MODULE DESCRIPTION CARD – SYLLABUS

This module is a part of the Intensive International Education Programs in the field of the … organised at Poznan University of Technology as part of the „IMPACT – Innowacyjne Międzynarodowe Programy w AI, Cyberbezpieczeństwie i Teleinformatyce" project implemented SPINAKER Program of the National Agency for Academic Exchange, financed by the European Social Development Fund 2021–2027 (ESDF).

Module name:	Number of hours:	Lecturer:
Digital Forensics	10	Michał Weissenberg, PhD

Module Descriptions:

The module introduces students to the foundations of digital forensics, including key concepts, methods, and tools used to acquire, preserve, analyze, and interpret digital evidence. It covers cybercrime basics, evidence handling procedures, memory and malware analysis, open-source intelligence (OSINT) techniques, and forensic methods for various operating systems and networks. Students will also explore current global cybersecurity threats, their geopolitical context, prevalence, trends, and societal impact. The course provides both theoretical knowledge and practical understanding of modern forensic challenges, ethical frameworks, and professional responsibilities.

Purpose of the support under Module:

The overall objective of the Innovative International Education Program in Cybersecurity within the IMPACT project is to raise the competencies of international students in key digital technologies and to support personalized, flexible, and modern education aligned with current global needs in the area of cybersecurity.

The specific purpose of this module is to equip students with essential competencies in digital forensics and cybersecurity, including:

- understanding digital evidence and forensic procedures,
- learning methods of collecting, processing, and analyzing digital artifacts,
- identifying and interpreting data from open sources (OSINT),
- analyzing current cyber-threats and understanding their impact on globally interconnected systems,
- developing awareness of the ethical, legal, and professional aspects of forensic investigations.

Method of support under Module:

Support within the module is provided with the participation of the instructor and divided into the following elements:

- 6-week self-study program using teaching materials provided by the instructor on the e-learning platform;
- 6 weeks of support from the instructor in the form of online consultations using tools that enable meetings to be held;

- a test to verify the acquisition of competences.

Module-related learning outcomes:

Descriptions of the new competences:

Participants gain new skills in digital forensics and cybersecurity, including knowledge of how to properly collect, analyse and interpret digital artefacts, apply open source intelligence techniques, and understand how modern cyber threats arise and evolve in a global connectivity environment. Students also develop an awareness of the ethical, legal and professional standards required in forensic investigations.

Knowledge:

1. Student has structured and theoretically grounded knowledge of key concepts in digital forensics, cybercrime, digital evidence handling, forensic procedures, and open source intelligence techniques.
2. Student understands development trends and modern achievements in computer science and cybersecurity, especially emerging forensic technologies, global cyber-threat landscapes, and current investigative challenges

Skills:

1. Student can critically assess and use information obtained from literature, online sources, and open-source intelligence in the context of digital forensics
2. Student is able to evaluate and apply new methods, tools, and technological solutions used in forensic investigations and cybersecurity, and understands their limitations
3. Student is able to independently continue learning in the field of digital forensics and to guide others in acquiring new competencies, keeping pace with evolving cyber-threats and forensic techniques

Social competences:

1. Student understands that knowledge in IT, cybersecurity, and digital forensics evolves rapidly, and therefore recognizes the need for continuous learning and skill development
2. Student demonstrates ethical and responsible behavior when handling sensitive information, personal data, or open-source material, and complies with the professional standards of forensic practice

Criteria for verifying learning outcomes

Learning outcomes are verified through an online single-choice test assessing the student's knowledge of digital forensics, OSINT methods, cyber-threats, evidence handling, and forensic procedures. The test checks both theoretical understanding and the ability to correctly interpret forensic concepts.

A minimum of 51% of correct answers is required to pass.

Method of verification/validation of learning outcomes

Verification is carried out using an online single-choice test delivered on the dedicated e-learning platform. The test is conducted individually, without access to supporting materials, and evaluates the extent to which the student has achieved the intended knowledge, skills, and social competences. The results are automatically recorded and validated according to predefined assessment criteria.

Workload

25 h (including work with teaching materials provided by the lecturer, consultation, and the student's own work) – 1 ECTS point

Level of the European Qualifications Framework