Introduction to Computer Forensics

Course description sheet

Basic information

Field of study Modern Technologies in Forensic Science **Major** - **Organisational unit** Faculty of Computer Science, Electronics and Telecommunications **Study level** First-cycle (engineer) programme **Form of study** Full-time studies **Profile** General academic	**Didactic cycle** 2026/2027 **Course code** INKTS.li2.08531.26 **Lecture languages** Polish **Mandatoriness** Obligatory **Block** Core Modules **Course related to scientific research** No

Course coordinator	Paweł Oberszt
Lecturer	Paweł Oberszt

Period	**Method of verification of the learning outcomes**	**Number of ECTS credits**
Semester 2	Exam **Activities and hours** Lectures: 30 Laboratory classes: 30	4

Goals

C1	To acquaint students with a wide range of technical issues touched by digital forensics.
C2	To provide knowledge of the basics of operating systems, file systems, computer networks, cryptography with a focus on digital forensics.

Course's learning outcomes

Code	Outcomes in terms of	Learning outcomes prescribed to a field of study	Methods of verification
Knowledge – Student knows and understands:			
W1	Zna konstrukcję systemów plików, pamięci i ruchu sieciowego w stopniu pozwalającym na ich analizę.	NKT1A_W04	Execution of laboratory classes
W2	Zna podstawowe artefakty w systemach Windows, Linux, macOS, Android i iOS.	NKT1A_W04	Execution of laboratory classes
Skills – Student can:			
U1	Potrafi przeprowadzić analizę dowodową w zakresie systemów plików, pamięci operacyjnej i ruchu sieciowego.	NKT1A_U04	Execution of laboratory classes
Social competences – Student is ready to:			
K1	Rozumie, jakie konsekwencje mogą mieć dane pozyskane w ramach analizy dowodowej.	NKT1A_K02	Examination

Student workload

Activity form	Average amount of hours* needed to complete each activity form
Lectures	30
Laboratory classes	30
Preparation for classes	20
Realization of independently performed tasks	25
Contact hours	5
Student workload	**Hours** 110
Workload involving teacher	**Hours** 60

* hour means 45 minutes

Program content

No.	Program content	Course's learning outcomes	Activities
1.	• Basics of cryptography. • Basics of operating systems. • Basics of computer networks. • Acquisition of digital evidence. • Artifacts on Windows, Linux, macOS. • Memory analysis. • File system analysis. • Network traffic analysis.	W1, W2, U1, K1	Lectures
2.	• Basics of cryptography. • Basics of operating systems. • Basics of computer networks. • Acquisition of digital evidence. • Artifacts on Windows, Linux, macOS. • Memory analysis. • File system analysis. • Network traffic analysis.	W1, W2, U1, K1	Laboratory classes

Extended information/Additional elements

Teaching methods and techniques :

Lectures, Case study, Flipped classroom, Project Based Learning, Problem Based Learning, E-learning, Gamification, Design thinking, Group work, Discussion

Activities	Methods of verification	Credit conditions
Lectures	Execution of laboratory classes, Examination	Receiving a positive exam grade
Lab. classes	Execution of laboratory classes, Examination	Receiving more than 50% of points from each laboratory AND receiving more than 50% of the sum of points from all laboratories AND receiving more than 50% of the test points (if it will be carried out in a given year).

Additional info

Classes conducted using innovative teaching methods developed during 2017-2019 in the POWR.03.04.00-00-D002/16 project, carried out by the Faculty of Computer Science, Electronics and Telecommunications under POWER 2014-2020.

Conditions and the manner of completing each form of classes, including the rules of making retakes, as well as the conditions for admission to the exam

- Laboratory: receiving more than 50% of points from each laboratory and receiving more than 50% of the sum of points from all laboratories and receiving more than 50% of the test points (if it is going to be carried out in a given year). Due to the nature of the course, it is not possible to attempt to pass it again within the retake period.
- Exam: no admission conditions, three pass attempts.

Method of determining the final grade

Weighted average of laboratory and exam grades.

Manner and mode of making up for the backlog caused by a student justified absence from classes

Students have to participate in laboratories on an ongoing basis. Failure to participate in the laboratory must be justified. Failure to join more than two laboratories without justification results in an entry „nb" at the end of the semester. If the absence is excused, it is possible to make up for it (maximum two absences).

Prerequisites and additional requirements

Students should:

- be familiar with Linux enough to navigate smoothly in the terminal and use advanced commands,
- be capable of writing scripts in Python.

Rules of participation in given classes, indicating whether student presence at the lecture is obligatory

1. Lecture: Students participate in the classes, learning about the next teaching content in accordance with the subject syllabus. Students should ask questions and explain doubts on a regular basis. Audio-visual recording of the lecture requires the consent of the lecturer.
2. Laboratory exercises: Students perform laboratory exercises in accordance with the materials provided by the teacher. The student is obliged to prepare for the subject of the exercise, which may be verified by an oral or written test. Completion of the course is based on the presentation of solutions to the problems posed.

Literature

Obligatory

1. Eoghan Casey, „Digital Evidence and Computer Crime: Forensic Science, Computers and the Internet." Academic Press, 2011.
2. Eoghan Casey, „Handbook of digital forensics and investigation." Elsevier Academic Press, 2010.
3. * Michael Hale Ligh & Andrew Case & Jamie Levy & Aaron Walters, „The Art of Memory Forensics." John Wiley and Sons, 214
4. Brian Carrier, „File System Forensic Analysis." Pearson Education, 2005.
5. Andrew S. Tanenbaum & Herbert Bos, „Modern Operating Systems: Fourth Edition." Pearson Education, 2015.
6. Charles M. Kozierok, „THE TCP/IP GUIDE. A Comprehensive, Illustrated Internet Protocols Reference." No Starch Press, 2005.

Learning outcomes prescribed to a field of study

Code	Content
NKT1A_K02	Ma świadomość roli społecznej oraz zawodowej absolwenta uczelni technicznej i ważności zachowania w sposób profesjonalny, przestrzegania zasad etyki zawodowej i dbałości o dorobek i tradycje zawodu oraz poszanowania różnorodności kultur. Ma także świadomość ważności i rozumie pozatechniczne aspekty i skutki działalności inżyniera, w tym jej wpływ na środowisko, i związaną z tym odpowiedzialność za podejmowane decyzje;
NKT1A_U04	Potrafi planować i przeprowadzać testy, eksperymenty i badania z dziedziny elektroniki, telekomunikacji i informatyki, w szczególności związane z analizą kryminlistyczną oraz analizą bezpieczeństwa, oparte na obliczeniach, symulacjach komputerowych i pomiarach.
NKT1A_W04	Ma uporządkowaną wiedzę na temat sieci teleinformatycznych, zasad adresacji, mechanizmów doboru tras; zna podstawowe pojęcia z zakresu przesyłania danych, zna rolę kodowania, modulacji i kryptografii, zna metody kodowania dźwięków, obrazów i tekstu w multimediach; w zakresie architektury komputerów, systemów i sieci komputerowych, baz danych oraz systemów operacyjnych, niezbędną do instalacji, obsługi i utrzymania narzędzi informatycznych służących do przetwarzania informacji; ma wiedzę na temat bezpieczeństwa komunikacji oraz bezpieczeństwa systemów operacyjnych