POLITIHØGSKOLEN

CURRICULUM

POSTGRADUATE EDUCATION

In

NORDIC COMPUTER FORENSIC INVESTIGATORS

MODULE 1: CORE CONCEPTS IN DIGITAL INVESTIGATION & 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

Digital evidence is no longer only of importance in cybercrime investigation, nowadays the prevalence of technology in society has meant that there is digital evidence in almost all crimes. Society exists in a technical and connected world and as a result the amount of digital evidence has increased substantially. In addition, the type of digital evidence has changed over the years, no longer is it the physical hard drive that we are most interested in. Often it is the smart device, or the online presence that is required. The acquisition and interpretation of these require additional skills to that of traditional forensics.

In the past only a small number of police required training in this area, however, this has changed dramatically. It is now essential that more police officers are trained in the areas of Online Investigation, First Response, and Digital Forensics etc., in order to improve the efficiency of investigation. This module will introduce students to these fields and prepare them for further studies in specialist areas in the future.

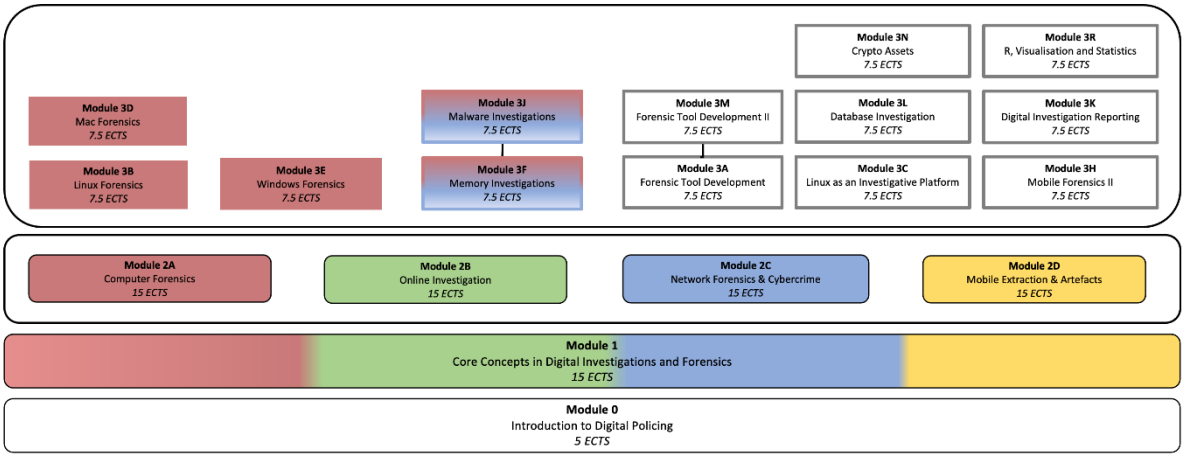
The postgraduate study programme shall contribute to police practitioners being better able to perform investigative and analysis tasks involving digital devices, and thus contribute to the quality and development of digital investigation and forensics.

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

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:

- digital forensic methodologies and their application
- computer and network components
- cybercrime and anti-forensics
- the ACPO Principles of digital evidence
- the benefits of open source software in investigation

4.3. Skills

After completing the module, students will be able to:

- interpret information stored in a digital system
- use Linux as a digital investigative platform
- conduct online investigations
- use digital forensic tools to analyse file systems
- apply the digital forensic methodology in all forensic analysis tasks
- report 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 participation in up to five days of mandatory lectures. This amounts to approximately 40 hours of study. 100% participation is required at these events.

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.

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 quizzes. (Students may have multiple attempts at these tests, if necessary.)
- Two assignments
- Participation in up to five days of mandatory lectures

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 a two-part exam:

- an individual practical take-home exam over 6 hours
- an individual theoretical take-home exam over 6 hours

Both parts of the exam **must** be passed in order to successfully complete the module.

Students will be graded on a Pass / Fail scale.

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

No assumed knowledge. Please refer to the admission criteria.