Digital forensics

Andrej Brodnik

Digital forensics

- lectures: dr. Andrej Brodnik
- lab sessions: dr. Gašper Fele-Žorž, Aleks Huč
- e-sources: učilnica

Course description

- Literature:
  - ***Eoghan Casey: Digital Evidence and Computer Crime (third edition)***
  - DFRWS (Digital Forensics Research Conference): http://www.dfrws.org/
  - Digital Investigation – Elsevier: http://www.journals.elsevier.com/digital-investigation/
  - SSDDFJ (Small Scale Digital Device Forensics Journal): http://www.ssddfj.org/
  - IFIP Working Group 11.9 Digital Forensics: http://www.ifip119.org/
  - IJDCF (International Journal of Digital Crime and Forensics): http://www.igi-global.com/Bookstore/TitleDetails.aspx?TitleId=1112

Course description – cont.

- lectures: including at least two invited lectures
- homework (HW):
  - four homework assignments from lectures (!), exercises and books
  - *for a positive grade: each homework is at least 20% and an average of at least 40%*
- lab work (LW):
  - two practical laboratory tasks
  - tasks placed in učilnica, where the results are also submitted
  - *for a positive grade: each task at least 20% and an average of at least 50%*

Course description – cont.

- seminar (SN):
  - a group will have to read: a scientific article from a magazine or conference, books, tools, or alike
  - presentation (20 minutes) and a written product, which is reviewed by colleagues and ultimately a final product
  - timetable:
    - by 4.3. group selection; by 11.3. each group issues a proposal for the topic of its seminar paper, which is confirmed or rejected, but no later than 18. 3. confirmed;
    - by 27.5. submitted presentation; by 13.5. submitted seminar; by 27.5. review; by 10.6. final text;
    - presentation of seminar papers in May and June
  - *for a positive grade: all assignments submitted and at least 40% from the presentation and 40% from the final written product and at least 50% from the overall grade of the seminar paper*

Course description – cont.

- written exam (WE):
  - only one written exam mid-year (scheduled for week 7. 5.)
  - *for a positive grade: at least 50%*

- final grade:

$$1/3 * WE + 1/3 * SN + 1/3 * (½ * LW + ½ * HW)$$

Course content

- Introduction and basics
- Investigation of an electronic device with an introduction to criminal proceedings
- Computers – hardware
- Operating Systems (MS Windows, Unix/Linux)
- Computer networks
- Mobile devices
- Performing a digital investigation
- Digital forensics of images

images in slides are from the book © 2011: ***Eoghan Casey: Digital Evidence and Computer Crime (third edition)***

Course content – cont.

- invited lectures:
  - Digital forensics at the Police
  - Protection of personal data (Information Commissioner)
  - Digital forensics of networks (SI-CERT)

Introduction and basics

chapters 1 – 5

The basics of digital forensics

chapter 1

- What is digital evidence?
  - Digital evidence is any digital information that is stored or transferred which enables confirmation or denial of a [criminal] act.
- What is a computer system?
  - open computer systems
  - communication systems
  - embedded systems

The basics of digital forensics

- to carry out a forensic investigation, knowledge is not enough, as it requires certification of personnel, organization, laboratory, ...

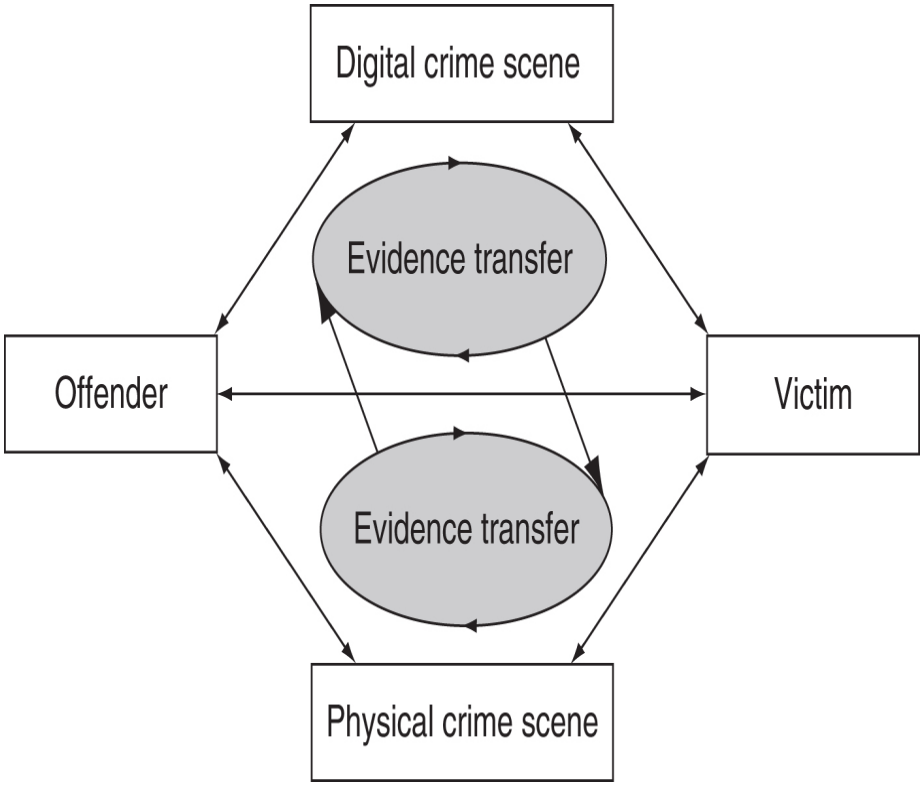
Principles of digital forensics

- use of science for the needs of law
- the importance of distinguishing between certainty and probability :

The lack of evidence is not evidence of non-existence!

- preparation and storage of material for potential litigation

Exchanging evidence



- fingerprints (on the keyboard)
- e-mail and notes
- notes about visited sites
- communication trails
- ...

Exchanging evidence between the victim and the perpetrator (or scene)

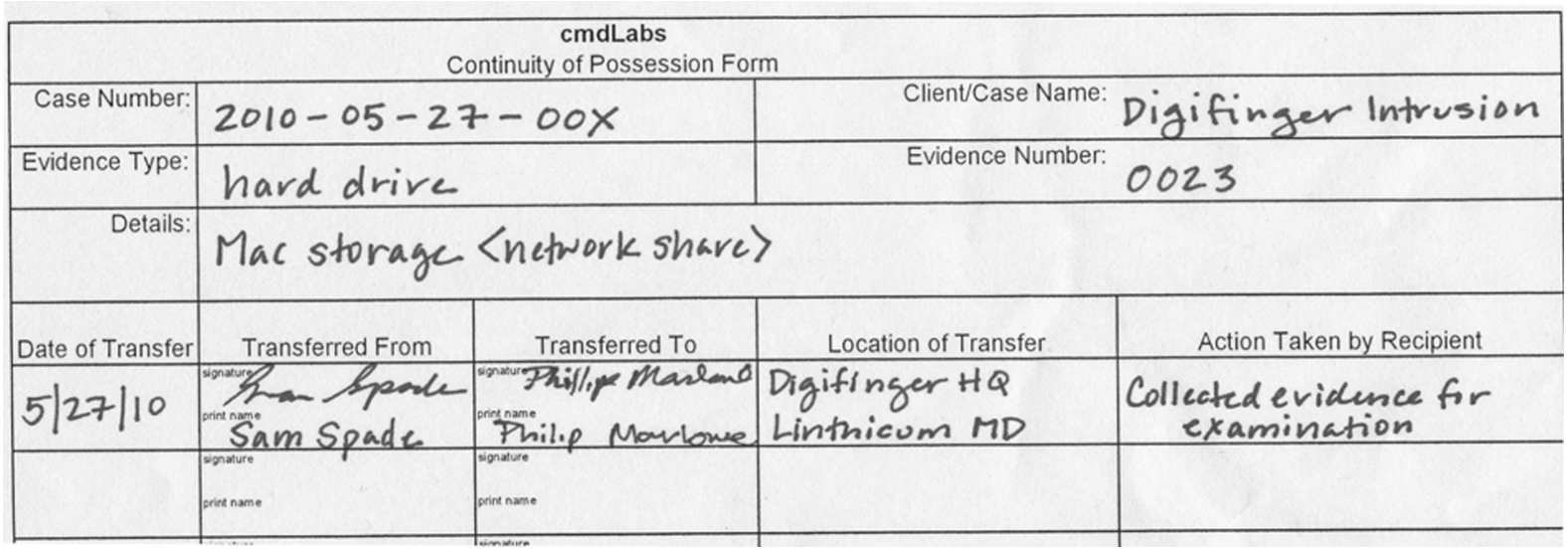
Locard's principle of exchange

Evidence

- evidence has common properties (all programs of this type) and special properties (concrete settings)
- digital evidence acceptable in court:
  - must be properly processed (captured) and
  - must be stored in a forensically correct manner
- that‘s why all actions on the scene must be recorded

Evidence

- ensuring authenticity:
  1. the content must be unchanged
  2. content must originate from the scene (recording the order of possession of evidence - the evidence chain)
  3. additional information on the handling of evidence



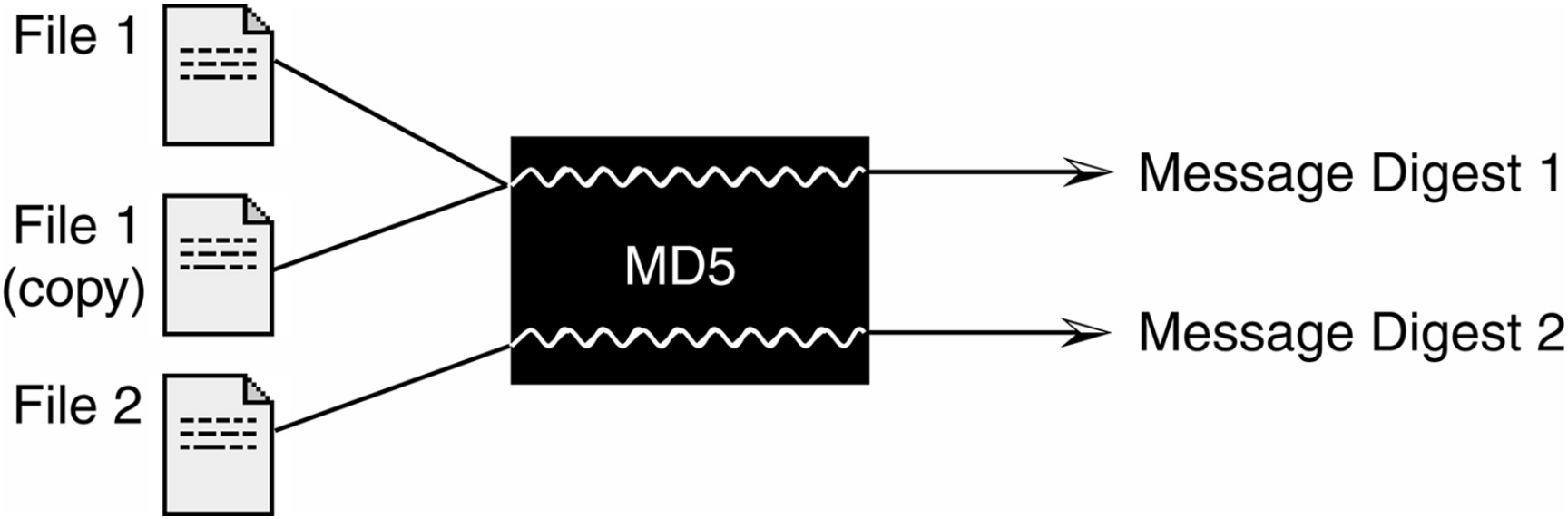
cmdLabs
Continuity of Possession Form

Case Number:	2010-05-27-00X	Client/Case Name:	Digifinger Intrusion
Evidence Type:	hard drive	Evidence Number:	0023
Details:	Mac storage <network share>		

Date of Transfer	Transferred From	Transferred To	Location of Transfer	Action Taken by Recipient
5/27/10	signature: Sam Spade print name: Sam Spade	signature: Phillip Marlowe print name: Philip Marlowe	Digifinger HQ Linthicum MD	Collected evidence for examination
	signature print name	signature print name		

The integrity of the evidence

- the accepted form of ensuring the integrity of evidence is signing it with a spray function
  - MD5, SHA-1, ...



Handling evidence

- objectivity of evidence
  - contains interpretation and presentation of evidence
- repeatability of evidence analysis

The challenges of handling digital evidence

- residue or reconstruction is not the same as the whole material:
  - the reconstructed file that was deleted is not the same as the partitions of it
  - the remnants of the sent e-mail are not the same as the entire e-mail
- the connection between (digital) evidence and the perpetrator is not always obvious
- data is not eternal
  - traffic information on the network

The challenges of handling digital evidence

- evidence is not necessarily error-free
  - the administrator has already tried to save the deleted file
  - the system administrator changed the content to secure the system
  - there was an error during data capture (non-standard procedure)
  - during the data capture, an infected medium was used
  - the media with the stored data has been damaged
  - ...

The digital world is not separate from the real one

- example: a buyer bought a good through eBay
  - *case example: Auction Fraud, 2000*; str. 29
- data can come from unexpected places

Developing the language of computer crime research

chapter 2

- there were no computers at the beginning, and the law only protected material evidence
- digital evidence includes:
  - computer (file) forensics
  - network forensics
  - mobile forensics
  - malware forensics
- important difference between research and data analysis
  - the investigation includes capture, organization, ...
  - the analysis represents the actual processing of evidence

The role of computer

According to Parker:

1. as the object of a crime
   - when a computer is stolen or destroyed
2. as the subject of a crime - a computer is the environment in which the crime is committed
   - when a computer is infected by a virus or impaired in some other way to inconvenience the individuals who use it
3. as the tool for conducting or planning a crime
   - when a computer is used to forge documents or break into other computers
4. the symbol of the computer itself to intimidate or deceive
   - offering services or the capabilities of computer services: gains on the stock exchange, ...

- data source(!!) - remains of files, e-mails, ...

The role of computer

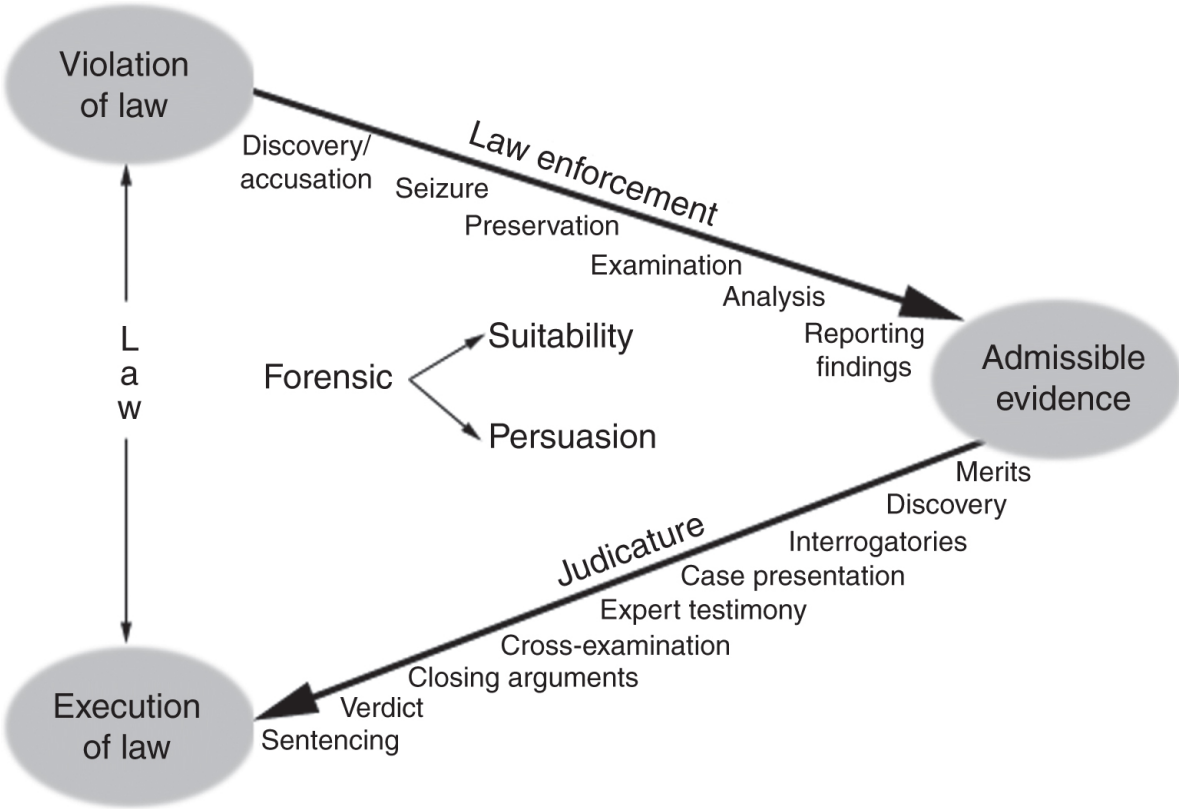
USDOJ (*US Department of Justice*):

- hardware as Contraband or Fruits of Crime
- hardware as an Instrumentality
- hardware as Evidence
- information as Contraband or Fruits of Crime
- information as an Instrumentality
- information as Evidence

Digital evidence in court

chapter 3

Digital evidence in court



Tasks of an expert

- presentation of evidence material:
  - do not succumb to influences
  - to reject prematurely set theories
  - use of scientific truth for the needs of the legal process
- ACM Code of ethics
- IEEE Code of ethics

Admissibility

- five basic rules:
  1. relevance of the material for the case
  2. authenticity of the material *(capture, traceability, ...)*
  3. not hearsay or admissible hearsay *(the evidence is not hearsay unless the speaker is present)*
  4. the best possible evidence *(original and copy)*
  5. not unduly prejudicial
- search warrant

Levels of Certainty

- we have a record in the notes:

```
2009-04-03 02:28:10 W3SVC1 10.10.10.50 GET
   /images/snakeoil13.jpg-80-192.168.1.1
   Mozilla/4.0+(compatible;+MSIE+6.0;Windows+NT+5.1) 200
   0 0
```

- what do we conclude from it?
- levels of Certainty:
  - (1) almost definitely; (2) most probably; (3) probably; (4) very possibly; (5) possibly
  - statistical probability

Computer Legislation

chapter 4

- legislation USA
  - 50 legislations
  - Washington DC legislation
  - federal legislation

Computer Legislation

chapter 5

- legislation ES (*EU*)
  - Ireland and Great Britain separate system – *common law*
  - the rest of the countries – *civil law*
- common legislation:
  - parliament EU
  - Convention on Cybercrime, 1. July 2004
    - has not been ratified by Ireland and the United Kingdom
  - Protocol on acts of racism and xenophobia, 1. March 2006

Crimes over the integrity of the computer

- Access to a computer is not allowed unless authorized by the owner
- Examples – *read 5.4.**:
  - hackers
  - stealing data
  - intercepting data
  - Influencing data and/or systems (DOS, viruses)
  - ››incorrect‹‹ or unintentional use of the unit/device

Crimes with the help of computers

- forgery
- fraud
- abuse

Crimes related to data content

- Crimes that affect the content of the data – *read 5.6.**
  - child pornography
  - web seduction - *what is this???*
  - racism and xenophobia

Other crimes

- copyright infringement
- computer blackmail
- …