BÖLÜM 1: BİLİŞİM SUÇLARI

1.1 Temel Tanımlar

1.2 Anatomi

1.3 Örnekler

1.4 Bilişim Suçları Kategorizasyonu

1.5 TCK ve Bilişim Suçları

1.1 Bilişim Suçu

Tanım:

Bilgileri otomatik işleme tabi tutan veya verilerin nakline yarayan bir sistemle; gayri kanuni, gayri ahlaki veya yetki dışı gerçekleştirilen her türlü davranış.

AET Uzmanlar Komisyonu

Mayıs 1983 Paris

1.1 Bilişim Suçu

Tanım:

Verilerin bilişim temelli olarak ve otomatik şekilde işlenmesi, saklanması, tasnif edilmesi, terkibi, ve iletilmesi ile ilgili ve bilişim alanı içinde işlenen, bir bilgisayar ya da ağına yönelik olarak ya da onları kullanarak icra edilen her türlü yasadışı haksız eylem.

Levent KURT

Hakim

2005

1.2 Bilişim Suçunun Anatomisi

Temel Nitelikler:

- Suçun işlenmesi-belirlenmesi arasındaki ters oran.
- "White-collar crime".
- Suçun dört boyuttan bağımsız olması.
- Suçun rapor edilmeyişi.
- Delil elde etme güçlüğü.
- Bilişimdeki dinamizm, suç-ceza tanımı, tedbir ve kanunların sürekli değişmesi gerekliliği.

1.3 Bazı Bilişim Suçu Örnekleri

- Çöp toplama
- Dinleme-Kocakulak
- Truvavatı-Virüs-Solucan ve kombinasyonları
- Salam dilimleme, Tuzak kapılar
- Spam e-posta, Web yönlendirme, IP-ARP-DNS Protokol Aldatmacaları (IP Spoofing)
- Ağ koklayıcılar (snifers)
- Oltalama-Phishing
- Casus yazılımlar, şifre kırıcılar
- Mantık bombaları
- Zaafiyet tarayıcıları
- Sosyal Mühendislik.

1.4 Bilişim Suçları Kategorizasyonu

Amerika Birleşik Devletleri Sınıflaması

1. Mülkiyete karşı hırsızlıklar
2. Veri veya hizmetlere karşı hırsızlıklar
3. Giriş ihlali
4. Veri sahtekarlığı
5. İnsan hatasından kaynaklanan ihlaller
6. Gasp
7. Sır aleyhine ihlaller
8. Sabotajlar
9. Maddi kısımlara yönelik hırsızlıklar
10. Evrak sahtekarlığı
11. ATM hırsızlıkları
12. Manyetik kart PIN hırsızlıkları

1.4 Bilişim Suçları Kategorizasyonu

Birleşmiş Milletler Sınıflaması

1. Bilgisayar sistem veya ağlarına izinsiz giriş.
2. Hak sahibinin rızası olmadan bilgisayar veri ve programlarına zarar vermek, silmek, bozmak, tahrip etmek ve elde etmek.
3. Bilgisayarın işlemesini veya telekomünikasyon sistemini engellemek amacıyla bilgisayar veri ve sistemlerini tahrip etmek, veri yüklemek, değiştirmek, silmek veya elde etmek.
4. Hukuk dışı olarak iletişime müdahale etmek.
5. Menfaat temin edebilmek için ticari sırları izin almadan veya hukuken bir hak olmaksızın ifşa etmek veya tevzii etmek veya kullanmak.

1.4 Bilişim Suçları Kategorizasyonu

Avrupa Topluluğu Siber Suç Sınıflaması, Temmuz 2001 (European Convention on Cyber Crime, June 2001)

1. Bir kaynağın veya herhangi bir değerin hukuka aykırı olarak transferini sağlamak için kasten bilgisayar verilerine ve/veya programlarına girmek, bozmak, silmek ve/veya yok etmek.
2. Sahtekarlık yapabilmek için kasten bilgisayar verilerine ve/veya programlarına girmek, bozmak, silmek ve/veya yok etmek.
3. Bilgisayar ve/veya telekomünikasyon sistemlerinin çalışmasını engellemek amacıyla kasten bilgisayar verilerine ve/veya programlarına yahut bir bilgisayar sistemiyle bağlantı sağlayan mekanizmaya girmek, bozmak, silmek ve/veya yok etmek.

1.4 Bilişim Suçları Kategorizasyonu

Avrupa Topluluğu Siber Suç Sınıflaması, Temmuz 2001 (European Convention on Cyber Crime, June 2001)

4. Piyasaya sürmek ve ticari olarak yararlanmak amacıyla bir bilgisayar programının yasal malikinin sahip olduğu hakları zarara uğratmak.
5. Bir bilgisayar ve/veya telekomünikasyon sistemi sorumlusunun izni olmaksızın veya mevcut emniyet tedbirlerini aşarak bu sistemlere kasten girmek veya müdahalede bulunmak.

1.5 TCK – 5237 SK Bilişim Suçları

- **TCK (Bilişim Suçları)**
  - ✓ **MADDE 243** – Yekisiz Erişim – Sisteme Girme
  - ✓ **MADDE 244** – Hacking, Verileri Engelleme, Bozma, Değiştirme, Yok etme.
  - ✓ **MADDE 245** – Kredi Kartı ve Banka'ya karşı işlenen suçlar.
  - ✓ **MADDE 246** - Tüzel kişiler hakkındaki tedbirler

- **TCK (Bilişim Vasıtalı Suçlar)**
  - ✓ **MADDE 124** – Haberleşmenin engellenmesi
  - ✓ **MADDE 125** – Hakaret
  - ✓ **MADDE 132** – Haberleşmenin Gizliliğini İhlal.
  - ✓ **MADDE 133** – Kişiler arası konuşmaların dinlenmesi ve kayda alınması.
  - ✓ **MADDE 135** – Kişisel verilerin kaydedilmesi.
  - ✓ **MADDE 136** – Verileri hukuka aykırı olarak verme veya ele geçirme.
  - ✓ **MADDE 138** – Verileri hukuka aykırı olarak verme veya ele geçirme.
  - ✓ **MADDE 142** – Nitelikli Hırsızlık.
  - ✓ **MADDE 158** – Nitelikli Dolandırıcılık.
  - ✓ **MADDE 226** – Müstehcenlik.

1.5 Diğer Kanunlar

- **Ceza Muhakemesi Kanunu**
  - ✓ **MADDE 134** – Bilgisayarlarda, bilgisayar programlarında ve kütüklerinde arama, kopyalama ve elkoyma

    Bilgisayarda Arama (CMK 134-1)
    Kopya Çıkarma (CMK 134-1)
    Çözümleme (CMK 134-1)
    El Koyma (CMK 134-2)
    Yedekleme (CMK 134-3)
    Kopya Verme (CMK 134-4).

1.5 “Internet Kanunu”

Resmî Gazete
Tarih:23 Mayıs 2007 ÇARŞAMBA
Sayı : 26530

Kanun No. 5651 **Kabul Tarihi : 4/5/2007**

Internet Ortamında Yapılan Yayınların Düzenlenmesi ve Bu Yayınlar Yoluyla İşlenen Suçlarla Mücadele Edilmesi Hakkında Kanun

BÖLÜM 2: ADLİ BİLİŞİME GİRİŞ

2.1 Temel Tanımlar

2.2 Adli Bilişimde Delil Kavramı ya da Sayısal (=elektronik) Delil

2.3 Sayısal Delillerin Bilişim Sistemi İçindeki Konumları

2.4 Sayısal Delil - Kağıt Ortamda Delil

DO NOT CROSS CRIME SCENE DO NOT CROSS CRIME SCENE DO NOT CROSS CRIME SCENE

2.1 Adli Bilişim

Tanım:

Adli Bilişim; elektromanyetik-elektrooptik ortam(lar)da muhafaza edilen ve/veya bu ortamlarca iletilen; ses, görüntü, veri/bilgi veya bunların birleşiminden oluşan her türlü bilişim nesnesinin, mahkemede **sayısal (elektronik-dijital) delil** niteliği taşıyacak şekilde:

- Tanımlanması,
- elde edilmesi,
- saklanması,
- incelenmesi ve
- mahkemeye sunulması

çalışmaları bütünüdür.

2.1 Adli Bilişim

Tanım:

Adli Bilişim; olay yeri incelemesi veya bir kurban üzerinde yapılan otopsinin eşdeğeridir.

"Computer forensics is the equivalent of surveying a crime scene or performing an autopsy on a victim"

James Barek, 2001

2.2 Sayısal (=Elektronik) Delil: TANIM

Akla, maddi gerçeğe ve hukuka uygun olmak gerekliliklerini sağlamanın yanı sıra; suça delil niteliği taşıyan ve

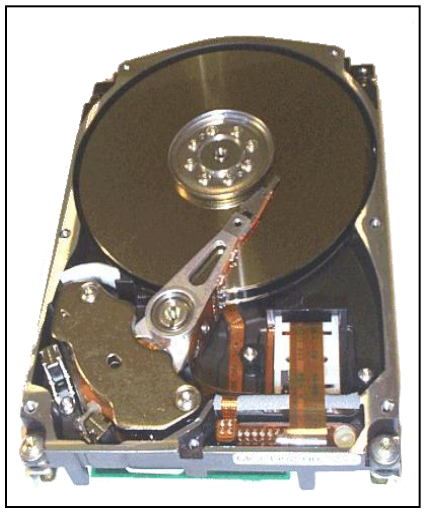
- **Yasal şekilde edinilmiş,**
- **Özgün,**
- **Doğrulanabilir,**
- **Yeterli derecede ikna edici,**
- **Konuyla ilgili ve**
- **Mahkemeye sunulabilecek şekilde olmak üzere;**

dijital ses, görüntü, veri ve/veya programları saklayabilen – işleyebilen; elektronik, elektromanyetik, elektrooptik yapılı; disk, disket, CD, DVD, cep telefonu, PDA cihazları, flash bellek, SIM-SD-MMC kartlar, bilgisayar ve bilgisayara ait dahili veya harici donanımlar, basım, iletim ve ağ aktif cihazları ve bunların yazılımları ve benzeri elektronik cihazların tümü ve bu sayılan ortamlarda tutulan; ses, görüntü, veri ve yazılımların tümü.

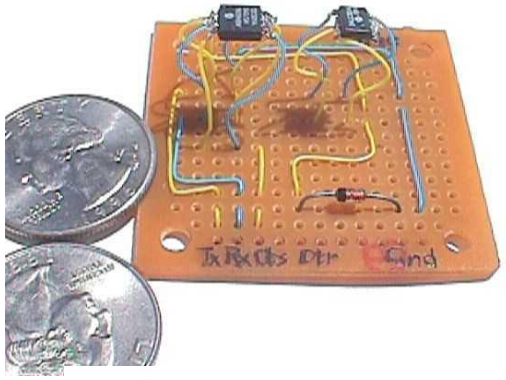
2.3 Sayısal Delil Nerededir?

Nerelerde Bulunur?

- Disket, Zip Disk, USB disk
- Hardiskler, Cd'ler
- Teyp Yedekleme Üniteleri
- Dijital Kameralar
- Bellek kartları, El bilgisayarları
- Oyun Konsolları
- Network-Internet Ortamları
- Yazıcılar, Fax makineleri
- Cep telefonları
- ...



2.3 Sayısal Delil Nerededir



2.4 Sayısal Delil ile Kağıt Esaslı Delil Arasındaki Farklar

Nicel (Kantitatif) Farklar:

1. Boyut farkı: Çok küçük hacimde çok fazla doküman saklayabilme.
2. Format farklılıkları: Hızlı değişen teknoloji yüzünden eskiyen bilgisayarlar ve elektronik dokümanların kurtarılmasında bu açıdan yaşanan sıkıntılar.
3. Çoğalma hızı: Elektronik dokümanlar kağıt dokümanlara nazaran; daha kolay, daha hızlı ve çok daha fazla miktarlarda çoğaltılabilir.
4. Elektronik dokümanlar kağıt dokümanlara nazaran daha zor yok edilir.

2.4 Sayısal Delil ile Kağıt Esaslı Delil Arasındaki Farklar

Nitel (Kalitatif) Farklar:

Kağıttan farklı olarak;

1. Bilgisayar veri/bilgileri, insan müdahalesi olmaksızın da zaman içinde değişebilir.
2. Bilgisayar veri/bilgileri; ait oldukları ortamlarından ayrıldıklarında anlaşılamaz hale gelebilmektedir.
3. Elektronik dokümanlar, çok farklı formatlarda gelebilir, değişkendirler.
4. Elektronik veri/bilgiler, zengin gizli bilgileri (yardımcı verileri) ihtiva edebilir.
5. Elektronik dokümanların kaynağını tespit etmek bazı durumlarda güç olabilir.

BÖLÜM 3: ADLİ BİLİŞİMDE OLAY YERİ KAVRAMI VE OLAY YERİ İNCELEME PRENSİPLERİ

3.1 Locard'ın Değişim Prensibi

3.2 Adli Bilişimde Olay Yeri Kavramı

3.3 Olay Yerine Gitmeden Önceki Hazırlıklar

3.4 Olay Yerinde Sayısal Delil Eldesi/İlk Muhafazası/İletilmesi

3.5 Olay Yerinde Yapılmayacaklar

3.1 Locard'ın Değişim Prensibi

"Bir suçlu; olay yerindeki herhangi bir nesne üzerinde kendinden bir şeyler bırakırken; olay yerinden de kendi üzerine mutlaka bir şeyler alır."

Suçun işlenmesi sırasında; suçlu ile olay yeri arasında bir fiziksel bilgi değiş tokuşu gerçekleşir.

Locard, 1920, Lyons Fransa; ilk Kriminal Laboratuvar.

3.2 Adli Bilişimde Olay Yeri Kavramı

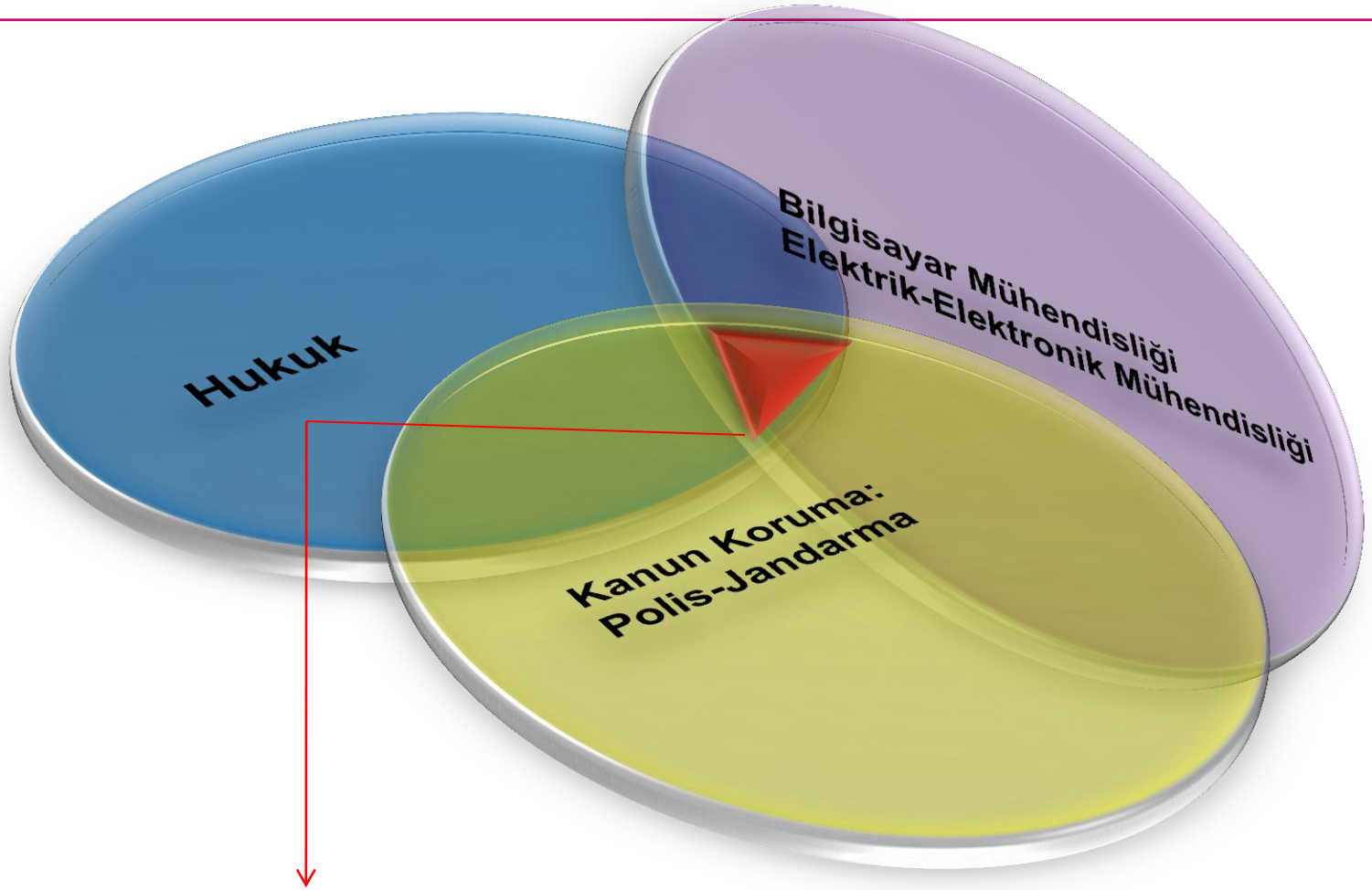
Bilişim sistemleri dört boyuttan bağımsızdır.

Wellington, Yeni Zelanda'da başlatılan bir işlem;
önce Turku, Finlandiya'ya
oradan Singapur'a ve nihayet
sonunda İstanbul'a varır.

Bu işlemin bir para aklama operasyonu olduğunu ve internet üzerinden gerçekleştirildiğini varsayarsak

Yer ve zaman kavramları ortadan kalkmış olur.

3.3 Olay Yerine Gitmeden Önceki Hazırlıklar



ADLİ BİLİŞİM UZMANI

3.3 Olay Yerine Gitmeden Önceki Hazırlıklar

Üç alanda da eğitim almış uzmanlara olan gereksinim

- Adli Bilişim Uzmanı; Bilgisayar ve/veya Elektrik-Elektronik Mühendisliği üzerine Adli Bilişim Uzmanlık eğitimi almış, bununla beraber Hukuk ve Kanun Koruma eğitimleri de almış olmalıdır.

Farklı İşletim Sistemlerini İçeren Laptoplar

- Microsoft-Mac-Linux

Donanım Bileşenleri

- Disk-DVD-CD-SD/MMC Kart çoklayıcılar

Hash Programları

Adli Bilişimsel Analiz İçin Yazılım Araçları

Paketleme – Sayısal Delil Muhafaza Malzemeleri

- Antistatik torbalar-Köpük-Sünger içli taşıma malzemeleri

Kameralar, GPS cihazları, Hemen her cins kablo ve bağlantı elemanı. Elektronikçi El aletleri

3.4 Olay Yerinde Sayısal Delil Elde Edilmesi

Genel Prensipler - 1

Olay yeri güvenliği alınmalı, delillerin fiziki fotoğrafları çekilmelidir.

Karşılaşılan sahne detaylarıyla raporlanmalıdır.

Olay yerinde kapalı bir bilgisayar var ise asla açılmamalıdır.

Olay yerinde çalışan bir bilgisayar var ise;

- Bilgisayar asla kullanılmamalı, varsa ekran görüntüleri alınmalı,
- Bilgisayar Windows bir sistem ise kablosu çekilerek kapanmalı,
- Unix/Linux türevi ise duruma göre kablo çekilmeli veya kapatılmalıdır.

3.4 Olay Yerinde Sayısal Delil Elde Edilmesi

Genel Prensipler – 2

Tüm bilgisayar medyaları not edilmelidir.

Tüm veri aygıtları toplanmalı ve güvenli bir şekilde taşıma ortamı hazırlanmalıdır.

Yapılan her işlem not edilmelidir.

Sistemin bire bir imajı alınmalıdır.

İmaj almadan önce yazma koruma cihazları kullanılmalıdır.

3.4 Olay Yerinde Sayısal Delil Elde Edilmesi

1. Delilleri Toplamaya Başlamadan Önce
   - Herkesi bilgisayar sisteminin başından uzaklaştır
   - Olay yerinin tüm ayrıntılarıyla kamera kaydını yap.
   - Olay yerindeki bilişim sistem(ler)inin bağlantılarını çiz.
   - Zarar verebilecek aktivitelere dikkat et
   - Olay yerindeki şifre olabilecek notlara dikkat et
2. Bilgisayar açık ise
   - Ekran görüntüsünün fotoğrafını çek
   - Ekran koruyucu varsa, iptal etmek için bulunan şifreleri kullan
   - Sıradışı görünenleri not al
   - Bilgisayarı kapama, elektriğini kes
   - UPS sistemlerine dikkat et - Ağ kablosunu sök
3. Bilgisayar Kapalı ise
   - Elektriğini kes -UPS sistemlerine dikkat - Ağ kablosunu sök

3.4 Olay Yerinde Sayısal Delil Elde Edilmesi

4. Fotoğrafını çekmeden önce
   Kabloları ve portları isimlendir.
   Kabloların başını ve sonunu işaretle. ETİKETLE ve NUMARALANDIR
   Kablo takılı değilse belirt.
   Seri numaralarını kaydet.
5. Daha sonra
   Tüm harici donanımları ve kabloları çıkar
   Dahili diskleri ve kartları sökme, birlikte paketle.

3.4 Olay Yerinde Sayısal Delil Elde Edilmesi

7. Ortamda bulunabilecek

Lazer-Kartuşlu-Matris vuruşlu her türlü yazıcıyı; kapatmadan ve fakat doğrudan akımdan çekerek kontrol altına al.

Aynı işlemi ağ aktif cihazları (hub, switch, router, DHCP server gibi) için yap.

Eğer PDA varsa kapatmadan olduğu gibi muhafaza altına al. PDA'e ait disk varsa, diskler için tanımlanmış olan özet çıkartma işlemini yap.

3.4 Olay Yerindeki Sayısal Delillerin Muhafazası ve İletimi

8. Her donanımı ayrı ayrı paketle

- Anti-statik poşet-balon ve köpük kullan
- Varsa, sistemlere ait orijinal taşıma kutularını kullan
- Isı, statik elektrik, yüksek elektro-manyetik ortamlardan (yüksek gerilim, baz istasyonu gibi) koru.
- Elinden düşürme, patlak-zayıf torbalara dikkat.
- Özel araçlar ile sarsıntıdan, sıcaktan ve soğuktan koruyarak naklet.
- Araç içinde (mümkünse) özel kemer ile sıkıca bağla.

3.4 Olay Yerindeki Sayısal Delillerin Muhafazası ve İletimi

9. Delil zincirini başlat

10. Delili en iyi şekilde ve en güvenli biçimde ilet: “DİKKAT DELİL! devirmeyiniz ve kullanmayınız !” diye işaretle.

11. En kısa zamanda, inceleyecek uzmana il

12. Özel saklama odaları ve rafları oluştur.

13. Giriş çıkışın kontrollü olduğu, güvenli yerlerde muhafaza et.

3.4 Olay Yerindeki Sayısal Delillerin Muhafazası ve İletimi

Dikkat Çok Önemli: İmaj Alma: Bire-bir Kopyalama.

Delil niteliğindeki medya üzerinde mümkünse direk olarak hiç bir inceleme yapılmamalı ve yazma koruması alındıktan sonra, bire bir kopyası (imaj) alınmalıdır.

Medyanın bire bir kopyasının alınması mümkün değilse, yine yazma koruma önlemi olan donanımsal cihazlar üzerinde inceleme yapılmalıdır.

3.5 Olay Yerinde Sayısal Delil Elde Edilmesi: Yapılmayacaklar

En önemli ayrıntı:

Bilmiyorsan, anlamıyorsan, bildiğini zannediyorsan,

SAKIN DOKUNMA!

Sayısal delil ile sadece UZMANI uğraşır...

BÖLÜM 4: ADLİ BİLİŞİMSEL ANALİZ PRENSİPLERİ

4.1 Adli Bilişimde İnceleme Metodolojisi

4.2 Analizde Kullanılan Yazılım ve Donanımlar

4.3 Analiz

4.4 Raporlama

4.5 Sayısal Delil Eldesindeki Güçlükler

4.1 Adli Bilişimde Analiz Metodolojisi

- Amerikan Adalet Bakanlığı
Bilgisayar Suçları ve Fikri Haklar Bölümü,
Siber Suç Laboratuvarı
(http://www.cybercrime.gov)

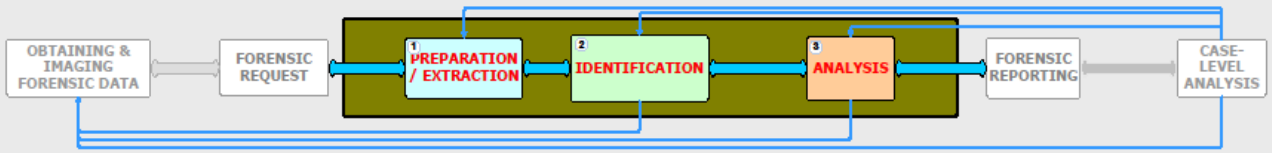
Analiz Metodolojisi
(22 Ağustos 2007 itibariyle)

4.1 Adli Bilişimde Analiz Metodolojisi

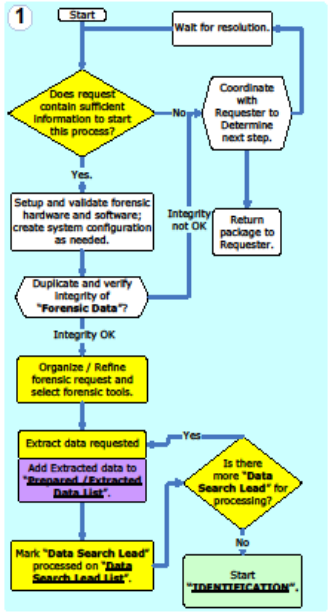
DIGITAL FORENSIC ANALYSIS METHODOLOGY

Last Updated: August 22, 2007

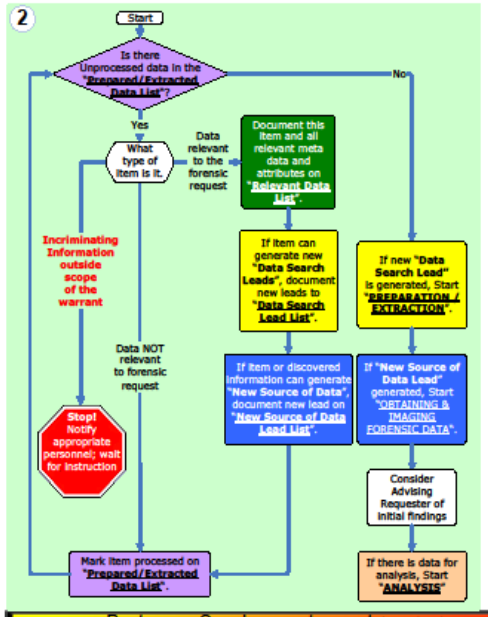
PROCESS OVERVIEW



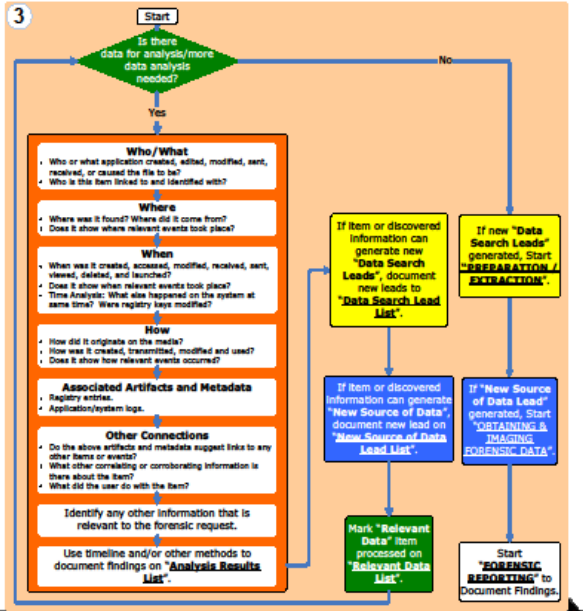
PREPARATION / EXTRACTION



IDENTIFICATION

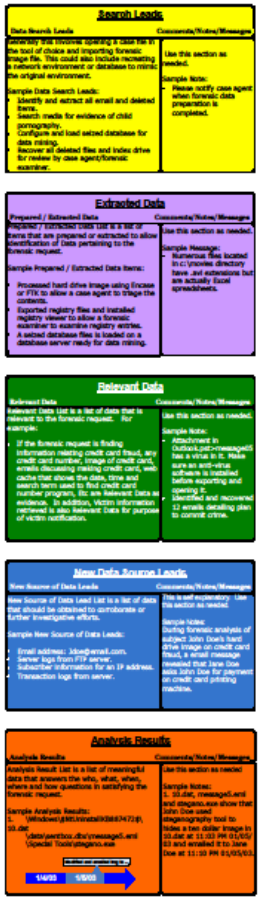


ANALYSIS



Return On Investment (Determine when to stop this process. Typically, after enough evidence is obtained for prosecution, the value of additional forensic analysis diminishes.)

LISTS



Department of Justice (DOJ)
Computer Crime and Intellectual Property Section (CCIPS)
Cybercrime Lab
http://www.cybercrime.gov
(202) 514-1026

4.1 Adli Bilişimsel Analiz Metodolojisi

• Adli Bilişim incelemesi dört temel adımdan oluşur; bunlar sırasıyla:

1. Elde Etme ve Muhafaza (Acquisition)

Olay yeri güvenliği, delil toplama, birebir kopyalama, araştırma yöntemlerinin belirlenmesi.

2. Tanımlama (Identification)

Suça konu içeriğin taranarak sistem üzerinde araştırmanın yapılması.

3. Değerlendirme (Evaluation)

Bulunan suç unsurlarının değerlendirilmesi.

4. Sunum (Presentation)

Elde edilen verilerin Adli makamlar için dökümantasyonu

4.2 Analizde Kullanılan Yazılım ve Donanımlar

EnCase©

- Guidance Software
- Enterprise
- Forensic
- Fastbloc©
  - İmaj Alma
  - Delil Üzerinde İnceleme
  - Adli Merciler İçin Raporlama
- www.encase.com

4.2 Analizde Kullanılan Yazılım ve Donanımlar

FTK – Forensic Tool Kit

- Access Data
  - İmaj Alma
  - Delil Üzerinde İnceleme
  - Adli Merciler için Raporlama
- Indexleme özelliği
- Şifre Kırma
- Dağıtık Network Atağı
- www.accessdata.com

4.2 Analizde Kullanılan Yazılım ve Donanımlar

✓Cep Telefonu İnceleme Kitleri (CellBrite, Paraben Device Seizer)

✓ Şifre Kırma Hızlandırıcısı (TACC1441 Hardware Accelerator)

4. 2 Analizde Kullanılan Yazılım ve Donanımlar

✓Donanımsal İmaj Alma Cihazları (Solo, HardCopy 2)

4.3 Analiz

- Karşılaşılan suça ilişkin ne tür verilerin araştırılacağının saptanmasıdır. Araştırılacak veriler genellikle karşılaşılan suç ile aynı suça konu medyaya göre değişebilme eğilimi taşır.

- Her analiz, konusuna ve aranana göre eşsizdir.
  - Tek bir dosyanın aranması
  - Kriptolu & Şifreli Dosyalar
  - Nadir karşılaşılan dosya türleri

DO NOT CROSS CRIME SCENE DO NOT CROSS CRIME SCENE DO NOT CROSS CRIME SCENE

4.3 Analiz

- Analizi Yapılan Ortamlar
  - PC & Dizüstü İncelemesi
  - Hafıza Kartı, USB Stick İncelemesi
  - Cep Telefonu İncelemesi
  - Ağ (Network) İncelemesi
  - Donanımsal ve/veya Yazılımsal Veri Kurtarma
  - Kiptanaliz (Şifre veya Kripto Kırma)
  - Kablosuz (wireless) İnceleme

4.4 Raporlama

1. İlk önce; elde edilen verilerden hangilerinin Adli Makamlara iletilmek üzere hazırlanacak rapora dahil olacağı, verilerin güvenli, zarar görmeden ve birebir değişmemiş halinin çıkartılmış olup olmadığının değerlendirilmesi ile kontrolu yapılmalıdır.

2. Verilerin doğru ve öz olması, veri bütünlüğü ve anlaşılabilirliği son derece önemlidir.

4.5 Sayısal Delil Analizinde Güçlük Yaratan Oluşumlar

- Silme/imha araçlarının kullanılmış olması (degaussers, datawipe)
- Şifreleme yapılmış olması
- Virüs gibi zararlı yazılımların etkileri
- Rebooting işlemleri
- Sistemin durum değişimleri (reverting to initial state)
- Formatlanmış medya
- Defragmentation işleminin yapılmış olması
- Manyetik alan bozulmaları
- Fiziksel hasarlar