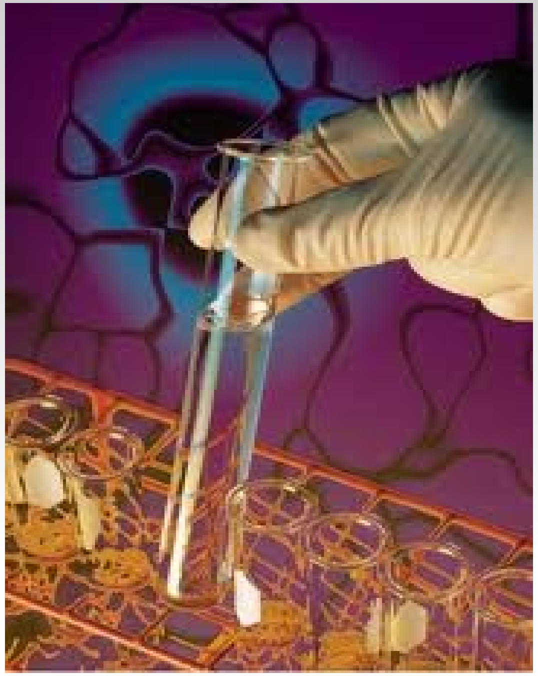
Digital Forensics & Incident Response

Davide Balzarotti
davide.balzarotti@eurecom.fr



Part A - Computer Forensics

Computer Forensics

fo·ren·sic

Adjective: Of, relating to, or denoting the application of *scientific methods and techniques* to the *investigation* of crime

Computer Forensics

fo·ren·sic

Adjective: Of, relating to, or denoting the application of *scientific methods and techniques* to the *investigation* of crime

Digital forensics involves the *preservation*, *collection*, *validation*, *identification*, *analysis*, *interpretation*, *documentation*, and *presentation* of digital evidences derived from computer media in a way that can be used in a court of law

- Artifact: an observable trace left behind as a consequence of a certain activity or event
- Evidence: something that can be used in a legal proceeding

A bit of History (1/3)

1978 The Florida Computer Crimes Act includes legislation against the *unauthorized modification or deletion of data* on a computer system

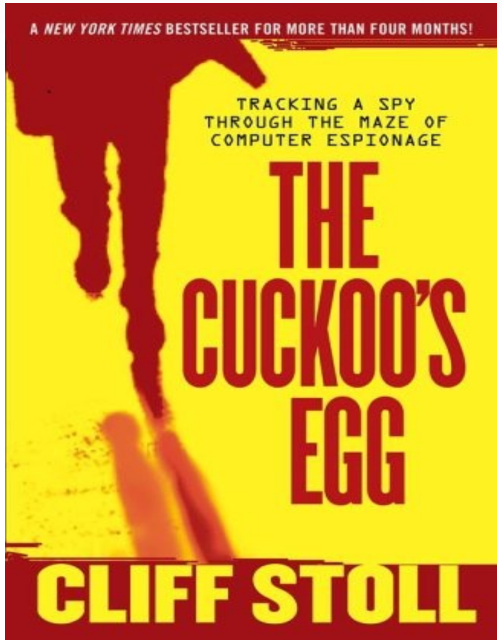
1982 Norton Utilities 1.0 for MS-DOS include the `undelete` program

1983 Canada is the first country to pass a federal law incorporating computer offense (the US *Federal Computer Fraud and Abuse Act* will follow in 1986, making hacking a crime)

1984 Fred Cohen coined the term Virus in the paper "*Computer Viruses – Theory and Experiments*“

1984 The FBI establishes the Computer Analysis and Response Team (CART), the first investigative group specialized in retrieving computer evidence (in the first year, they analyzed three cases)

1986 Cliff Stoll's pursuit of hacker Markus Hess (cool story, check the “*The Cuckoos's Egg*” book)


A NEW YORK TIMES BESTSELLER FOR MORE THAN FOUR MONTHS!
TRACKING A SPY THROUGH THE MAZE OF COMPUTER ESPIONAGE
THE CUCKOO'S EGG
CLIFF STOLL

A bit of History (2/3)

1988 The Morris Worm spread through the Internet.
This prompted DARPA to create the first *Computer Emergency Response Team* (CERT) at Carnegie Mellon.
Morris was the first person to be tried and convicted under the *Computer Fraud and Abuse Act*

1991 The International Law Enforcement meeting discusses the need for a standardized approach in computer forensic

1993 FBI hosted the *“International Law Enforcement Conference on Computer Evidence”*

1997 The G8 countries in Moscow declared that “*Law enforcement personnel must be trained and equipped to address high-tech crimes*”.

1998 The G8 appointed IICE to create international principles, guidelines and procedures relating to digital evidence

2000 First FBI *Regional Computer Forensic Laboratory* is established

A bit of History (3/3)

2001 First Digital Forensic Research Workshop (DFRWS)
"*A Road Map for Digital Forensic Research*"
[http://www.dfrws.org]

2003 The FBI CART examine over 780 TB of data in one year

2004 The Convention on Cybercrime is signed by 43 nations

2005 DFRWS Memory Analysis Forensics Challenge kickstarts the research in memory forensics

2007 The FBI CART examine over 2.5 PetaBytes of data in one year

2012 The FBI CART performed over 13K examinations accounting for over 10.5 PetaBytes of data in one year

The Law Side

- Very interesting and delicate subject but – I'm not a Lawyer –
- The course will focus only on the technical side of the problem
- If you want to know more about the legal side...

> *“Digital Forensics for Legal Professionals: Understanding Digital Evidence From The Warrant To The Courtroom”*
>
> \- Larry Daniel, Lars Daniel

The CSI Effect

The CSI Effect

- The CSI tv series depicted an exaggerated portrayal of forensic science
  - Wrong user perception
  - Unreasonable expectations of forensic results
    (forensic is always successful and has no false positives)
- Jurors are increasingly reluctant to convict without hi-tech forensic evidence

  … Yes, even when eyewitness are available :(

Locard's Principle

- Formulated by Edmond Locard, director of the first crime laboratory in existence (located in Lyon, France)

“*With contact between two items, there will be an exchange*”

Edmond Locard at work.

Locard's Principle

- Formulated by Edmond Locard, director of the first crime laboratory in existence (located in Lyon, France)

> “*With contact between two items, there will be an exchange*”

- Any interaction with a system causes some changes
  - User interaction
  - Investigator interaction
    (e.g., through data collection tools)
  - Other system interaction
    (e.g., network connections, peripherals,...)
  - … or the simple passage of time

Edmond Locard at work.

Lifecycle of a Forensic Examination

- Seizure
- Data acquisition
- Data analysis
- Reporting

Lifecycle of a Forensic Examination

- **Seizure**
  - (Optional) first step in a digital examination
  - It involve taking photographs, marking, tagging, and storing all the components
  - May require data acquisition of volatile information
  - Often performed by non-experts
  - Illegal seizure or improper methodology can affect the admissibility of the evidence in court
- Data acquisition
- Data analysis
- Reporting

Lifecycle of a Forensic Examination

- Seizure
- **Data acquisition**
  - Acquire a forensic copy of the data without altering or damaging the source
  - Validate that the data is identical to the original
  - Proper conservation and transportation
  - Access control
  - Chain of custody
- Data analysis
- Reporting

Lifecycle of a Forensic Examination

- Seizure
- Data acquisition
- **Data analysis**
  - Extract meaningful information from the acquired data
  - Interpret the information to extract evidence
  - Involve analysis, aggregation, and correlation of different data sources
- Reporting

Lifecycle of a Forensic Examination

- Seizure
- Data acquisition
- Data analysis
- **Reporting**
  - Presentation of the results in a final document
  - Carefully document each step of the examination
  - Based on the notes produced during the entire forensic process

Lifecycle of a Forensic Examination

- Seizure
- Data acquisition
- Data analysis
- Reporting

Focus of this course

Lifecycle of a Forensic Examination

- Seizure
- Data acquisition
- Data analysis
- Reporting

Step I - Seizure

- If the computer is off, leave it like that!

Step I - Seizure

- If the computer is off, leave it like that!
- If it is running, there are three options:
  - Properly shut it down
  - Pull the plug
  - Perform live forensic to acquire volatile information
- Remember: any action will alter the system...
  but also the lack of action will have effects !!!

Deadman Switches

- Originally a mechanism to automatically stop a machine in case the operator is incapacitated
- In computer forensic, normally refers to an automated process designed to wipe evidence
  - Can be triggered by certain events
    - If the computer is shut down
    - If the malware looses network connection
  - Or by the lack of certain events
    - The user does not type a certain code after boot

- Fortunately, many computer forensic cases involve relatively inexperienced people

To Pull or not to Pull

- Reasons to pull the plug:
  - It is much easier than performing live forensic
    (even untrained people can do it)
  - Running software on the live system will modify its data and possibly destroy evidences
  - A skillful attacker could detect and react to your presence
    (e.g., through a deadman switch)
  - You have to immediately stop what the system is doing
    (deleting, modifying, or exfiltrating data)

To Pull or not to Pull

- Reasons to pull the plug:
  - It is much easier than performing live forensic (even untrained people can do it)
  - Running software on the live system will modify its data and possibly destroy evidences
  - A skillful attacker could detect and react to your presence (e.g., through a deadman switch)
  - You have to immediately stop what the system is doing (deleting, modifying, or exfiltrating data)
- Often a bad choice in a incident response case

A Real Example

- To investigate an homicide on the street with no witnesses, investigators search the victim house and found a computer turned on
- The investigator collect volatile evidence and identify a suspect based on an instant messaging conversation
  - The suspect is later arrested and found guilty
- The same analysis could have been much harder if only the disk image would have been analyzed

To Pull or not to Pull

- Cutting the power vs Pressing the button
  - A clean shut down will prevent file system errors (which are anyway not a big issue today)
  - ...but will trigger many processes and changes in the system

- Cutting the power may allow the investigator to take a snapshot of the computer memory

→ Cutting the power is almost always better than a shutdown

To Pull or not to Pull

- Good reasons to not pull the plug
  - You will loose volatile data
  - You may loose access to the disk (encrypted disks)
  - You need to observe and collect some ongoing or future behavior (e.g., network traffic)
  - Collateral damage – shutting down a server for many hours (think about copying terabytes of disk) may be very costly
  - Sometimes you are not even sure the system was really compromised

→ Perform online data acquisition

Online Acquisition

- Be careful – data can be altered
  - By the investigator
  - By the tool
  - By the attacker
- It could compromise offline analysis
  - E.g., by modifying file timestamps
- The accuracy of the acquisition tools could be challenged

(more on this topic during the memory forensics class....)

Not Just the Computers

- Forensic Evidence can be anywhere
  - Printers
  - Mobile phones
  - Home routers
  - Memory sticks
  - IP phones
  - MP3 Players
  - GPS devices
  - Smart watches
  - Smart Home appliances
  - … and the **Internet of Things** is coming (!)

Lifecycle of a Forensic Examination

- [Seizure]
- Data acquisition
- Data analysis
- Reporting

Step II - Acquisition

- Acquire a bit-level copy of the data without altering or damaging the original
  - RFC 3227: Guidelines for Evidence Collection and Archiving

- Proceed from the volatile to the less volatile data
- The methods used to collect evidence should be transparent and reproducible
- Run statically-linked acquisition programs stored on appropriately protected media - do not trust programs or libraries installed in the target system

Order of Volatility

Certain information last longer than others

- Registers, peripheral memory, ...
- RAM Memory
- Swap Files
- Network State (ARP, routing, connections)
- Running Processes
- System settings
- Disk

Order of Volatility

Certain information last longer than others

Registers, peripheral memory, ...

RAM Memory

Swap Files

Network State (ARP, routing, connections)

Running Processes

System settings

Disk

Remember to collect the difference between the system clock and the real time

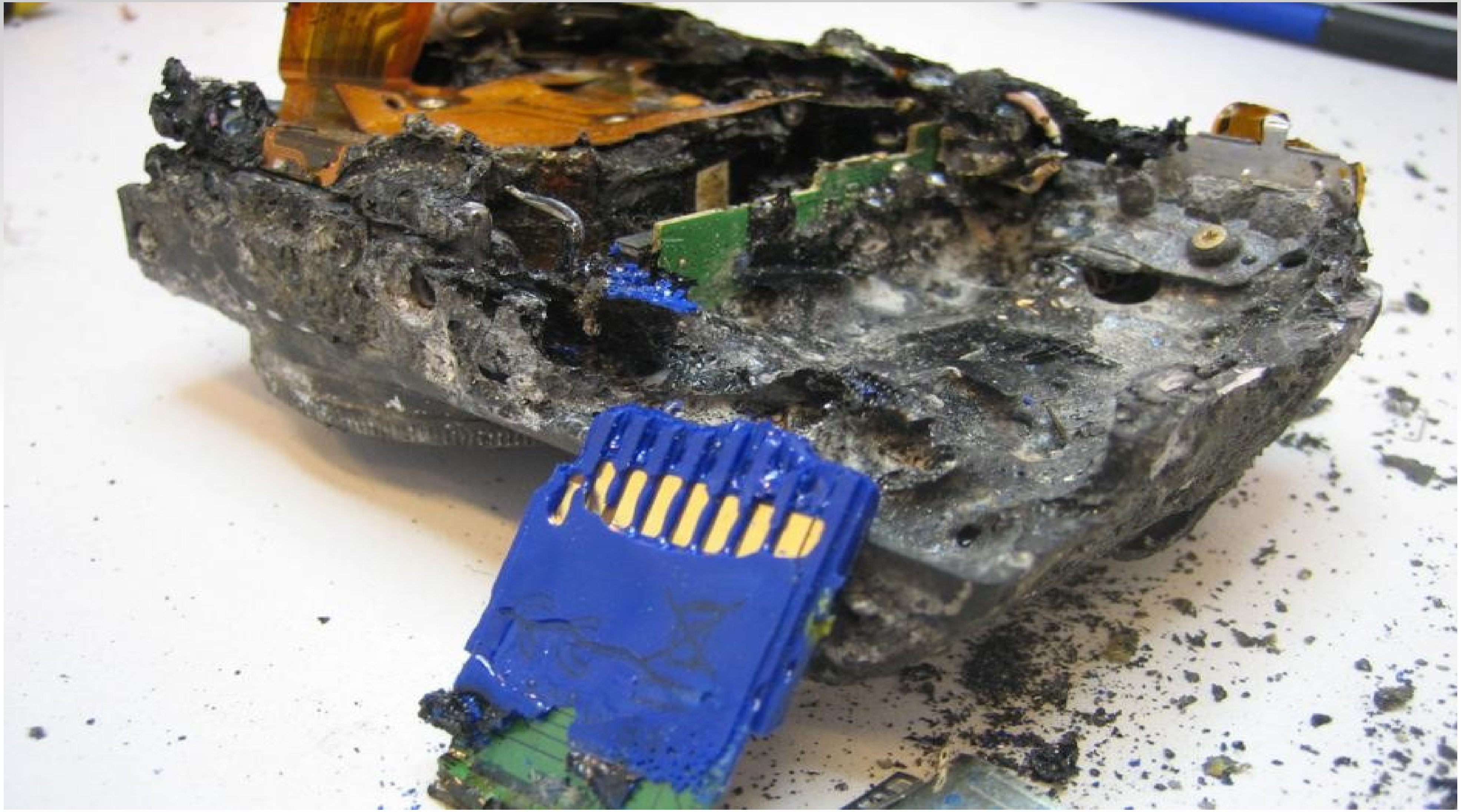
Logical & Physical Acquisition

- Logical acquisition
  - Bit-by-bit copy of a logical object
    E.g., copying the file system files (using `cp`, `tar`, …) preserving the timestamps
  - You can only get what the system wants to show
    (e.g., no deleted files and no unallocated space)
- Physical acquisition
  - Bit-by-bit copy of a physical storage device
  - Internal firmware can affect acquisition
    (E.g., hard disks FTL and bad blocks)

Evidence Integrity & Authentication

- Process to verify that the collected data is the same as it was in the original system
- Often based on checksums comparison
  - Two data are considered identical if their hashes match
  - Not always possible to hash the original data
  - Original data may “mutate” over time

Not Always in a Pristine State



Handling the Evidence

- Document in a log book each and every step of the evidence during the entire duration of the case

Who collected it?

- How and where?

Who took possession of it?

- How and where?

How the evidence was stored and protected?

Who took it out of storage?

- When and Why?

Lifecycle of a Forensic Examination

- [Seizure]
- Data acquisition
- Data analysis
- Reporting

Analysis

- May or may not involve data interpretation
- Two main approaches:
  - Looking for something we do not know in something we know
  - Looking for something we know in something we do not know

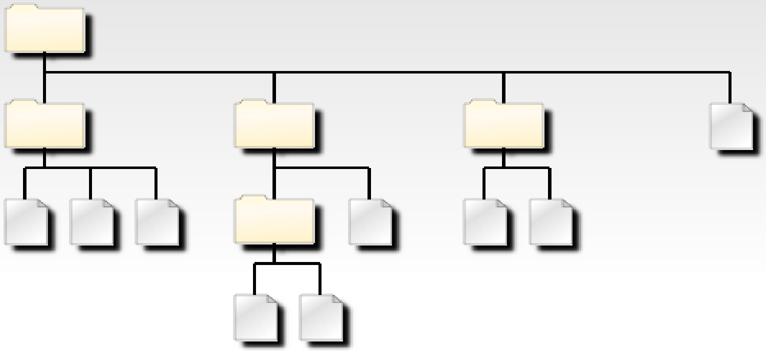
Analysis

Looking for something we do not know in something we know

acquisition

```
75 15 39 f1 76 41 f7 f1
5e 5f 5d c3 8d 74 26 00
1f 89 45 ec 75 51 3b 4d
89 f2 8b 75 f0 29 ce 19
c4 20 5e 5f 5d c3 66 90
00 31 d2 f7 f1 89 c1 89
eb a5 8d b6 00 00 00 00
c3 8d b4 26 00 00 00 00
ec c7 45 f0 20 00 00 00
```

interpretation
identification

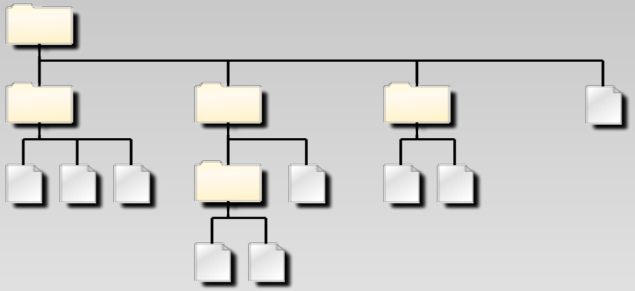


analysis

...
Infected applications
Deleted documents
Browser history
…

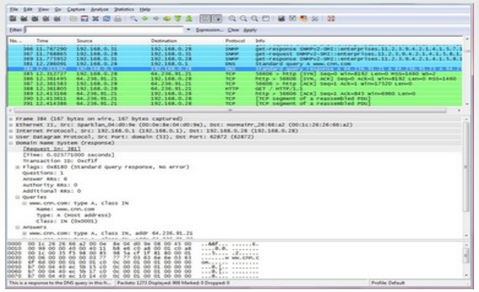
Source *Raw Data* *Interpreted Data* *Findings*

```
75 15 39 f1 76 41 f7 f1
5e 5f 5d c3 8d 74 26 00
1f 89 45 ec 75 51 3b 4d
89 f2 8b 75 f0 29 ce 19
c4 20 5e 5f 5d c3 66 90
00 31 d2 f7 f1 89 c1 89
eb a5 8d b6 00 00 00 00
c3 8d b4 26 00 00 00 00
ec c7 45 f0 20 00 00 00
```

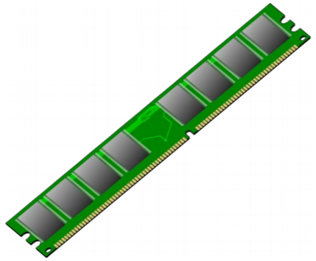


...
Infected apps
Deleted documents
Browser history
…

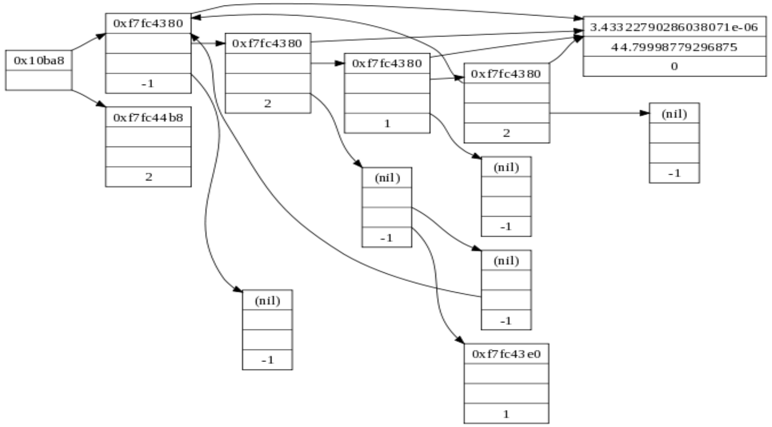
```
75 15 39 f1 76 41 f7 f1
5e 5f 5d c3 8d 74 26 00
1f 89 45 ec 75 51 3b 4d
89 f2 8b 75 f0 29 ce 19
c4 20 5e 5f 5d c3 66 90
00 31 d2 f7 f1 89 c1 89
eb a5 8d b6 00 00 00 00
c3 8d b4 26 00 00 00 00
ec c7 45 f0 20 00 00 00
```



...
Downloaded pics
Infected webpages
Voip calls
…



```
75 15 39 f1 76 41 f7 f1
5e 5f 5d c3 8d 74 26 00
1f 89 45 ec 75 51 3b 4d
89 f2 8b 75 f0 29 ce 19
c4 20 5e 5f 5d c3 66 90
00 31 d2 f7 f1 89 c1 89
eb a5 8d b6 00 00 00 00
c3 8d b4 26 00 00 00 00
ec c7 45 f0 20 00 00 00
```



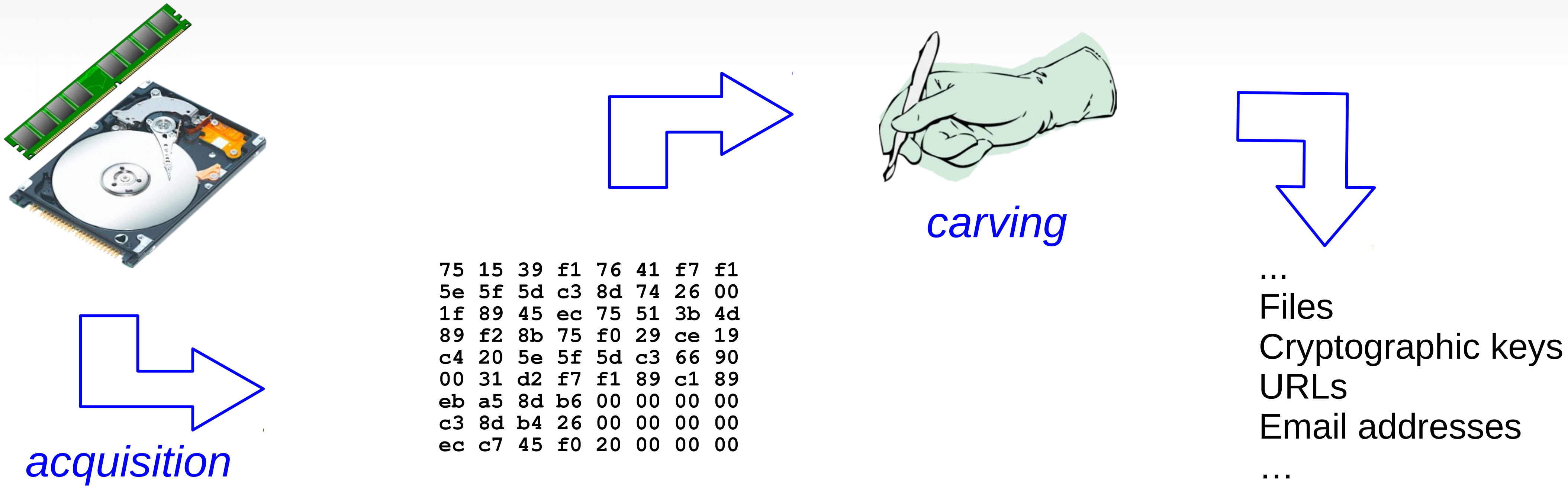
...
Open connections
Running processes
…

“When all else fails, we carve”

- Looking for something we know in something we do not know
- Extraction of meaningful information from unstructured data
  - Regular expressions to extract simple strings-like information
  - Signatures to extract files

“When all else fails, we carve”

- Looking for something we know in something we do not know
- Extraction of meaningful information from unstructured data
  - Regular expressions to extract simple strings-like information
  - Signatures to extract files



acquisition

```
75 15 39 f1 76 41 f7 f1
5e 5f 5d c3 8d 74 26 00
1f 89 45 ec 75 51 3b 4d
89 f2 8b 75 f0 29 ce 19
c4 20 5e 5f 5d c3 66 90
00 31 d2 f7 f1 89 c1 89
eb a5 8d b6 00 00 00 00
c3 8d b4 26 00 00 00 00
ec c7 45 f0 20 00 00 00
```

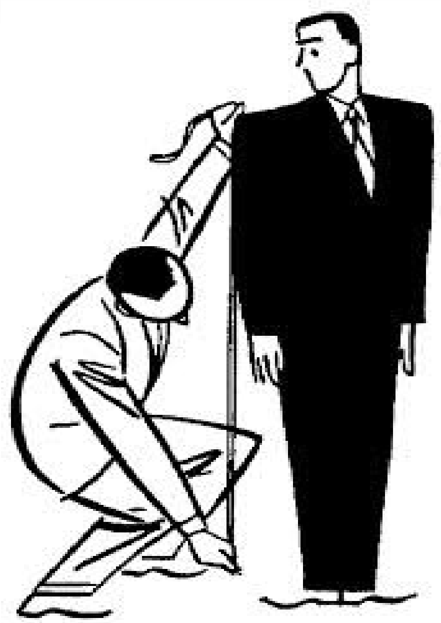
carving

...
Files
Cryptographic keys
URLs
Email addresses
…

Know Your Enemy

- It is important to estimate the technical ability of the suspect
  - Is further technical analysis necessary?
  - Is the suspect able/likely to hide data?
  - Should we expect anything *very* sophisticated?

- Background information on the suspect profile can provide valuable information



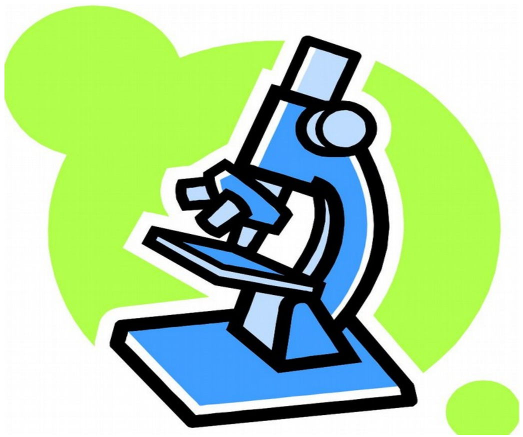
The Research Corner

- “A history of Digital Forensics”
  Mark Pollitt

- “Digital forensics research: The next 10 years”
  Simson L. Garfinkel – Tenth Annual DFRWS Conference 2010

- “A survey of digital forensic investigator decision processes and measurement of decisions based on enhanced preview”
  J.I. James, P.Gladyshev – Digital Investigation Journal 2013

- “Computer Forensics In Forensis”
  S.Peisert, M.Bishop, K.Marzullo – SADFE 2008



Part B - Incident Response

Computer Incidents

in·ci·dent

ISO27001: any event which is not part of the standard operation of a service and which causes or may cause an interruption to, or a reduction in, the quality of that service.

- Denial-of-Service attack
- Malware infection
- Hacker broke into a network
- Web page modified to serve malicious content
- Stolen credentials because of a phishing email
- Employee stole or intentionally deleted critical data
- ...

Incident Response

“All operations and activities performed to respond to the compromise (or attempted compromise) of the confidentiality, integrity, and availability of all the information that is processed, stored and transmitted using a computer”

- Within large organizations, these activities are performed by a Computer Security Incident Response Team (CSIRT)

Computer Forensics vs Incident Response

- Different goal, but large overlapping in terms of techniques
- In forensic, the focus is on linking a subject with a certain action
  - Often related to civil/criminal litigation
  - Need to establish knowledge and intent

Computer Forensics vs Incident Response

- Different goal, but large overlapping in terms of techniques
- In forensic, the focus is on linking a subject with a certain action
  - Often related to civil/criminal litigation
  - Need to establish knowledge and intent
- In Incident response, the focus is on the analysis of a system that has been compromised
  - Often involves containment, recovery, and mitigation
  - Can be successful even without user attribution

Computer Forensics vs Incident Response

- Different goal, but large overlapping in terms of techniques
- In forensic, the focus is on linking a subject with a certain action
  - Often related to civil/criminal litigation
- In
  ha
  - Often involves containment, recovery, and mitigation
  - Can be successful even without user attribution

> ≈ *“ Forensic deals with systems suspected to be used to commit a crime. Incident response deals with systems suspected to be the victim of a crime ”*

IR Activities

- Handle the incident:
  - Identify, stop, contain, and remove the incident
- Recover from the incident:
  - Repair the damage and restore the system to a clean state
- Investigate the incident:
  - Determine the cause of the incident and all affected systems/data
  - Collect and analyze forensic evidences
  - Binary analysis
- Assist in the prevention of a reoccurrence of the incident

IR Activities

- Handle the incident:
  - Identify, stop, contain, and remove the incident
- Recover from the incident:
  - Repair the damage and restore the system to a clean state
- Investigate the incident:
  - Determine the cause of the incident and all affected systems/data
  - Collect and analyze forensic evidences
  - Binary analysis
- Assist in the prevention of a reoccurrence of the incident

Something to Play with

- You can analyze your computer
  - It may seem boring, but it is a good exercise to see how many artifacts are stored in your system. → It makes you think about your privacy
  - And you may discover that your computer has already been compromised :)
- You *cannot* analyze somebody else computer
  - You need a proper consent
  - Privacy is really an issue here
  - Hard to have a “crime scenario” anyway (hopefully)

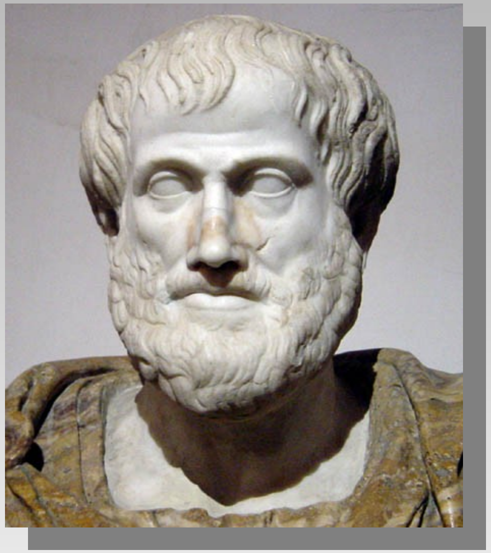
Something to Play with

- Public datasets for forensics
  - NIST Computer Forensics Reference Data Sets (CFReDS)

    http://www.cfreds.nist.gov
  - Digital corpora

    http://digitalcorpora.org/
  - Digital Forensics Tool Testing Images

    http://dftt.sourceforge.net/
  - Pcap files from malware analysis
- Hacker Forensic Challenges
  - Many hacking competition have forensic challenges available online
  - Definitely non-standard (malformed or corrupted files, complex exfiltration mechanisms, ...)



> “ *The search for truth is in one way hard and in another way easy, for it is evident that no one can master it fully or miss it wholly. But each adds a little to our knowledge of nature, and from all the facts assembled there arises a certain grandeur* ”
>
> – Aristotele