



**POLITI HØGSKOLEN**

**CURRICULUM**

**POSTGRADUATE EDUCATION  
FOR  
NORDIC COMPUTER FORENSIC INVESTI-  
GATORS**

**Module 2B: Online Investigation**

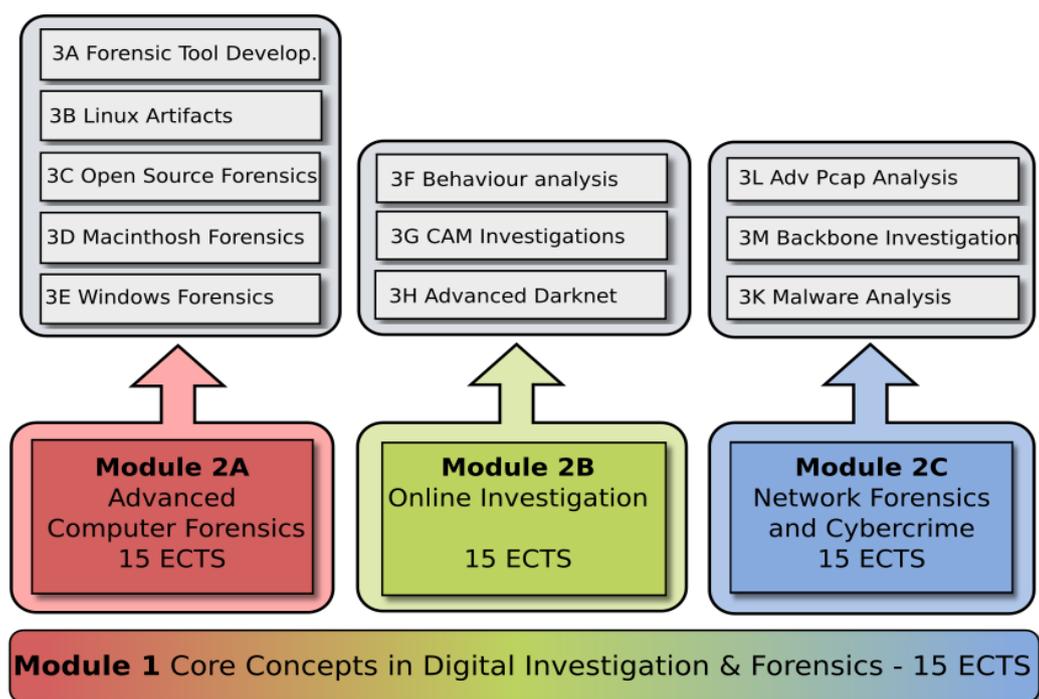
**15 ECTS**

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

## 1. Introduction

As more of society live their lives in an online environment it is important that law enforcement agents are in a position to perform investigations in this arena. This online arena consists of traditional social media services such as Facebook and Twitter to more specialised services such as Instagram and Tinder. In addition we have recently witnessed criminal organisations moving from the traditional web to the dark web. The dark web allows the anonymous purchase of items such as drugs, people, weapons, and criminal services. The dark web is facilitated through the use of cryptocurrencies, digital currencies that are difficult to trace. These currencies have helped to anonymise the dark web even further. Investigating these sources requires specialist skills which are now more necessary than ever.

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 online 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 online 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:

- The various social media platforms that exist
- The deep and dark web and how the challenges that they pose to investigation
- Cryptocurrencies and their use in criminality
- The potential risks of online investigation

### 4.3 *Skills*

After completion of the module candidates will be able to:

- Construct an environment from which online investigations can be safely conducted
- Acquire online resources in a forensically sound manner
- Conduct covert investigations and document results
- Identify people from online personae
- Conduct advanced web and multimedia searches
- 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
- 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 (425 pages)

### 7.1 Mandatory literature

Bazzell, M. (2016): *Open Source Intelligence Techniques: Resources for Searching and Analysing Online Information*. USA: CreateSpace Independent Publishing Platform, ISBN-13: 978-1530508907. Chapters 1-12 (280 pages).

Golbeck, J. (2015): *Introduction to Social Media Investigation: A Hands on Approach*. USA: Syngress, ISBN-13: 978-0128016565. Chapters 1 - 6, 8, 9, 12, 13, 15, & 16 (145 pages).

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»