POLITIHØGSKOLEN

CURRICULUM

POSTGRADUATE EDUCATION
FOR
NORDIC COMPUTER FORENSIC INVESTIGATORS

Module 3K
Report Generation
&
Visualisation

7.5 ECTS

Approved by the Police University College Educational Committee
22th of November 2019

1. Introduction

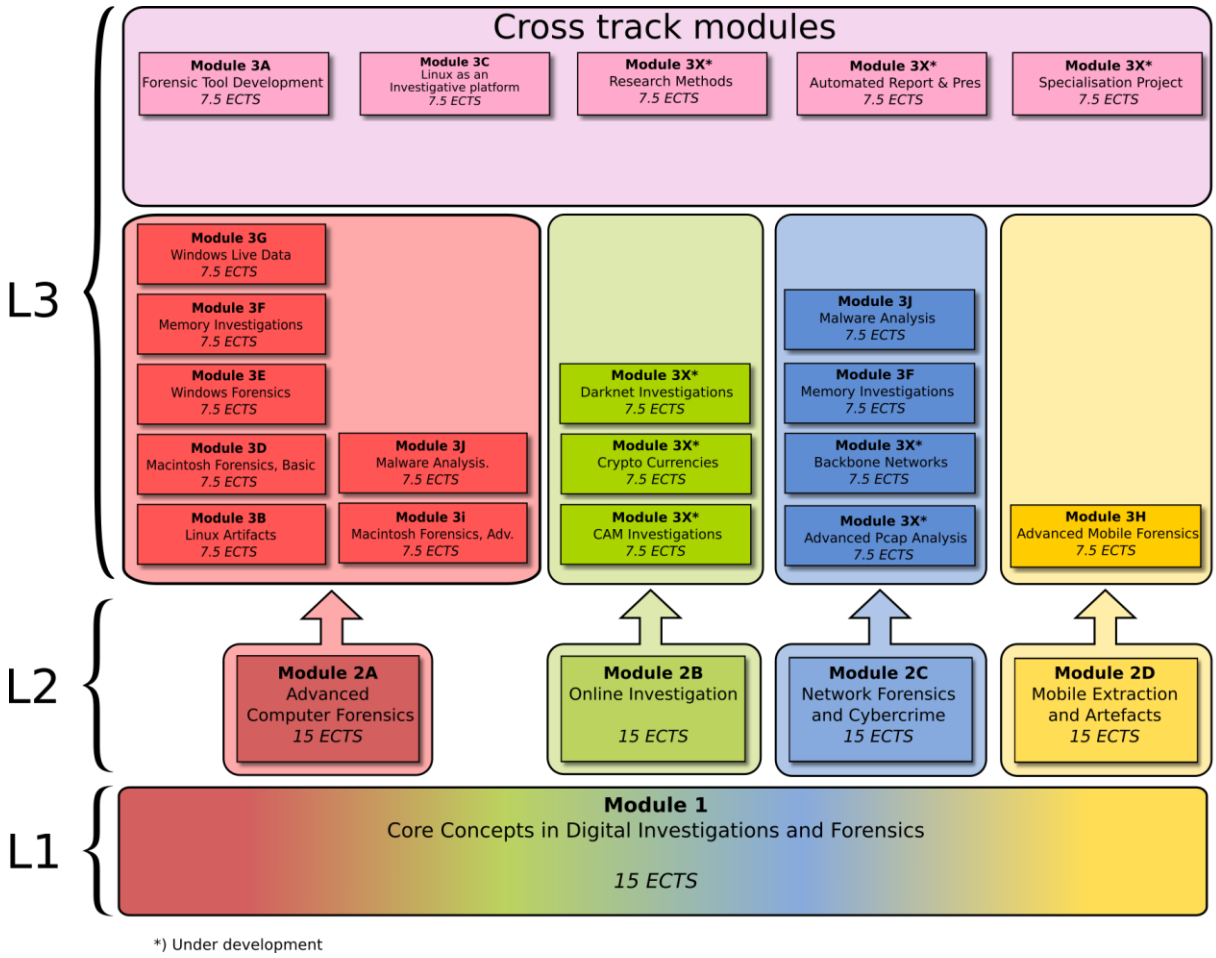
The proliferation of digital information in society has a direct influence on the amount of data being processed and analysed during investigations. The sheer volume of exhibits and range of data stored on devices has also led to challenges seen of working practices. Investigators who have an in-depth understanding of digital forensic methodology, can advantageously strengthen their workflow by applying techniques for automation and software generated reports to present findings.

To strengthen the rule of law, investigations must be carried out in a manner of high quality, efficiency and by the means of techniques, which support interpretation of evidence. Data analysis, presentation and reporting are crucial components of digital investigations; the use of automation and generated reports along with the ability to present findings in the most appropriate way might have influence on case outcomes.

For this reason, it is important to develop skills that can be used to provide good quality, a standardised view and approach which not only strives for an absolute minimum quality in reports but also facilitates cross-party exchange (e.g., court, victim, internal and external partners) and readability of information.

While challenges are likely to continue for a range of investigators. By providing education in the use of automation and visualisation, the law enforcement officers are better placed to report and present digital findings. This module is designed to help investigators gain both knowledge and skills which can be used to help automate investigative processes including the delivery of reporting mechanisms which may help emphasise important findings and support the presentation, delivery and interpretation of evidence.

This module is part of the NCFI programme, which consists of the following:



*) Under development

2. Aim

The aim of this programme is to ensure that the quality of digital forensic investigation is of a high level, guaranteeing legal protection and the right to privacy.

3. Target group and admission criteria

3.1 Target group

The primary target group is police staff in the Nordic countries whose main task is handling and investigating digital evidence. It is a prerequisite that participants are selected in accordance with local competency plans.

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

3.2 Admission criteria

Applicants for module 3K must:

- possess higher Education Entrance Qualification
- be employed by a national or local governmental agency
- have passed either NCFI Module 2A Advanced Computer Forensics, NCFI Module 2B Online Investigation, NCFI Module 2C Network Forensics & Cybercrime or NCFI Module 2D Mobile Extraction & Artefacts. The former NCFI Module 2 (25 ECTS) is also accepted
- have at least one year's experience in digital forensics or cybercrime investigation.

International applicants are only entitled to apply if:

- the applicant's country has a partnership agreement with PHS
- they have been selected in accordance with the partner's competency plans

Applicants who do not have the higher education entrance qualification have to provide:

- a minimum of 5 years' work experience, of which a maximum of 2 years can be education, replace the requirements for Higher Education Entrance Qualification. This arrangement only applies to applicants over the age of 25

The prerequisite of having completed NCFI modules may be overridden if the applicant can:

- either provide documentation for having completed equivalent education
- or demonstrate qualifying skills and knowledge necessary to follow the module

To be considered as equivalent education or qualifying experience, the following topic must be documented:

- digital forensic methodology

and in addition, document education or experience in at least one of the following topics:

- computer forensics
- network forensics
- cybercrime
- mobile forensics

The total workload of the education should be equivalent to approximately 30 ECTS. For those who apply based on their experience, a relevant test will be provided in order to demonstrate the necessary skills and knowledge.

4. Learning outcomes

4.1 General competence

After completion of the module candidates will be able to:

- perform professional tasks in the role of digital forensic investigator with increased insight and confidence
- see the role of digital forensics in a broader perspective during an investigation

- identify ethical and legal issues during investigation

4.2 Knowledge

After completion of the module candidates will have knowledge of:

- the basic theory in data analysis
- the different frameworks for visualisation of data
- the automation of data extraction during analysis
- the importance and identification of satisfactory criteria needed for a report
- reporting of findings meeting satisfactory requirements and key values of a good report (e.g. develop and create standardised approaches and documents, and demonstrate good court presenting techniques)

4.3 Skills

After completion of the module candidates will be able to:

- analyse findings with a statistical approach
- find creative solutions for automation of data extraction and visualisation
- use frameworks for dynamic representation of data
- demonstrate in-depth understanding of typesetting frameworks
- recognise the benefit of, and create a standardised approach to documentation to facilitate exchange of information with other parties
- create and present findings in a suitable and court friendly matter

5. Organisation and Study Requirements

This module is delivered on-line as a part-time education, and the students are expected to complete the program within one semester. The expected duration of the module is 210 hours of study.

The module comprises of online learning materials, individual work, exercises, quizzes, assignments and literature. Student support will be delivered via electronic means such as: email, discussion fora, chat or virtual classrooms.

The working methods of the study should help to provide students with good learning outcomes, and the emphasis is on flexible and diverse forms of work with a high

degree of student activity. The programme is organised around key issues and challenges in the investigation of electronic traces, which is illuminated with relevant theory.

An e-learning platform is used for the administration and implementation of the module.

Study requirements

The following individual working requirements must be approved before students may sit the exam:

- Successful completion of automatically graded quizzes. Students may have multiple attempts at these tests if necessary.
- Two practical assignments

6. Assessment

The module is concluded with an 8 hours practical take-home exam.

Grading is on a scale of A – F (in which A – E are passing grades and F is a fail).

7. Literature (shall not exceed 525 pages)

7.1. Mandatory literature

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.

Venables, W. N., Smith, D. M (2019): An Introduction to R: Notes on R: A programming Environment for Data Analysis and Graphics, Version 2.6.3, Chapters 1-7,9,12-14 (52 pages), https://cran.r-project.org/doc/manuals/r-release/R-intro.pdf

LaTeX. en.wikibooks.org. Chapters 1-21,44,46 and 47 (310 pages), https://upload.wikimedia.org/wikipedia/commons/2/2d/LaTeX.pdf.

Thomas, S. (2015): Data Visualization with JavaScript. USA: No Starch Press, ISBN-13: 978-1-59327-605-8. Chapters 1,3,5-6 (161 pages), http://www.softouch.on.ca/kb/data/Data%20Visualization%20with%20JavaScript%20(2015).pdf

In addition, students may wish to refer to the following:

These are to be added

7.2. Assumed knowledge

Literature from NCFI Module 1 Core concepts in Digital Investigation and Forensics and one of NCFI Module 2A Advanced Computer Forensics, NCFI Module 2B Network Forensics and Cybercrime, NCFI Module 2C Online Investigation or NCFI Module 2D Mobile Extraction and Artefacts (or similar educations).