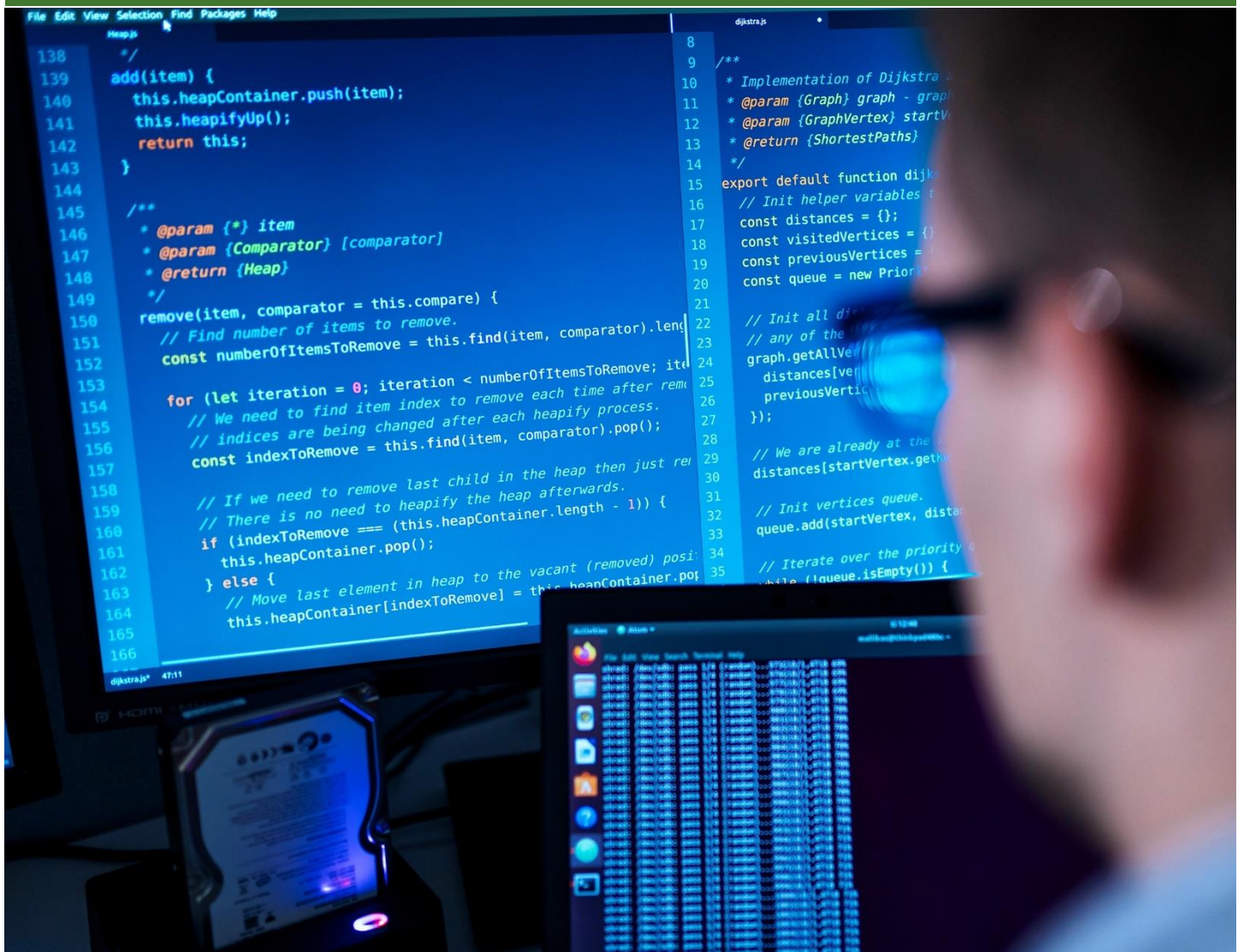


Curriculum for specialisation studies for cybercrime prevention (35 credits)

2023–2025



The Board of the Police University College approved the curriculum of specialisation studies for cybercrime prevention on 24 May 2023. (POL-2023-62865)

The European Union Internal Security Fund has supported the implementation of specialisation studies for cybercrime prevention.



**Co-funded by
the European Union**

Contents

1 Aiming for professional excellence	3
2 European and national qualification frameworks	4
3 Pedagogical policies for the curriculum	5
3.1 Creating future security.....	5
3.2 This is how we reach our goals.....	5
3.3 The principles of our education.....	6
4 Sustainable development in police training.....	7
5 Competency-based curriculum.....	7
6 Student admission and study completion times.....	8
7 Study attendance	8
8 Assessment of study attainments.....	9
9 Curriculum and teaching implementation methods.....	9
10 Courses	10
11 Compulsory studies (20 credits).....	11
11.1 Core Concepts in Digital Investigations and Forensics (15 credits).....	11
11.2 Development project (5 credits)	12
12 Elective studies (15 credits)	13
12.1 Cryptocurrencies (2 credits).....	13
12.2 Basics of forensic programming (3 credits)	13
12.3 Basics of malware analysis (3 credits)	14
12.4 Internet in crime prevention (1.5 credits).....	15
12.5 Internet in crime prevention, advanced course (1.5 credits).....	16
12.6 Hardware-oriented digital forensics (2 credits).....	17
12.7 Linux as investigative tool (3 credits)	17
12.8 MacOS forensics (4 credits).....	18
12.9 Basics of mobile forensics (3 credits).....	19
12.10 Advanced course in mobile forensics (4 credits)	20
12.11 Memory and live forensics (3 credits).....	20
12.12 Basics of tactical cybercrime investigation (2 credits)	21
12.13 Advanced course in tactical cybercrime investigation (2 credits).....	22
12.14 Data communications technologies and protocols (2 credits).....	23

12.15 Basic course in cybercrime investigation (2 credits).....	24
12.16 Advanced course in cybercrime investigation (2 credits).....	24
12.17 Windows forensics (4 credits)	25
12.18 NCFI Level 2 –courses (15 op)	26

1 Aiming for professional excellence

Specialisation studies are long-term training modules that may be completed after the attainment of a higher education degree. These studies help promote the professional development and specialized skills of those already in working life. The purpose of specialisation studies is to create a systematic opportunity for those who have completed their basic degree (Bachelor of Police Services or previous degree or other applicable university degree) and who have served in working life. Specialisation studies allow these individuals to deepen their expertise and refocus their competence in other ways than in connection with the attainment of their degree, while also flexibly supporting the needs of new and emerging areas of expertise, primarily for the police and, as far as possible, for other public authorities.

Police officers are expected to possess multifaceted expertise that is based on the generally accepted values and codes of conduct of police work. The objective of the Police University College is to provide higher education in internal security, based on the cultural knowledge of and research conducted in the field, for those aiming for specialist and leadership positions, as well as for supporting each individual’s professional growth and promoting lifelong learning objectives. In addition, the Police University College conducts applied research and development work that support the planning and development of policing and internal security, as well as the teaching activities conducted at the College.

The objective of the specialisation studies for cybercrime prevention is to provide students with sufficient fundamental theoretical and practical knowledge as well as the skills necessary for working in cybercrime prevention positions, and the capabilities for developing their work communities and themselves.

Students who complete the specialisation studies for cybercrime prevention:

- Possess extensive practical and fundamental knowledge as well as the skills and theoretical principles necessary for working in specialist positions in the field of cybercrime prevention.
- Have acquired the capabilities necessary for continuous learning and are able to assess their own professional growth trajectories in cybercrime prevention positions.
- Are able to assess and develop the activities of their organisations and work communities in the field of cybercrime prevention.

Students are awarded with a certificate upon completion of a training module at the Police University College.

2 European and national qualification frameworks


The European Qualifications Framework (EQF) and National Framework for Qualifications and Other Competence (NQF) classify degrees to certain requirement levels on the basis of competence. Finland observes the EQF requirement level classification. The Act (93/2017) and Decree (120/2017) on the Framework for Qualifications and Other Learning Modules define the requirement levels of degrees, courses and other extensive learning modules. For each requirement level, the Act specifies the knowledge, understanding and capabilities of a student who has attained the level. These requirement level descriptions are applied to the curriculum planning work of the Police University College, creation of competence profiles, and the evaluation of competence.

Specialisation studies for cybercrime prevention are at Level 6. In the national qualifications framework, level 6 and the shared national competences describe the level of competence of graduates of universities of applied sciences.

Level 6 (degrees from universities of applied sciences, Bachelor's degrees)

- The student has gained a broad and advanced knowledge of the field of study, including a critical understanding and assessment of the key concepts, methods and principles.
- Holder understands the scope and limits of professional fields and/or scientific disciplines
- Holder has advanced cognitive and practical skills that demonstrate mastery of concepts, the ability to apply them and the ability to come up with creative solutions and implementations that are required in a specialized professional, scientific or artistic field to solve complex or unpredictable problems.
- Holder works independently in expert positions in the field and in international cooperation or runs a business.
- Holder manages complex professional operations or projects.
- Holder is capable of making decisions in unpredictable operating environments.
- Holder is responsible not just for the evaluation and development of their own expertise but also for the development of individuals and groups.
- Holder has the prerequisites for lifelong learning.
- Holder works with different kinds of people in educational and working communities as well as in other groups and networks, taking into account collaborative and ethical perspectives.
- Holder communicates fluently in their mother tongue to audiences both within and outside their field orally and in writing.
- Holder communicates and interacts in the other national language and is capable of international communication and interaction in at least one other foreign language in their own field. (Government Decree (120/2017) on the framework for qualifications and other learning modules.)

3 Pedagogical policies for the curriculum

PEDAGOGIC POLICIES OF THE POLICE UNIVERSITY COLLEGE (POLAMK) 

We combine strong expertise in policing with higher education as well as the skills, knowledge and attitudes required by both. We educate experts in internal security and leadership who act ethically and learn continuously throughout their careers.

We use forward-looking education to meet the expectations directed at the police and respond to changes in the operational environment. We experiment boldly and try out new things. We encourage participation in the research and development of working life practices.

We build a common view of our education and ensure in-depth learning and well-being within the university college community. We support the ability to study and learn based on the principle of a constantly learning organization.

THIS IS HOW WE REACH OUR GOALS

- Forward-looking approach**
 - In the planning of our education, we utilize foresight information as well as information about the operational environment systematically.
 - We develop learning outcomes, contents, teaching and evaluation methods and learning environments on the basis of research data and best practices.
 - We strengthen compatibility with working life through personal rotation and other competence development practices.
- A competent university college community**
 - We plan and implement education based on the principles of constructive alignment.
 - We encourage everyone to think, act, investigate, and experiment creatively.
 - We appreciate and support the continuous improvement of know-how and expertise.
- Strong partnerships**
 - We are active in partnership networks within the fields of education and research and with various authorities that support teaching and studying.
 - We develop our education and working life together with our partners.
 - We offer diverse student and staff exchange programs and cross-institutional studies.
- Social responsibility**
 - We implement our sustainable development goals and strengthen our competence in responsibility.
 - We comply with the ethical principles of teaching, research, open science and the police.
 - We support diverse ways of learning.

THE PRINCIPLES OF OUR EDUCATION

- Student-centricity**
Students have an active role. We take the needs of diverse learners into consideration. We ensure a safe and confidential atmosphere. We promote learning by using diverse teaching methods, evaluation practices and both authentic and digital learning environments. We encourage feedback.
- Collegiality**
We study, teach and work in multiprofessional teams. Our education is based on co-teaching. We encourage sharing of skills and knowledge as well as experimentation with new methods. We are accountable for the welfare of ourselves and each other. We strengthen an interactive university college community together.
- Competency-based curriculum**
Our education is based on the national qualification framework. Our competency-based curricula ensure compliance with the standards of higher education, close cooperation with working life and the development of professional and general competencies.
- Shared pedagogic management**
We share pedagogic management. We promote cooperation and collegiality between actors. We support and guide the planning and development of education and everyday work in teaching. We manage competence to enable each individual, the team and the whole organization to learn, develop and reach their goals.


 #creatingfuturesecurity

Figure 1 Pedagogic policies of the police university college (POLAMK)

3.1 Creating future security

We combine strong expertise in policing with higher education as well as the skills, knowledge and attitudes required by both. We educate experts in internal security and leadership who act ethically and learn continuously throughout their careers.

We use forward-looking education to meet the expectations directed at the police and respond to changes in the operational environment. We experiment boldly and try out new things. We encourage participation in the research and development of working life practices.

We build a common view of our education and ensure in-depth learning and well-being within the university college community. We support the ability to study and learn based on the principle of a constantly learning organization.

3.2 This is how we reach our goals

Forward-looking approach

- In the planning of our education, we utilize foresight information as well as information about the operational environment systematically.
- We develop learning outcomes, contents, teaching and evaluation methods and learning environments on the basis of research data and best practices.

- We strengthen compatibility with working life through personal rotation and other competence development practices.

A competent university college community

- We plan and implement education based on the principles of constructive alignment.
- We encourage everyone to think, act, investigate, and experiment creatively.
- We appreciate and support the continuous improvement of know-how and expertise.

Strong partnerships

- We are active in partnership networks within the fields of education and research and with various authorities that support teaching and studying.
- We develop our education and working life together with our partners.
- We offer diverse student and staff exchange programs and cross-institutional studies.

Social responsibility

- We implement our sustainable development goals and strengthen our competence in responsibility.
- We comply with the ethical principles of teaching, research, open science and the police.
- We support diverse ways of learning.

3.3 The principles of our education

Student-centricity

Students have an active role. We take the needs of diverse learners into consideration. We ensure a safe and confidential atmosphere. We promote learning by using diverse teaching methods, evaluation practices and both authentic and digital learning environments. We encourage feedback.

Collegiality

We study, teach and work in multiprofessional teams. Our education is based on co-teaching. We encourage sharing of skills and knowledge as well as experimentation with new methods. We are accountable for the welfare of ourselves and each other. We strengthen an interactive university college community together.

Competency-based curriculum

Our education is based on the national qualification framework. Our competency-based curricula ensure compliance with the standards of higher education, close cooperation with working life and the development of professional and general competencies.

Shared pedagogic management

We share pedagogic management. We promote cooperation and collegiality between actors. We support and guide the planning and development of education and everyday work in teaching. We manage competence to enable each individual, the team and the whole organization to learn, develop and reach their goals.

4 Sustainable development in police training

The vision of the police is: The Finnish police keeps everyone safe at all times. The aim of the police is to:

- safeguard everyday life and maintain high trust in the police
- prevent crime and disturbances in advance
- effectively reveal and investigate serious crimes in particular
- produce modern, safe and developing services
- collaborate and communicate effectively.

Fairness, competence, a service-minded approach, and staff wellbeing form the cornerstones of the police force's operations. The police have an ethical code of conduct confirmed in 2019.

Sustainable development is often divided into ecological, economic and socio-cultural dimensions that all affect one another (Rohweder L. et al. 2008)¹. The ecological sustainability of educational activities can be promoted through natural resource-conscious teaching methods, such as online studies and simulations. Economic sustainability also places some constraints on the planning and implementation of the degree education provided for Bachelor of Police Services students.

Sociocultural sustainability is a natural part of police education and its contents. It is evident in the observance of fundamental and human rights and equality in the contents and implementation of the training. The Police Barometer is used regularly to measure the sociocultural dimension of police work and the results indicate trust in the police. The training and education provided by the Police University College promote sociocultural sustainable development in society in particular. The objective is to train police officers whose work method is equal, fair and ethical.

5 Competency-based curriculum

The Police University College's curricula are competency-based. Competency-based curricula determine the learning outcomes for the degree and for the courses included in the degree, in other words, what the student should know, understand and be able to do as a result of the learning process. Assessment is focused on learning results and based on learning outcomes. The principles of assessment are described in the Police University College degree regulation.

Factors that guide teaching and study include the goal-oriented development of competence, reinforcement of the aspects of learning, and creation of modules that reflect the everyday professional work.

¹ Rohweder Liisa, Virtanen Anne, Tani Sirpa, Kohl Johanna ja Arja Sinkko (2008) Näkökulmia opetukseen ja oppimiseen. (Aspects of teaching and learning, in Finnish) Rohweder, L. & Virtanen, A. (eds.). Kohti kestäväää kehitystä. Pedagoginen lähestymistapa. (Towards sustainable development. A pedagogic approach, in Finnish) Ministry of Education publication No 2008:3. Available in electronic format: <https://julkaisut.valtioneuvosto.fi/bitstream/handle/10024/79112/opm03.pdf?sequence=1>

Characteristics of competency-based learning include the following:²

- Self-assessment by students plays a key role in the study path.
- Competence is recognised and acknowledged regardless of the place, time or way in which it was acquired.
- Personalised and individual study paths are implemented in education.
- Teachers play a strong role in guidance and the recognition of competences.
- The curriculum comprises competence areas relevant in working life.
- Competence areas include student-oriented learning outcomes.
- Clear assessment criteria have been set for the learning outcomes.
- There are different ways to acquire or complement any competences missing according to the learning outcomes.
- The assessment of learning is constant, versatile and conducted by several assessors.

6 Student admission and study completion times

The target group of the training is officials working in specialist positions in cybercrime prevention, or officials in training for such positions. The Police University College decides on the grounds for student admission, the application procedure, and the final admission selection process. According to the Police University College's Rules of Procedure, the selection criteria for specialisation studies are confirmed by the Board of the Police University College.

The scope of the specialisation studies for cybercrime prevention is 35 credits and the target completion time is two years. One credit corresponds to approximately 27 study hours. The student's work input is calculated on the basis of the time that they are expected to spend completing the course, including all contact teaching and independent studies. The student's right to study is valid for three years. If a student's commanding unit has submitted a study interruption proposal, the student may, at the request of the unit, be admitted to the next corresponding course.

7 Study attendance

The studies require attendance in lectures and exercises.

To progress in the training program, the student must pass all study attainments included in the training. A development project is included in the specialisation studies.

As a rule, students participating in the specialisation studies are public servants in the police administration who have been commanded to attend the training by their respective police units. By participating in the training, they fulfil their duties as public servants.

² Alaniska, Hanna, Keurulainen Harri, Tauriainen Tiia-Mariia (eds.) 2019. Osaamisperustaisia käytäntöjä korkeakouluissa. (Competency-based practices in universities, in Finnish) R&D publications of the Oulu University of Applied Sciences, ePooki 58/2019.

In the event of an illness, the student must notify the teacher in charge of their absence in addition to following the instructions for reporting any illness-related absences from work.

If a student is repeatedly absent during a contact teaching period, they must complete the substitute exercises/learning assignments assigned by the teacher in charge of the course or, if necessary, retake the course in full.

8 Assessment of study attainments

The purpose of assessment is to guide students and help them achieve their study objectives. Study assessment forms a part of the learning and teaching process, and the study attainments are assessed after the completion of the course. The basic principle of the assessment is that each student's performance is compared with the learning outcomes specified in the curriculum. The assessment process follows the Police University College degree regulations.

All written exercises and development projects are analysed using an anti-plagiarism system. In dealing with cases of student fraud, the Police University College's guidelines on the topic will be followed.

9 Curriculum and teaching implementation methods

The curriculum describes the required study attainments. The curriculum for specialization studies is approved by the Board of the Police University College. The contents and implementation of each course are described in more detail in the separate implementation plan, approved by the Head of Education.

The studies comprise the following compulsory courses:

- Core Concepts in Digital Investigations and Forensics, (15 credits)
- Development project (5 credits).

In addition to the compulsory courses, the students select at least 15 credits of elective studies from the range of elective courses on offer (The teaching materials on the course are partly in English and on some courses, the language of instruction can be English).

Applicable higher education studies completed elsewhere can be included in the elective studies of the specialisation studies. Such studies are not required to correspond to the courses of the specialisation studies in terms of their content, but they must support the development of a police officer's professional cyber competence. In their applications, students must justify how the studies to be included will support the professional development of a police officer. The students must have the study attainments, that are not part of the curriculum, approved by the teachers in charge of the education.

The teaching materials on the course are partly in English and on some courses, the language of instruction can be English.

Specialisation studies for cybercrime prevention 35 ECTS

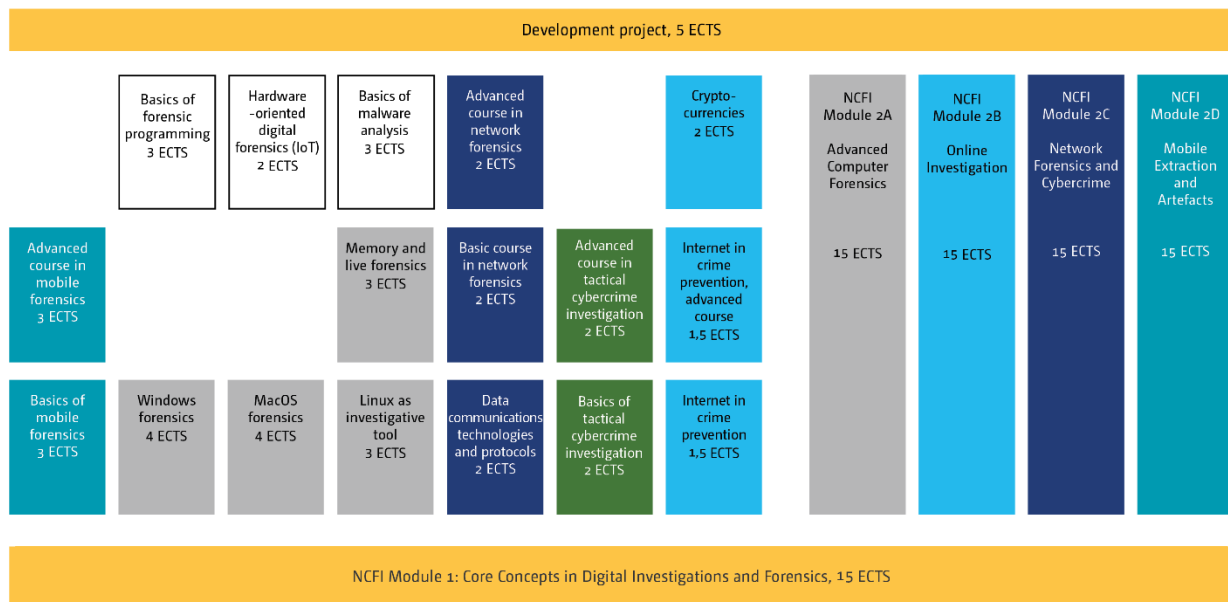


Figure 2 Specialisation studies for cybercrime prevention (35 credits)

10 Courses

Compulsory studies (20 credits)

- Core Concepts in Digital Investigations and Forensics (15 credits)
- Development project (5 credits).

Elective studies (at least 15 credits)

The elective courses will be opened for application in the Police University College's education calendar for continuing education and applications can be filed through the study administration system.

- 1) Cryptocurrencies (2 credits)
- 2) Basics of forensic programming (3 credits)
- 3) Basics of malware analysis (3 credits)
- 4) Internet in crime prevention (1.5 credits)
- 5) Internet in crime prevention, advanced course (1.5 credits)
- 6) Hardware-oriented digital forensics (2 credits)
- 7) Linux as investigative tool (3 credits)
- 8) MacOS forensics (4 credits)
- 9) Basics of mobile forensics (3 credits)
- 10) Advanced course in mobile forensics (3 credits)
- 11) Memory and live forensics (3 credits)
- 12) Basics of tactical cybercrime investigation (2 credits)
- 13) Advanced course in tactical cybercrime investigation (2 credits)
- 14) Data communications technologies and protocols (2 credits)
- 15) Basic course in network forensics (2 credits)

16) Advanced course in network forensics (2 credits)

17) Windows forensics (4 credits)

In addition to the courses listed above, elective studies can include Level 2 modules from the inter-Nordic Nordic Computer Forensic Investigators study programme (NCFI). These modules are administered by The Norwegian Police University College (PHS). Applications for Level 2 modules in the NCFI study programme are sent through the application system of PHS. The language of instruction is English. The following modules can be included in the elective courses of the specialisation studies for cyber-crime prevention:

- Module 2A Advanced Computer Forensics (15 credits)
- Module 2B Online Investigation (15 credits)
- Module 2C Network Forensics and Cybercrime (15 credits)
- Module 2D Mobile Extraction and Artifacts (15 op)

11 Compulsory studies (20 credits)

11.1 Core Concepts in Digital Investigations and Forensics (15 credits)

Description

The course provides the investigator with basic knowledge for working in tasks relating to cybercrime prevention. The aim of the course is to develop understanding of digital forensic methodologies, key principles and legislation and their application to cybercrime investigation.

The course is concurrent with Module 1 of the Nordic Computer Forensic Investigators study programme (NCFI). Completion of the course provides students with eligibility to apply for Level 2 modules in the NCFI study programme.

Learning outcomes

After completion of the course, the student will:

- be able to see the role of digital forensics in a broader perspective during a criminal investigation
- be able to identify ethical and legal issues during investigation
- know how to assess and apply relevant legislation to investigations
- be able to interpret evidence found in IT devices
- know how to use digital forensic tools and analyse results.

Subject matters

- Digital forensic methodologies and their application to criminal investigation
- Legislation
- Cybercrime and its investigation

Required performances

Participation in lectures, successful completion of exercises and passing the exam.

Assessment scale

The course will be graded as pass/fail.

Prerequisite studies

Not required.

11.2 Development project (5 credits)

Description

The development project is a practical project that students conduct during their studies.

The development project increases the student's capacity to serve as an active participant in various development projects and tasks in one's own organisation and provides basic information on project management and quality work from the perspective of work management. Where applicable, the guidelines on academic theses of the Bachelor of Police Services degree apply to both the development project and reporting during the specialisation studies for cybercrime prevention.

Learning outcomes

After completion of the course, the student will:

- know how to plan a development project/prepare a project plan
- know how to deliver a practical development project
- know how to report the outcomes of a development project
- be able to evaluate with a critical approach the implementation of development activities and propose further plans
- be able to develop operations on the basis of monitoring and feedback

Subject matters

- Development of operations and quality
- Planning of and reporting on the development task
- Project work
- Development methods
- Implementation of the development project

Required performances

Successful completion of the development project.

Assessment scale

The course will be graded on a scale of 0–5.

Prerequisite studies

Core Concepts in Digital Investigations and Forensics

12 Elective studies (15 credits)

Both compulsory and recommended preliminary knowledge requirements apply to the courses in elective studies. These are described under prerequisite studies in the curriculum of each course. The recommended prerequisite studies promote the attainment of the learning outcomes of the course.

12.1 Cryptocurrencies (2 credits)

Description

The objective of the course is to provide students with an overview of cryptocurrencies and most common investigation methods. The course offers practical exercises related to Bitcoin blockchain.

Learning outcomes

After completion of the course, the student will:

- be able to describe how virtual currencies are used and confiscated
- be able to identify cryptocurrencies during an investigation
- be able to follow Bitcoin transactions

Subject matters

- Cryptocurrencies
- Transactions and addresses
- Wallets
- Inquiries and their analysis

Required performances

Participation in lectures and successful completion of exercises.

Assessment scale

The course will be graded as pass/fail.

Prerequisite studies

Recommended:

Core Concepts in Digital Investigations and Forensics

12.2 Basics of forensic programming (3 credits)

Description

The objective of the course is to provide the skills to design simple programs for automating digital forensics processes and to facilitate the collection of data from open data sources.

Learning outcomes

After completion of the course, the student will:

- be able to explain the key concepts of software technology
- know how to design small-scale programs in the Python programming language
- know how to use the basic functions of SQLite database engine.

Subject matters:

- Basic concepts of programming languages and software technical problem solving
- Basics of Python programming language
- Basic data types
- Flow control
- Software branching and iteration
- Code reuse
- Input validation
- File processing (file input/output)
- Basics of SQLite databases
- Gathering data from the open sources

Required performances

Participation in lectures and successful completion of exercises.

Assessment scale

The course will be graded as pass/fail.

Prerequisite studies

Recommended:

Core Concepts in Digital Investigations and Forensics

Linux as investigative tool

12.3 Basics of malware analysis (3 credits)

Description

The course introduces students to malware analysis processes and technologies. The objective of the course is to provide students with the skills to identify and find malware and analyse their functioning.

Learning outcomes

After completion of the course, the student will:

- be able to describe the key concepts relating to malware
- know how to search possible malware in a device analyzed
- know how to safely process software assumed or found to be malicious
- know how to use the tools utilised during the course for analysing malware functioning.

Subject matters

- Basic concepts relating to malware analysis
- Searching, recognising and saving malicious software code
- Processing of malware in a safe environment
- Static and dynamic analysis in basic format

Required performances

Participation in lectures and successful completion of exercises.

Assessment scale

The course will be graded as pass/fail.

Prerequisite studies

Recommended:

Core Concepts in Digital Investigations and Forensics

Windows forensics

Basics of forensics programming credits

12.4 Internet in crime prevention (1.5 credits)

Description

The course introduces the structure and range of uses of the Internet and the relevant/applicable legislation.

Learning outcomes

After completion of the course, the student will:

- know how to use and apply learning in day-to-day criminal investigation work
- be able to describe the structure of the Internet and its range of uses
- manage the various knowledge acquisition possibilities of the Internet and know the legislation relating to Internet surveillance
- know how to search and use evidence from the Internet.

Subject matters:

- Anonymous computers
- WWW
- Information gathering and legislation
- Email
- OSINT (Open Source Intelligence)
- Social media

Required performances

Participation in lectures and successful completion of exercises.

Assessment scale

The course will be graded as pass/fail.

Prerequisite studies

Recommended:

Core Concepts in Digital Investigations and Forensics

12.5 Internet in crime prevention, advanced course (1.5 credits)

Description

The course is an in-depth introduction to Open Source Intelligence (OSINT) and the related processes. The course is intended for advanced students wishing to familiarise themselves in-depth with OSINT and the related methods.

Learning outcomes

After completion of the course, the student will:

- know how to apply learning in day-to-day criminal investigation work
- know how to use a computer outside the government authorities' networks safely for OSINT
- know the process for OSINT
- know how to use various applications relating to OSINT
- recognise the risks and opportunities relating to virtual currencies and Tor network.

Subject matters

- Tor
- Linux
- Virtual currencies
- The OSINT process
- Virtual machines

Required performances

Participation in lectures and successful completion of exercises.

Assessment scale

The course will be graded as pass/fail.

Prerequisite studies

Compulsory:

Internet in crime prevention

Recommended:
Core Concepts in Digital Investigations and Forensics

12.6 Hardware-oriented digital forensics (2 credits)

Description

The course examines the tracking and analysis of data in embedded systems, particularly the so-called IoT devices. The course also examines the malware found in IoT devices and analysis of their configurations.

Learning outcomes

After completion of the course, the student will:

- know how to acquire the most common IoT devices
- know how to analyse the functioning and interfaces of an IoT device
- know how to search for malware and recognise malicious configurations in IoT environments

Subject matters

- Basics of embedded systems
- IoT technologies
- Investigation methods and tools for IoT devices
- Acquiring data from embedded systems
- Analysis of embedded system data
- Malware in IoT environments

Required performances

Participation in lectures and successful completion of exercises.

Assessment scale

The course will be graded as pass/fail.

Prerequisite studies

Recommended:
Core Concepts in Digital Investigations and Forensics

12.7 Linux as investigative tool (3 credits)

Description

The course examines new methods and techniques using open source-based investigation environment and tools. The course introduces automated forensic investigation and the verifiability of current software. Students learn the value of open source code and develop their skills of possibly creating new tools for example for restoring data and adapting existing tools with new scripts.

Learning outcomes

After completion of the course, the student will:

- be able to perform digital forensic investigation tasks more precisely and securely than before
- understand the importance of open source code tools in investigation
- know how to use new methods and techniques in investigation
- know how to automate forensic investigation
- know how to adapt and develop existing tools for new challenges.

Subject matters:

- Open source code applications
- Automation
- Linux
- Programming

Required performances

Participation in lectures and successful completion of exercises.

Assessment scale

The course will be graded as pass/fail.

Prerequisite studies

Recommended:

Core Concepts in Digital Investigations and Forensics.

12.8 MacOS forensics (4 credits)

Description

The course introduces the methods in which the MacOS operating system processes and stores data and how to search, interpret and utilise this data in cyber crime prevention.

Learning outcomes

After completion of the course, the student will:

- be able to perform digital forensic investigation tasks more precisely and securely than before
- be able to find the most important artefacts in MacOS environments
- know how to use the methods and techniques learned on the course in practical work
- know how to act in line with basic principles of forensics in MacOS environments.

Subject matters

- MacOS operating system
- JSON data formats

- APFS and HFS file systems
- The Apple ecosystem
- T2 chip and encryption

Required performances

Participation in lectures and successful completion of exercises.

Assessment scale

The course will be graded as pass/fail.

Prerequisite studies

Recommended:

Core Concepts in Digital Investigations and Forensics

12.9 Basics of mobile forensics (3 credits)

Description

The course introduces mobile devices, the related networks and the basics of mobile device forensics.

Learning outcomes

After completion of the course, the student will:

- identify important mobile devices for criminal investigation
- know how to use the appropriate procedures in the processing of digital evidence
- understand the core concepts of acquiring a mobile device
- have the basic knowledge of the most common forensics tools

Subject matters

- Legislation relating to the search of data contained in a device and confiscation
- Taking possession of a device and handling of devices
- Mobile devices
- Basics of telecom networks
- Basics of mobile device forensics

Required performances

Successful completion of an advance assignment before contact studies, participation in lectures and successful completion of exercises.

Assessment scale

The course will be graded as pass/fail.

Prerequisite studies

Recommended:
Core Concepts in Digital Investigations and Forensics

12.10 Advanced course in mobile forensics (4 credits)

Description

The course deepens the skills of students in the topics handled on the Basics of mobile forensics course. The course focuses specifically on mobile device forensics and data analyses.

Learning outcomes

After completion of the course, the student will:

- know how to use the appropriate procedures in the processing of digital evidence
- know how to perform the acquisition of a mobile device
- know how to use the most common forensics tools independently
- know how to apply learning in day-to-day criminal investigation work

Subject matters

- Mobile devices
- Mobile device forensics
- Alternative methods
- Data analysis
- Reporting / statement

Required performances

Successful completion of the advance assignment, participation in lectures and successful completion of exercises.

Assessment scale

The course will be graded as pass/fail.

Prerequisite studies

Compulsory:
Basics of mobile forensics

Recommended:
Core Concepts in Digital Investigations and Forensics

12.11 Memory and live forensics (3 credits)

Description

The course introduces live forensics and memory analysis methodologies. The course focuses particularly on the basic concepts and investigative methods of live forensics in workstation environments (Windows, Mac, Linux).

Learning outcomes

After completion of the course, the student will:

- know how to prepare the tools used in live forensics for the investigation to be performed
- know how to choose the most appropriate investigative tools for each case
- know how to conduct a basic live forensic investigation
- know how to acquire data in a live environment, incl. RAM image
- know how to analyse the RAM image
- know how to document the investigative measures performed
- know how to assess the changes caused by the investigative measures in the target environment.

Subject matters

- Basic tools for live and memory forensics
- Acquisition of live data from computers remote environments
- Making a RAM dump
- Basic memory analysis methods

Required performances

Participation in lectures and successful completion of exercises.

Assessment scale

The course will be graded as pass/fail.

Prerequisite studies

Recommended:

Core Concepts in Digital Investigations and Forensics

Linux as investigative tool

12.12 Basics of tactical cybercrime investigation (2 credits)

Description

The course introduces students to the tactical investigation of common cybercrimes through key concepts and technology relating to cybercrime prevention, the relevant legislation, investigation methods and tactics, production of evidence and stakeholder cooperation. The topics are covered partly through case examples.

Learning outcomes

After completion of the course, the student will:

- recognise the differences between cyber enabled and cyber dependent crimes
- be able to describe common methods of cybercrime and investigative methods
- know how to perform a tactical investigation of common cybercrimes
- be able to assess the significance of digital evidence in the case

- know how to utilise the key methods to access information and coercive methods relevant in cybercrime investigation

Subject matters

- Basic concepts of cybercrime and the principles of cybercrime investigation
- Basics of cybercrime legislation (essential elements of cybercrimes, coercive methods and powers/authority/competencies)
- Utilisation of international instruments in cybercrime investigation
- Digital forensics in cybercrime investigation
- Key cybercrime artefacts, access to information, investigative tactics and presentation of evidence
- Profile of cybercriminals
- Key stakeholders in cybercrime prevention and cooperation between the police and prosecution service
- Europol's SIENA and EIS systems

Required performances

Participation in lectures and successful completion of exercises.

Assessment scale

The course will be graded as pass/fail.

Prerequisite studies

Recommended:

Core Concepts in Digital Investigations and Forensics

12.13 Advanced course in tactical cybercrime investigation (2 credits)

Description

The course deepens the skills of students in the topics covered on the basic course in tactical cybercrime investigation by covering the tactical investigation of complex cybercrimes, log analysis, the investigative methods of digital forensics and data acquisition from open sources to assist the cybercrime investigation. The topics are covered partly through case examples.

Learning outcomes

After completion of the course, the student will:

- be able to conduct tactical investigation of complex crimes targeting the cyber operating environment
- know how to utilise the services of key stakeholders to assist the investigation
- be able to interpret logs and utilise log analysis tools

Subject matters

- Tactical investigation of complex cybercrimes

- Log analysis
- Introduction to the investigative methodology of digital forensics
- OSINT in cybercrime investigation

Required performances

Participation in lectures and successful completion of exercises.

Assessment scale

The course will be graded as pass/fail.

Prerequisite studies

Compulsory:

Basics of tactical cybercrime investigation

Recommended:

Core Concepts in Digital Investigations and Forensics

12.14 Data communications technologies and protocols (2 credits)

Description

The course covers the basics of data communication architectures and protocols key in cybercrime investigation and their interlinkage.

Learning outcomes

After completion of the course, the student will:

- recognise the various protocols in TCP/IP protocol stack
- know the structures and architecture of data communication networks
- know how to analyse IT network traffic
- know how to use the TOR web as a tool and subject of investigation

Subject matters:

- Various protocols in TCP/IP protocol stack
- Configuration of protocols that utilise the TCP/IP protocol stack
- Configuration of modern IT network structures
- Analysis of various network protocols
- Utilisation of tools used in network traffic analysis
- TOR as a tool and subject of investigation

Required performances

Participation in lectures and successful completion of exercises.

Assessment scale

The course will be graded as pass/fail.

Prerequisite studies

Recommended:

Core Concepts in Digital Investigations and Forensics.

12.15 Basic course in cybercrime investigation (2 credits)

Description

The course introduces students to the basic tools and methods of cybercrime prevention and the most common cybercrime techniques. The main focus is on practical exercises. The course also covers network protocol analysis and the legal aspects relevant to the topic. Course exercises are mainly performed in pairs. The aim is to form the pairs so that one member has a technical background and the other is a tactical investigator/head investigator. The objective of this approach is to utilise the strengths of both and provide insight into the other party's viewpoints in investigative work.

Learning outcomes

After completion of the course, the student will:

- know how to use the most common cybercrime prevention and network analysis tools
- know how to apply the methods taught on the course to cybercrime investigation.

Subject matters:

- Key legal aspects relevant in cybercrime prevention
- Introduction to malware and their joint usage
- Basic tools and methods of cybercrime prevention

Required performances

Participation in lectures and successful completion of exercises.

Assessment scale

The course will be graded as pass/fail.

Prerequisite studies

Recommended:

Core Concepts in Digital Investigations and Forensics

Data communications technologies and protocols

Basics of tactical cybercrime investigation

12.16 Advanced course in cybercrime investigation (2 credits)

Description

The course examines the themes covered on the basic course in cybercrime investigation in depth. As on the basic course, the course contents comprise both theoretic modules and exercises that support them, with a special focus on complex enterprise network environments. The course introduces the investigation of cybercrime targeting a company, from the perspective of the police, in cooperation with the injured party's representatives.

Learning outcomes

After completion of the course, the student will:

- identify the key factors in securing digital evidence in connection with cybercrime investigation
- know how to use the malware analysis and digital forensics tools, based on training received on the course
- be able to designate the key data security controls used by companies.

Subject matters

- Data security controls used by companies
- Incident response
- Malware and analysis of malware
- Digital forensics in cybercrime investigation

Required performances

Participation in lectures and successful completion of exercises.

Assessment scale

The course will be graded as pass/fail.

Prerequisite studies

Compulsory:

Basic course in cybercrime investigation

Recommended:

Core Concepts in Digital Investigations and Forensics

12.17 Windows forensics (4 credits)

Description

The course introduces the methods in which the Windows operating system processes and stores data and how to search, interpret and utilise this data in cybercrime prevention.

Learning outcomes

After completion of the course, the student will:

- be able to perform digital forensic investigation tasks more precisely and securely than before
- be able to find the most important information sources in Windows environments
- know how to use the methods and techniques learned on the course in practical work
- know how to act in line with the basic digital forensic procedures in Windows environments

Subject matters

- Windows operating systems
- Windows registers
- NTFS and other file systems
- Office software
- RAM, pagefile, shadow copy
- Bitlocker and other encryption techniques

Required performances

Participation in lectures and successful completion of exercises.

Assessment scale

The course will be graded as pass/fail.

Prerequisite studies

Recommended:

Core Concepts in Digital Investigations and Forensics

12.18 NCFI Level 2 –courses (15 op)

Description

The Norwegian Police University College offers students having completed the Core Concepts in Digital Investigations and Forensics advanced studies of 15 credits, including:

- Module 2A Advanced Computer Forensics (15 credits)
- Module 2B Online Investigation (15 credits)
- Module 2C Network Forensics and Cybercrime (15 credits)
- Module 2D Mobile Extraction and Artifacts (15 credits)

These modules can be included in the elective studies in the specialization studies for cybercrime prevention.

[More detailed descriptions of the modules, learning outcomes, grading scale and admission criteria are presented on the website of The Norwegian Police University College](https://www.politihogskolen.no/en/post-graduate/nordic-computer-forensic-investigators)³.

³ <https://www.politihogskolen.no/en/post-graduate/nordic-computer-forensic-investigators>