EP2780 Digital forensics and incident response 7.5 credits

Digital forensik och incidenthantering

This is a translation of the Swedish, legally binding, course syllabus.

Establishment

The official course syllabus is valid from autumn semester 2025 according to the decision of Director of First and Second Cycle Education: HS-2025-0428. Date of decision: 2025-03-14

Grading scale

A, B, C, D, E, FX, F

Education cycle

Second cycle

Main field of study

Computer Science and Engineering

Specific prerequisites

Knowledge of cyber security, 6 credits, equivalent to completed course DD2391/DD2395/IK2206/IV1013.

Language of instruction

The language of instruction is specified in the course offering information in the course catalogue.

Intended learning outcomes

After passing the course, the student should be able to:

- describe central concepts, models and methods in digital forensics and incident response
- describe the differences and similarities between a forensic situation and an incident response situation
- apply known methods for data collection and analysis in given situations
- plan and carry out data collection and data analysis for a forensic or incident analysis
- present and explain conclusions from a forensic analysis and an incident analysis and propose future actions
- explain the degree of certainty of the conclusions that can be drawn from a forensic analysis
- explain how one distinguishes between digital forensics and incident response
- critically review and source-critically assess a forensic report and an incident management report.

Course contents

The course gives the student both practical and theoretical knowledge of technologies, methods, models, laws/rules that apply at investigations of digital crimes or incidents.

For example the course covers the following:

- The history of forensics
- Digital forensics and digital evidence
- The investigation process of forensics/incident response
- Legislation and international cooperations in digital forensics
- Standards in the area and the requirements of an organisation that works with digital forensics or incident management
- Computer forensics
- Forensics for embedded systems and mobile units
- Network forensics

Examination

- LAB1 - Laborative work, 2.0 credits, grading scale: P, F
- QUI1 - Written quizzes, 5.5 credits, grading scale: A, B, C, D, E, FX, F

Based on recommendation from KTH's coordinator for disabilities, the examiner will decide how to adapt an examination for students with documented disability.

The examiner may apply another examination format when re-examining individual students.

If the course is discontinued, students may request to be examined during the following two academic years.

Ethical approach

- All members of a group are responsible for the group's work.
- In any assessment, every student shall honestly disclose any help received and sources used.
- In an oral assessment, every student shall be able to present and answer questions about the entire assignment and solution.