New Course

Computer Forensics

A new 5 ECTS special course on computer forensics is being offered in the 3 week period in January 2015. The course is particularly intended for students who follow the Computer Security study line and it is mandatory for students who wish to obtain the special Diploma in Cyber Security, but any student who is interested in computer forensics may register.

General course objectives:
The aim of this course is to provide a working knowledge of computer forensics. The goal of computer forensics is to examine digital media in a forensically sound manner with the aim of identifying, preserving, recovering, analysing and presenting facts and opinions about the digital information.

The course will focus on the technical difficulties of identifying and recovering information from computer and communication systems, such as client computers, servers and smartphones. It will also address common techniques to analyse such information and establish situational awareness. Finally, it will address the difficulty of preserving data obtained from compromised systems, so that they can be used as evidence in court and to present facts and opinions about the data so that they can be included as expert testimony in court.

Learning objectives:
A student who has met the objectives of the course will be able to:
- Setup a forensics investigation plan
- Identifies common places to look for evidence in common computer systems
- Preserve authenticity of evidence that may have to be used in a court case
- Recover evidence from different types of computer systems and media (e.g. files and memory)
- Analyse evidence to provide a timeline and attribution of events
- Establish situational awareness in the case of an ongoing security incident
- Perform forensics analysis of a compromised subsystem
- Present the results of a forensics analysis, so that it can be used as evidence in court

Course content:
- Common computer forensics analysis tools and techniques
- Common formats for system data and meta-data (OS structures, file systems, etc.)
- Forensic information extraction techniques for data in memory and permanent storage
- Core elements of legal proceedings and expert witness behaviour

Exam form:
An overall grade (7-scale) will be given for the course. The grade is based on a number of small reports following each of the three main subjects and a final oral presentation.

Practical Information:
This course is taught by KPMG Forensic Technology in Denmark and UK, who have extensive experience in Computer Forensics. KPMG will be supported by domain experts from other organisations.
Course responsible: Christian D. Jensen (cdje@dtu.dk)
Registration for this course is done through email to the course responsible before 20 December 2014; please include the string “Computer Forensics registration” in the email subject. There are a limited number of places available on this course, so priority will be given to students who follow the cyber security program; remaining places will be offered on a first come first served basis.

Danmarks Tekniske Universitet
Institut for Matematik og Computer Science
Matematiktorvet
Bygning 324
2800 Kgs. Lyngby
Tlf. 45 25 30 31
Dir. 45 25 37 24
Fax 45 88 13 99
cdje@dtu.dk
www.compute.dtu.dk