POLITIHØGSKOLEN

CURRICULUM

POSTGRADUATE EDUCATION FOR NORDIC COMPUTER FORENSIC INVESTI-GATORS

Module 2A: Advanced Computer Forensics

15 ECTS

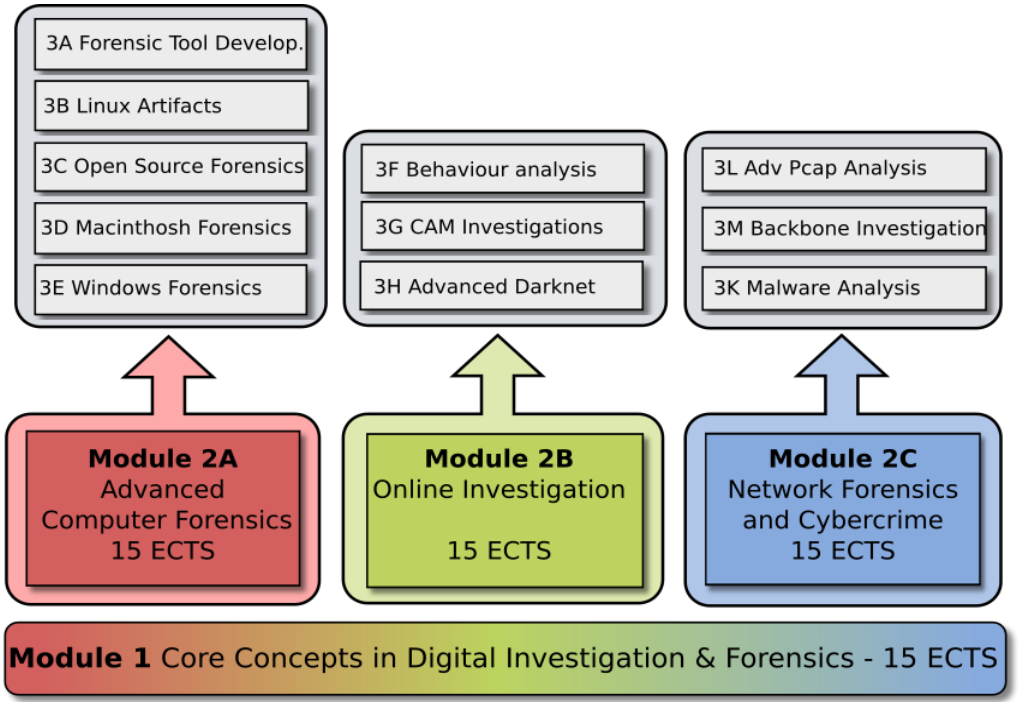
Approved by the Police University College Board
6th of December 2017

1. Introduction

Law enforcement's need for digital forensics is constantly increasing. Traditionally digital forensics was utilised in only a small number of investigations, however, with the advent of the web and smart devices there is the potential for digital evidence in all cases. The analysis of digital devices is now more important than ever. It is not sufficient however, for analysts to merely push a button to discover to process digital evidence. The analyst must understand the processes by which the information is recovered and be able to explain these to the courts.

This course provides the students with the skills needed to not only process digital evidence but to explain both how the information was created and also how the forensic tools recovered that information.

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
- 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 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
- Apply the digital forensic methodology in all forensic analysis tasks
- Understand the scientific principles that underlie digital evidence

4.2. Knowledge

After completion of the module candidates will have knowledge about:

- The functioning of windows file and operating systems
- The present and future challenges of digital forensics

4.3. Skills

After completion of the module candidates will be able to:

- Explain how the file and operating systems function
- Analyse Windows Systems (inc. File Systems; Operating Systems and Recovered Artifacts)
- Compare the results of multiple forensic tools and select tools that are most appropriate for the task in hand
- Automate simple forensic tasks

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 approximate 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 have to be approved before students may sit the exam:

- Automatically graded quizzes for each topic
- A practical assignment
- A case Study
- 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"