POLITIHØGSKOLEN

# CURRICULUM

# POSTGRADUATE EDUCATION FOR NORDIC COMPUTER FORENSIC INVESTIGATORS

## Module 3F
## Memory Investigation

## 7.5 ECTS

Approved by the Police University College Board
5th of December 2018

## 1. Introduction

Traditionally most of the investigation on personal computers have been focused on data stored on disk. A personal computer both have a disk storage but also a huge amount of data stored in the memory (RAM). This is data stored temporary and is available as long as the machine is turned on.

The importance of this temporary storage has been known as very important to reveal traces of evidential value or other information to be used further in the investigation. Memory contains information about the most recent activities from the user, possible passwords and encryption keys.

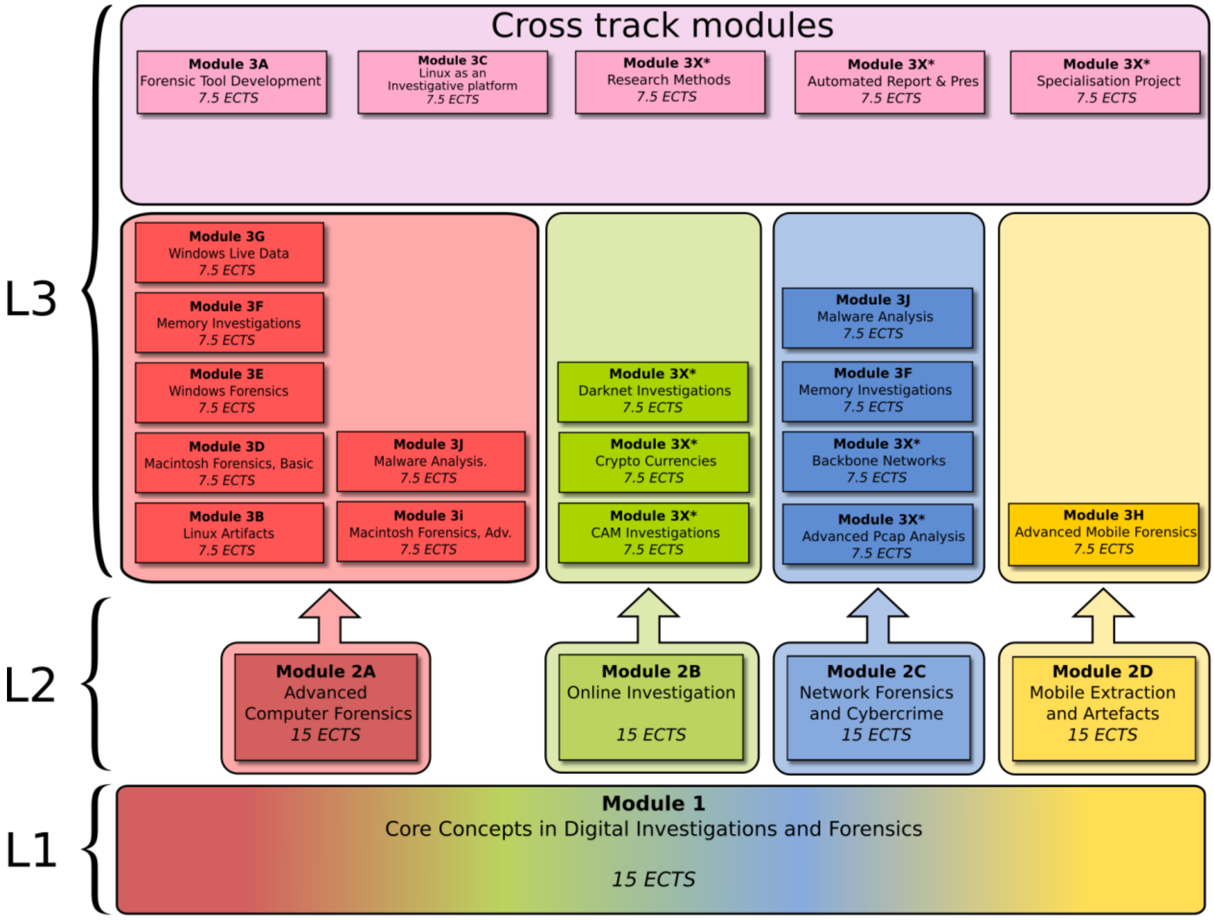
The content of memory is not so well organized as a file system on a disk and collecting from this storage demand more knowledge and skills for the investigator.

In a time when more personal computers have the content on disk protected by encryption, is becomes more important to have alternate sources for evidence or information to give access to these protected storages.

Investigating memory could be a valuable source for information about the user's activity in cyberspace, both legal and illegal.

It is now essential that more police officers are trained in memory investigation in order to improve the efficiency of investigation.

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


Cross track modules
Module 3A Forensic Tool Development 7.5 ECTS
Module 3C Linux as an Investigative platform 7.5 ECTS
Module 3X* Research Methods 7.5 ECTS
Module 3X* Automated Report & Pres 7.5 ECTS
Module 3X* Specialisation Project 7.5 ECTS
L3
Module 3G Windows Live Data 7.5 ECTS
Module 3F Memory Investigations 7.5 ECTS
Module 3E Windows Forensics 7.5 ECTS
Module 3D Macintosh Forensics, Basic 7.5 ECTS
Module 3J Malware Analysis. 7.5 ECTS
Module 3B Linux Artifacts 7.5 ECTS
Module 3i Macintosh Forensics, Adv. 7.5 ECTS
Module 3X* Darknet Investigations 7.5 ECTS
Module 3X* Crypto Currencies 7.5 ECTS
Module 3X* CAM Investigations 7.5 ECTS
Module 3J Malware Analysis 7.5 ECTS
Module 3F Memory Investigations 7.5 ECTS
Module 3X* Backbone Networks 7.5 ECTS
Module 3X* Advanced Pcap Analysis 7.5 ECTS
Module 3H Advanced Mobile Forensics 7.5 ECTS
L2
Module 2A Advanced Computer Forensics 15 ECTS
Module 2B Online Investigation 15 ECTS
Module 2C Network Forensics and Cybercrime 15 ECTS
Module 2D Mobile Extraction and Artefacts 15 ECTS
L1
Module 1 Core Concepts in Digital Investigations and Forensics 15 ECTS

*) 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 3F must:

- possess higher Education Entrance Qualification
- be employed by a national or local governmental agency
- have passed NCFI Module 2A Advanced Computer Forensics. The former NCFI Module 2 (25 ECTS) is also accepted
- Have at least one year of experience in digital forensic 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 outcome

### *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 completion of the module candidates will have knowledge of:

- the potential computer memory could have in an investigation
- explaining how information are stored in computer memory
- how to recognise traces in computer memory
- the distinction between memory in different operating system

### *4.3 Skills*

After completion of the module candidates will be able to:

- use software to perform acquisition of computer memory
- interpret information stored in a memory using forensic tools
- relate the digital forensic methodology in all forensic analysis tasks.
- write a forensic report for other 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 210 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.

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
- Three practical assignments

## 6. Assessment (To be more evaluated)

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

Grading is on a scale of A – F (in which A – E are passing grades and F is a fail).

## 7. Literature

### *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. Assumed knowledge*

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