DIFO

Senast uppdaterad 2012-02-08, Utskrivet 2012-04-19

Namn: Digital forensik
Högskolepoäng: 7.5
Datum: 2012-01-16 till 2012-03-17
förkunskapskrav: Dokumenterad kunskap om:
- grundläggande begrepp och principer inom datasäkerhet
- grunderna i struktur och organisation av operativsystem

Mål

The course main goal is to expose the student on an introductory level to the discipline of digital forensics, the relevant subject areas, the dependencies and the cross-fertilization with other disciplines such as computer science, law, sociology, ethics, economics, and political science. The students would attain the goal by meeting the following objectives:
1.Understanding and knowledge of the theoretical framework of digital forensics,
2.Recognize the need for rigorous and scientifically validated forensic examination,
3.Identify, evaluate and use some of the basic hardware and software tools,
4.To be aware of more complex digital forensics problems, adequate demanding forensic procedures, and sophisticated tools to solve them,
5.Know the basics and understand the Internet architecture for global networking and to be able to subject them to digital forensic analysis in order to determine the value of the dynamic evidence,
6.Appreciate the concept of Network protection and the Internet and the ways of keeping the Cyberspace safe and amicable, and
7.Comprehend the basic techniques and the range of problems relative to evidence found in small scale digital devices
Learning outcomes
Upon successful completion of the course the student should be able to understand and state the fundamental principles and concepts of digital forensics, be conversant with the importance of digital evidence and know the basics of the digital forensic examination, and be able to engage in a competent discourse about the essential role digital forensics play in the digital world. The student should be able to understand and explain the basic digital tools for forensic analysis, and apply them in an operating system environment such as Windows, analyze and evaluate digital evidence retrieved during forensic examination, and appreciate the need for rigorous observation of the professional and ethical standards. The student should gain some insight into the way network and the Internet forensics is being conducted and assists in the protection or recovery of the normal operation of networks and the Internet.

Innehåll

The course is a rounded introduction to the basic concepts and principles of Digital Forensics addressing both the theoretical and the technological aspects. We shall start with a brief history of the discipline along the key ideas and reasons behind its emergence and development. In addition, in the prologue, the main subjects that constitute the area of digital forensics are enumerated in the context of technological, legal and social perspectives. The nature and the role of digital evidence are examined along the procedures for its collection,

preservation, analysis, and presenting. Some problems with digital evidence from a real life shall be discussed in order to underline the inherent difficulties that stem from the information stored or retrieved in a digital form. Digital forensics deals with scientific examination and analysis of data stored in a digital form that should be eventually admissible in the court of law, hence the use of acknowledged and peer-reviewed scientific methods is necessary in order to preserve the evidential integrity of the data.
Before going into analysis in the digital data that is stored on a single (standalone) computer with all different peripheral devices, there will be brief review of the basic machine hardware and software components, in particular the inner workings of operating systems, and entities such as working memories, processors, disks, and file system organization. Since Windows is a dominant operating system and primary technological platform, the environment created by its operation should be subject to thorough examination which includes its file systems, metadata and hidden location such as caches, spool files, unallocated depository spaces and memory. An optional and informational light reading some points related to Unix OS family and Mackintosh OS may be addressed.
While a significant amount of evidence (static) could be found on a single computer or even some part of it, there are much more possibilities when computers are interconnected, like most of them are at the present world, the data is linked and always in transition from one place to another (dynamic). So, the course will proceed with some basics of networking, especially TCP/IP networks and the architecture of the Internet, the fundamental protocols, the organization and the structure of the packets, data and control units, and the place where the information is stored, how it is going to be retrieved and made into an evidence that would give us an insight on the meaning of the data, and the actions and the deeds that generated the evidence or cyber trails. The last part is basically an outline of the elementary issues related to digital forensics in Small Scale Digital Devices (SSDDs).

Genomförande

In summary, the following topics are studied during the course:
•Fundamental ideas and concepts of the digital forensic science
•Differences, similarities and relations between security and digital forensics
•The chain of custody and the importance of probative digital evidence
•Elementary concepts in civil and criminal laws
•The process of collecting, storing and analyzing digital evidence in a scientific manner
•Identify and recover evidence from Windows based file systems and registries
•Internet protocols and technology for network forensics
•Analysis of network traffic and evidence of various events
•Elementary concepts related to the evidence found in small scale digital devices

Litteratur

- Eoghan Casey: Handbook of Digital Forensics and Investigation (Upplaga: Second edition), Academic Press, 2009, 978-0123742674

Kompendier

Course text
•Eoghan Casey Handbook of Digital Forensics and Investigation, Academic Press, 2010, 2e.
Lecture notes
•Hand-outs from the lectures and the labs
Background reading

•Materials posted in the respective conferences such as
- popular articles
- scientific papers
•Dan Farmer, Wietse Venema: Forensic Discovery, Addison Wesley/Pearson Education, 2007, 2e.

Examination

Examination
Evaluation and grading policy
All three parts that constitute the course such as the labs, term project and the final exam will be part of a separate summative assessment and grading.
The three labs are equal to a credit of 3 ECTS points, the term project is also equal to 3 ECTS points, while the final exam is worth 1.5 ECTS points. Both the labs and project represent group work, while the final exam is on individual basis. The fragmentation was introduced in order to provide students with flexibility and induce their continues work and interests.
The students will receive formative assessment through the work in the lab, subsequent discussions, and during the presentations of their work.
Lab attendance is mandatory. Naturally, a student may be excused if there are extenuating circumstances. One week after a lab is completed the report of the working group should be submitted. It will be graded and applied towards the total credit for the lab part of the course
2. Self-assessment tests are designed to assist you in learning and understanding the material covered during the course. These tests should not be turned in and would not be graded.
3. The final report should be also turned within the deadline, so there will be enough time for proper assessment and for the group which is selected as an opponent to write their review. The duration of the project will be around four to five weeks.
Task: Lab assignments – 3 ECTS credits
There are three lab assignments that deal with different aspects of digital scene investigations and using various tools that are available in the CSI lab. Each lab assignment is done by a group of two or three students and carries 10 points. The total number of points is 40.
ECTS scale for Lab assignments
0 – 14 F
15 –19 Fx
20 – 23 E
24 – 27 D
28 – 31 C
32 – 35 B
36 – 40 A
Task: Term project - 3 ECTS credits
The project will be similar to the assignments you are going to do for the labs; however it should be more involved and require some longer time to do it. The work on the project consists of four different parts, and all of them should be completed. Each project should go through the following steps:
1. Writing the report on the work completed.
2. Reading the report done by another group, writing a review, and preparing questions to be asked during the seminar session. The review should be about one page.

3. Presenting the results during the seminar session and answering the questions. For this you will need to prepare a Power Point Presentation (PPP).
4. Prepare questions for the reviewed project and take part in the overall discussion
The seminar session per group should last about 20 minutes. The presentation of the project should not take more than 10 minutes, while the opposition along with the Q/A from the audience should last approximately 10 minutes.
ECTS scale for the term project
0 – 14 F
15 –19 Fx
20 – 23 E
24 – 27 D
28 – 31 C
32 – 35 B
36 – 40 A
Task: Final exam-1.5 ECTS credits
The exam consist of twenty short questions that range on the whole material covered and they come from the self-assessment tests that are distributed to the students during the course. Therefore the students are familiar with all of the questions that might appear on the final exam.
ECTS scale for the final exam:
0 – 6 F
7 - 9 Fx
10 – 11 E
12 – 13 D
14 – 15 C
16 – 17 B
18 – 20 A

Medverkande

Kurs-/delkursansvarig
Oliver Popov

Föreläsare
Oliver Popov

Lektionsledare
Oliver Popov
Spyridon Dosis
Irvin Homem

Handledare
Oliver Popov
Spyridon Dosis
Irvin Homem
Andrius Januta

Gästföreläsare
Oliver Popov