UNIVERSITY OF SKÖVDE

TRANSLATION FROM SWEDISH

COURSE SYLLABUS

Digital Forensics for Incident Response A1F

7.5 credits

Course code: IT771A
Version number: 6
Valid from: 1 January 2025
Ratified by: Curriculum Committee for Informatics
Date of ratification: 16 August 2024

1. General information about the course

The course is provided by the University of Skövde and is named Digital Forensics for Incident Response A1F (IT-forensik inom incidenthantering A1F). It comprises 7.5 credits and is a second-cycle course. The level of progression is A1F.

The course is a part of the main field of study in Informatics. The disciplinary domain of the course is Technology.

2. Entry requirements

The course has the following entry requirements: passed IT760A Network Security Operations A1N (or the equivalent).

3. Course content

The course gives the student in-depth knowledge about processes and techniques used in incident handling. The student will acquire knowledge about methods and processes for incident handling and in-depth theoretical and practical knowledge in malware analysis. The student will also acquire in-depth knowledge about and discuss current research directions in the field.

4. Objectives

After completed course the student should be able to:

- explain how forensic methods are used in incident handling,
- explain malware on a deep technical level,
- apply forensic tools with the purpose of detecting and analyzing malware,
- analyze and problematize the content of research directions in the field, and
- independently and critically review reports and orally presented materials from intrusion detection research.

5. Examination

The course is graded A (Excellent), B (Very good), C (Good), D (Satisfactory), E (Sufficient) or F (Fail).

The examinations of the course consist of the following modes of assessment:

- **Seminar Assignments**
  5 credits, grades: A/B/C/D/E/F (determines the final grade)
- **Practical assignment**
  2.5 credits, grades: G/U

Students with a permanent disability who have been approved for directed educational support may be offered adapted modes of assessment.

6. Types of instruction and language of instruction

The teaching is comprised of seminars/group discussions, lectures and supervision.

The teaching is conducted in English.

7. Course literature and other educational materials

Kävrestad, J., Birath, M., Clarke, N. (2024). *Fundamentals of digital forensics: A guide to theory, research and applications* (3rd ed.). Springer. ISBN 9783031536489. DOI: 10.1007/978-3-031-53649-6

8. Student influence

Student influence in the course is ensured by means of course evaluation. The students are informed about the results of the evaluation and potential measures that have been taken or are planned, based on the course evaluation.

9. Additional information

Further information about the course, as well as national and local governing documents for higher education, is available on the website of the University of Skövde.