1. Overview

Description

Digital forensics is a sub-field of computer security concerned with the theory and techniques of conducting investigations in an attempt to solve crimes where digital media and/or devices were involved, as well as to investigate security breaches and/or failures.

Prerequisites

None.

Related modules

This module assumes knowledge of topics covered in the following courses: Computer Security (COS 330), Information Security I (honours) (COS 720), Information Security II (honours) COS 721).

Study units

This module will broadly look at some of the following units as central to the main themes in Digital Forensic Investigations:

- An overview of digital forensics
- The Science of digital forensics
- The digital forensic investigation process
- Digital forensic readiness
- Digital forensic standards
- Digital forensic tools
2. Outcomes

Career

The aim of the course is to equip students with a broad knowledge of Digital Forensics. This will equip students for any ICT career where Digital forensics is used or developed on a continuous basis.

Course

During the course we will focus on the following outcomes subject to be modified at the discretion of the lecturer:

- Discuss the fundamental ideas of digital forensics and define digital forensics. Distinguish between the use of security and digital forensics. Summarise common digital forensic practices.
- Define digital forensics as a science using the Daubert case. Distinguish between forensic science and digital forensic science.
- Understand the digital forensic investigation process. Realise that the process needs to be followed rigorously due to legal implications worldwide.
- See how digital forensics are standardised into various international standards on ISO level.
- Explain how digital forensic readiness compliments digital forensics investigations and how it is similar to information security practices.
- Experience the application and development of digital forensic investigation software and hardware tools.

3. Plagiarism policy

The Department of Computer Science considers plagiarism as a serious offence. Disciplinary action will be taken against students who commit plagiarism. Plagiarism includes copying someone else's work without consent, copying a friend's work (even with consent) and copying material (such as text or program code) from the Internet.

Copying will not be tolerated in this course. For a formal definition of plagiarism, the student is referred to http://www.ais.up.ac.za/plagiarism/index.htm. (From the main page of the University of Pretoria site, follow the Library quick link, and then click the Plagiarism link). If you have any form of question regarding this, please ask one of the lecturers. Also note that the OOP principle of code re-use does not mean that you should copy and adapt code to suit your solution.

4. Study Material

You are advised to regularly monitor the COS783 website at http://www.cs.up.ac.za/courses/COS783 for any updates and new announcements. You should treat this website as part and parcel of this study guide.

Class attendance is vital to maintain a good academic record. Additional material may also be discussed during lectures, not found in the published study material.
Please ensure that you attend these forums so that you are aware of important announcements, additional discussions and material not covered in this study guide.

*Background book (not compulsory to buy)*

Title: The Basics of Digital Forensics: The Primer for Getting Started in Digital Forensics  
Author: John Sammons  
Publisher: Syngress

*Additional references*

During the course, lecturers may prescribe a number of articles. References will be given, and it is the students’ responsibility to ensure that they obtain a copy. Note that such material is examinable, unless stated otherwise.

*Software*

All of the software you are required to familiarise yourself with will be available on the course website or similar repositories. Some of the tools will be made available on ftp://ftp.cs.up.ac.za.

5. Assessment

The semester mark will be calculated from the following components:

*Theory*

– Background class tests: 30% of theory component  
– Semester test: 70% of theory component

*Practical and other assignments*

A number of assignments will be posted throughout the course; their marks will differ from assignment to assignment (based on the complexity of the assignment) and add up to 100 (or just above 100). The total earned for all submitted assignments will form the practical mark (considered as a percentage).

*Semester Mark*

The theory assessments will count 70% of the semester mark and the practical marks earned will count 30% of the semester mark.

*Final Mark*

The semester and examination marks will each count 50% of the final mark. A subminimum of 40% applies for both the semester and examination marks.
6. Absence from assessment

The Department of Computer Science has the following policy about being absent from any assessment. A valid sick note needs to be handed to one of the lecturers in person NO LATER THAN 3 (three) days to the hour after the assessment opportunity took place. If no such valid documentation has been provided within the three days, the student cannot be accommodated.

Note that, due to EBIT Faculty regulations, lecturers may not accept any sick letters or similar documentation for the absence from the exam. All such valid documentation needs to be handed in at Faculty Administration, Engineering Building 1, level 6.

7. Lecture schedule

There is one lecture per week on a Wednesday from 16:30-18:20, in IT 4-3.

<table>
<thead>
<tr>
<th>Week</th>
<th>Date</th>
<th>Topic</th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td>22/7</td>
<td>Introduction – Overview</td>
</tr>
<tr>
<td>2</td>
<td>29/7</td>
<td>The conventional digital forensic investigation process</td>
</tr>
<tr>
<td>3</td>
<td>5/8</td>
<td>Digital forensic readiness</td>
</tr>
<tr>
<td>4</td>
<td>12/8</td>
<td>The harmonised digital forensic investigation process</td>
</tr>
<tr>
<td>5</td>
<td>19/8</td>
<td>Digital forensic standardisation</td>
</tr>
<tr>
<td>6</td>
<td>26/8</td>
<td>DF Tools: Hardware tools</td>
</tr>
<tr>
<td>7</td>
<td>2/9</td>
<td>DF Tools: Software</td>
</tr>
<tr>
<td>8</td>
<td>9/9</td>
<td>Guest lecture: Dariel Solutions: Network Forensics</td>
</tr>
<tr>
<td>9</td>
<td>16/9</td>
<td>Semester Test</td>
</tr>
<tr>
<td>10</td>
<td>23/9</td>
<td>No lectures due to Spring Day</td>
</tr>
<tr>
<td>11</td>
<td>30/9</td>
<td>Setting up a DF lab</td>
</tr>
<tr>
<td>12</td>
<td>7/10</td>
<td>Recess – no lecture</td>
</tr>
<tr>
<td>13</td>
<td>14/10</td>
<td>Capita Selecta</td>
</tr>
<tr>
<td>14</td>
<td>21/10</td>
<td>Capita Selecta</td>
</tr>
<tr>
<td>15</td>
<td>28/10</td>
<td>Capita Selecta</td>
</tr>
<tr>
<td>16</td>
<td>4/11</td>
<td>Capita Selecta</td>
</tr>
<tr>
<td></td>
<td>TBA</td>
<td>Exam: 12:00-14:00 (tentative)</td>
</tr>
</tbody>
</table>