POLITIHØGSKOLEN

CURRICULUM

POSTGRADUATE EDUCATION

In

NORDIC COMPUTER FORENSIC INVESTIGATORS

MODULE 3L: DATABASE INVESTIGATION AND DATA MINING

7.5 credits

Approved by the Education Committee 12th May 2023
Changes approved by the head of department
30th November 2023

1. Introduction and purpose

The proliferation of digital information in society has had a direct influence on the amount of data being processed and analysed during investigations. To strengthen the rule of law, investigations must be conducted using the highest quality standards. Investigations must be efficient and utilise techniques which support the valid interpretation of evidence.

Today, the vast majority of people have multiple digital devices on their person at all times. All of these digital devices contain databases, with many of these databases being excellent sources of potential evidence. All major operating systems utilise database technology to store information from many different electronic sources. It is estimated (source: https://www.sqlite.org) that there are over 1 trillion SQLite databases in use in the world. These are found on computers and laptops, tablets and phones, smart devices (tvs, watches, etc), IoT devices, vehicles, etc. Additionally, many organisations run enterprise level database management systems which contain employee / customer details and can be a tempting target for cybercriminals.

Recent years have also seen the growth of Big Data, large, diverse sets of information from a variety of sources that grow at ever-increasing rates, and contain structured, semi-structured and unstructured data. Many of these data sources are available to law enforcement (LE) (e.g. social media content, internal case management systems, etc). In order to analyse these big data resources, the most successful techniques to date have been in the area of data mining, an automated analysis approach based on the principles of artificial intelligence. Going forward, the volume of data will continue to grow. Already the data quantity to be analysed is straining many digital investigation units. Without adopting modern techniques for the analysis of this data there is a risk that much will be lost. The introduction of techniques in data mining will help to overcome this problem.

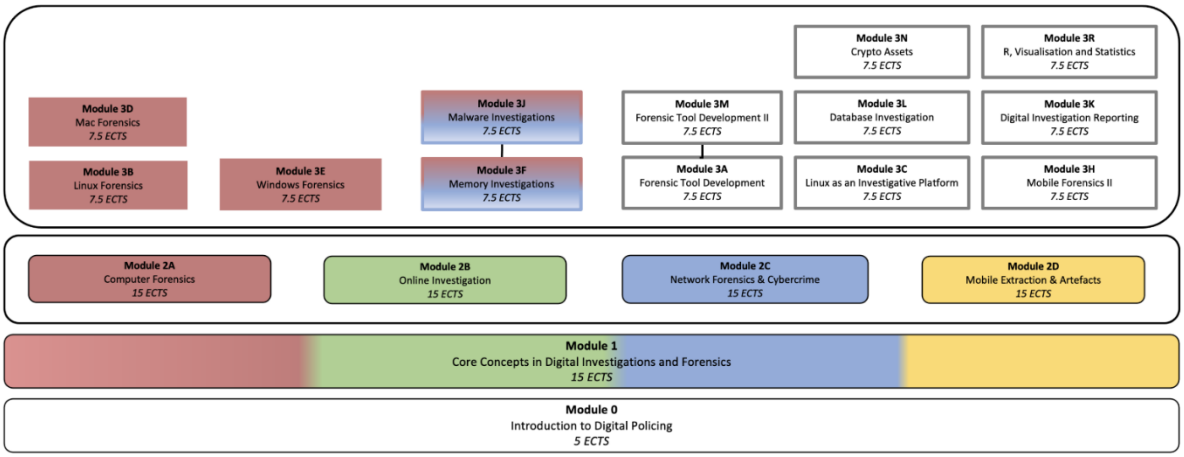
The postgraduate study programme shall contribute to police practitioners being better able to perform investigative and analysis tasks involving digital devices, and thus contribute to the quality and development of digital investigation and forensics.

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 at least one NCFI M2X module.[1]

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)

[1] The former NCFI Module 2 (25 ECTS) is also accepted.

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:

- general database concepts and their ubiquity and particular relevance to investigation
- how data mining algorithms function
- applications of data mining to investigation

4.3. Skills

After completing the module, students will be able to:

- design and query relational databases
- analyse previously unseen database schemas and evaluate recovered data
- recover data from damaged / corrupt databases
- use data mining tools in 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 examined on all material published in the lessons, and a number of specific web resources and research articles which are provided to students during the course. These form part of the mandatory reading requirements and will be examinable.

The recommended text for the course is:

> Sanderson, P. (2018) SQLite Forensics, ISBN: 9-781-980-293-071 [Chapters 1, 2, 3, & 5 – 130 pages]

Research papers related to the topic will be provided during the course. These will form part of the mandatory reading also.

Students may also wish to refer to the following web resources:

- DBMS Tutorial: https://www.tutorialspoint.com/dbms/index.htm
- SQL Tutorial: https://www.tutorialspoint.com/sql/index.htm

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** at least one NCFI M2X module of 15 ECTS (or similar education).