



Department of Computer Science

Course Plan

Digital Forensics, 4 Credits

1. Level

Graduate course in Computer Science.

2. Course Aims

The aim of the course is to study state-of-the-art techniques for digital forensics analysis.

3. Course Content

The course consists of three modules: (1) file system forensics, (2) networked-based forensics, and (3) forensics analysis. Both host-based and network-based techniques are studied in the course.

4. Teaching and Examination

The course is organized as a seminar course. In order to pass the course the student is required to actively participate in at least at 80% of the meetings.

5. General Information

Course certificates are available from the department upon request.

6. Specific Prerequisites

Enrollment in the graduate program in computer science or permission of instructor.

7. Literature

See appendix.

Literature

- B. Carrier. “File System Forensics Analysis”. Addison-Wesley, Upper Saddle River, NJ, USA, 2005.
- M. Karresand and N. Shahmehri. “Oscar – File Type Identification of Binary Data in Disk Clusters and RAM Pages”. In Proceedings of IFIP TC-11 International Information Security Conference (IFIP/SEC 2006), Volume 21, Pages 413-424, Karlstad, Sweden, 2006. Springer, New York, NY, USA.
- M. Karresand and N. Shahmehri. “Oscar – Using Byte Pairs to Find File Type and Camera Make of Data Fragments”. In Proceedings of the Annual Workshop on Digital Forensics and Incident Analysis, Volume 1, Pages 85-94, Pontypridd, Wales, UK, 2006. Springer-Verlag, London, UK.
- H. Berghel and D. Hoelzer. “Disk Wiping By Any Other Name: What does a disk wiper wipe when a disk wiper does wipe disks?”. *Communication of the ACM* 49(8):17-21, August 2006.
- K. J. Jones, R. Bejtlich, and C. W. Rose. “Real Digital Forensics: Computer Security and incident Response”. Addison-Wesley, Upper Saddle River, NJ, USA, 2006.