University of Gdańsk

Subject card

Subject name and code	Digital Forensics, PG_00188512		
Field of study	Informatyka sądowa (Ćw.laboratoryjne)		
Date of commencement of studies	October 2026	Academic year of realisation of subject	2026/2027
Education level	Bachelor's studies	Subject group	Obligatory subject group in the field of study
Mode of study	full-time studies	Mode of delivery	at the university
Year of study	1	Language of instruction	Polish
Semester of study	2	ECTS credits	2.0
Learning profile	academic	Assessment form	credit
Conducting unit			
Name and surname of lecturer (lecturers)	Subject supervisor	dr inż. Stanisław Witkowski	
	Teachers		

Lesson types

Lesson type	Lecture	Tutorial	Laboratory	Project	Seminar	SUM
Number of study hours	0.0	0.0	30.0	0.0	0.0	30

E-learning hours included: 0.0

Learning activity and number of study hours

Learning activity	Participation in didactic classes included in study plan	Participation in consultation hours	Self-study	SUM
Number of study hours	30	5.0	15.0	50

Subject objectives

The primary goal of computer forensics is to provide digital evidence for legal proceedings. This involves collecting, retrieving, analyzing, and presenting digital data from various media (e.g., hard drives, mobile phones, cloud storage) to investigate crimes, abuses, or reconstruct the course of events. Key goals of computer forensics:
1. Data collection and recovery
2. Data analysis
3. Evidence provision
4. Support for legal authorities
5. Investigating abuses

Learning outcomes	Course outcome	Subject outcome	Method of verification
	[AKRL3_K05] The graduate is ready to promote science and raise social awareness in the field of forensic analytics.	The student is able to use the software he/she has learned to legally obtain information from the Internet.	[SK1] wypowiedź ustna/rozmowa/ dyskusja [SK2] prezentacja/projekt/referat/ raport [SK3] opracowanie tekstowe/ praca pisemna [SK5] realizacja zadania problemowego [SK8] obserwacja samodzielnej lub zespołowej pracy studenta
	[AKRL3_U06] The graduate is able to use specialised software and advanced ICT techniques to develop and visualise experimental data.	Is prepared to supplement his/her knowledge; is able to assess the degree of his/her understanding of the problem.	[SU1] wypowiedź ustna/rozmowa/ dyskusja [SU3] opracowanie tekstowe/ praca pisemna [SU5] realizacja zadania problemowego [SU6] demonstracja umiejętności praktycznych [SU8] obserwacja samodzielnej lub zespołowej pracy studenta
	[AKRL3_W08] The graduate knows and understands the application of information technologies in data analysis, interpretation of results, and reporting of forensic research.	The student knows and understands issues related to obtaining information from IT systems, as well as the legal regulations and standards that must be met in order to obtain information legally	[SW4] test/egzamin - ustny lub pisemny [SW1] wypowiedź ustna/rozmowa/ dyskusja [SW5] realizacja zadania problemowego

Subject contents	1. Introduction. Computer forensics and electronic evidence: definitions, concepts, and risks. Incident response based on the 27000 series of standards. Computer forensics processes and procedures. Computer forensics best practices. 2. Selected legal aspects Basic regulations and legal acts. Rights and obligations of experts. Expert opinions and private opinions. 3. Computer forensics workshop Blockers. Copying devices. Mobile devices. 4. Securing evidence Basic principles and preparation for securing media/data. Securing with blockers. Securing with mobile devices. Data security methodology. 5. Securing Linux systems. Using Linux computer forensics distributions. Introduction. Overview of the dd command. Basic presentation of the Sumuri Paladin/CAINE Linux distribution. 6. Introduction to FTK Imager Preparing to work with FTK Imager. Program overview. Creating a binary copy. Initial data selection, TRIAGE. 7. Introduction to Magnet Acquire Program overview. Creating a binary copy. Discussion of the differences in image file configuration options between FTK Imager and Magnet Acquire. 8. Introduction to Autopsy. Preparing and configuring the program. Creating a case. Disk image analysis. Reviewing image files and documents. 9. Alternative data streams in NTFS Basics Practical exercises 10. Forensic analysis of prepared evidence - independent exercises Working on prepared evidence. The student conducts basic forensic analysis based on previously acquired knowledge. 11. Securing and analyzing RAM images Introduction to Volatility Practical exercises 12. Live Forensic Preparing a mobile version of the Autopsy program Useful free software Practical exercises 13. Analysis of selected judicial norms and standards in Poland and the EU. 14. "Project" of a court case a) Creating a safe work environment.

b) Information acquisition techniques (state registers, web browsers, social networking sites, Deep Web).

c) Advanced data analysis techniques (metadata analysis, image analysis techniques, infrastructure analysis, deanonymization methods).

15. Final Test

Forensic computer experts can, among other things: retrieve deleted data from a computer; retrieve data hidden within a computer; detailedly analyze the operation of a computer and its system (i.e., determine all actions taken on a given computer, step by step); retrieve data from damaged media (crashed hard drives, flooded or burned computers, cell phones, etc.); recover deleted emails and text messages (including reconstructing their content); determine a computer user's internet usage history (e.g., to determine whether they accessed websites with prohibited content); analyze computer programs installed on a given computer (e.g., whether a given program has a valid license and determine its purpose); analyze the level of computer security to determine whether a computer has been hacked by an outsider, and if so, what actions they took on the compromised computer.

Prerequisites and co-requisites

Ability to search for information online.
Ability to identify the basic logic of events based on available materials.
Basic knowledge of cybersecurity and computer networks, and the ability to obtain information from identified sources.

Assessment methods and criteria

Subject passing criteria	Passing threshold	Percentage of the final grade
	50.0%	100.0%

Recommended reading

Basic literature

1. William Oettinger, Computer Forensics: Collecting, Analyzing, and Securing Electronic Evidence for Beginners, 2022, published by Helion S.A.

2. C. Altheide, H. Carvey, Computer Forensics: A Guide to Open Source Tools, Helion 2014

3. Journal of Laws of 2018, item 1560, Act of 5 July 2018 on the National Cybersecurity System

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

5. W. Oettinger, "Learn Computer Forensics: A Beginner's Guide to Searching, Analyzing, and Securing Digital Evidence," Packt Publishing, 2020

6. A. Chojnowski, Computer Forensics in Practice. Published by Helion, 2020

Supplementary literature

1. C. Altheide, H. Carvey, Computer Forensics. A Guide to Open Source Tools, Gliwice 2014
2. A. Kalinowski, Surveillance Methods and Elements of Computer Forensics, Kwidzyn 2013
3. H. Carvey, Forensic and Post-Compromise Analysis. Advanced Techniques for Analysis in Windows, Gliwice 2013
4. M. SZMIT, Elements of Forensic Computer Science, Polish Information Processing Society 2011

eResources addresses

Example issues/ example questions/ tasks being completed	1. How to determine if a storage device contains files named ABC? 2. How to determine if a storage device contains files containing the words XYZ? 3. How to determine if a storage device contains files such as Office files, multimedia files, or graphics files. 4. How to determine if data from a storage device has been deleted, erased, modified, copied, saved to external media, transferred to another location, or sent via electronic communication channels. 5. How to determine when the operating system currently stored on the storage device was installed. 6. How to determine if a hard drive was formatted, and if so, when and by which user. 7. How to determine if email correspondence was sent via the computer from the account of user Jan Kowalski. 8. How to determine if an email inbox contains email correspondence sent and received from user Jan Nowak. 9. How to determine if an email inbox contains attachments indicating content XYZ. 10. How to determine if the email correspondence history contains content indicating the theft of trade secret data. 11. How to determine if email correspondence contains files indicating the inspector's failure to comply with occupational health and safety procedures? 12. How to determine if a file called a database is among the data deleted from a storage device? 13. How to determine if a computer contains pornographic files? 14. How to determine if a user has used a computer to visit websites related to ABC? 15. How to determine if a user has logged into the ABC portal or application using a computer? 16. Do the IT system logs contain information indicating the forgery of patient records? 17. How to determine if a phone contains text messages from the 123 number? 18. How to determine if the call history (including the deleted one) contains calls to the 123 number? 19. How to determine if the text message history contains content of a persistent harassment nature, i.e., stalking? 20. How to extract data on frequently asked questions.
Work placement	Not applicable

Document generated electronically. Does not require a seal or signature.