JÖNKÖPING UNIVERSITY
School of Engineering

COURSE SYLLABUS

Forensics, Cybercrime, and Incident Response, 7.5 credits

Forensik, cyberbrott och incidenthantering, 7.5 högskolepoäng

Course Code:	T2FCOI	Education Cycle:	Second-cycle level
Confirmed:	Sep 01, 2025	Disciplinary domain:	Technology
Valid From:	Jan 18, 2027	Subject group:	Computer Technology
		Specialised in:	A1F Second cycle, has second-cycle course/s as entry requirements
		Main field of study:	Computer Science

Intended Learning Outcomes (ILO)

On completion of the course the student shall:

Knowledge and understanding

- display knowledge of key standards and frameworks for incident response
- display knowledge of key concepts relating to cyber-enabled crime and cyber-dependent crime
- display knowledge of different tools and applications for security monitoring, digital forensics, and evidence collection

Skills and abilities

- demonstrate skills in using tools for security monitoring
- demonstrate skills in performing and reporting on forensic investigations
- demonstrate skills in creating and using an incident response plan

Judgement and approach

- demonstrate insights into the different phases of a cyberattack and suggest how an organisation can protect itself against cyberattacks during the different phases
- demonstrate insight into how forensics principles can assist in the handling of advanced cyberattacks
- demonstrate insights into the societal, legal, and ethical aspects of incident response

Content

The course starts with discussing key standards and frameworks for incident response, key concepts relating to cybercrime, and digital elements in crime. The course includes technical concepts of network security, intrusion detection, security monitoring, and digital forensics. The course will also discuss digital evidence and the process of lawful evidence collection and elaborate on how forensic principles can aid the incident response process. During the course, students will gain hands-on experience with common tools and applications used for security monitoring, digital forensics, and intrusion detection.

The course includes the following elements:

- Key standards and frameworks for incident response (e.g., NIST SP800-61), different phases in the incident response plan, and handling of cybersecurity incidents
- Categories of cybercrime and cybercriminals
- Digital forensics and digital evidence, with emphasis on memory forensics
- Security monitoring, intrusion data analysis, security information, and event management (SIEM)

Type of instruction

The course consists of lectures, laboratory work, and seminars.

Language of instruction is in English.

Entry requirements

Passed courses at least 90 credits within the major subject in Computer Science, Informatics, Information Systems, Computer Engineering, or the equivalent, and taken the course Penetration Testing, 7,5 credits or equivalent. Proof of English proficiency is required.

Examination and grades

The course is graded 5, 4, 3 or U.

Registration of examination:

Name of the Test	Value	Grading
Laboratory [1]	6 credits	5/4/3/U
Seminar	1.5 credits	G/U

[1]Determines the final grade of the course, which is issued only when all course units have been passed.

Course literature

Please note that changes may be made to the reading list up until eight weeks before the start of the course.

Kävrestad, J., Birath, M., Clarke, N. (2024). *Fundamentals of digital forensics: A guide to theory, research and applications.* Cham: Springer