EP2780 Digital forensics and incident response 7.5 credits

Digital forensik och incidenthantering

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

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

Establishment

The official course syllabus is valid from the autumn semester 2022 in accordance with the decision from the head of school: J-2021-1872.Decision date: 14/10/2021

Grading scale

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

Education cycle

Second cycle

Main field of study

Computer Science and Engineering

Specific prerequisites

Knowledge in cybersecurity, 7.5 higher education credits, equivalent to completed course DD2391 or completed courses DD2394 and DD2395.

Active participation in a course offering where the final examination is not yet reported in LADOK is considered equivalent to completion of the course.

Being registered for a course counts as active participation.

The term 'final examination' encompasses both the regular examination and the first re-examination.

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

in terms of knowledge and understanding:

- describe central concepts, models and methods in digital forensics and incident response
- describe the national and international contexts and the laws, regulations, and conventions that are negotiated within these contexts, and how these are applied both internationally and nationally
- describe differences and similarities between a forensic scenario and an incident response scenario

in terms of skills and abilities:

- apply known methods for data collection and analysis in given situations
- plan and carry out data collection and analysis, in order to run a forensic analysis or an incident analysis
- present and explain conclusions from a forensic analysis
- present and explain conclusions from an incident, as well as suggest future measures

in terms of judgement and approach:

- explain limitations with forensic analysis with regard to how certain conclusions can be drawn
- explain how the previous separate between digital forensics and incident response
- review critically and source-critically a forensic and incident response report
- evaluate when forensic work (particularly when it does not take place in connection with a crime scene investigation) has a negative effect on the personal integrity of individuals.

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
- PRO1 - Project, 2.5 credits, grading scale: P, F
- TEN1 - Written exam, 3.0 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.

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.