kullanıcılardır.

ZIP sürücüleri: Çıkarılabilir bir sabit disk sistemidir. ZIP sürücüsü, öncelikle kişisel bilgisayar dosyalarını yedeklemek ve arşivlemek için kullanılan küçük, taşınabilir bir disk sürücüsüdür. Ticari marka olan ZIP sürücüsü, Iomega Corporation şirketi tarafından geliştirilmiş ve satılmıştır. Zip sürücüleri ve disklerin iki boyutu bulunmaktadır.

12 Daha Fazla Bilgi

12.1 Kitaplar / Kılavuzlar

12.1.1 Uluslararası

- ISO/IEC
  - 17025: 2017: Test ve kalibrasyon laboratuvarlarının yeterliliğine ilişkin genel şartlar
  - 27037: 2012: Dijital delillerin tespit edilmesi, toplanması, elde edilmesi ve korunması hakkında kılavuz
  - 27041: 2015: Olay soruşturma yönteminin uygunluğunun ve yeterliliğinin sağlanmasına hakkında kılavuz
  - 27042: 2015: Dijital delillerin analiz edilmesi ve yorumlanması hakkında kılavuz
  - 27043: 2015: Olay soruşturma ilkeleri ve süreçleri

  https://www.iso.org/standards.html
- İnterpol:
  - Dijital Adli Bilişim Laboratuvarları için Küresel Kılavuz.

  https://www.interpol.int/en/content/download/13501/file/INTERPOL_DFL_GlobalGuidelinesDigitalForensicsLaboratory.pdf
  - Dijital Adli İnceleme İlk Müdahale Ekipleri için Kılavuz - Elektronik ve dijital delillerin aranması ve bunlara elkonulması için en iyi uygulamalar

  https://www.interpol.int/content/download/16243/file/Guidelines%20to%20Digital%20Forensics%20First%20Responders_V7.pdf
- SWGDE:
  - Mobil Cihazdan Delil Toplanması ve Korunması, İşlenmesi ve Elde Edilmesi için En İyi Uygulamalar, Bilimsel Çalışma Grubu DE v1.2 (2020);
  - Mobil Cihaz Adli Analizi için En İyi Uygulamalar_v1.0 (2020)
  - Bulut Hizmeti Sağlayıcılarından Dijital Delil Toplama için En İyi Uygulamalar_v1.0 (2020);
  - Gömülü Cihaz Adli İncelemesi için Temel Yetkinlikler_v1.0 (2020)
  - ve daha fazlası

  https://www.swgde.org/documents/published
- Stephen Mason, *Elektronik Delil* (4. baskı, İleri Yasal Araştırmalar Enstitüsü, Londra Üniversitesi, 2017)

- Stephen Mason (Editör), *Uluslararası Elektronik Delil* (İngiliz Uluslararası ve Karşılaştırmalı Hukuk Enstitüsü, 2008)

12.1.2 Amerika Birleşik Devletleri

- ABD Adalet Bakanlığı - Elektronik Olay Yeri İncelemesi - İlk müdahale ekipleri için bir kılavuz.

  https://www.ncjrs.gov/pdffiles1/nij/187736.pdf

- ABD Adalet Bakanlığı - Dijital Delillerin Adli İncelemesi: Kolluk Kuvvetleri için bir Kılavuz.

  https://www.ncjrs.gov/pdffiles1/nij/199408.pdf

- Michael R Arkfeld, *Arkfeld ile Elektronik Keşif ve Delil* (3. baskı, Lexis, 2011) Looseleaf
- Adam I. Cohen ve David J. Lender, *Elektronik Keşif: Hukuk ve Uygulama* (2. baskı, Aspen Publishers, 2011) Looseleaf
- Jay E. Grenig, William C. Gleisner, Troy Larson ve John L. Carroll, *e-KEşif ve Dijital Deliller* (2. baskı, Westlaw, 2011) Looseleaf
- Michele C.S. Lange ve Kristen M. Nimsger, *Elektronik Deliller ve Keşif: Her Avukatın Bilmesi Gerekenler* (2. baskı, American Barolar Birliği, 2009)
- George L. Paul, *Dijital Delilin Temelleri* (Amerikan Barolar Birliği, 2008)
- Paul R. Rice, *Elektronik Delil – Hukuk ve Uygulama* (Amerikan Barolar Birliği, 2005)

12.1.3 Avrupa

- Dijital Teknolojinin Adli İncelemesi için ENFSI En İyi Uygulama Kılavuzu

  https://enfsi.eu/wp-content/uploads/2016/09/1._forensic_examination_of_digital_technology_0.pdf

- Kraliyet Savcılık Servisi Yasal Kılavuzu. https://www.cps.gov.uk/prosecution-guidance
- Emniyet Amirleri Derneği (ACPO) Elektronik Delil Kılavuzu.

  https://www.7safe.com/docs/default-source/default-document-library/acpo_guidelines_computer_evidence_v4_web.pdf

12.2 Dergiler

- Uluslararası Adli Bilim: Dijital Soruşturma

  https://www.journals.elsevier.com/forensic-science-international-digital-investigation

- Uluslararası Dijital Suç ve Adli Bilişim Dergisi.

  https://www.igi-global.com/journal/international-journal-digital-crime-forensics/1112

- Uluslararası Adli Bilgisayar Bilimleri Dergisi.

  http://ijofcs.org

- Dijital Delil ve Elektronik İmza Hukuku İncelemesi.

  https://journals.sas.ac.uk/deeslr/

- Adli Bilişim, Güvenlik ve Hukuk Dergisi.

  http://www.jdfsl.org

- Adli Bilişim ve Güvenlik Konusunda IEEE İşlemleri.

  https://signalprocessingsociety.org/publications-resources/ieee-transactions-information-forensics-and-security

12.3 Yazarlar Hakkında

Avrupa Konseyi, bu kılavuzu yazmak için birbirini tamamlayan geçmişlere sahip bireyleri seçmiştir. Bunlar:

Victor Völzow, Hesse Eyalet Kamu Yönetimi ve Güvenliği Üniversitesi'nde adli bilişim ve bilişim suçları soruşturması konusunda eğitmendir. Bu pozisyonda, adli bilişim denetçilerine yönelik müfredatın geliştirilmesinden ve uygulanmasından sorumludur. Akademideki işi, öğretmenliğin yanı sıra, Yüksek Teknoloji Suç birimleri ve diğer kolluk kuvvetleri için pratik destek ve teknik danışmanlık sağlanmasını da içermektedir. Victor, Avrupa Konseyi (CoE), Avrupa Dolandırıcılıkla Mücadele Ofisi (OLAF), Avrupa Birliği Kolluk Kuvvetleri Eğitim Ajansı (CEPOL) ve AGİT gibi kuruluşlar için uzman düzeyinde eğitimler geliştirmekte ve sunmaktadır. Elektronik delil, adli bilişim ve farklı kuruluşlara yönelik eğitim konularında bir kitap ve bir dizi kılavuz yazmıştır ve 10 yılı aşkın bir süredir uluslararası kapasite geliştirme projelerinde yer almaktadır. Farklı üniversiteler için konuk konuşmacı olarak görev yapmış ve Bundeskriminalamt'ta (BKA) Alman adli bilişim uzmanı eğitim programında yer almıştır. 20 yılı aşkın bir süredir polis memuru olarak adli bilişim alanında yaklaşık 15 yıl geçirmiş ve çeşitli vesilelerle bilirkişilik yapmıştır. Adli bilişim alanında çeşitli profesyonel sertifikalara sahip olmasının yanı sıra Victor, 2011 yılında University College Dublin'de Adli Bilişim ve Bilişim Suçları Araştırmaları alanında yüksek lisans derecesini tamamlamış ve en yüksek notu alarak Garda Komiserlik Madalyası ile ödüllendirilmiştir.

Mark Cameron MSc, şu anda bilişim suçları, adli bilişim ve mobil cihaz adli incelemesi, açık kaynaklı istihbarat, çevrimiçi gizli polislik ve çocuk sömürüsü ve istismarı konularında uzmanlık sağlayan küçük bir eğitim danışmanlığı işi yürüttüğü Birleşik Krallık'ta yaşayan bir emekli polis memurudur. 2013 yılında Birleşik Krallık'taki Cumbria Polisi'nden emekli olan Mark, 18 yılını teknolojinin söz konusu olduğu birçok farklı suç türüyle mücadele ederek ve sayısız davada delil sağlayarak geçirmiştir.

1999 yılında ACPO "Bilgisayar Tabanlı Deliller – İyi Uygulama Kılavuzu"nun orijinal yazımında yer almış ve bu çalışma alanında katılım göstermeyi sürdürmüştür. Mark, son derece deneyimli bir uygulayıcı olmanın yanı sıra, 20 yılı aşkın bir süredir bilişim suçlarının tüm yönleri ile ilgili eğitimler vermekle ve yazmakla uğraşmış ve Birleşik Krallık'taki Polislik Koleji, Interpol, UNICEF ve Avrupa Konseyi de dahil olmak üzere

birçok ulusal ve uluslararası eğitim organizasyonu ile hem Birleşik Krallık'ta hem de yurtdışında çalışmıştır. Avrupa, Asya, Afrika, Amerika Birleşik Devletleri ve Karayipler'de eğitimler vermiştir.

Ayrıca bir dizi kuruluş için ulusal ve uluslararası düzeylerde çalışmış ve Birleşik Krallık'ın Çocuk İstismarı ve Çevrimiçi Koruma Merkezi de dahil olmak üzere farklı kuruluş ve yargı alanlarında adli laboratuvarların kurulmasından sorumlu olmuştur. Yüksek lisans derecesini (MSc), 2006 yılında Kraliyet Askeri Bilim Koleji ve Cranfield Üniversitesi'nden Adli Bilişim alanında almıştır.

Jan Kerkhofs, Brüksel'deki Belçika Federal Savcılığı'nda görev yapan bir Federal Hâkimdir. Belçika Federal Savcılığı bünyesindeki Siber Birimin bir üyesidir. Alfa-case siber soruşturmalarını yönetmekte ve ulusal ve uluslararası bilişim suçları soruşturmalarını koordine etmektedir.

Buna ek olarak, Jan Kerkhofs bir Belçika Federal Polisi ve Yargı eğitmenidir ve yeni atanan sulh hâkimlerinin yanı sıra Belçika Yargı Eğitim Enstitüsü'nde (IGO) uzmanlaşmış bilişim suçları sulh hâkimlerinin de bilişim suçları, elektronik delillerin ele alınması ve çevrimiçi soruşturmalar konularındaki eğitimlerinin sorumlularından biridir. Aynı zamanda farklı kolluk kuvvetlerine, barolara ve (Avrupa Konseyi, IAP/GPEN, OSCE, EC/TAIEX, ERA, EJTN, ICCT gibi) uluslararası kuruluşlara bilişim suçları konularında eğitimler vermektedir.

Jan Kerkhofs, ulusal ve uluslararası düzeyde tanınmış bir bilişim suçları uzmanıdır. Belçika Bilişim Suçları Uzmanlık Ağı'nın yönetim kurulu üyesidir. Bilişim suçları, terörle mücadele ve özel soruşturma yöntemleri konularında bir devlet uzmanı ve danışmanıdır. Ayrıca, Budapeşte Bilişim Suçları Sözleşmesi'nin (CoE) Bilişim Suçları Sözleşmesi Komitesi'ne (T-CY) Belçika delegasyonunun uzmanı olarak atanmıştır ve Eurojust'taki Avrupa Adli Bilişim Suçları Ağı'nın (EJCN) Belçika ulusal temsilcisidir.

Bilişim suçları ve terörle mücadele konularında düzenli olarak yayınlar yapmaktadır ve bilişim suçları üzerine "*Bilişim Suçları*" (2013) ve onun devamı olan "*Bilişim Suçları 3.0*" (2019) Belçika standart çalışma ve saha kılavuzunun ve "*Belçika ve Hollanda Asli Terörizm Mevzuatının Karşılaştırmalı Analizi*" kitabının ve "*Terörle Mücadele: Belçika'da terörizmine yargısal yaklaşım*" kitabının yazarlarından biridir.

Jan Kerkhofs, Belçika'da bulunan KULeuven üniversitesinden Hukuk Yüksek Lisans derecesi (1996) ve Paris, Fransa'da bulunan l'Université Panthéon-Assas-Paris II üniversitesinden Ceza Hukuku ve Ceza Bilimleri İleri Araştırmalar Diploması (DEA) (1997) sahibidir. Ayrıca Siber Güvenlik alanında SANS GSEC401 sertifikasına sahiptir ve teknik bilgi ve uzmanlığa sahip sertifikalı bir siber güvenlik uzmanıdır.

Nigel Jones MBE FBCS, teknoloji risk çözümleri ve eğitiminde uzmanlaşmış bir şirket olan Technology Risk Limited'in direktörlüğünü yapmıştır ve İngiltere'de bulunan Canterbury Christ Church Üniversitesi'nde misafir öğretim üyesidir. Ayrıca eğitim, araştırma ve öğretim konusunda bir bilişim suçları mükemmellik merkezi ağının geliştirildiği bir projede (2CENTRE) kolluk kuvvetleri koordinatörü olarak görev almıştır. Bundan önce, Birleşik Krallık'ta Wyboston'da bulunan Ulusal Polislik Faaliyetleri Mükemmellik Merkezi'ndeki Ulusal Yüksek Teknoloji Suçları Eğitim Merkezi'nin kurulmasından ve işletilmesinden sorumlu idi. ACPO "Bilgisayar Tabanlı Delil - İyi Uygulama Kılavuzu"nun yazarlarından biridir ve ABD'de Elektronik Delillerin Soruşturulması Teknik Çalışma

Grubunun (TWGIEE) üyesidir. Nigel, Birleşmiş Milletler 10. Suç Kongresi'nde yüksek teknolojili bir suç senaryosunun hazırlanması ve moderasyonu da dahil olmak üzere çok sayıda ulusal ve uluslararası etkinlikte sunumlar yapmıştır. Ocak 2005'te Nigel, Üye Ülkeler tarafından Interpol Avrupa Bilişim Suçları Çalışma Grubu Başkanı olarak seçilmiştir. Nigel, Interpol adına kendi personeline verdiği bilişim suçları eğitimlerinin yanı sıra Hindistan, Kıbrıs ve Suriye'de de uluslararası kurslar vermiştir. Nigel, Avrupa Konseyi adına Avrupa, Orta Doğu ve Kuzey Amerika'daki ceza hukuku makamlarına eğitimler vermiştir.

Esther George (Birleşik Krallık) LLB (Hons), LLM, MA. 2014 yılına kadar Esther, İngiltere ve Galler Kraliyet Savcılık Servisi'nde (CPS) politika danışmanı ve kıdemli başsavcı olarak görev yapmıştır. Şu anda uluslararası bir danışman olarak çalışmaktadır. Esther, internet ve bilgisayar destekli suç, dijital delil, fikri mülkiyet hırsızlığı ve verilerin korunması konularında uzmanlaşmıştır. Savcılar için Kraliyet Savcılık Servisi ulusal yüksek teknolojili suçlar eğitim kursunu tasarlamış ve geliştirmiştir. 2010 yılında Esther, dünya çapında yüksek teknolojili suçların çözülmesine yardımcı olmak için çevrimiçi bir bilgi paylaşım ağı olan Küresel Savcılar E-Suç Ağı'nı (GPEN) başlattığı ve geliştirdiği için Uluslararası Savcılar Birliği'nden bir Üstün Başarı Belgesi almıştır. Esther, ulusal ve uluslararası konferanslarda ve eğitim oturumlarında yüksek teknolojili suçlar hakkında düzenli olarak konuşmalar yapmaktadır.

Fredesvinda Insa Mérida, hukuk fakültesi mezunudur ve Bilgi ve İletişim Teknolojisi Doktorasına sahiptir. 2004 yılından başlayarak, Price Waterhouse Coopers ve Avrupa Konseyi için ve daha sonra da Cybex için faaliyetlerini durdurduğu 2010 yılına kadar avukat olarak çalışmıştır. Cybex'te Strateji Geliştirme Direktörü olarak görev yapmış ve ulusal düzeyde, Avrupa düzeyinde ve uluslararası düzeyde kurumsal ilişkileri yönetmiştir. Cybex'te hukuk, eğitim, proje ve iletişim departmanlarını yönetmiştir. Elektronik ortam ve elektronik delillerin hukuki açıdan adli analizi, İspanya ve Avrupa'daki elektronik delillerin hukuki durumunun incelenmesi ve analiz edilmesi, sektörün teşvik edilmesi ve bu konular ile ilgili bilgilerin yayılması konusunda uzmanlaşmıştır. Avrupa Komisyonu tarafından finanse edilen "Elektronik Delillerin Mahkemede Kabul Edilebilirliği: Yüksek Teknolojili Suçlarla Mücadele", "Bilişim Suçları ve Elektronik Deliller ile ilgili Avrupa Sertifikası" ve "Bilişim Suçları ile Mücadele hakkında Elektronik Bülten" adlı Avrupa projelerini yönetmiştir. Bu konularda Avrupa Komisyonu ve Avrupa Konseyi tarafından tanınmış bir uzmandır ve Birleşmiş Milletler Uluslararası Telekomünikasyon Birliği ajansının Üst Düzey Uzman Grubunun da üyelerinden biridir. 2004 yılından bu yana İspanya'da İspanya Yargı Gücü Genel Konseyi'nde her yıl düzenlenen Elektronik Delil Seminerlerinin yaratıcısı ve organizatörüdür. Uzmanlık dergileri ile işbirliği yapmakta ve konferans ve etkinliklere katılmaktadır. Fredesvinda Insa, halen CFLabs'ın Strateji Geliştirme Direktörüdür.

Uwe Rasmussen, Paris merkezli hukuk firması August & Debouzy'nin Fikri Mülkiyet/Bilişim departmanında telif hakkı, veritabanı hakları, kişisel verilerin korunması ve uygunluk alanlarındaki davalarını yöneten bir kıdemli avukattır. 2006 yılından beri, geçici görevlendirmeyle Microsoft'un Dijital Suçlar Birimi ile bilişim suçlarının tenfiz edilmesi ve işbirliği girişimleri üzerine çalışmaktadır. Sayın Rasmussen, Paris'teki Sorbonne Üniversitesi'nden ve Kopenhag Üniversitesi'nden hukuk derecelerine sahiptir, Santa Clara Üniversitesi'nde fikri mülkiyet hukuku eğitimi almıştır ve ayrıca Microsoft Sertifikalı bir Sistem Mühendisidir. Danca, Felemenkçe, İngilizce, Fransızca, Almanca ve İspanyolca bilmektedir.

13 Ekler

13.1 Ek A - Arama ve Elkoyma Kolluk Kuvvetleri Akış Şeması

Funded by the European Union and the Council of Europe

EUROPEAN UNION

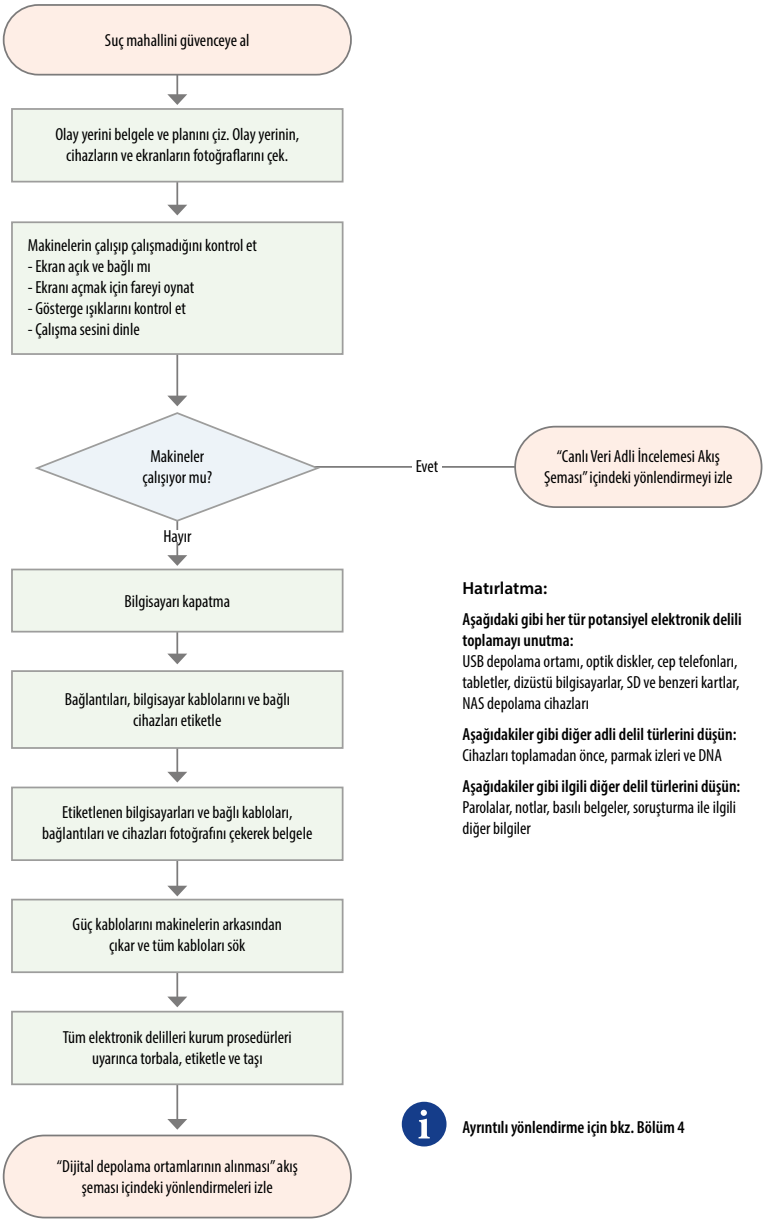
COUNCIL OF EUROPE

CONSEIL DE L'EUROPE

Implemented by the Council of Europe

Elektronik Delil Kılavuzu

Arama ve Elkoyma Akış Şeması

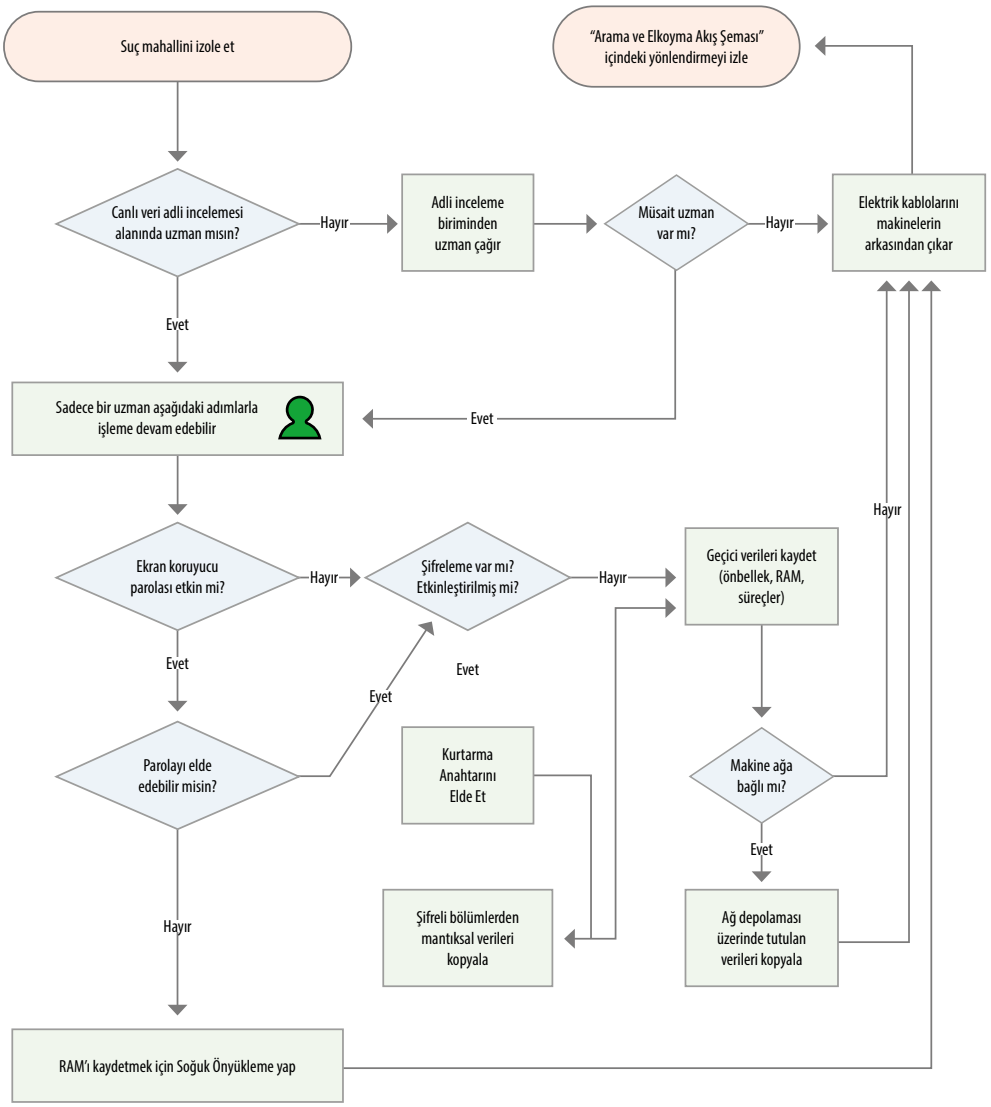


13.2 Ek B - Canlı Veri Adli İncelemesi Akış Şeması

Funded by the European Union and the Council of Europe
EUROPEAN UNION
COUNCIL OF EUROPE
CONSEIL DE L'EUROPE
Implemented by the Council of Europe

Elektronik Delil Kılavuzu

Canlı Veri Adli İncelemesi Akış Şeması



Ayrıntılı yönlendirme için bkz. Bölüm 4

13.3 Ek C - Özel Sektör Hazırlığı Akış Şeması

Funded by the European Union and the Council of Europe

EUROPEAN UNION

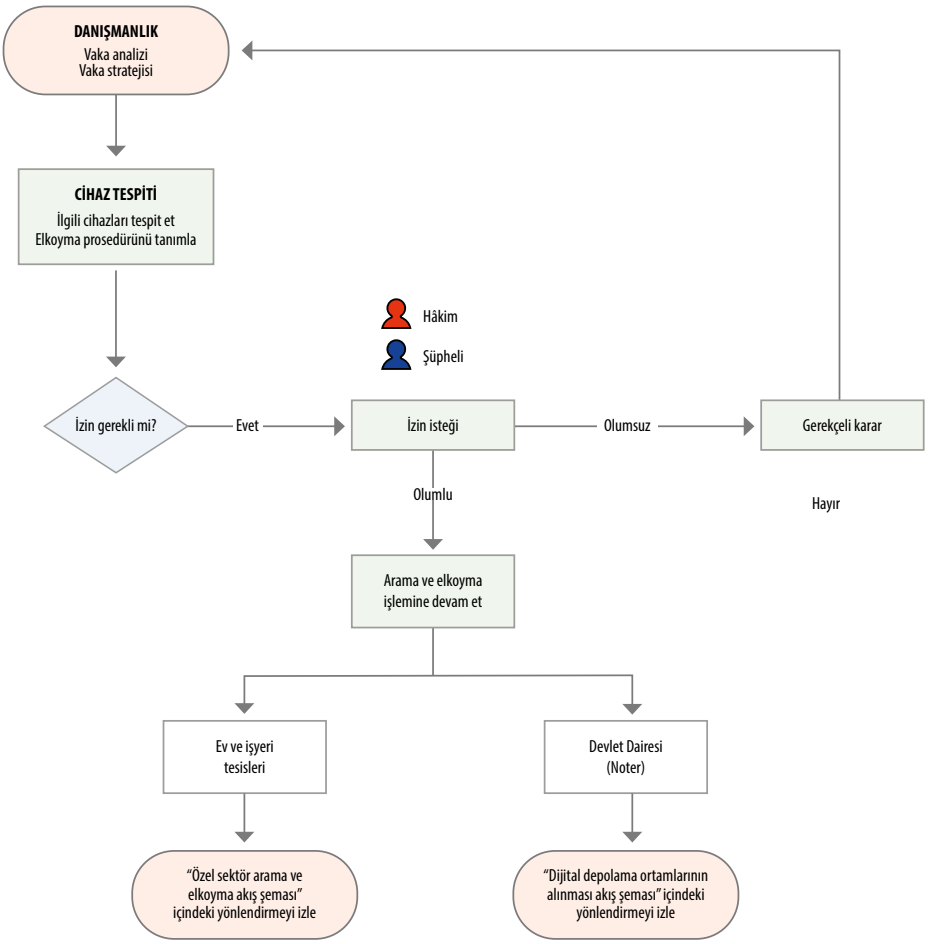
COUNCIL OF EUROPE

CONSEIL DE L'EUROPE

Implemented by the Council of Europe

Elektronik Delil Kılavuzu

Özel sektör hazırlık akış şeması



Ayrıntılı yönlendirme için bkz. Bölüm 4

13.4 Ek D - Özel Sektör Arama ve Elkoyma Akış Şeması

Funded by the European Union and the Council of Europe

EUROPEAN UNION

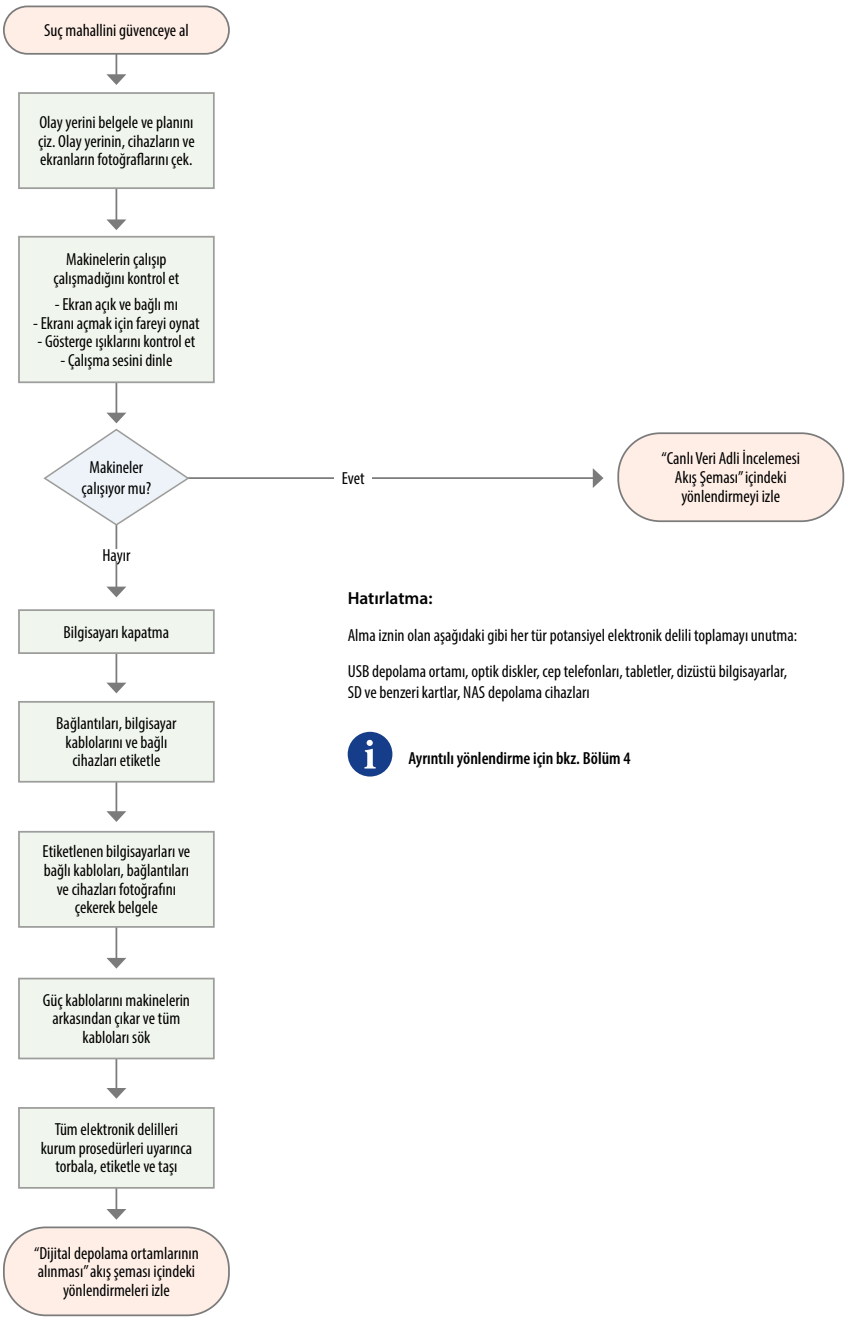
COUNCIL OF EUROPE

CONSEIL DE L'EUROPE

Implemented by the Council of Europe

Elektronik Delil Kılavuzu

Özel sektör arama ve elkoyma akış şeması



Hatırlatma:

Alma iznin olan aşağıdaki gibi her tür potansiyel elektronik delili toplamayı unutma:

USB depolama ortamı, optik diskler, cep telefonları, tabletler, dizüstü bilgisayarlar, SD ve benzeri kartlar, NAS depolama cihazları

Ayrıntılı yönlendirme için bkz. Bölüm 4

13.5 Ek E - Dijital Delil Toplama Akış Şeması

Funded
by the European Union
and the Council of Europe

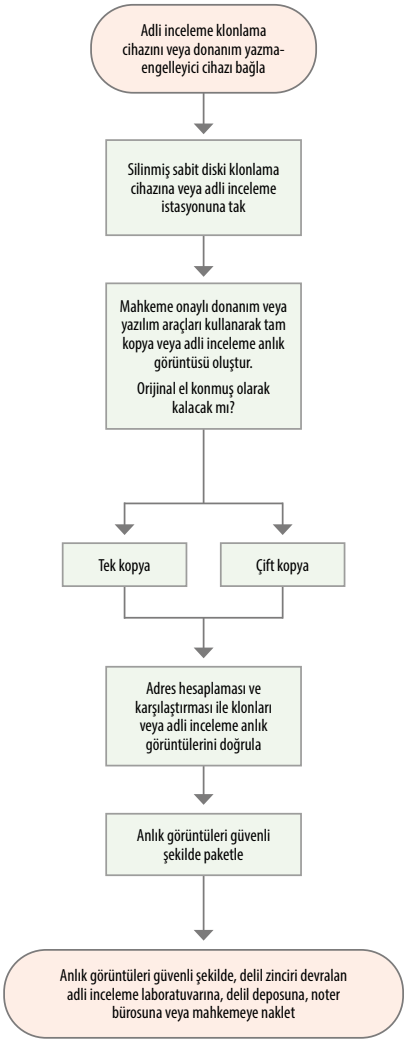
EUROPEAN UNION

COUNCIL OF EUROPE
CONSEIL DE L'EUROPE

Implemented
by the Council of Europe

Elektronik Delil Kılavuzu

Dijital delil toplama akış şeması



13.6 Ek F - Delil Zinciri Kaydı

DELİL ZİNCİRİ KAYDI

Vaka Referans No ……

Kayıt …… / ……

BU KAYDIN KULLANIMINA İLİŞKİN GENEL YÖNLENDİRME

Bu kayıt, bir öğeye elkonulacağı her durumda (veya anlık görüntü oluşturulduğu takdirde) kullanılmak üzere tasarlanmıştır ve daha sonra mahkemede delil olarak sunulması gerekebilir.

Delillerle ilgili güvenlik zincirinin kesintisiz olması esastır ve bu nedenle, soruşturma boyunca delillerin saklanması ve güvenliği her şeyden önce gelmelidir.

Soruşturma sırasında elkonulan öğelerin yasal olarak elde edildiğinden emin olmak için özen gösterilmeli ve gerektiğinde izin/onay bölümünden (sayfa 10 ila 11) yararlanılmalıdır.

Bu kitapçığın içindeki bölümler, olası her durumu öngörmek amacıyla eklenmiştir ve bu nedenle sorumlular, bazı bölümlerin her durumda doldurulması gerekmediğini bilmelidir.

Aynı şekilde, bu kitapçıkta özetlenen soruların hiçbir şekilde eksiksiz olmasının amaçlanmadığı ve bazılarının her durumda geçerli olmayacağı unutulmamalıdır. İlave bazı soruların eklenebilmesi için ek notlar alanı bırakılmıştır, ancak bu alanın tamamen kullanıldığı hallerde daha fazla soru ve cevap 'Olay Yeri Notları' bölümüne (sayfa 12 ila 15) kaydedilebilir.

DELİL İBRAZ TALİMATLARI

Elkonulan her öğeye, olay yerinde doldurulması gereken bir delil etiketi takılacaktır.

Bir öğeyi ilk elkoyan kişi o öğeyi delil haline getirmelidir. Bunlara delil referans numarası verilecektir.

Bu delil referans numaraları benzersiz olmalı ve kişinin adının ve soyadının baş harflerini takiben 1'den başlayan bir sıra numarasından oluşmalıdır; örneğin, Anne Browne'ın ilk delili AB/1 olacaktır. Delile başvuran veya delile bakan herkes delil etiketini imzalamalıdır.

Her delilin benzersiz bir referans numarası olmalıdır ve bu numara daha sonra o öğeye atıfta bulunan herkes tarafından kullanılmalıdır.

Bir sorumlunun, olay yerinde elkonulan bir öğenin mahkemede sunulan öğe ile aynı olduğunu mahkemede göstermesi gerekecektir. Bu nedenle, bir öğenin başka bir kişiye teslim veya tevdi edilmesi durumunda, bu işlemlerin eksiksiz olarak belgelenmesi çok önemlidir.

Bir delili alan herhangi bir kişi, ilgili delil etiketini imzalamalı, dolayısıyla delil güvenlik zincirini muhafaza etmelidir.

Bir sonraki raporda veya beyanda bir delile atıfta bulunan herhangi bir kişi, delilin referans numarasını da eklemelidir.

Aynı zamanda ve yerde birbirinin aynısı olan öğeler bulunursa, bunlar aynı delil referans numarası altında birlikte gruplanabilir, ancak gruplanan öğelerin doğru sayıldığından emin olmak için özen gösterilmelidir, *örneğin* otuz dört (34) DVD.

SORGULAMA / İFADE ALMA

Delillerle ilgili tüm soru ve cevap kayıtları eş zamanlı olarak kaydedilmelidir.

Bir elkoymanın sonunda, sorgulanan herhangi bir kişinin, doğruysa her cevabı paraflaması, her sayfanın altını imzalaması ve son kayıt kelimelerinden sonra "Bunun ifademin doğru bir kaydı olduğunu onaylıyorum" yazması ve imzasını atması istenmelidir.

Delillere elkoyan herkes, ilgili kayıtları paraflamalı ve sayfayı imzalamalıdır.

Bir kişinin bir kaydı paraflamayı veya imzalamayı reddettiği durumlarda, hazır bulunan kıdemli kişi her cevabı paraflamalı ve her sayfayı imzalamalıdır.

Sorular ve cevaplar bir kayıt içine yazılamazsa, aşağıdaki bir sonraki sütuna yazmaya devam edin. Delil kayıt sütunu boyunca çapraz bir çizgi çizilmelidir.

KONUMDAKİ ESAS KİŞİDEN ALINACAK BİLGİLER

İsim			
Yaş		Doğum Tarihi	/ /
Uyruğu			
Adres			
Telefon			
Cep telefonu			
Unvanı/Mesleği			
Diğer Bilgiler			

Vaka ile ilgisi	☐ Tanık	☐ Şüpheli
İfadeye başlama zamanı	/ /	

EK NOTLAR

.....

.....

.....

.....

.....

.....

.....

GENEL

Olay yerindeki cihazlar:

Bağımsız bilgisayarlar ☐ adet

Taşınabilir (örneğin dizüstü) bilgisayarlar ☐ adet

Bir ağa bağlı bilgisayarlar ☐ İş istasyonları ☐ Sunucular

Diğer ☐

Soru: Bilgisayar sistemlerinin kullanımına kimler aşina?

☐ Ben

☐ .....

☐ .....

Soru: Sistem/ağ yönetimi ile kim ilgileniyor?

.....

.....

Soru: Bu cihazlarda hangi işletim sistemleri kurulu?

Adı, Sürümü .....

.....

(örneğin, PC: MSDOS, Windows, Unix, Linux, Mac OS; PDA: Palm OS, Psion EPOC, Windows CE)

SİSTEM / AĞ BİLGİLERİ

Soru: Sistem düzenli aralıklarla yedekleniyor mu? Cevap evet ise:

Yedekleme yazılımı .....

Yedekleme geri yükleme yazılımı .....

Soru: Burada bir ağ var mı? Cevap evet ise:

.....

Soru: Bir ağ planı var mı? (Yoksa, bir tane çizmelerini isteyin).

.....

Soru: Cihazda hangi ağ işletim sistemi/sistemleri kurulu?

Adı, Sürümü .....
.....

Soru: Ağ yönetimi ile kim ilgileniyor?

.....
.....

EK NOTLAR

.....
.....
.....
.....
.....
.....
.....
.....
.....

SİSTEM GÜVENLİK BİLGİLERİ

Soru: Bilgisayar yetkisiz erişime karşı korunuyor mu?

☐ EVET ☐ HAYIR

Soru: Ne tür bir koruma var?

BIOS Parolası: .....
Parola korumalı diğer özellikler: .....
Klavye kilidi: .....
Ekran kilidi: .....
Ekran koruyucu(lar): .....
Diğer yazılım korumaları: .....
Diğer yazılım korumaları: .....
Şifre için gizli soru ve cevap: .....

Soru: Cihazdaki yazılım ve/veya veriler yetkisiz erişime karşı korunuyor mu?

☐ EVET ☐ HAYIR

Program/dosya: .....
Parola: .....

Program/dosya: .....

Parola: .....

Program/dosya: .....

Parola: .....

Program/dosya: .....

Parola: .....

Diğer erişim cihazları (akıllı kartlar, teçhizat kilitleri, biyometrik tarayıcılar, belirteçler):

.....

.....

Soru: Bu sistem/cihaz için şifreleri/erişim kodlarını başka kim bilebilir?

.....

.....

EK NOTLAR

.....

.....

.....

.....

.....

.....

.....

.....

.....

.....

.....

.....

.....

.....

.....

.....

.....

İNTERNET BİLGİLERİ

Soru: İnternet erişiminiz var mı?

İnternet hizmet sağlayıcısı: .....

Oturum açma adı/kullanıcı adı: .....

Parola: .....

Şifre için gizli soru ve cevap

.....

.....

E-posta adresi: .....

POP/SMTP sunucusu: .....

Web alanı, Boş alan (sanal sürücü)

.....

.....

AĞA BAĞLANABİLEN DİĞER CİHAZLAR

.....

.....

.....

.....

.....

.....

.....

.....

.....

.....

.....

.....

.....

.....

.....

.....

.....

.....

.....

.....

İfadenin sona erme zamanı	/ / (Bitiş Zamanı)

İZİN/ONAY

1	Adınızı Yazın:	Kuruluş:
X KURUMU'nun (ve temsilcilerinin) soruşturmaları için gerekli tüm bilgisayar ekipmanlarını ve öğelerini almalarına izin/onay veriyorum.		
İmza:		Tarih/Saat: /
Kayıt No:		

2	Adınızı Yazın:	Kuruluş:
X KURUMU'nun (ve temsilcilerinin) soruşturmaları için gerekli tüm bilgisayar ekipmanlarını ve öğelerini almalarına izin/onay veriyorum.		
İmza:		Tarih/Saat: /
Kayıt No:		

3	Adınızı Yazın:	Kuruluş:
X KURUMU'nun (ve temsilcilerinin) soruşturmaları için gerekli tüm bilgisayar ekipmanlarını ve öğelerini almalarına izin/onay veriyorum.		
İmza:		Tarih/Saat: /
Kayıt No:		

4	Adınızı Yazın:	Kuruluş:
X KURUMU'nun (ve temsilcilerinin) soruşturmaları için gerekli tüm bilgisayar ekipmanlarını ve öğelerini almalarına izin/onay veriyorum.		
İmza:		Tarih/Saat: /
Kayıt No:		

OLAY YERİ NOTLARI

Notların alınmaya başlandığı zaman		Notların tamamlandığı zaman	
Notların alındığı yer			
Notları alan kişi			

.....

.....

.....

.....

.....

.....

.....

.....

OLAY YERİNDE BULUNAN KİŞİLER

1

İsim .....

Yaş ..... Doğum Tarihi .....

Adres .....

.....

Unvanı/Mesleği .....

Mevcut Zaman .....

Diğer Bilgiler .....

2

İsim .....

Yaş ..... Doğum Tarihi .....

Adres .....

.....

Unvanı/Mesleği .....

Mevcut Zaman .....

Diğer Bilgiler .....

3

İsim .....

Yaş ..... Doğum Tarihi .....

Adres .....

.....

Unvanı/Mesleği .....

Mevcut Zaman .....

Diğer Bilgiler .....

4

İsim .....

Yaş ..... Doğum Tarihi .....

Adres .....

.....

Unvanı/Mesleği .....

Mevcut Zaman .....

Diğer Bilgiler .....

5

İsim .....

Yaş ..... Doğum Tarihi .....

Adres .....

.....

Unvanı/Mesleği .....

Mevcut Zaman .....

Diğer Bilgiler .....

6

İsim .....

Yaş ..... Doğum Tarihi .....

Adres .....

.....

Unvanı/Mesleği .....

Mevcut Zaman .....

Diğer Bilgiler .....

7

İsim .....

Yaş ..... Doğum Tarihi .....

Adres .....

.....

Unvanı/Mesleği .....

Mevcut Zaman .....

Diğer Bilgiler .....

8

İsim .....

Yaş ..... Doğum Tarihi .....

Adres .....

.....

Unvanı/Mesleği .....

Mevcut Zaman .....

Diğer Bilgiler .....

ORADA BULUNAN KİŞİLER HAKKINDA İLGİLİ HERHANGİ BİR BİLGİ

Kayıt No.	Deliller	i. Nerede bulundu ii. Kim buldu	iii. Elkoyma zamanı iv. Delil Ref No.
		i. ii.	iii. iv.
		i. ii.	iii. iv.
		i. ii.	iii. iv.
		i. ii.	iii. iv.
		i. ii.	iii. iv.
Öğelere elkoyan kişilerin imzaları		…… …… ……	
Sorular ve cevaplar		**v.** Nerede mühürlendi **vi.** Kim mühürledi **vii.** Mühür No.	**viii.** Koyulduğu yer **ix.** Koyan kişi **x.** Diğer referans
		v. vi. vii.	viii. ix. x.
		v. vi. vii.	viii. ix. x.
		v. vi. vii.	viii. ix. x.
		v. vi. vii.	viii. ix. x.
		v. vi. vii.	viii. ix. x.
Doğru şekilde kaydedilmiş her cevabı parafladım.			
Sorgulanan kişilerin imzaları		…… …… ……	

ALINDI BÖLÜMÜ

Aşağıdaki Kayıt No. ile listelenen ..... (adet) öğe .....'den alındı.										
Kayıt No:										
Adınızı Yazın:						Kuruluş:				
İmza:						Tarih/Saat: /				

Aşağıdaki Kayıt No. ile listelenen ..... (adet) öğe .....'den alındı.										
Kayıt No:										
Adınızı Yazın:						Kuruluş:				
İmza:						Tarih/Saat: /				

Aşağıdaki Kayıt No. ile listelenen ..... (adet) öğe .....'den alındı.										
Kayıt No:										
Adınızı Yazın:						Kuruluş:				
İmza:						Tarih/Saat: /				

Aşağıdaki Kayıt No. ile listelenen ..... (adet) öğe .....'den alındı.										
Kayıt No:										
Adınızı Yazın:						Kuruluş:				
İmza:						Tarih/Saat: /				

Aşağıdaki Kayıt No. ile listelenen ..... (adet) öğe .....'den alındı.										
Kayıt No:										
Adınızı Yazın:						Kuruluş:				
İmza:						Tarih/Saat: /				

Aşağıdaki Kayıt No. ile listelenen ..... (adet) öğe .....'den alındı.										
Kayıt No:										
Adınızı Yazın:						Kuruluş:				
İmza:						Tarih/Saat: /				

Aşağıdaki Kayıt No. ile listelenen ..... (adet) öğe .....'den alındı.										
Kayıt No:										
Adınızı Yazın:						Kuruluş:				
İmza:						Tarih/Saat: /				

KROKİ PLANLAR

13.7 Ek G - Delil Muhafaza Anketi

SORUMLU ANKET

-GİZLİ-

Vaka Adı	
Sorumlu Adı	
Vaka Referans No	

KİŞİSEL BİLGİLER

Soyadı			
Adı		Başka Adları	
Şirket Adres			
Telefon			
Telefon			
Cep telefonu			
Birincil E-posta Adresi			
Ek E-posta Adres(ler)i			
Mevcut Pozisyon / Rütbe / Derece:			
Mevcut Pozisyon / Rütbe / Derece:			
Görev Süresi:			

İZİN/ONAY

İşbu belge ile (kurum adını yazın) (ve temsilcilerinin) soruşturmaları için gerekli tüm bilgisayar ekipmanlarını almalarına izin/onay veriyorum.	
İmza	Pozisyon
Adınızı Yazın	Tarih / Saat

BİLGİSAYAR BİLGİLERİ

Kişisel Bilgisayar Markası ve Modeli				
Seri numarası				
Aon Numarası				
Görüntü Depolama ortamı	EVET	HAYIR	Tamamlanma Tarihi	
Dizüstü Bilgisayar Markası ve Modeli				
Seri numarası				
Aon Numarası				
Görüntü Depolama ortamı	EVET	HAYIR	Tamamlanma Tarihi	
Ağ Dizinleri				
Hangi Alan Adına bağlısın				
Ağ Kimliğin nedir				
Ev Dizini				
Bir dosya paylaşımı üzerindeki Ana Dizine erişimin var mı?				
Cevap Evet ise – Ev Dizininin adı ne?				
Ev Dizinlerinin Anlık Görüntüsü	EVET	HAYIR	Tamamlanma Tarihi	
Paylaşılan Dizinler				
Bir Ağ Dosya Sunucusunda herhangi bir paylaşılan dizin veya alt klasör oluşturdun mu?				
Cevap Evet ise – İsimleri nelerdir?				
Paylaşılan Dizinlerin Anlık Görüntüsü	EVET	HAYIR	Tamamlanma Tarihi	
Eposta				
Geçerli Posta Kutusunun Anlık Görüntüsü	EVET	HAYIR	Tamamlanma Tarihi	

EK BİLGİLER

.....

.....

.....

.....

.....

.....

.....

.....

.....

.....

13.8 Ek H – Delil Etiket Şablonları

Funded by the European Union and the Council of Europe — EUROPEAN UNION — COUNCIL OF EUROPE — CONSEIL DE L'EUROPE — Implemented by the Council of Europe

Delil Referans No.	
CCR Kayıt No.	Diğer referans

Delilin tanımı: .....

.....

Kaynak: .....

.....

Tarih: ..... Saat: .....

BU DELİLİ TANIMLARIM

İmza: .....

Adınızı Yazın: .....

Ek tanık(lar)ın imzaları

Funded by the European Union and the Council of Europe — EUROPEAN UNION — COUNCIL OF EUROPE — CONSEIL DE L'EUROPE — Implemented by the Council of Europe

Delil Referans No.	
CCR Kayıt No.	Diğer referans

Delilin tanımı: .....

.....

Kaynak: .....

.....

Tarih: ..... Saat: .....

BU DELİLİ TANIMLARIM

İmza: .....

Adınızı Yazın: .....

Ek tanık(lar)ın imzaları

Funded by the European Union and the Council of Europe — EUROPEAN UNION — COUNCIL OF EUROPE — CONSEIL DE L'EUROPE — Implemented by the Council of Europe

Delil Referans No.	
CCR Kayıt No.	Diğer referans

Delilin tanımı: .....

.....

Kaynak: .....

.....

Tarih: ..... Saat: .....

BU DELİLİ TANIMLARIM

İmza: .....

Adınızı Yazın: .....

Ek tanık(lar)ın imzaları

Funded by the European Union and the Council of Europe — EUROPEAN UNION — COUNCIL OF EUROPE — CONSEIL DE L'EUROPE — Implemented by the Council of Europe

Delil Referans No.	
CCR Kayıt No.	Diğer referans

Delilin tanımı: .....

.....

Kaynak: .....

.....

Tarih: ..... Saat: .....

BU DELİLİ TANIMLARIM

İmza: .....

Adınızı Yazın: .....

Ek tanık(lar)ın imzaları

13.9 Ek I - Görüntü Alma Kaydı

VAKA BİLGİLERİ
Vaka No (1):
Proje / Konu Adı (2):
Sorumlu Adı (3):
Vaka Yöneticisi (5):

HEDEF BİLGİSAYAR BİLGİLERİ					
Sistemin Bulunduğu Yer (6):					
Sistem Türü (7):	☐ Masaüstü	☐ Dizüstü	☐ Sunucu	☐ Diğer:	
Delil Türü (8):	☐ Sabit Disk	☐ SSD	☐ Optik	☐ RAID	☐ Diğer:
Sistem Durumu (9):	☐ Açık	☐ Kapalı	☐ Oturum Açık	☐ Diğer:	
Sistem Tarihi / Saati (10):					
Geçerli Tarih / Saat (11):					
Toplam depolama ortamı sayısı (12):					
Depolama ortamını söken kişi (13):					
Fotoğraflar Çekildi (14):	☐ Evet	☐ Hayır - Sebep:			

İZİN/ONAY	
İşbu belge ile (kurum adını yazın) (ve temsilcilerinin) soruşturmaları için gerekli tüm bilgisayar ekipmanlarını almalarına izin/onay veriyorum.	
İmza	Pozisyon
Adınızı Yazın	Tarih / Saat

(xx) Sayfa 4'teki Yönlendirme Notlarına bakın

	BİLGİSAYAR	DEPOLAMA ORTAMLARI
Üretici	(15)	(18)
Model Numarası	(16)	(19)
Seri Numarası	(17)	(20)

(xx) Sayfa 4'teki Yönlendirme Notlarına bakın

GÖRÜNTÜ ALMA BİLGİLERİ

Alan kişi (21):			
Görüntü Alınan Yer (22):			
Görüntü Alma Yöntemi (23):	☐ Fiziksel Görüntü ☐ Klon	☐ Mantıksal ☐ Mantıksal Dosya	☐ Kısmi Görüntü ☐ Diğer:
Alma Tekniği (24):	☐ Donanım W/B ☐ Yazılım W/B	☐ Ağ ☐ Diğer:	☐ Adli önyükleme ortamı
Delil Ortamları (25):	☐ Sabit Disk / SSD	☐ Diğer:	
Seri Numarası (25):			
Delil Disk Sürücüsü Kimlik Numarası (25):			
Depolama Boyutu (26):	☐ TB	☐ GB *(birini belirtin)*	
Görüntü Boyutu (27):	☐ TB	☐ GB *(birini belirtin)*	
Görüntü Doğrulandı (28):	☐ Evet	☐ Hayır	
Hatalar (29):	☐ Evet	☐ Hayır	
Adres (Hash) Değeri (30):			

Görüntü Alma Kaydı Yönlendirme Notları

Bu bölüm, standart formda yer almayan ek notları eklemek veya alınan hata türleri, görüntü alma işlemi sırasında karşılaşılan sorunlar gibi notları genişletmek için kullanılabilir.

.....
.....
.....
.....
.....
.....
.....
.....
.....
.....
.....
.....
.....

Standart (kurum adını girin) Görüntü Alma Kaydı, bir sabit diskin veya diğer türdeki ortamların herhangi bir adli amaçla elde edilmesi (görüntüsünün alınması) sırasında kullanılacaktır.

VAKA BİLGİLERİ

1. **Proje Kimliği** - konu için tahsis edilen numarayı ifade eder.
2. **Konu Adı** - proje yöneticisi tarafından tahsis edilen "kod" adını ifade eder
3. **Sorumlu Adı** - bilgisayara atanan son kullanıcıyı ifade eder
4. **İzin/Onay** - makineyi almak için izin gerekiyorsa, makineyi teslim eden kişinin bir imzasını alın
5. **Yönetici** - vakayı yönetmek üzere atanan Proje Yöneticisini ifade eder

HEDEF BİLGİSAYAR BİLGİLERİ

6. **Sistemin Bulunduğu Yer** - olay yeri adresi, bilgisayar doğrudan bir ofisten alındıysa ofis numarasını içerebilir
7. **Sistem Türü** - makinenin masaüstü, dizüstü, sunucu vb. olduğunu gösterir. Cihaz bağımsız bir sürücü ise, 'diğer'i işaretleyin ve 'bağımsız sürücü' yazın
8. **Delil Türü** - görüntüsü alınacak/kopyalanacak cihazı işaretleyin
9. **Sistem Durumu** - şüpheli makinesinin açık, kapalı, oturum açmış vb. olduğunu belirtir. Makine açıksa, makineyi kimin kapattığını belirtin
10. **Sistem Tarihi/Saati** - şüpheli makinesindeki bios'u ifade eder
11. **Geçerli Tarih/Saat** - inceleme uzmanının bilgisayarındaki tarihi ve saati ifade eder
12. **Bilgisayardaki toplam sabit disk sayısı** - yeterince açıklayıcı
13. **Depolama Ortamını Söken Kişi** - bilgisayarı kimin söktüğünü belirtin
14. **Fotoğraflar Çekildi** - lütfen bilgisayarın ve sabit diskin fotoğraflarının çekilip çekilmediğini belirtin. Cevabınız hayır ise fotoğrafların neden çekilmediğini açıklamalısınız.

BİLGİSAYAR

15. **Hedef Bilgisayar Üreticisi** - makinenin türü ve sabit diskin boyutu
16. **Model Numarası** - bilgisayarın model numarası
17. **Seri Numarası** - bilgisayardan seri numarası. Makinede birden fazla seri numarası varsa, hepsini kopyalayın.

SABİT DİSK/DİĞER

18. **Üretici** - sabit disk türü
19. **Model Numarası** - sabit diskin model numarası
20. **Seri Numarası** - sabit diskin seri numarası. Birden fazla seri numarası varsa, hepsini kopyalayın

ALMA BİLGİLERİ (bu form, her görüntü için bir kez olmak üzere iki kez doldurulacaktır)

21. **Alan kişi** - cihazı fiziksel olarak teslim alan inceleme uzmanını ifade eder
22. **Görüntü Alınan Yer** – makinenin görüntüsünün yerinde mi, Laboratuarda mı alındığını belirtin - hangi laboratuar vb. belirtin.
23. **Görüntü Alma Yöntemi** - cihazın görüntüsünü almak için kullanılan yazılım türünü belirtir. Kullanılan yazılımın sürüm numarasını not edin.
24. **Alma tekniği** - bir yazma bloğu cihazı, çapraz kablolar, önyükleme diski vb. kullanıp kullanmadığınızı, alma türünü belirtin.
25. **Delil Ortamları** - görüntünün konulacağı sürücüyü ifade eder. Sürücü Markasını, seri numarasını ve Delil Disk Sürücüsü Kimlik Numarasını belirtin
26. **Depolama Boyutu** - TB veya GB cinsinden toplam sabit disk boyutu
27. **Görüntü Boyutu** - görüntünün toplam boyutunu belirtin (sabit diskin boyutunu DEĞİL), TB veya GB olarak belirtin
28. **Görüntü Doğrulandı** - görüntü tamamlandığında ve doğrulandığında EVET kutusunu işaretleyin
29. **Hatalar** - doğrulama işlemi sırasında herhangi bir hata bulunup bulunmadığını belirtin. Bulunduysa, belirli hataları kaydetmek için sayfanın arkasındaki "Notlar" bölümünü kullanın.
30. **Adres (Hash) Değeri**- görüntü alma işlemi sırasında üretilen adres değerini kaydedin. Alma sırasındaki adres değerinin ve doğrulama sırasındaki adres değeri ile aynı olduğundan emin olun.

Bu kılavuz Avrupa Birliği ve Avrupa Konseyi'nin finansal desteği ile hazırlanmıştır.
Burada ifade edilen görüşler hiçbir şekilde her iki tarafın da resmi görüşünü yansıtmamaktadır.

TUR

Avrupa Konseyi, Avrupa kıtasının önde gelen insan hakları kuruluşudur. Avrupa Birliği'ne üye devletlerin tamamı dâhil, kuruluşun 46 üyesi vardır. Avrupa Konseyine üye devletlerin tamamı insan hakları, demokrasi ve hukukun üstünlüğünü korumaya yönelik bir antlaşma olan Avrupa İnsan Hakları Sözleşmesi'ni imzalamıştır. Avrupa İnsan Hakları Mahkemesi, Sözleşme'nin üye devletlerdeki uygulamasını denetler.
www.europa.eu

Avrupa Birliği'ne üye devletler teknik bilgi birikimlerini, kaynaklarını ve kaderlerini bir araya getirmeye karar vermişlerdir. Hep birlikte kültürel çeşitliliği, hoşgörüyü ve bireysel özgürlükleri muhafaza ederken aynı anda bir istikrar, demokrasi ve sürdürülebilir kalkınma alanı inşa etmişlerdir. Avrupa Birliği, kazanımlarını ve değerlerini sınırları ötesindeki ülkeler ve haklarla paylaşmaya bağlılığını sürdürmektedir.
www.coe.int

Funded
by the European Union
and the Council of Europe

EUROPEAN UNION

COUNCIL OF EUROPE
CONSEIL DE L'EUROPE

Implemented
by the Council of Europe