



POLITIHØGSKOLEN

CURRICULUM

POSTGRADUATE EDUCATION

In

**NORDIC COMPUTER FORENSIC
INVESTIGATORS**

MODULE 2A: COMPUTER FORENSICS

15 credits

**Approved by the Police University College Board 6th of
December 2017. Changes approved by the head of department
30th November 2023**

1. Introduction and purpose

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 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 how the forensic tools recovered that information.

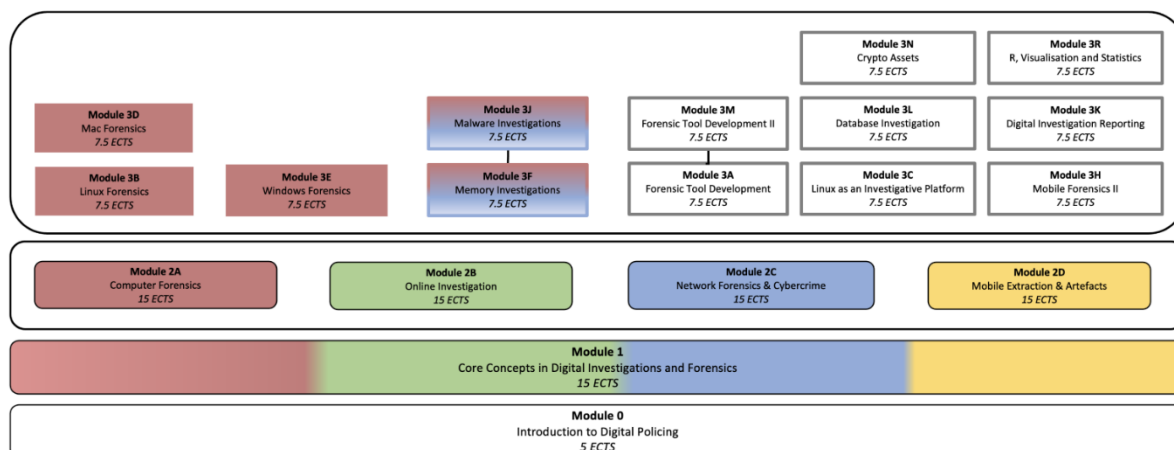
The postgraduate study programme shall contribute to police practitioners being better able to perform investigative and analysis tasks involving digital devices, and thus contribute to the quality and development of digital investigation and forensics.

2. When applicable: Educational pathways and formal approval

2.1. Education

The education gives 15 credits and is included as a course in an educational portfolio (the 'NCFI Portfolio') according to the following model depicted below.

Admission requirements, content and organisation of the individual courses are described in more detail in the study plan for each course.



3. Target group and admission requirements

3.1. Target group

The primary target group for this education is police staff in the Nordic countries whose main task is, or will be, handling and investigating digital evidence.

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

Applicants must be recommended by the employer.

3.2. Admission Requirements

Applicants must document the following requirements:

Education:

- Higher Education Entrance Qualification
- M1 Core Concepts in Digital Investigation & Forensics, 15 ECTS

Employment, work experience and additional requirements:

- Current employment in a government agency (e.g., law enforcement agency or other cooperating governmental agencies/organisations)

Applicants who do not satisfy the requirement for higher education entrance qualification must document the following:

- A minimum of 5 years of relevant work experience (of which up to 2 years may be relevant education).
- Meet the English proficiency requirements.

The scheme only applies to applicants who are over 25 years of age.

4. Learning outcomes

4.1. General Competence

After completing the module, students can:

- perform professional and research tasks in digital policing
- see the role of digital policing in a broader perspective during an investigation

4.2. Knowledge

After completing the module, students have knowledge of:

- Windows file and operating systems
- locations of various forensic artefacts
- disk partitioning schemes
- challenges of digital forensics
- validation of forensic tools

4.3. Skills

After completing the module, students will be able to:

- manually interpret various partitioning schemes
- analyse Windows file systems
- analyse various Windows artefacts
- apply relevant methodologies in all forensic analysis tasks
- automate simple forensic tasks
- communicate technical findings

5. Organisation of teaching and learning activities

The education is organised as an online part-time programme and must be completed within 5 months. The scope of further education is estimated to be approx. 420 hours of study.

This education includes a single week campus held online using appropriate video conferencing tools. The campus amounts to approximately 40 hours of study. Attendance is mandatory, and there is a requirement of 100% participation at this gathering.

Teaching and learning activities shall contribute to providing students with good learning outcomes, and emphasis is placed on flexible and diverse working methods with a high degree of student activity. Furthermore, the study is organised around key issues and challenges in the investigation of electronic traces, which are illuminated with relevant theory.

The teaching and learning activities include lectures, presentations, individual and group work, practical exercises, cases, quizzes, assignments, and literature study. Student support will be delivered via electronic means such as: email, discussion fora, chat, and virtual classrooms. Teaching and learning activities also include optional live online lectures throughout the semester (totalling no more than 16 hours).

An online learning platform is used in the administration and pedagogical implementation of the programme.

Coursework requirements

The following requirements must be approved before the students can take the exam:

- Successful completion of up to 10 automatically graded online quizzes. (Students may have multiple attempts at these tests, if necessary.)
- Two assignments
- Campus participation

Guidance will be given related to the coursework requirements.

6. Assessment

Students are assessed along the way through coursework requirements and receive feedback on these according to specified criteria based on the descriptions of learning outcomes.

The module is concluded with an individual take-home exam over 6 hours.

The exam **must** be passed in order to successfully complete the module.

Letter grades are used on a scale from A to F, where A is the highest passing grade, E is the lowest passing grade and F is a failing grade.

7. Literature

7.1. Syllabus

Students will be expected to read several web resources, lessons, reports, and academic research papers. These will 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, such resources must be provided to students during the study. This will ensure that the reference materials are up to date and based on current trends.

The mandatory reading shall not exceed 975 pages.

7.2. Assumed Knowledge

Literature from The Norwegian Police University College's NCFI M1 Core Concepts in Digital Investigation and Forensics of 15 ECTS.