Türkiye'deki Hâkim ve Savcılar için siber suçların soruşturulması ve kovuşturulması esnasında elektronik delillerin ele alınması çalıştayı

2. Oturum

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

Siber suçlarda fiziki ve elektronik delillerin toplanmasına ve işlenmesine ilişkin kurallar ve en iyi uygulamalar.

Ayrıca Avrupa Konseyi tarafından geliştirilen Standart Operasyon Prosedürü Kılavuzuna göre kolluk prosedürü ve en iyi uygulamalar.

Oturumun Hedefleri

Bu oturumun sonunda katılımcılar:

- Elektronik delil ilkelerini daha iyi anlayacak;
- Siber suçlarda fiziki ve elektronik delillerin toplanmasına ve işlenmesine ilişkin kurallar ve en iyi uygulamaları takdir edecek;
- Canlı deliller, ölüm sonrası edinilen deliller ve geleneksel deliller arasındaki farkı anlayacak;
- Avrupa Konseyi tarafından geliştirilen Standart Operasyon Prosedürlerine giriş eğitimi alacaktır.

Elektronik Delil İlkeleri

1. İlke

Veri Bütünlüğü

Yapılan hiçbir faaliyet daha sonra mahkemede delil olarak kullanılabilecek herhangi bir veriyi, elektronik cihazı veya ortamı önemli ölçüde değiştirmemelidir.

2. İlke

Denetim İzi

Elektronik deliller ele alınırken yapılan tüm faaliyetlerin bir kaydı oluşturulmalı ve daha sonra denetlenebilmek üzere saklanmalıdır. Bağımsız bir üçüncü taraf sadece bu faaliyetleri tekrarlayabilmekle kalmayıp aynı zamanda aynı sonucu elde edebilmelidir.

3. İlke

Uzman Desteği

Planlanan bir operasyon esnasında elektronik delil bulunması bekleniyorsa operasyondan sorumlu kişi uzmanlara/dış danışmanlara zamanında haber vermeli ve mümkünse hazır bulunmalarını sağlamalıdır.

4. İlke

Uygun Eğitim

Elektronik delilleri ele alan kişiler gerekli ve uygun eğitime sahip olmalıdır.

5. İlke

Yasallık

Davadan sorumlu kişi ve kurumlar, kanunlara, delillere ilişkin güvencelere ve genel adli ve usuli ilkelere harfiyen uyulmasını sağlamakla yükümlüdür.

Toplama için Hazırlık

Toplama için Hazırlık

- Suç mahallinin türü (ticari/özel)
- Olay yeri (yargı yetkisi)
- Aramada gerekli kişi sayısı
- İstihbarattan edinilen şüpheliler
- Aranacak delil türleri
- Prosedürler/politikalar/belgeler
- Soruşturma konusu olan suç

Ekibi bilgilendirme

- Ekip üyelerinin seçilmesi (gerekirse dış uzmanlar dâhil);
- Ekip üyelerine bireysel görevler atanması;
- Ekip üyelerinin görevlerinin yerine getirilmesi konusunda bilgilendirilmesi (ilgili temel eğitimi geçmiş olmaları gerekir);
- Gerekli el koyma araç ve gereçlerinin temin edilmesi.

Gerekli aletler

Sökme ve çıkarma aletleri:

- Tornavidalar (düz başlı ve yıldız başlı ve üreticiye özel (örn. Hewlett Packard, Apple));
- Anahtarlar (altıgen somun, yıldız tipi somun ve emniyetli uç);
- Penseler (standart ve kargaburun);
- Tel kesiciler (kablo bağlarının sökülmesi için);
- Küçük cımbızlar;

Belgelendirme

- Arama ve el koyma kaydı (mal-mülk)
- Etiketler ve teyp (kablolar ve prizler dâhil olmak üzere sistemin bileşen parçalarını işaretlemek ve tanımlamak için);
- Kablo etiketleri; Delil etiketleri (asmalı ve yapıştırmalı);
- Suç mahallinde görevi tamamlamak için gerekli diğer formlar ve belgeler
- Fotoğraf makinesi ve/veya video kamerası (suç mahallini ve ekrandaki görüntüleri fotoğraflamak için)

Ambalaj ve taşıma malzemeleri:

- Antistatik poşetler (devre kartları gibi sökülen ekipmanların korunması için).
- Faraday torbaları
- Kablo bağları (kabloları sabitlemek için);
- Delil torbaları, teyp, etiketler;
- USB cihazları, DVD veya CD'ler gibi harici depolama ortamlarını ambalajlamak için kutular.

Diğer kalemler:

- Braketli küçük meşale;
- Eldivenler;
- Büyüteç;
- Tüm standart adli bilişim araçlarının yüklü olduğu bir dizüstü bilgisayar;
- WiFi tarayıcısı (WiFi ağlarını ve cihazlarını ortaya çıkarmak ve belgelemek için);
- Yeterli sabit disk kapasitesi (örneğin birkaç terabaytlık harici ve sabit disk sürücüleri);
- Donanım yazma engelleyiciler (yerinde görüntüleme ve triyajlama amaçlı);
- Adli bilişim önyükleme DVD'leri (eğitimli görevliler tarafından kullanılmak üzere);
- Canlı veri inceleme araçları (eğitimli görevliler tarafından kullanılmak üzere);

Suç mahallinin güvenliğinin sağlanması

Elektronik delilleri içeren bir suç mahallinde hangi önemli tedbirler alınmalıdır?

Suç mahallinin güvenliğinin sağlanması

Suç mahallinin güvenliğini sağlamak amacıyla kendi yetki alanınızdaki standart politika ve prosedürü izleyin:

- Cihazları tanımlayın;
- Şüphelinin erişimini yasaklayın;
- Suç mahallini belgeleyin;
- Koruyucu eldivenler kullanın;
- Cihazların çalışıp çalışmadığını kontrol edin;
- Şifreleri elde edin.

Delillerin Tespit Edilmesi

- Bilgisayarlar, telefonlar, sunucular
- Depolama aygıtları, hafıza kartları, harici sabit diskler
- Fotoğraf makinaları, video kameraları, CCTV
- USB cihazları, flaş sürücüler
- CD, DVD, Blue-ray
- Yönlendiriciler
- Nesnelerin interneti
- Dijital olmayan deliller, yazılı şifreler, belgeler, parmak izleri, DNA vb.

Suç mahallindeki elektronik deliller

- Açık olan bilgisayarlar (canlı inceleme)
- Kapatılmış bilgisayarlar (post mortem inceleme)
- İş açısından kritik makineler (canlı inceleme)
- Nesnelerin interneti (canlı inceleme)
- Mobil cihazlar (ağ bağlantısını kaldırın)

Canlı inceleme ve post mortem inceleme

Uçucu veriler için örnekler:

- Önbellekler (ör. arp ve dns önbellekleri)
- Kaydedilmemiş belgeler
- Devam eden işlemler
- Şifreler ve **şifreleme anahtarları**
- Açık ağ bağlantıları
- Sistem bilgisi
- Giriş yapan kullanıcılar
- Geçici olarak bağlı uzaktan depolama
- Kötü amaçlı yazılım ikili dosyaları yalnızca RAM'de saklanır

Canlı inceleme ve ölüm sonrası inceleme

İki tür uçucu veri mevcuttur

- **Fiziki bilgisayardaki uçucu veriler**: açık ağ bağlantıları, devam eden işlemler ve hizmetler, arp ve dns önbellekleri.
- **Geçici veriler**: doğası gereği uçucu olmayan ancak yalnızca suç mahallinde erişilebilen veriler. Şifrelenmiş birimler ve uzak kaynaklar bu tür verilere örnektir. Soruşturma görevlisinin bu verileri elde edememesi durumunda arama sonrasında verilerin içeriği erişilemez hâle gelebilir, değiştirilebilir veya silinebilir.

Canlı inceleme

Canlı inceleme yalnızca aşağıdaki kriterleri karşılayan araçları kullanan uzmanlar tarafından gerçekleştirilmelidir:

- Yalnızca sistem üzerinde en az etkiye sahip araçları seçin.
- Araç, kendi yürütülebilir dosyası ve kitaplıkları ile birlikte gelmelidir.
- Yalnızca işlevselliğini mahkemede açıklayabileceğiniz araçları ve komut dosyalarını kullanın.
- Araç/komut dosyası otomatikleştirilmelidir.
- Acil durumlar veya güvenlik olayları için triyaj işlevini göz önünde bulundurun.
- Araç yalnızca uçucu olan verileri toplamalıdır.

Delil Zinciri

CHAIN OF CUSTODY

Received from: .....

Received by: .....

Date: ..... Time: ..... am/pm

Received from: .....

Received by: .....

Date: ..... Time: ..... am/pm

Received from: .....

Received by: .....

Date: ..... Time: ..... am/pm

Received from: .....

Received by: .....

Date: ..... Time: ..... am/pm

El Koyma

- El koyan kişi
- İlgili kurum
- Saat ve tarih
- Yer
- Delil referansı (ALB/01)
- Vaka referansı (R ve Badboy)
- İmza
- Nesnenin tarifi (seri numarası dâhil)

İnceleme

- Emniyet belirteçli bant
- İnceleme görevlisi tarafından imzalanır
- Saat ve tarih
- Açıklama ve inceleme notlarına uygun olmalıdır

Elektronik delillerin toplanması, analizi ve korunması için Standart Operasyon Prosedürleri

İçindekiler

4. Bilgisayar sistemlerinin, bilgisayar verilerinin ve dijital cihazlar ile mobil cihazların adli analizi.

5. Bulguların sunumu – rapor hazırlama

6. Ekler

   - Teknik terimler sözlüğü
   - Rapor şablonları

Verilerin işlenmesi

- Mevcut bilgisayarların/cihazların depolama kapasitesi 1 TB'nin üzerinde olacaktır.
- İşlenecek büyük miktarda veri
- Adli araçlar bu sürece yardımcı olur
- Soruşturmaların hedefe yönelik olması gerekir.
- Anahtar kelime aramaları, hedefe yönelik bir soruşturmaya yardımcı olur
- Farklı suçların farklı delil verileri olacaktır.

Çevrim İçi Çocuk Cinsel İstismarı ve Sömürüsü (OCSEA)

Dijital

- Resimler, videolar,
- Üst veriler
- İnternet etkinliği,
- Silinen veriler,
- Sohbet günlükleri
- Sosyal medya,
- IP adresleri,
- FTP kullanımı vb.

Fiziki

- Basılı kopya
- Şifreler
- Seks oyuncakları
- DNA
- Parmak izleri
- Sağlık kontrolleri vb.

Fidye yazılımı

Dijital

- Kaynak kodu
- Darknet etkinliği,
- Silinen veriler,
- Sohbet günlükleri
- IP adresleri,
- Kripto cüzdanları,
- Şifreleme,
- Sistem günlükleri vb.

Fiziki

- Yazılı kopya
- Şifreler
- Nakit para
- Banka hesabı hareketi
- Suçtan elde edilen gelirler

Oturum Değerlendirmesi

Bu oturumun sonunda katılımcılar:

- Elektronik delil ilkelerini daha iyi anlayacak;
- Siber suçlarda fiziki ve elektronik delillerin toplanmasına ve işlenmesine ilişkin kurallar ve en iyi uygulamaları takdir edecek;
- Canlı deliller, ölüm sonrası edinilen deliller ve geleneksel deliller arasındaki farkı anlayacak;
- Avrupa Konseyi tarafından geliştirilen Standart Operasyon Prosedürlerine giriş eğitimi alacaktır.

Sorunuz var mı?