POLITIHØGSKOLEN

# CURRICULUM

# POSTGRADUATE EDUCATION FOR NORDIC COMPUTER FORENSIC INVESTIGATORS

## Module 3C

## Linux as an Investigative Platform

### 7.5 ECTS

**Approved by the Police University College Board**

**5th of December 2018**

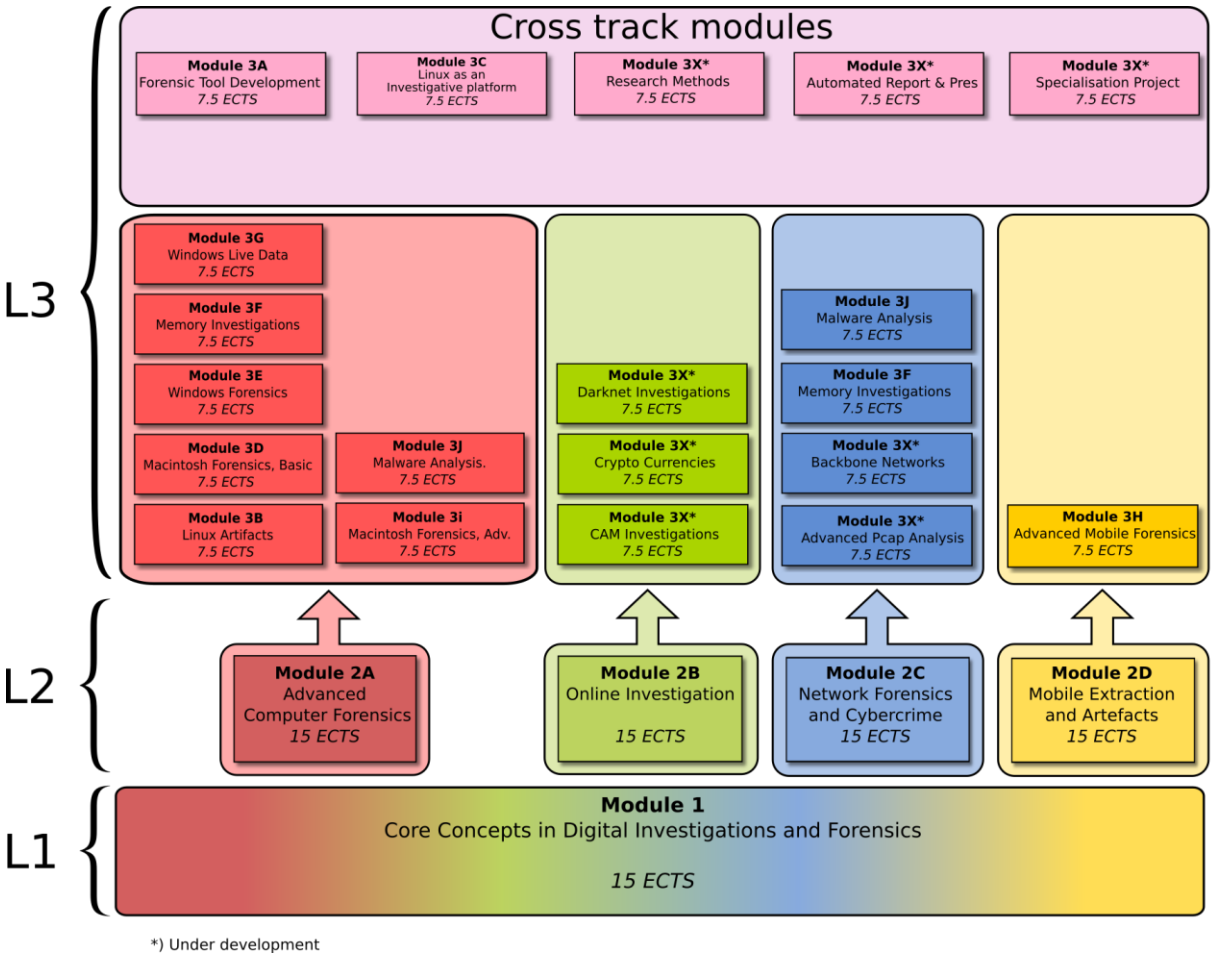
# 1. Introduction

The number of investigations involving computer technology has grown significantly in recent years. This applies to both new forms of crime and also traditional crime that is now being committed using new technology. Typical examples are the use of digital media and communication equipment in human and drug trafficking, sexual offenses, and economic crime.

Increasing use of information technology has given rise to new challenges in terms of legislation and policing methods. For this reason it is important to develop skills that can provide an understanding of information and communication technologies, and their relationship to police tactics. The Nordic Computer Forensics Investigators programme will contribute to this.

Investigators have traditionally used tools from commercial software vendors usually running on the Windows Operating System. The software from these is proprietary and gives little or no opportunity for access to the behaviour of the programs. From a legal perspective, this may be problematic. Moreover, these tools are large and complex, and often only have a limited degree of possible adaptation. By providing education in the use of Linux and open source software, the police are better placed to verify that the current software functions as intended and are comfortable with tools other than those provided commercially.

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




## 2. Aim

The purpose of this study is to allow investigation of electronic traces using open source tools and to ensure the investigation is performed in a way that safeguards the rule of law and personal 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 3C must:

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

Foreign applicants are only entitled to apply if:

- the applicant's country has a partnership 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 maximum 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:

  - computer forensic methodology

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

  - network forensics
  - cybercrime
  - mobile forensics

The total workload of the education should be equivalent to approximately 30 ECTS. For they who are applying on the basis of their experience, a relevant test will be provided in order to demonstrate 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 completing the course candidates will have knowledge of:

- the importance of open source tools in investigation
- new methods and techniques for use in investigation
- the automation of forensic techniques
- the value of adapting tools for specific challenges
- legal and ethical issues

## 4.3. Skills

After completion of the module candidates will be able to:

- utilise the potential of open source tools
- evaluate tools for customisation to different situations
- develop scripts / tools for use in investigation
- understand and customise other developers' scripts
- evaluate the performance of both proprietary and open source tools

# 5. Organisation and Study Requirements

This course will be delivered on-line through a combination of lectures, exercises, quizzes and assignments.

The approximate duration of the module is 210 hours. Students may choose to study at their own pace. However, it is expected that the course is completed within a single semester.
During this course students will build a Linux-based forensic workstation. This will be created as a virtual machine. As such the student must install virtualisation software and then build the workstation throughout the course. Students will be guided through compulsory steps during this process. This work forms part of the final assessment.

Student support will be delivered via electronic means such as: email, discussion fora, chat and virtual classrooms.

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

### *Study requirements*

The following individual course requirements must be met and approved before students are allowed to attend the examination:

- Completion of one scripting assignment

## 6. Assessment

The study concludes with an exam consisting of two parts:

- an individual take-home examination over 4 hours
- assessment of the student's workstation configuration

Grading is from A – E, which are passing grades, and F, which is a failing grade. Both parts of the examination must be passed. Each part of the assessment has equal weight.

# 7. Literature

## 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 (both technical and legal) which are provided to students during the course. These form part of the mandatory reading requirements and will be examinable.

The mandatory reading shall not exceed 450 pages.

## 7.2. Assumed knowledge

Literature from NCFI Module 1 Core concepts in Digital Investigation and NCFI Module 2A Advanced Computer Forensics (or similar educations).