Bilişim Suçları, Adli Bilişim, İnceleme Araçları ve Örnek Olay Analizi (EnCase ile Uygulama)

A.Hakan EKİZER
Komiser
Bilişim Suçları Uzmanı
ahmethakan@ekizer.net

Paradigma

- Bilişim Suçları
- Yüksek Teknoloji Suçları
- Bilgisayar Suçları
- İnternet Suçları
- Siber Suçlar

Sadece Bilişim Sistemlerine karşı işlenen suçlar.

Bilişim Sistemleri ile işlenen her türlü suç.

Bilişim Suçları; Bilgileri Otomatik olarak işleme tabi tutan yahut verilerin nakline yarayan bir sisteme karşı veya sistem ile gayri kanuni, ahlak dışı ve yetkisiz gerçekleştirilen he türlü davranıştır.

(AVRUPA EKONOMİK TOPLULUĞU-1983)

Bilişim Suçlarının Sınıflandırılması

- **Hedef olarak bilişim sistemleri**

  Yetkisiz erişim, Servis dışı bırakma, verilere zarar, vs.

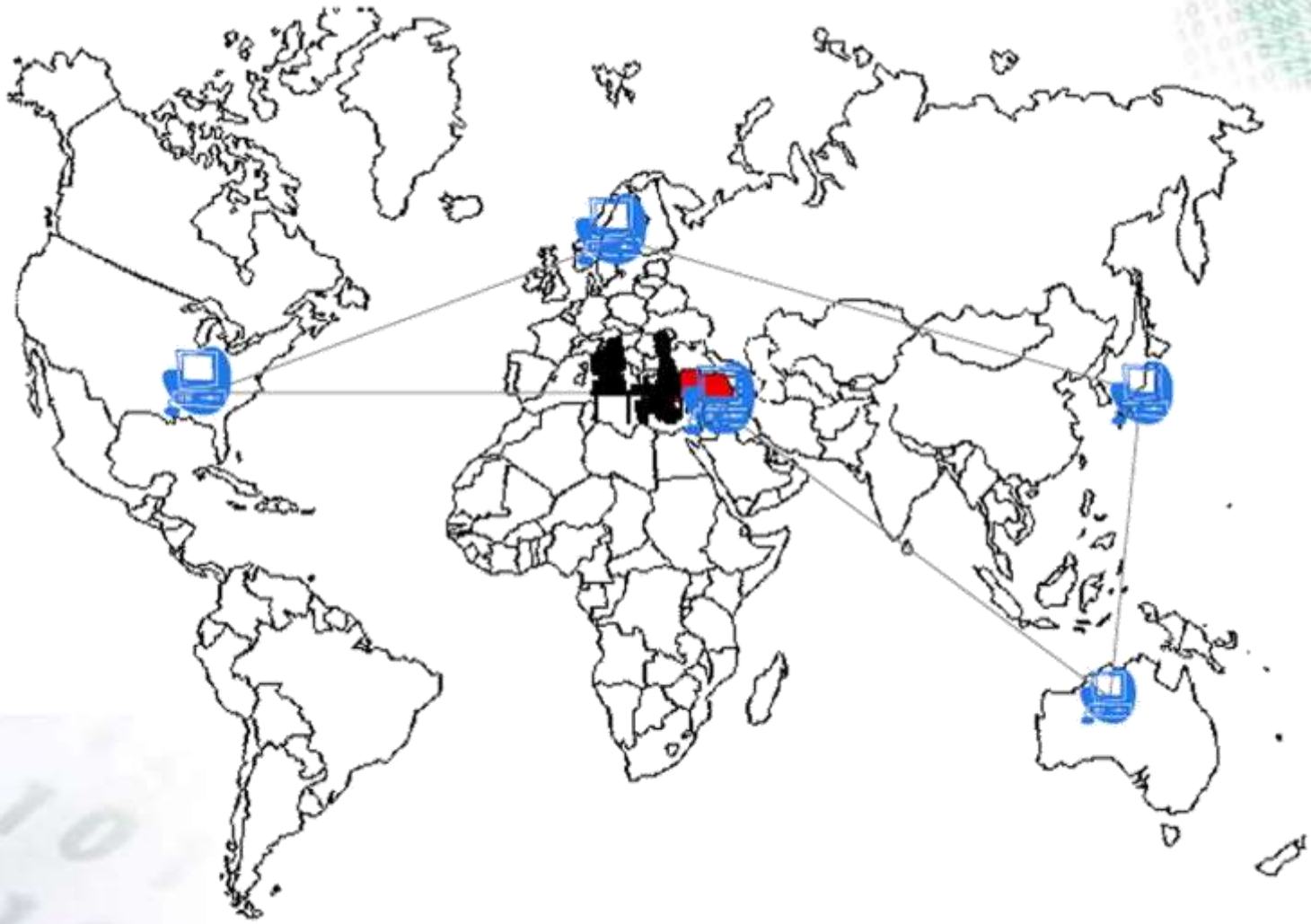
- **Bilişim Bağlantılı Suçlar.**

  Kredi kartı ve Internet bankacılığı dolandıcılığı, Telif hakları ihlali vs.

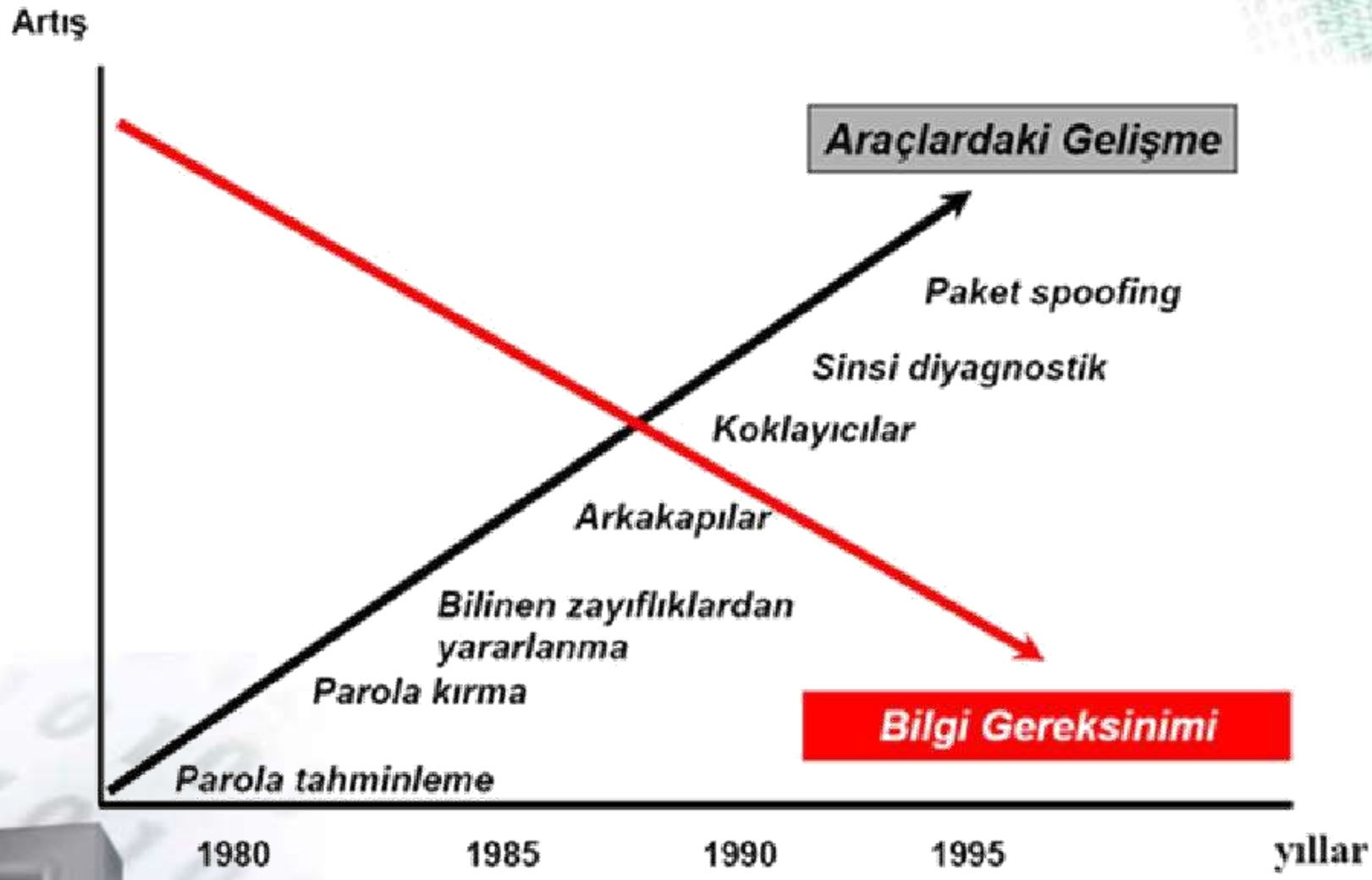
- **Bilişim Vasıtalı Normal Suçlar.**

  Uyuşturucu trafiği, kara para aklama, hakaret sövme, terör, vs.

İnternet İle Birlikte



Bilişim Teknolojisi ile Birlikte



Kaynak CERT

Suçlu Profili.

- **Hedefli ve Bilinçli Saldırgan**
  - Amaçlıdır, planlı ve programlıdır.
  - Tehlikelidir.Teknik Bilgi ve Becerisi Yüksektir.
  - Kendini Saklamaya Özen Gösterir.
  - Kendine Özel Araçlar Kullanır.
- **Hedefsiz ama Bilinçli Saldırgan**
  - Amacı yoktur, rastgele hedef seçer
  - Tehlikelidir, Teknik Bilgi ve Becerisi Mevcuttur.
  - Kendine Özel veya Rastgele Araçlar Kullanır.
  - Yakalanma kaygısı vardır. Gizlenir.
- **Hedefli ama Bilinçsiz Saldırgan**
  - Amacı vardır, plansız ve programsızdır.
  - Bilgi seviyesi az düzeyde genelde kulaktan dolmadır.
  - Otamatik araçlar kullanır. Kendini ispatlama çabası vardır.
  - Çok fazla iz bırakır
- **Hedefsiz ve Bilinçsiz Saldırgan**
  - Amacı yoktur, rastgele hedef seçer
  - Teknik düzeyi zayıftır, Kulaktan dolma bilgisi vardır.
  - Kolay takip edilir ve yakalanır.
  - Tehlikelidir, Saldırgan kitlesinin büyük çoğunluğunu oluşturur.

Suçlu Tipleri.

Hacker

En iyileri, Siyah Şapkalı (Black Hat) – Beyaz Şapkalı (White Hat). Kimliklerini ve faaliyetlerini gizlerler.

Cracker

Şifre Kırıcılar. Genellikle yazılım şifreleri. Kimliklerini ve faaliyetlerini gizlerler. Hacker olma yolundadırlar.

Lamer

Hazır araçları ve virusleri kullanırlar. Şan ve Şöhret Peşindedirler. Hacker olduklarını iddia ederler.

Script-Kid / Cyber-Punk

Bilgisayar konusunda uzman, genç yaşta ve hazır araçları kullanırlar. Egolu ve kendini ispat peşindedirler.

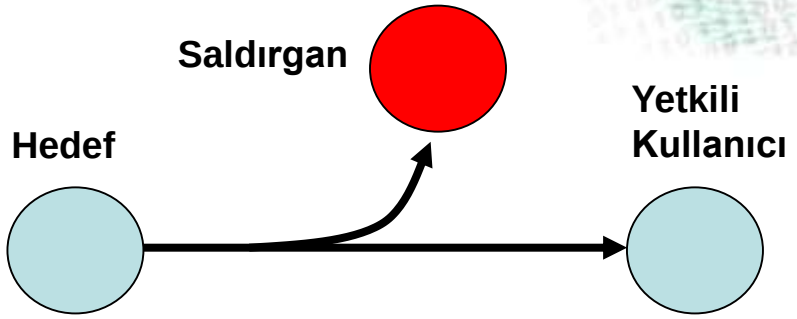
Meraklılar – Kullanıcılar

Bilgisayar konusunda meraklı, çoğunlukla farkında olmadan zarar veren, veya çalıştığı yerden intikam alma amacında olan kişilerdir.

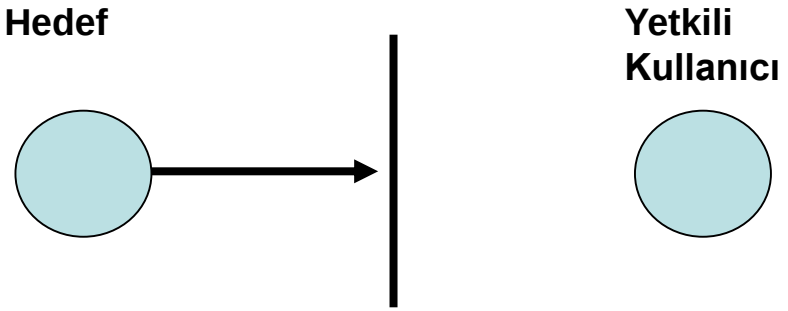
Suç Tipleri

Hedef olarak bilişim sistemleri

- **Yetkisiz-İzinsiz Erişim**
  - *Sisteme Girme*
  - *Kopyalanma*
  - *Dinlenme*



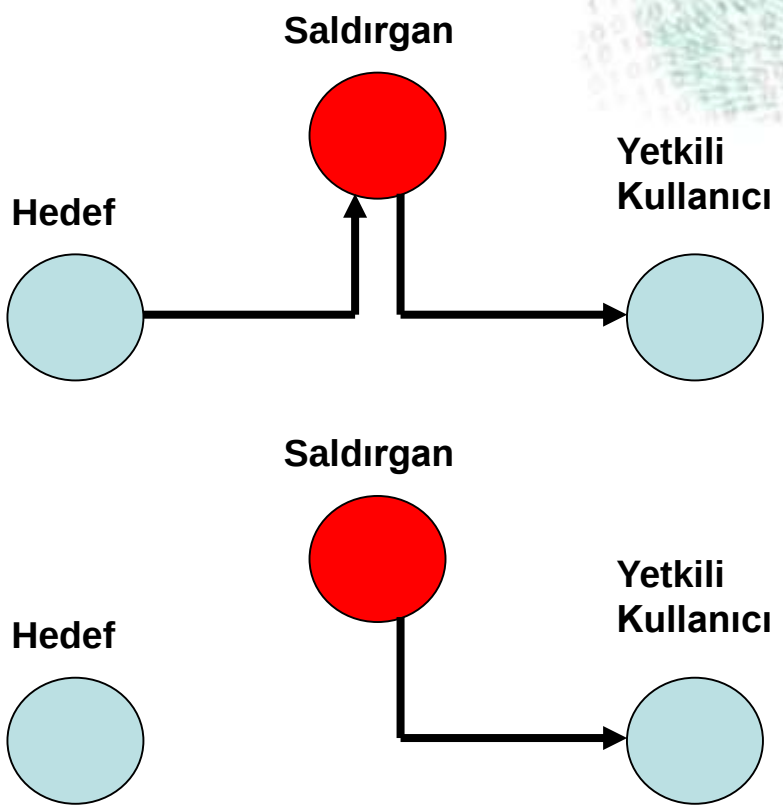
- **Zarar Verme (Engelleme)**
  - *Verileri Silme*
  - *Verilere hasar verme*
  - *Servis Dışı Bırakma.*



Suç Tipleri

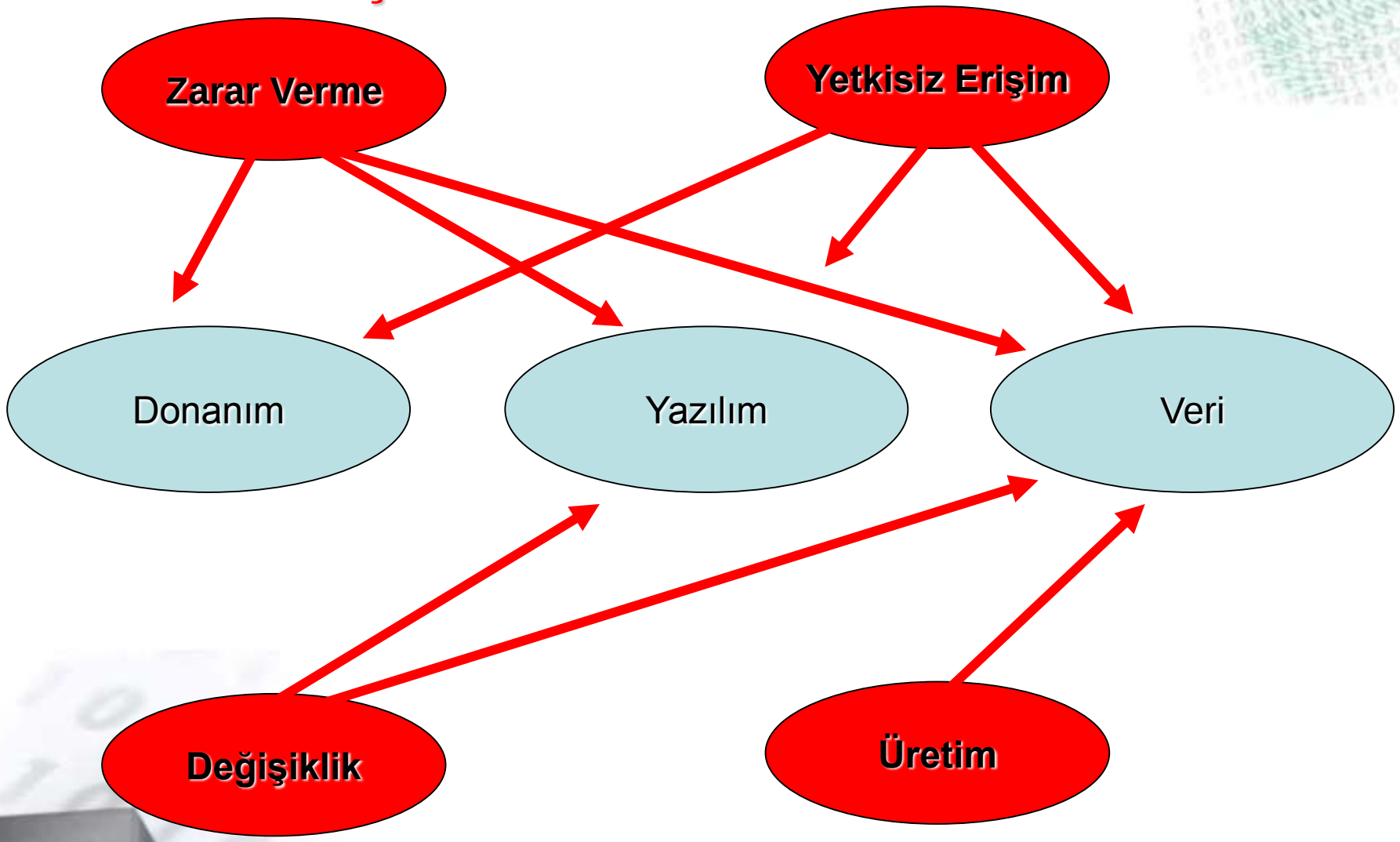
Hedef olarak bilişim sistemleri

- **Değişiklik Yapma**
  - *Program kodları*
  - *Durgun Veri*
  - *Aktarılan Veri*
- **Üretim**
  - *Veri taklidi*
  - *Veri ekleme*



Suç Tipleri

Hedef olarak bilişim sistemleri



İşleniş Şekilleri

İşleniş Şekilleri ve Araçları Klasik Suçlardan farklı.

Zararlı Yazılımlar ile.

- Truva Atları (Trojan Horses)
- Virüsler
- Ağ Solucanları (Worms)
- Casus Yazılımlar (SpyWare)

İşleniş Şekilleri

İşleniş Şekilleri ve Araçları Klasik Suçlardan farklı.

Zararlı Yazılımlar ile.

- Mantık Bombaları
- Şifre Kırıcılar
- Ağ Koklayıcıları (Sniffers)
- Zafiyet Avcıları (Vuln. Scanners)

İşleniş Şekilleri

İşleniş Şekilleri ve Araçları Klasik Suçlardan farklı.

Aldatmacalar ile

- Sosyal Mühendislik.
- IP, ARP, DNS… Protokol Aldatmacaları(Spoofing)
- Phishing,
- Scam Page.
- Spam&Fake Mail.

Bilişim Suçları İlgili Mevzuat

A.Hakan EKİZER
Komiser
Bilişim Suçları Uzmanı
ahmethakan@ekizer.net

Bilişim Suçları ile ilgili Kanunlar

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.*

Bilişim Suçları ile ilgili Kanunlar

- **Fikir ve Sanat Eserleri Kanunu**

  - ✓ ***MADDE 71*** *– Manevi Haklara Tecavüz.*
  - ✓ ***MADDE 72*** *– Mali Haklara Tecavüz.*
  - ✓ ***MADDE 73*** *– Diğer Suçlar.*

- **Kaçakçılıkla Mücadele Kanunu**

  - ✓ ***MADDE 12*** *– Gümrük idarelerinde sahte beyan ve belge.*

- **Ceza Muhakemesi Kanunu**

  - ✓ ***MADDE 134*** *– Bilgisayarlarda, bilgisayar programlarında ve kütüklerinde arama, kopyalama ve elkoyma.*

TCK'daki Bilişim Suçları

Bilişim Sistemine Girme

MADDE 243. – Yekisiz Erişim – Sisteme Girme

(1) Bir bilişim sisteminin bütününe veya bir kısmına, hukuka aykırı olarak giren ve orada kalmaya devam eden kimseye bir yıla kadar hapis veya adlî para cezası verilir.

(2) Yukarıdaki fıkrada tanımlanan fiillerin bedeli karşılığı yararlanılabilen sistemler hakkında işlenmesi hâlinde, verilecek ceza yarı oranına kadar indirilir.

(3) Bu fiil nedeniyle sistemin içerdiği veriler yok olur veya değişirse, altı aydan iki yıla kadar hapis cezasına hükmolunur.

TCK'daki Bilişim Suçları

- **Sistemi engelleme, bozma, verileri yok etme veya değiştirme**

MADDE 244. – Hacking

(1) Bir bilişim sisteminin işleyişini engelleyen veya bozan kişi, bir yıldan beş yıla kadar hapis cezası ile cezalandırılır.

(2) Bir bilişim sistemindeki verileri bozan, yok eden, değiştiren veya erişilmez kılan, sisteme veri yerleştiren, var olan verileri başka bir yere gönderen kişi, altı aydan üç yıla kadar hapis cezası ile cezalandırılır.

(3) Bu fiillerin bir banka veya kredi kurumuna ya da bir kamu kurum veya kuruluşuna ait bilişim sistemi üzerinde işlenmesi halinde, verilecek ceza yarı oranında artırılır.

(4) Yukarıdaki fıkralarda tanımlanan fiillerin işlenmesi suretiyle kişinin kendisinin veya başkasının yararına haksız bir çıkar sağlamasının başka bir suç oluşturmaması hâlinde, iki yıldan altı yıla kadar hapis ve beşbin güne kadar adlî para cezasına hükmolunur

TCK'daki Bilişim Suçları

Banka veya Kredi Kartlarının Kötüye Kullanılması

MADDE 245. – Kredi Kartı ve Banka'ya karşı

(1) Başkasına ait bir banka veya kredi kartını, her ne suretle olursa olsun ele geçiren veya elinde bulunduran kimse, kart sahibinin veya kartın kendisine verilmesi gereken kişinin rızası olmaksızın bunu kullanarak veya kullandırtarak kendisine veya başkasına yarar sağlarsa, üç yıldan altı yıla kadar hapis cezası ve adlî para cezası ile cezalandırılır.

(2) Sahte oluşturulan veya üzerinde sahtecilik yapılan bir banka veya kredi kartını kullanmak suretiyle kendisine veya başkasına yarar sağlayan kişi, fiil daha ağır cezayı gerektiren başka bir suç oluşturmadığı takdirde, dört yıldan yedi yıla kadar hapis cezası ile cezalandırılır.

Tüzel kişiler hakkında güvenlik tedbiri uygulanması

MADDE 246. *- (1) Bu bölümde yer alan suçların işlenmesi suretiyle yararına haksız menfaat sağlanan tüzel kişiler hakkında bunlara özgü güvenlik tedbirlerine hükmolunur*

TCK'daki Bilişim Vasıtalı Diğer Suçlar

- **Kişilere Karşı İşlenen Suçlar - Hürriyete Karşı Suçlar.**

MADDE 124. – Haberleşmenin engellenmesi

(1) Kişiler arasındaki haberleşmenin hukuka aykırı olarak engellenmesi hâlinde, altı aydan iki yıla kadar hapis veya adlî para cezasına hükmolunur.

(2) Kamu kurumları arasındaki haberleşmeyi hukuka aykırı olarak engelleyen kişi, bir yıldan beş yıla kadar hapis cezası ile cezalandırılır.

(3) Her türlü basın ve yayın organının yayınının hukuka aykırı bir şekilde engellenmesi hâlinde, ikinci fıkra hükmüne göre cezaya hükmolunur.

TCK'daki Bilişim Vasıtalı Diğer Suçlar

Kişilere Karşı İşlenen Suçlar - Şerefe Karşı Suçlar.

MADDE 125. – Hakaret

(1) Bir kimseye onur, şeref ve saygınlığını rencide edebilecek nitelikte somut bir fiil veya olgu isnat eden ya da yakıştırmalarda bulunmak veya sövmek suretiyle bir kimsenin onur, şeref ve saygınlığına saldıran kişi, üç aydan iki yıla kadar hapis veya adlî para cezası ile cezalandırılır. Mağdurun gıyabında hakaretin cezalandırılabilmesi için fiilin en az üç kişiyle ihtilât ederek işlenmesi gerekir.

……

(2) Fiilin, mağduru muhatap alan sesli, yazılı veya görüntülü bir iletiyle işlenmesi hâlinde, yukarıdaki fıkrada belirtilen cezaya hükmolunur.

……

(4) Ceza, hakaretin alenen işlenmesi hâlinde, altıda biri; basın ve yayın yoluyla işlenmesi hâlinde, üçte biri oranında artırılır.

TCK'daki Bilişim Vasıtalı Diğer Suçlar

- **Kişilere Karşı İşlenen Suçlar – Özel hayata ve Hayatın gizliliğine karşı suçlar.**

MADDE 132. – Haberleşmenin Gizliliğini İhlal.

(1) Kişiler arasındaki haberleşmenin gizliliğini ihlâl eden kimse, altı aydan iki yıla kadar hapis veya adlî para cezası ile cezalandırılır. Bu gizlilik ihlâli haberleşme içeriklerinin kaydı suretiyle gerçekleşirse, bir yıldan üç yıla kadar hapis cezasına hükmolunur.

(2) Kişiler arasındaki haberleşme içeriklerini hukuka aykırı olarak ifşa eden kimse, bir yıldan üç yıla kadar hapis cezası ile cezalandırılır.

(3) Kendisiyle yapılan haberleşmelerin içeriğini diğer tarafın rızası olmaksızın alenen ifşa eden kişi, altı aydan iki yıla kadar hapis veya adlî para cezası ile cezalandırılır.

(4) Kişiler arasındaki haberleşmelerin içeriğinin basın ve yayın yolu ile yayınlanması hâlinde, ceza yarı oranında artırılır.

TCK'daki Bilişim Vasıtalı Diğer Suçlar

- **Kişilere Karşı İşlenen Suçlar – Özel hayata ve Hayatın gizliliğine karşı suçlar.**

MADDE 133. – Kişiler arası konuşmaların dinlenmesi ve kayda alınması .

(1) Kişiler arasındaki alenî olmayan konuşmaları, taraflardan herhangi birinin rızası olmaksızın bir aletle dinleyen veya bunları bir ses alma cihazı ile kaydeden kişi, iki aydan altı aya kadar hapis cezası ile cezalandırılır.

……

(1) Yukarıdaki fıkralarda yazılı fiillerden biri işlenerek elde edildiği bilinen bilgilerden yarar sağlayan veya bunları başkalarına veren veya diğer kişilerin bilgi edinmelerini temin eden kişi, altı aydan iki yıla kadar hapis ve bin güne kadar adlî para cezası ile cezalandırılır. Bu konuşmaların basın ve yayın yoluyla yayınlanması hâlinde de, aynı cezaya hükmolunur.

TCK'daki Bilişim Vasıtalı Diğer Suçlar

- **Kişilere Karşı İşlenen Suçlar – Özel hayata ve Hayatın gizliliğine karşı suçlar.**

MADDE 135. – Kişisel verilerin kaydedilmesi.

(1) Hukuka aykırı olarak kişisel verileri kaydeden kimseye altı aydan üç yıla kadar hapis cezası verilir.

(2) Kişilerin siyasî, felsefî veya dinî görüşlerine, ırkî kökenlerine; hukuka aykırı olarak ahlâkî eğilimlerine, cinsel yaşamlarına, sağlık durumlarına veya sendikal bağlantılarına ilişkin bilgileri kişisel veri olarak kaydeden kimse, yukarıdaki fıkra hükmüne göre cezalandırılır

MADDE 136. – Verileri hukuka aykırı olarak verme veya ele geçirme.

(1) Kişisel verileri, hukuka aykırı olarak bir başkasına veren, yayan veya ele geçiren kişi, bir yıldan dört yıla kadar hapis cezası ile cezalandırılır.

MADDE 138. – Verileri hukuka aykırı olarak verme veya ele geçirme.

(1) Kanunların belirlediği sürelerin geçmiş olmasına karşın verileri sistem içinde yok etmekle yükümlü olanlara görevlerini yerine getirmediklerinde altı aydan bir yıla kadar hapis cezası verilir.

TCK'daki Bilişim Vasıtalı Diğer Suçlar

- **Kişilere Karşı İşlenen Suçlar – Mal Varlığına Karşı Suçlar.**

MADDE 142. – Nitelikli Hırsızlık.

(1) Hırsızlık suçunun;

……

(e) Bilişim sistemlerinin kullanılması suretiyle

……

İşlenmesi hâlinde, üç yıldan yedi yıla kadar hapis cezasına hükmolunur.

MADDE 158. – Nitelikli Dolandırıcılık.

(1) Dolandırıcılık suçunun;

……

(e) Bilişim sistemlerinin, banka veya kredi kurumlarının aracı olarak kullanılması suretiyle,

(f) Basın ve yayın araçlarının sağladığı kolaylıktan yararlanmak suretiyle,

……

İşlenmesi halinde, iki yıldan yedi yıla kadar hapis ve beş bin güne kadar adli para cezasına hükmolunur.

TCK'daki Bilişim Vasıtalı Diğer Suçlar

Topluma Karşı Suçlar – Genel Ahlaka Karşı Suçlar.

MADDE 226. – Müstehcenlik.

1)

a) Bir çocuğa müstehcen görüntü, yazı veya sözleri içeren ürünleri veren ya da bunların içeriğini gösteren, okuyan, okutan veya dinleten,

b) Bunların içeriklerini çocukların girebileceği veya görebileceği yerlerde ya da alenen gösteren, görülebilecek şekilde sergileyen, okuyan, okutan, söyleyen, söyleten,

c) Bu ürünleri, içeriğine vakıf olunabilecek şekilde satışa veya kiraya arz eden,

d) Bu ürünleri, bunların satışına mahsus alışveriş yerleri dışında, satışa arz eden, satan veya kiraya veren,

e) Bu ürünleri, sair mal veya hizmet satışları yanında veya dolayısıyla bedelsiz olarak veren veya dağıtan,

f) Bu ürünlerin reklamını yapan,

Kişi, altı aydan iki yıla kadar hapis ve adlî para cezası ile cezalandırılır.

Fikir ve Sanat Eserleri Kanunu

Fikir ve Sanat Eserleri Kanunun 71, 72, 73 Maddeleri

- ✓ ***MADDE 71 – Manevi Haklara Tecavüz.***

  Yazılımı kamuya sunma hakkı,Yazılım sahibinin adını belitme hakkı, Değişiklik yapılmaması hakkı

- ✓ ***MADDE 72 – Mali Haklara Tecavüz.***

  Değiştirmek, kopyalamak, çoğaltmak yaymak, ticaret konusu yapmak, aracılık etmek, suçtur.

- ✓ ***MADDE 73 – Diğer Suçlar.***

Fikir ve Sanat Eserleri Kanunu

Fikir ve Sanat Eserleri Kanunun 71, 72, 73 Maddeleri

- ***MADDE 71 – Manevi Haklara Tecavüz.***

  Yazılımı kamuya sunma hakkı,Yazılım sahibinin adını belitme hakkı, Değişiklik yapılmaması hakkı

- ***MADDE 72 – Mali Haklara Tecavüz.***

  Değiştirmek, kopyalamak, çoğaltmak yaymak, ticaret konusu yapmak, aracılık etmek, suçtur.

- ***MADDE 73 – Diğer Suçlar.***

Fikir ve Sanat Eserleri Kanunu

Fikir ve Sanat Eserleri Kanunun 71, 72, 73 Maddeleri

- ✓ ***MADDE 71 – Manevi Haklara Tecavüz.***

  Yazılımı kamuya sunma hakkı,Yazılım sahibinin adını belitme hakkı, Değişiklik yapılmaması hakkı

- ✓ ***MADDE 72 – Mali Haklara Tecavüz.***

  Değiştirmek, kopyalamak, çoğaltmak yaymak, ticaret konusu yapmak, aracılık etmek, suçtur.

- ✓ ***MADDE 73 – Diğer Suçlar.***

Kaçakçılıkla Mücadele Kanunu

Kaçakçılıkla Mücadele Kanunu (4926)

- ✓ ***MADDE 12 – Gümrük idarelerinde sahte beyan ve belgeler.***

Gümrük idarelerinde işlem görmediği halde işlem görmüş gibi herhangi bir belge veya beyanname düzenleyenler veya bu suçları bilişim yoluyla işleyenler hakkında Türk Ceza Kanununun evrakta sahtekarlık ve bilişim alanındaki suçlarla ilgili hükümlerinde belirtilen cezalar bir kat artırılarak uygulanır.

CMK Bilgisayar incelemeleri

Ceza Muhakemesi Kanunu

- ***MADDE 134***. – *Bilgisayarlarda, bilgisayar programlarında ve kütüklerinde arama, kopyalama ve elkoyma.*

(1) Bir suç dolayısıyla yapılan soruşturmada, başka surette delil elde etme imkânının bulunmaması halinde, Cumhuriyet savcısının istemi üzerine şüphelinin kullandığı bilgisayar ve bilgisayar programları ile bilgisayar kütüklerinde arama yapılmasına, bilgisayar kayıtlarından kopya çıkarılmasına, bu kayıtların çözülerek metin hâline getirilmesine hâkim tarafından karar verilir.

(2) Bilgisayar, bilgisayar programları ve bilgisayar kütüklerine şifrenin çözülememesinden dolayı girilememesi veya gizlenmiş bilgilere ulaşılamaması halinde çözümün yapılabilmesi ve gerekli kopyaların alınabilmesi için, bu araç ve gereçlere elkonulabilir. Şifrenin çözümünün yapılması ve gerekli kopyaların alınması halinde, elkonulan cihazlar gecikme olmaksızın iade edilir.

(3) Bilgisayar veya bilgisayar kütüklerine elkoyma işlemi sırasında, sistemdeki bütün verilerin yedeklemesi yapılır.

(4) İstemesi halinde, bu yedekten bir kopya çıkarılarak şüpheliye veya vekiline verilir ve bu husus tutanağa geçirilerek imza altına alınır.

(5) Bilgisayar veya bilgisayar kütüklerine elkoymaksızın da, sistemdeki verilerin tamamının veya bir kısmının kopyası alınabilir. Kopyası alınan veriler kâğıda yazdırılarak, bu husus tutanağa kaydedilir ve ilgililer tarafından imza altına alınır.

Yaşanılan Sorunlar Değerlendirme

ADLİ BİLİŞİM VE DİJİTAL DELİL

Dijital Delil

"Bilişim Sistemleri medyaları veya dijital ortamlarda bulunabilen; suç ile ilgili delil niteliği taşıyabilecek veriler Dijital delil olarak nitelendirilebilir."

Nerelerde Bulunur?

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

Üzerinde veri saklama kabiliyeti bulunan her türlü elektronik cihaz dijital delil ihtiva edebilmektedir.

Bilgisayar Kriminalistiği (Computer Forensics)

"Bilgisayar Kriminalistiği (Computer Forensic), Bilişim Suçları veya diğer suçlarla ilgili bir soruşturma için adli makamlara intikal ettirmek üzere; bilgisayar veya dijital ortamlarda bulunabilen, delil niteliği taşıyabilecek verilerin korunarak, zarar görmeden ve doğru bir şekilde elde edilmesi için kullanılan prensiplerin oluşturduğu bilim dalıdır.."

Dört Önemli Adım.

- **Elde Etme (Acquisition)**
  Olay yeri güvenliği, delil toplama, birebir kopyalama, araştıma yöntemlerinin belirlenmesi.
- **Tanımlama (Identification)**
  Suça konu içeriğin taranarak sistem üzerinde araştırmanın yapılması
- **Değerlendirme (Evaluation)**
  Bulunan suç unsurlarının değerlendirilmesi.
- **Sunum (Presentation)**
  Adli makamlar için elde edilen verilerin dökümante edilmesi

İlk Olay yeri

Genel Prensipler.

- Olay yeri güvenliği alınmalı, delillerin fiziki fotoğrafları çekilmelidir
- Karşılaşılan sahne detaylarıyla roparlanmalıdır.
- Olay yerinde kapalı bir bilgisayar var ise asla açılmamalı!
- 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 kapatılmalı
- Tüm bilgisayar medyaları not edilmeli.
- Tüm veri aygıtları toplanmalı güvenli bir şekilde taşıma ortamı hazırlanmalı.
- Yapılan her işlem not edilmeli.
- Network ortamlarında kıritik sistem ise online inceleme yapılabilir.
- Sistem üzerinde direkt inceleme yapılamayacağı için birebir imaj alınmalı
- İmaj almadan inceleme için yazma koruma cihazları kullanılmalı.

Delilleri Toplama / Nakletme

"Bilgisayar sistemleri ile medyaları ısıya, fiziksel soklara, static elektrik akımlarına ve manyetik akımlara karşı oldukça hassas cihazlardır. Bu nedenle delil olarak toplanmasına, paketlenmesine, nakledilmesine ve saklanmasına oldukça önem gösterilmelidir."

- **Paketleme**
  - *Delilleri tespit et, sahneyi raporla, Etiketle ve numaralandır.*
  - *Manyetik medyaları anti-statik paketlerle paketle.*
  - *Sıcaklık, su ve darbelerden koru*
  - *Sistemleri birbirinden kopmadan paketle.*
- **Nakletme**
  - *Delilleri manyetik akımlardan uzak tut. (Yüksek Gerilim, Baz istasyonları vs.)*
  - *Özel araçlar ile sarsıntıdan, sıcaktan ve soğuktan koruyarak naklet.*
  - *Mümkünse araçlarda sıkıça özel kemerler ile bağla.*
- **Saklama**
  - *Özel saklama odaları ve rafları oluştur.*
  - *Giriş çıkışın kontrollü olduğu güvenli yerlede muhafaza et.*
  - *Mümkünse araçlarda sıkıça özel kemerler ile bağla.*

Bire-bir Kopyalama.

"Delil niteliğindeki Medyalar üzerinde mümkünse direk olarak hic bir inceleme yapılmamalı ve yazma koruması alındıktan sonra bire bir kopyası (imaj) alınmalı."

"Medyaların birebir kopyasının alınması mümkün değilse yine yazma koruma önlemi olan donanımsal cihazlar üzerinde inceleme yapılacaktır."

Araştırma Yöntemlerinin Belirlenmesi.

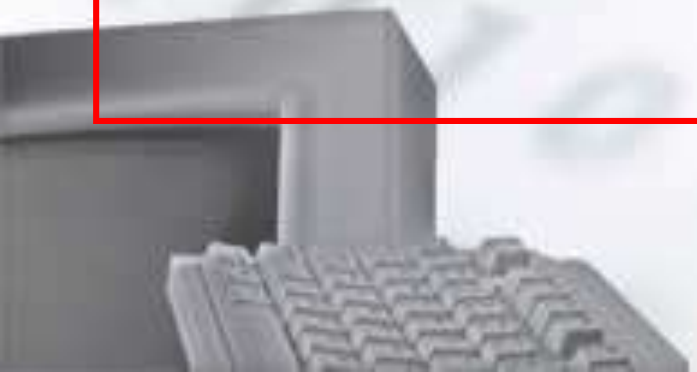
"Burada amaç karşılaşılan suça ilişkin ne tür verilerin araştırılacağının saptanmasıdır. Araştırılacak veriler genellikle karşılasılan suça ile aynı suça konu medyaya göre değişebilmektedir."

Suç : Çocuk Pornografisi

- Chat Kayıtları
- E-mailler, Notlar
- Resimler, Animasyon ve Filimler
- İlgili Oyunlar
- Tarajıcı Çerezleri
- Sık Kullanılan imgeleri
- Resim işleme yazılımları
- Silinmiş veriler (resim, Video)
- VS....

Medya : Hafıza kartları

- Yedeklenmiş Dosyalar
- Silinmiş Dosyalar
- Sıkıştırımış dosyalar
- Disk bölümleri
- Formatlanmış alan
- Şifreli alanlar
- Gizlenmiş dosya ve alanlar
- Dijital kamera dosyaları
- Bozuk, Kayıp, sektör ve segment
- Belirlenmemiş Alan ve Slack Alanı
- VS...



Suça konu içeriğin taranarak sistem üzerinde araştırmanın yapılması

"Araştırma yöntemlerinin belirlenmesinin ardından suça konu içerik bilgisayar sistemleri ve medyaları üzerinde araştırılır.

Disk Bölümleri
Uygulama Dosyaları
Registry Kayıtları
Log Dosyaları
Temp Dosyaları
Swap Alanı
Gizli Dosyalar.
Silinmiş Alan ve Dosyalar
VS....

İçerik (Ne tür veriler?)
Yakalama (Konu ile tam uyuşma)
Aktarım (Verilerin Çıkarılması)
Silinmiş Datalar (recovery)
Keyword (kelime aratması)
Parola Deşifresi

Bulunan suç unsurlarının değerlendirilmesi

"Bu aşamada elde edilen verilerden nelerin Adli Makamlara iletilmek üzere hazırlanacak rapora dahil olacağı, verilerin güvenli, zarar görmeden ve birebir değişmemiş halinin çıkartılmış olup olmadığının değerlendirilmesi ile kontrolü yapılmaktadır."

- Doğru ve Öz veriler
- Veri Bütünlüğü
- Anlaşılabilirliği

Değerlendirme (Evaluation)

Adli makamlar için elde edilen verilerin dökümante edilmesi

"Elde edilen ve değerlendirilmesi tamamlanmış verileri Adli makamlar tarafından soruşturmada kullanılmak üzere anlaşılır bir dilde raporlanması"

- Raporun dili ve İçeriği Anlaşılabilir olmalı
- Teknik terimler açıklanmalı
- Kesin ve Somut Veriler olmalı
- Delile Ulaşmak için kullanılan yöntemler anlatılmalı
- Yapılan Tüm işlemler ek bir raporda belirtilmeli

ADLİ BİLİŞİM ARAÇLARI

A.Hakan EKİZER
Komiser
Bilişim Suçları Uzmanı
ahmethakan@ekizer.net

EN ÇOK KULLANILANLAR

EnCase©

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

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

ILook

- Elliot Spencer - Programcı
- Amerikan Senatosu Tarafından Onaylı
- Adli Merciler ve Kolluk Kuvvetlerine Bedava
  - İmaj Alma
  - Delil Üzerinde İnceleme
  - Adli Merciler için Raporlama
- www.ilook-forensics.org

Image Master Solo

- ICS – Intelligent Computer Systems
- Hızlı BIT bazında kopyalama
- MD5 ve SHA1 ile Hash değeri
- Sadece Kopyalama yapar
- www.ics-iq.com

Logicube

- BIT bazında bire bir kopya
- HASH değeri alma
- IDE-SATA desteği
- www.logicube.com

Diğer Araçlar

- Fire Forensic Linux
- Helix Linux
- Penguen Sleuth Linux
- ‘Bedava’ CD den çalışabilen
- Açık Kaynak Kodlu Bir Çok aracı içerir.
- TASK – AutoSpy Forensic Yazılımları
- Otomatik Donanım tanıma ve Yazma koruması
- DD ve Diğer İmaj alma yazılımları
- Network Üzeriden Boot ile inceleme yapabilme

Yazma Koruma Cihazları

Drive Lock

Wiebetech

Notebook

Drive Lock

Wiebetech

Dosya Göstericileri

- IrfanView
- Ofiice View
- ACDSee
- Quick View Plus
- Outside In
- Disk Jockey 2000
- WhatFormat
- Paint Shop Pro

Bunlar En Çok Kullanılanlar. Bunların yanında bir çok firmanın farklı ürünleri mevcuttur.

EnCase ile Uygulama.

SHOWTIME ☺