EMNİYET GENEL MÜDÜRLÜĞÜ
SİBER SUÇLARLA MÜCADELE DAİRE BAŞKANLIĞI
Furkan YILMAZ*

***Başkomiser, Adli Bilişim Uzmanı, Adli Bilişim Doktora Adayı**

SUNUM PLANI

- Siber Suçlarla Mücadele Daire Başkanlığına Genel Bakış
- Adli Bilişim Birimi
- Adli Bilişimin Zorlukları
- EGM'de Delil Zinciri
- En İyi Senaryo

Genel Bakış: SSMDB

Soruşturmalar
İstihbarat
Elektronik Deliller

2 binden fazla
polis memuru

Genel Merkez
ANKARA

Genel Merkez
ve 17 Yerel
Adli bilişim
laboratuvarı

81
İl emniyet müdürlüğü
Siber suçlarla mücadele birimi

~2.000.000
Dijital materyal son üç yılda incelendi

~800
Adli bilişim
personeli

Emniyet Genel Müdürlüğü (EGM) Siber Suçlarla Mücadele Daire Başkanlığı (SSMDB), özellikle aşağıdakiler olmak üzere çok çeşitli emniyet görevini yerine getirir:

Siber suçların soruşturulması:

- Bilişim ve ağ suçları,
- Bilişim ve ağ sistemi kullanılarak işlenen suçlar,
- Çocuk istismarı,
- İnternet üzerinden yasa dışı bahis ve kumar oynama

Siber suçlar konusunda farkındalık yaratmak;

Siber suçların gözetimi;

Açık kaynak istihbaratı;

Adli bilişim:

- İlk müdahale,
- İnceleme ve analiz,
- Verilerin kurtarılması,
- Mobil cihazlarda adli bilişim,
- Kötü amaçlı yazılım analizi,
- Kriptoanaliz,
- Adli bilişim ile ilgili koordinasyon, strateji ve eğitim.

Kanunlar, yönetmelikler ve hükümet tasarrufları ile verilen adli görevler gibi idari görevlerin yerine getirilmesi;

ADLİ BİLİŞİM BİRİMİ

Birimin Görevleri

- Dijital Delillere İlk Müdahale
- Dijital Delil Zinciri
- Delillerin Adli Görüntüsünü Elde Etme
- Veri Kurtarma
- Kripto Analizi
- Kötü Amaçlı Yazılım Analizi
- Dijital Delilleri Raporlama

Dijital Delillere İlk Müdahale ve İnceleme Öncesi Dijital Delillerin Hazırlanması

- Veri işleyen ve/veya saklayan her türlü dijital materyale ilk müdahale operasyonlarını yürütmek ve bu delillerin koruma, arama emri ve el koyma süreçlerine teknik destek sağlamak;
- Dijital Delilleri Görüntülemek;
- İnceleme ve Raporlama Süreçlerinden Önce Dijital Delilleri Hazırlamak;
- Elde edilen görüntüleri incelenmesi için adli bilişim uzmanlarına teslim etmek;
- İncelenmiş ve Belgelenmiş dijital delilleri İnceleme Raporları ile Müfettişlere teslim etmek;
- Dijital Delillere ilişkin verileri (Delillerin ne zaman Daire Başkanlığımıza ulaştığı, kimin dijital delillerinin teslim edildiği vs.) Kaydetmek ve Arşivlemek (Şüpheliler hakkında herhangi bir kişisel veri içermez)
- Delil zincirine sıkı bir şekilde uyulur.

Delil Koruma Kutusu ve Çantası

Dijital Delillerin İncelenmesi

- Dijital delilleri incelemek;
- Dijital delillerden elde edilen dijital bulguları raporlamak;
- Yazılım kullanarak silinen verileri kurtarmak;
- Dijital cihazlardan dijital bulguları çıkarmak.
- Gerekirse ön inceleme sonrası ön inceleme raporunu hazırlamak.

Mobil Cihazlarda Adli Bilişim

- Bir mobil cihazdan dijital delilleri veya ilgili verileri kurtarmak;
- Bir mobil cihaz arızalıysa ve görüntülemeye ve incelemeye uygun değilse tamir edebiliriz;
- Özel (Chip-off, J-Tag, internet servis sağlayıcısı gibi) veri kurtarma yolları kullanılarak hasarlı mobil cihazlardan deliller elde etmek;
- Analiz ve raporlama veri bellekleri manyetik şeritlidir.

Kötü Amaçlı Yazılım Analizi

- Bir soruşturma kapsamında kötü amaçlı yazılımın faaliyetlerini analiz etmek ve tespit etmek, ardından şüpheli IP ve alan adını tespit etmek;
- Bilgisayar günlüklerini analiz ederek yasa dışı uzaktan erişimi tespit etmek;
- İnternet sayfalarına siber saldırı gerçekleştiren web günlüklerini analiz etmek;
- İstismar ve yük saldırıları gerçekleştiren bir şüpheliyi tespit etmek için RAM'i analiz etmek;
- Kötü Amaçlı Yazılım Analiz Laboratuvarı'nın (KAYAL) kurulumu devam ediyor.

Kripto Analizi

- Şifrelenmiş dosyaları ve disk şifrelemelerini analiz ederek şifreleme türünü algılamak;
- Sözlük saldırısına yönelik olarak her şüpheli için kelime listesi hazırlamak;
- Kompakt, sıvı soğutmalı donanımlı sunucu sistemleri kullanmak.

Veri Kurtarma

- Arızalı sabit sürücüleri ve NAND flash belleklerini onarmak;
- Teknik müdahale sonucunda erişilebilen verilerin adli kopyalarını almak.
-

ZORLUKLAR

- Çok fazla dijital materyal (Darbe girişimi nedeniyle)

TOPLAM: +2,1 Milyon

Soruşturma kapsamında incelenen ve rapor edilen: ~2,5 Milyon

Geriye kalan: 90 Bin

- Hukuki usuller
- Şifreleme (Sql şifresi, tam disk, TrueCrypt, OS in OS, dosya şifreleme vb.)
- Bulut bilişim
- İmha edilmeye çalışılan materyaller (hasar, su...)
- 81 İl Birimi

DELİL ZİNCİRİ

- Tüm sürecin belgelendirilmesi
- Uluslararası Standartlar (ISO vb.)
- Antistatik delil torbaları
- Mühürlü delil torbalarının açılması sırasında video kaydı
- Delil odasında saklama

DELİL ZİNCİRİ

Olay Yerine Ulaşmadan Önce:

- Hukuki hususların kontrolü,
- Duruma göre hazırlanma (sunucu, kötü amaçlı yazılım vb.),
- Güvenlik önlemlerinin alınması.

DELİL ZİNCİRİ

HUKUKİ KONULAR

- Kontrol listesi
  - Hâkim/Savcı kararı
  - Sadece el mi koyulacak yoksa bilgisayarlar da aranacak mı?
  - Adres/Özel adres (Şirket, Askerlik, Avukatlık Bürosu)
  - Şüpheliler/Özel şüpheliler (Avukat, Mağdur)

DELİL ZİNCİRİ

ÇALIŞMA KİTİ

- TD cihazları, kablolar ve adaptörler
- SATA, IDE veri kabloları
- Tableau ultra blok SATA, IDE, SCSI, USB Köprüleri ve Protokolleri
- SD/micro SD kart okuyucular ve adaptörler
- Kullanılmamış veya silinmiş boş sabit disk sürücüsü ve yeterli sayıda CD/DVD.
- FTK Imager yüklü bir flash bellek
- Deft zero yüklü bir flash bellek
- Helix yüklü bir flash bellek
- Sabit disk sürücüsü yerleştirme istasyonu
- Çeşitli boyutlarda delil torbaları
- Tek taraflı yapışkan etiket, A4 kağıt, mavi tükenmez kalem ve koli bandı
- Klavye ve Fare
- Tornavida takımı
- Laboratuvar eldivenleri
- Dizüstü bilgisayar
- Taşınabilir yazıcı

*Her cihaz çalıştırılmadan önce kontrol edilmelidir.

DELİL ZİNCİRİ

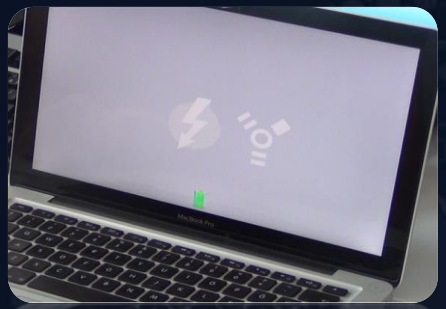
İlk müdahale sırasında:

- Adres ve şüphelilerin kontrolü.
- Geniş ve farklı açılardan fotoğrafların çekilmesi.
- Arama ve el koyma sırasında video kaydı.
- Tespit edilen tüm delilller kağıda geçirilir:
  - Tür, marka ve model
  - Seri numarası veya imei
  - Delilin kime ait olduğu, nerede bulunduğu
  - Delilin herhangi bir özelliği (hasar, renk vb.)
  - Delil başka bir depolama içeriyorsa, yukarıda yer alan bilgileri
- Dijital delilller, benzersiz numaralı delil torbaları ile mühürlenir.
- Dava ile ilgili her türlü fiziki delile el koyulur.
- Biyolojik veya parmak izi analizi gerekiyorsa buna yönelik önlemler alınır.

DELİL ZİNCİRİ

İlk müdahale sırasında:

- Suç mahallinde adli görüntü elde edilmişse, yöntem ve karma değerleri kağıda geçirilir.
- Yöntemler şunlar olabilir:
  - Çoğaltıcı (TD) ile deadbox adli görüntüleme
  - Yerleşik bellek aygıtı (taşınabilir yazılım kullanılarak veya hedef modunda)
  - Canlı elde etme (RAM ve Çalıştırma sistemleri, taşınabilir yazılım ve gerekirse NAS Sunucusu kullanılarak)



**Hedef modu*

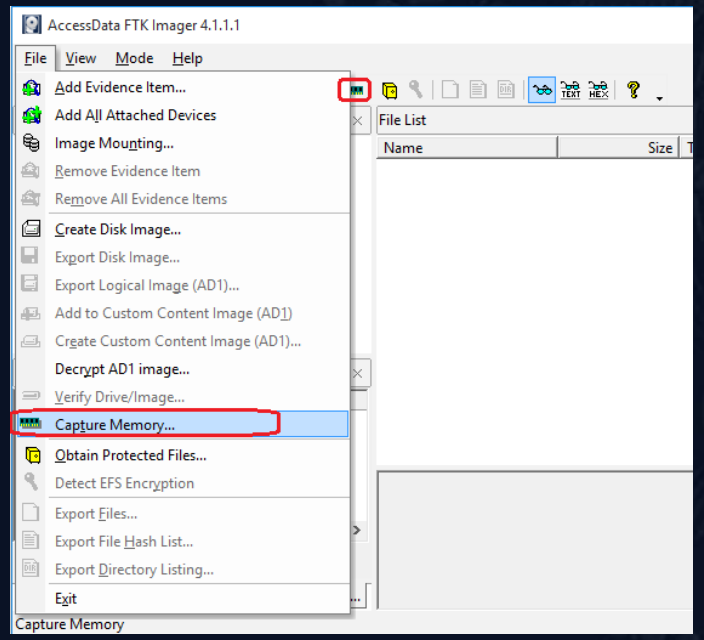
**Deft kullanımı*

**TD Aygıtının kullanımı*

DELİL ZİNCİRİ

İlk müdahale sırasında:

- Delil yürütülürken:
  - Saat, saat dilimi ve çalışan uygulamaları tespit etmek
  - Uçucu verileri yakalamak
- Mobil cihaz:
  - Uçuş modu,
  - Telefon sinyal kesici,
  - Faraday çantası.



DELİL ZİNCİRİ

Laboratuvar işlemleri sırasında:

- Kağıt kontrolü
- Video kaydı yaparak mührü açma
- Delilin sisteme girilmesi
- Delillerin sınıflandırılması (aciliyet, gereken uzmanlık vb.)
- Delillerin delil odasında saklanması
- Görüntü alma
- İnceleme
- Raporlama
- Delillerin mühürlenmesi
- Soruşturma birimine veya mahkemeye gönderilmek üzere hazırlama.

Delil odası

- Bu odaya sadece yetkili personel girebilir.
- Toz ve fiziksel hasara karşı önlemler alınır.
- Deliller önceliklerine ve konularına göre sınıflandırılır (ör. Kripto, Kötü Amaçlı Yazılım ve Mobil Cihazlar vb.).

EN İYİ SENARYO

12 Ocak 2016'da İstanbul'un Fatih ilçesindeki Sultanahmet Meydanı'nda gerçekleştirilen Ocak 2016 İstanbul saldırıları veya 2016 Sultanahmet Camii saldırısı kapsamında DEAŞ militanı Suriye doğumlu 28 yaşındaki Nabil Fadl, turist konvoyunun arasına girerek bombalı intihar saldırısı gerçekleştirdi.

BBC Sign in News Sport Reel Worklife

NEWS

Home Video World UK Business Tech Science Stories Entertainment & Art

World Africa Asia Australia Europe Latin America Middle East US & Canada

Turkey: 'IS suicide bomber' kills 10 in Istanbul Sultanahmet district

12 January 2016 Share

Mark Lowen reports from Istanbul where the attack took place

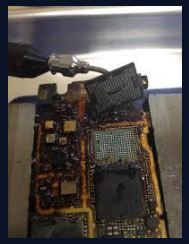
A suspected member of the Islamic State (IS) group has killed 10 people, at least eight of them German tourists, in a suicide bomb attack in the Turkish city of Istanbul, officials say.

They say the Syrian national carried out the attack in the Sultanahmet district, near famous Blue Mosque.

people were wounded, many of them also German.

EN İYİ SENARYO

- **Sultanahmet bombacısının parçalanmış tabletinden veriler kurtarıldı.**
- Verilerde şifreli terör örgütü talimatları ve İstanbul'daki olası başka bir saldırının hedef noktalarının görüntüleri tespit edildi.



Bu durumda chip-off yöntemi aracılığıyla verilere ulaştık. Bu yöntem kullanılarak veri çip kartı çıkarıldı ve veriler ikili düzeyde okundu.

AKSAM · Irak güçlerinin, göstericilere karşı müdahale.

30 Ocak 2016 Cumartesi 09:31 | Son Güncelleme: 30 Ocak 2016 Cumartesi 09:31

Bu 6 noktaya dikkat: Canlı bomba keşif yapmış!

Sultanahmet bombacısına ait kırık tabletin hafıza kartında, keşif sırasında çektiği fotoğraflara ulaşıldı.

Sultanahmet bombacısı Suudi Arabistan uyruklu, terör örgütü DAEŞ üyesi Nabil Fadlı'nın saldırıya nasıl hazırlandığına dair detaylar ortaya çıktı.

Fadlı'nın ikâmet ettiği evde yapılan aramada bulunan kırık tabletin hafıza kartında, keşif sırasında çektiği fotoğraflara ulaşıldı.

bacının Sultanahmet Meydanı'nın yanı sıra Ayasofya Camii, Taksim Meydanı, Topkapı Galata Kulesi, Yerebatan

iliselerde keşif yaptığını tespit eden polis, olası yeni saldırılara karşı önlemleri

İLGİNİZ İÇİN TEŞEKKÜRLER!