POLITIHØGSKOLEN

CURRICULUM

POSTGRADUATE EDUCATION FOR NORDIC COMPUTER FORENSIC INVESTIGATORS

Module 2D

Mobile Extraction and Artifacts

15 ECTS

Approved by the Police University College Board

5th of December 2018

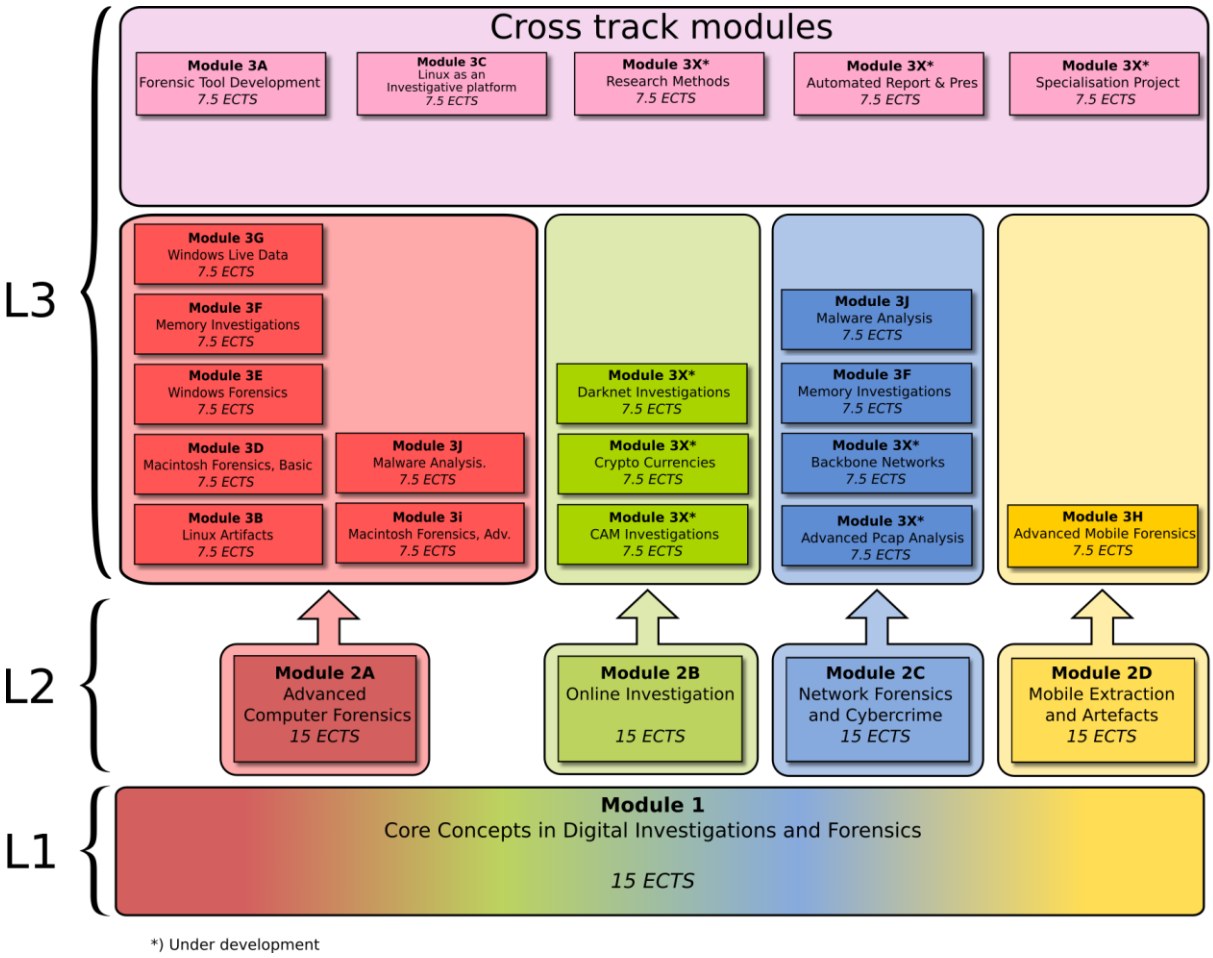
1. Introduction

Law enforcement's need for investigation of digital devices is constantly increasing. Traditionally this type of investigation was utilised in only a small number of cases, however, with the advent of the web and smart devices, such as the mobile phones, there is the potential for digital evidence in all cases. The analysis of digital devices is now more important than ever, because mobile phones are more used than the traditional computer. It is not sufficient however, for analysts to merely push a button to investigate digital evidence. The analyst must understand the processes by which the information is recovered and be able to explain these to the courts.

This course provides the students with the skills needed to process digital evidence from the most popular mobile phones, and to validate information found by automated tools.

The students will further get knowledge about how to acquire information from mobile phones, and skills to perform simple acquisitions of selected devices using backup solutions.

This module is part of the NCFI programme which consists of the following:



2. Aim

The aim of this program is to ensure that the quality of computer forensic investigation is of a high level, guaranteeing legal protection and the right to privacy.

3. Target group and admission criteria

3.1 Target group

The primary target group is police staff in the Nordic countries whose main task is handling and investigating digital evidence. It is a prerequisite that participants are selected in accordance with local competency plans.

Employees in other International police services or governmental agencies who work, or will work, with digital evidence are also eligible to apply.

3.2 Admission criteria

Applicants for module 2D must:

- possess Higher Education Entrance Qualification
- be employed by a national or local governmental agency
- have passed NCFI Module 1 Core Concepts in Digital Investigation and Forensics. The former NCFI Module 2 (25 ECTS) is also accepted

Foreign applicants are only entitled to apply if:

- the applicant's country has a partnership with PHS
- they have been selected in accordance with the partner's competency plans

Applicants who do not have the higher education entrance qualification have to provide:

- a minimum of 5 years work experience, of which maximum 2 years can be education, replace the requirements for Higher Education Entrance Qualification. This arrangement only applies to applicants over the age of 25

The prerequisite for having completed NCFI modules may be overridden if the applicant provides documentation for having completed equivalent education. To be considered as equivalent, the education must cover the following topic:

- computer forensic methodology

and in addition at least one of the following topics:

- digital forensics
- mobile forensics
- online investigations

The total workload of the education should be equivalent to approximately 15 ECTS.

4. Learning outcome

4.1 General competence

After completion of the module candidates will be able to:

- perform professional tasks in the role of investigator with increased insight and confidence

- see the role of investigation in a broader perspective during an investigation of mobile phones
- identify ethical and legal issues during investigation

4.2. Knowledge

After completion of the module candidates have knowledge about:

- The logical functioning of mobile phone file and operating systems
- The different types of mobile networks currently in use
- The present and future challenges of mobile phone digital forensics
- The different methods of acquisition
- Preservation and isolation of mobile phone devices
- External, internal and cloud sources for evidence from mobile phones
- The functionality of the most used Apps, including how and where they save data
- scientific principles that underlie digital evidence

4.3. Skills

After completion of the module candidates will be able to:

- handle, preserve and acquire selected mobile phone devices
- acquire from cloud sources used by mobile phones
- explain how the mobile phone file and operating systems function on a logical abstraction level
- perform an analysis of artefacts in mobile phone systems
- validate the results of automated tools and select tools that are most appropriate for the task in hand
- investigate and document each phase of a mobile phone investigation
- use open source tools as a platform for investigation
- apply a sound methodology in all analysis of mobile phones

5. Organization and Study Requirements

This module is delivered on-line as a part-time education, and the students are expected to complete the program within one semester. The approximate duration of the module is 420 hours of study.

The module comprises lectures, individual and group work, exercises, quizzes, assignments and literature study. Student support will be delivered via electronic means such as: email, discussion fora, chat and virtual classrooms. Certain mandatory live online lectures, no more than 7 days, will be conducted during the course.

The working methods of the study should help to provide students with good learning outcomes, and the emphasis is on flexible and diverse forms of work with a high degree of student activity. The program is organized around key issues and challenges in the investigation of electronic traces, which is illuminated with relevant theory.

An e-learning platform is used for the administration and implementation of the module.

Study requirements

The following requirements have to be approved before students may sit the exam:

- Automatically graded quizzes for each topic
- Three practical assignment
- A Case Study
- Attendance at mandatory lectures

6. Assessment

The module is concluded with a two-day take-home exam.

Students will be graded on a scale from A – F. A – E are passing grades and F is a failing grade.

7. Literature (900 pages)

7.1. Mandatory literature

Reiber, L. (2016): *Mobile Forensic Investigations*. USA: McGraw-Hill Education, ISBN-13: 978-0-07-184363-8. Chapter 1 (23 pages), chapter 3 (26 pages), chapter 4 (24 pages), chapter 6 from Tools available (8 pages), chapter 8 (44

pages), chapter 10 (48 pages), chapter 11 (50 pages), chapter 13 (40 pages), chapter 14 (22 pages). Total of 279 pages.

In addition to the listed mandatory literature, students need to read and use a number of specific web resources, lessons and academic research papers. These will also form part of the mandatory reading requirements and thus be examinable. Due to the rapid changes in the fields of digital forensics and cybercrime investigation, these need to be provided to students during the course of the study, to ensure they are up to date and based on current trends. The mandatory reading shall not exceed 900 pages.

7.2. Assumed knowledge

Literature from NCFI Module 1 Core concepts in Digital Investigation and Forensics (or similar educations).