

CEEPUS Lecture Budapest 2008

Computer forensics

Michael Sonntag

Content (1 Semester-hour, combined lecture and practice):

Day 1: Lecture on theory of computer forensics

Day 2: Lecture on data retention

Day 3: Lecture on privacy

Day 4: Lecture on file systems and data hiding

Day 5: Practice hard drive investigation: deleted files, file slack

Each lecture/practice is set for a duration of two hours (=120 minutes).

Practical part

In the practical part, the theoretical knowledge obtained in the lectures will be applied to practical problems as an introduction to basic forensic techniques: Some volume images will be investigated e.g. for deleted/hidden files and data otherwise not directly accessible.

Examination

Participants will prepare seminary papers on topics related to the course. These will be handed in, published on the web, discussed by all participants, and graded by the lecturer.

Required environment:

1. Computers for each (or each two) students
 - a. Operating system of the computer must be Windows
 - b. Alternative boot option to Linux would be a plus, but is not required
 - c. CD-ROM drive is required
 - d. 1 GB of free hard disk space for the software and images to investigate
2. Possibility to install additional programs (Administrator rights): Various software for forensic analysis
 - a. Evaluation/full versions are provided by the teacher (course CD-ROM)
3. Beamer in the lecture and the computer room (to show slides during the practical part)

Basic knowledge required by participants:

1. Knowledge about operating systems
2. Basic knowledge of networks, especially the Internet, and its protocols

Detailed content of the course

Lecture 1: Computer forensics

- What is computer forensics; when and where is it used?
- The relation of computer forensics to encryption
- Introduction to steganography in its various forms
- Securing evidence: Aspects regarding running and inert systems
- What information can be obtained in which circumstances?
- Classifying information to look for according to crimes
- Admissibility of evidence

Lecture 2: Data Retention

- The EU directive on data retention and its importance for computer forensics
- Implementations, respectively plans for it, in Europe
- Theoretical background of the directive: Why was it enacted, what are its aims?
- Pros & cons of the directive
- Technical implementation: Obtaining data, secure storage, access and logging
 - Interception/Logging of Internet protocols
- Estimating its effectivity

Lecture 3: Privacy

- The basics of privacy – EU legislation
 - What is "informed consent"?
 - When which data can be used for what purpose
- Privacy as the counterpart to data retention
- Privacy enhancing measures
 - Anonymisation proxies/networks for various protocols (SMTP, HTTP, ...)
 - Software development methods to reduce personal data usage
 - Secure deletion of data
- Countermeasures to avoid surveillance/data retention

Lecture 4: File systems

- Physical disk layout: Partitions and MBR
- The FAT, FAT32, NTFS, and EXT3 file systems in detail
 - Theoretical foundations
 - Advantages and problems
 - Special features regarding computer forensics
- The boot sequence and the resulting changes on disks
- Hidden parts in file systems: Streams, slack space (partition, file, ...), swap etc.
- Accessing hidden disk data
- Duplication of disks: Complete, secure, and provably unchanged

Practice 5: Hard-Drive Investigation

- Accessing disk images with various tools: Hex Editors, other OS, ...
- Finding files according to their (hidden) type: Identifying files according to content instead of extension/name
- Accessing deleted elements: Deleted files, file remnants
- Timestamps and their importance: When did what happen, when was the computer turned on, time/duration of internet connections etc.