COURSE DESCRIPTION CARD - SYLLABUS

Course name
Multimedia Cyberforensics [S1Cybez1>CMm]

Course

Field of study
Cybersecurity

Year/Semester
3/6

Area of study (specialization)
–

Profile of study
general academic

Level of study
first-cycle

Course offered in
Polish

Form of study
full-time

Requirements
elective

Number of hours

Lecture
16

Laboratory classes
16

Other
0

Tutorials
0

Projects/seminars
16

Number of credit points

3,00

Coordinators

dr inż. Sławomir Maćkowiak
slawomir.mackowiak@put.poznan.pl

Lecturers

Prerequisites

The student should have basic knowledge of multimedia technologies, including audiovisual data analysis and processing. Familiarity with fundamental concepts of computer science, such as computer system architecture and computer networks, as well as knowledge of tools used for digital data analysis, is also required. An additional advantage would be the ability to interpret metadata, identify manipulations in multimedia materials, and understand basic procedures related to conducting forensic investigations in a digital environment.

Course objective

The aim of the course Multimedia Cyberforensics is to familiarize students with methods and tools used in the analysis and verification of multimedia data in a forensic context. The course is designed to develop skills in identifying and analyzing audiovisual materials, including detecting manipulations, recovering hidden data, and analyzing metadata. Students will acquire both theoretical and practical knowledge of using information technology in the investigation of digital evidence, with an emphasis on its application in legal and investigative processes.

Course-related learning outcomes

Knowledge:
K1_W05: Possesses advanced knowledge of complex data structures; understands the fundamentals of theory, principles of data administration, and related standards; is familiar with cybersecurity and privacy principles used to manage risks associated with the utilization, processing, storage, and transmission of information or data.
K1_W07: Has in-depth knowledge of the lifecycle, design, and use of attack-resistant software systems; understands their principles of operation; is familiar with tools used to identify vulnerabilities in communication software and understands the impact of software configuration on security.
K1_W11: Understands the principles of data concealment, such as cryptography and steganography; possesses advanced knowledge of cryptography, cryptographic algorithms, their limitations, and their role in cybersecurity.

Skills:
K1_U03: Is able to plan and conduct tests of software, systems, and computer networks to identify vulnerabilities to attacks and can propose solutions to improve operational security.
K1_U05: When formulating and solving engineering tasks in the field of cybersecurity, is able to use known mathematical models, algorithms, as well as simulation, experimental, and analytical methods.
K1_U09: Is capable of performing a critical analysis and evaluation of the functionality of existing solutions in software, data processing, and computer systems and networks using appropriately selected methods and tools.
K1_U10: Based on available documentation, specifications, and standards, is able to design and implement a secure web or mobile application using high-level programming languages.
K1_U11: Using technical documentation, applicable standards, appropriate methods, tools, and components, is able to build, configure, and launch a typical system or computer network that meets cybersecurity requirements.

Social competences:
K1_K01: Understands the importance of enhancing professional, personal, and social competencies; is aware that knowledge and skills in the field of cybersecurity evolve rapidly.
K1_K02: Recognizes the significance of knowledge in solving cybersecurity problems; is aware of the necessity to rely on expert knowledge when addressing engineering tasks that exceed their own competencies.
K1_K03: Understands the need to formulate and communicate information and opinions to society about the positive and negative aspects of cybersecurity and is ready to act in the public interest.
K1_K05: Is aware of the importance of individual work and the necessity to adhere to professional ethics; is prepared to follow teamwork principles, take responsibility for shared tasks, and preserve the achievements and traditions of the profession.

Methods for verifying learning outcomes and assessment criteria

Learning outcomes presented above are verified as follows:

1. Lecture
Problem-solving task: Case studies requiring teamwork to analyze and resolve problems. Assessment of collaboration skills, setting priorities, and proposing effective solutions. Evaluation of critical thinking, problem-solving abilities, and team dynamics.
The passing threshold is 50% of the total points.
In the case of written and oral assessments, points are combined.
Grading scale:
• <50% - 2.0 (fail);
• 50% to 59% - 3.0 (pass);
• 60% to 69% - 3.5 (satisfactory+);
• 70% to 79% - 4.0 (good);
• 80% to 89% - 4.5 (good+);
• 90% to 100% - 5.0 (very good).
2. Laboratory
Skills acquired in the laboratory are assessed based on reports (documentation) of completed laboratory exercises (OL) and a final assessment (ZK), which takes the form of an independently executed exercise or project.
Social competencies (KS) are evaluated based on the ability to actively listen, collaborate, and effectively participate in team discussions, as well as the level of engagement in problem-solving processes.

A weighted average is calculated:
OK = 0.5 x OL + 0.3 x ZK + 0.2 x KS, and grades are assigned as follows:
• 5.0 for OK > 4.75;
• 4.5 for 4.75 > OK > 4.25;
• 4.0 for 4.25 > OK > 3.75;
• 3.5 for 3.75 > OK > 3.25;
• 3.0 for 3.25 > OK > 2.75;
• 2.0 for OK < 2.75.
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

The course introduces students to techniques for analyzing digital multimedia in the context of detecting manipulations and forgeries, recovering hidden data, and examining the authenticity and integrity of multimedia files. It offers an in-depth exploration of methods and tools used in digital trace analysis, particularly focusing on images, video sequences, and audio.

Course topics

Students will learn how to extract critical information from metadata, such as geolocation, timestamps, technical attributes, and other details that may reveal potential manipulations or unusual changes, which are essential in forensic investigations.
A significant part of the course focuses on detecting manipulations and forgeries, with an emphasis on digital images and video sequences. Techniques for identifying edits, such as splicing, shadow modifications, compression level adjustments, and multiple JPEG compressions, will be covered. Students will learn how various manipulations affect file structures and how they can be detected using specialized tools and techniques. The course also includes the application of histogram, gradient, and texture analysis to identify changes and visual inconsistencies.
Another integral part of the course is the recovery and analysis of hidden data in multimedia. Students will explore steganographic techniques and methods for retrieving information embedded within multimedia files. Topics include data hiding in images, audio, and video, as well as methods for detecting and decrypting such information. Participants will gain insight into techniques for identifying unusual structures and inconsistencies in multimedia formats, which may indicate the presence of hidden data or nested archives.
The final module of the course focuses on tools for forensic audio and video analysis. Students will investigate how audio and video formats can be examined for manipulations, hidden signals, and integrity issues. The course introduces spectral analysis techniques and methods for detecting changes resulting from editing and compression, as well as basic tools used in forensic audio and motion picture analysis. Additionally, technical aspects related to file formats, codecs, and tools supporting multimedia analysis and processing will be discussed.
The course combines theory with practice to equip participants with the skills necessary for independent multimedia analysis in a forensic context. Upon completion, students will be able to identify and analyze various manipulations and retrieve critical information to support digital investigations.
Practical laboratory sessions include:
• Metadata analysis and its role in forensics
• Detection of manipulations and forgeries in multimedia
• Recovery and analysis of hidden data in multimedia
• Tools for forensic audio and video analysis

Teaching methods

• Active Learning Techniques: Strategies such as group discussions, problem-solving, and case studies to actively engage students in the learning process. Encouraging collaborative learning and interaction to foster critical thinking and the practical application of knowledge.
• Technology Integration: Utilizing technological tools and platforms to enhance learning quality. Leveraging online collaboration tools during brainstorming sessions, virtual simulations for problem-solving, and multimedia presentations to deliver engaging content. Additionally, using online discussion forums or learning management systems for asynchronous learning and resource sharing.

• Case-Based Learning: Incorporating real-world case studies into lectures and labs to demonstrate the practical application of creative thinking in solving technical problems. This approach encourages students to analyze and discuss cases, identify creative solutions, and reflect on decision-making processes.
• Feedback and Peer Teaching: Introducing mechanisms for student feedback, where learners provide constructive critiques of their peers' problem-solving approaches or project solutions. Encouraging peer-teaching sessions where students can share their knowledge and creative techniques with classmates.
• Project-Based Learning: Embedding project-based learning into the curriculum, where students tackle real-world problems or design challenges requiring creative thinking. This approach enables them to apply their skills, conduct in-depth research, and develop innovative solutions through hands-on, experiential learning.
• Online lectures

Bibliography

Basic:
• A. E. Hassanien, M. M. Fouad, A. A. Manaf, M. Zamani, R. Ahmad, and J. Kacprzyk, Multimedia Forensics, Singapore: Springer, 2021. DOI: 10.1007/978-981-16-7621-5.
• A. T. S. Ho and S. Li (Eds.), Handbook of Digital Forensics of Multimedia Data and Devices, Hoboken, NJ, USA: Wiley, 2015. DOI: 10.1002/9781118757079.

Additional:
• A. E. Hassanien, M. M. Fouad, A. A. Manaf, M. Zamani, R. Ahmad, and J. Kacprzyk (Eds.), Multimedia Forensics and Security: Foundations, Innovations, and Applications, Cham, Switzerland: Springer, 2016. DOI: 10.1007/978-3-319-44270-9.
• S. Li and K. A. Renaud (Eds.), Handbook of Research on Multimedia Cyber Security, Hershey, PA, USA: IGI Global, 2020. DOI: 10.4018/978-1-7998-4311-1.

Breakdown of average student's workload

	Hours	ECTS
Total workload	88	3,00
Classes requiring direct contact with the teacher	48	1,50
Student's own work (literature studies, preparation for laboratory classes/ tutorials, preparation for tests/exam, project preparation)	40	1,50