COURSE DESCRIPTION CARD - SYLLABUS

Course name
Computer forensics [S1Cybez1>INFŚ]

Course

Field of study
Cybersecurity

Year/Semester
2/4

Area of study (specialization)
–

Profile of study
general academic

Level of study
first-cycle

Course offered in
Polish

Form of study
full-time

Requirements
compulsory

Number of hours

Lecture
8

Laboratory classes
16

Other
0

Tutorials
0

Projects/seminars
0

Number of credit points

2,00

Coordinators

dr inż. Michał Weissenberg
michal.weissenberg@put.poznan.pl

Lecturers

Prerequisites

• Basic knowledge of information system security. • Familiarity with operating systems (Windows, Linux) at an advanced user level. • Understanding of the fundamentals of computer networks.

Course objective

The purpose of the course is to familiarize students with the methods and techniques used in digital forensics, including the collection, analysis, and interpretation of digital evidence. Students will learn to apply digital forensics tools in compliance with legal regulations and gain an understanding of the processes involved in cybercrime investigations.

Course-related learning outcomes

Knowledge:
• Knows the basic concepts and principles of digital forensics. [K1_W22]
• Understands the processes of collecting, securing, and analyzing digital evidence. [K1_W05]
• Understands the legal requirements for conducting investigative activities in a digital environment. [K1_W17]

Skills:
• Is able to identify and secure digital evidence in accordance with applicable standards. [K1_U03]
• Can diagnose problems and analyze them using IT tools. [K1_U09]
• Is able to solve forensic problems using selected IT tools.[K1_U02]
• Can prepare digital investigation reports suitable for use in legal proceedings. [K1_U04]

Social competences:
• Understands the importance of an ethical approach in digital forensics and adheres to the principles of confidentiality and data integrity.[K1_K05]
• Can collaborate effectively in a group, presenting findings in a clear and understandable manner.[K1_K05]
• Recognizes the significance of digital forensics and the societal risks posed by cybercrime.[K1_K03]

Methods for verifying learning outcomes and assessment criteria

Learning outcomes presented above are verified as follows:

Lecture:
The knowledge acquired in the lecture is verified by a test in (1) written or (2) oral form.
In the written form, students have to answer 3 - 5 questions (test and open) with different scoring.
In the oral form, the student first draws 2 topic groups from among the 3 main topics taken up in the lecture part, and then in each group draws 1 question. For each question drawn, the student may be asked an additional question (related to the question drawn). Assessment of the question (includes the answer to both the drawn question and the supplementary question) includes the range of answers and the depth of understanding of the topic.
Laboratory:
The skills acquired in the laboratory will be reviewed each time in class on the basis of assignments or projects involving the use of case study tools.
Grading scale for lecture and lab sections:
In both didactic forms a pass threshold of 50% of the possible points is adopted. The following grading scale applies: < 50% 2.0; 50%-59% 3.0; 60%-69% 3.5; 70%-79% 4.0; 80%-89% 4.5; 90%-100% 5.0
The course completion rules and the exact passing thresholds will be communicated to students at the beginning of the semester through the university’s electronic systems and during the first class meeting (in each form of classes).

Programme content

During the semester, students will learn fundamental concepts, definitions, and procedures in digital forensics, with a particular focus on cyber forensics. They will acquire both theoretical and practical knowledge of cybercrime, as well as methods for gathering and analyzing digital artifacts in criminal investigations. The course will present tools that support the identification, indexing, copying, and creation of digital fingerprints for digital evidence, as well as tools that enable the automation of digital evidence analysis. Students will gain knowledge of conducting forensic intelligence using digital forensics tools and will become familiar with the practical aspects of the forensics profession.

Course topics

1. Introduction to Digital Forensics
• Basic concepts and definitions
• The digital forensics process
• The role of digital forensics, including ethical and legal issues
2. Cybercrime
• Definitions and characteristics of cybercrime
• Specific environment and attack mechanisms
• Legal regulations and statistical data
3. Digital Forensics Tools
• Overview of tools
• Examination of fundamental tools: securing evidence, analysis, and presentation
4. Case Studies
• Analysis of specific incidents and criminal cases
• Event reconstruction

• Procedural practices
Laboratory classes will cover the practical aspects discussed in the lectures, including methods of securing evidence, data analysis, event reconstruction based on collected information, artifact analysis, and the preparation of reports.

Teaching methods

• Lectures with multimedia presentation and additional practical elements to discuss the application of IT tools in the form of case studies.
• Laboratories including exercises in the application of computer forensics tools based on instructions provided by the instructor and/or a project involving a case study.

Bibliography

Basic:
• Daren Hayes, “A Practical Guide to Digital Forensics Investigations”
• Joakim Karvestad, “Fundamentals of Digital Forensics. Theory, Methods, and Real-Life Applications”
• Gerard Johansen “Digital Forensics and Incident Response - Second Edition”

Additional:
• Casey, E. "Digital Evidence and Computer Crime", Academic Press, 2011.
• Sammons, J. "The Basics of Digital Forensics", Syngress, 2015.
• Industry reports, social organisations

Breakdown of average student's workload

	Hours	ECTS
Total workload	54	2,00
Classes requiring direct contact with the teacher	24	1,00
Student's own work (literature studies, preparation for laboratory classes/ tutorials, preparation for tests/exam, project preparation)	30	1,00