POLITIHØGSKOLEN

CURRICULUM

POSTGRADUATE EDUCATION

In

NORDIC COMPUTER FORENSIC INVESTIGATORS

MODULE 3J: MALWARE INVESTIGATION

7.5 credits

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

1. Introduction and purpose

The activities where an attacker intends to steal or compromise information are increasing, often with an economic motivation. To accomplish such threats, the attacker may use attacking mechanisms such as electronic viruses, worms, spyware, backdoors, rootkits, sniffers, or other tools to gain access or compromise the digital infrastructure. This involves information stored at the end user, on servers, in the cloud or data in transport between such. To detect such threats, the forensic investigator must perform deep analysis of the victim's infrastructure to detect such attacks have been performed and evaluate the attack behaviour and the resulting damage. The investigator must possess extensive skills to detect the presence of such threats, the behaviour of these and potentially be able to identify the attacker, either an organisation or individual. This study aims to provide practitioners with the required knowledge and skill for preforming malware investigations.

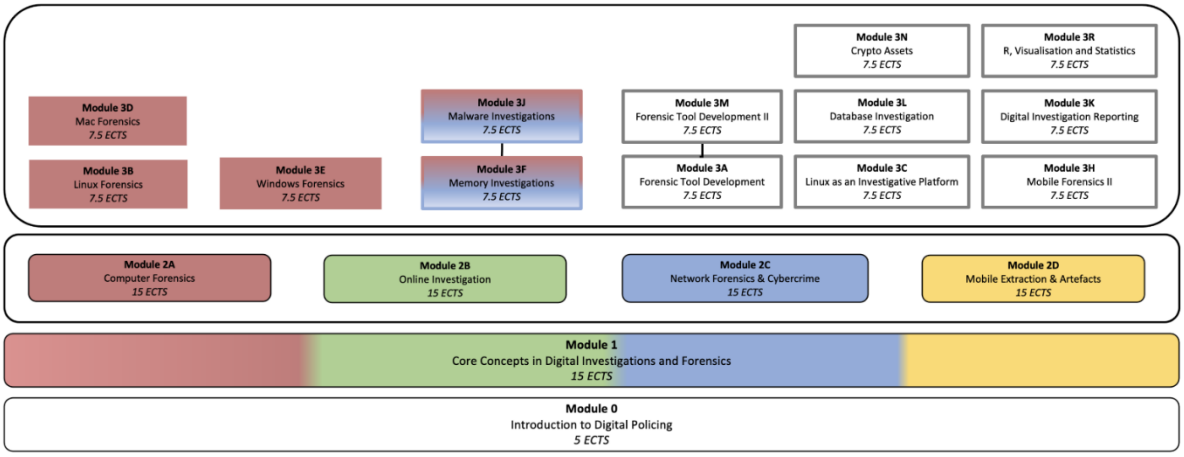
The postgraduate study programme shall contribute to police practitioners being better able to perform investigative and analysis tasks involving digital devices, and thus contribute to the quality and development of digital investigation and forensics.

2. When applicable: Educational pathways and formal approval

2.1. Education

The education gives 7.5 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.

Applicants must be recommended by the employer.

3.2. Admission Requirements

Applicants must document the following requirements:

Education:

- Bachelor's degree
- have passed M3F Memory Investigations

Applicants who do not satisfy the requirement for a bachelor's degree must document the following:

- Passed and completed 2-year education at a higher level than upper secondary school, and in addition either:
  - Minimum 60 ECTS

    - (of which NCFI Core Concepts of 15 ECTS and any NCFI M2X of 15 ECTS each. The former NCFI Module 1 (5 ECTS) and former NCFI Module 2 (25 ECTS) are also accepted.), or
- 1680 hours of continuing education courses, or
- 5 years of practice

Employment, work experience and additional requirements:

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

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:

- different types and categories of malware and their functionality
- various malware artefacts
- potential impact of malware and intentions of the attacker

4.3. Skills

After completing the module, students will be able to:

- design a malware analysis environment
- use software to detect, analyse and interpret malware from multiple data sources
- apply basic reverse engineering and tracing techniques to link malware to organisation(s) or person(s)
- communicate technical findings related to malware investigation

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. 210 hours of study.

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. The teaching and learning activities also include optional live online lectures throughout the semester (totalling no more than 8 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

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 4 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 450 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, **and** one relevant NCFI M2X module of 15 ECTS, **and** M3F Memory Investigation of 7.5 ECTS (or similar education).