ADLİ BİLİŞİMİN EVRELERİ

TOPLAMA

OLAY YERİ GÜVENLİĞİ

CİHAZLARIN GRUPLANDIRIP ETİKETLENDİRMEK

- UÇUCU VERİLERİ SAPTAMAK

KONTROLLER

CANLI ANALİZ

- AÇIK BİR BİLGİSAYARIN BULUNMASI DURUMUNDA

MUHAFAZA VE NAKLİYE

NORMAL ANALİZ

- LABRATUVAR ORTAMINDA

İNCELEME

İMAJIN ADLİ KOPYASI ÜZERİNDEN YAPILIR.

Küçüktaşdemir

ÇÖZÜMLEME

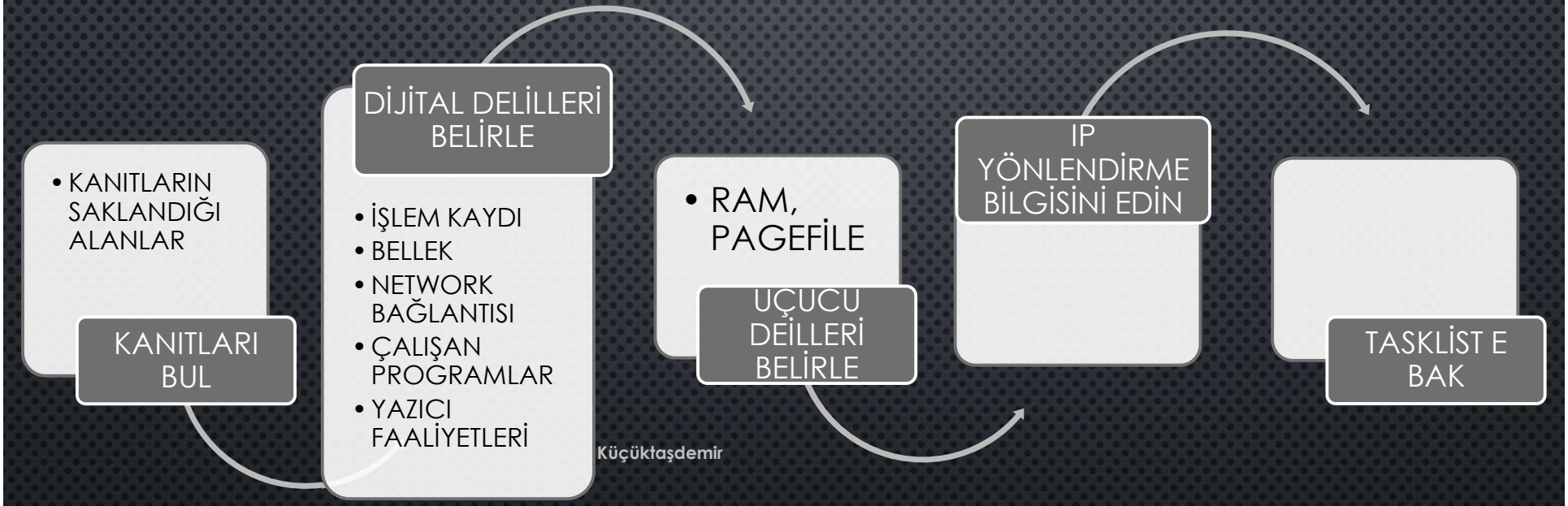
RAPORLAMA

DELİLLER TOPLANIRKEN

- BİLGİSAYAR KAPALIYSA AÇMAYIN, AÇIKSA KAPATMAYIN
- ORTAMIN VE DONANIMIN HER AÇINDAN FOTOĞRAFINI ÇEKİN
- MÜMKÜN MERTEBE ELLE FİZİKSEL TEMASTAN KAÇINILMALI
- SADECE ADLİ BİLİŞİM UZMANI BULUNMALI
- DONANIMIN DIŞ DÜNYAYLA BAĞLANTISI KESİLMELİ
- ADLİ BİLİŞİM ALANINDA KULLANILAN İMAJ ALMA PROGRAMLARI KULLANILMALI
- ÇALIŞMANIN YAPILDIĞI SAAT İLE BİLGİSAYARIN SAATİNE DİKKAT EDİLMELİ
- DİJİTAL DELİLLERİ BULUNDURAN DONANIMLARIN KORUNMASI İÇİN DIŞ DÜNYA İLE BAĞLANTISI KESİLMELİ
- ALINAN İMAJLAR, ORTAMDAN TOPLANAN USB, CD, VB. DEPOLAMA ARAÇLARI ÖZENLE SAKLANMALI
- MEVCUT DONANIMLARIN ÜZERİNDE, KULLANICIDAN KALAN TÜY, DERİ VB. BİYOLOJİK İZLERİN DE BULUNABİLECEĞİ UNUTULMAMALI.

Küçüktaşdemir

DELİLLERİN TOPLANMA SÜRECİ



Küçüktaşdemir

ADLİ BİLİŞİMDE BİLİNMESİ GEREKENLER

DELİL İNCELEMESİ SİSTEMİN KAPALI VEYA AÇIK OLMSINA GÖRE FARKLI BİÇİMLERDE YAPILIR.

- ADLİ İMAJ ALMA
- AĞ TRAFİK VERİLERİ
- HASH DEĞERİ
- METAVERİ

ADLİ İMAJ ALMA

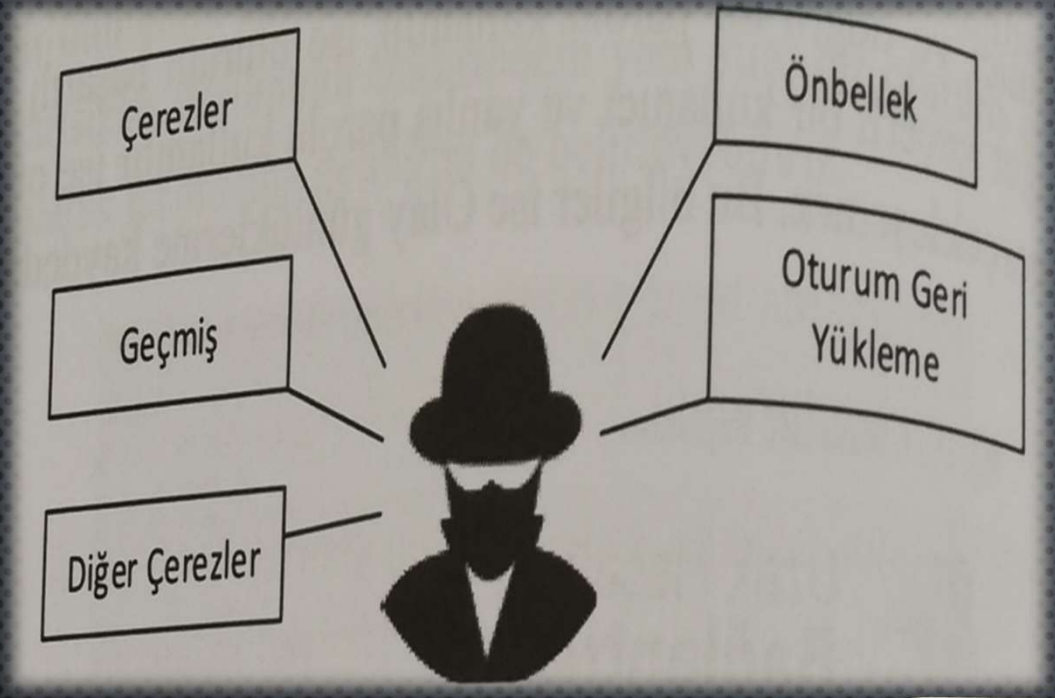
- KLONLAMA DEĞİLDİR.
- SABİT DİSKTEKİ HER BİR SEKTÖRÜN AYRI AYRI KOPYALANMASI
  - SİLİNMİŞ, GEÇMİŞTE DEĞİŞTİRLMİŞ VERİLER DAHİ EN İNCE AYRINTISINA KADAR EDİNİLİR.
  - ÖZEL ADLİ BİLİŞİM YAZILIMLARI İLE YAPILIR.
  - ÖRN. FORENSIC EXPLORER

Küçüktaşdemir

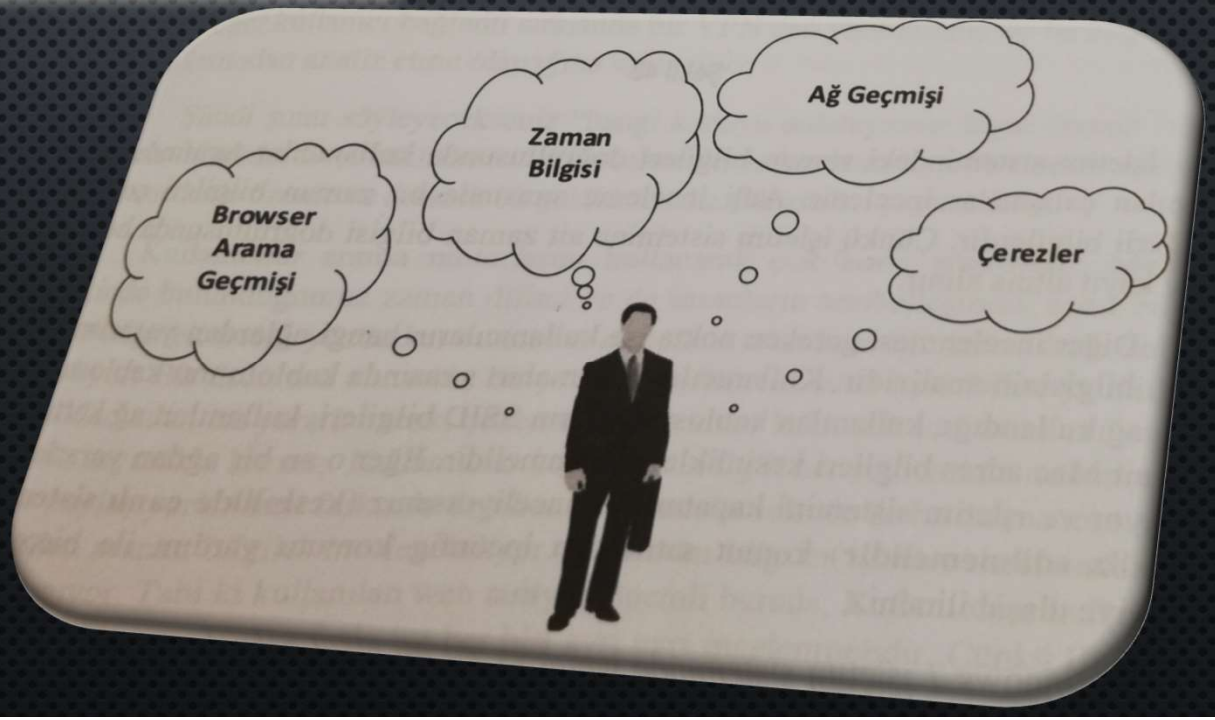
BİRE BİR KOPYALAMA (SEKTÖR VE SEKTÖR, BİT BİT) İŞLEMİ YAPILIR. SABİT DİSKİN ÜZERİNDE YER ALAN TÜM DOSYA/DİZİN YAPISI, GİZLİ ALANLAR KOPYALANIR. ORJİNAL DİSK İLE ELD EDİLEN KOPYA EŞDEĞERDEDİR.

AĞ TRAFİK VERİLERİ

- **AĞ BAĞLANTISI**
  - INTRANET (YEREL AĞ)
  - INTERNET (GLOBAL)
- **AĞ ADLİ BİLİŞİM**
  - AĞ ÜZERİNDEN GÖNDERİLEN VERİ PAKETLERİNİN ELDE EDİLMESİ
- **AĞ TRAFİK KAYITLARI (LOG) KULLANILIR.**
  - SERVİS SAĞLAYICILAR BELİRLİ BİR SÜRE BU KAYITLARI TUTARLAR.
- **AĞ TRAFİK KAYDI ELDE EDİLEBİLECEK SİSTEMLER**:
  - GÜVENLİK DUVARI (FIREWALL)
  - SALDIRI TESPİT SİSTEMLERİ
  - BALKÜPÜ SİSTEMLERİ



Grafikler kaynakçada gösterilen adli bilişim kitabından alınmıştır.



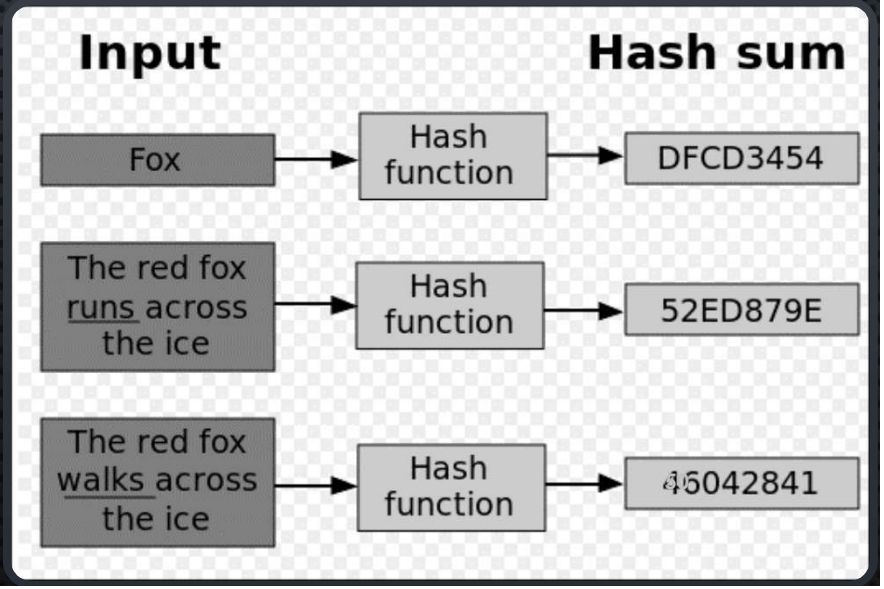
Küçüktaşdemir

HASH DEĞERİ

- DEPOLAMA ALANLARINDAKİ VERİ ÜZERİNDE DEĞİŞİKLİK OLUP OLMADIĞINI ANLAMAK İÇİN KULLANILIR.
- KİMİNE GÖRE BİR ANLAMDA DİJİTAL İMZADIR.
- KİMİNE GÖRE DNA VEYA PARMAK İZİ İLE BENZETİLİR.
- HASH BİR ALGORİTMA OLUP, DOSYANIN ŞİFRELİ ÖZETİDİR.
  - ŞİFRELİ ÖZET TEK YÖNLÜ OLDUĞU İÇİN DEĞİŞTİRİLMESİ OLANAKLI DEĞİL.
- AİT OLDUĞU DOSYA VE DİSKE ÖZEL VE TEKTİR.
- HER DEĞİŞİKLİKTE AYRI HASH DEĞERİ OLUŞUR.
- HASH ALGORİTMASI STANDARDI OLARAK BİLİRKİŞİ RAPORLARINDA MD5 VEYA SHA-1 KULLANILIR.

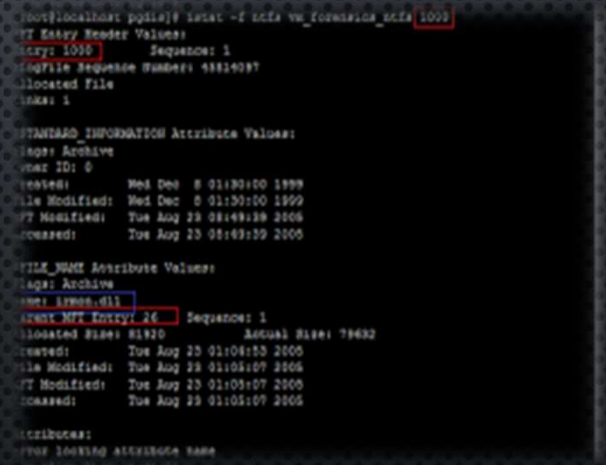
HASH DEĞERİ

- «HASH FONKSİYONU, DEĞİŞKEN UZUNLUĞA SAHİP BİR MESAJI GİRDİ OLARAK ALIR VE SABİT UZUNLUKLU BİR MESAJI ÇIKTI OLARAK ÜRETİR. BU ÇIKTI MESAJI BELİRLİ BİR GİRDİ İÇİN TEK BİR SONUÇ ÜRETİR VE BAŞKA BİR GİRDİNİN AYNI SONUCU ÜRETMESİ MÜMKÜN DEĞİLDİR.»
  - **HASH DEĞERLERİ ALINARAK ORJİNAL DİSK İLE KOPYASI ARASINDA KARŞILAŞTIRMA YAPILIR.**
  - **HASH DEĞERİNİN AYNI OLMASI GEREKİR!!**
  - **TAKİPÇİSİ OLUNMALIDIR!**



METAVERİ

- VERİ İÇEREN DOSYANIN HANGİ UYGULAMAYA AİT OLDUĞU
- DOSYAYI OLUŞTURAN İŞLEME AİT BİLGİ VERİR
  - ZAMAN, KULLANICI, HANGİ FORMATTAN HANGİ FORMATA DÖNÜŞTÜRÜLDÜĞÜ
- DOSYAYI OLUŞTURAN DONANIMIN VE YAZILIMIN BİLGİSİNİ VERİR.
- FOTOĞRAF İSE, LENS, GPS, KAÇ KİŞİ BULUNDUĞU, RAKIM, TARİH VE FLAŞ BİLGİSİ
- WİNDOWS KAYIT BİLGİLERİNE VE OLAY GÜNLÜKLERİNE BAKILIR. (HKEY CUURENT USER)
- ÜCRETSİZ YAZILIM: EXİTFOOL



BİLİRKİŞİ RAPORU HAZIRLARKEN

GİRİŞ

OLAYLARIN NİTELİĞİNİ AÇIKLANMASI

MAĞDURLARIN BELİRİTLMESİ

TANIKLARIN BELİRTİLMESİ

KANITLARIN YERLERİ

- **NASIL TOPLANDIKLARI**

GELİŞME

Küçüktaşdemir

KANIT ZİNCİRİNİN TANITILMASI

DİJİTAL DELİLLERİN SAPTANMASI VE BELİRTİLMESİ

DİJİTAL DELİLLERİN ANALİZİ

- **İNCELEM YÖNTEMİ DE BELİRTİLİR.**

SONUÇ