

# Adli Bilişimin Temelleri (Fundamentals of Digital Forensics)

## İçerik

Adli Bilişim Kavramı, Tanımı ve Safhaları

Hukuki Mevzuat

Sayısal Delil ve İlk Müdahale Kavramı

İmaj Alma ve Hash Kavramı

İmajın İncelenmesi ve Elde Edilebilecek Bulgular

Rapor Yazımı

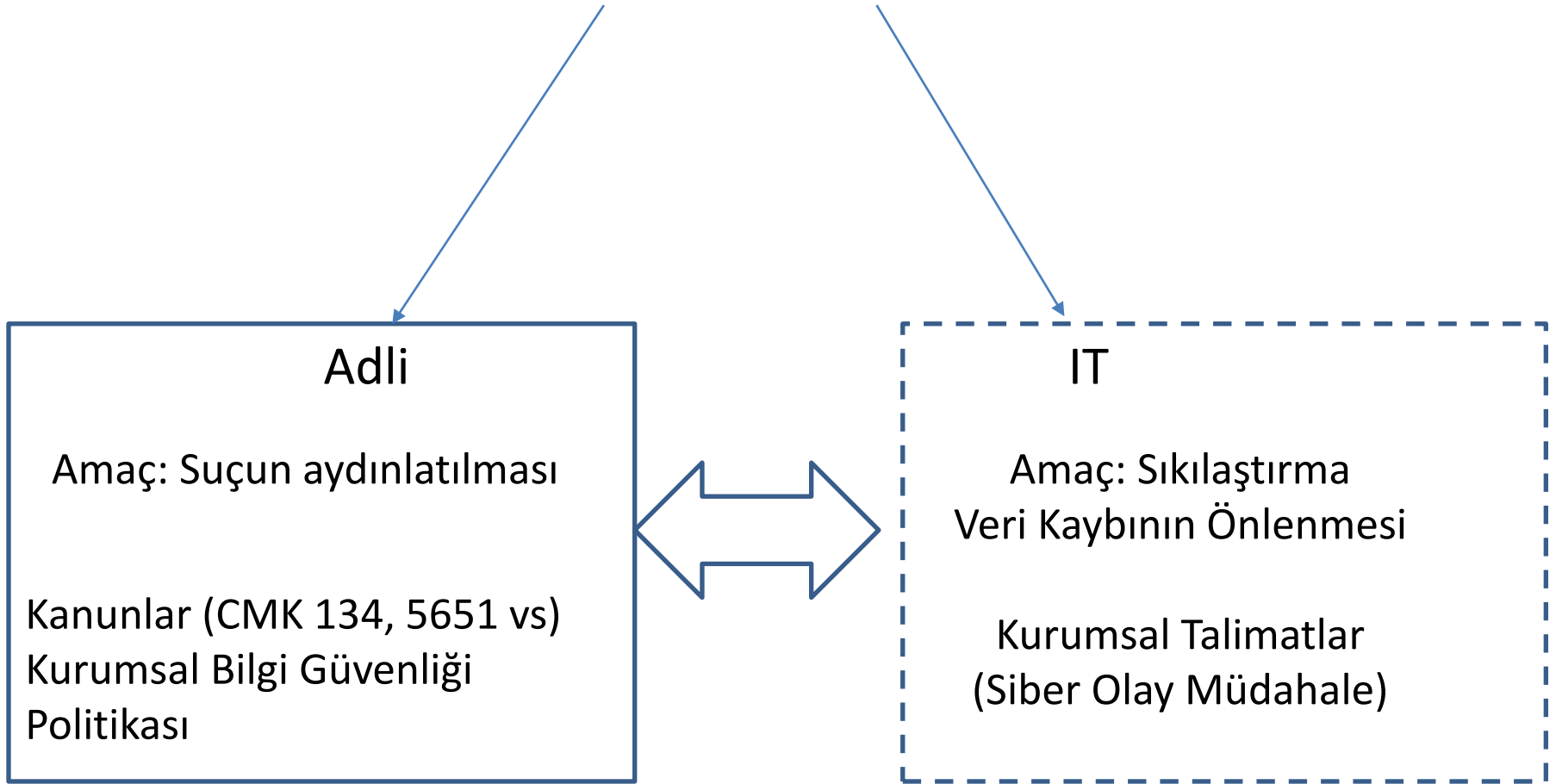
# Adli Bilişim Temel Eğitimi (Fundamentals of Digital Forensics)

# Adli Bilişim

## Tanım

Adli Bilişim, '*yargıya intikal etmiş*' bir olayla ilgili olarak potansiyel kanuni delillerin belirlenmesi için bilgisayar soruşturması ve analiz tekniklerinin bir uygulamasıdır

# Adli Bilişim



Bilişim öğelerinin içinde olduğu olayların aydınlatılması için hem kanuni hem de teknik bir altyapının gerekli olduğu kaçınılmazdır.

Bizler biliyoruz ki kimya, biyoloji(DNA), parmak izi, balistik gibi suçun aydınlatılmasında rol oynayan disiplinlerin teknik ve hukuki bir altyapısı oldukça eskidir.

Adli Bilişim de hem hukuk hem de bilişimin ortaklaşa kullanıldığı bir **ihtiyaç** olarak ortaya çıkmıştır. Diğer adli bilim dalları ile beraber birçok olayın aydınlatılmasında önemli rol oynamıştır.



# Locard'ın Değişim Teorisi

Her temas bir iz bırakır.



"Every contacts leaves a trace"  
Edmund Locard

İki cisim birbirine temas ettiğinde fiziksel bir izin yer değişim söz konusu olacaktır.

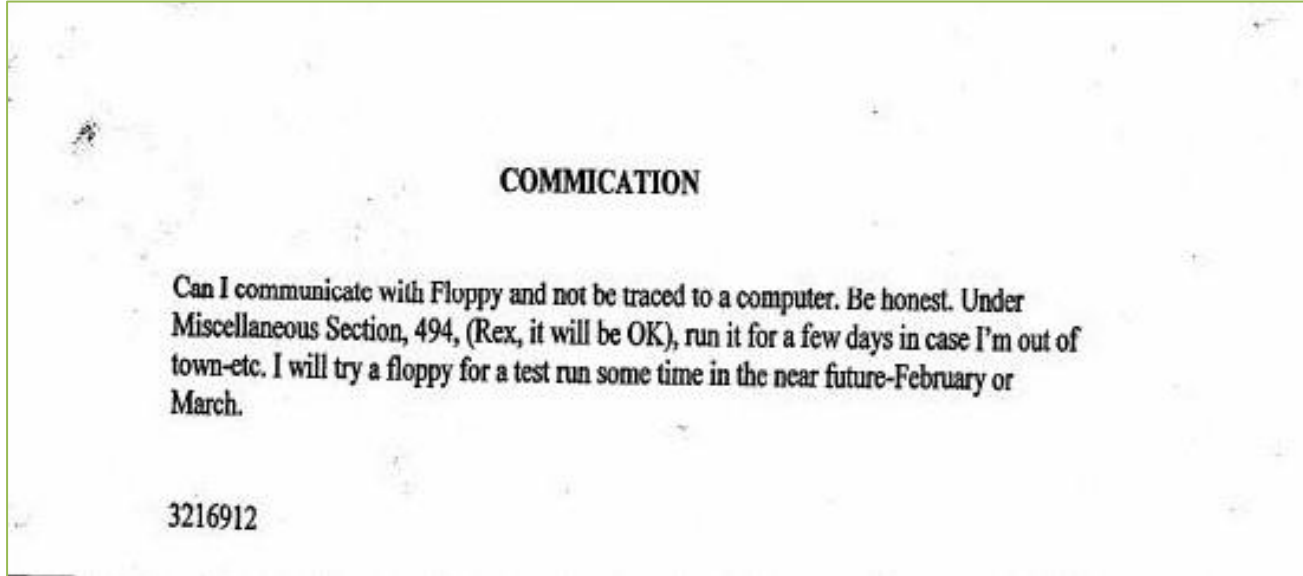
Örneğin hırsız Bir evde yani olay yerinde bir nesneye dokunduğunda parmak izi bırakabilir.

- Edmund Locard ,1910 yılıında bir izin forensic(adli bilim) açısından önemini vurgulamıştır. Locard, Fransada bulunan bir kriminal laboratuvarın yöneticisiydi.

- Edmond Locard modern adli bilimlerin öncüsü bilim adamı. "Fransız Sherlock Holmes" olarak tanınan Locard, "Her temas bir iz bırakır." diyerek, adli bilimlerin en temel prensibini açık ve kesin bir şekilde belirtmiştir.(Vikipedi)

## ÖRNEK-1

### *Adli Bilişim yöntemleri ile çözülen en önemli suç dosyası*



Google search: Btk killer,Dennis Lynn Rader

30 yıldır çözölemeyen bir dosya nasıl çözüldü? Peki incelenen delil neydi? Sadece bir disket



Silinmiş Word belgesi üstveri  
( EnCase Forensics Software)

### BTK Killer

- Onlarca vahşi cinayet,Otero ailesi katliamı
- Tam 30 yıl yakalanamayan seri katil
- Harcanan milyonlarca dolar ve binlerce saat
- Binlerce biyolojik,kimyasal,parmak izi gibi incelemeler
- Yüzlerce şüpheli şahıs ifadesi
- Katil tarafından polise gönderilen alay edici mektuplar, tuhaf bulmacalar

Ve nihayetinde bir disket....

Disketin **Adli Bilişim Uzmanlarınca** incelenmesi sonucu;

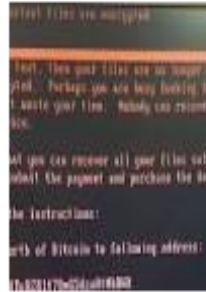
Silinmiş bir word belgesinin kurtarılması ve üst verisinde “Son kaydeden :Dennis” ibaresi ile “Christ Lutheran Church” ibaresinin tespiti sonucunda katilin yakalanması....



Bilişim öğeleri hayatımızın vazgeçilmez parçası haline gelmiştir. Günlük hayatımızı kolaylaştırmanın yanında bir suçun parçası (*doğrudan/dolaylı*) haline de gelebilmektedir.

## Aşk cinayetini bilgisayar çözecek

Üniversite öğrencisi ...  
...`in liseli sevgilisini  
öldürdükten sonra intihar  
etmesiyle ilgili soruşturma  
derinleşti.



Küresel çapta siber saldırılar birçok **şirketi** etkiledi

BBC Türkçe - 27 Haz 2017

Ukrayna'da başlayan kapsamlı siber saldırıların dünya çapında birçok şirkete yayıldığı bildiriliyor. Fidye yazılım kullanılarak siber saldırılar ...

Siber saldırı dünyayı sarmaladı

Sabah - 28 Haz 2017

Tümünü görüntüle

## Bilgisayarda 12 bin ço pornosu görüntüsü bu

Konya`da ...  
başkanının evindeki  
bilgisayarda çocuk  
 pornosu görüntüleri çıktı.  
35 kişinin sorgusu  
sürüyor..



WannaCry'dan Bile Daha Tehlikeli Bir **Fidye Yazılımı**, Binlerce ...

Webtekno - 28 Haz 2017

WannaCry'ın çalışma mantığına benzeyen Petya Fidye Yazılımı, ... gibi 80 şirketin sistemlerine yayılan Petya isimli fidye yazılımı, bir güvenlik ...

Yeni siber saldırı nasıl bulaşıyor? Nasıl korunabiliriz?

Görüşler - STAR - 27 Haz 2017

Tümünü görüntüle

Zaman zaman televizyonda, internette içerisinde bilişim öğelerinin olduğu çeşitli olaylar ile ilgili haberleri görüyorsunuz.

### Görüntüleri silmek istedi, başaramadı

Cinayetin işlendiği Bahçeşehir`deki villayı gösteren güvenlik kayıtları 4 gün sonra silinmek istendi. Tesadüfen ortaya çıkan tanığın ifadeleriyle bilgisayar incelendi Meçhul bir el kayıtları ö

2009-09-23 Sabah

### Katili belki de telefonda gizli

Engin Temel cinayetini aydınlatmaya çalışan polis, genç adamın ölümünden bir gün önce yaptığı telefon görüşmelerini incelemek için mahkemeye iki kez başvurdu. Ancak bu talepleri `özel hayatın

### TÜRKİYE - SON DAKİKA

önceki haber

güncellenme zamanı 19.35 | 13.5.2009

## Diyarbakır Tapu Müdürlüğü'ne rüşvet baskını

Canan ALTINTAŞ-Serdar SUNAR/DİYARBAKIR, (DHA)

DİYARBAKIR'da jandarmanın rüşvet alındığı ve yolsuzluk yapıldığı ihbarları üzerine Tapu Sicil Müdürlüğü'ne baskın yaptı, bilgisayar kayıtlarına el koydu

Diyarbakır İl Jandarma Komutanlığı Kaçakçılık ve Organize Suçlarla Şube Müdürlüğü, Tapu Sicil Müdürlüğü'nde rüşvet alındığı ve yolsuzluk yapıldığı ihbarları üzerine 4 ay önce teknik takip başlattı. Teknik takip ve yapılan araştırma sonucu Cumhuriyet Başsavcılığı'ndan alınan arama izniyle Tapu Sicil Müdürlüğü'ne bugün saat 17.00 sıralarında baskın yapıldı. Çok sayıda jandarma görevlileri binaya girerek arama yaparken personelin büyük bölümünün dışarıya çıkmasına da izin verilmedi. Diyarbakır Valiliği'nin arka kısmında bulunan bina çevresinde güvenlik önlemi alındı.

Jandarma ekipleri Tapu Sicil Müdürlüğü'nde bazı belgelere el koyarken, bilgisayar kayıtları ile hard disklerini de kopyaladı. El konulan belgeler jandarma görevlileri tarafından araçlara taşınırken, arama çalışmalarının geç saatlere kadar sürebileceği belirtildi.

Antalya Emniyet Müdürlüğü Kaçakçılık ve Organize Suçlarla Mücadele Bilişim Suçları Büro Amirliği ekipleri, Antalya ve İstanbul'da düzenlenen eş zamanlı operasyonda, 6'sı Antalya'da olmak üzere toplam 8 kişiyi yakaladı.

Zanlıların ikametlerinde, işyerlerinde, otolarında ve üzerlerinde yapılan aramalar sonucu; 1 adet kart kopyalamaya yarayan MSR Encoder cihazı, 35 adet, sahte oluşturulduğu belirlenen manyetik şeritli kart, 5 değişik bankaya ait pos cihazı, 2 dizüstü bilgisayar, 2 sahte sürücü belgesine el konuldu. Soruşturmanın sürdüğü bildirildi.

Tarih: 06 Eylül 2009 Pazar - 13:22



### Yol verme cinayeti güvenlik kamerasında

Yol verme inatlaşması nedeniyle çıkan kavgada 19 yaşındaki Hakan Eron'un sevgilisinin gözü önünde öldürülmesi güvenlik kamerasına yansdı.



+ Büyüt - Küçült

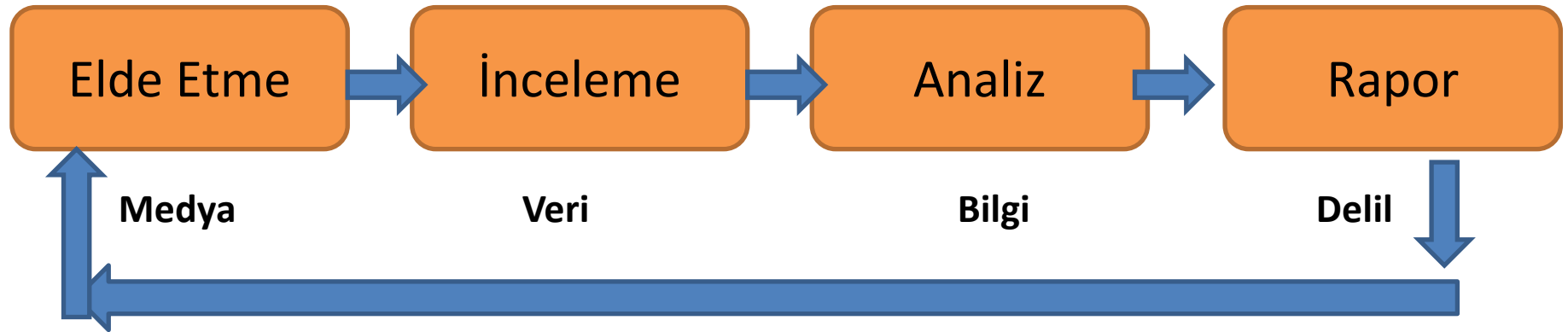
# Adli Biliřim Ařamaları

## Adli Bilişim;

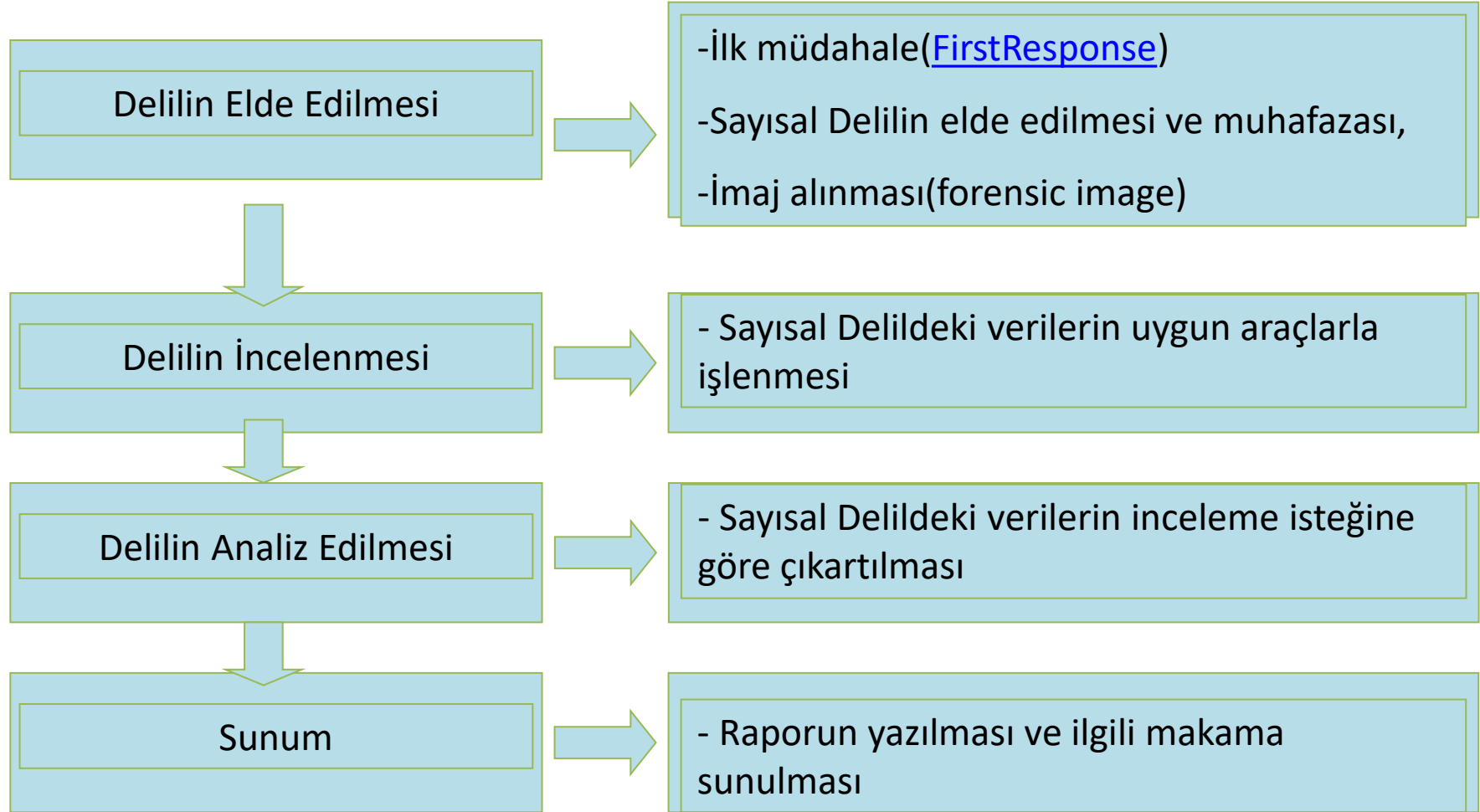
- \* Elde etme (Collection/Acquisition)
- \* İnceleme (Examination)
- \* Analiz etme (Analysis)
- \* Sunum/Rapor(Presentation/Reporting)

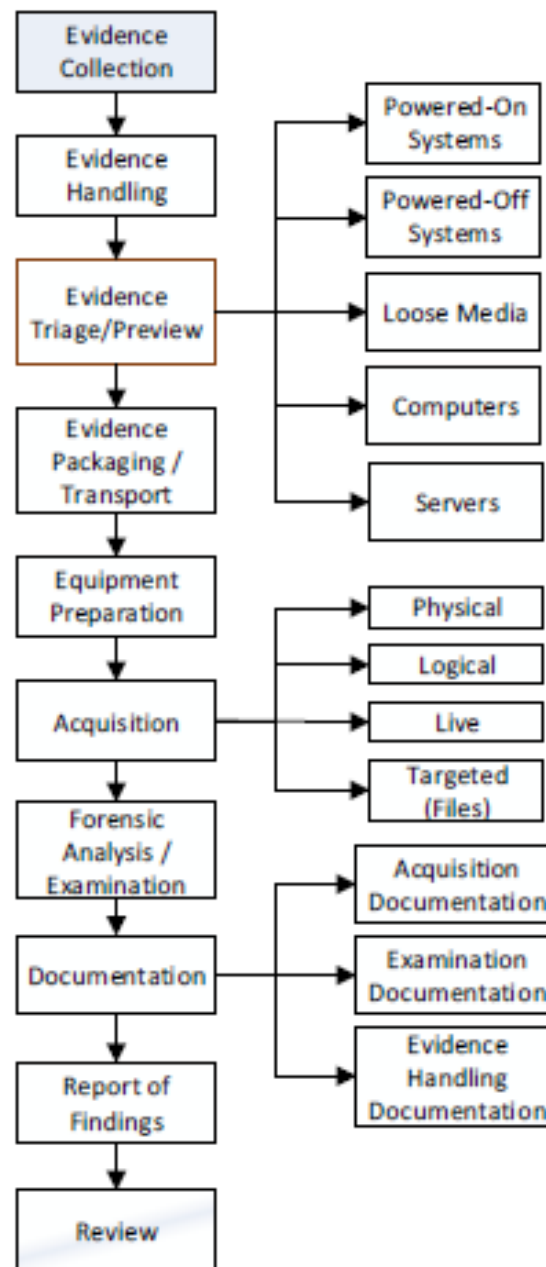
aşamasına kadar, delilin gereklerine uygun olarak uygulanmasıdır.

( [\*Guide to Integrating Forensic Techniques into Incident Response\*,bölüm:3-1](#) ,NIST)



*Diğer Adli Bilişim Aşama Modelleri*





## *SWGDE Best Practices*

SWGDE: Best Practices for Computer Forensics V3-1 (2014)

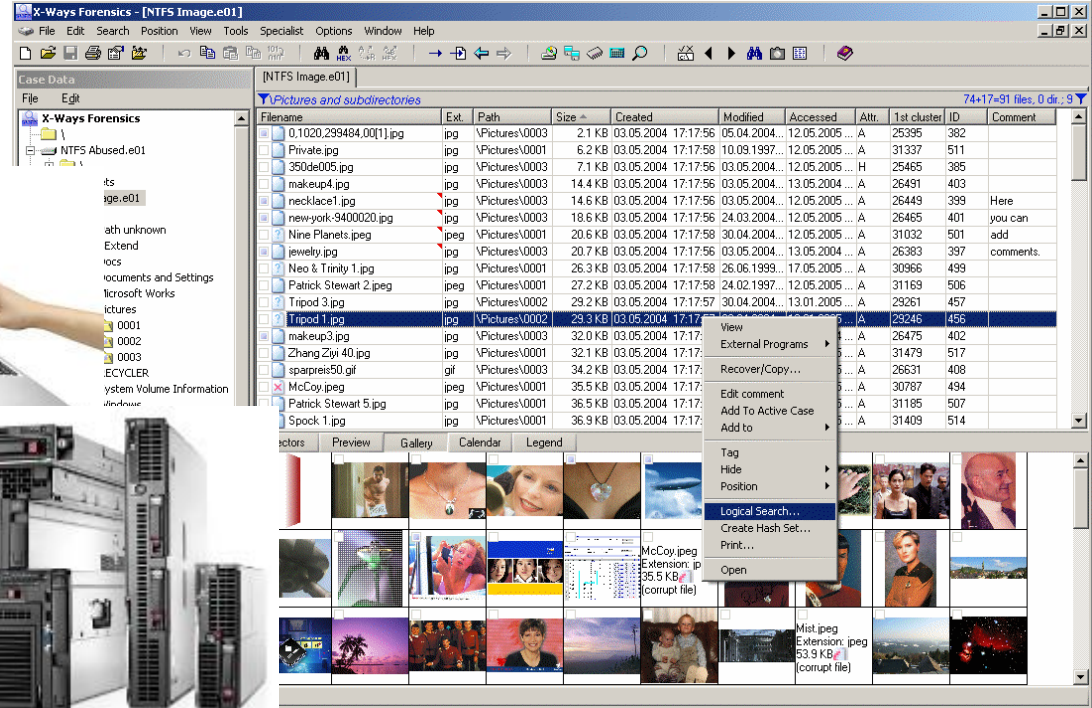
# Adli Bilişim Türleri



Adli Bilişim türlerini üç başlıkta gruplandırabiliriz...

- Computer Forensics (*Bilgisayarlarda Adli Bilişim*)

Bilgisayarlar ve bilgisayarlar kütüklerini kapsar. (*Harddisk, Disket, CD/DVD/USB Bellek , hafıza kartları, mp3 çalar, manyetik kart okuyucular vb.*)





## -Mobile Forensics (Mobil cihazlarda Adli Bilişim)

*Cep telefonu ve tablet gibi cihazları kapsar.*



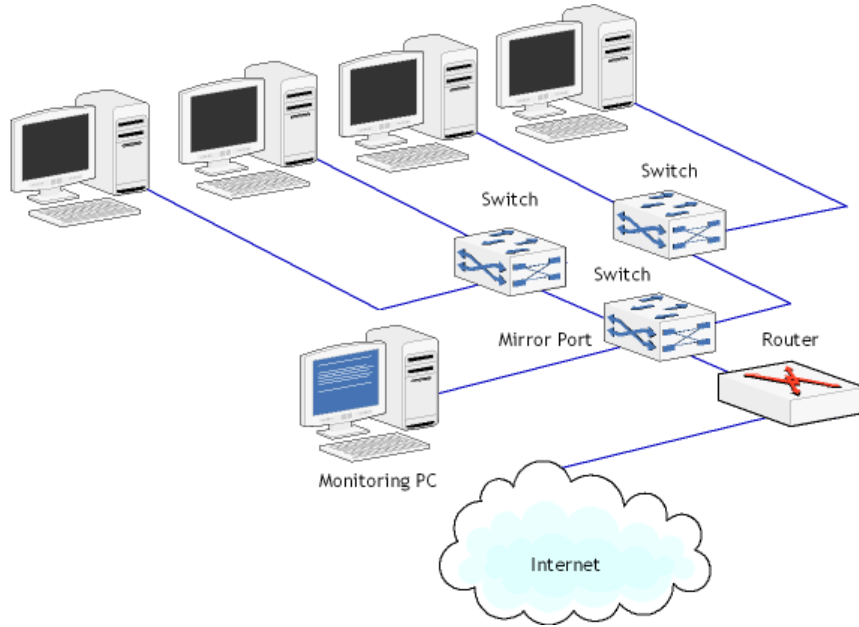
## SMARTPHONE IS A SMALL PC



<http://www.oxygen-forensic.com>

# Network Forensics (Ağ üzerinde Adli Bilişim)

*Ağ aygıtları, ağ üzerinde çalışan uygulamalar ve ağ aygıtların ürettiği kayıtları kapsar. (Network paketleri ve loglar)*



The image shows a Wireshark packet capture interface. The top menu bar includes View, Go, Capture, Analyze, Statistics, Telephony, Tools, Internals, and Help. Below the menu is a toolbar with various icons. The main display area shows a list of captured packets. The first packet is a TCP SYN packet from 192.168.1.19 to 216.49.88.118. The second packet is a TCP RST, ACK packet from 192.168.1.78 to 216.49.88.118. The third packet is a DNS Standard query from 192.168.1.227 to 208.48.15.13. The fourth packet is a DNS Standard query response from 208.48.15.13 to 192.168.1.19. The fifth packet is a TCP SYN packet from 192.168.1.19 to 208.48.15.13. The sixth packet is a TCP SYN, ACK packet from 208.48.15.13 to 192.168.1.19. The seventh packet is a TCP ACK packet from 192.168.1.19 to 208.48.15.13. The eighth packet is an HTTP GET request from 192.168.1.19 to 208.48.15.13. The ninth packet is a TCP ACK packet from 192.168.1.19 to 208.48.15.13. The tenth packet is a TCP segment of a reassembled PDU from 192.168.1.19 to 208.48.15.13. The eleventh packet is a TCP segment of a reassembled PDU from 192.168.1.19 to 208.48.15.13. The twelfth packet is a TCP ACK packet from 192.168.1.19 to 208.48.15.13.

No.	Time	Source	Destination	Protocol	Length	Info
1	0.000	192.168.1.19	216.49.88.118	TCP	62	192.168.1.19 → 216.49.88.118:80 [SYN] Seq=0 Win=16384 Len=0 MSS=1460
2	0.000	192.168.1.78	216.49.88.118	TCP	60	192.168.1.78 → 216.49.88.118:80 [RST, ACK] Seq=1 Ack=1 Win=0 Len=0
3	0.000	192.168.1.227	208.48.15.13	DNS	82	Standard query 0x9702 A updates.virtumonde.com
4	0.000	208.48.15.13	192.168.1.19	DNS	193	Standard query response 0x9702 A 208.48.15.13 A 208.48.15.13
5	0.000	192.168.1.19	208.48.15.13	TCP	62	192.168.1.19 → 208.48.15.13:80 [SYN] Seq=0 Win=16384 Len=0 MSS=1460
6	0.000	208.48.15.13	192.168.1.19	TCP	62	208.48.15.13 → 192.168.1.19:80 [SYN, ACK] Seq=0 Ack=1 Win=5840 Len=0
7	0.000	192.168.1.19	208.48.15.13	TCP	60	192.168.1.19 → 208.48.15.13:80 [ACK] Seq=1 Ack=1 Win=17520 Len=0
8	0.000	192.168.1.19	208.48.15.13	HTTP	201	GET /bkinst.exe HTTP/1.1
9	0.000	192.168.1.19	208.48.15.13	TCP	60	192.168.1.19 → 208.48.15.13:80 [ACK] Seq=1 Ack=148 Win=5840 Len=0
10	0.000	192.168.1.19	208.48.15.13	TCP	1514	[TCP segment of a reassembled PDU]
11	0.000	192.168.1.19	208.48.15.13	TCP	1514	[TCP segment of a reassembled PDU]
12	0.000	192.168.1.19	208.48.15.13	TCP	60	192.168.1.19 → 208.48.15.13:80 [ACK] Seq=148 Ack=2921 Win=17520 Len=0

# Adli Bilişim Türleri

- Windows Forensics*
- Linux Forensics*
- Mac Forensics*
- Database Forensics,*
- Internet Forensics,*
- Cloud computing forensics,*
- DVR/NVR/CCTV Forensics,*
- GPS Forensics*
- ???? Forensics*
- VS VS...*

**Adli Bilişim Nelere Cevap Arar?**

*-Örneğin;*

*-Bu bilgisayarda hangi facebook hesabında oturum açılmış?*

*-Bu bilgisayara takılan usb belleklerin seri numaraları nelerdir?*

*-Bu bilgisayarda sahte nüfus cüzdanı hazırlanmış mı?*

*-Bu sunucuya uzaktan oturum(RDP) açılmış mı? Açılmış ise hangi IP,ne zaman erişmiş?*

*-Silinmiş Excel belgelerinin kurtarılması...*

*-XXXXXXXXXX kredi kartı ile bu bilgisayardan harcama yapılmış mı?*

*-Xx-xxx tarihleri arasındaki kamera kayıtlarının çıkartılması...*

*-Şifreli dosyaları tespiti ve şifrelerinin kırılması/bulunması...*

*-Bu belge bu bilgisayarda mı oluşturulmuş?*

*-Whatsapp sohbet kayıtlarının çıkartılması...*

*-İnternet üzerinde xxx-xxx tarihleri arasında hangi sitelere erişilmiştir?*

- Bu bilgisayarda zararlı yazılım(trojan,keylogger) var mıdır?
  - Xxx muhasebe programı üzerinde manipölasyon yapılmış mıdır?
  - Sahte ATM düzeneği içerisinde kaydedilmiş kredi kartı bilgisi var mıdır?
  - GPS cihazında bulunan güzergah bilgisinin tespiti?
  - Hangi IP üzerinden port taraması yapılmıştır?
  - Cep telefonu üzerinden yapılan arama,mesaj,rehber bilgisinin tespiti...
  - Uzantısı değiştirilmiş dosyaların tespiti...
  - xxx.xxx.x.xxi p numarasında Google Drive upload edilen dokümanların tespiti...
  - Uninstall edilmiş programların listesi...
  - Bu bilgisayarda sahte web sitesi(fake,phishing) hazırlama kodları var mı?
  - Xx,yy,zz arama motorlarında hangi kelimeler aratılmıştır?
- gibi inceleme konusu ile ilgili istekler gelebilir.*

# Adli Bilişimin Kullanıldığı Birimler/Alanlar

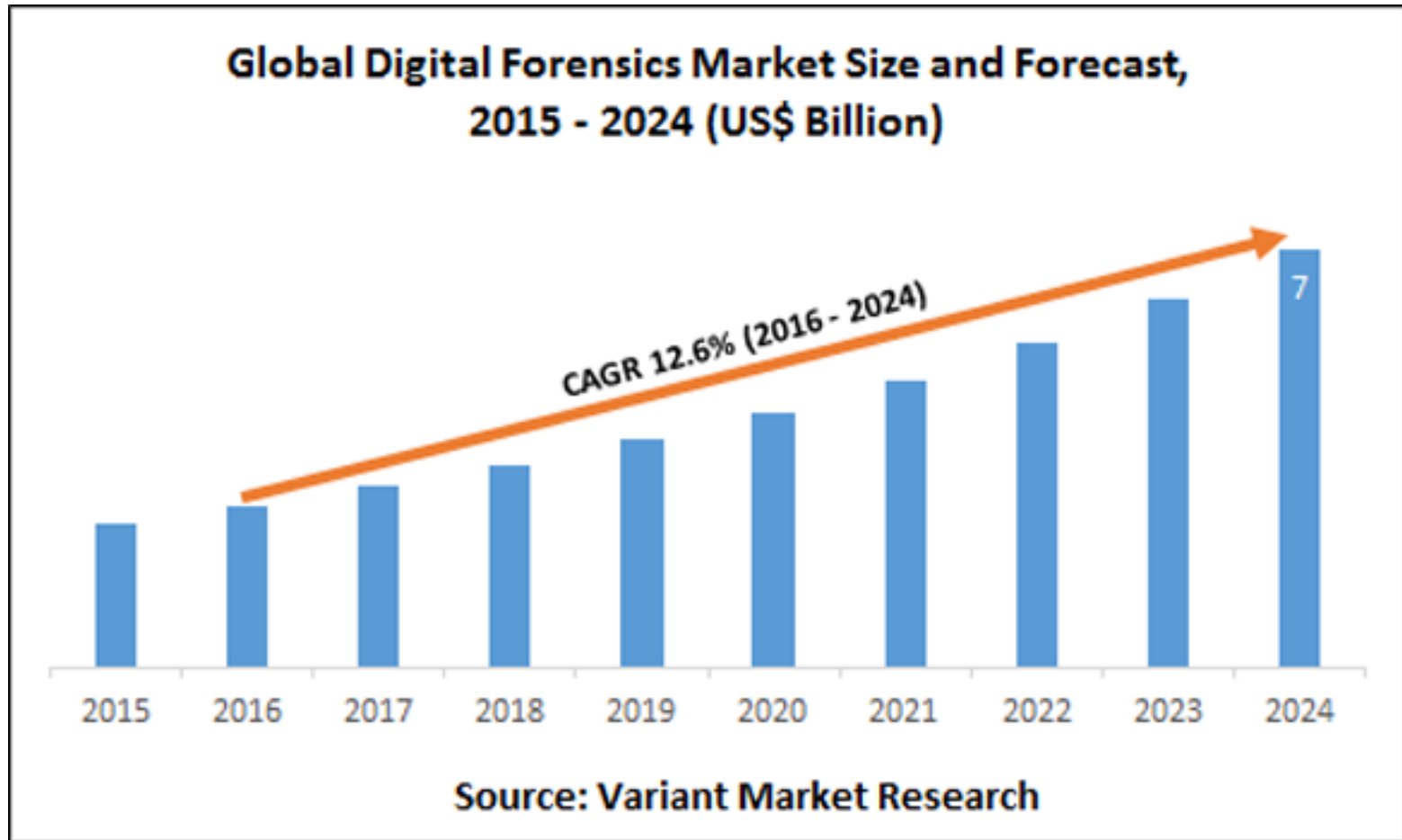
- Kolluk Birimleri (polis,jandarma)*
- Kriminal Laboratuvarları (Emniyet,Jandarma,Adli Tıp,FBI,NFI,BKA, [Özel lab.](#))*
- Adli Soruşturmalar/Yargılamalar(savcılık/mahkemeler)*
- İdari Soruşturmalar(kurumiçi/kamu/özel)*
- Kurumsal Bilgi Güvenliği (kurumiçi/kamu/özel)*
- Suiistimal İncelemesi(PwC,EY,KPMG)*
- [İç Denetim \(IT Auditing\)](#)*
- Güvenlik Operasyon Merkezi(SOC)*
- SOME(Siber Olaylara Müdahale Ekibi)*

# Adli Bilişim Sertifikaları

Sertifika Adı	Kuruluş
The Certified Computer Examiner (CCE)	International Society of Forensic Computer Examiners (ISFCE)
EnCase Certified Examiner (EnCE)	Guidance Software
The Certified Forensic Computer Examiner (CFCE)	The International Association of Computer Investigative Specialists (IACIS)
GIAC Certified Forensic Examiner (GCFE) GIAC Certified Forensic Analyst (GCFA) GIAC Reverse Engineering Malware (GREM) GIAC Network Forensic Analyst (GNFA) GIAC Advanced Smartphone Forensics (GASF)	SANS
CyberSecurity Forensic Analyst	The CyberSecurity Institute
Computer Hacking Forensic Investigator (CHFI)	EC Council
Certified Cyber Forensics Professional (CCFP)	ISC2
Certified Digital Forensics Examiner (CDFE) Certified Network Forensics Examiner (CNFE)	Mile2

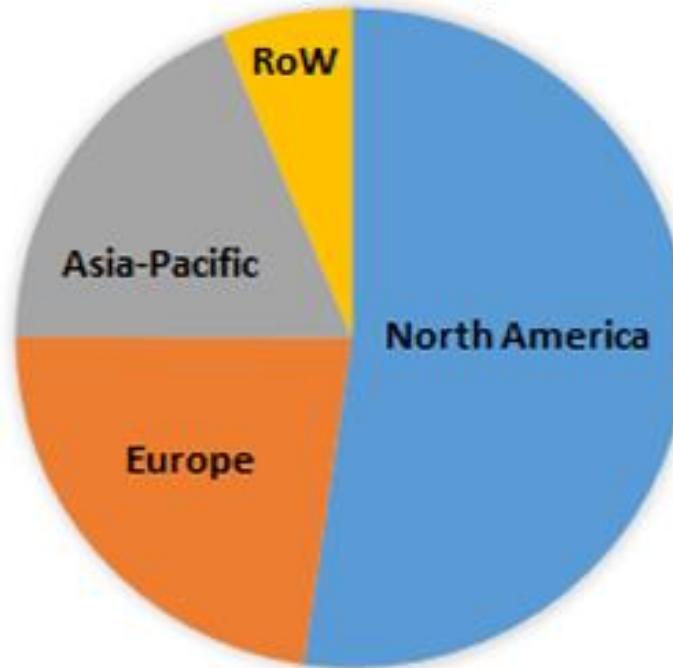


# Adli Bilişim Pazar Araştırması



# Adli Bilişim Pazar Araştırması-Bölgesel

**GLOBAL DIGITAL FORENSICS MARKET SHARE BY REGION,  
(VALUE%)**



**Source: Variant Market Research**

# Adli Bilişim Pazar Araştırması-Şirketler

- Global Digital Forensics,
- Binary Intelligence,
- LogRhythm, Inc.,
- ASR Data,
- Paraben Corporation,
- Guidance Software, Inc.,
- Access Data Group,
- FireEye Inc.,
- Digital Detectives and Lancope, Inc.

# Adli Bilişim Pazar Araştırması

## Tür ve Uygulama Alanları

- Network Forensics
  - Computer Forensics
  - Mobile device Forensics
  - Cloud Forensics
  - Database Forensics
- 
- Law Enforcement(Kolluk Birimler)
  - Healthcare(Sağlık)
  - Education(Eğitim)
  - Banking, Financial services & Insurance (BFSI)(Finans)
  - Information Technology(IT)
  - Transportation & Logistics(Ulaşım)
  - Defense & Aerospace(savunma)

# Adli Bilişim Ürünleri Kullanan Bazı Kuruluşlar

## Guidance Software Customers



# Adli Bilişim Ürünleri Kullanan Bazı Kuruluşlar

Guidance Software Customers



SAMSUNG



HUNTSMAN



Sprint

Southwest

LOWE'S

IBM

DUPONT

CBS

starwood  
Hotels and  
Resorts

Microsoft

BEST  
BUY

GAP

facebook



# Sayısal Delil Kavramı

Sayısal delil: Digital Evidence, Electronic Evidence, Electronically Stored Information (ESI)

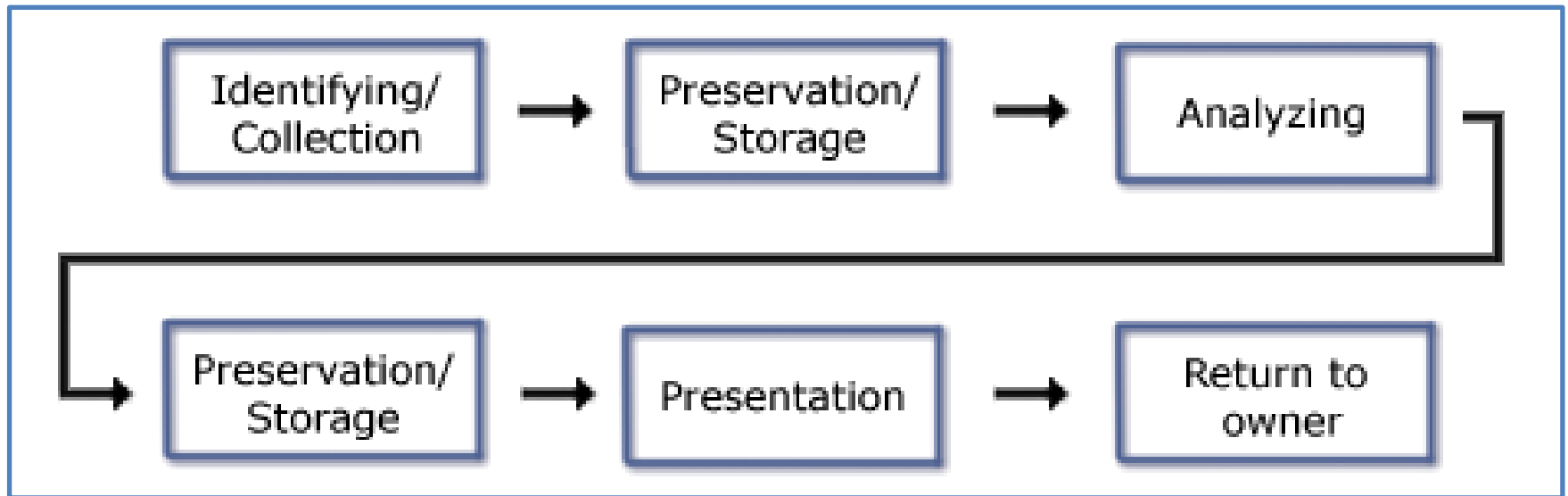
**Sayısal delil:** Sayısal (elektronik) biçimde iletilen veya saklanan, ispat kuvveti olan bilgidir.

Adlî Bilişim Soruşturmasında elektronik ortamda bulunan bilgiler kolaylıkla manipüle edilebilir olduğundan bu bilgilerin delil sayılabilmesi için bir takım kanuni prosedürlerin geçirilmesi gerekmektedir.

Bu prosedürler delilin alınmasından *mahkemeye* sunulmasına kadar geçen bir süreci(chain of custody, emanet zinciri) içermektedir.



Delilin yaşam döngüsü diyebileceğimiz bu süreç delillerin toplanması, tanımlanması, saklanması, korunması, ulaştırılması, mahkemede sunulması ve sahibine dönmesini kapsamaktadır



# Sayısal Delilin 5 Kuralı

1-Kabul Edilebilir (Admissible) : Hukuka uygun olarak elde edilmelidir.

*\*yapılan işlemler kayıt altına alınmalı...*

2- Doğrulanabilir (Authentic): İçerik değişmeden kaldığı gösterilebilmeli..

*\*Hash değeri ile gösterilebilir.*

3-Eksiksiz(Complete):Sadece suçluluğu değil suçsuzluğu da kapsamalıdır.

*Örnek.....: xxxx web sitesine girilmiş mi? Evet girilmiş...ama yönlendirme var..URL REDR*

4-Güvenilir (Reliable): Şüphe edilmemeli,tekrarlanabilmeli...

*\*eğer edilirse başkası yeniden inceleyebilir.*

5-İnanılır (Believable): ispat gücü olmalıdır.

*\*başka verilerle desteklenebilir.*

# Sayısal Delil Prensipleri

- 1- Kolluk kuvvetlerinin/IT personelinin -daha sonra- mahkemeye verilecek olan verileri değiştirmemesi gerekmektedir.
- 2- Bir kişinin orijinal verilere erişmek için gerekli gördüğü durumlarda, bu kişi bunu yapmak için yetkin olmalı ve eylemlerinin geçerliliğini ve etkilerini açıklayan bir kanıt sunabilmelidir.
- 3- Sayısal delillere uygulanan tüm süreçlerin bir denetim kayıtları veya başka bir kaydı olmalıdır. Bağımsız bir üçüncü taraf bu süreçleri inceleyip aynı sonucu elde edebilmelidir.
- 4- Soruşturmadan sorumlu kişi, kanunun ve bu ilkelere uyulmasının sağlanmasından genel olarak sorumludur.

\*ACPO Good Practice Guide for Digital Forensics

# Sayısal Delil Prensipleri

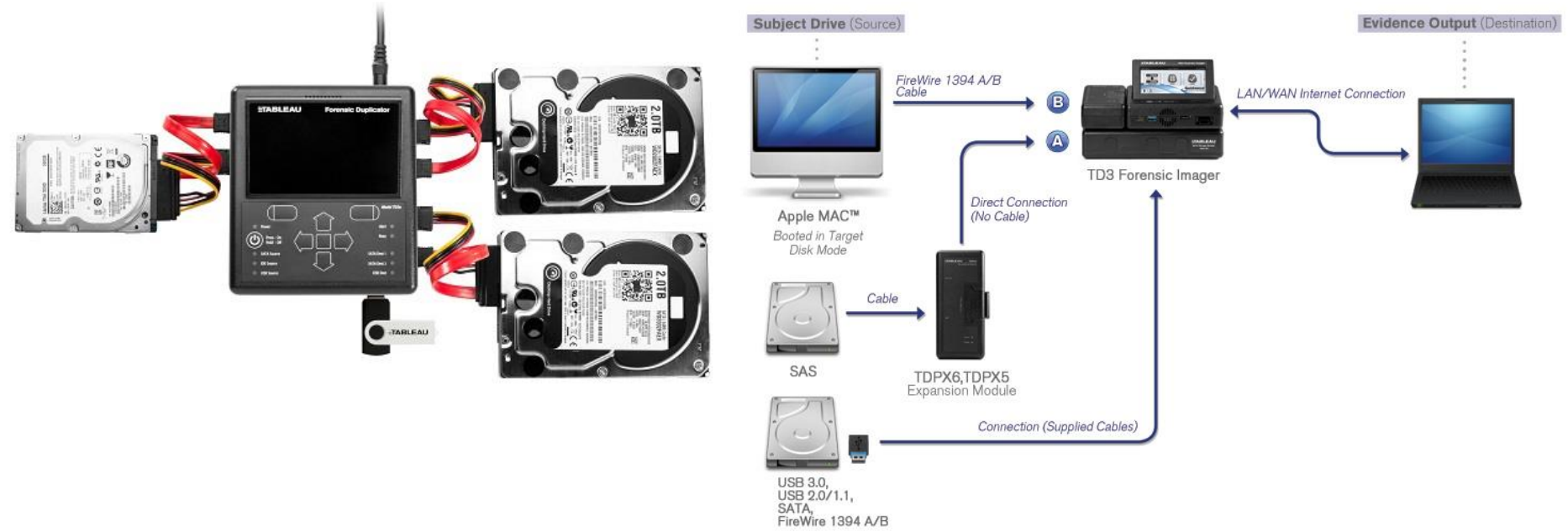
- İşletim sistemleri ve diğer programlar sıklıkla elektronik(veri) depolama içeriğini değiştirir, ekler ve siler. Bu, kullanıcının verileri değiştirdiğinin farkında olmadan otomatik olarak gerçekleşebilir.(Heisenberg'in Belirsizlik ilkesi)

Tüm bilgileri bir bilgisayardan aslında imkansızdır. Bunu Heisenberg'in veri toplama ve sistem analizi ilkesi olarak adlandırıyoruz. Bellek, süreçler ve dosyalar o kadar hızlı değişebilir ki bu değişimlerin tamamının doğru ve zamanında kaydetmek mümkün değildir.

Disk Etkinliği						
2575 KB/sn Disk G/Ç						
%71 En Uzun Etkinlik Süresi						
Resim	PID	Dosya	Oku (...)	Yaz (B/sn)	Toplam (B/...	G/Ç Önceliği
System	4	C:\	0	69	69	Arka Plan
System	4	C:\\$BitMap (NTFS Boş Al...	0	876	876	Arka Plan
System	4	C:\\$Extend\\$\UsnJrnl:\$J	0	308	308	Arka Plan
System	4	C:\\$LogFile (NTFS Birim G...	0	9.238	9.238	Normal
chrome.exe	6268	C:\\$LogFile (NTFS Birim G...	0	1.095	1.095	Normal
dllhost.exe	8188	C:\\$LogFile (NTFS Birim G...	0	4.779	4.779	Normal
svchost.exe (L...	1176	C:\\$LogFile (NTFS Birim G...	0	2.458	2.458	Normal
svchost.exe (ut...	2552	C:\\$LogFile (NTFS Birim G...	0	636	636	Normal
SearchIndexer....	6548	C:\\$Mft (NTFS Ana Dosya...	2.048	0	2.048	Normal
SearchUI.exe	6180	C:\\$Mft (NTFS Ana Dosya...	33.792	0	33.792	Normal
backgroundTa...	5856	C:\\$Mft (NTFS Ana Dosya...	16.384	0	16.384	Normal
explorer.exe	5816	C:\\$Mft (NTFS Ana Dosya...	4.096	0	4.096	Normal
perfmon.exe	5892	C:\\$Mft (NTFS Ana Dosya...	332	0	332	Normal
ctfmon.exe	5588	C:\\$Mft (NTFS Ana Dosya...	819	0	819	Normal
svchost.exe (L...	1176	C:\\$Mft (NTFS Ana Dosya...	819	0	819	Normal
System	4	C:\\$Mft (NTFS Ana Dosya...	819	9.402	10.221	Normal
System	4	C:\\$Mft::\$BITMAP	0	147	147	Arka Plan
Memory Comp...	1804	C:\pagefile.sys (Disk Bell...	65.536	0	65.536	Normal
RuntimeBroke...	6412	C:\pagefile.sys (Disk Bell...	28.087	0	28.087	Normal

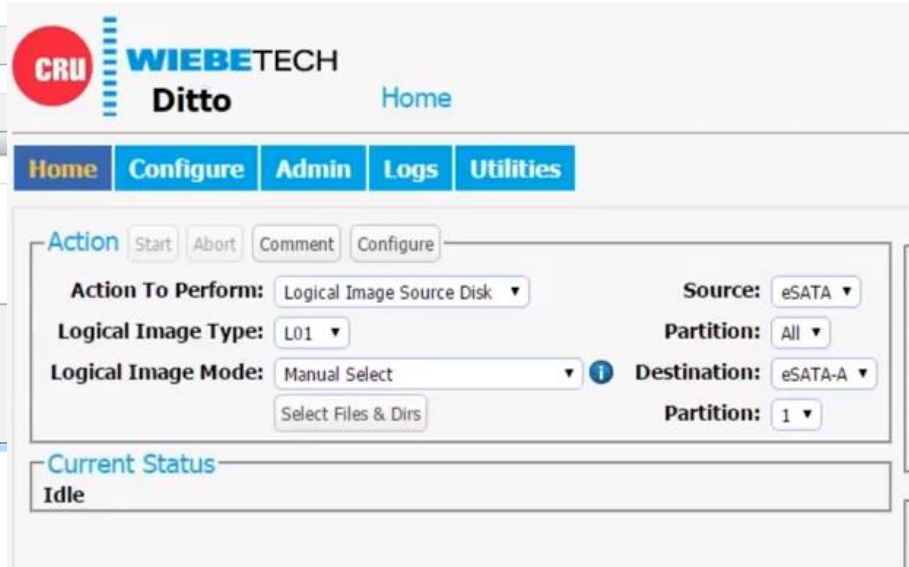
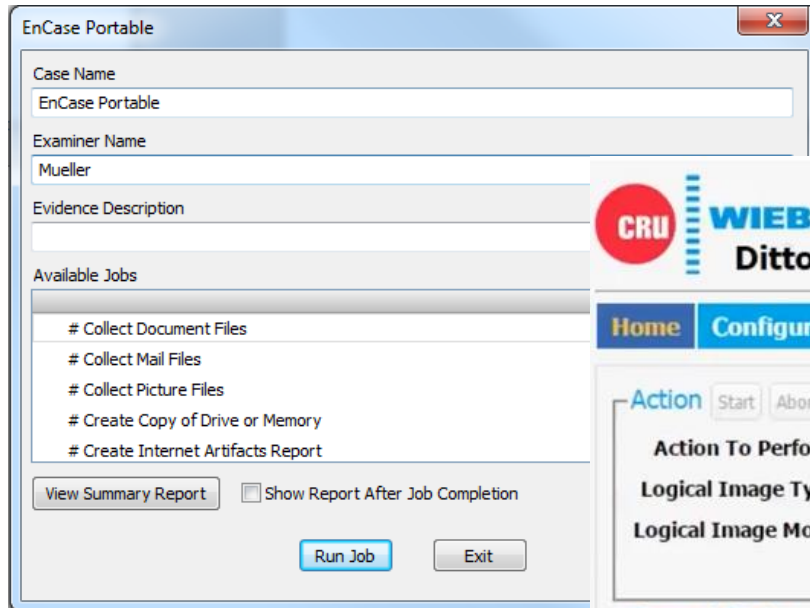
# Sayısal Delil Prensipleri

- Sayısal delil prensiplerine uymak için, mümkün olan her durumda veri depolama cihazının (hdd, usb vs) imajının alınması yapılması gerekir. Bu, orijinal verinin korunmasını ve bağımsız bir üçüncü tarafın yeniden incelemesini ve ilke 3'ün gerektirdiği gibi aynı sonucu elde etmesini sağlayacaktır.



# Sayısal Delil Prensipleri

- Bu, tüm aygıtın fiziksel / mantıksal bir blok imajı veya kısmi veya seçici veri içeren (bir triyaj işleminin sonucu olarak yakalanabilen) mantıksal bir imajı olabilir. Adli Bilişim Uzmanı veya sorumlular, bu yaklaşım benimsenirse tüm ilgili kanıtları ele geçirmeye gayret etmek için mesleki yargılarını kullanmalıdır. (CMK'da bu durumdan bahsedilmiş.)



## AutoSelect Mode

- Logically image only those files of interest to you
- Specify file types (e.g. JPG, XLS, etc.) that Ditto and Ditto DX will automatically search for while performing a logical image

[How to Target Specific File Types For A Logical Image with Ditto & Ditto DX](#)

# Sayısal Delil Prensipleri

-Lokal olarak depolanmayan ancak uzak bir yerde depolanan, muhtemelen erişilemeyen bir yerde saklanan verilerde, bir imaj/adli kopya elde etmek mümkün olmayabilir. Orijinal verilere doğrudan erişilmesi gerekli olabilir.

facebook

Kolluk Kuvvetleri Çevrimiçi Talepler



## Request Secure Access to the Law Enforcement Online Request System

We disclose account records solely in accordance with our terms of service and applicable law.

If you are a law enforcement agent or emergency responder who is authorized to gather evidence in connection with an official investigation or in order to investigate an emergency involving the danger of serious physical injury or death, you may request records from Facebook through this system.

☐ I am an authorized law enforcement agent or government employee investigating an emergency, and this is an official request

Erişim İste

Warning: Requests to Facebook through this system may be made only by governmental entities authorized to obtain evidence in connection with official legal proceedings pursuant to Title 18, United States Code, Sections 2703 and 2711. Unauthorized requests will be subject to prosecution. By requesting access you are acknowledging that you are a government official making a request in official capacity. For further information please review the [Emniyet teşkilatı kuralları](#).

# Sayısal Delil Prensipleri

- Başka bir yargı bölgesinde yer alan veriler elde edilirse, ilgili mevzuata da ayrıca dikkat edilmelidir.

*Başlık 4 – Depolanmış bilgisayar verilerinin aranması ve bunlara el konulması*

## **Madde 19 – Depolanmış bilgisayar verilerinin aranması ve bunlara el konulması**

1. Taraflardan her biri, kendi ülkesindeki yetkili makamların,
  - a. bir bilgisayar sisteminin tamamını veya bir kısmını ve içerisinde depolanmış bilgisayar verilerini; ve
  - b. bilgisayar verilerinin depolanmış olabileceği bir bilgisayar verileri depolama aygıtını arama ve benzer şekilde bunlara erişme yetkisine sahip olmaları için gerekli olabilecek yasama tedbirlerini ve diğer tedbirleri kabul edecektir.
2. Taraflardan her biri, paragraf 1.a uyarınca, makamlarının özel bir bilgisayar sisteminin tamamını veya bir kısmını araması veya benzer şekilde bunlara erişim sağlaması sözkonusu olduğunda ve aranan verilerin kendi ülkesindeki başka bir bilgisayar sisteminin tamamında veya bir kısmında depolanmış olduğuna inanmak için gerekçeleri bulunduğu ve sözkonusu veriler yasalara uygun biçimde ilk sistemden erişilebilir veya ilk sistem için kullanılabilir olduğunda, makamlarının arama veya benzer şekilde sisteme erişim işlemlerini süratle diğer sisteme teşmil edebilmelerini sağlamak için gerekli olabilecek yasama tedbirlerini ve diğer tedbirleri kabul edecektir.



# Sayısal Delil Prensipleri

- Bir mahkemede nesnelliği, ayrıca sürekliliği ve bütünlüğünü sergilemek esastır. Kanıtların nasıl elde edildiğini göstermek de gereklidir. Kanıtlar, üçüncü bir tarafın aynı süreci tekrarlayabileceği ve mahkemeye sunulanla aynı sonuca varabileceği ölçüde korunmalıdır.

# Sayısal Deliller

# Sayısal Deliller

Dijital cihazların çoğalması ve dijital iletişimdeki ilerlemeler, sayısal delillerin şimdi hemen hemen her suçta mevcut veya potansiyel olarak mevcut olduğu anlamına gelir.

Sayısal deliller bir dizi farklı yerde bulunabilir:

- Son kullanıcı cihazında yerel olarak - tipik olarak bir kullanıcının bilgisayar, mobil / akıllı telefon, uydu navigasyon sistemi, USB flash sürücü veya dijital kamera;
- Halka açık(public) olan uzak bir kaynak üzerinde - örneğin sosyal ağlar, tartışma forumları ve haber grupları için kullanılan web siteleri;

# Sayısal Deliller

- Özel(private) bir uzak kaynakta - bir İnternet Servis Sağlayıcısının kullanıcı etkinliklerinin günlükleri, bir mobil telefon şirketinin müşterinin fatura kayıtları, bir kullanıcının web posta hesabı ve bir kullanıcının uzak dosya depolama alanı;
  - Transit - örneğin cep telefonu kısa mesajları veya sesli çağrılar, e-postalar veya internet sohbeti.
- \* Bir suçun yukarıda belirtilen yerlerden birden fazlasında olduğuna dair kanıtlar oldukça yaygındır. Ancak, kanıtları bir diğerinden ziyade bir yerden elde etmek daha kolay olabilir; Kanıtların elde edilmesi için gerekli kaynaklara dikkat edilmelidir.

# Sayısal Delil Nereden Elde Edilir?

## 1-Bilgisayarlar

Klasik anlamda donanım ve yazılım bileşenlerine sahip klavye,fare,monitör,kasa(anakart, işlemci, bellek, hdd sürücü) gibi birimlerden oluşan sistem. Bilgisayarlar masaüstü,dizüstü,rack-mounted,minibilgisayar,mainframe,all-in-one, anabilgisayar gibi çeşitlerden oluşabilir.



## Potansiyel Deliller

Bilgisayarlar ve bileşenleri bir soruşturmada değerli bir delil olabilir. Bilgisayardaki donanımlar,yazılımlar,belgeler, fotoğraflar, yedekleme dosyaları, işletim sistemine özgü dosyalar, log dosyaları, veritabanları,e-postalar, finans verileri, internet geçmişi verileri, sohbet kayıtları, olay günlükleri gibi veriler birer potansiyel delildir.

# Sayısal Delil Nereden Elde Edilir?

## 2-Veri Depolama Birimleri(Data Storage Units)

### 2.1-Sabit Diskler(Fixed Hdd)

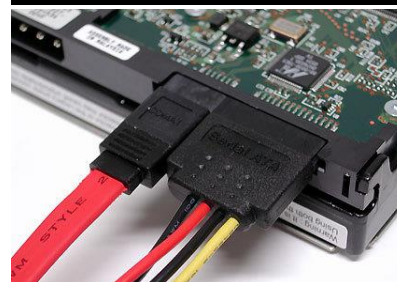
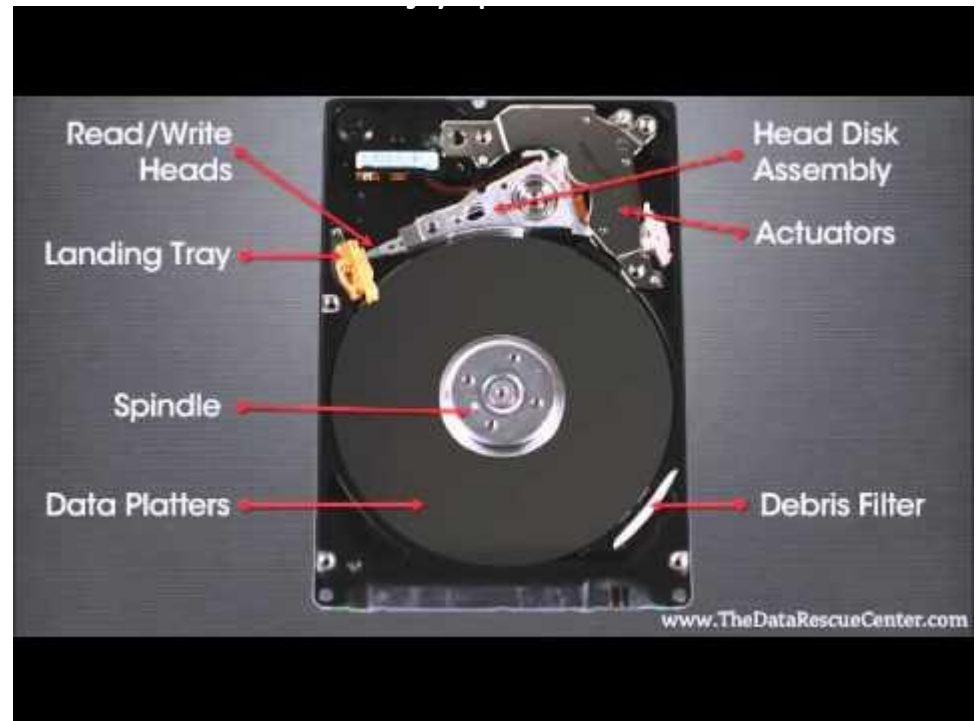
Sabit diskler kasa içerisinde veri ve güç bağlantıları yapılmış veri depolama birimleri olarak karşımıza çıkmaktadır. Olay yerinde bilgisayara bağlantısı yapılmamış sabit diskler de bulunabilir.



Bağlantı arayüzlerine (interface) göre IDE, SATA, SCSI, SAS sabit diskleri kullanılmaktadır.

SSD(Solid State Sürücü)'ler de veri depolamada kullanılmakta,SATA arayüzü ile bağlanmaktadır. Ancak içerisinde bir disk-plaka bulunmamaktadır. USB bellekler gibi NAND Flash depolama teknolojisi Kullanmaktadır.

# Sayısal Delil Nereden Elde Edilir?



# Sayısal Delil Nereden Elde Edilir?

## 2-Veri Depolama Birimleri(Data Storage Units)

### 2.2-Harici Sabit Diskler(External Hdd)

Bilgisayara Kablosuz, USB, Firewire, Ethernet portları üzerinden bağlanan,harici güç isteyen veri depolama birimleridir. Daha çok veri yedeklemek amacı ile kullanılır.



3.5" Hard drive



2.5" Hard drive



Network storage device





# Sayısal Delil Nereden Elde Edilir?

## 2-Veri Depolama Birimleri(Data Storage Units)

### 2.3-Çıkarılabilir (Removable) Depolama Birimleri

Çıkarılabilir depolama birimleri daha çok veri depolama, taşıma,arşivleme amaçlı olarak kullanılmaktadır.



# Sayısal Delil Nereden Elde Edilir?

## 2-Veri Depolama Birimleri(Data Storage Units)

### 2.4-USB Bellek(Thumbdrive)

USB bağlantı noktası üzerinden kullanılan çıkarılabilir veri depolama birimleridir.



# Sayısal Delil Nereden Elde Edilir?

## 2-Veri Depolama Birimleri(Data Storage Units)

### 2.5- Hafıza Kartları (Memory Cards)



Veri depolama birimleri de sabit diskler gibi belgeler, fotoğraflar, yedekleme dosyaları, log dosyaları, veritabanları, e-postalar, finans verileri, internet geçmişi verileri, sohbet kayıtları, olay günlükleri gibi veriler i içerebilir.

# Sayısal Delil Nereden Elde Edilir?

## 3-Mobil Cihazlar(Mobile/Handheld Devices)



## Potansiyel Deliller

Rehber, arama kayıtları, belgeler, fotoğraflar, videolar, veritabanları, e-postalar, finans verileri, internet geçmişi verileri, sohbet kayıtları, GPS gibi veriler i içerebilir.

# Sayısal Delil Nereden Elde Edilir?

## 4-Çevre Aygıtları(Peripheral Devices)

Çevre aygıtları kullanıcının bilgisayarın fonksiyonlarına erişmek ve daha etkin kullanmak amacı ile bilgisayara bağlantısı yapılan aygıtlardır.Klavye, fare ,yazıcı,scanner,faks, kart okuyucu...



## Potansiyel Deliller

Cihazların veri depolama imkanları eğer varsa fonksiyonlarına göre veriler tespit edilebilir. Ayrıca parmak izi incelemesi de yapılabilir. Yazdırılan belgeler, tarana belgeler, gelen-giden faks bilgisi gibi veriler tespit edilebilir.

# Sayısal Delil Nereden Elde Edilir?

## 5-Diğer Potansiyel Delil Olabilecek Cihazlar

Olay yerinde veri depolama özelliği olan ve potansiyel delil olabilecek elektronik cihazlara dikkat edilmelidir.

- Dijital Kameralar, Fotoğraf makinası
- Ses kaydedici cihazlar
- DVR (Digital Video Recorder)/NVR/CCTV
- MP3 çalar
- Oyun konsolu
- Sim kart
- Manyetik Kart Okuyucu (Mini123,MSR206)

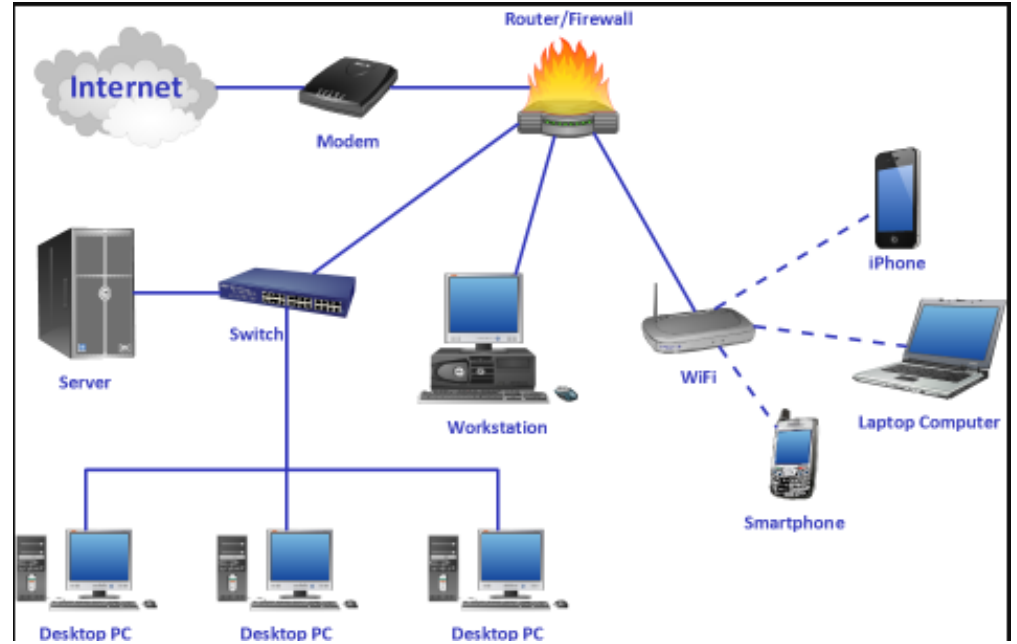
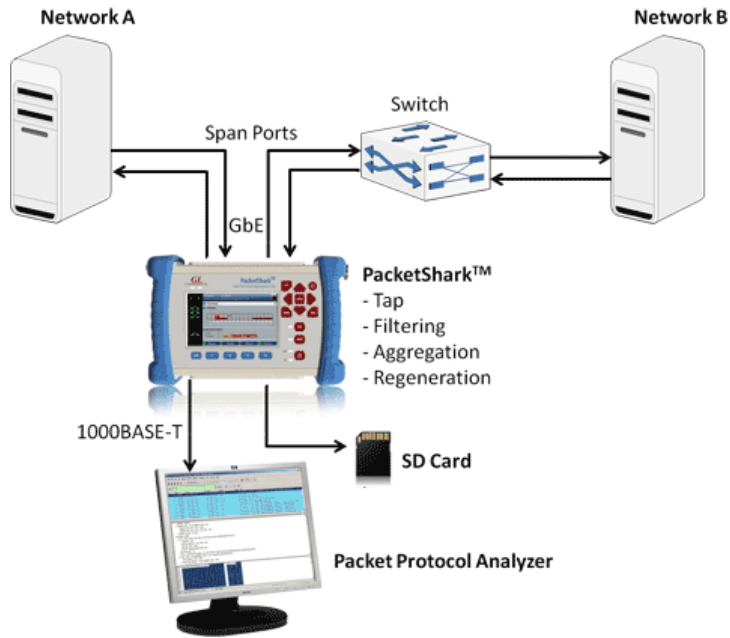
## Potansiyel Deliller

Cihazların veri depolama imkanları eğer varsa fonksiyonlarına göre veriler tespit edilebilir. Ayrıca parmak izi incelemesi de yapılabilir. DVR , tarih ve saat bilgisine göre kamera kayıtları tespit edilebilir.



# Sayısal Delil Nereden Elde Edilir?

## 6-Bilgisayar Ağları(Networks)



Potansiyel  
Deliller

Ağda kullanılan bilgisayarlardaki veriler, ağ cihazlarının kapasitesine bağlı olarak ürettiği kayıtlar(log) delil olarak incelenebilir. \*Firewall,IDS/IPS,Web server logları vs

# Sayısal Delil

Fiziksel Cihaz

Fiziksel Cihazın Bire-Bir kopyası(Fiziksel)

Fiziksel Cihazın Bire-Bir kopyası(Mantıksal)

Fiziksel Cihazın Kısmi içeriği (dosya/klasör)

Fiziksel Cihazın Ürettiği Kayıtlar(Log)



İlk Müdahale (First Response)

# Sayısal Delillere İlk Müdahale

## Genel Prensipler

- 1- Olay yerinin güvenliği alınır. Bunu genellikle kolluk birimleri yapar. Kurumsal bir şirkette bu işlemi İlk Müdahale eğitimi almış ve yetkili bir bilişim uzmanı(SOME) yapabilir. Burada güvenlik almada amaç delillerin karartılmasını/yok edilmesini/bozulmasını engellemektir.
- 2-Deliller muhafaza altına alınmalı,fotoğraflanmalı ve tutanağa geçirilmelidir.
- 3-Yetkisiz kişiler olay yerine yaklaştırılmamalı ve bu kişilerden yardım alınmamalıdır.
- 4-Eğer olay yerinde bilgisayar kapalı vaziyette bulunmuş ise kapalı olarak kalmalı, açılmamalıdır.

# Sayısal Delillere İlk Müdahale

## Genel Prensipler

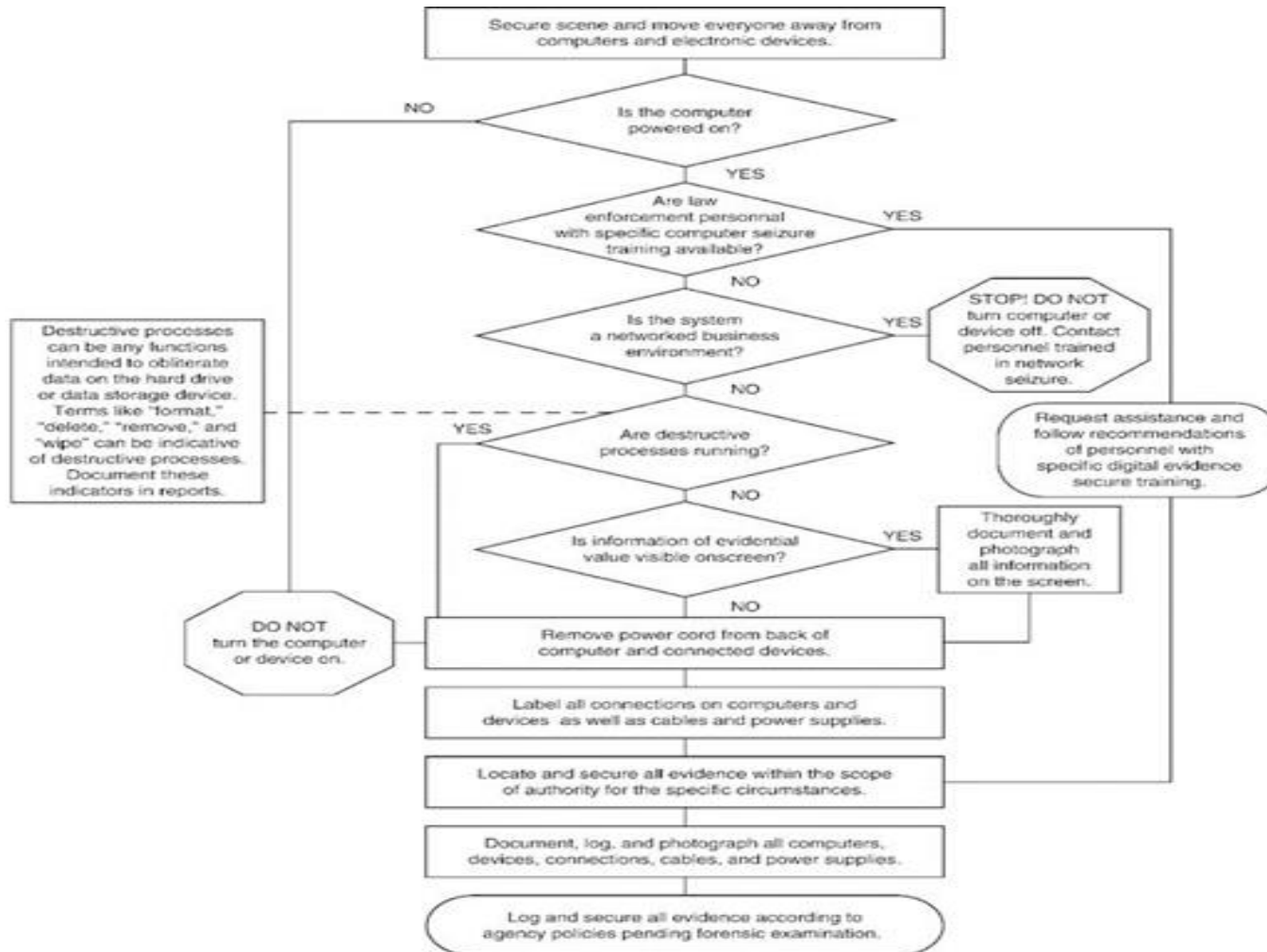
5-Eğer bilgisayar açık ise; ekran fotoğrafı çekilir.Tarih/saat bilgisi not edilir. El konulacaksa güç kablosu kasadan çekilir. Ağa bağlı bilgisayar ise önce ağdan izole edilmelidir.

6-Sunucu bilgisayar kapatılmaması gereken durumlarda yine ekran görüntüsü, tarih/saat bilgileri alınır.

7-Olay yerinde sayısal delillerin yanı sıra klasik deliller de bulunabilir. Parmak izi,DNA,saç teli gibi. Örneğin CD/DVD'de parmak izi aranabilir.

# Sayısal Delil İlk Müdahale Akış Grafiği

Aşağıdaki çizelgede sayısal delile ilk müdahale akış şeması görülmüyor. Spesifik durumlara göre ve mevzuatın dışına çıkmamak koşulu ile bu akış şeması değişebilir. Arama motorunda «Digital Evidence First Response» anahtar kelimesini arattığımızda değişik akış şemaları görülecektir.



İmaj Alma ve Hash

**İmaj Alma (Forensic Duplicate):** Veri depolama biriminin bit-to-bit(birebir kopya, adli kopya) kopyalanması Raw/dd, E01, ISO, vmdk gibi formatlarda alınabilir.

Öncelik:

**Volatile:** Uçucu veriler. Örneğin RAM'de bulunan veriler.

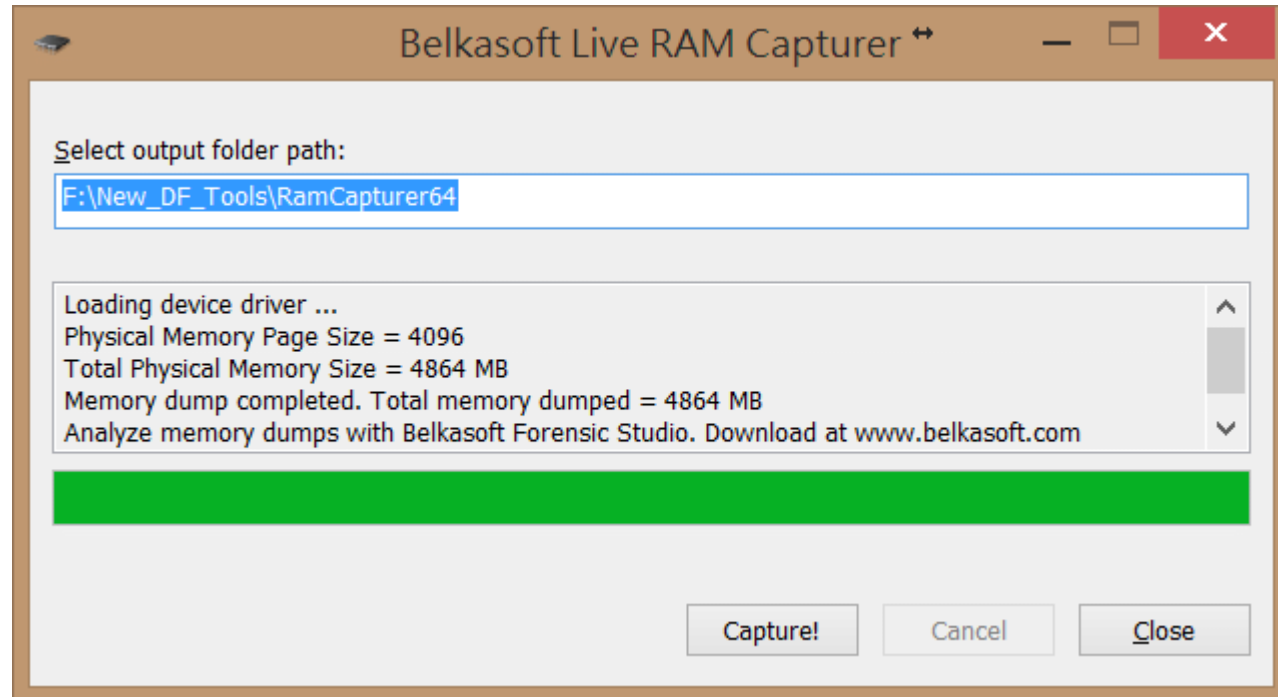
**Non-Volatile:** Uçucu olmayan veriler. Örneğin HDD'de bulunan veriler.

*\*İmajın alınması olaya ve duruma göre değişkenlik gösterebilir.*

## Açık Bilgisayardan(suspicious/infected):

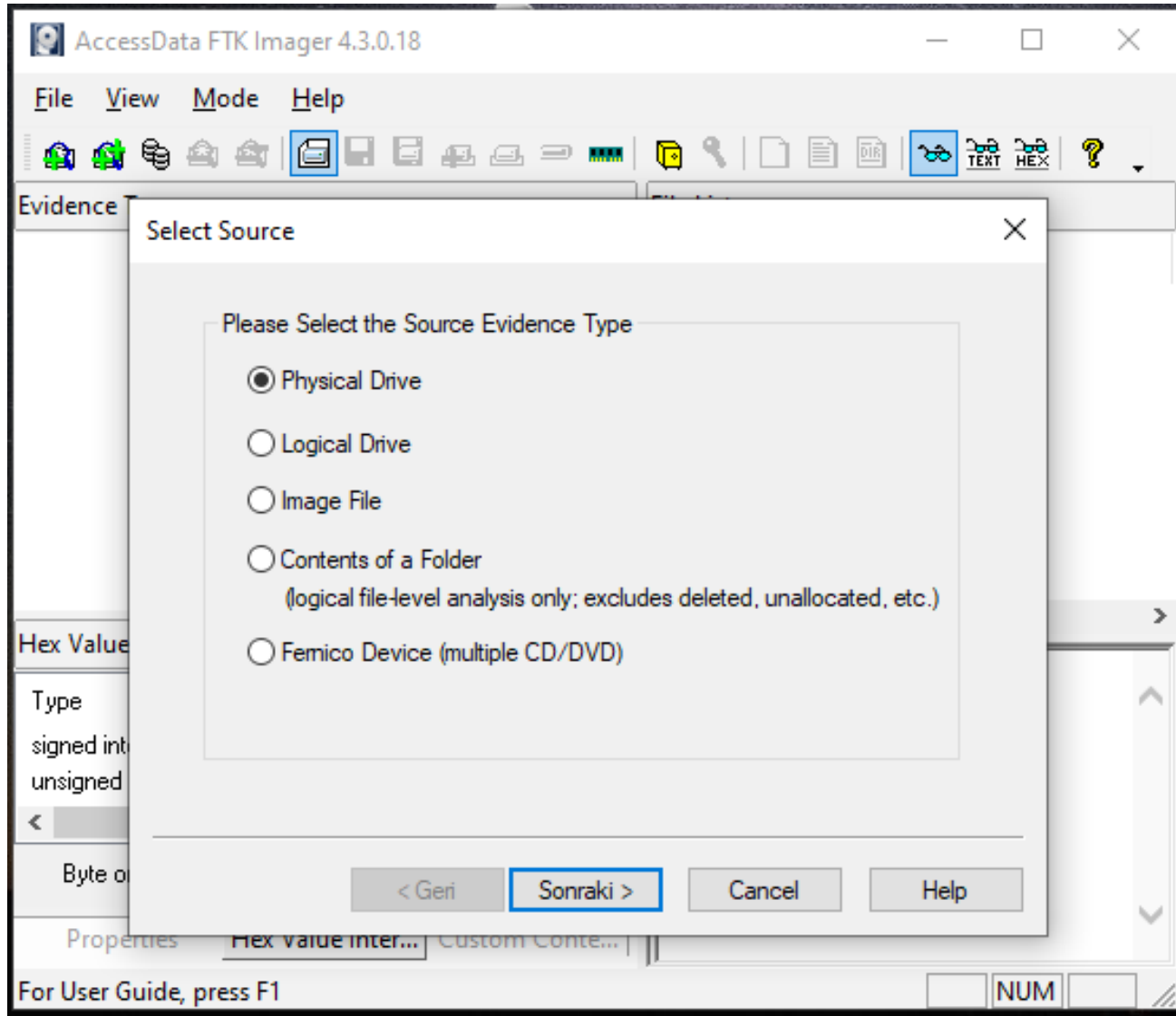
**1-RAM İmaj Alma:** Açık olan bir bilgisayardan RAM, Hiberfil.sys, PageFile.sys gibi bellek verilerinin imajı alınır.

<https://thanursan.medium.com/comparison-of-memory-acquisition-software-for-windows-e8c6d981db23>




## 2-HDD İmaj Alma: HDD'nin tamamının veya bir kısmının imajı alınır.

Live CD/USB→ FTK Imager Lite





### 3-Kısmi Kopya Alma/Triage: HDD'nin tamamı yerine öncelikle inceleme konusu ile ilgili veriler toplanır.

 TACTICAL | Binalyze

General

Evidences

Artifacts

Triage / IoC Scan

Custom Collection

Evidence	Description
System	
<input checked="" type="checkbox"/> Clipboard	Collect Clipboard Contents
<input checked="" type="checkbox"/> Crash Dump Information	Collect Information About Crash Dumps
<input type="checkbox"/> Recycle Bin Information	Collect Information About Items in Recycle Bin
<input checked="" type="checkbox"/> System Restore Points Information	Collect Information About System Restore Points
<input type="checkbox"/> Drivers List	Collect Driver List
<input type="checkbox"/> Processes and Modules	Collect Process and Modules List
<input checked="" type="checkbox"/> Window Screenshots	Capture Screenshot of Application Windows
<input type="checkbox"/> Antivirus Information	Collect Information About Installed Antivirus
<input type="checkbox"/> DNS Servers	Collect DNS Server Addresses
<input checked="" type="checkbox"/> Proxy List	Collect Information About Proxy List
<input type="checkbox"/> Downloaded Files Information	Collect Information About Downloaded Files
<input type="checkbox"/> Autoruns	Collect Information About Autoruns
<input type="checkbox"/> Installed Applications	Enumerate Installed Applications

Select All / Clear All

Back

OK

Send Feedback | Documentation

b!nalyze

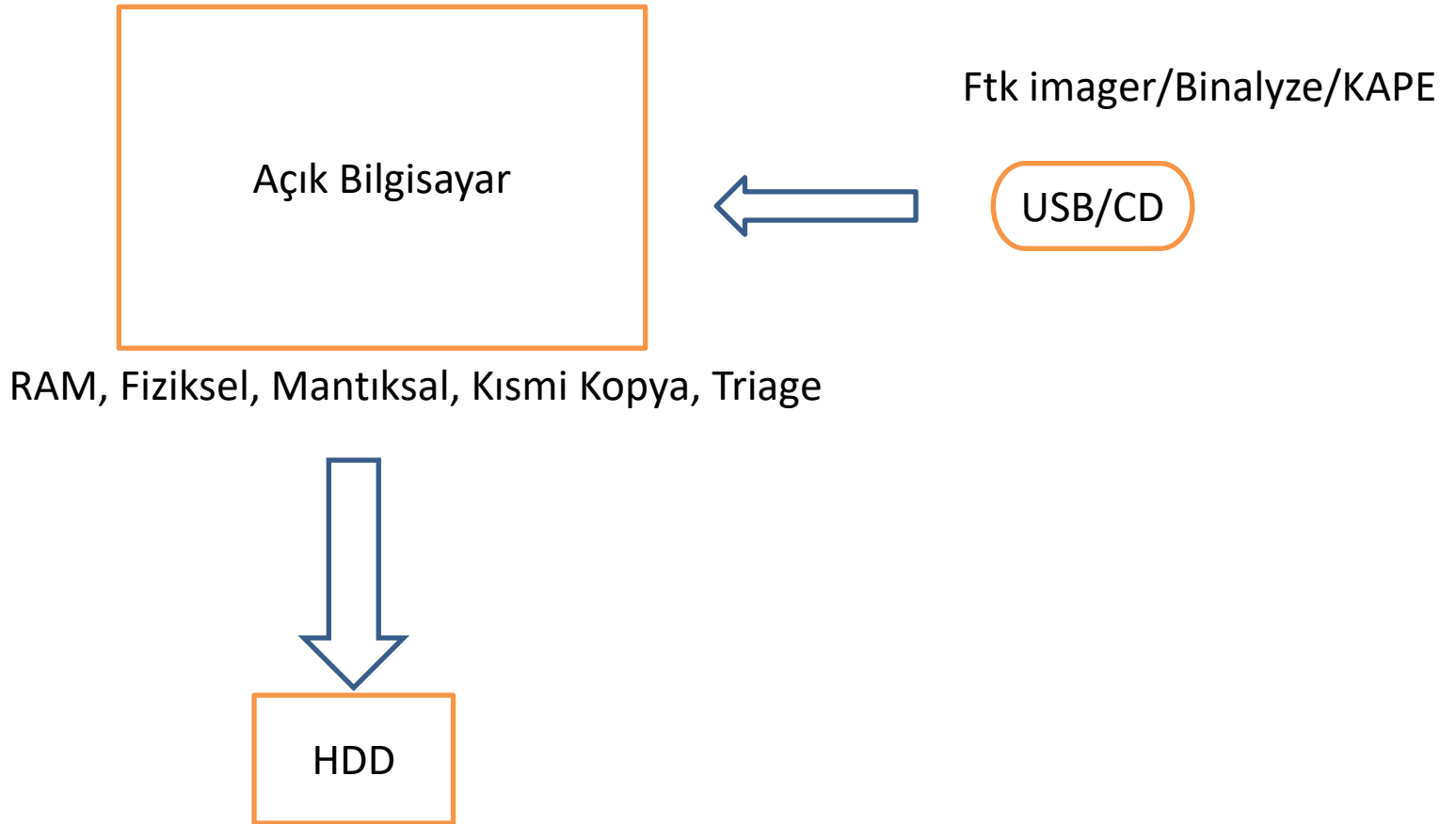
2.6.4

# DEMO

Ram imaj

HDD imaj

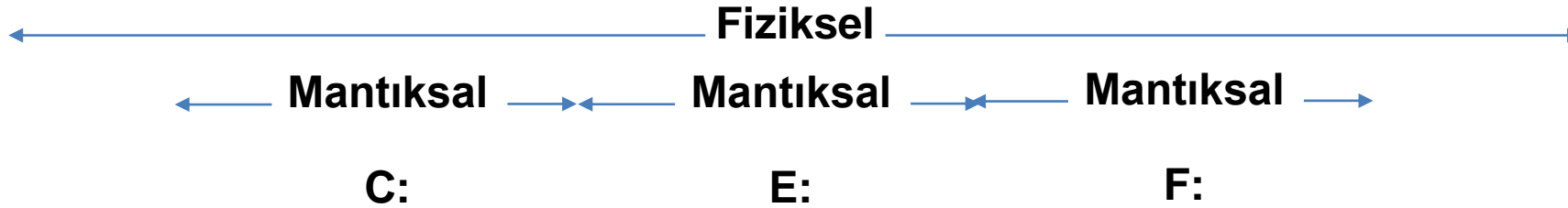
Triage



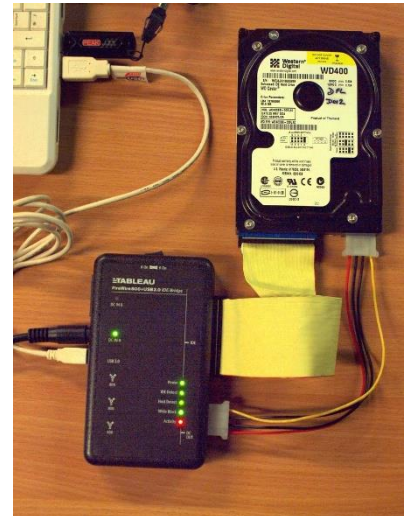
# Kapalı Bilgisayardan (suspicious/infected):

**1-Disk Sökülerek HDD İmaj Alma:** HDD'nin tamamının veya bir kısmının imajı alınır

<b>Disk 0</b> Temel 931,50 GB Çevrimiçi	260 MB Sağlam (EFI Sist)	<b>Windows (C:)</b> 344,34 GB NTFS Sağlam (Önyükleme, Disk Belleği Dosya)	<b>Yeni Birim (E:)</b> 487,30 GB NTFS Sağlam (Temel Veri Bölümü)	<b>Yeni Birim (F:)</b> 98,63 GB NTFS Sağlam (Temel Veri Bölümü)	980 MB Sağlam (Kurtarma B
--	-----------------------------	---	--	---	------------------------------

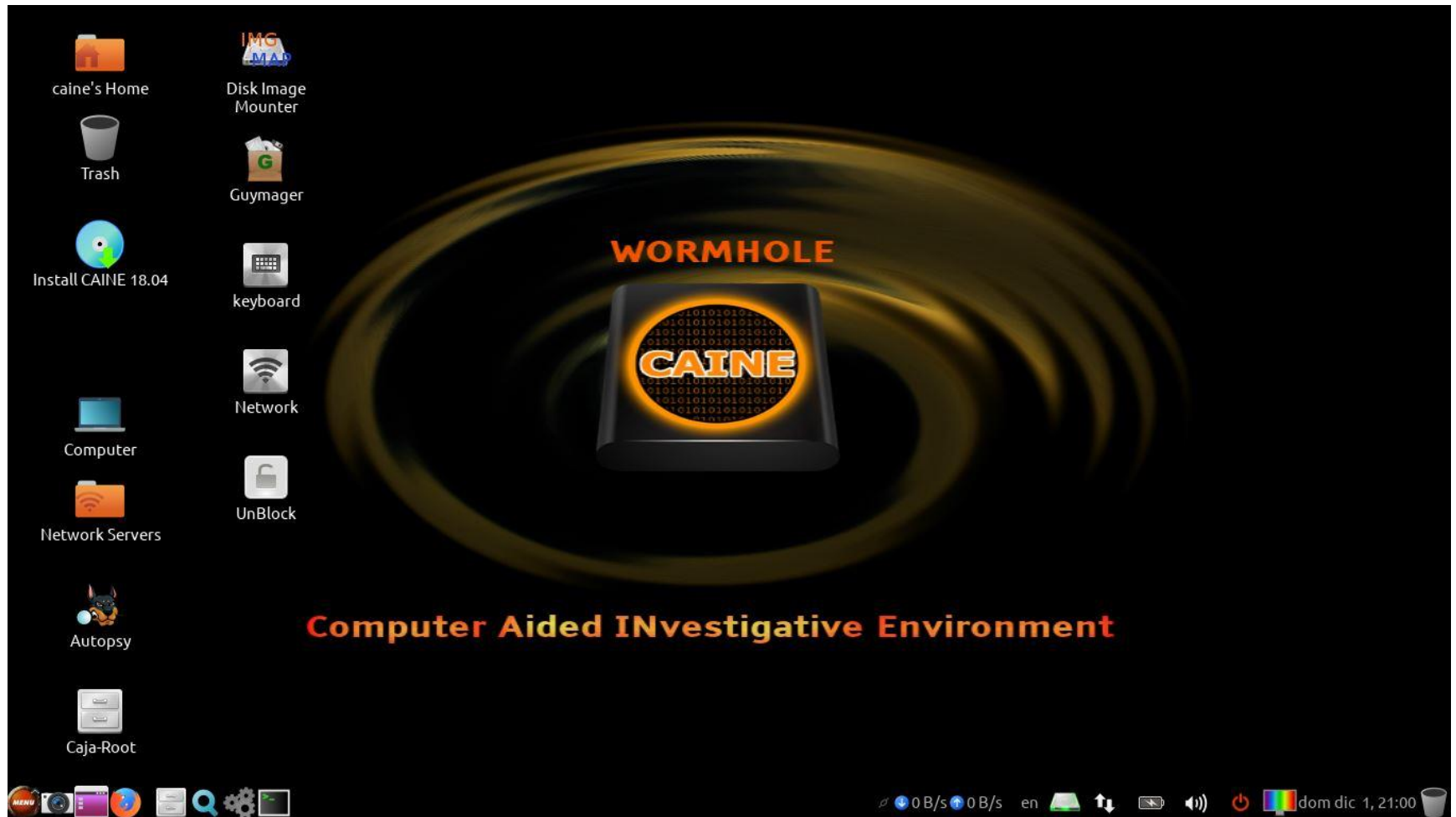


Kapalı Sistem/Donanımsal imaj alma



Write Blocker ile imaj alma

**2-Boot CD/DVD/USB ile Açılarak HDD İmaj Alma:** HDD'nin tamamının veya bir kısmının imajı alınır. Guymager, Caine, Deft, Kali vs.



## Hash

Girilen veriyi, sabit uzunlukta çıktıya dönüştüren matematiksel işleme hash denir. MD-5 hash 128 bit, SHA-1 hash 160 bit uzunluğundadır.

SHA-1	23812B61A41E01F61AF0DA048B80AD25F1D4C8BA
-------	--

### **HDD Image 1 (software write-blocker)**

MD5	F8BE2078382A68ADC792B734FFB480CD
-----	----------------------------------

SHA-1	23812B61A41E01F61AF0DA048B80AD25F1D4C8BA
-------	--

### **HDD Image 2 (no write-blocker)**

MD5	CF4539F0E98E67F368E5EB1D3119EB03
-----	----------------------------------

SHA-1	31CE3038803A8B4BE39FD197905123664C5C2C5C
-------	--

# DEMO

USB Bellek imaj Alınması

Ftk imager  
İnceleme Bilgisayarı

Donanımsal



Yazılımsal



USB/CD

Registry'den USB portu yazma-koruma yapılacak.  
[HKEY\_LOCAL\_MACHINE\SYSTEM\CurrentControlSet\Control  
\StorageDevicePolicies]  
"WriteProtect"=dword:00000001