Introduction to digital forensics – what is CSI: Cyber in real life
Jussi Eronen
Chief Specialist
NCSC-FI
Forensics – The Field

Digital Forensics

- Computer Forensics
- Mobile Device Forensics
- Database Forensics
- Network Forensics
- Disk Forensics
- Live Forensics
- Memory Forensics
- Live OS Forensics

These topics will be covered in the course.
Forensics – The Field

Figure 1 Classification of Digital Forensics
Locard's Exchange Principle

- Every contact leaves a trace
  - Presence or absence of something
  - Either physical or electronically
“Wherever he steps, whatever he touches, whatever he leaves, even unconsciously, will serve as a **silent witness** against him. Not only his fingerprints or his footprints, but his hair, the fibers from his clothes, the glass he breaks, the tool mark he leaves, the paint he scratches, the blood or semen he deposits or collects. All of these and more, bear mute witness against him. This is evidence that does not forget. It is not confused by the excitement of the moment. It is not absent because human witnesses are. It is factual evidence. **Physical evidence cannot be wrong**, it cannot perjure itself, it cannot be wholly absent. **Only human failure to find it, study and understand it, can diminish its value.**”

Source: [7]
"The Daubert standard is a rule of evidence regarding the admissibility of expert witnesses' testimony during United States federal legal proceedings. Pursuant to this standard, a party may raise a Daubert motion, which is a special case of motion in limine raised before or during trial to exclude the presentation of unqualified evidence to the jury."

Goal: No junk science in a courtroom
Way: Adhere to scientific standards
Court defined "scientific methodology": Formulate hypotheses and conduct experiments to prove or falsify the hypotheses.

- Empirical testing: the theory or technique must be falsifiable, refutable, and testable.
- Subjected to peer review and publication.
- Known of potential error rate.
- The existence and maintenance of standards and controls concerning its operation.
- Degree to which the theory and technique is generally accepted by the relevant scientific community.
Four principles according to APCO for the police [11]:

1. No action taken by law enforcement agencies or their agents should change data held on a computer or storage media which may subsequently be relied upon in court.
2. In circumstances where a person finds it necessary to access original data held on a computer or on storage media, that person must be competent to do so and be able to give evidence explaining the relevance and the implications of their actions.
3. An audit trail or other record of all processes applied to computer-based electronic evidence should be created and preserved. An independent third party should be able to examine those processes and achieve the same result.
4. The person in charge of the investigation (the case officer) has overall responsibility for ensuring that the law and these principles are adhered to.
Five Ws (and one H)

• Method for getting the full story on something by asking the following questions:
  – **Who** is it about?
  – **What** happened?
  – **Where** did it take place?
  – **When** did it take place?
  – **Why** did it happen?
  – **How** did it happen?

• These questions have to be addressed in the report.
• Follow the law of the relevant jurisdiction
  – Every jurisdiction has different rules that have to be considered
  – Sovereign vs. Non-sovereign investigations
    • E.g. the police has the rights for house searches under certain restrictions), whereas you or your organization do not have that right.
    • Permission for search and seizure (house searches / private property)

• Follow forensic standards
  – International or local common “scientific” standards

• Organizational Policies
  – Internal regulations that apply also in forensic investigations

• Declaration of Confidentiality
• Letter of Intent
Legal Risks

• Data protection
  – Privacy rights

• Labour/Employment Law
  – Might not access folders marked as private even on company-owned computers
  – CCTV surveillance not permitted in some jurisdictions
  – Content inspection might be illegal (eg. E-Mail)

• Company Policies
  – Devices can be use for private stuff (privacy)

• Pornographic material
  – Civilians might not hold or distribute pornographic material

• Technical possibilities for forensic analysis go far beyond what is legally possible!
• If in doubt: Ask your lawyer(s) / your legal department

• Technically
  – Do not press a single key if in doubt (not even the power switch)
  – Ask your forensics specialist
  – Avoid altering evidence as much as possible
• Prevent infection of Analysis System
  – Suspect device might contain malware
  – Separate Analysis Lab Infrastructure (including LAN and Internet Connectivity)

• Data Security
  – Classification
  – Need-to-know principle applies
  – Store evidence in a safe when not in use
  – Only authorized personnel with the necessary clearance has access to evidence / lab
  – Same rules apply for backups
Procedures

- Establish Forensic Readiness
- Incident Response
- Containment
- Gather Evidence
- Analyze Evidence
- Reporting
- Archiving / Storage

Lessons Learned
Order of Volatility

- Taken from [13]: Guidelines for Evidence Collection and Archiving

<table>
<thead>
<tr>
<th>Volatile</th>
<th>Static</th>
</tr>
</thead>
<tbody>
<tr>
<td>Registers, Cache</td>
<td>Archival media</td>
</tr>
<tr>
<td>Routing table, arp cache, process table, kernel statistics, memory</td>
<td>Physical configuration, network topology</td>
</tr>
<tr>
<td>Temporary file systems</td>
<td>Remote logging and monitoring data that is relevant to the system in question</td>
</tr>
<tr>
<td>Disk</td>
<td></td>
</tr>
</tbody>
</table>

Registers, Cache: Volatile data that changes quickly and is relevant to the system in question.
Archival media: Static data that is not volatile and is relevant to the system in question.
The ON vs. OFF Debate

- Depends on the circumstances whether to leave a computer running or to turn it off

- Turning a computer off means losing all volatile evidence
  - RAM
  - Might be a problem with encrypted file systems where the password is not known

- Keeping a computer running means altering evidence
  - Memory content changes constantly
  - Disk is used and file fragments might be overwritten
Secure scene and move everyone away from computers and electronic devices.

Is the computer powered on?

Are law enforcement personnel with specific computer seizure training available?

Is the system a networked business environment?

Are destructive processes running?

Is information of evidential value visible on screen?

Remove power cord from back of computer and connected devices.

Label all connections on computers and devices as well as cables and power supplies.

Locate and secure all evidence within the scope of authority for the specific circumstances.

Document, log, and photograph all computers, devices, connections, cables, and power supplies.

Log and secure all evidence according to agency policies pending forensic examination.

Destructive processes can be any functions intended to obliterate data on the hard drive or data storage device. Terms like "format", "delete", "remove", and "wipe" can be indicative of the destruction process. Document these indicators in reports.

DO NOT turn the computer or device on.

STOP! DO NOT turn computer or device off. Contact personnel trained in network seizure.

Request assistance and follow recommendations of personnel with specific digital evidence seizure training.

Source: [9]
Chain of Evidence & Custody

• Definition from [12]:
  – **Chain of custody** (CoC) refers to the chronological documentation or **paper trail**, showing the seizure, custody, control, transfer, analysis, and disposition of **evidence**, physical or electronic. Because evidence can be used in court to convict persons of crimes, it must be handled in a scrupulously careful manner to avoid later allegations of tampering or misconduct which can compromise the case of the prosecution toward **acquittal** or to overturning a guilty verdict upon **appeal**. The idea behind recording the **chain of custody** is to establish that the alleged evidence is in fact related to the alleged crime, rather than having, for example, been **planted fraudulently** to make someone appear guilty.

• Goal: Prove that the evidence came from or was produced by the suspect and not inserted or altered by the forensics analyst.

• Document who had access (physical and electronic) to the evidence at every given moment.

• Prepare for the worst during an investigation!
  – Quick-and-dirty approach → Other party might sue the investigator afterwards or court rejects the evidence
**Chain of Evidence & Custody**

- **How**
  - Create a paper trail by documenting acquisition, ownership and handling of evidence
    → Forensics logbook
  - Document Cryptographic checksums
  - Time stamping
  - Evidence forms
  - Signatures
  - Seals

<table>
<thead>
<tr>
<th>Nr. (No.)</th>
<th>Datum (Date)</th>
<th>Zeit (Time)</th>
<th>Kürzel (Paraphil)</th>
<th>Aktion (Action)</th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>2</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>3</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>4</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>
Where to find Evidence

- **DMZ**
  - VPN Gateway
  - Proxy
  - Web / Mail
  - Switch

- **Internet**
  - www
  - nfsen
  - syslog

- **DMZ**
  - Files server / Groupware
  - Desktop PC's
  - Printer's
  - Wireless AP
  - Laptop PC's

- **Intranet**
  - Mobile Phone

- **Files server / Groupware**
Where to find Evidence

• Computer Forensics
  – Hard drive Imaging
    ❑ Create a 1:1 image of a memory device
    ❑ Post mortem analysis
  – Memory Forensics
    ❑ Memory (RAM) snapshot of a running system
    ❑ Live analysis
    ❑ (Cold boot attack)
  – Other Storage Media
    ❑ CD-Rom / DVD
    ❑ USB Sticks
    ❑ SD/Flash cards
Where to find Evidence

• Network Forensics
  – Preserve the state of a network device that cannot be reachable physically (e.g., web pages, DNS records, network flow data, etc.)
  – Document a situation that might change over time

• Mobile Device Forensics
  – Cellphones
  – Smartphones

• Database Forensics
Preparation

• What to expect on-site...

Spot the hidden USB-key...
Preparation

- **Hardware**
  - Interface adapters and cables, spare disks, write blockers, etc.

- **Software**
  - To create forensically sound disk images
  - To perform live analysis
  - To investigate the evidence

- **Procedures / Knowledge**
  - Tested and documented procedures
  - How to handle the hardware safely
  - How to start the computer without booting the operating system
  - How to create the disk images

- **Practice**
  - Exercise regularly!
• Depends heavily on the environment and the actual case

• Operating system internals
  – Windows / Mac / *nix / etc.
  – Where do the systems store logs, cache data, etc.
  – How does the file system work (eg. for deleted files and folders)
  – How do they behave in corporate environments (eg. evidence on central servers)
  – Any encryption that might prevent or hinder forensic investigations
  – Could there be a dead man’s switch?

• Applications
  – Eg. Mail applications, browsers, chat / IM software, office software, etc.
  – Storage locations and file format specifications (features of the document format)
  – Meta data contained in documents / old revisions of documents
  – Caches, logs
• Documentation how to perform forensic analysis
  – Standard procedures for specific tasks
  – Eases following the legal rules in your jurisdiction
  – Everyone follows the same procedures (standardization)

• But also manuals from the hardware vendor
  – Eg. Apple: Howto disassemble a MacBook
Toolbox: Hardware

• Paper and Pencils (yes, even nowadays...)
• Tools
  – Screwdrivers (Torx, Crosshead, Flathead, etc.)
  – Tweezers
  – Antistatic wrist strap
  – etc.

Image Source: http://www.nachi.org/images10/wrap.jpg

Toolbox: Interfaces, Cables and Connectors

- SCSI (internal & external)
- IDE / EIDE
- SATA / eSATA / mSATA / M.2
- USB / Firewire / Lightning
- etc.
Toolbox: Memory Cards

- Flash
- SD-Card
- MemoryStick
- USB Memory Stick
Toolbox: Other Storage Media

- CD-Rom / DVD
- ZIP / JAZ Drives
- Tape Drives (DAT)
- Magneto Optical Drives
- Floppy Disks
- etc.
Write Blockers

- Altering evidence must be avoided either
  - with software
    - Mounting read-only
  - with hardware
    - Some hard disks (e.g., SCSI drives) have jumpers
    - Forensic write blockers

- The suggested way to go is hardware write blockers
  - Depends on circumstances
Workstation / Lab

- For acquiring data in the field
- For analyzing acquired data in the lab

- Manufactured forensic workstations
- Low-cost solutions with off-the-shelf hardware
Wait, there's more
Incidents already seen

- Coffee machine calls home
- Home audio amplifier is a bot
- Milking machine used to commit fraud
- Cow heat detection participates in DDoS
- Ground-source heat pump scans for vulns
The Nedap Heat Detection system - how it works

1. The Nedap Smarttag records the behaviour and movements of the individual animals.

2. The data from all the individual animals is continuously recorded by the antenna.

3. The Process Controller - the heart of the system - analyses the individual data for each animal and sends the results to a PC, smartphone or tablet.

4. The results can be displayed on a PC, smartphone or tablet. The system automatically sends attention alerts about animals in heat or changes in behaviour that may indicate health problems.

5. The data received by the antenna and sent to the Process Controller.
DDoS Attack Takes Down Central Heating System Amidst Winter In Finland

Wednesday, November 09, 2016  Mohit Kumar

Just Imaging — What if, you enter into your home from a chilling weather outside, and the heating system fails to work because of a cyber attack, leaving you in the sense of panic?

The same happened late last month when an attack knocks heating system offline in Finland.
Don't worry, it's going to get worse
SMM Rootkits: 
A New Breed of OS Independent Malware

Shawn Embleton  
University of Central Florida  
embleton@cs.ucf.edu

Sherri Sparks  
University of Central Florida  
ssparks@cs.ucf.edu

Cliff Zou  
University of Central Florida  
czou@cs.ucf.edu


Processor firmware upgrases  
Ring -3 (AMT)
The Big Hack

How China used a tiny chip to infiltrate America’s top companies
Me explaining the SuperMicro news to the norm's:

ALL RIGHT, *takes drag of cigarette* SO THERE ARE COMPUTERS RUNNING WITHIN COMPUTERS ON MOST COMPUTERS THESE DAYS INCLUDING YOUR PHONE

https://twitter.com/pr1ntf/status/1047957577395400704?s=12
Super Micro Computer Inc. said it has found no malicious hardware in its products and that no government agency has contacted the company about such hardware, rejecting a report that China’s intelligence services planted malicious chips in the company’s server motherboards.

In a letter emailed to Senators Marco Rubio, a Florida Republican, and Richard Blumenthal, a Connecticut Democrat, Supermicro disputed Bloomberg reports on hacking of the company’s hardware. The letter, in response to a request for information from the senators, reiterates previous denials.
I have worked in card payment industry. We would be getting products from China with added boards to beam credit card information. This wasn't state-sponsored attack. Devices were modified while on production line (most likely by bribed employees) as once they were closed they would have anti-tampering mechanism activated so that later it would not be possible to open the device without setting the tamper flag.

Once this was noticed we started weighing the terminals because we could not open the devices (once opened they become useless).

They have learned of this so they started scraping non-essential plastic from inside the device to offset the weight of the added board.

We have ended up measuring angular momentum on a special fixture. There are very expensive laboratory tables to measure angular momentum. I have created a fixture where the device could be placed in two separate positions. The theory is that if the weight and all possible angular momentums match then the devices have to be identical. We could not measure all possible angular momentums but it was possible to measure one or two that would not be known to the attacker.

https://twitter.com/arbedout/status/1047822585009004545
(TSI/SI/REL) IRONCHEF provides access persistence to target systems by exploiting the motherboard BIOS and utilizing System Management Mode (SMM) to communicate with a hardware implant that provides two-way RF communication.

(TSI/SI/REL) IRONCHEF Extended Concept of Operations

(TSI/SI/REL) This technique supports the HP Proliant 380DL G5 server, onto which a hardware implant has been installed that communicates over the PC Interface (WAGONBED).
(TS//SI//REL) IRATEMONK provides software application persistence on desktop and laptop computers by implanting the hard drive firmware to gain execution through Master Boot Record (MBR) substitution.
The NSA's Undetectable Hard Drive Hack Was First Demonstrated a Year Ago

A paper published last year proved the NSA's newly discovered exploit can be done by any skilled hacker.
Gone in 60 Milliseconds
Intrusion and Exfiltration in Server-less Architectures

Rich Jones

https://media.ccc.de/v/33c3-7865-gone_in_60_milliseconds