CURRICULUM

POSTGRADUATE EDUCATION

FOR

NORDIC COMPUTER FORENSIC

INVESTIGATORS

Module 3i
Macintosh Forensics, Advanced

7,5 ECTS

Approved by the Police University College Board

5th of December 2018

1. Introduction

Law enforcement's need for digital forensics is constantly increasing. Traditionally digital forensics was utilised in only a small number of investigations, however, with the advent of the web and smart devices there is the potential for digital evidence in all cases.

The need for special investigative competence in Apple-based units has increased considerably the last years, and reports from computer investigators indicate that such units make up an ever-increasing proportion of seizures. These are units with particular features and technology requiring special competence to handle.

This course provides the students with the advanced skills needed to document and develop a forensically sound tool utilising current best practice.

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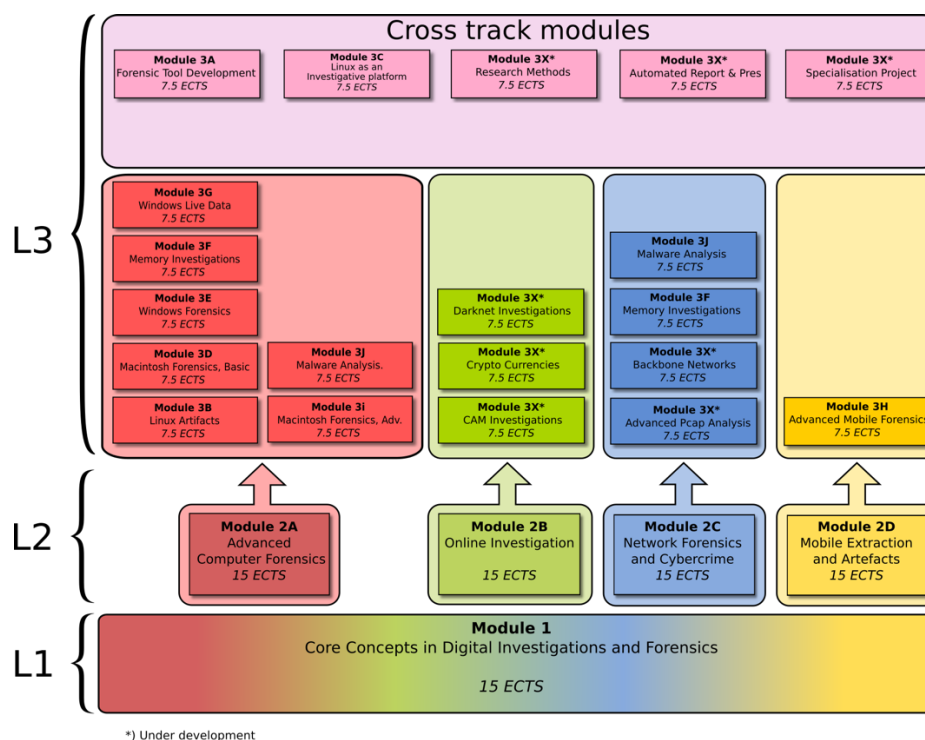
2. Aim

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 3i must:

- be employed by a national or local governmental agency
- have passed NCFI Module 3D Macintosh Forensics, Basic

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

4.   Learning outcome

4.1   General competence

After completion of the module candidates will be able to:

- perform professional tasks in the role of digital forensic investigator with increased insight and confidence
- see the role of digital forensics in a broader perspective during an investigation
- identify ethical and legal issues during investigation

4.2.   Knowledge

After completion of the module candidates will have knowledge of:

- recognising more advanced and complex traces in macOS and iOS architecture
- describing and identifying structures in file systems used by macOS and iOS

4.3.   Skills

After completion of the module candidates will be able to:

- use software tools to perform Live Data Forensics according to basic principles and best practice
- interpret various advanced artefacts in macOS and iOS
- use of the command line interface in macOS to solve investigational challenges
- interpret advanced artefacts in Apple file systems

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 210 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 4 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 selected topics
- two individual assignments related to defined topics
- attendance at mandatory lectures

6.   Assessment

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

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

7.   Literature (450 pages)

The students will include an individual literature research on macOS and iOS Forensics, and the selected literature will be examinable.

In addition to the mandatory literature research, 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 450 pages.

7.2.   Assumed knowledge

Literature from NCFI Module 1 Core Concepts in Digital Investigation, NCFI Module 2A Advanced Computer Forensics and NCFI Module 3D Macintosh Forensics, Basic (or similar educations).