Digital Forensics and Incident Response

Digital forensik och incidentrespons
6 credits

Programme course

TSIT14

Valid from:

Determined by	**Main field of study**	
Board of Studies for Computer Science and Media Technology	Information Technology, Computer Science and Engineering, Computer Science	
Date determined	**Course level**	**Progressive specialisation**
2023-08-31	Second cycle	A1X
Revised by	**Disciplinary domain**	
	Technology	
Revision date	**Subject group**	
	Computer Technology	
Offered first time	**Offered for the last time**	
Autumn semester 2024		
Department	**Replaced by**	
Institutionen för systemteknik		

Course offered for

- Master's Programme in Cybersecurity
- Master of Science in Computer Science and Engineering
- Master of Science in Information Technology
- Master of Science in Computer Science and Software Engineering

Prerequisites

Computer networks, Ethical hacking

Intended learning outcomes

In the course the basic requirements for and limitations of digital forensics and how to be able to find and secure traces in digital systems, and evaluate digital evidenceis is taught.

After completing the course, the student must be able to:

- Define basic concepts and principles for digital forensics.
- Summarize, choose and use efficient methods to find and secure traces in digital systems.
- Describe principles, challenges, methods, and tools for handling cyber security incidents.
- Investigate the sequence of events in cyber security incidents from traces in digital systems.
- Present and evaluate digital evidence.
- Summarize relevant laws and how they influence choice of method and forensic argumentation in example cases.
- Exemplify the impact of digital forensics for a sustainable society in the sense of social and economic resilience against internal and external threats.

Course content

During the course the following subjects will be included:

- Network forensics
- Incident response
- Digital forensics on hardware
- Mobile forensics
- Memory forensics
- Forensics on image and video
- Log management, preserving evidence
- Particulars of SCADA environments and critical infrastructure
- Theoretical models
- Advanced and narrow topics, e.g., adversary simulation
- Laws and use of digital forensic material as evidence

Teaching and working methods

The course consists of lectures and a series of laborations

Examination

LAB1	Laboratory work	4 credits	U, G
TEN1	Written examination	2 credits	U, 3, 4, 5

Grades

Four-grade scale, LiU, U, 3, 4, 5

Other information

About teaching and examination language

The teaching language is presented in the Overview tab for each course. The examination language relates to the teaching language as follows:

- If teaching language is “Swedish”, the course as a whole could be given in Swedish, or partly in English. Examination language is Swedish, but parts of the examination can be in English.
- If teaching language is “English”, the course as a whole is taught in English. Examination language is English.
- If teaching language is “Swedish/English”, the course as a whole will be taught in English if students without prior knowledge of the Swedish language participate. Examination language is Swedish or English depending on teaching language.

Other

The course is conducted in such a way that there are equal opportunities with regard to sex, transgender identity or expression, ethnicity, religion or other belief, disability, sexual orientation and age.

The planning and implementation of a course should correspond to the course syllabus. The course evaluation should therefore be conducted with the course syllabus as a starting point.

The course is campus-based at the location specified for the course, unless otherwise stated under “Teaching and working methods”. Please note, in a campus-based course occasional remote sessions could be included.