IMT4022 Digital Forensics 2 - 2013-2014

Course code:
IMT4022

Course name:
Digital Forensics 2

Course level:
Master (syklus 2)

ECTS Credits:
10

Duration:
Vår

Language of instruction:
English

Prerequisite(s):

- BSc level basics in operating systems, data communication and network security
- IMT4012 Digital Forensics 1 or IMT3551 Digital Forensics or equivalent.

Expected learning outcomes:
Knowledge:

- The course develops deep understanding in the methodology, technology and application of digital forensics.
- Students are expected to reach an advanced level of knowledge in the broad spectrum of digital evidence, analysis methods and tools.
- The course is oriented towards profound theoretical background, where the students learn contemporary techniques and advanced research topics.

Skills:

- The students are capable of analyzing existing theories, methods and interpretations in the field of digital forensics and working independently on solving theoretical and practical problems.
- The students can use relevant scientific methods in independent research and development in digital forensics.
- The students are capable of performing critical analysis of various literature sources and applying them in structuring and formulating scientific reasoning in digital forensics.
- The students are capable of carrying out an independent limited research or development project in digital forensics under supervision, following the applicable ethical rules.

General competence:

- The students are capable of analyzing relevant professional and research ethical problems in digital forensics.
- The students are capable of applying their knowledge and skills in new fields, in order to accomplish advanced tasks and projects in digital forensics.
- The students can work independently and are familiar with terminology of digital forensics.
- The students are capable of discussing professional problems, analyses and conclusions in the field of digital forensics, both with specialists and with general audience.
- The students are capable of contributing to innovation and innovation processes.

Topic(s):

- Forensics and Incident Response
- Microsoft Windows Host Forensic
- Unix and Linux Host Forensics
- Live Forensics and RAM Analysis
- Network and Cloud Forensics
- Botnet and Malware Analysis
- Mobile and Embedded Device Analysis
- Securing Evidence, Cryptanalysis and Anti-Forensics
- Steganography
- eDiscovery: Fingerprinting, Correlation, and Search

Teaching Methods:
Lectures
Laboratory work

Teaching Methods (additional text):
The course will be made accessible for both campus and remote students. Every student is free to choose the pedagogic arrangement form that is best fitted for her/his own requirement. The lectures in the course will be given on campus and are open for both categories of students. All the lectures will also be available on Internet through GUC's learning management system (ClassFronter).

Form(s) of Assessment:
Other

Form(s) of Assessment (additional text):
An overall evaluation based on a 100 point scale, where project work counts up to 50 points and final exam (3 hours) counts up to 50 points (at least 18 at the written exam MUST be obtained). Conversion from 100 point scale to A-F scale according to recommended conversion table. In specific circumstances, the course responsible can slightly adjust the limits in the conversion table to enforce compatibility with the qualitative descriptions on the A-F scale.

Grading Scale:
Alphabetical Scale, A(best) – F (fail)

External/internal examiner:
Internal examiner. An external examiner will be used every 4th year. Next time in the school-year 2013/2014.

Re-sit examination:
For the final exam: Ordinary re-sit examination.

Tillatte hjelpemidler:

Coursework Requirements:
None

Academic responsibility:
Faculty of Computer Science and Media Technology

Course responsibility:
Professor Katrin Franke (katrin.franke@hig.no) /Adjunct Associate Professor André Årnes (andre.arnes@hig.no)

Teaching Materials:
Keith J. Jones, Richard Bejtlich, Curtis W. Rose: Real Digital Forensics: Computer Security and Incident Response. Addison-Wesley, 2005, (0-321-24069-3)

Dan Farmer and Wietse Venema: Forensic Discovery, Addison-Wesley, 2005 (ISBN 0-201-63497-x)

Presentation material and selected academic papers

Additional information:
Knowledge of Linux is an advantage

In case there will be less than 5 students that will apply for the course, it will be at the discretion of the head of the study program whether the course will be offered or not an if yes, in which form.

Publish:
Yes