POLITIHØGSKOLEN

CURRICULUM

POSTGRADUATE EDUCATION FOR NORDIC COMPUTER FORENSIC INVESTIGATORS

Module 3B

Linux Artefacts

7.5 ECTS

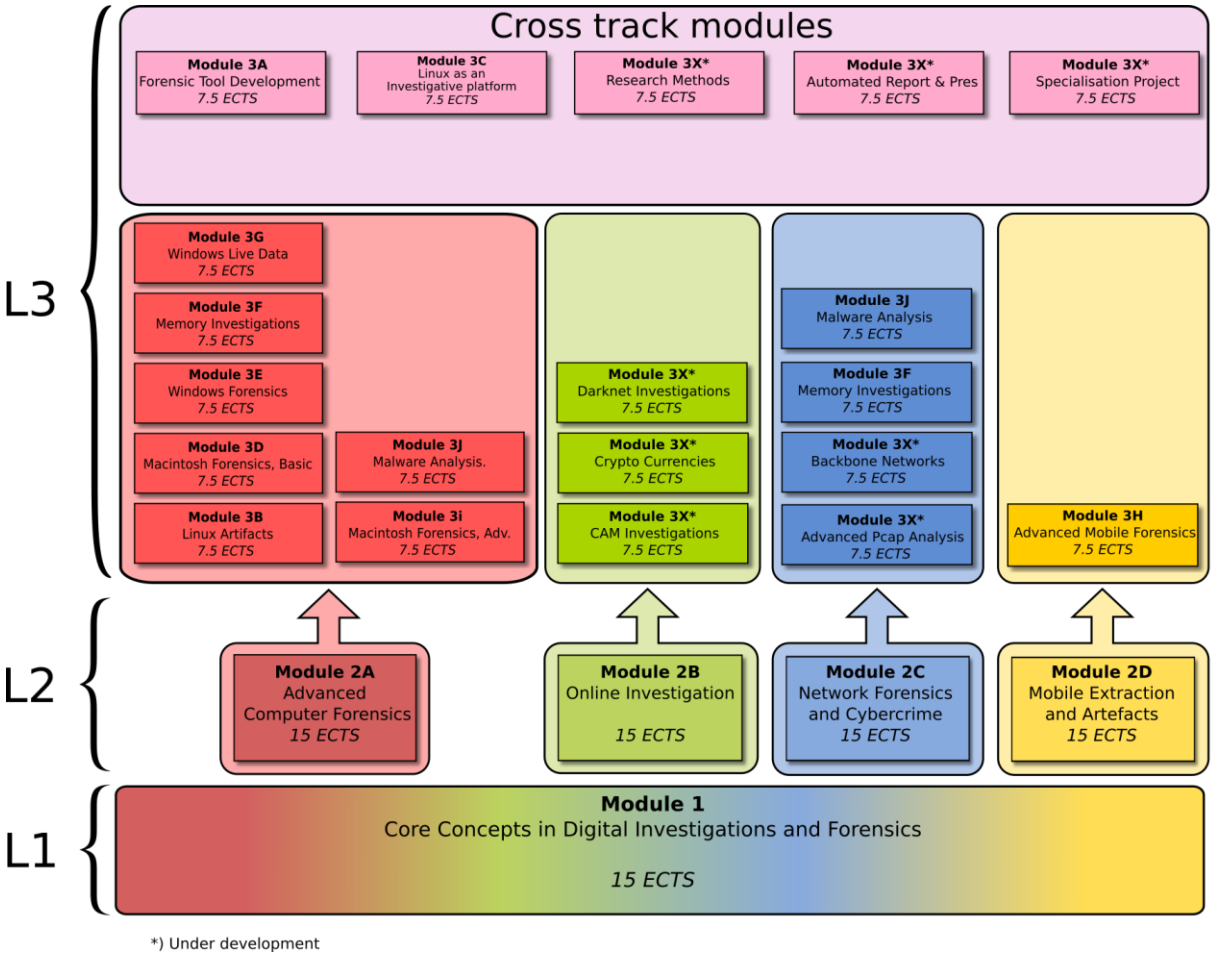
Approved by the Police University College Board

5th of December 2018

1. Introduction

Personal computing has for years been dominated by the Windows operating system and lately there has been an increase in the use of Macintosh operating systems. There are also other operating systems which are widely used but not as well known. These systems form the core services provided by the Internet. UNIX or UNIX-like systems such as Linux have been part of the Internet and corporate servers for many years and are expected to remain so for the foreseeable future. Furthermore, the majority of embedded systems, such as those for navigation and the Internet of Things, are using Linux. As the ultimate aim of every case is the successful prosecution of the case in a courtroom, so in this course, the students will be capable of utilising Linux artefacts in an investigation and thereby ensuring that any evidence acquired from such systems will be admissible in court.

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



*) Under development

2. Aim

The aim of this program is to ensure that the quality of computer 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 3B 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, NCFI Module 2C Network Forensics and Cybercrime or NCFI Module 2D Mobile Extraction and Artifacts. 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:

- different Linux distributions

- the artefacts available within a Linux system and their potential evidential value
- the distinctions between different Linux file systems.

4.3. Skills

After completion of the course candidates are able to:

- utilise Linux artefacts in an investigation
- evaluate the relevance of Linux artefacts
- conduct live data forensics on Linux systems.

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.

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

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 up to 8 online tests throughout the course. Students may have multiple attempts at these tests if necessary.

6. Assessment

The module concludes with an examination consisting of two parts:

- one individual assignment

- oral examination based on the submitted assignment

Grading is on a scale of A – F (in which A – E are passing grades and F is a fail). Both parts of the examination must be passed. An overall grade is given, which may be adjusted one step up or down based on the oral examination.

7. Literature (450 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.

The mandatory reading shall not exceed 450 pages.

7.2. Optional literature

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

- Nemeth, E., Snyder, G., Hein, T. R., Whaley, B. & Mackin, D. (2017) *Unix and Linux System Administration Handbook* (5th Ed.), Addison-Wesley, ISBN-13: 978-0134277554, Chapters 2 – 6, 10, 13, & 18 (340 pages)

7.3. Assumed knowledge

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