



POLITI HØGSKOLEN

CURRICULUM

POSTGRADUATE EDUCATION FOR NORDIC COMPUTER FORENSIC INVESTIGATORS

Module 3E: Windows Forensics

7,5 ECTS

**Approved by the Police University College Board
5th of December 2018**

1. Introduction

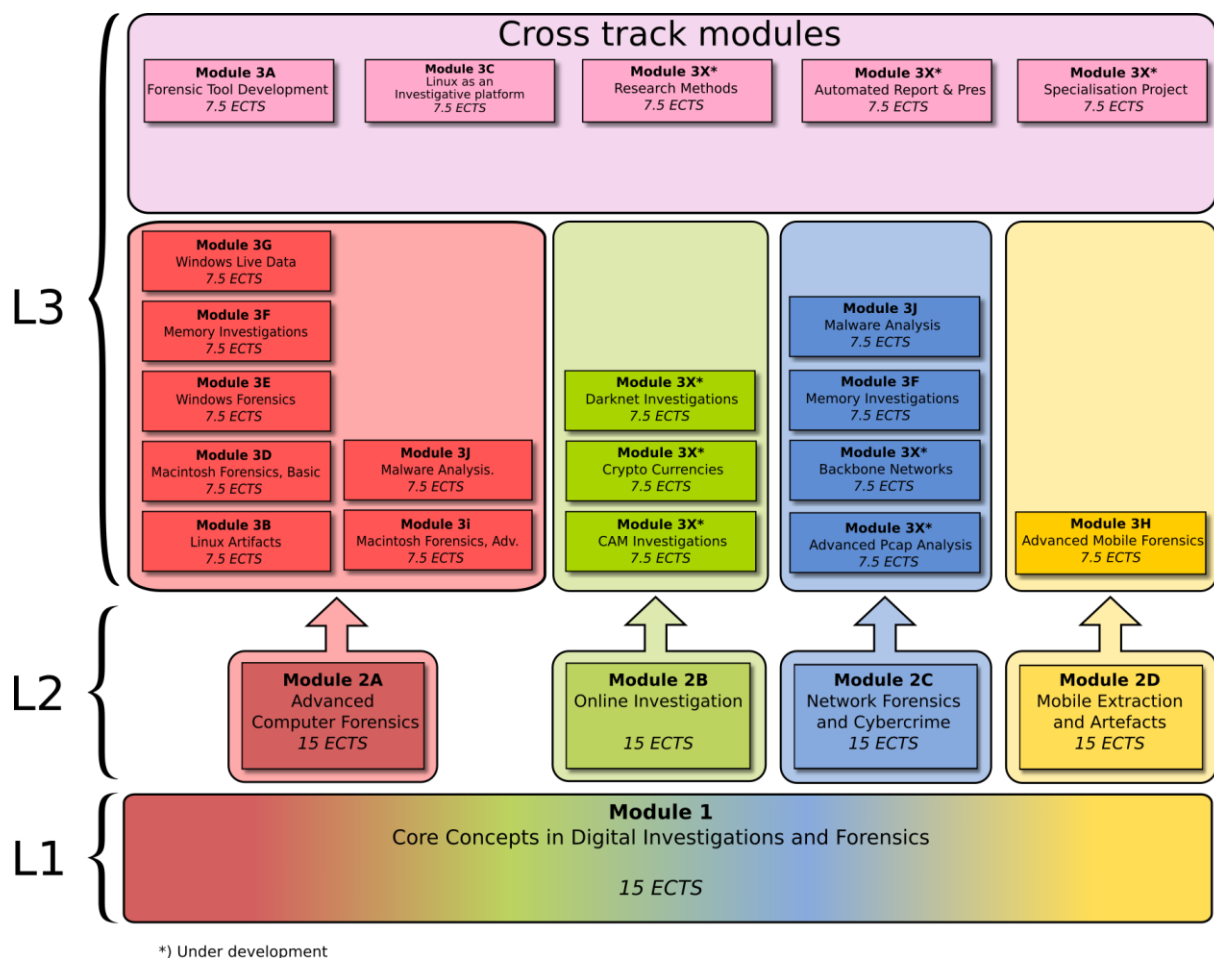
Law enforcement's need for digital forensics is constantly increasing. Traditionally digital forensics was utilised in only a small number of investigations, however, with the advent of the web and smart devices there is the potential for digital evidence in all cases.

Personal computing has for years been dominated by Windows operating system (OS). Most personal computers have Windows operating system (OS) installed, and Windows is embedded as OS on small-scaled devices like smart phones and tablets.

The analysis of digital devices is now more important than ever. It is not sufficient however, for analysts to merely push a button to discover to process 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 not only process digital evidence but to explain both how the information was created and also how the forensic tools recovered that information.

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 3E must:

- possess higher Education Entrance Qualification
- be employed by a national or local governmental agency
- have passed NCFI Module 2A Advanced Computer Forensics. The former NCFI Module 2 (25 ECTS) is also accepted
- have at least one year's experience in digital forensics or cybercrime investigation

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

The prerequisite of having completed NCFI modules may be overridden if the applicant can:

- either provide documentation for having completed equivalent education
- or demonstrate qualifying skills and knowledge necessary to follow the module

To be considered as equivalent education or qualifying experience, the following topic must be documented:

- computer forensic methodology

and in addition document education or experience in at least one of the following topics:

- network forensics
- cybercrime
- mobile forensics

The total workload of the education should be equivalent to approximately 30 ECTS. For they who are applying on the basis of their experience, a relevant test will be provided in order to demonstrate necessary skills and knowledge.

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 advanced knowledge about:

- The functioning of windows file and operating systems
- The location of different artefacts within Windows

4.3. Skills

After completion of the module candidates will be able to:

- Utilise the use of open source forensic tools in Windows
- Explain how the file and operating systems function
- Analyse in-depth Windows Systems (File Systems; Operating Systems and Recovered Artefacts) and utilise the findings in an investigation
- Evaluate the relevance of Windows artefacts in relation to an investigation

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 practical assignments
- Attendance at mandatory lectures

6. Assessment

The module is concluded with a 6 hours 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

7.1. Mandatory literature

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 450 pages.

7.2. *Assumed knowledge*

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