

## COURSE SYLLABUS

Academic year 2025 - 2026

### 1. Programme Information

1.1. Higher education institution	Lucian Blaga University of Sibiu
1.2. Faculty	Faculty of Science
1.3. Department	Mathematics and Informatics
1.4. Field of study	Informatics
1.5. Level of study <sup>1</sup>	Master
1.6. Programme of study/qualification	Cybersecurity

### 2. Course Information

2.1. Name of course	Digital Forensics	Code	FSTI.MAI.CS.M.SO .4.2020.E-7.3
2.2. Course coordinator	Professor PhD. Remus Brad		
2.3. Seminar/laboratory coordinator	Professor PhD. Remus Brad		
2.4. Year of study <sup>2</sup>	2	2.5. Semester <sup>3</sup>	2
2.6. Evaluation form <sup>4</sup>	E		
2.7. Course type <sup>5</sup>	R	2.8. The formative category of the course <sup>6</sup>	S

### 3. Estimated Total Time

3.1. Course Extension within the Curriculum – Number of Hours per Week				
3.1.a. Lecture	3.1.b. Seminar	3.1.c. Laboratory	3.1.d. Project	Total
2		2		4
3.2. Course Extension within the Curriculum – Total Number of Hours within the Curriculum				
3.2.a. Lecture	3.2.b. Seminar	3.2.c. Laboratory	3.2.d. Project	Total <sup>7</sup>
24		24		48
<b>Time Distribution for Individual Study<sup>8</sup></b>				<b>Hours</b>
Learning by using course materials, references and personal notes				40
Additional learning by using library facilities, electronic databases and on-site information				30
Preparing seminars / laboratories, homework, portfolios, and essays				30
Tutorial activities <sup>9</sup>				13
Exams <sup>10</sup>				6
<b>3.3. Total Individual Study Hours<sup>11</sup> (NOI<sub>sem</sub>)</b>				<b>119</b>
<b>3.4. Total Hours in the Curriculum (NOAD<sub>sem</sub>)</b>				<b>56</b>
<b>3.5. Total Hours per Semester<sup>12</sup> (NOAD<sub>sem</sub> + NOI<sub>sem</sub>)</b>				<b>175</b>
<b>3.6. No. of Hours / ECTS</b>				<b>25</b>
<b>3.7. Number of credits<sup>13</sup></b>				<b>7</b>

#### 4. Prerequisites (if needed)

4.1. Courses that must be successfully completed first (from the curriculum) <sup>14</sup>	-
4.2. Competencies	-

#### 5. Conditions (where applicable)

5.1. For course/lectures <sup>15</sup>	Classroom, equipped with blackboard, computer, video projector and software
5.2. For practical activities (lab/sem/pr/app) <sup>16</sup>	Laboratory room equipped with computers

#### 6. Learning Outcomes<sup>17</sup>

Number of credits assigned to the discipline: 7				
Learning outcomes				Credit distribution by learning outcomes
Nr. crt.	Knowledge	Skills	Responsibility and autonomy	
LO 1	The student explains the fundamentals of digital forensics, the principles of evidence handling, and legal and ethical considerations.	The student applies proper procedures for collecting and preserving digital evidence.	The student demonstrates responsibility in complying with legal standards and adopts an ethical conduct in investigations.	1.5
LO 2	The student describes investigation methods for computer systems, mobile devices, cloud environments, and mobile applications.	The student recovers, analyzes, and interprets digital data from various storage media and applications.	The student shows autonomy in using forensic tools and assumes responsibility for the accuracy of results.	2.5
LO 3	The student understands techniques of network forensics and incident response.	The student identifies suspicious activities in network traffic and applies incident response procedures.	The student assumes responsibility for accurate incident documentation and complies with best practices in investigation.	1.5
LO 4	The student explains the role of forensic reporting and presentation in investigations and court.	The student prepares forensic reports and presents digital evidence in legal contexts.	The student shows high responsibility as an expert witness and complies with professional standards.	1.5

#### 7. Course objectives (resulted from developed competencies)

7.1. Main course objective	Acquiring and understanding the necessary notions to analyse different types of cyber crimes and offer solution for prevention in this way.
7.2. Specific course objectives	Accumulating knowledge related to the basic rules for securing hardware and software systems, consulting advice, forensic preservations of digital devices and detecting mistakes in the design of information security architectures.

#### 8. Content

8.1. Lectures <sup>18</sup>	Teaching methods <sup>19</sup>	Hours
-----------------------------	--------------------------------	-------

Introduction to digital forensics. Fundamentals of digital forensics, including the principles of evidence handling, the legal and ethical considerations of digital forensics, and the types of digital crimes that may require forensic investigation	Lecture, use of video projector, discussions with students	4
Computer and mobile device forensics. Investigation of computer and mobile device storage media, including the recovery of deleted files, file carving, and file system analysis	Lecture, use of video projector, discussions with students	4
Network forensics. Investigation of network traffic to identify suspicious activity	Lecture, use of video projector, discussions with students	4
Cloud forensics. Investigation of data stored in cloud environments	Lecture, use of video projector, discussions with students	4
Mobile application forensics. Investigation of mobile applications, including the analysis of application data, network traffic, and memory forensics	Lecture, use of video projector, discussions with students	4
Incident response and cybercrime investigation. Procedures and protocols for responding to security incidents, including incident reporting, incident response planning, and the collection of digital evidence. Legal considerations of cybercrime investigation and the role of digital forensics in supporting criminal investigations	Lecture, use of video projector, discussions with students	4
Forensic reporting and presentation. Techniques for reporting and presenting digital forensic findings, preparation of expert witness testimony and the use of tools for presenting digital evidence in court	Lecture, use of video projector, discussions with students	4
<b>Total lecture hours:</b>		<b>28</b>

<b>8.2. Practical activities</b> (8.2.a. Seminar <sup>20</sup> / 8.2.b. Laboratory <sup>21</sup> / 8.2.c. Project <sup>22</sup> )	<b>Teaching methods</b>	<b>Hours</b>
Disk imaging and analysis. How to create forensic images of digital storage media, including hard drives, solid-state drives, and USB drives. How to analyze the images using tools like Autopsy and EnCase, and how to recover deleted files and data	Use of video projector, discussions with students	4
Tools such as EnCase and FTK for forensic analysis	Use of video projector, discussions with students	4
Use of network monitoring tools and packet analysis tools such as Wireshark	Use of video projector, discussions with students	4
Forensic tools for cloud services, Amazon Web Services (AWS) and Microsoft Azure	Use of video projector, discussions with students	4
Tools for mobile application analysis, Frida and Hopper	Use of video projector, discussions with students	4
Memory forensics: How to investigate the memory of a running computer or mobile device to uncover evidence of digital crimes. Memory analysis tools like Volatility and Rekall to extract data from memory, and how to analyze the data to uncover evidence of cyber attacks	Use of video projector, discussions with students	4
Incident response and forensics: How to respond to security incidents, including incident reporting, incident response planning, and digital forensics. Incident response tools, such as SIEM and log analysis tools, to detect and respond to cyber attacks	Use of video projector, discussions with students	4
<b>Total seminar/laboratory hours:</b>		<b>28</b>

## 9. Bibliography

9.1. Recommended Bibliography	<ol style="list-style-type: none"> <li>1. M.T. Britz, Computer Forensics and Cyber Crime, Pearson 2017</li> <li>2. EC Council, Computer Forensics Investigating Network Intrusions &amp; Cyber Crime, 2020</li> <li>3. H. Jahankhani, Cyber Criminology, Springer 2018</li> <li>4. S. Parkinson, A. Crampton, R. Hill, Guide to Vulnerability Analysis for Computer Networks and Systems, Springer 2021</li> </ol>
a. Additional Bibliography	<ol style="list-style-type: none"> <li>1. J. Grand, R. Russel, Hardware Hacking, Syngress 2004</li> <li>2. An Introduction to Computer Security, NIST 2017</li> <li>3. L. Ayala, Cybersecurity Lexicon, Apress 2016</li> <li>4. The Complete Internet Security Manual, BDiTS 2019</li> <li>5. K. Mitnick, The art of invisibility, IKP 2017</li> <li>6. C. Hadnagy, Social Engineering: The Science of Human Hacking, Wiley 2018</li> </ol>

## 7. Conjunction of the discipline's content with the expectations of the epistemic community, professional associations and significant employers of the specific study program<sup>23</sup>

It is done through regular contacts with the representatives of the companies. Cybersecurity topic is actual and is of great interest in existing software companies on the local, national and global market.

## 8. Evaluation

Activity Type	11.1 Evaluation Criteria	11.2 Evaluation Methods		11.3 Percentage in the Final Grade	Obs. <sup>24</sup>
11.4a Exam / Colloquy	• Theoretical and practical knowledge acquired (quantity, correctness, accuracy)	Tests during the semester <sup>25</sup> :	%	50% (minimum 5)	CEF
		Homework:	%		
		Other activities <sup>26</sup> :	%		
		Final evaluation:	50%		
11.4b Seminar	• Frequency/relevance of participation or responses	Evidence of participation, portfolio of papers (reports, scientific summaries)		5% (minimum 5)	nCPE
11.4c Laboratory	• Knowledge of the equipment, how to use specific tools; evaluation of tools, processing and interpretation of results	• Written questionnaire • Oral response • Laboratory notebook, experimental works, reports, etc. • Practical demonstration		5% (minimum 5)	nCPE
11.4d Project	• The quality of the project, the correctness of the project documentation, the appropriate justification of the chosen solutions	• Self-evaluation, project presentation • Critical evaluation of a project		40% (minimum 5)	nCPE
11.5 Minimum performance standard <sup>27</sup> To pass the exam, the candidate must have a basic knowledge of the digital forensics					

**The Course Syllabus will encompass components adapted to persons with special educational needs (SEN – people with disabilities and people with high potential), depending on their type and degree, at the level of all curricular elements (skills, objectives, contents, teaching methods, alternative assessment), in order to ensure fair opportunities in the academic training of all students, paying close attention to individual learning needs.**

Filling Date: | 1 | 5 | / | 0 | 9 | / | 2 | 0 | 2 | 5 |

Department Acceptance Date: | 3 | 0 | / | 0 | 9 | / | 2 | 0 | 2 | 5 |



	Academic Rank, Title, First Name, Last Name	Signature
Course Teacher	Professor PhD. Remus Brad	
Study Program Coordinator	Associated Professor PhD. Nicolae Constantinescu	
Department Head	Professor PhD. Mugur Acu	

<sup>1</sup> Bachelor / Master

<sup>2</sup> 1-4 for bachelor, 1-2 for master

<sup>3</sup> 1-8 for bachelor, 1-3 for master

<sup>4</sup> Exam, colloquium or VP A/R - from the curriculum

<sup>5</sup> Course type: R = Compulsory course; E = Elective course; O = Optional course

<sup>6</sup> Formative category: S = Specialty; F = Fundamental; C = Complementary; I = Fully assisted; P = Partially assisted; N = Unassisted

<sup>7</sup> Equal to 14 weeks x number of hours from point 3.1 (similar to 3.2.a.b.c.)

<sup>8</sup> The following lines refer to individual study; the total is completed at point 3.37.

<sup>9</sup> Between 7 and 14 hours

<sup>10</sup> Between 2 and 6 hours

<sup>11</sup> The sum of the values from the previous lines, which refer to individual study.

<sup>12</sup> The sum (3.5.) between the number of hours of direct teaching activity (NOAD) and the number of hours of individual study (NOSI) must be equal to the number of credits assigned to the discipline (point 3.7) x no. hours per credit (3.6.)

<sup>13</sup> The credit number is computed according to the following formula, being rounded to whole neighbouring values (either by subtraction or addition

$$\text{No. credits} = \frac{\text{NOCpSpD} \times C_C + \text{NOApSpD} \times C_A}{\text{TOCpSdP} \times C_C + \text{TOApSdP} \times C_A} \times 30 \text{ credits}$$

Where:

- NOCpSpD = Number of lecture hours / week / discipline for which the credits are calculated
- NOApSpD = Number of application hours (sem./lab./pro.) / week / discipline for which the credits are calculated
- TOCpSdP = Total number of course hours / week in the Curriculum
- TOApSdP = Total number of application hours (sem./lab./pro.) / week in the Curriculum
- C<sub>C</sub>/C<sub>A</sub> = Course coefficients / applications calculated according to the table

Coefficients	Course	Applications (S/L/P)
Bachelor	2	1
Master	2,5	1,5
Bachelor - foreign language	2,5	1,25

<sup>14</sup> The courses that should have been previously completed or equivalent will be mentioned

<sup>15</sup> Board, video projector, flipchart, specific teaching materials, online platforms, etc.

<sup>16</sup> Computing technology, software packages, experimental stands, online platforms, etc.

<sup>17</sup> Competences from the Grids related to the description of the study program, adapted to the specifics of the discipline

<sup>18</sup> Chapter and paragraph titles

<sup>19</sup> Exposition, lecture, board presentation of the studied topic, use of video projector, discussions with students (for each chapter, if applicable)

<sup>20</sup> Discussions, debates, presentations and/or analyses of papers, solving exercises and problems

<sup>21</sup> Practical demonstration, exercise, experiment

<sup>22</sup> Case study, demonstration, exercise, error analysis, etc.

<sup>23</sup> The relationship with other disciplines, the usefulness of the discipline on the labour market

<sup>24</sup> CPE – Conditions Exam Participation; nCPE – Does Not Condition Exam Participation; CEF - Conditions Final Evaluation; N/A – not applicable

<sup>25</sup> The number of tests and the weeks in which they will be taken will be specified

<sup>26</sup> Scientific circles, professional competitions, etc.

<sup>27</sup> The minimum performance standard in the competence grid of the study program is customized to the specifics of the discipline, if applicable