POLITIHØGSKOLEN

CURRICULUM

POSTGRADUATE EDUCATION FOR NORDIC COMPUTER FORENSIC INVESTIGATORS

Module 1: Core Concepts in Digital Investigation & Forensics

15 ECTS

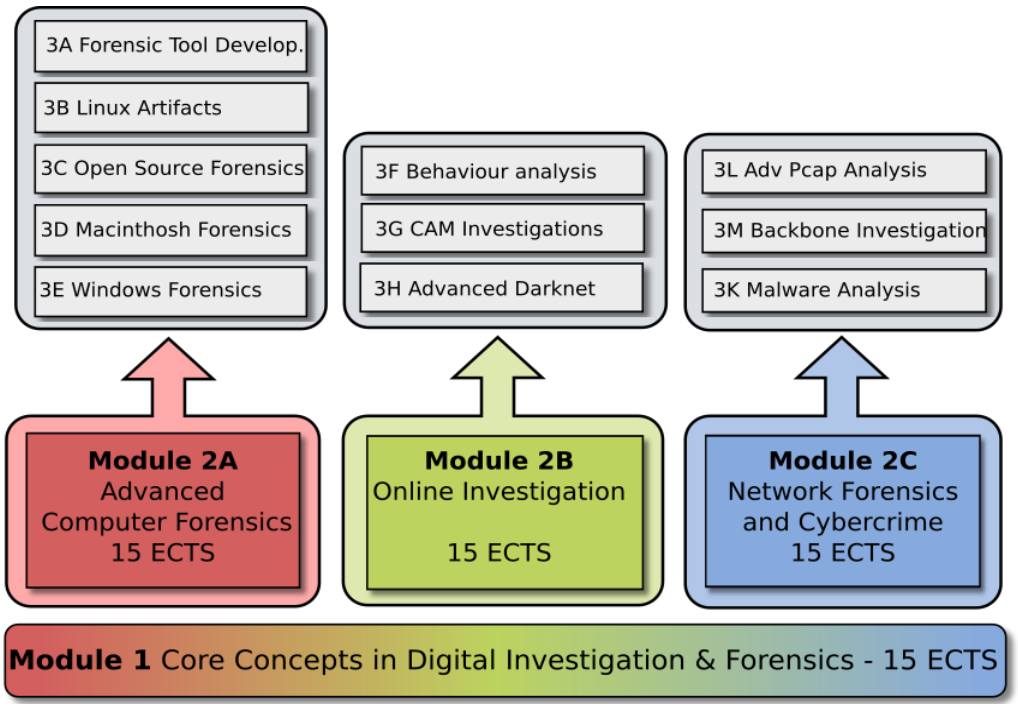
Approved by the Police University College Board
6th of December 2017

1. Introduction

Digital evidence is no longer only of importance in cybercrime investigation, nowadays the prevalence of technology in society has meant that there is digital evidence in almost all crimes. Society exists in a technical and connected world and as a result of this the amount of digital evidence has increased substantially. In addition the type of digital evidence has changed over the years, no longer is it the physical hard drive that we are most interested in. Often it is the smart device, or the online presence that is needed. The acquisition and interpretation of these require additional skills to that of traditional forensics.

In the past only a small number of police required training in this area, however, this has changed dramatically. It is now essential that more police officers are trained in the areas of Online Investigation, First Response, and Digital Forensics etc. in order to improve the efficiency of investigation. This module will introduce students to these fields and also prepare them for further studies in specialist areas in the future.

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



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 or will be handling and investigating digital evidence.

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 are required to provide the following documentation:
Education:

- Higher Education Entrance Qualification

Employment, work experience and additional requirements:

- current employment in a governmental agency

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

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

4. Learning outcome

4.1 General competence

After completion of the module candidates will:

- Perform professional tasks in the role of digital forensic investigator with increased insight and confidence and identify situations in which their personal knowledge is insufficient
- See the role of digital forensics in a broader perspective during an investigation
- Identify ethical and legal issues during investigation
- Assess and apply relevant transnational legislation to investigations

4.2 Knowledge

After completion of the module candidates will have knowledge about:

- Digital Forensic Methodologies and their application
- Relevant legislation
- Cybercrime and Anti-Forensics
- ACPO Principles

4.3 Skills

After completion of the module candidates will be able to:

- Interpret information stored in a computer system
- Identify computer and network components
- Conduct online investigations
- Use digital forensic tools to analyse file systems
- Apply the digital forensic methodology in all forensic analysis tasks.
- Present technical evidence to investigators, prosecutors and courts

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 420 hours of study. There is a single week physical campus at which attendance is mandatory.

The module comprises lectures, individual and group work, exercises, quizzes, assignments and literature study. Student support will be delivered via electronic means such as: email, discussion fora, chat and 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 program is organized 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 requirements must be approved before students may sit the exam:

- Automatically graded quizzes for each topic
- Campus participation
- A practical assignment
- A case study

6. Assessment

The module is concluded with a one day take-home practical exam, and a one day take-home theoretical exam. Both must be passed in order to successfully complete the module.

Students will be graded on a Pass / Fail scale.

7. Literature

7.1. Mandatory literature

In addition to the listed mandatory literature, students need to read and use a number of specific web resources, lessons and academic research papers. These will also 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, these need to be provided to students during the course of the study, to ensure they are up to date and based on current trends. The mandatory reading shall not exceed 975 pages.

7.2. Assumed knowledge

The Norwegian Police University College's introductory course "NCFI Introduction", or equivalent course(s)