Part 1
Digital Forensics Module

Jaap van Ginkel
Silvio Oertli

July 2016

Agenda

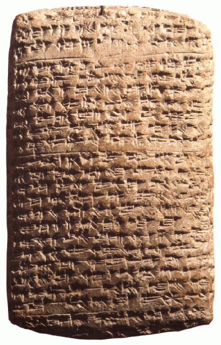
- Part 1: Introduction
  - Definitions / Processes
- Part 2: Theory in Practice
  - From planning to presentation
- Part 3: Live Forensics
  - How to acquire a memory image
  - Investigate the image
- Part 4: Advanced Topics
  - Tools
  - Where to go from here
  - And more

§ Disclaimer

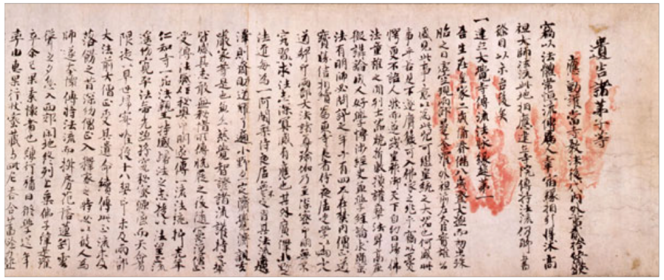
- A one or two-day course on forensics will not make you a forensics expert.
  - Professionals spend most of their working time performing forensic analysis and thus become an expert.
- All we can offer is to shed some light on a quickly developing and broad field and a chance to look at some tools.
- We will mostly cover Open Source Forensic Tools.

Introduction
Forensics in History

Forensics – History



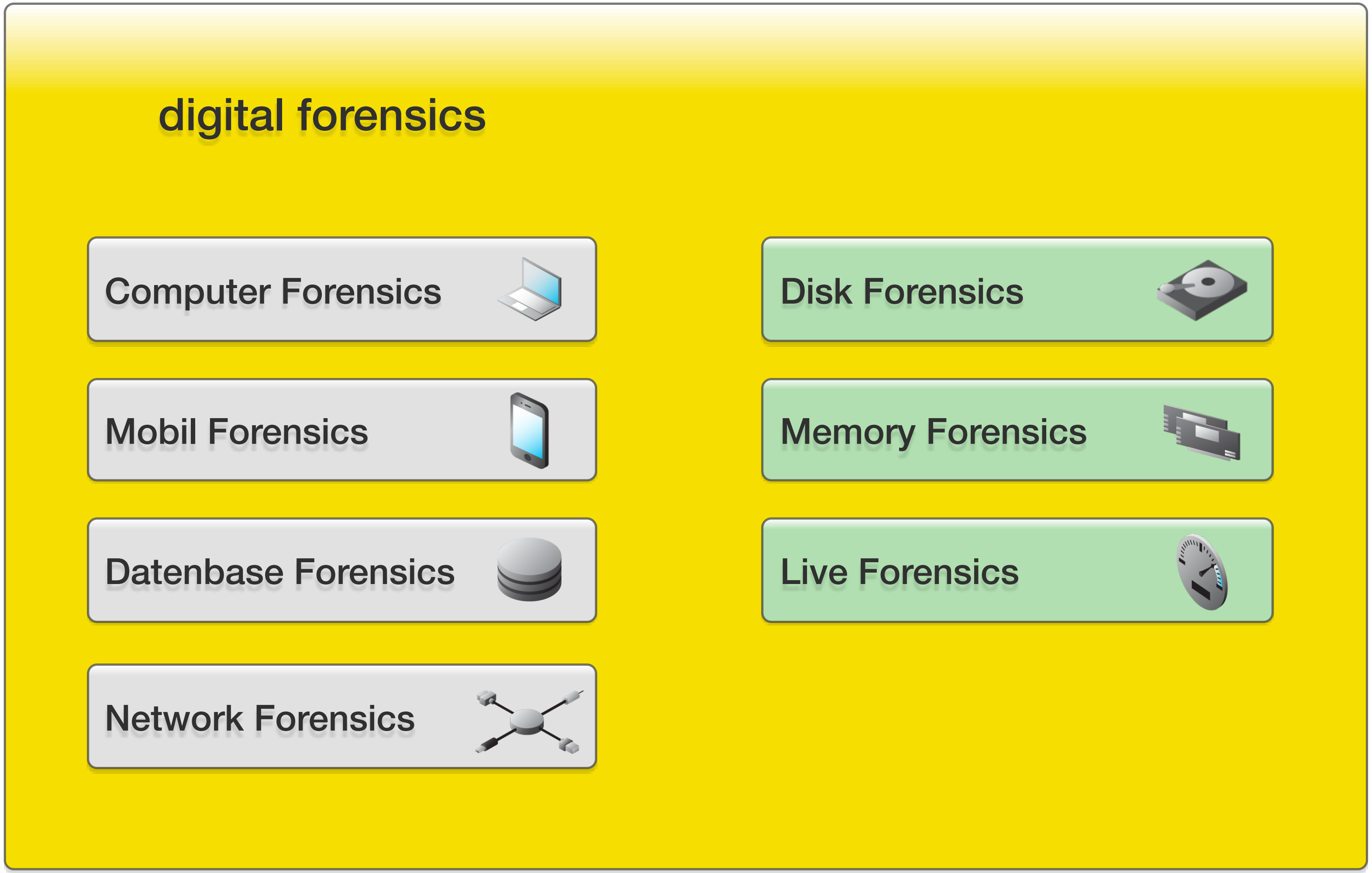
2000 BC



1200 BC

Introduction
Definitions / Processes

Forensics – The Field



digital forensics

- Computer Forensics
- Mobil Forensics
- Datenbase Forensics
- Network Forensics
- Disk Forensics
- Memory Forensics
- Live Forensics

Forensics - Definition

- Digital Forensics [1]:
  - **Digital forensics** (sometimes known as **digital forensic science**) is a branch of forensic science encompassing the recovery and investigation of material found in digital devices, often in relation to computer crime.

- Computer Forensics [2]:
  - **Computer forensics** (sometimes known as **computer forensic science**) is a branch of digital forensic science pertaining to legal evidence found in computers and digital storage media. The goal of computer forensics is to examine digital media in a forensically sound manner with the aim of identifying, preserving, recovering, analyzing and presenting facts and opinions about the information.

Forensics - Definitions

- Network Forensics [3]:
  - **Network forensics** is a sub-branch of digital forensics relating to the monitoring and analysis of computer network traffic for the purposes of information gathering, legal evidence, or intrusion detection.[1] Unlike other areas of digital forensics, network investigations deal with volatile and dynamic information. Network traffic is transmitted and then lost, so network forensics is often a pro-active investigation.

- Database Forensics [4]:
  - **Database Forensics** is a branch of digital forensic science relating to the forensic study of databases and their related metadata.

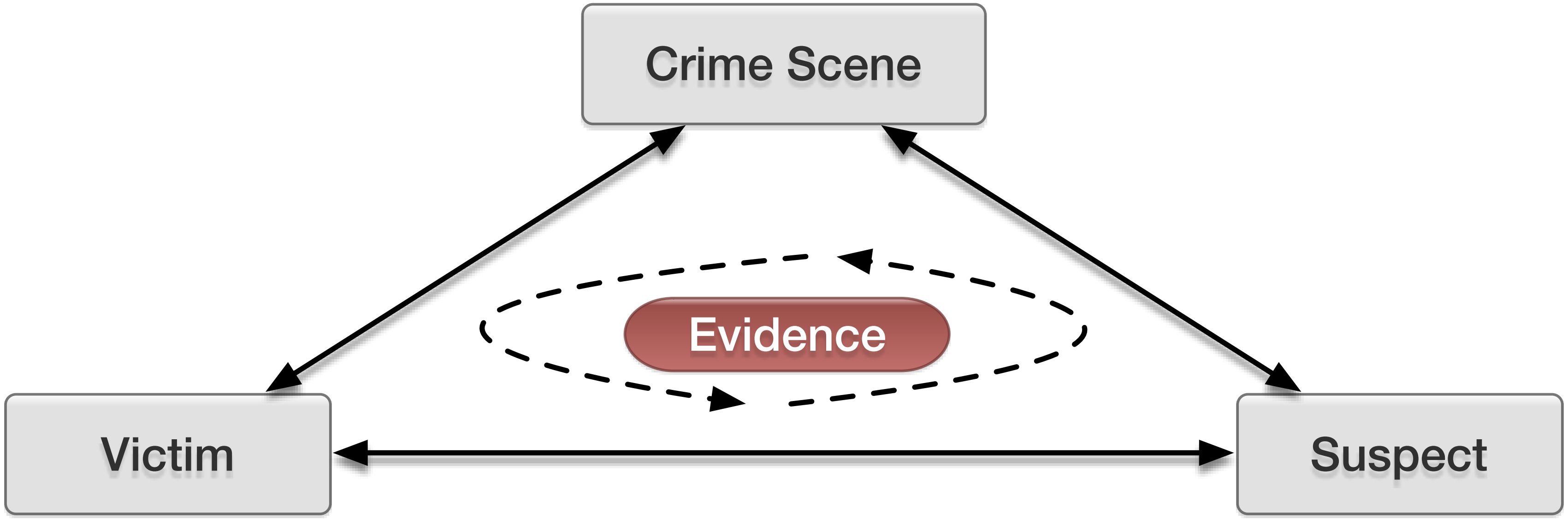
- Mobile Forensics [5]:
  - **Mobile device forensics** is a branch of digital forensics relating to recovery of digital evidence or data from a mobile device under forensically sound conditions. The phrase *mobile device* usually refers to mobile phones; however, it can also relate to any digital device that has both internal memory and communication ability.

What it's not like…

Image Source: http://www.clickcultural.com.br/foto/10/fto_thb_15510.jpg

Locard's Exchange Principle

- Every contact leaves a trace
  - Presence or absence of something
  - Either physical or electronically



Source: [3]

Locard’s Exchange Principle

“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]

Daubert Standard (US)

“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.”*

Source: [8]

Goal: No junk science in a courtroom

Way: Adhere to scientific standards

Daubert Standard (US)

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.

Principles (UK)

Four principles according to ACPO 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.

Legal Aspects - IANAL

§

- 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!**

Legal – General Advice

- 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

IT Security in Forensics

- 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

TLP RED

Part 1
References

References - Definitions

1 Digital Forensics: http://en.wikipedia.org/wiki/Digital_forensics

2 Computer Forensics: http://en.wikipedia.org/wiki/Computer_forensics

3 Mobile Device Forensics: http://en.wikipedia.org/wiki/Mobile_device_forensics

4 Database Forensics: http://en.wikipedia.org/wiki/Database_forensics

5 Network Forensics: http://en.wikipedia.org/wiki/Network_forensics

6 Chain of Custody: http://en.wikipedia.org/wiki/Chain_of_custody

References – Standards & Guidelines

7 Loccard‘s Exchange Principle: http://en.wikipedia.org/wiki/Locard%27s_exchange_principle

8 Daubert Standard: http://en.wikipedia.org/wiki/Daubert_standard

9 Electronic Crime Scene Investigation, Second Edition: http://www.ncjrs.gov/pdffiles1/nij/219941.pdf

10 FIRST Responders Guide to Computer Forensics: http://www.cert.org/archive/pdf/FRGCF_v1.3.pdf

11 Good Practice Guide for Computer-Based. Electronic Evidence: http://www.7safe.com/electronic_evidence/ACPO_guidelines_computer_evidence.pdf

12 NIST Guide to Integrating Forensic Techniques into Incident Response: http://csrc.nist.gov/publications/nistpubs/800-86/SP800-86.pdf

13 RFC 3227 - Guidelines for Evidence Collection and Archiving: http://tools.ietf.org/html/rfc3227

14 ISO 27037 - Guidelines for identification, collection and/or acquisition and preservation of digital evidence (Due 2012-10-26): http://www.iso.org/iso/iso_catalogue/catalogue_tc/catalogue_detail.htm?csnumber=44381

References – Forensics Tools

15 DEFT Linux: http://www.deftlinux.net/

16 SANS SIFT: http://computer-forensics.sans.org/community/downloads

17 CAINE: http://www.caine-live.net/

18 Backtrack Linux: http://www.backtrack-linux.org/

19 FCCU Forensic Boot CD: http://www.lnx4n6.be/index.php

20 eFence Helix: http://www.e-fense.com/products.php

21 Sleuthkit / Autopsy: http://www.sleuthkit.org/index.php

22 PyFLAG: http://www.pyflag.net/cgi-bin/moin.cgi

23 PTK: http://ptk.dflabs.com/

24 DFF: http://www.digital-forensic.org/

25 Encase: http://www.guidancesoftware.com/

26 FTK: http://accessdata.com/products/computer-forensics/ftk

27 X-Ways Forensics: http://www.x-ways.net/forensics/index-m.html