Bilişim Suçları ve Adli Bilişim

Sunum Planı

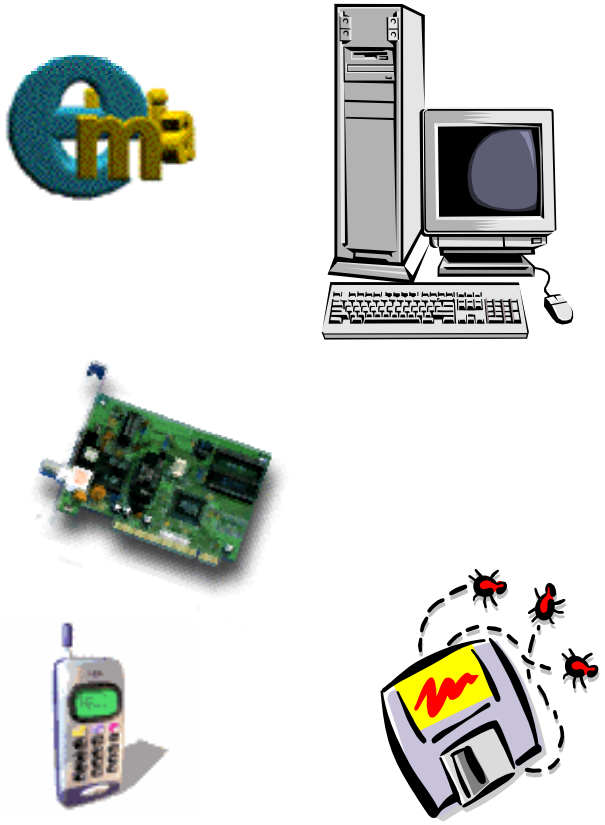
- Bilgisayar Suçları
  - Tanımı
  - Sınıflandırması
  - Yöntemleri
  - Hukuki Durumu
  - Yaşanan Problemler
  - Emniyet Teşkilatındaki Yapılanma

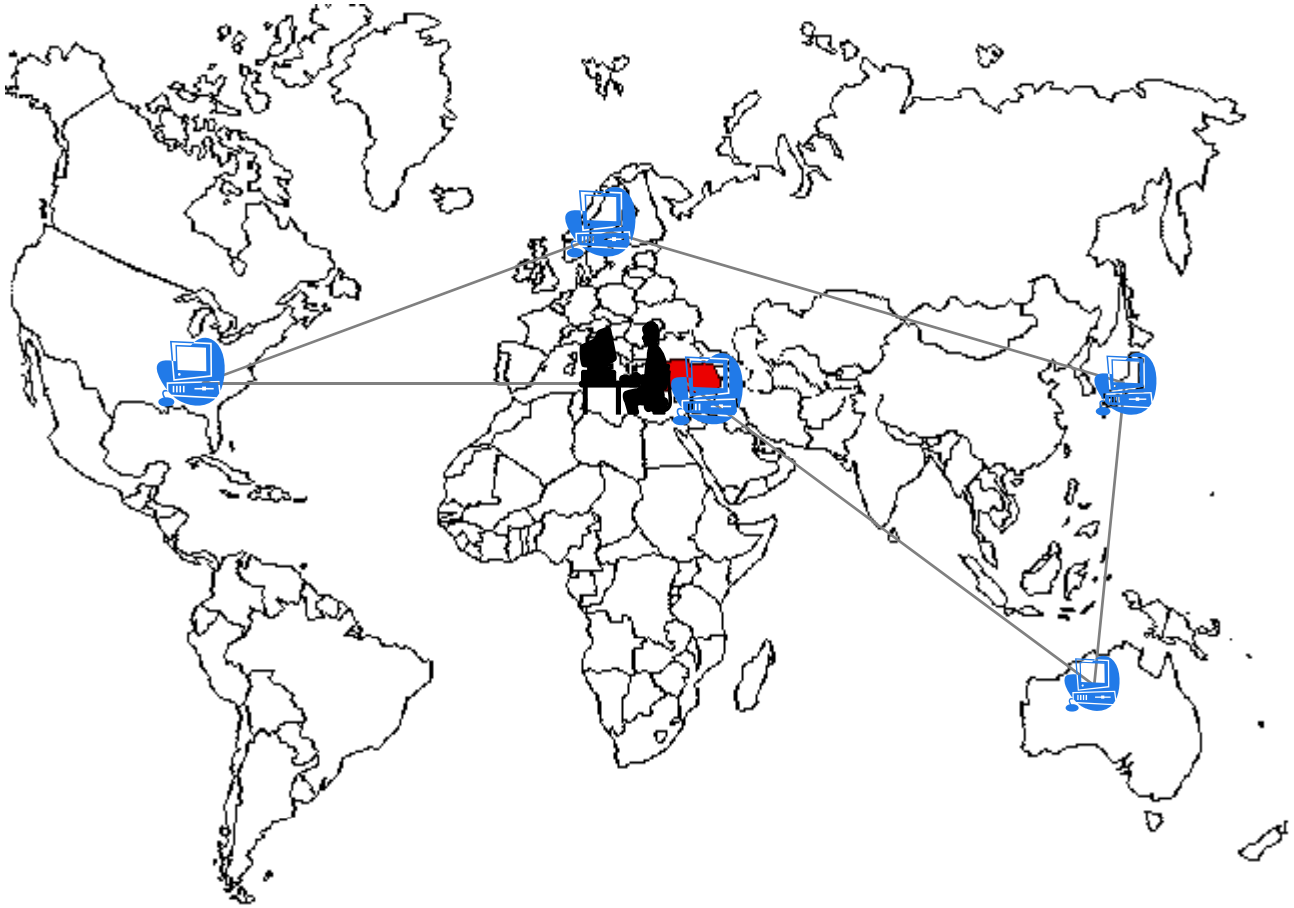
- Digital Delil

- Adli Bilşim Süreçleri
  1. Delili Elde Etme ve Muhafaza
  2. İnceleme ve Analiz
  3. Raporlama ve Mahkemeye Sunma

Bilişim Suçu ve Kapsamı Nedir?

- Bilişim Suçları
- Bilgisayar Suçları
- Siber Suçlar
- İnternet Suçları
- Yüksek Teknoloji Suçları
- IT Crime
- Computer Related Crime
- Computer Crime
- Syber Crime
- Vs.





Bilişim Suçlarının Tasnifi

- Bilgisayar Sistemlerine ve Servislerine Yetkisiz Erişim ve Dinleme
- Bilgisayar Sabotajı
- Bilgisayar Yoluyla Dolandırıcılık
- Bilgisayar Yoluyla Sahtecilik
- Bilgisayar Yazılımlarının İzinsiz Kullanımı
- Yasadışı Yayınlar

Yöntemler

- Şifre çalma
- Arka kapılar ve bilgisayarların açıkları
- Ağları izleme
- Programlar
  - Trojanlar
  - Viruseler
  - DoS atakları

Hukuki Açıdan 1

- **Geleneksel Suçlar**
  - Dolandırıcılık
    - TCK 503-507 : Dolandırıcılık ve İflas
  - Sahtecilik
    - TCK 316-368 : Sahtecilik Suçları
  - Lisans Hakları
    - 5846 nolu Fikir ve Sanat Eserleri Kanunu (FSEK)
  - Yasadışı yayınlar
    - TCK 125-200 : Devletin Şahsiyetine karşı cürümler
    - TCK 480-490 : Hakaret ve Sövme Cürümleri
    - TCK 426-427 : Halkın ar ve haya duygularını inciten veya cinsi arzuları tahrik eden ve istismar eder nitelikte genel ahlaka aykırı: …… ve diğer anlatım araç ve gereçleri

Hukuki Açıdan 2

- **Teknolojinin Gelişimiyle Karşılaştığımız Suçlar**
  - Bilgisayar servislerine yetkisiz erişim ve dinleme
  - Bilgisayar Sabotajı

BİLİŞİM ALANINDA SUÇLAR

TCK 525-a : Bilgileri otomatik işleme tabi tutulmuş bir sistemden, programları, verileri veya diğer herhangi bir unsuru hukuka aykırı olarak ele geçiren kimseye ...

TCK 525-b : Bilgileri otomatik işleme tabi tutulmuş bir sistemi veya verileri veya herhangi bir unsuru kısmen veya tamamen tahrip eden veya değiştiren veya silen veya sistemin işlemesine engel olan veya yanlış biçimde işlemesini sağlayan kimseye ...

TCK 525-c : Bilgileri otomatik olarak işleme tabi tutan bir sisteme, verileri veya diğer unsurları yerleştiren veya var olan verileri, diğer unsurları tahrif eden kimseye …

TCK 525-d : Meslek icrası ise…

Hukuki Açıdan 3

- Yeni Türk Ceza Kanunu
  - Madde 243 – Bilişim Sistemine girme Suçu

    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.
  - Madde 244 – Bilişim Sistemine girme Suçu
  - Madde 245 – Bilişim Sistemine girme Suçu
  - Madde 246 – Bilişim Sistemine girme Suçu
- Yeni Ceza Muhalemeleri Kanunu
  - Madde 134 – Dijital Delillere El Koyma
- Elektronik İmza Kanunu
  - Madde 15 – Denetim
  - Madde 16 – İzinsiz Kullanım
  - Madde 15 – Sahtecilik

Güvenlik Birimleri Açısından

- Olay Öncesi
  - Bilgi alma faaliyetleri
  - Devriye
- Olay Sonrası
  - İnceleme
  - Analiz

Yaşanan Problemler

- Delillerin Elde Edilmesi
- Delillerin Hukuki Durumu
- Uluslararası İşbirliği
- Uluslararası Suç Tanımı

Dijital Delil

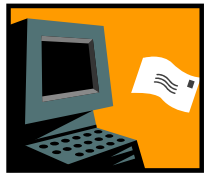
- Delil nedir ?
  - Vasıtanın gerçekte olayı temsil ediyor olabilmesi
  - Olayı temsil eden vasıtanın akla, maddi gerçeğe ve hukuka uygun olması gerekliliğidir.

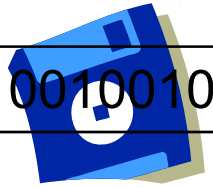
Dijital Delil

- Dijital delil nedir ?
  - Temel delil şartlarını sağlamanın yanında suça delil niteliği sağlayan ve mahkemelere sunulabilecek dijital veri saklayabilen ve/veya elektronik devre akımları ile çalışan disk, disket, CD, bilgisayarlar, cep telefonları, PDA cihazları, flash bellekler, SIM kartlar, bir bilgisayara ait dahili veya harici donanımlar gibi çeşitli elektronik cihazlardır.

Dijital Delil

•Defter •Kağıt •Adres Telefon Rehberi	•Cep Telefonu •PDA •Bilgisayar
•Klasik Mektup	•Elektronik Posta
•Firmaların Dosyaları	•Dijital Veri Bankaları
•Bu bir delildir.	•1010001001001001 00





Adli Bilişim Süreçleri

- Adli Bilişim süreci hazırlık soruşturması içerisindeki laboratuar incelemelerini kapsamaktadır. Tüm adli bilimlerde olduğu gibi Adli Bilişim de adli bir olayın maddi delillerle ispatlanması için laboratuar ortamında gerçekleştirilen bir çalışmadır. Ancak bu çalışma öncesi olay yerinden delillerin toplanması işlemi ve mahkemede bu delillerin açıklanabilir bir şekilde ifade edilmesi de özel bir bilgi birikimi istediğinden Adli Bilişimin konusu içerisine girmektedir.

Adli Bilişim Süreçleri

- **Delil Elde Etme ve Muhafaza**
- İnceleme ve Analiz
- Raporlama ve Mahkemeye Sunma

Delili Elde Etme ve Muhafaza

- Olay yerine varıldığında çevre güvenliğinin sağlanmasından, delilerin laboratuara ulaştırılmasına kadar olan süreci kapsar.

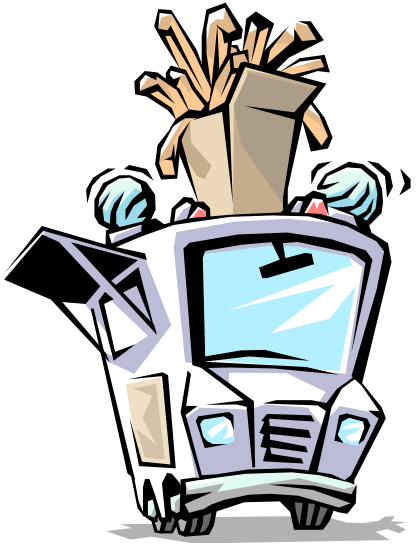
- Olay yerinden delillerin toplanması en temel aşamadır. Çünkü deliller ne kadar sağlıklı toplanırsa bundan sonraki aşamalar da o kadar başarılı bir şekilde sonuçlanacaktır.

- Delillerin toplanması dahi özel bir uzmanlık gerektirmektedir.

- Olay yeri ekipleri bilişim sistemleri konusunda yeterli bilgiye sahip olmalı ve delilleri yok edebilecek dijital bubi tuzaklarına karşı dikkatli davranmalıdır.

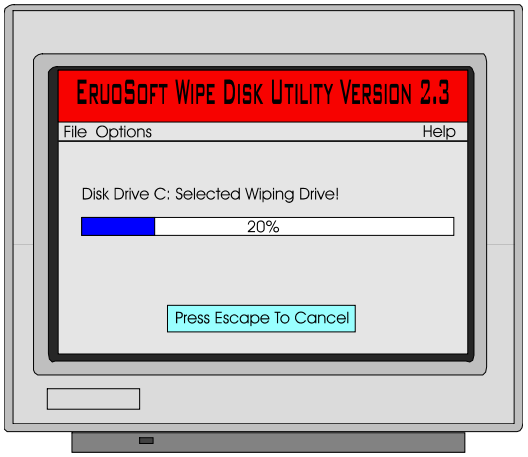
Delili Elde Etme ve Muhafaza

- Olay yerinde elde edilen delillerin laboratuvara getirilmesine kadar olan zaman diliminde delillerin bozulmadan saklanması ve laboratuvara sevk edilmesi de bu süreç içerisindedir.



Delili Elde Etme ve Muhafaza

- Delilleri Toplamaya <u>Başlamadan Önce</u>
  - Herkesi bilgisayar sisteminin başından uzaklaştır
  - Olay yerinin fotorafını çek
  - Olay Yerinde bulunan bilgisayar sisteminin bağlantı diagramını çiz
  - Zarar verecek aktiviteleri dikkat et
  - Olay yerindeki şifre olabilecek notlara dikkat et



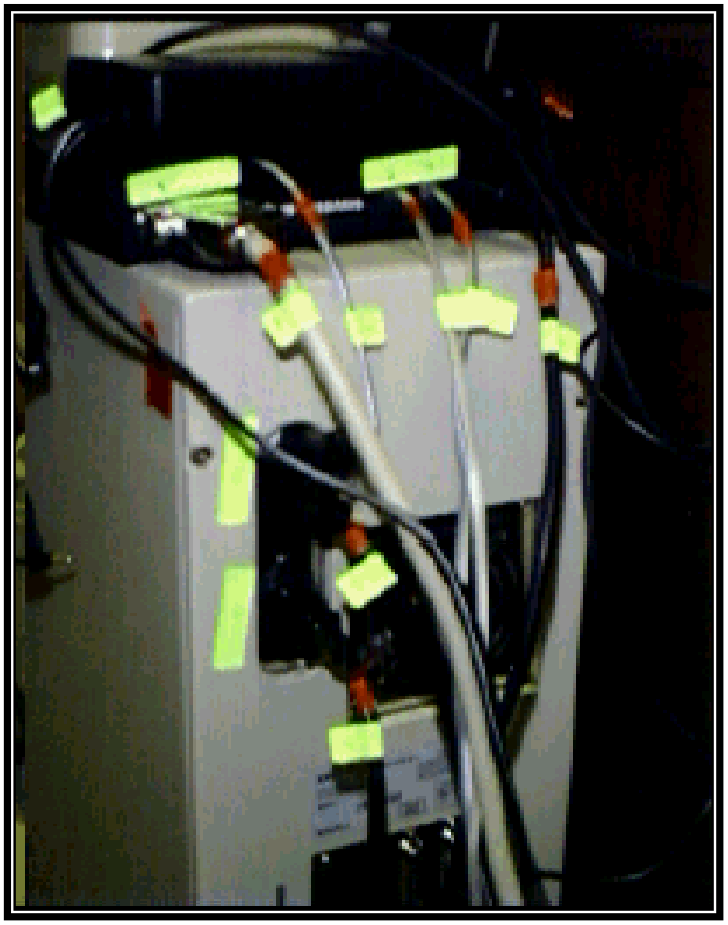
Delili Elde Etme ve Muhafaza

- Bilgisayar açık ise
  - Ekran görüntüsünün fotorafını çek
  - Ekran koruyucu var iptal etmek için bulunan şifreleri kullan
  - Sıradışı görünenleri not al
  - Bilgisayarı kapama, elektrigini kes
  - UPS sistemlerine dikkat et
  - Network kablosunu sök
  - Gerekirse Jammer kullan
- Bilgisayar Kapalı ise
  - Elektrigini kes
  - UPS sistemlerine dikkat et
  - Network kablosunu sök
  - Gerekirse Jammer kullan

Delili Elde Etme ve Muhafaza

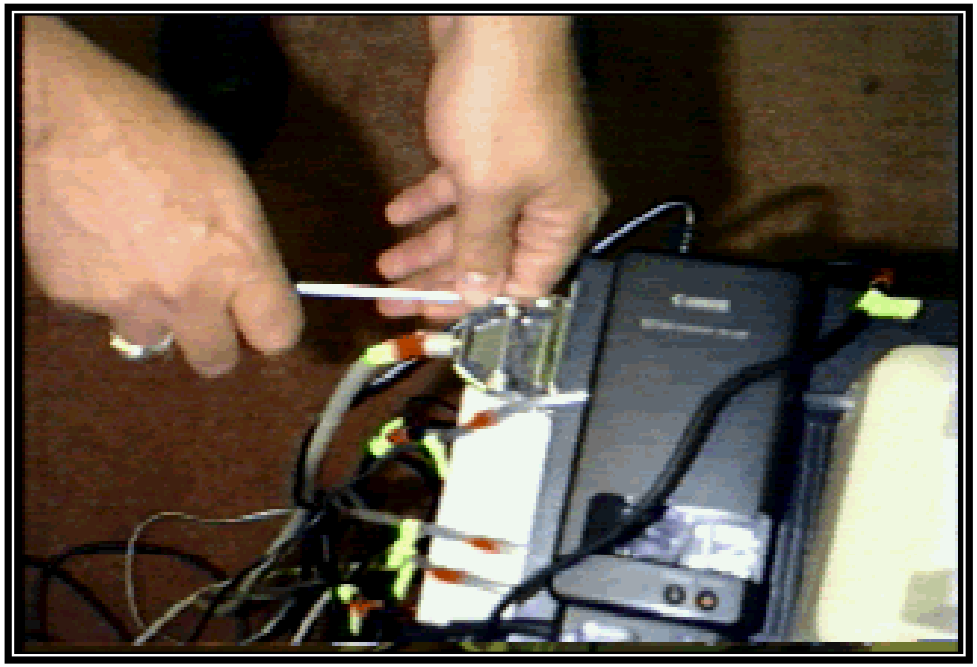
<u>Fotorafını çekmeden evvel</u>

- Kabloları ve portları isimlendir.
- Kabloların başını ve sonun işaretle
- Kablo takılı değilse belirt
- Seri numaralarını kaydet



Delili Elde Etme ve Muhafaza

- Tüm harici donanımları ve kabloları çıkar
- Dahili diskleri ve kartları sökme
- Mümkünse her donanımı ayrı ayrı paketle

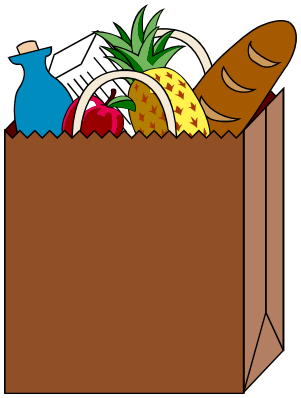


Delili Elde Etme ve Muhafaza

Anti-Statik Balon Poşet

Anti-Statik köpük

Orjinal Taşıma Kutuları



Kağıt Torbalar

Delili Elde Etme ve Muhafaza

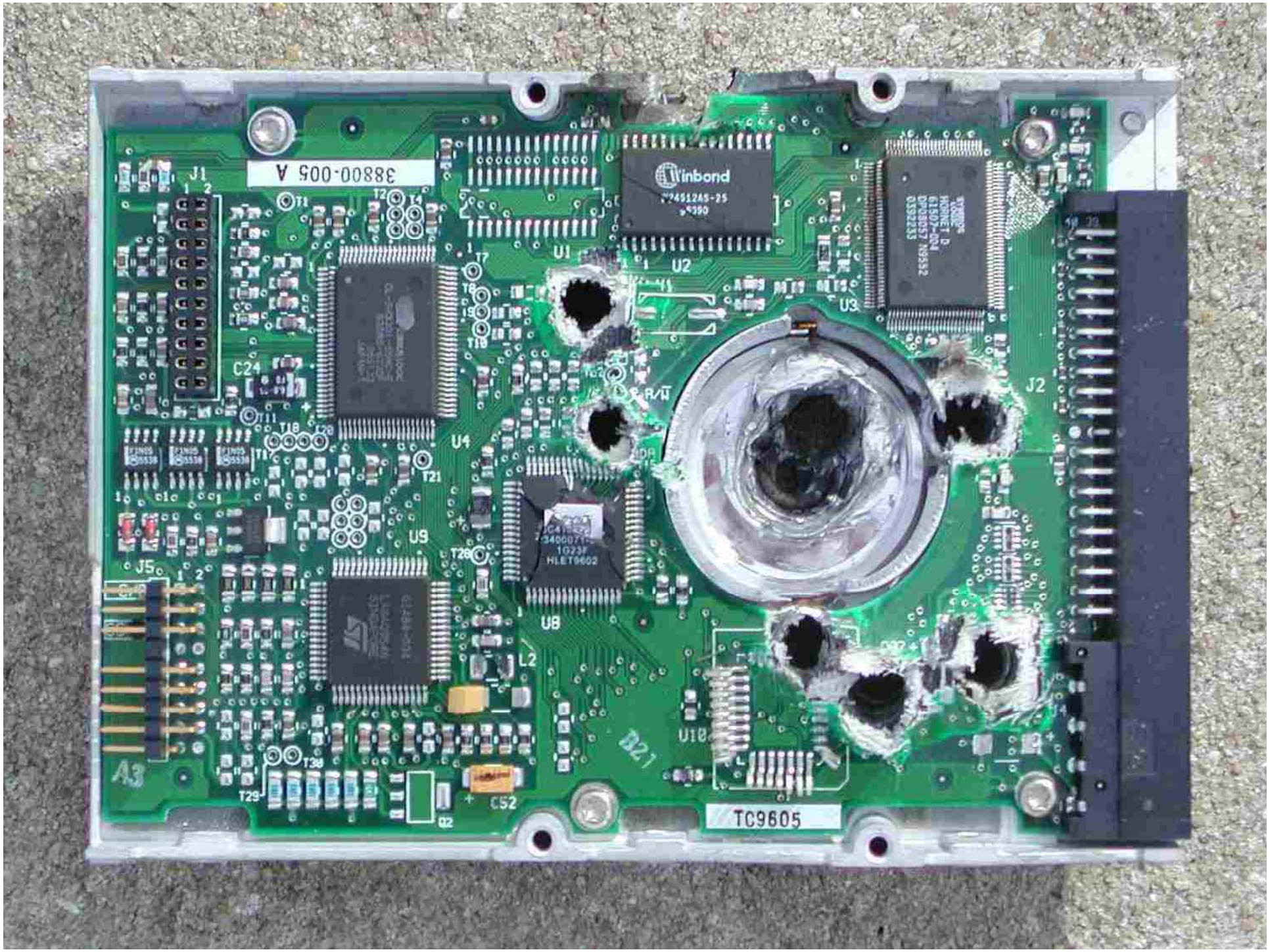
- Sıcaklık
- Statik elektirik
- Cihazları düşürmek
- Zayıf taşıma kutuları

Delili Elde Etme ve Muhafaza

- Delil zincirini başlat
  - Bir önceki halkayı görmeden zinciri devam etme
- Delilin en iyi şekilde ilet
  - Güvenli bir güzergah üzerinden
  - “DELİL devirmeyiniz ve kullanmayınız !” diye işaretle
  - Elektrikten koru
- En kısa zamanda inceleyecek uzmana ilet

OLAY YERİ GÖRÜNTÜLERİ

Water Heater Ex


38800-005 A
Winbond
J1
J2
J5
U1
U2
U3
U4
U8
U9
U10
C24
C52
L2
R/W
TC9605

CONNER
ZCP
COVERED BY ONE OR MORE OF THE FOLLOWING PATENTS:
5,482,200 / 5,121,262 / 4,979,064
OTHER PATENTS PENDING IN THE U.S. AND ELSEWHERE.
MADE IN MALAYSIA
5V 400mA
12V 125mA
CYL: 3146 HDS: 16 SECT: 63
MASTER: C/D IN SLAVE: C/D OUT
CABLE SELECT OPTION ACTIVE: CS IN
FJB4P6X
CFS1621A
SGR03
CFSMA1.30 C12111 9607 U ML2

Adli Bilişim Süreçleri

- Delil Elde Etme ve Muhafaza
- **İnceleme ve Analiz**
- Raporlama ve Mahkemeye Sunma

İnceleme ve Analiz

- Sağlıklı bir inceleme ve bu inceleme sonucunda maddi gerçeğe uygun bir delil elde edilebilmesi için, olay yerinden toplanan materyallerin incelemesini yapacak her türlü cihaz ve konusunda uzman personelin bulunduğu bir laboratuar ortamına gerek duyulmaktadır.

- Her türlü ihtimale karşı, inceleme yazılımları, bir çok dönüştürücü cihaz ve tamir bakım setleri gibi araç gereçlerin her an hazır tutulması gerekmektedir.

İnceleme ve Analiz

- Laboratuar delil bütünlüğünü bozmaması gerekir
- İmaj dosya üzerinde çalışmak lazım
- İncelemeye başlamadan evvel imajın özeti alınmalı

İnceleme ve Analiz

- Donanımlar
  - İnceleme İstasyonu
  - Her türlü dönüştürücü
  - Depolama Ünitesi
- Yazılımlar
  - Delil İnceleme Yazılımları
  - Delil Silme Yazılımları
  - İşletim sistemleri

İnceleme ve Analiz

- Hangi İşlemler Yapılabilir?
  - Geriye doğru günlük inceleme
  - Delil tespit etme
  - Veri kurtarma
  - Şifre kurtarma

Adli Bilişim Süreçleri

- Delil Elde Etme ve Muhafaza
- İnceleme ve Analiz
- **Raporlama ve Mahkemeye Sunma**

İnceleme ve Analiz

- Bilirkişi ile soruşturmacı ortak çalışmalıdır.
- Bilirkişi istenilen dışında bilgiyi rapora yazamaz
- Bilirkişi maddi gerçek dışında bilgiyi rapora yazamaz

Teşekkürler