POLITIHØGSKOLEN

CURRICULUM

POSTGRADUATE EDUCATION

In

NORDIC COMPUTER FORENSIC INVESTIGATORS

MODULE 0: INTRODUCTION TO DIGITAL INVESTIGATION AND POLICING

5 credits

Approved by the Police University College Board 5th of December 2018. Changes approved by the head of department 12th of August 2022 and 30th November 2023

1. Introduction and purpose

Law enforcement's need for an understanding of digital concepts is constantly increasing. Whether it is as proactive measures, for criminal intelligence or as a part of an investigation, the utilisation of digital policing is important to strengthen the capacity of police services around Europe. Traditionally, the digital traces were utilised only in a small number of investigations, however, with the advent of the web and smart devices, there is a potential for digital evidence in all cases. There are several ways to build the capacity, but the most important one will be to increase the skills and knowledge to personnel not traditionally dealing with digital evidence on daily basis. This course will provide the understanding of modern digital concepts. Furthermore, the students will learn how to support investigations by a basic understanding of methods and new technologies.

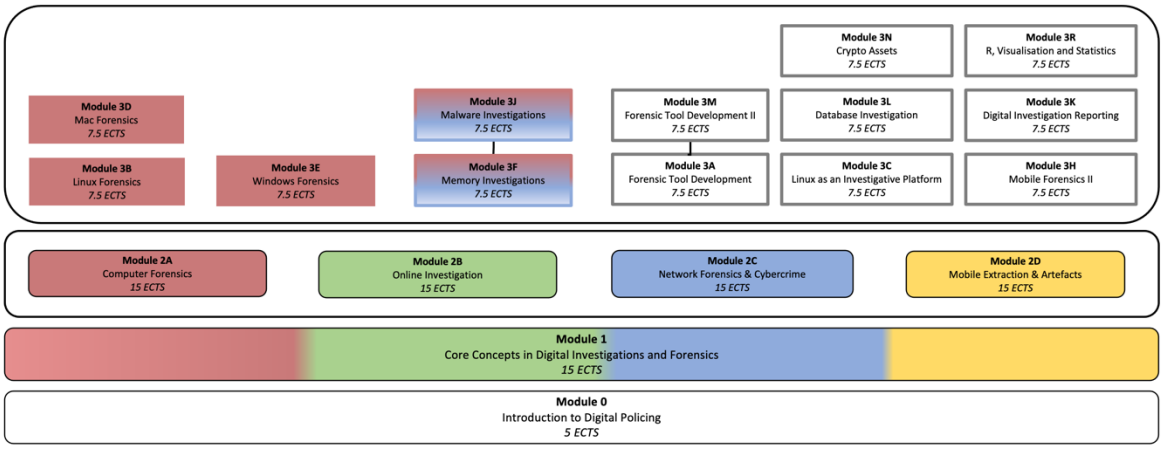
The postgraduate study programme shall contribute to police practitioners being better able to perform investigative and analysis tasks involving digital devices, and thus contribute to the quality and development of digital investigation and forensics.

2. When applicable: Educational pathways and formal approval

2.1. Education

The education gives 5 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.

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:

- computer and mobile terms and technology
- Internet and network technology
- digital evidence workflow
- digital criminal phenomena and trends
- relevant legal framework and ethics
- safety and security
- digital sources for evidence

4.3. Skills

After completing the module students will be able to:

- build necessary documentation to support investigations
- identify sources for digital evidence
- first responder skills - seizing items containing digital evidence
- acquisition of information from open sources on the Internet
- assess the need for special competence and bring this into operation

5. Organisation of teaching and learning activities

The course consists of web-based learning and totals approximately 140 hours. This includes assignments and individual studies. The study methods are intended to provide students with good learning outcomes and will illustrate in particular the connection between theory and practice. Emphasis is placed on varying methods of study to include a large element of student

participation. A learning platform is used for the administrative and pedagogical implementation of the course.

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 automatically graded quizzes for selected topics. (Students may have multiple attempts at these tests, if necessary.)

6. Assessment

The examination consists of a final individual digital test.

Students will be graded on a Pass / Fail scale.

7. Literature

7.1. Syllabus

Online material presented in the course.

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 300 pages.

7.2. Assumed Knowledge

No assumed knowledge. Please refer to the admission criteria.