HI2009 IT-Security III: Computer Forensics Lab 7.5 credits

IT-säkerhet III: Laborationer

This is a translation of the Swedish, legally binding, course syllabus.

If the course is discontinued, students may request to be examined during the following two academic years

Establishment

Course syllabus for HI2009 valid from Autumn 2011

Grading scale

A, B, C, D, E, FX, F

Education cycle

Second cycle

Main field of study

Electrical Engineering

Specific prerequisites

Knowledge corresponding to HI119V IT-Sec II and documented proficiency in English corresponding to English A/English 5.

Language of instruction

The language of instruction is specified in the course offering information in the course catalogue.

Intended learning outcomes

The course goal is to enable the student to work with typical Computer Forensics tools, as a continuation to th Computer Forensics theory studied in the IT-Sec II Computer Forensics course.

Course contents

How to use typical Computer Forensics tools and techniques. Hard disk analysis, Mobile phone analysis, Sniffers, Network Monitoring. Wireless Surveillance.

Disposition

Course disposition: The course is given in English and is of half time studies. The course is a distance course. For further information in English, please contact the teacher.

Course literature

Kursmaterial kan rekvireras från Högskolans Bokservice på Campus Haninge, telefon: 08-790 4885; e-post: bokservice@sth.kth.se.

Kurslitteratur: **Real Digital Forensics**, Jones, Bejtlich & Rose, Addison-Wesley, ISBN-10: 0321240693, ISBN-13:9780321240699.

Forensic Tools & Technology, Eoghan Casey, 2001, 448 pp, Academic Press,ISBN-10: 0121631036, ISBN-13: 9780121631031

Kurskompendium HI2009 på CD-ROM med laborationsmaterial, studieanvisningar och övningsuppgifter, programvara och referensmaterial. Förf. L.O. Strömberg.

Vi utgår från att studenterna redan har kursmaterialet från HI119V, och vi kommer i kursen att använda mjukvara och annat material som återfinnes i HI119V:s digitala kurskompendium och lab-kit (HI119V är

förkunskapskrav till denna kurs).

Equipment

You will need:

* A personal computer (PC) running Windows XP / Vista / 7/8

* Internet access

* two working email addresses (do not use free webmail clients, use POP3)

   * A scientific pocket calculator

Examination

- LAB1 - Laboratory Work, 1.5 credits, grading scale: P, F
- LAB2 - Laboratory Work, 1.5 credits, grading scale: P, F
- LAB3 - Laboratory Work, 1.5 credits, grading scale: P, F
- TEN1 - Examination, 3.0 credits, grading scale: A, B, C, D, E, FX, F

Based on recommendation from KTH's coordinator for disabilities, the examiner will decide how to adapt an examination for students with documented disability.

The examiner may apply another examination format when re-examining individual students.

Examinations are offered three times a year: typically the first Saturday in May, August, and December.

Written examinations are four hours long, and consist of 68 questions; 60 of which are multiple choice (5 choices each) and 8 are in depth questions, including mathematical calculations. The Final examination in IT-Sec III is a lab project.

Written examinations worldwide can usually be arranged at other universities, as well as at Swedish embassies and consulates.

Ethical approach

- All members of a group are responsible for the group's work.
- In any assessment, every student shall honestly disclose any help received and sources used.
- In an oral assessment, every student shall be able to present and answer questions about the entire assignment and solution.