SYLLABUS

1. Data about the program of study

1.1 Institution	The Technical University of Cluj-Napoca
1.2 Faculty	Faculty of Automation and Computer Science
1.3 Department	Computer Science
1.4 Field of study	Computer Science and Information Technology
1.5 Cycle of study	Masters
1.6 Program of study / Qualification	Cybersecurity Engineering / Masters
1.7 Form of education	Full time

2. Data about the subject

2.1 Subject name	***Digital Forensics and Incident Response***			Subject code	**11**
2.2 Course responsible / lecturer	Dr. eng. Lutas Dan - dan.lutas@cs.utcluj.ro				
2.3 Teachers in charge of seminars / Laboratory / project	Dr. eng. Lutas Dan - dan.lutas@cs.utcluj.ro				
2.4 Year of study	II	2.5 Semester	1	2.6 Type of assessment (E - exam, C - colloquium, V – verification)	E
2.7 Subject category	Formative category: DF – fundamental, DS – speciality, DC – complementary				DS
	Optionality: DOB – mandatory, DOP – optional (alternative), DFA – optional (free choice)				DOB

3. Estimated total time

3.1 Number of hours per week	3	of which:	Course	2	Seminars	-	Laboratory	1	Project	-
3.2 Number of hours per semester	42	of which:	Course	28	Seminars	-	Laboratory	14	Project	-
3.3 Individual study:										
(a) Manual, lecture material and notes, bibliography										30
(b) Supplementary study in the library, online and in the field										18
(c) Preparation for seminars/laboratory works, homework, reports, portfolios, essays										33
(d) Tutoring										-
(e) Exams and tests										2
(f) Other activities:										-

3.4 Total hours of individual study (suma (3.3(a)…3.3(f)))	83
3.5 Total hours per semester (3.2+3.4)	125
3.6 Number of credit points	5

4. Pre-requisites (where appropriate)

4.1 Curriculum	Information Security, Reverse Engineering and Malware Analysis
4.2 Competence	Computer Architecture, Operating Systems Architecture, Basic knowledge about computer networks

5. Requirements (where appropriate)

5.1. For the course	blackboard, beamer, computers
5.2. For the applications	blackboard, beamer, computers

6. Specific competence

6.1 Professional competences	• implement ICT recovery system • identify ICT security risks • perform risk analysis • establish an ICT security prevention plan • implement ICT security policies • ensure compliance with legal requirements • ensure information privacy • monitor developments in field of expertise • keep up with the latest information systems solutions
6.2 Cross competences	• develop an analytical approach • taking a proactive approach • developing strategies to solve problems • being open minded

7. Expected Learning Outcomes

Knowledge	The student has knowledge of: • digital systems • information security strategy • ICT network security risks • cyber attack counter-measures • operating systems • system backup best practices • computer forensics • cyber security • information confidentiality • attack vectors • security threats
Skills	The student is able to: • interpret technical texts • keep up with the latest information systems solutions • address problems critically • implement ICT security policies • protect personal data and privacy • remove computer viruses or malware • respond to incidents • collect cyber defence data • communicate with stakeholders • create incident reports • engage with stakeholders • handle cybersecurity incidents
Responsibilities and autonomy	The student has the ability to work independently in order to: • develop an analytical approach • take a proactive approach • develop strategies to solve problems • be open-minded

8. Discipline objective (as results from the *key competences gained*)

8.1 General objective	Familiarizing students with basic knowledge about the process of responding to security incidents, understanding the activities needed for preparing and organizing the incident response, understanding what, how and when certain events happened during an incident, responding in an optimal manner to reduce the effects of the incident, and developing procedures for preventing similar future incidents.

	Gaining the needed knowledge for a deep technical analysis of the incident by investigating (identifying, collecting, and analysing) digital artefacts that resulted during the incident.
8.2 Specific objectives	1. Understanding the steps needed to plan the incident response activity (team organization, role of each member, necessary competencies, interactions between members and team interaction with other teams of an organization). 2. Developing knowledge about specific tools needed for preventing security incidents (e.g. patch management, log monitoring etc). 3. Developing knowledge about specific incident response tools used in a security incident analysis. 4. Developing knowledge about the inner workings and advanced usage of specific tools used in different types of digital investigations (disk analysis, volatile memory analysis, network traffic capturing and analysis, database forensics etc). 5. Understanding techniques used to evade or impair the activity of digital forensics (such as disk encryption, preventing the volatile memory analysis etc).

9. Contents

9.1 Lectures	Hours	Teaching methods	Notes
Legal aspects, handling digital evidence, limitations (steganography, metadata)	2	Blackboard illustrations and explanations, beamer presentations, discussions, short challenges.	
Collecting digital evidence using hardware methods, tools for hardware inspection	2		
Handling security incidents (response procedures : identification, verification, prioritization, isolation, eradication, recovery)	2		
Disk and file-system analysis (1) : details about NTFS, FAT, EXT3 etc	2		
Disk and file-system analysis (2) : digital forensics tools	2		
The Registry in Windows OS : structure, types of information, tools for analysing	2		
Memory dump analysis (1) : creating a memory dump, Volatility framework	2		
Memory dump analysis (2) : searching for advanced malware, rootkits etc	2		
Network traffic analysis using Wireshark : examining different types of attacks, extracting data from network packets for attack reconstruction	2		
Creating malware/attack signatures for IDS/IPS : introduction to Snort, analysing and developing Snort signatures	2		
Event correlation : tools for log processing on Windows/Linux, specific types of logging, timestamps	2		
Digital investigations on mobile devices: Android, open/closed tools	2		
Database forensic investigations	2		
Impairing digital investigation tools : safe delete, full disk encryption, preventing memory acquisition	2		

Bibliography

- Incident Response and Computer Forensics (Prosise, Chris – 2014 – McGraw-Hill) (3nd ed)
- Blue Team Handbook: Incident Response Edition: A condensed field guide for the Cyber Security Incident Responder (Murdoch, Don – 2014 – CreateSpace Independent Publishing)
- File System Forensic Analysis (Carrier, Brian – 2005 – Addison-Wesley)
- The Practice of Network Security Monitoring: Understanding Incident Detection and Response (Bejlitch, Richard – 2013 – No Strach Press)
- The Art of Memory Forensics: Detecting Malware and Threats in Windows, Linux, and Mac Memory (Ligh, Michael Hale – 2014 – Wiley)
- Placing the Suspect Behind the Keyboard: Using Digital Forensics and Investigative Techniques to Identify Cybercrime Suspects (Shavers, Brett – 2013 – Syngess)

9.2 Applications - Seminars/Laboratory/Project	Hours	Teaching methods	Notes

Tools and techniques for hardware inspection	1	Brief reviews, blackboard illustrations and explanations, tutorials, roadmaps, short live demos and guidance of code development, discussions, homework.	
Tools and techniques for inspecting the file-system	1		
Tools and techniques for Registry analysis on Windows OS, analysing a memory dump, using Windbg	1		
Analysing network traffic/packets using Wireshark, studying different IDS, IPS solutions. Applications.	1		
Tools and techniques for log analysis. Event correlation	1		
Tools and techniques for analysing mobile devices and databases	1		
Tools and techniques for impairing digital forensics	1		

Bibliography

- Incident Response and Computer Forensics (Prosise, Chris – 2014 – McGraw-Hill) (3nd ed)
- Blue Team Handbook: Incident Response Edition: A condensed field guide for the Cyber Security Incident Responder (Murdoch, Don – 2014 – CreateSpace Independent Publishing)
- File System Forensic Analysis (Carrier, Brian – 2005 – Addison-Wesley)
- The Practice of Network Security Monitoring: Understanding Incident Detection and Response (Bejlitch, Richard – 2013 – No Strach Press)
- The Art of Memory Forensics: Detecting Malware and Threats in Windows, Linux, and Mac Memory (Ligh, Michael Hale – 2014 – Wiley)
- Placing the Suspect Behind the Keyboard: Using Digital Forensics and Investigative Techniques to Identify Cybercrime Suspects (Shavers, Brett – 2013 – Syngess)

10. Bridging course contents with the expectations of the representatives of the community, professional associations and employers in the field

Achieved through periodic discussions with the representatives of significant employers, mainly companies that have projects in information security.
Digital Forensics and Incident Response disciplines are present in many similar master programs in computers and information security, like :
• CS6963 Digital Forensics, Masters in Cybersecurity, New York Polytechnic School of Engineering, New York, USA, http://engineering.nyu.edu/academics/course/CS6963
• CSEC 661 Digital Forensics Investigation, Master of Science in Digital Forensics and Cyber Investigation, University of Maryland University College, USA, http://www.umuc.edu/academic-programs/masters-degrees/digital-forensics-and-cyber-investigations.cfm
• Masters in Computer Forensics, University of Westminster, UK,
http://www.westminster.ac.uk/courses/subjects/computer-science-and-software-engineering/postgraduate-courses/full-time/p09fpcfs-msc-computer-forensics

11. Evaluation

Activity type	Assessment criteria	Assessment methods	Weight in the final grade
Course	Ability to to define concepts and methods and solve problems specific to the Digital Forensics and Incident Response domain. Attendance frequency, interest, and interactivity during lecture classes.	**Summative evaluation** consisting in a written exam and/or multiple-choice questions on Moodle and/or giving a presentation about a topic studied during the lectures.	60%
Laboratory	Ability to solve problems specific to the Digital Forensics and Incident Response domain. Attendance frequency, interest, and interactivity during lab classes.	**Summative evaluation** consisting in completion of practical activities, on-time submission of homework and/or solving specific problems in a practical exam.	40%

Minimum standard of performance:
Course: Attendance to minimum 50% of lecture to be admitted to the final exam.
Students must prove understanding of basic knowledge about the activity of incident response, such as the need for planning the incident response activity, incident response team members and their responsibilities and needed

competencies, incident analysis. Students must prove understanding of basic knowledge about digital forensics, such as specific types of digital forensics (disk, memory, network), evidence handling, methods for preventing and rapid detection of security incidents. Demonstrated understanding regarding the limitations of digital forensics techniques.
Laboratory: Attendance to 100% of classes (1 class can be recovered during the semester and a second one during the re-examination interval) to be admitted to the final exam. Students must prove practical abilities to understand, analyse and reconstruct, based on digital artefacts (disk and/or memory images, network traffic capture) analysis the steps performed by an attacker during a security incident.

Date of filling in: 29.04.2026	**Responsible**	**Title First name Last name**	**Signature**
	Course	Dr. eng. Dan Horea LUȚAȘ	
	Applications	Dr. eng. Dan Horea LUȚAȘ	

Date of approval in the department	Head of department, Prof.dr.eng. Rodica Potolea
Date of approval in the Faculty Council	Dean, Prof.dr.eng. Vlad Mureșan