



COURSE DESCRIPTION CARD - SYLLABUS

Course name

Digital Forensics [S2Inf1E-CYB>DIGF]

Course

Field of study

Computing

Year/Semester

1/1

Area of study (specialization)

Cybersecurity

Profile of study

general academic

Level of study

second-cycle

Course offered in

English

Form of study

full-time

Requirements

compulsory

Number of hours

Lecture

15

Laboratory classes

0

Other

0

Tutorials

0

Projects/seminars

0

Number of credit points

1,00

Coordinators

dr inż. Michał Weissenberg

michal.weissenberg@put.poznan.pl

Lecturers

Prerequisites

The student starting this course should have basic knowledge of cybersecurity, ICT networks, and have basic programming skills. He should also have the ability to obtain information from the indicated sources. The student should demonstrate such qualities as honesty, responsibility, perseverance, cognitive curiosity, creativity, personal culture, respect for other people.

Course objective

1. Provide students with a theoretical foundation about digital forensic. 2. Familiarize students with the theoretical information about cybercrime, evidence, and data collecting. 3. Introducing students to typical tools used in digital forensics and methods of analyzing the most popular operating systems. 4. Show students the social, ethical, and legal aspects of cybercrime.

Course-related learning outcomes

Knowledge:

a student has structured and theoretically founded general knowledge related to key issues in the field of computer science, including analysis of operating systems. [k2st_w2]

a student has advanced detailed knowledge regarding selected it issues and their applications in digital

forensics. [k2st_w3]

a student knows development trends and the most important cutting-edge achievements in computer science, particularly in the area of digital forensics. [k2st_w4]

a student knows the basic programs and applications used to collect data and analyze them in the process of forensic investigation. [k2st_w6]

Skills:

a student is able to assess the usefulness and the possibility of using the information obtained in the literature analysis and available on the internet in the area of digital forensics. [k2st_u1]

a student is able to assess the suitability and the possibility of using new achievements (methods and tools) and new IT products in the field of digital forensics. [k2st_u6]

a student is able to assess the usefulness and the possibility of using and developing the basic tools used in digital forensics. [k2st_u8]

a student knows the basic concepts of digital forensics and is able to use them to describe the process of forensic proceedings. [k2_u12]

a student can define the stages of further acquisition of knowledge in the field of digital forensics, as well as obtain information on this subject and implement the process of self-education, including other people in this area. [k2_u16]

Social competences:

a student understands that in the field of IT, cybersecurity, and digital forensics the knowledge and skills quickly become obsolete. [k2st_k1]

a student understands the importance of using the latest knowledge in the field of computer science, cybersecurity, and digital forensics in solving research and practical problems. [k2st_k2]

a student understands the importance of popularization activities concerning the latest achievements in the field of digital forensics. [k2st_k3]

a student is aware of the need to develop professional achievements and comply with the rules of professional ethics. [k2st_k4]

Methods for verifying learning outcomes and assessment criteria

Learning outcomes presented above are verified as follows:

Learning outcomes presented above are verified as follows:

Lecture: knowledge is verified by a written and/or oral test. The pass mark is 51% of the points, and it is not allowed to use any auxiliary materials during the test.

Programme content

Lecture:

1. Introduction - concepts, definitions, and acts related to forensics.
2. Digital Forensics - presentation of what is digital forensics and digital artifacts.
3. Cybercrime and evidence - basic knowledge about cybercrime, incident response, collecting evidence, and analyzing data.
4. Collecting data - most important information about indexing, searching, cracking, and finding artifacts.
5. Tools - describing open-source and freeware tools.
6. Memory analysis and malware analysis.
7. Digital evidence on different operation systems.
8. Network forensics.

Course topics

Lecture:

1. Introduction - concepts, definitions, and acts related to forensics.
2. Digital Forensics - presentation of what is digital forensics and digital artifacts.
3. Cybercrime and evidence - basic knowledge about cybercrime, incident response, collecting evidence, and analyzing data.
4. Collecting data - most important information about indexing, searching, cracking, and finding artifacts.
5. Tools - describing open-source and freeware tools.

6. Memory analysis and malware analysis.
7. Digital evidence on different operation systems.
8. Network forensics.

Teaching methods

1. Lectures: multimedia presentation illustrated with examples.

Bibliography

Basic

J. Kavrestad, "Fundamentals of Digital Forensics: Theory, Methods, and Real-Life Applications", Springer, 2nd Edition, 2020

A. Arnes, "Digital Forensics", Willey, 2018

E. Casey, "Digital Evidence and Computer Crime", Academic Press, 3rd Edition, 2011

T. J. Holt, A. M. Bossler, K. C Seigfried-Spellar, "Cybercrime and Digital Forensics," Routledge, 2018.

Dz. U. 2018 poz. 1560, Ustawa z dnia 5 lipca 2018 r. o krajowym systemie cyberbezpieczeństwa

Additional

N. A. Hassan, "Digital Forensics Basics. A practical guide using Windows OS", Apress, 2019

W. Oettinger, "Learn Computer Forensics: a beginner's guide to searching, analyzing, and securing digital evidence", Packt Publishing, 2020

Breakdown of average student's workload

| | Hours | ECTS |
|-----------------------------------------------------------------------------------------------------------------------------------------|-------|------|
| Total workload | 25 | 1,00 |
| Classes requiring direct contact with the teacher | 15 | 0,50 |
| Student's own work (literature studies, preparation for laboratory classes/ tutorials, preparation for tests/exam, project preparation) | 10 | 0,50 |