Blekinge Institute of Technology
Department of Computer Science

Revision: 1
Reg.no: BTH-4.1.14-0831-2021

COURSE SYLLABUS

Avancerad digital undersökningsteknik

Advanced Digital Forensics

7.5 credits (7,5 högskolepoäng)

Course code: DV2611
Main field of study: Computer Science, Software Engineering
Disciplinary domain: Technology
Education level: Second cycle
Specialization: A1N - Second cycle, has only first cycle course/s as entry requirements

Language of instruction: English
Applies from: 2022-01-17
Approved: 2021-09-01

1. Decision

This course is established by Dean 2021-04-29. The course syllabus is approved by Head of Department of Computer Science 2021-09-01 and applies from 2022-01-17.

2. Entry requirements

Admission to the course requires at least 120 credits, of which at least 90 credits are in a technical area, and a minimum of 2 years professional experience within an area related to software-intensive product and/or service development (shown by, for example, a work certificate from an employer).

3. Objective and content

3.1 Objective

Companies and their IT systems are affected by advanced intrusions, various ransomware attacks and or thefts of both sensitive and secret information. In case of being compromised companies need to understand their weak points, ways of intrusion and attackers attributes.
The course focuses on developing the student's skills to investigate and analyze complex cyber attacks (Cyber Kill Chain) and to track the threat actor, discover exploited vulnerabilities so that companies can restore data and system integrity.

3.2 Content

- Digital forensic (DF) methodology, processes and standards.
- Detailed tracks and artefacts in different OS.
- Network and email forensic
- Memory analysis
- Mobile forensic
- Cloud specific aspects of forensic
- APT (Advanced Persistent Threats) and the seven steps of the Cyber Kill Chain
- Report writing and presentation

4. Learning outcomes

The following learning outcomes are examined in the course:

4.1 Knowledge and understanding

On completion of the course, the student will be able to:

- DF standards and methodologies.
- DF analysis approach.
- Filesystems DF specifics.
- The artefacts reflect the user behaviour that could be obtained from OS.
- Malware activities, defence evasion technologies and it's analysis.
- Representation of user and system behaviour in network activity.
- Technologies and tools for data acquisition and analysis.
- OS, network and cloud forensic readiness.
- Requirements for the good forensic report.

4.2 Competence and skills

On completion of the course, the student will be able to:

• Independently conduct DF activities compliant with acceptable practice standards.
• Identify when digital forensics may be useful and understand how to escalate an investigation.
• Develop and maintain a digital forensics capacity in on-site and cloud infrastructure.
• Analyse network traffic separately to identify activity patterns or specific actions that warrant further investigation and use of historical NetFlow data to identify events.
• Understand how to perform artefact analysis and how obtained information can be used to prove malicious intent.
• Obtain skills in memory analysis and special tools to detect hidden processes, malware, attacker commands, rootkits, network connections.
• Obtain knowledge of tracking user and attack activity in the system through in-depth timeline analysis.
• Be able to present the results of DF in court process.

4.3 Judgement and approach

On completion of the course, the student will be able to:

• Identify and implement appropriate methods and techniques for acquiring, exploring, analyzing and evaluating data and digital evidence.
• Generate, prove, or refute hypotheses about malicious activities in/with help of hosts, networks and cloud environments.
• Evaluate the aggregated artefacts and indicators of compromise to obtain the whole cybercrime: APT, "Cyber Kill Chain" attack timeline.

5. Learning activities

The teaching is organised around online lectures, pre-recorded videos, laboratory sessions, together with written material, literature, and research literature. Throughout the course, communication, feedback, and discussions with teachers and fellow participants will take place through email and the course's online learning platform.

6. Assessment and grading

Modes of examinations of the course

Code	Module	Credits	Grade
2205	Take-home examination	1.5 credits	GU
2215	Laboratory session 1	1 credits	GU
2225	Laboratory session 2	1 credits	GU
2235	Laboratory session 3	1 credits	GU
2245	Laboratory session 4	1 credits	AF
2255	Written report	2 credits	AF

The course will be graded G Pass, UX Fail, supplementation required, U Fail.

The information before a course occasion states the assessment criteria and make explicit in which modes of examination that the learning outcomes are assessed.

An examiner can, after consulting the Disability Advisor at BTH, decide on a customized examination form for a student with a long-term disability to be provided with an examination equivalent to one given to a student who is not disabled.

7. Course evaluation

The course evaluation should be carried out in line with BTH:s course evaluation template and process.

8. Restrictions regarding degree

The course can form part of a degree but not together with another course the content of which completely or partly corresponds with the contents of this course.

9. Course literature and other materials of instruction

Materials such as research articles and other course materials, as well as recommendations for additional reading, are provided via the courses' online platform.