# Beşinci Oturum

## Siber suçlarla mücadeleyle ilgili adli faaliyete (olay yeri aramasına) hazırlık

## Arama Öncesi

## iPROCEEDS-2

## - çevrim içi sürüm -

# Gündem

- **Birinci Bölüm: Adli faaliyet (arama kararı) ile ilgili resmi belgelerin düzenlenmesi**
  - ✓ Başvuru
  - ✓ Yetki
- **İkinci Bölüm: Arama öncesi planlama**
  - ✓ Soruşturmanın türü hakkında ayrıntılı bilgi edinin
  - ✓ Beklenen kazanımlar: canlı veri incelemesine olan ihtiyacı değerlendirin
  - ✓ Metodoloji geliştirme
- **Üçüncü Bölüm: Arama öncesi bilgilendirme**
  - ✓Arama ekibini bilgilendirin
  - ✓ Adli bilişim ekibini bilgilendirin
- **Dördüncü Bölüm: Delillerin değerlendirilmesi**
  - ✓ Delillere itiraz
  - ✓ Delillerin sunumu

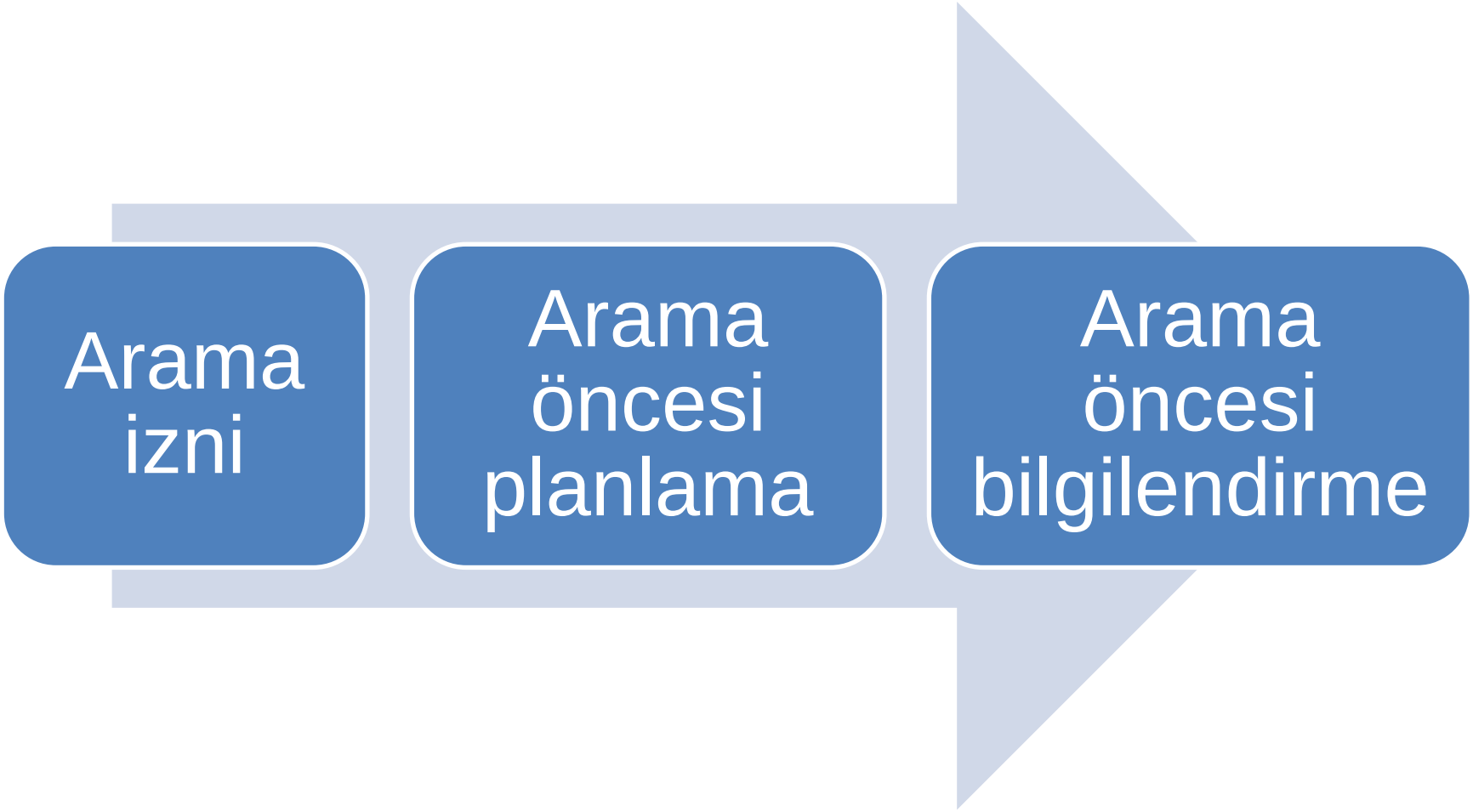
# Oturumun Hedefleri

- ✓ **Adli faaliyetle ilgili resmi belgelerin nasıl düzenlendiğini** anlamak
- ✓ **Arama öncesi bilgilendirme ve arama öncesi süreç ile ilgili** planlama yaparken göz önünde bulundurulması gereken hususları anlamak
- ✓ Nihai hedefin yargıç tarafından değerlendirilecek delil toplamak olduğunu anlamak

# Genel İlkeler - Delil Toplama

- HUKUKUN ÜSTÜNLÜĞÜNE UYULMASINI SAĞLAMAK
- YASALARI BİLMEK
- YASALARI UYGULAMAK
- GEREKTİĞİNDE İZİN ÇIKARMAK
- KOŞULLARA VE GÜVENCELERE UYMAK
- SAVUNMANIN HAKLARINA SAYGIYI TEMİN ETMEK

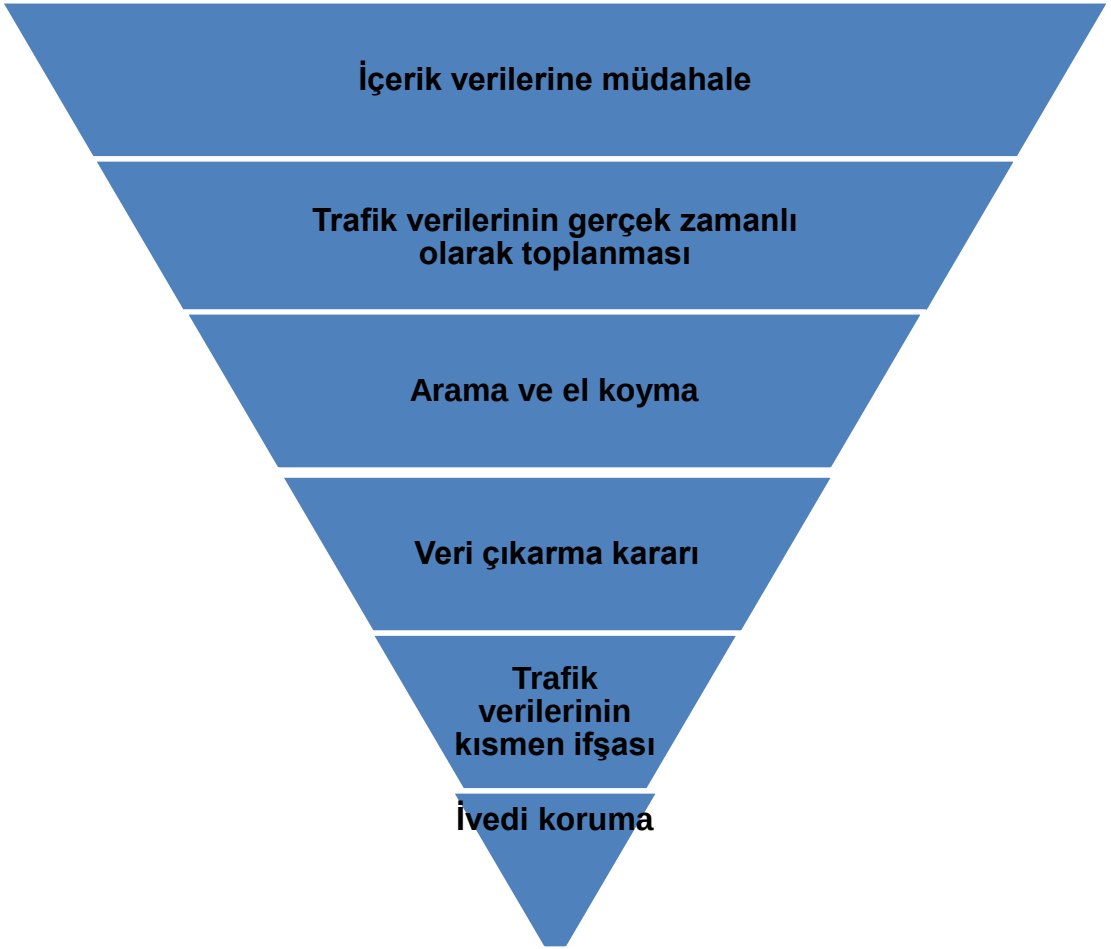
# Adli faaliyetin hazırlanması



# BİRİNCİ BÖLÜM
# Resmi belgelerin düzenlenmesi

- Başvuru
- Yetki
- Başvurudaki koşullar ve güvenceler

# Resmi belgelerin düzenlenmesi - Genel Kavramlar

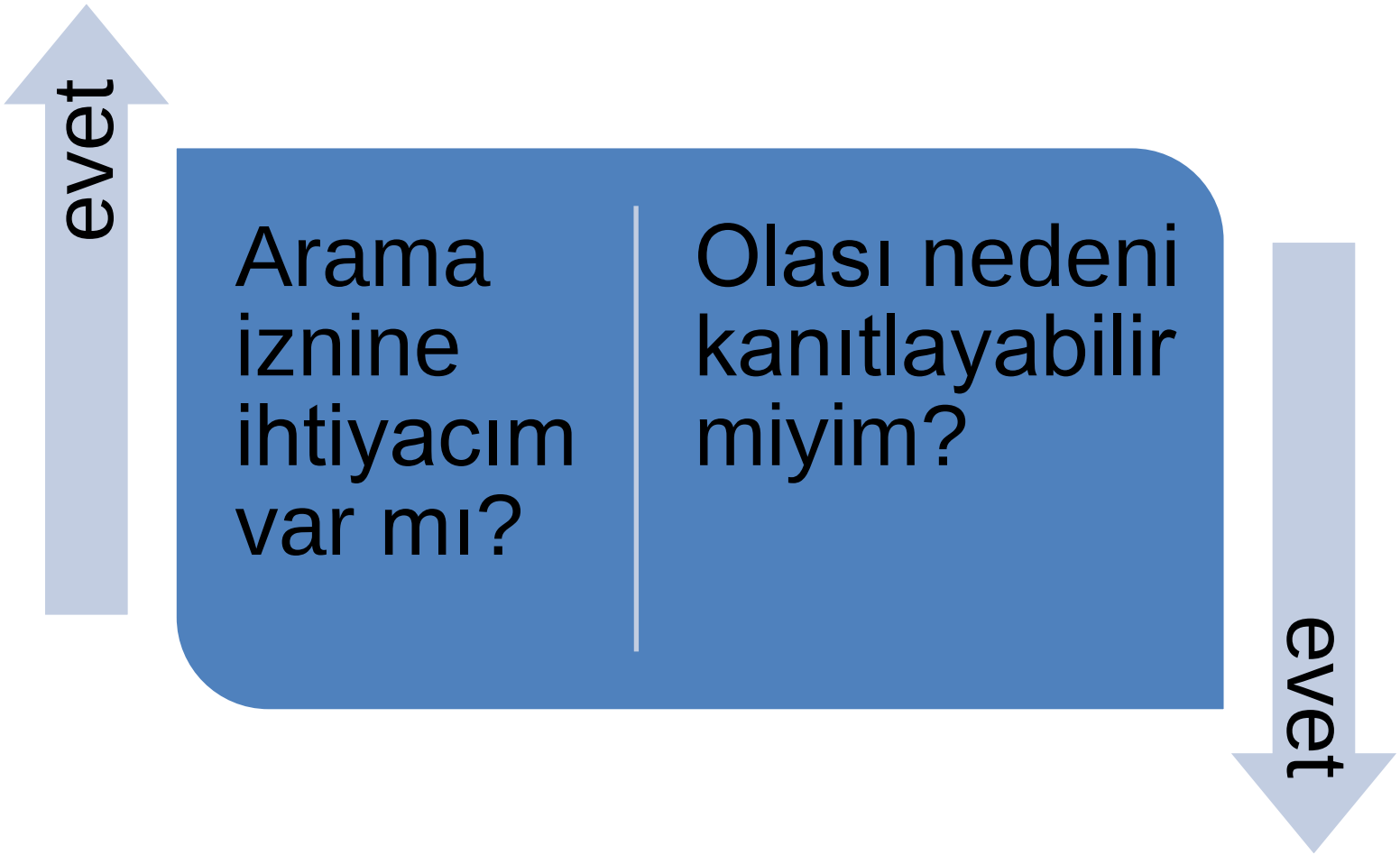


# Resmi belgelerin düzenlenmesi - güvenceler

Koşullar ve güvenceler aşağıdaki koşullarda dikkate alınmalı ve temin edilmelidir:

- **Başvurunun** düzenlenmesi
- Başvurunun **görülmesi** esnasında
- **Emrin/yetkinin** düzenlenmesi
- Usule ilişkin yetkilerin **kullanılması**

# Başvurunun düzenlenmesi



# Başvurunun düzenlenmesi
# Gerekli belgeler

- Gerekli belgeler yetki alanına bağlı olarak değişiklik gösterir!
- Belgeler şunları içerebilir:

  – Usule ilişkin yetkiyi kullanma yetkisi veren karar için **başvuru**
  – Başvuru sahibinin **taahhüdü/yeminli beyanı**
  – **Taslak karar**
  – İlgili cezai soruşturmaya ilişkin **destekleyici belgeler**
  – Usule ilişkin yetkinin kullanılmasıyla ilgili **karşılıklı yardım talebi**

# Başvurunun düzenlenmesi
# Gerekli belgeler

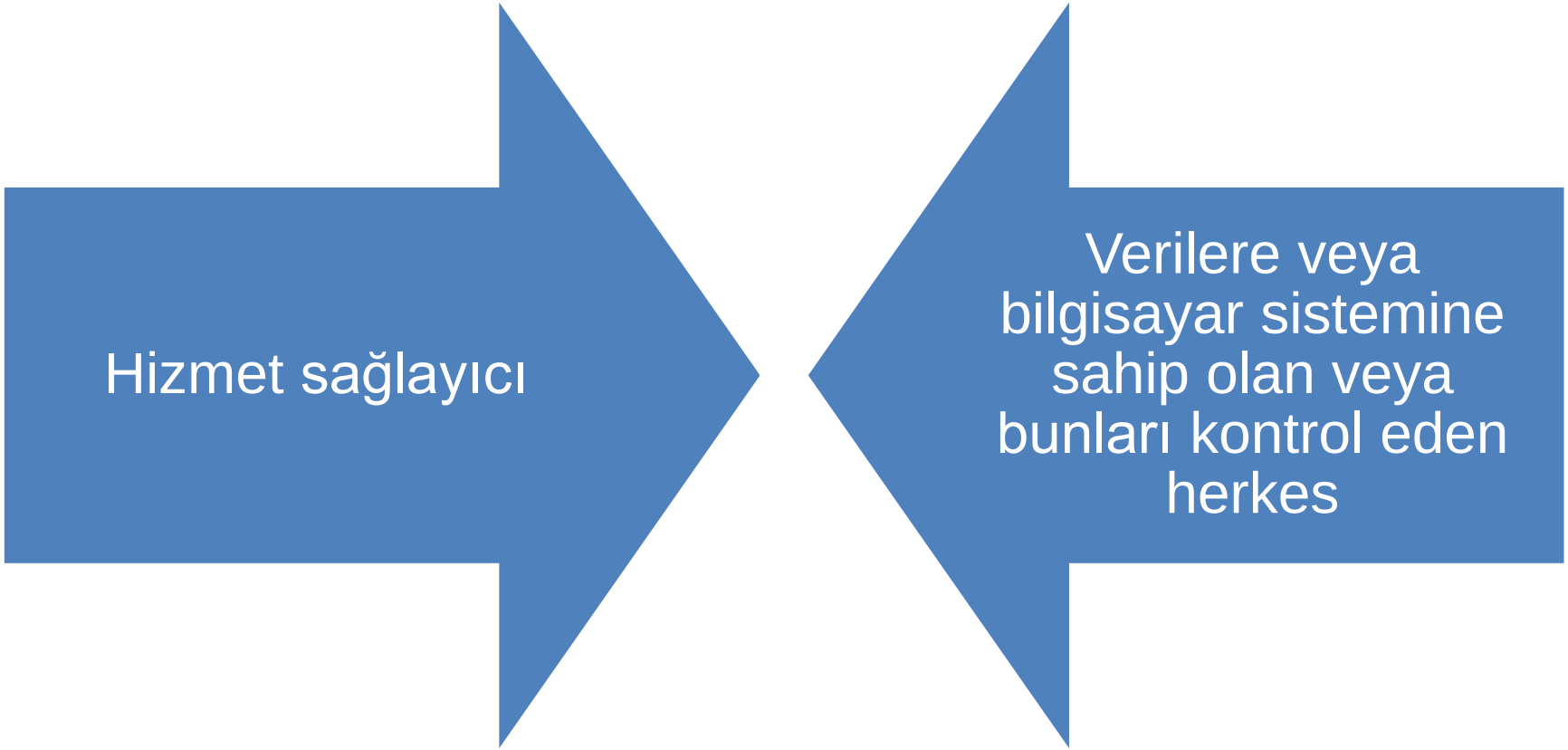

- **Yetkiyi kullanacak görevliye eşlik edecek kişileri listeleyin**
- Katılımlarının neden gerektiğini **açıklayın**
- Katılımlarının şüphelinin **gizlilik hakkı** üzerindeki **etkisini açıklayın**

# Başvurunun düzenlenmesi
# Gerekli belgeler

- İlgili cezai soruşturma detaylarının kısa özeti

- Bu şunları içerebilir:
  - Cezai soruşturmanın **açıklaması**
  - **Suçların** listesi
  - Suça uygun **cezalar** (ceza eşiğinin uygulanması gerektiğinde)
  - **Diğer ilgili soruşturmaların** detayları (ör. organize suç örgütlerine karşı soruşturma yapılması durumunda)

# Başvurunun konusu

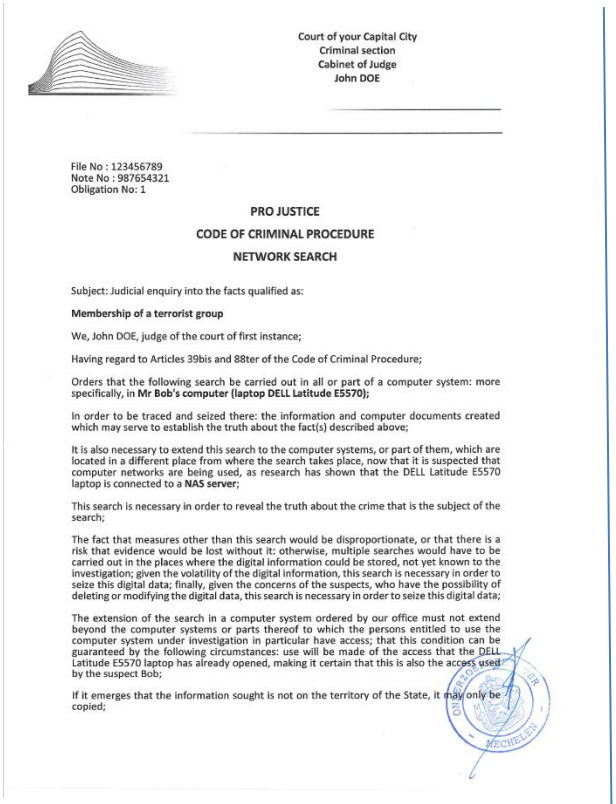


# Yetkinin düzenlenmesi - Arama izni

# Arama ve el koyma izinleri

- Dijital delillere özgü dil
- Saha dışı adli analiz için yetki
- Aramada kullanılan adli tekniklerde sınırlama yok
- İnceleme için izin verilen süre
- Hariç tutulan malzemeler

# Yetkinin düzenlenmesi - Arama izni



Court of your Capital City
Criminal section
Cabinet of Judge
John DOE

File No : 123456789
Note No : 987654321
Obligation No: 1

**PRO JUSTICE**

**CODE OF CRIMINAL PROCEDURE**

**NETWORK SEARCH**

Subject: Judicial enquiry into the facts qualified as:

**Membership of a terrorist group**

We, John DOE, judge of the court of first instance;

Having regard to Articles 39bis and 88ter of the Code of Criminal Procedure;

Orders that the following search be carried out in all or part of a computer system: more specifically, in **Mr Bob's computer (laptop DELL Latitude E5570);**

In order to be traced and seized there: the information and computer documents created which may serve to establish the truth about the fact(s) described above;

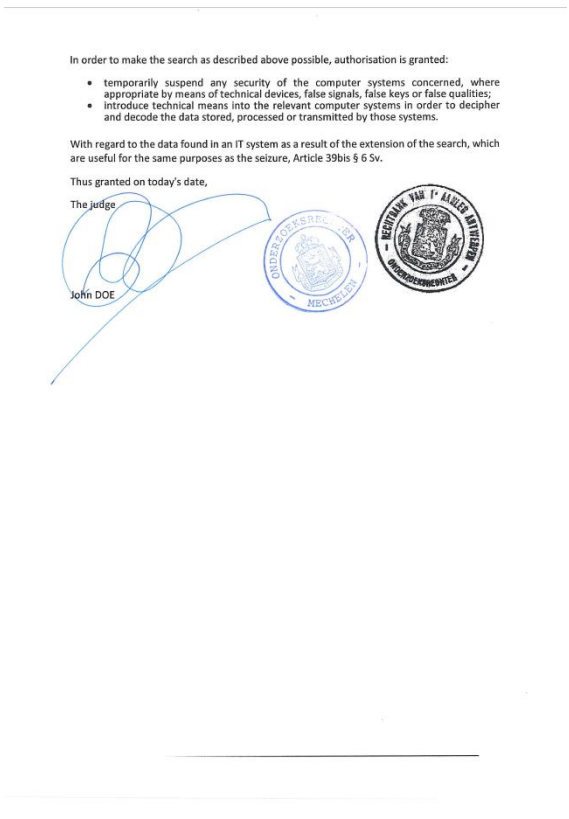
It is also necessary to extend this search to the computer systems, or part of them, which are located in a different place from where the search takes place, now that it is suspected that computer networks are being used, as research has shown that the DELL Latitude E5570 laptop is connected to a **NAS server**;

This search is necessary in order to reveal the truth about the crime that is the subject of the search;

The fact that measures other than this search would be disproportionate, or that there is a risk that evidence would be lost without it: otherwise, multiple searches would have to be carried out in the places where the digital information could be stored, not yet known to the investigation; given the volatility of the digital information, this search is necessary in order to seize this digital data; finally, given the concerns of the suspects, who have the possibility of deleting or modifying the digital data, this search is necessary in order to seize this digital data;

The extension of the search in a computer system ordered by our office must not extend beyond the computer systems or parts thereof to which the persons entitled to use the computer system under investigation in particular have access; that this condition can be guaranteed by the following circumstances: use will be made of the access that the DELL Latitude E5570 laptop has already opened, making it certain that this is also the access used by the suspect Bob;

If it emerges that the information sought is not on the territory of the State, it may only be copied;



In order to make the search as described above possible, authorisation is granted:

- temporarily suspend any security of the computer systems concerned, where appropriate by means of technical devices, false signals, false keys or false qualities;
- introduce technical means into the relevant computer systems in order to decipher and decode the data stored, processed or transmitted by those systems.

With regard to the data found in an IT system as a result of the extension of the search, which are useful for the same purposes as the seizure, Article 39bis § 6 Sv.

Thus granted on today's date,

The judge

John DOE

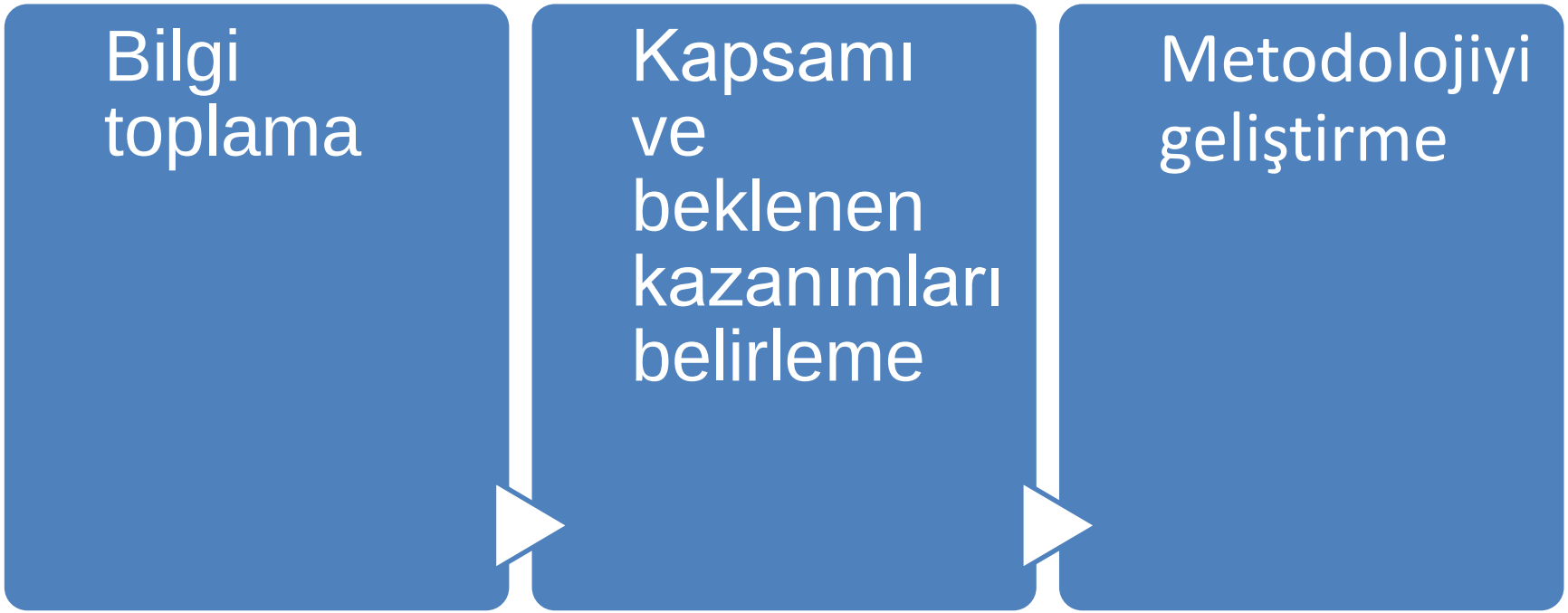
Network search
19 BC

# İKİNCİ BÖLÜM
## Arama öncesi planlama

- Soruşturmanın türü hakkında ayrıntılı bilgi edinin
- Baş soruşturma görevlisinin/savcının neye ulaşmayı umduğunu tartışın ve değerlendirin
- Metodolojinizi geliştirin
- Aramayı yürütün

# Arama öncesi planlama

# Arama öncesi planlama



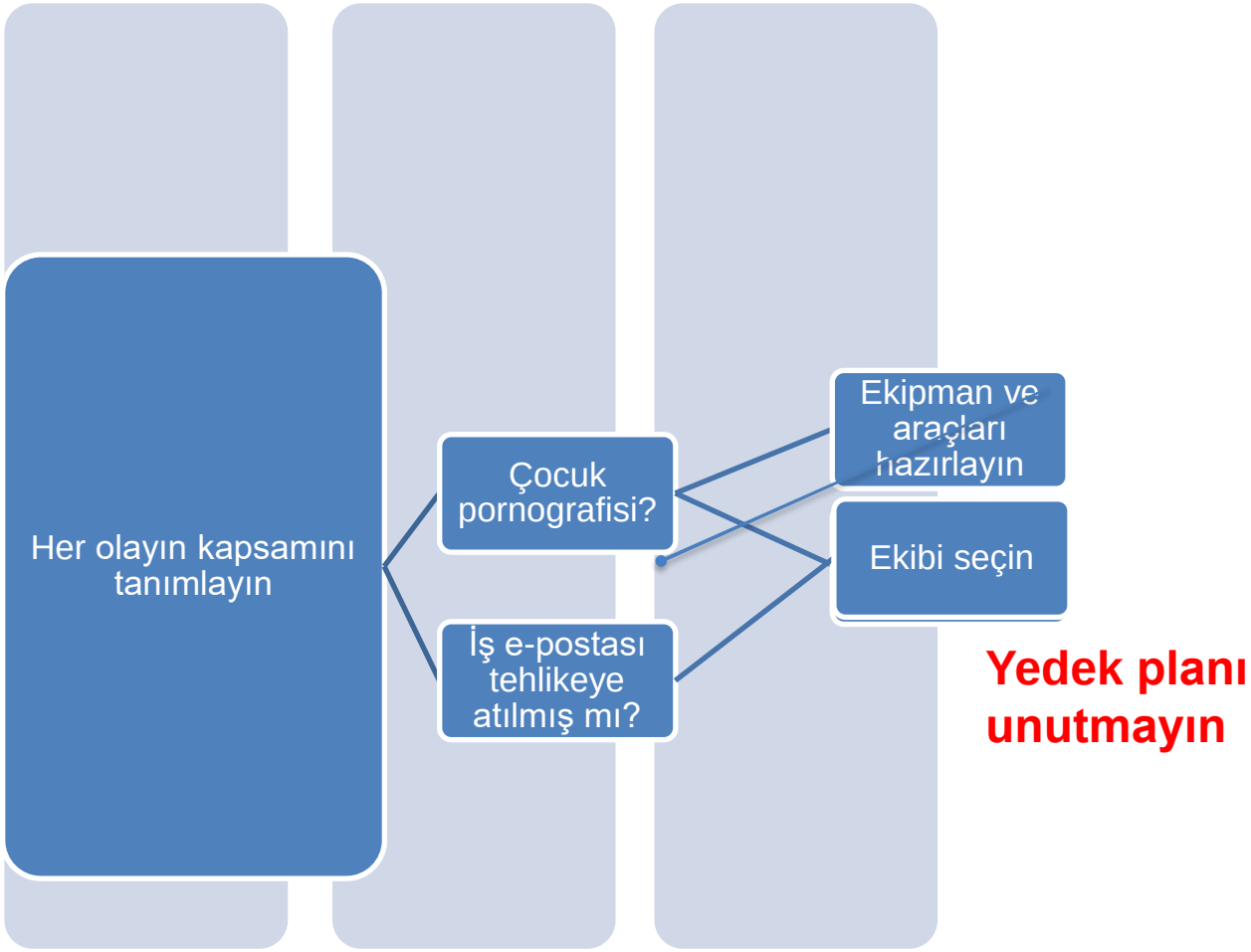
# Arama Öncesi Planlama: Bilgi Toplama

# Arama Öncesi Planlama: Bilgi Toplama

# Arama Öncesi Planlama: Kapsam

# Arama Öncesi Planlama: Kapsam

## Kapsam ve beklentiler




**Yedek planı unutmayın**

# Arama Öncesi Planlama: Metodoloji

## Metodolojiyi Geliştirin

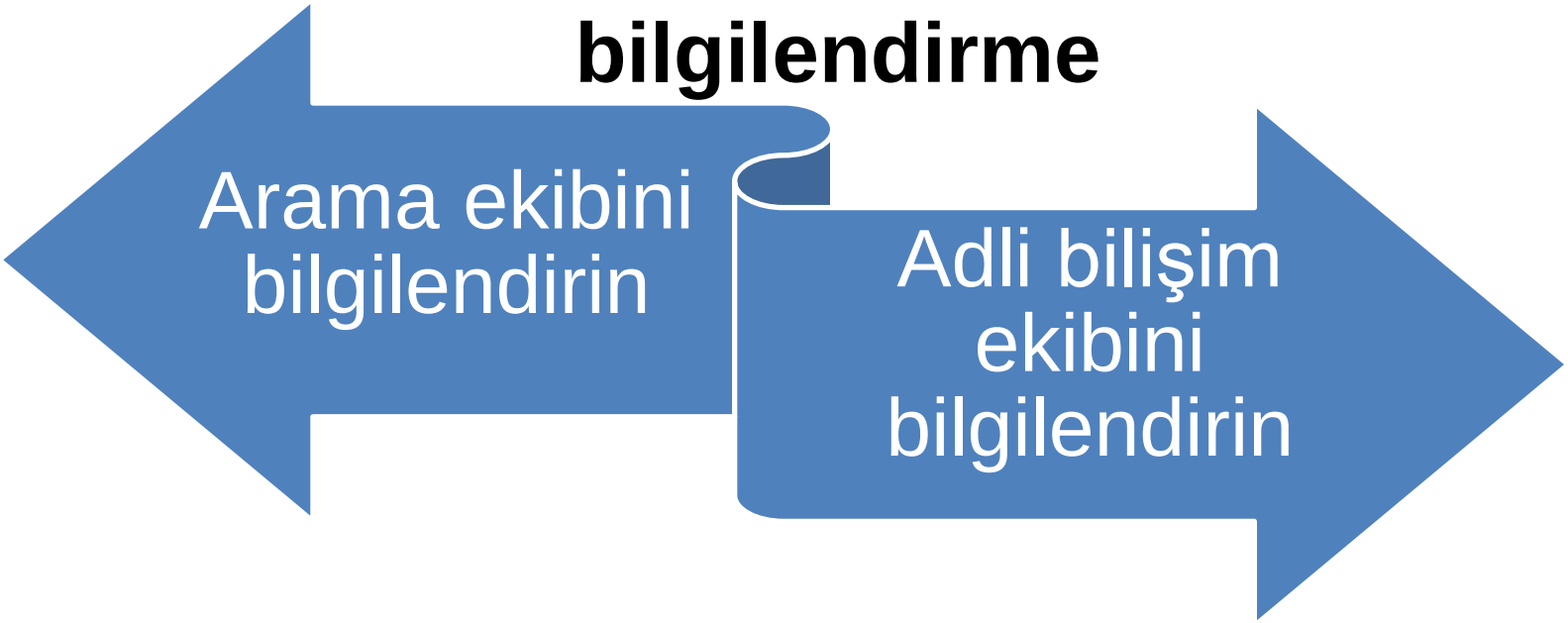
# Arama Öncesi Planlama: Metodoloji

## Metodolojiyi Geliştirin

Canlı adli veri metodolojisine ilişkin hususlar

- Uçuculuk sırasına uyulması
- Öncelikle en az müdahaleci eylemin gerçekleştirilmesi
- Öncelikle en değerli verilerin toplanması
- Her şeyin belgelenmesi
- Cihaz türü
- Cihaza nasıl erişileceği (yerel ana bilgisayar - uzaktaki ana bilgisayar - uzaktaki sunucu)

# ÜÇÜNCÜ BÖLÜM
# Arama öncesi bilgilendirme



# Arama ekibinin bilgilendirilmesi

- Depolama ortamının tanımlanması (büyük cihazlar)
- Elektronik delillerin güvenliğinin sağlanması (delillerin korunması)
- Kişilerin aranması ve bulunan eşyalara el konulması (Sistematik olun - Belgelendirin)
- Formun doldurulması

# Arama Öncesi Bilgilendirme

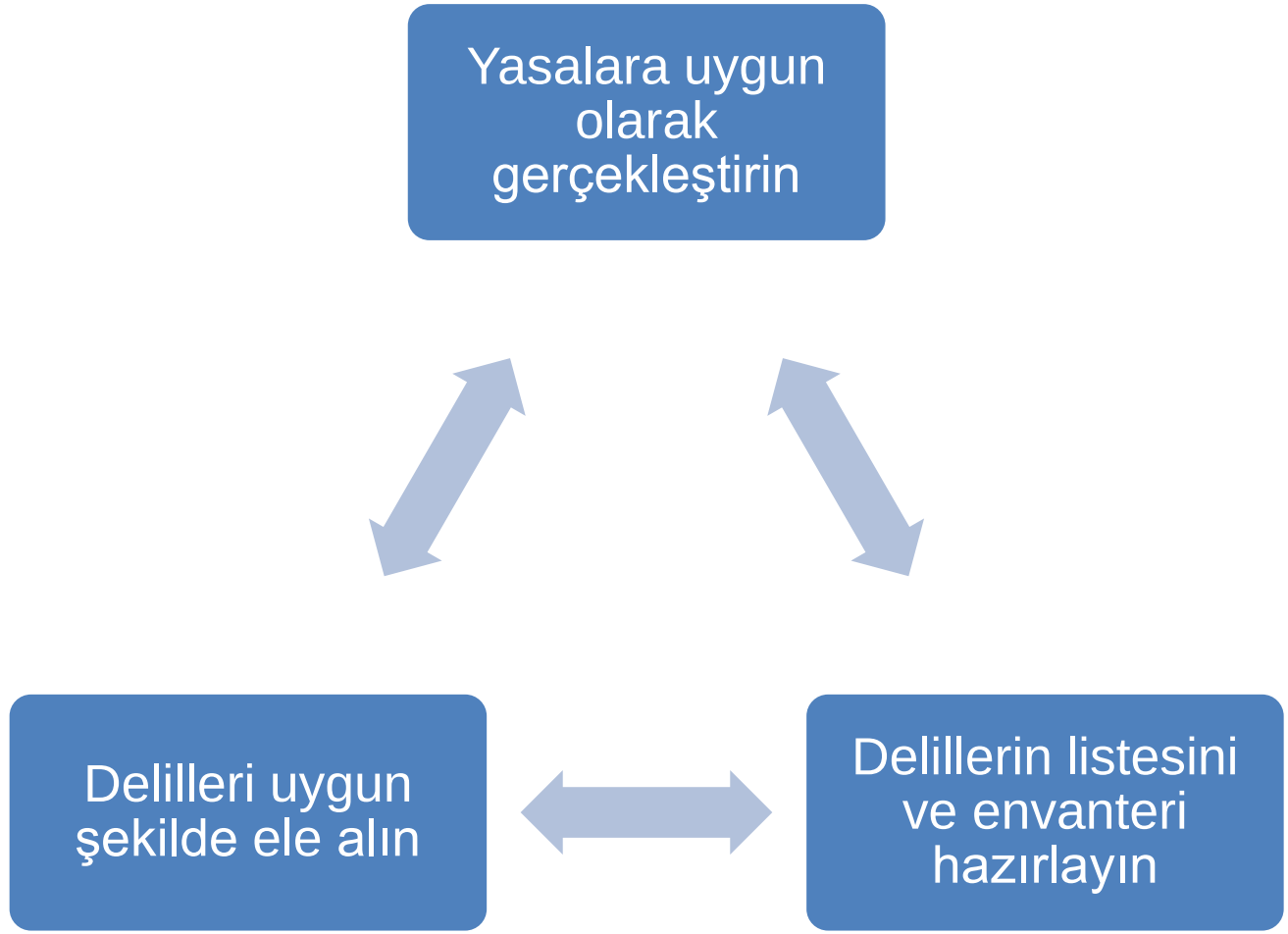
## Adli bilişim ekibinin bilgilendirilmesi

- Canlı sistemler için hangi usulün uygulanacağı
- Hangi ekipmanın mevcut olduğu
- Usulü kimin gerçekleştireceği
- Canlı veri incelemesinin planlanması

# Arama Öncesi Bilgilendirme

# Aramanın Yürütülmesi

# Aramanın Yürütülmesi



# Aramanın Yürütülmesi

# Rapor - Arama Sonrası

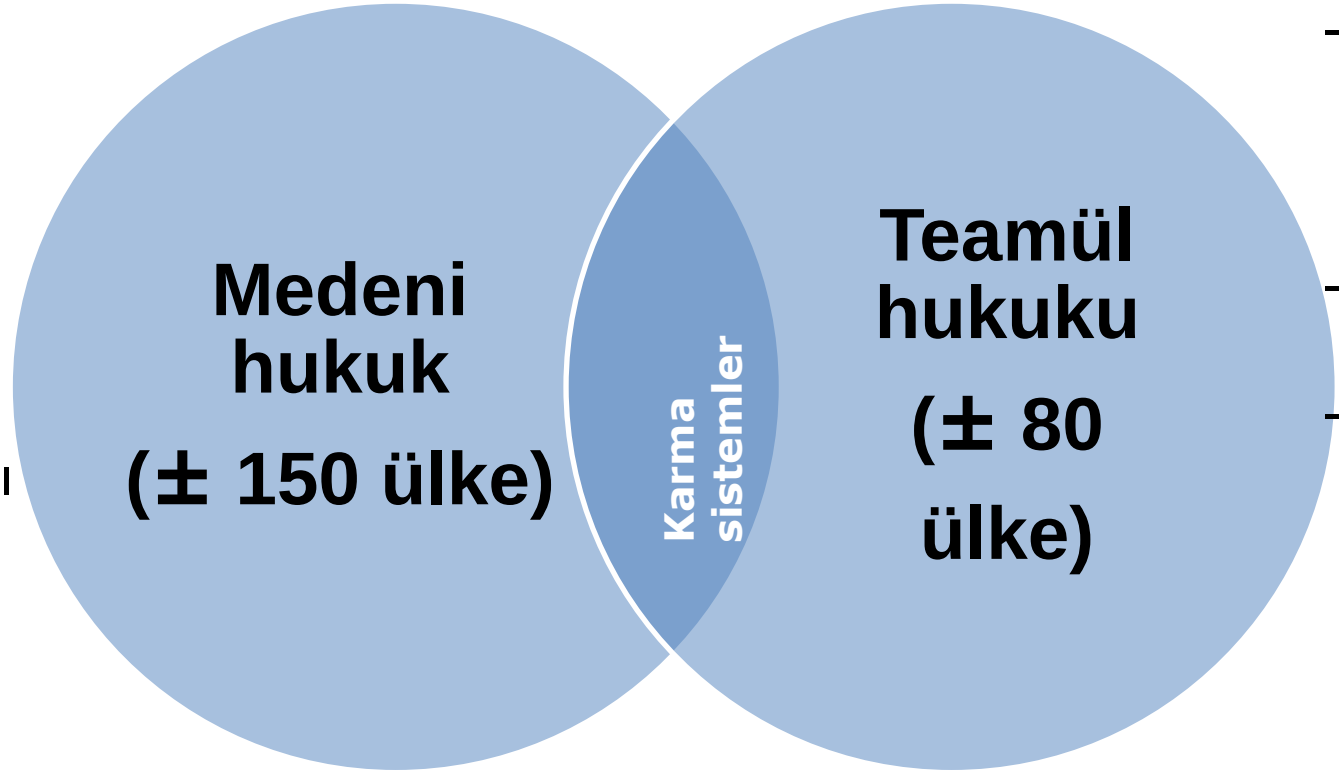
### 6.4 Report for forensic analysis of computer systems, computer data and digital devices

| | | |
|---|---|---|
| 1 | **Date and time** | |
| 2 | **Location/address where the activity is conducted** | |
| 3 | **Reference/Case number** | |
| 4 | **Authority in charge with the case** | |
| 5 | **Reference/number of the Authorization/Court Order and Issuing Authority** | |
| 6 | **Identification of the person/persons conducting the activity** | |
| 7 | **Identification of the person/persons assisting in the activity** | *people identified/arriving at the location* |
| | | *suspect/s* |
| | | *witness/s* |
| | | *lawyer/s* |
| | | *others* |
| 8 | **Description on how the computer systems or digital devices were packaged and sealed** | |
| 9 | **Identification of the computer systems or digital devices to be forensically analysed** | |
| 10 | **Identification of the hardware devices/software used to clone (imaging) the computer data** | *if applicable* |
| 11 | **Date and time when the cloning (imaging) started/ended** | *if applicable* |
| 12 | **Description of the storage media used to export the results obtained following the cloning (imaging)** | *if applicable* |
| 13 | **Identification of the hardware devices/software applications used for the forensic analysis** | |
| 14 | **Date and time when the forensic analysis started/ended** | |
| 15 | **Description of the forensic analysis (steps followed) on chronological order** | |
| 16 | **Reference to the technical report generated by the software applications used for the forensic analysis** | *if applicable* |
| 17 | **Description of the storage media used to export the results obtained following the forensic analysis** | *DVD/Hard disk* |
| 18 | **Description of computer systems and digital devices to be packaged and sealed after the forensic analysis** | |
| 19 | **Time when the forensic analysis ended** | |
| 20 | **Signature of the person/persons who conducted the forensic analysis** | |
| 21 | **Comments and signature of the person/persons from whom the evidence was seized** | |

# DÖRDÜNCÜ BÖLÜM
# Delillerin değerlendirilmesi

# Delillerin değerlendirilmesi

- Yazılı kanunlar
- Yargıç öncülük eder
- Soruşturmaya dayalı sistem
- Kapsamlı duruşma öncesi soruşturma
- Avukatlar tarafından sözlü tartışman




- İçtihat hukuku
- Yargıç "hakem" görevi görür
- Çekişmeli sistem
- Savcılık ve savunma arasında rekabetçi süreç
- Hukuk ve olgular üzerinde avukatları

# Elektronik Delillerin Değerlendirilmesi

## Hüküm Verme

# Elektronik Delillerin Değerlendirilmesi

## Eğitimli hakimler

# Elektronik Delillerin Değerlendirilmesi

## Delillere itiraz

# Delillere itiraz

## Savcı

- Kabul edilebilirliğin gösterilmesi
- Verilerin nasıl yönetildiğinin ve delil zincirinin gösterilmesi
- Delillerin aslına uygunluğunun kanıtlanması

## Savunma avukatı

- Delillere itiraz
  - Delillerin alternatif açıklamaları
  - Elektronik delillerin bütünlüğü sorununun gündeme getirilmesi

  Teknik (örn. korumasız kablosuz ağlar; IP tanımlamasının güvenilirliği)

  Usullere uymama

  Delil zincirinin kırılması
- Delil toplayan kişiye itiraz
- Toplanma şekline itiraz
  - Uzman - polis
  - Adli bilişim uzmanı

# Elektronik Delillerin Değerlendirilmesi

Bilgisayarda el koyulan resim

SHA-1: a109957cc2b78392e60bd2a3b1277243c170390f
MD5: feaaabf31c2e1ba2c7971a274bd8a414

**KARMA DEĞER =**

Mahkemede sunulan resim

SHA-1: a109957cc2b78392e60bd2a3b1277243c170390f
MD5: feaaabf31c2e1ba2c7971a274bd8a414

# Delillerin değerlendirilmesi

Bilgisayarda el koyulan resim

**KARMA DEĞER ≠**

Mahkemede sunulan resim

SHA-1: a109957cc2b78392e60bd2a3b1277243c170390f
MD5: feaaabf31c2e1ba2c7971a274bd8a414

SHA-1: 0265c76dfd67b50e261ed2db177ea55f593b2e94
MD5: d107862578e78810eed3871cd7b9ce50

# Elektronik Delillerin Sunumu

# Elektronik Delillerin Sunumu

## Kim sunacak?

- savcı
- soruşturma görevlisi
- adli bilişim uzmanı

## Sunum yöntemi

- Power Point?
- Teknik kelimeler için sözlük?
- Gösteriler

# Delillerin değerlendirilmesi

Karar

# Karar


Teşekkürler
Ende