POLITIHØGSKOLEN

CURRICULUM

POSTGRADUATE EDUCATION FOR NORDIC COMPUTER FORENSIC INVESTIGATORS

Module 2C: Network Forensics & Cybercrime

15 ECTS

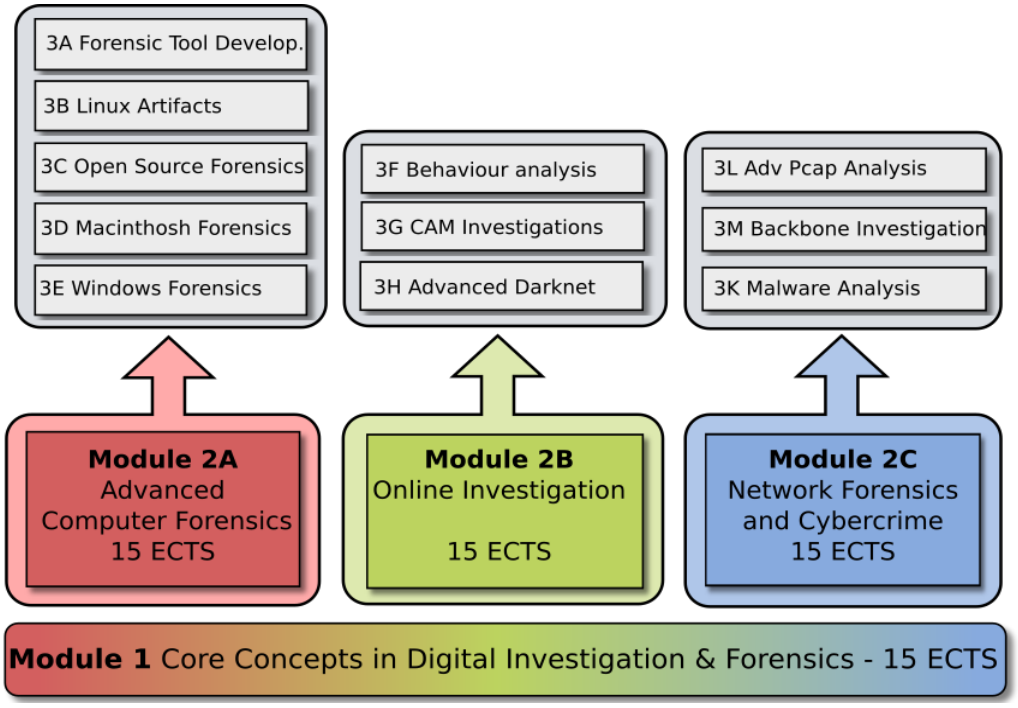
Approved by the Police University College Board

6th of December 2017

1. Introduction

Cybercrime as an area has grown substantially in recent years. Incidents of malware, hacking, financial fraud etc. have become more prevalent. Cybercrime has begun to realise large profits for criminal organisations. Cybercrime attacks usually involve a multinational component in which the attacks are conducted via computer networks. In order to counter this threat law enforcement agents require the ability to investigate attacks conducted through a network. For this they require network forensic skills and knowledge about the cybercrime area as a whole.

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 network 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
- Completion of the Core Concepts in Digital Investigation & Forensics module

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 network forensic investigator with increased insight and confidence and identify situations in which their personal knowledge is insufficient
- See the role of online investigation in a broader perspective during the course of 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:

- Types of cybercrime and their effect on society
- The modus operandi of cybercriminals
- How networks function
- Future cybercrime challenges for law enforcement

4.3 Skills

After completion of the module candidates will be able to:

- Intercept and analyse network traffic
- Design and configure network infrastructure
- Analyse communication artefacts
- Analyse log files
- Conduct and manage network forensics as part of a cybercrime investigation
- Apply the digital forensic methodology in all forensic analysis tasks
- Present technical evidence to investigators, prosecutors and courts

5. Organization 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.

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. Certain mandatory live online lectures, no more than 7 days, will be conducted during the course.

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
- Two practical assignments
- A reflective paper
- Attendance at mandatory lectures

6. Assessment

The module is concluded with a two-day take-home-exam.

Students will be graded on a scale from A – F. A – E are passing grades and F is a failing grade.

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

Literature from The Norwegian Police University College's module 1 «Core concepts in Digital Investigation and Forensics"