

# Computer Forensics and Cyber crime

## Definition

---

### **Computer Forensics and cyber crime analysis**

01GZDUV, 01GZDUW

A.A. 2024/25

# Agenda

---

## 1. Introduction

- ☐ *Digital/Electronic Evidence*
- ☐ *Case Law on Digital/Electronic Evidence*
- ☐ *Digital Forensics Definition*

## 2. Digital Forensics Procedure

- ☐ *Identify the Suspect*
- ☐ *Detecting and Seizing Illegal Contents*
- ☐ *Validating Digital Evidence*
- ☐ *Chain of Custody after Seizure*
- ☐ *Analysis of Digital Evidence*
- ☐ *Reporting of Digital Evidence Findings*

## 3. Privacy and Due Process Rights

- ☐ *Surveillance*
- ☐ *Cloud Computing: Jurisdiction and Privacy*

## What is Digital/Electronic Evidence?

---

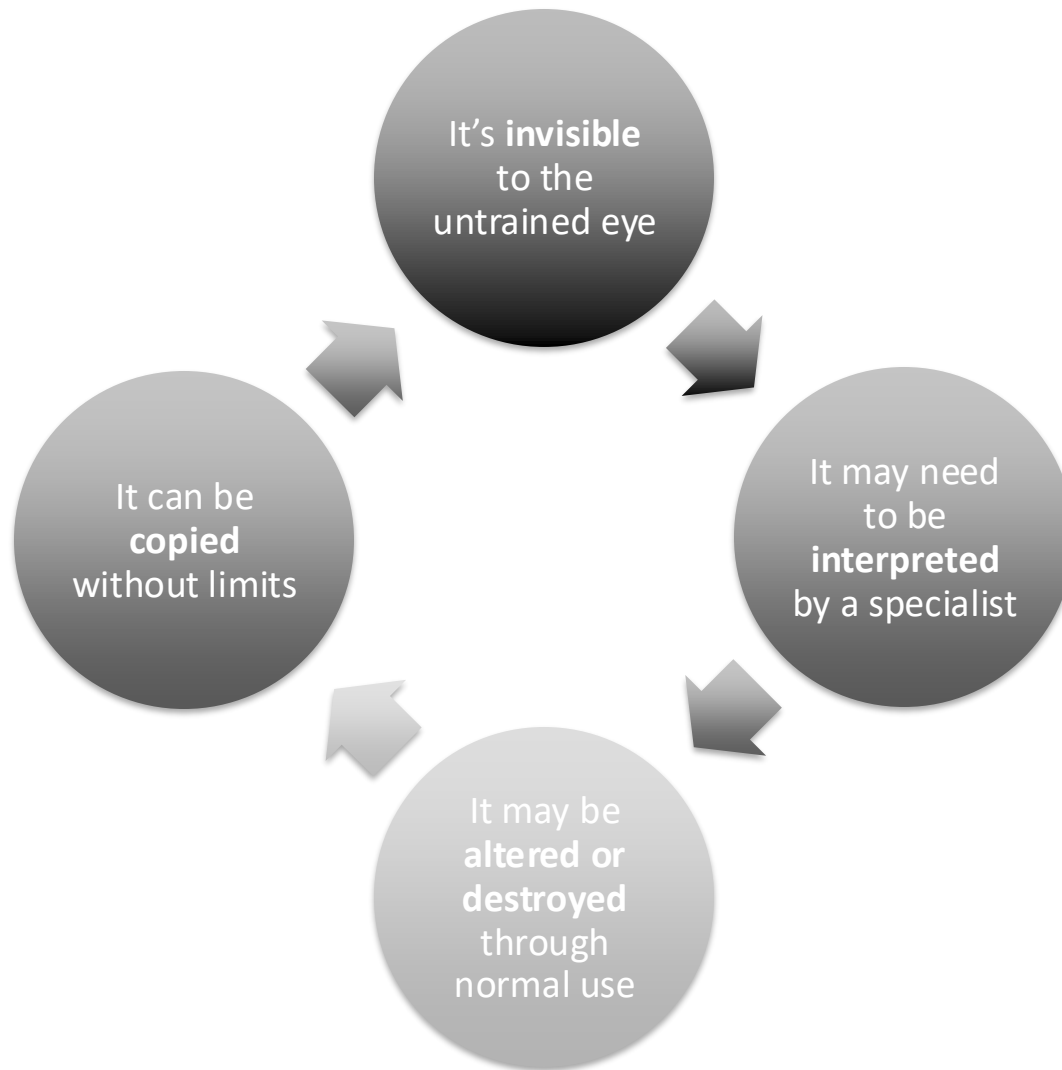
**Digital evidence** is 'any information of evidential value whether memorized or sent in a digital format' - definition by the Scientific Working Group on Digital Evidence (SWGDE )

**Digital evidence** or **electronic evidence** is 'any probative information stored or transmitted in digital form that a party to a court case may use at trial' (Eoghan Casey - 2004)

**Electronic evidence** is information generated, stored or transmitted using electronic devices that may be relied upon in court (Council of Europe - 2013)

# What is Digital Electronic/Evidence?

---



# Legal Requirements of Digital/Electronic Evidence?

---



# How to find a Digital/Electronic Evidence?

---



## How to find a Digital/Electronic Evidence?



<http://item.rakuten.co.jp/sastore/yeah-256/>

[http://thumbnail.image.rakuten.co.jp/@0\\_mall/sastore/cabinet/0img10621966667.jpg](http://thumbnail.image.rakuten.co.jp/@0_mall/sastore/cabinet/0img10621966667.jpg)



<http://www.solidalliance.com/press/press.html>



[http://thumbnail.image.rakuten.co.jp/@0\\_mall/sastore/cabinet/0img10621155722.jpg](http://thumbnail.image.rakuten.co.jp/@0_mall/sastore/cabinet/0img10621155722.jpg)

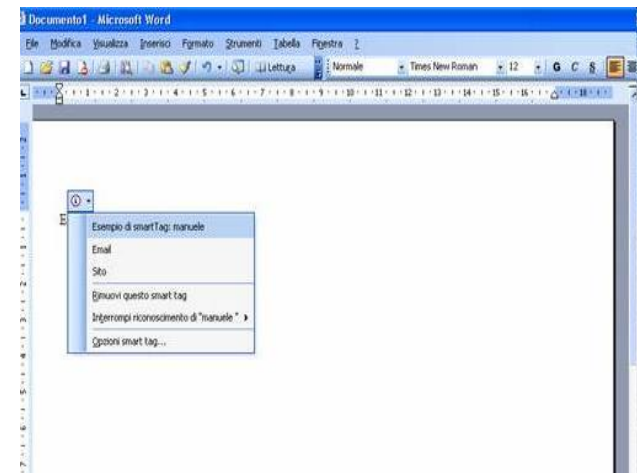
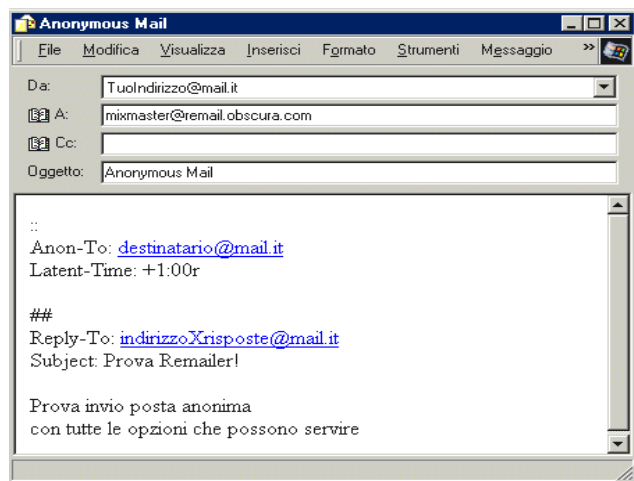
# Categories of Digital/Electronic Evidence

---

There are three types of digital evidence.

**Created by man:** any piece of digital data that is the result of a step or action taken by a human person. It can be of two types:

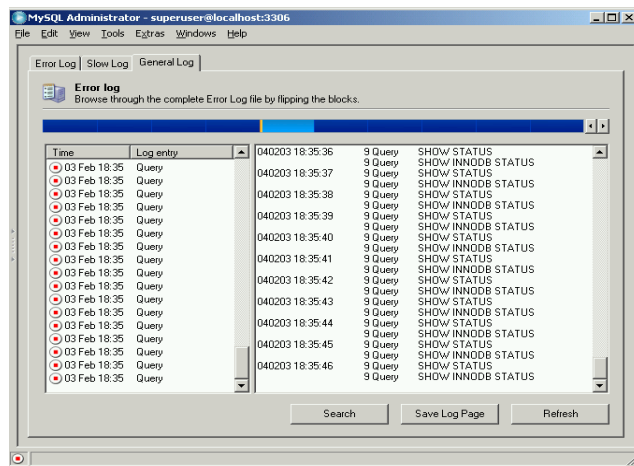
- a) Human to human (mail)
- b) Human to PC (Word document)





# Categories of Digital/Electronic Evidence

**Created independently by the computer:** any piece of digital data that is the result of the processing of data carried out by a software in accordance with a specific algorithm and without human intervention (e.g. telephone records or Internet Service Provider logs)



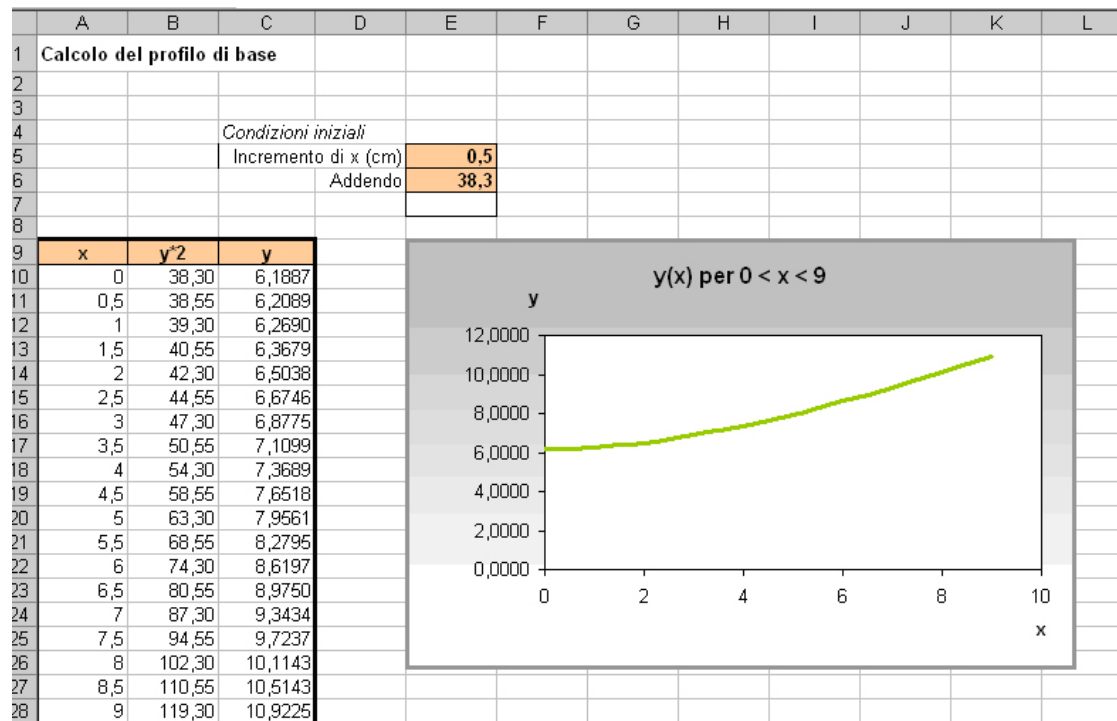
The screenshot shows the Log Analyzer interface. The 'Referring domains' and 'Referring URLs' sections are visible. The 'Referring domains' section shows a list of domains and their counts. The 'Referring URLs' section shows a list of URLs and their counts.

Referring domains	Count
Total	17027
www.actualcoach.com	9615 (56%)
www.soft32.com	949 (5%)
www.free-downloads.net	692 (4%)
www.downloads.ch	476 (2%)
www.gamesbum.com	368 (2%)
www.ultrasoftware.net	299 (1%)
games.soft32.com	249 (1%)
download.com.com	212 (1%)
www.gamearchives.com	175 (1%)
www.downloadatooz.com	158 (0%)
actualcoach.com	139 (0%)
www.download4you.com	136 (0%)
softak.com	125 (0%)
www.regnow.com	121 (0%)
www.indir.com	120 (0%)
baixaki.uq.com.br	116 (0%)
www.google.com	95 (0%)
softobzor.net	91 (0%)
www.stahuj.cz	88 (0%)
www.100files.com	86 (0%)

Referring URLs	Count
Total	17027
www.actualcoach.com/	6064 (35%)
www.actualcoach.com/screenshots.html	1387 (8%)
www.free-downloads.net/sub_category/Sports	638 (3%)
www.soft32.com/index-2-5-50-1-4.html	478 (2%)
www.downloads.ch/files/games/sports/	434 (2%)
www.actualcoach.com/download	397 (2%)
www.actualcoach.com	386 (2%)
www.soft32.com/index-2-5-51-1-4.html	365 (2%)
www.actualcoach.com/awards.html	341 (2%)
www.actualcoach.com/RUS/	293 (1%)
www.ultrasoftware.net/archive/category/Result	250 (1%)
www.gamearchives.com/sports.html	175 (1%)
www.actualcoach.com/index.htm	161 (0%)
www.downloadatooz.com/download.php	158 (0%)
games.soft32.com/index-2-5-50-0-4.html	153 (0%)
www.gamesbum.com/Games/Arcade/index6.ht	145 (0%)
download.com.com/2001-7427-10194501.html	145 (0%)
www.download4you.com/php/search.php	131 (0%)
www.regnow.com/softself/visitor.cgi	121 (0%)
actualcoach.com/	120 (0%)

## Categories of Digital/Electronic Evidence

**Created by both man and the computer:** an electronic spreadsheet where data is entered by the human, while the computer works out the result.



## The complex nature of digital evidence (the case of Julie Amero)

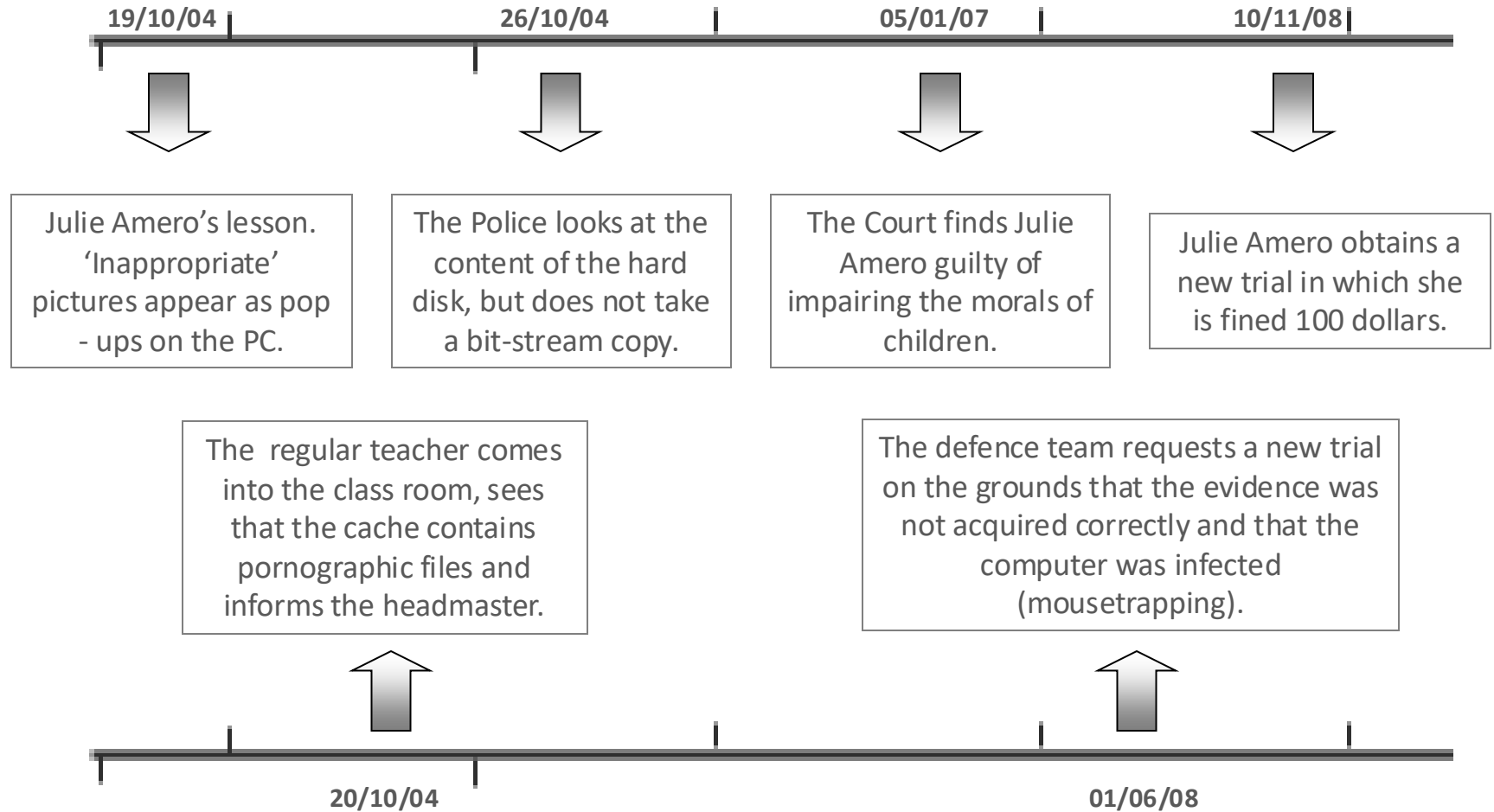
---

One of the principal characteristics of digital evidence is its complexity. One example is the Amero case.



Julie Amero is a supply teacher at Kelly School in Norwich, Connecticut who was found guilty of showing pornography to children under the age of 16

# The 'Amero' case: timeline

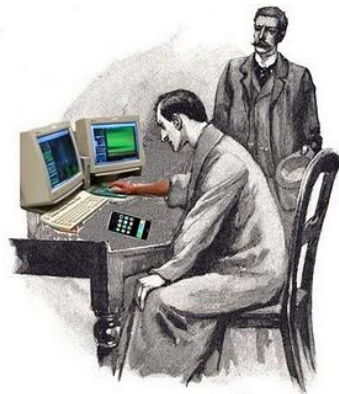


# What is Digital Forensics ?

---

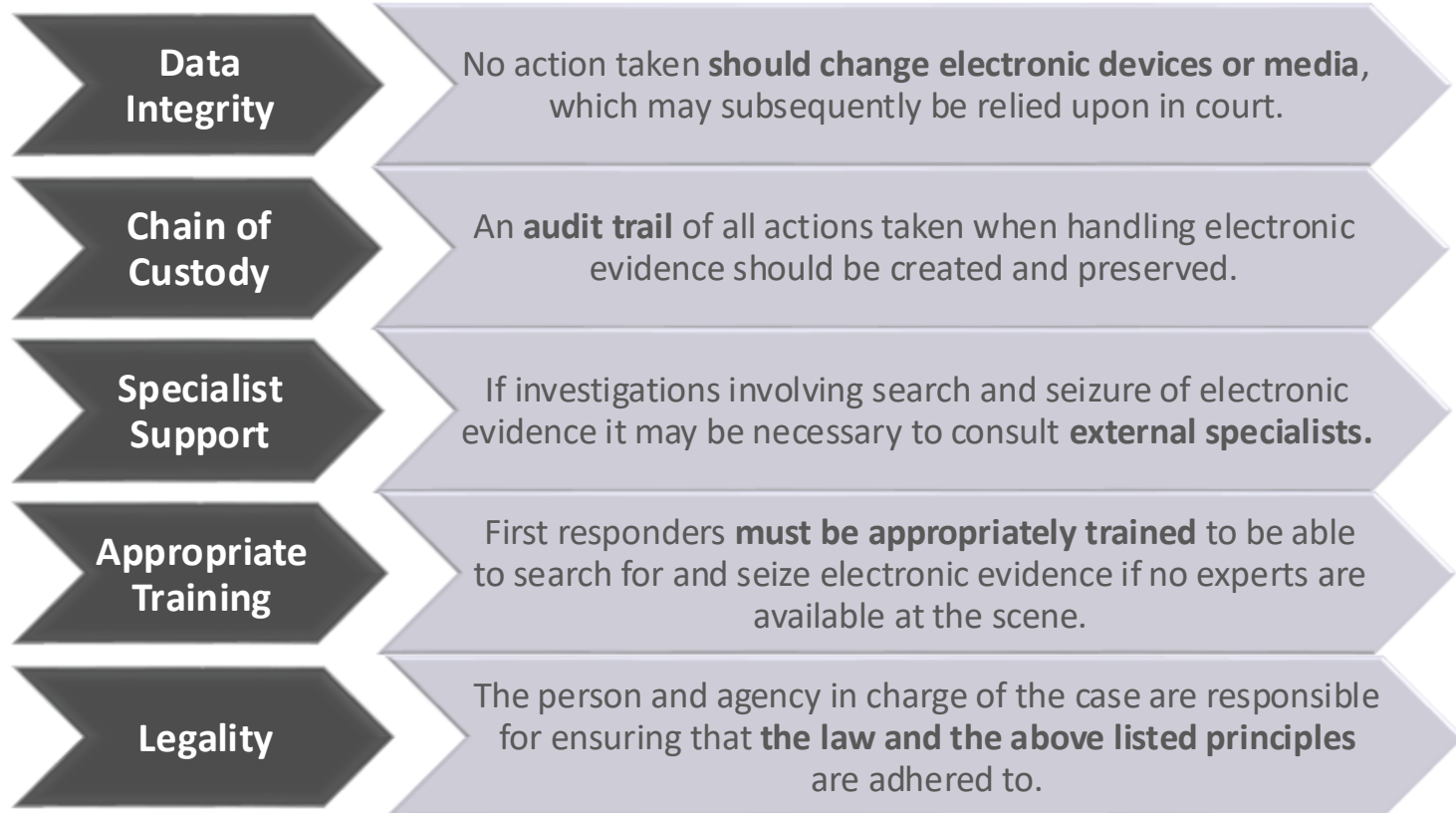
**Digital forensics**, in a traditional sense, is:

- get hold of evidence without modifying the IT system in which that evidence is found;
- ensure that the evidence acquired in another medium is identical to the original;
- analyse data without modifying it.



# The “Big Five” of Digital Forensics (Council of Europe)

---



---

# **Digital Investigation Procedure**

# Digital Investigation Procedure

---



Identify the Suspect



Detecting and Seizing Digital Evidence



Validating Digital Evidence



Chain of Custody



Analysis of Digital Evidence



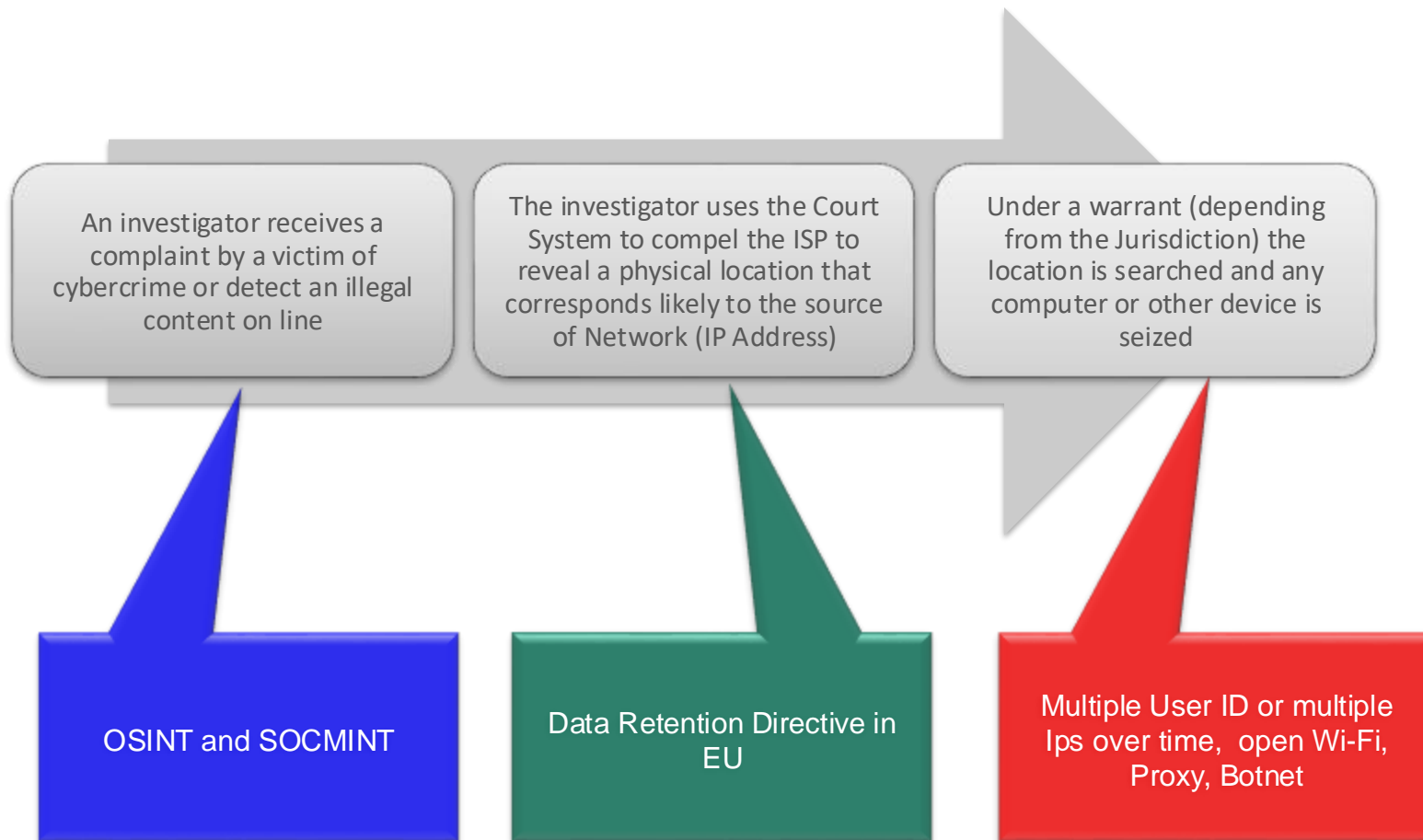
Presentation in Court



# Identify the Suspect

---

The general approach is the following:



## Identify the Suspect: Data Retention

---

- In the wake of the terrorist attacks in Madrid and London (respectively in 2004 and 2005), the European Parliament issued **Directive 2006/24/EC**.
- **Data retention** (or data preservation) generally refers to the storage of call detail records (CDRs) of **telephony** and **internet traffic** and **transaction data** (IPDRs) by governments and commercial organizations.
- Retention period: from **6** to **24 months**
- Scope of application: **serious crime**



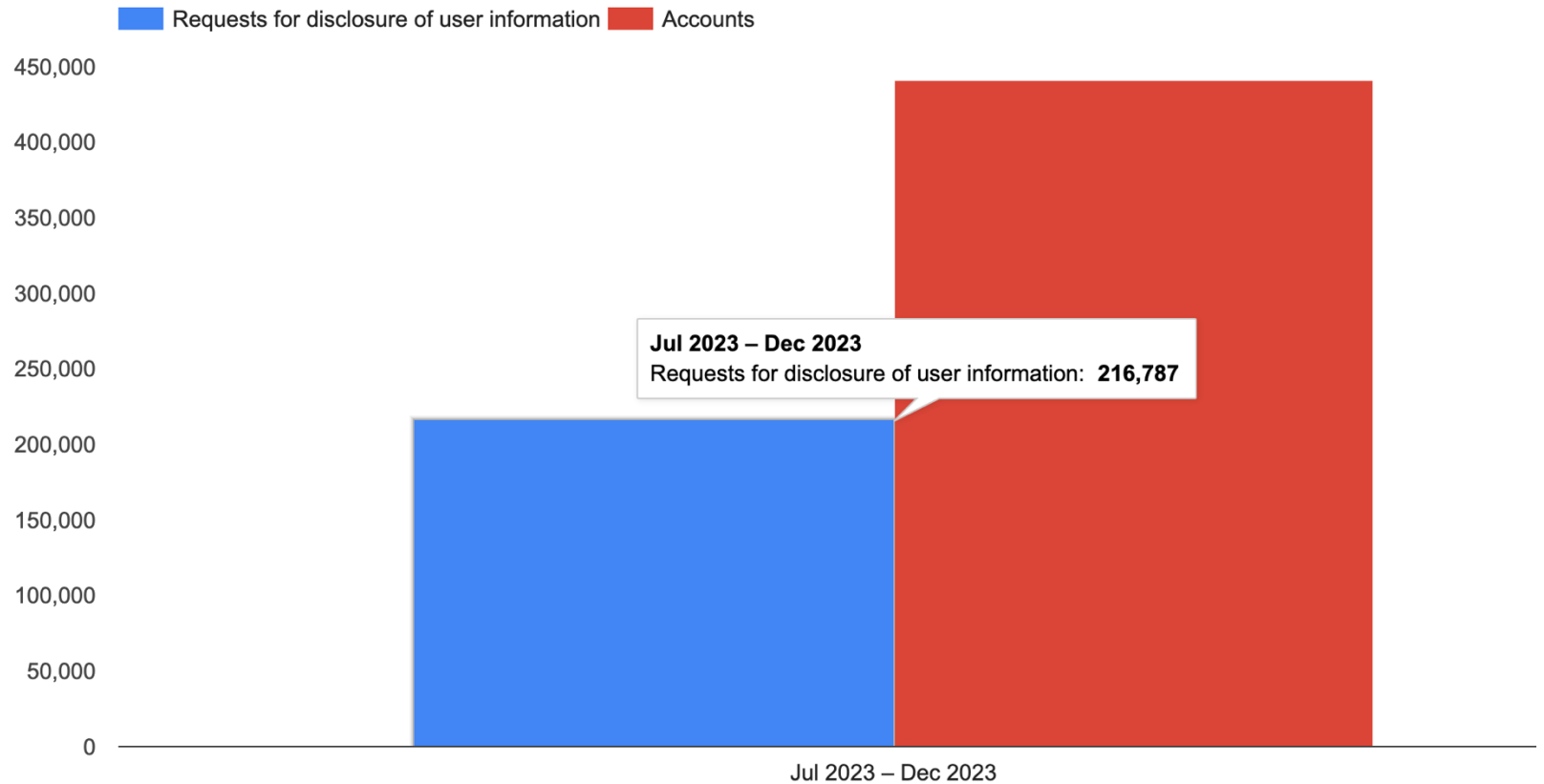
# Transparency Report: Google

---



## Transparency Report

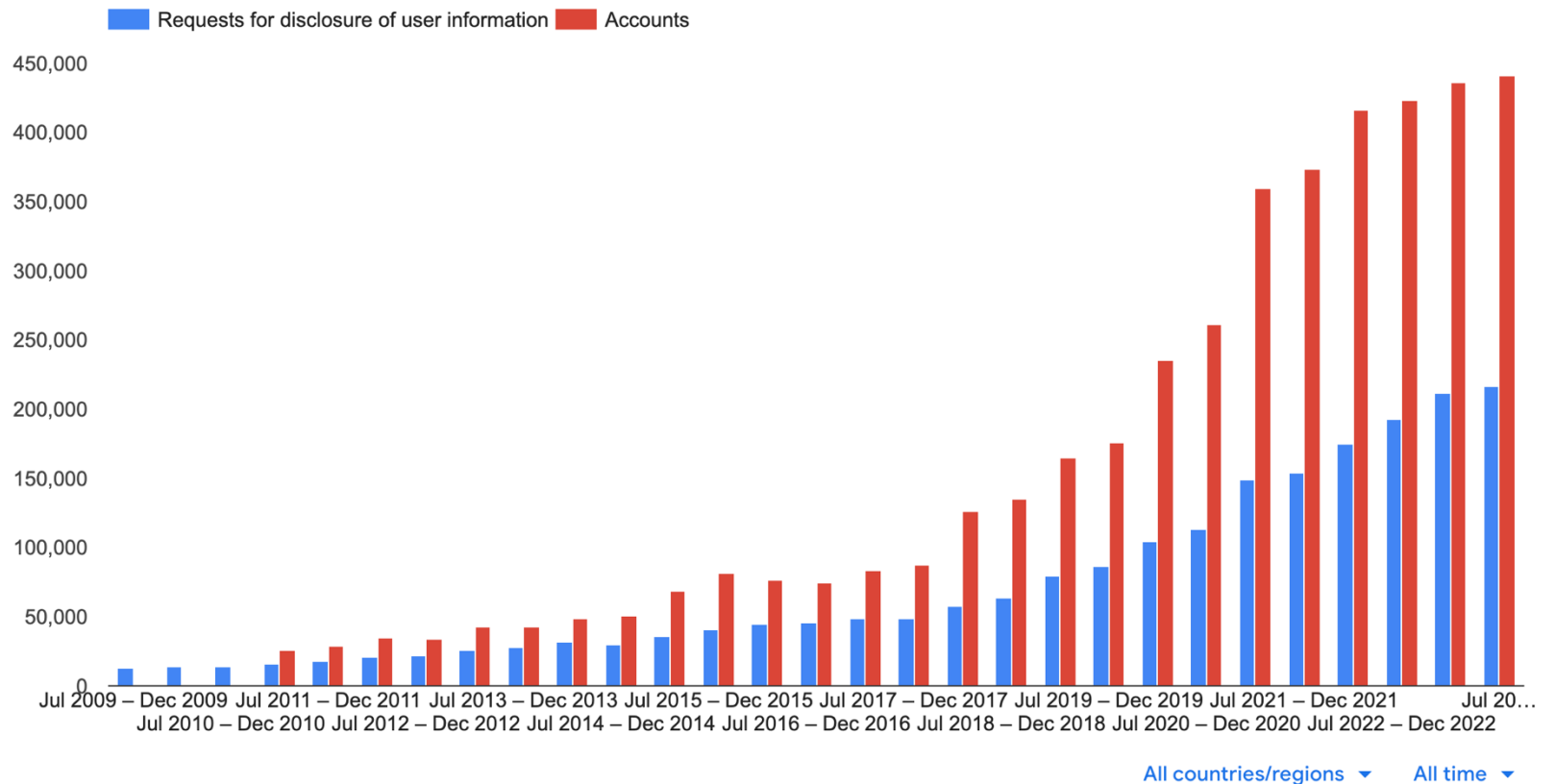
Global



# Transparency Report: Google



Global



## Transparency Report: Twitter

---

# Transparency Report

**TOTAL ACCOUNT  
SUSPENSIONS**

**5,296,870**

**TOTAL POSTS  
REMOVED OR LABELED**

**10,675,980**

**OVERALL POSTS  
VIOLATION RATE**

**0.0123%**



## Identify the Suspect – SOCMINT – Faces of Facebook

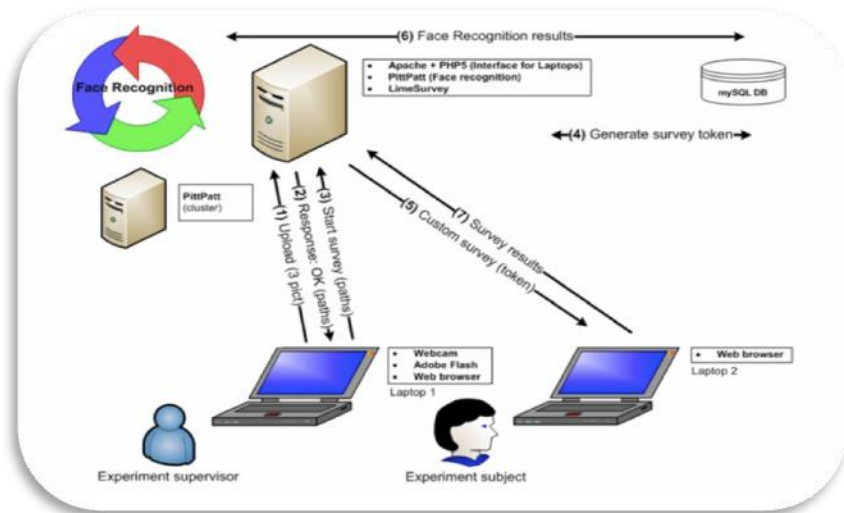
The research investigated the feasibility of combining publicly available Web 2.0 data with off-the-shelf face recognition software for the purpose of large-scale, automated individual re-identification. Two experiments demonstrated the ability of identifying strangers online (on a dating site) and offline (in a public space), based on photos made publicly available on a social network site.





# Identify the Suspect – Face Recognition Project

**Face Recognition Project**  
*Alessandro Acquisti*



**CCTV**  
*Fair Fax Media*





## Detecting and Seizing Digital Evidence: Bit-Stream Copy

---

Anyone wanting to seize and validate digital/electronic evidences (content of an e-mail or an entire hard-disk) has to respect two fundamental “rules”: **Bit-Stream Copy** and **Hash Function**

The bit-stream copy can ‘clone’ the entire hard-disk. It is a particular form of duplication in which the content of the physical unit is read sequentially loading the minimum quantity of data that can from time to time be directed, then recording it in the same sequence on a standard binary file, generating a physical image of the original medium.



## Seizing and Validating Digital Evidence: Hash Functions

---

During the forensic analysis of modifiable media, the Hash guarantees the **intangible** nature of the data that it contains.

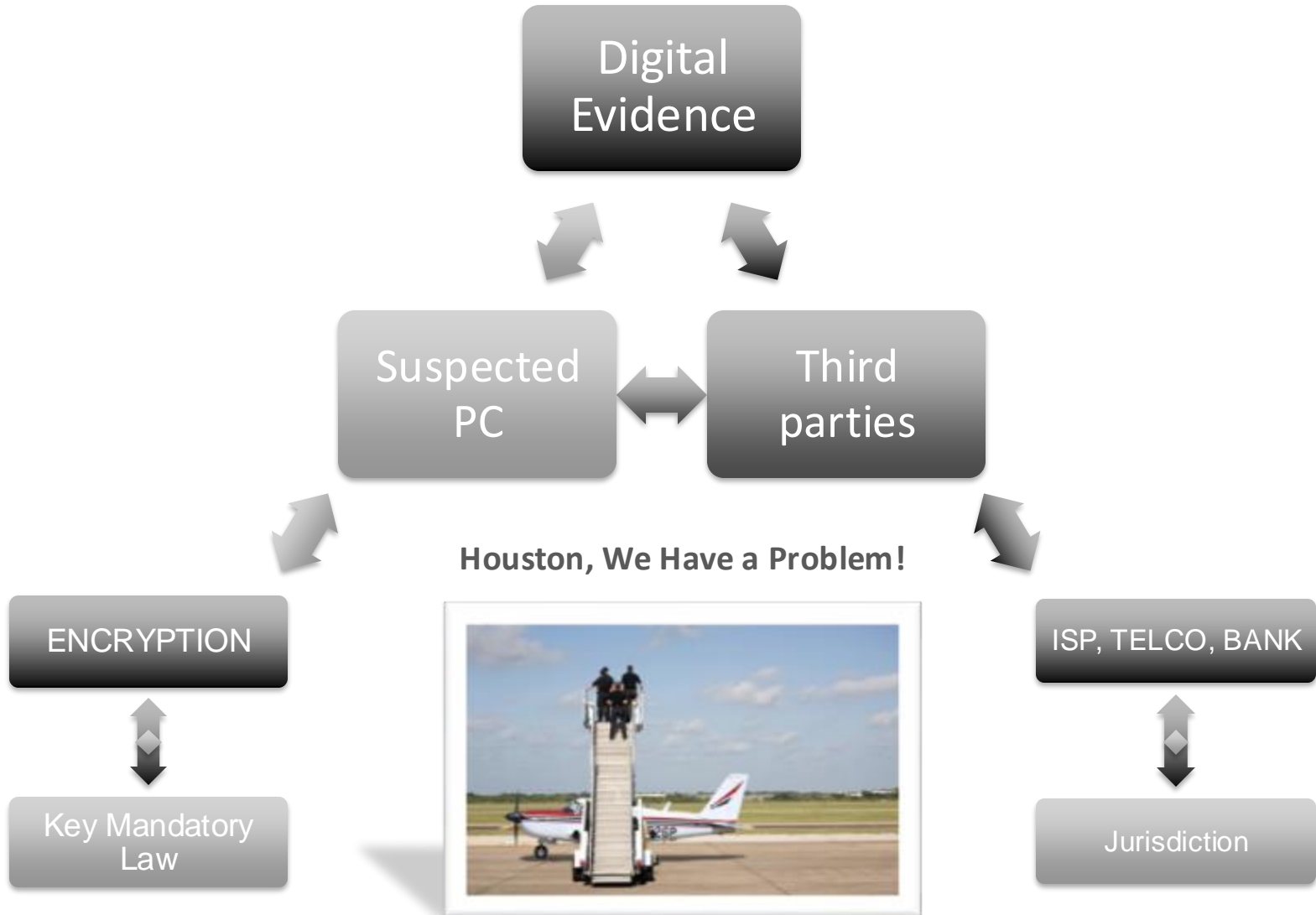
The Hash is a **unique function** that operates in only one direction (meaning that it cannot be reversed), by means of which a document of random length is converted into a limited and fixed length string.

This string represents a sort of '**digital fingerprint**' of the non-encrypted text, and is called the Hash Value or the Message Digest.

If the document is modified, even to the slightest extent, then the fingerprint changes as well. In other words, by calculating and recording the fingerprint, and then recalculating it, it can be shown beyond all doubt whether the contents of the file, or the medium, have been altered, even accidentally.

# Where and how is the digital/electronic evidence hosted?

---



# Why Third Parties are important during Digital Investigations?

---

Example: a forensics analysis reveals that a cybercrime victim had received a deceptive email that installed a spying software on her/his machine. What to do?



## Internet Access Provider

- Could reveal from which place the email was sent



## Mail Account Provider

- Could reveal from which places the email account was accessed



## Credit Card Company

- Could reveal where the goods bought with a cloned credit card were delivered

## Detecting and Seizing Digital Evidence: Cloud Computing

---

The new challenge with Cloud computing is a loss of data location due to:

- “Data at rest” does not reside on the device.
- “Data in transit” cannot be easily analysed because of encryption.
- “Data in execution” will be present only in the cloud instance

The investigator who wants to capture the bit-stream data of a given suspect image will be in the same situation as someone who has to complete a puzzle, whose pieces are scattered randomly across the globe



# Validating Digital Evidence on line

---

How is it possible to validate online digital evidence and immediately show that a particular piece of data on a particular online site is certain?



**Vuoi acquisire **prove online** per un caso di diffamazione ?**

La soluzione in cloud che permette di cristallizzare contenuti online da produrre come prove nei giudizi, in **pochi minuti** e con **estrema semplicità**.

ACQUISISCI ORA  
(1 CREDITO OMAGGIO)

SCARICA L'EBOOK SULLA PROVA DIGITALE



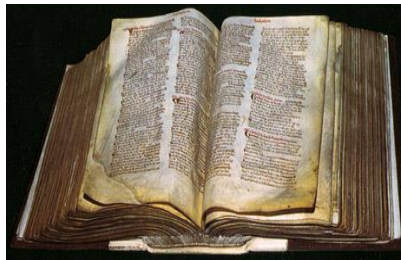
Valore probatorio garantito mediante una tecnologia idonea ad assicurare autenticità, integrità e non ripudio (**legge 18 marzo 2008, n. 48**)

## Chain of Custody of the digital evidence

---

Whilst the bit is eternal, its storage medium is not. Digital storage media last less than analogue media and devices to read such media last even less.

**Domesday Book (1086): Ink on parchment: legible after over 900 years.**



**Domesday Book 2 (1983): LaserDisc: illegible after 15 years.**



## Analysis of Digital Evidence

---

1. **Text searches:** aimed at scanning files, directories and even entire file systems for specific text terms
2. **Image searches:** aimed at identifying image files in various formats, and at generating still frames of digitally stored video footage
3. **Data recovery:** aimed at recovering all files stored on mass memory units, including deleted or damaged data
4. **Data discovery:** targeted at accessing hidden, encrypted or otherwise protected data
5. **Data carving:** focused on reconstructing damaged files by retrieving portions of their content
6. **Metadata recovery and identification:** this digital forensic tool is particularly useful for retracing the timeline of web accesses and file changes



# Analysis of Digital Evidence: two Italian issues

---

1. Digital forensics analysis is repeatable or unrepeatable, that is the question....



2. Open Source or Closet source

## Open Source Digital Forensics



**Autopsy®** is an easy to use, GUI-based program that allows you to efficiently analyze hard drives and smart phones. It has a plug-in architecture that allows you to find add-on modules or develop custom modules in Java or Python.



The **Sleuth Kit®** is a collection of command line tools and a C library that allows you to analyze disk images and recover files from them. It is used behind the scenes in Autopsy and many other open source and commercial forensics tools.

These tools are used by thousands of users around the world and have **community-based** e-mail lists and forums. Commercial training, support, and custom development is available from Sleuth Kit Labs.

 Follow @sleuthkit

**MAGNET  
FORENSICS®**

## **Presentation in Court of the Digital Evidence Findings**

---

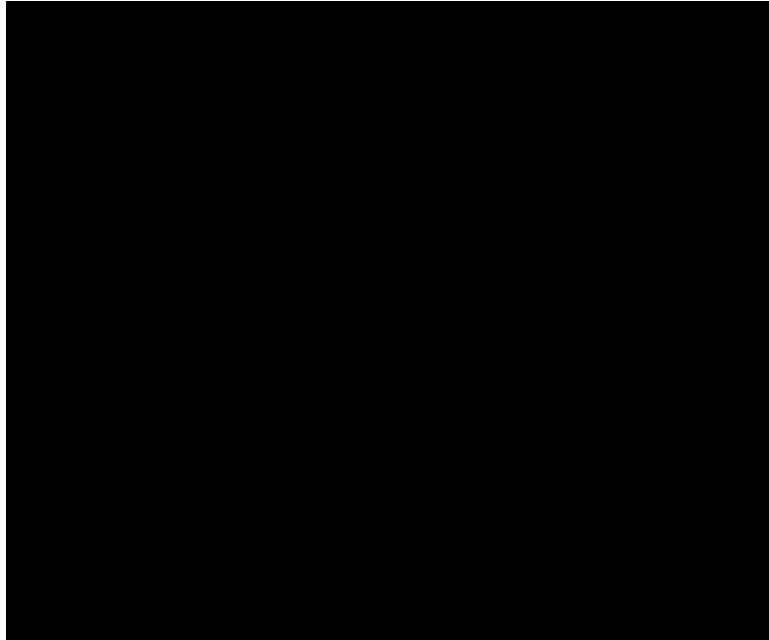
This stage is of key importance for Prosecutors, Judges and lawyers, as the outcome of the trial will depend not only on results achieved, but also the degree of clarity and comprehension of the report.

### **Operational recommendations**

- ❑ Presence of an index
- ❑ Presence of a glossary and reference notes if there are any technical terms
- ❑ Timeline table and flow charts
- ❑ Presentation slides with photos
- ❑ Possible video-recording of operations carried out

## Presentation in Court of the Digital Evidence Findings: Murtha Case

---



# A possible answer is Encryption

- ☐ Encryption is the process of obscuring information to make it unreadable without special knowledge
- ☐ Encryption can be used to ensure secrecy
- ☐ Encryption can be used to hide the fact that encrypted messages are exchanged
- ☐ Encryption used by criminals can lead to difficulties collecting the necessary evidence




## Legal Solution to Fight Encryption


*United States v. Boucher*  
(2007 WL 4246473)

## Privacy and Due Process Rights- United States v. Boucher 2-19-2009


**December 17, 2006** - Sebastien Boucher's laptop computer was inspected when he crossed the border from Canada into the USA at Derby Line, Vermont. Law Enforcement **seized the laptop**, questioned Boucher and then arrested him on a complaint charging him with transportation of child pornography in violation of 18 U.S.C. 2252A



**December 29, 2006** - When the laptop was switched on and booted, it was not possible to access its entire storage capability. This was because the laptop had been protected by PGP Disk encryption.



**January 12, 2007** - A grand jury subpoenaed the defendant to provide the password to the encryption key protecting the data



**November, 29 2007**- U.S. Magistrate Judge Jerome Niedermeier of the United States District Court for the District of Vermont stated "Compelling Boucher to enter the password forces him to produce evidence that could be used to incriminate him. **This is a evidence obtained in violation of fifth amendment**". Niedermeier quashed the subpoena

## Privacy and Due Process Rights - Mandatory Key Disclosure Laws

---

“Mandatory Key Disclosure” is the legislation that requires individuals to surrender cryptographic keys to law enforcement. Nations vary widely in the specifics of how they implement key disclosure laws.

Some, such as **Australia**, give law enforcement a wide-ranging power to compel assistance in decrypting data from any party.

Some, such as **Belgium**, concerned with self-incrimination, only allow law enforcement to compel assistance from non-suspects.

**France** requires only specific third parties, such as telecommunications carriers, certification providers, or maintainers of encryption services to provide assistance with decryption.

**Italy** doesn't have a Key Disclosure Law.



## Privacy and Due Process Rights - Mandatory Key Disclosure Laws

---

This legislative instrument doesn't work. Why?

1. **Technical reason:** an expert could always find a way to hide a file.
2. **Possible violation of European Convention on Human Rights:** Article 6  
*Everyone charged with a criminal offence shall be presumed innocent until proved guilty according to law.*





## Privacy and Due Process Rights - Mandatory Key Disclosure Laws

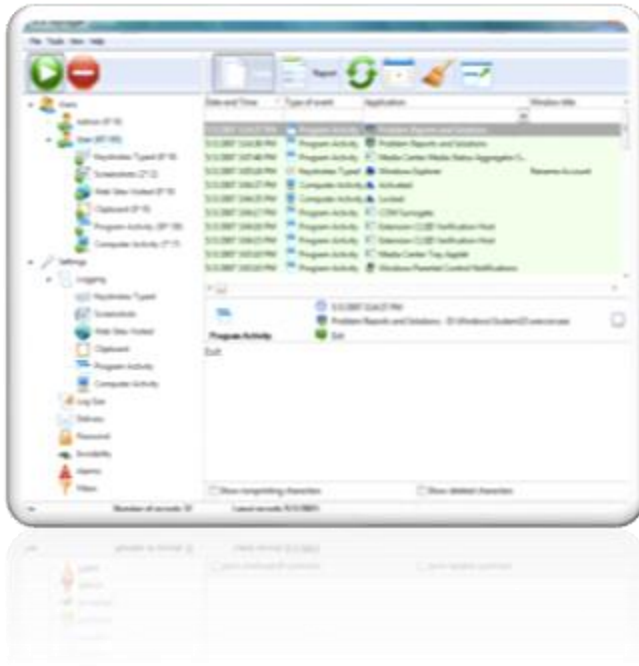
---

What is a “new” possible solution?

# Privacy and Due Process Rights – Remote Forensics

---

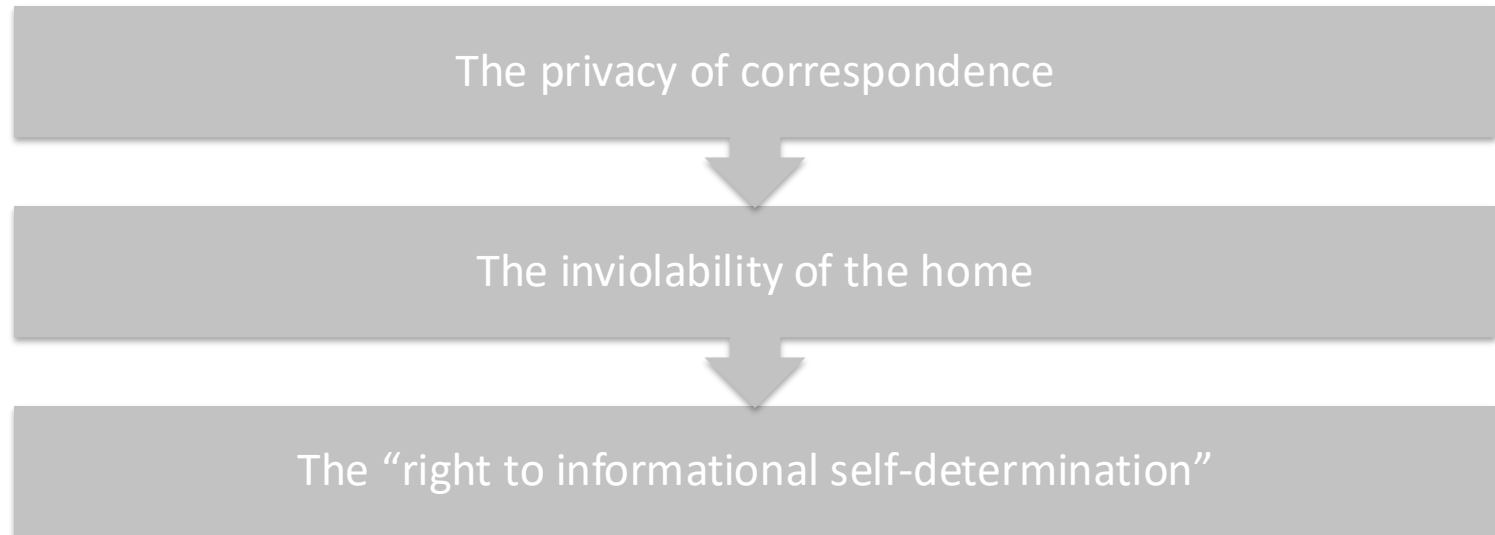
## Remote Forensics



## Privacy and Due Process Rights – Remote Forensics

---

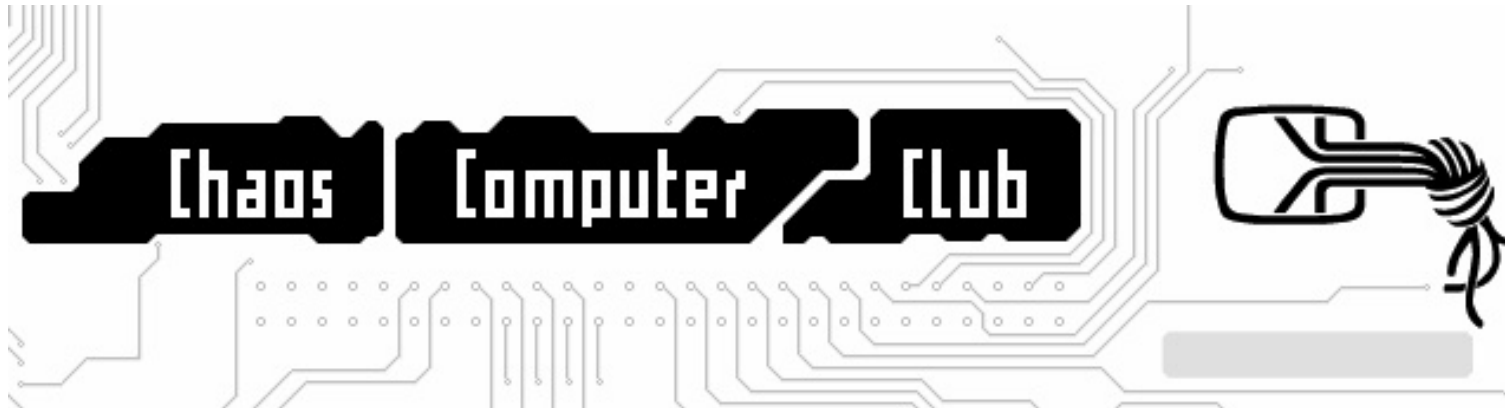
**On February 27, 2008** The German Constitutional Court determined that the amendment of NordWestfalia Law was unconstitutional as it violated:



The Constitutional Court establishes a new **“Right to the Confidentiality and Integrity of Information Technology Systems”** (right to the free development of one’s personality), read in conjunction with Article 1.1 GG (right to human dignity).

## Privacy and Due Process Rights – After 3 Years :(

---



Just three years after the ruling by the German Constitutional Court, Germany's Minister of Justice has called for an investigation after authorities in at least four German states acknowledged by using computer spywares to conduct surveillance on citizens (Bavaria, Baden-Wurttemberg, Brandenburg and Lower Saxony).

## Privacy and Due Process Rights – Cloud Computing

---

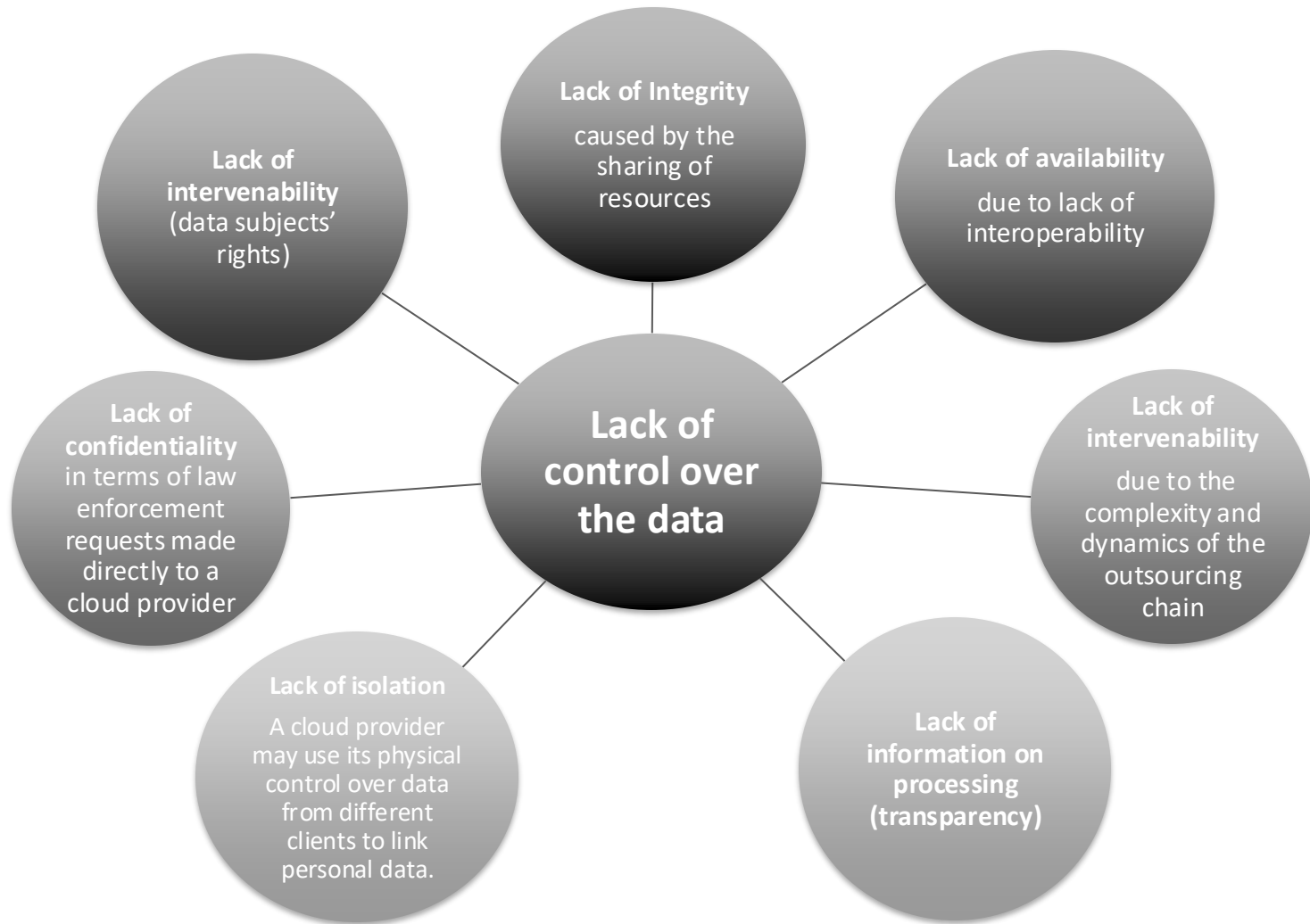
From a legal standpoint Cloud Computing services have to face these two distinct issues:

**Jurisdiction:** The “loss of location” of digital evidence in the cloud world creates problem of jurisdiction. With cloud computing, are the documents governed by the law of the state in which they are physically located or by the location of the company possessing them or by the laws of the state where a person resides? Over the last few years, various approaches have been offered to solve this problem.

**Privacy:** The “lack of control” over the data (cloud clients may no longer be in exclusive control of their data and cannot deploy the technical and organisational measures necessary to respect Data Protection Laws), and the “absence of transparency” (insufficient information regarding the processing operation itself) are the main data protection risks of cloud computing.

# Privacy and Due Process Rights – Cloud Computing and Privacy

---



## Privacy and Due Process Rights – Cloud Computing and Jurisdiction

---

We have 4 possible principles to solve the “loss of location” in a cloudy world:

- **Territorial principle:** the Court in the place where the data is located has jurisdiction.
- **Nationality principle:** the nationality of the perpetrator is the factor used to establish criminal jurisdiction.
- **“Flag principle”:** which basically states that crimes committed on ships, aircrafts and spacecrafts are subject to the jurisdiction of the flag state.
- **“Power of Disposal Approach”:** from a practical point of view, a regulation based on the power of disposal approach would make it feasible for law enforcement to access a suspect’s data within the cloud.

Thanks for your attention

---

Giuseppe Vaciago

*Linkedin:* <http://it.linkedin.com/in/vaciago>