SYLLABUS OF A MODULE

Polish name of a module	Inteligenta analiza w informatyce śledczej
English name of a module	Intelligent analysis in computer forensic
ISCED classification - Code	0619
ISCED classification - Field of study	
Languages of instruction	*English*
Level of qualification:	*2*
Number of ECTS credit points	*5*
Examination:	*A*
Available in semester:	*A*

Number of hours per semester:

Lecture	Exercises	Laboratory	Seminar	E-learning	Project
30		45			

<u>MODULE DESCRIPTION</u>

MODULE OBJECTIVES

O1. To acquaint students with the basic knowledge in the field of securing data carriers and the analysis of data obtained from secured media in terms of their use as evidence.

O2. To familiarise students with the basic skills in securing data carriers and analysing data obtained from secured media in terms of using them as evidence.

PRELIMINARY REQUIREMENTS FOR KNOWLEDGE, SKILLS AND OTHER COMPETENCES

1. Knowledge in the field of computer construction.
2. Ability to operate computers.
3. Knowledge of the construction of operating systems.

LEARNING OUTCOMES

LO 1 – The student knows the basic methods, techniques, tools, and materials to secure electronic evidence.

LO 2 - The student knows how to secure and analyse data for computer forensics.

MODULE CONTENT

Type of classes – lecture	**Number of hours**
1. Objectives, basic principles and area of computer forensics activities.	2
2. Creation of technical facilities.	2
3. Classification of data types and places of their occurrence.	2
4. Methods of acquiring and securing material for analysis.	2
5. Building popular file systems.	2
6. Windows essential data storage	2
7. Places where important data is stored in Linux	2
8. McOS data storage locations	2
9. Internet artefacts	2
10. Data analysis	2
11. Time analysis	2
12. Analysis of mobile devices	2
13. Hashing.	2
14. Location and recovery of deleted files. Carving data. Analysis of slack space and RAM slack.	2
15. Assessment.	2
Sum	**30**
Type of classes– laboratory.	**Number of hours**
1. Introduction	**2**
2. Creation of images of data carriers and their analysis.	**4**
3. Disk blockers and duplicators.	**4**

4. Acquiring and analysing data from web browsers, e-mail programs and messengers.	**4**
5. Recover Deleted Files.	**4**
6. Data recovery from damaged disks	**4**
7. Time analysis.	**4**
8. Analysing and securing data from a mobile device.	**6**
9. Analysis of an unknown file type in a hexadecimal editor.	**3**
10. Securing volatile data	**3**
11. Using and analysis the hashing function	**3**
12. Assessment	**4**
Sum	**45**

TEACHING TOOLS

1. Lectures using multimedia presentations
2. Laboratory guides
3. Computer stations with software
4. E-learning website
5. Tutorials

WAYS OF ASSESSMENT (F – FORMATIVE, S – SUMMATIVE

F1. - evaluation of the tests in the content of the lectures.
F2. - evaluation of laboratory exercises.
S1. - the average of the test marks.
S2. - average of the grades from laboratory exercises. *

*) in order to receive credit for the module, the student is obliged to receive positive grades from all laboratory exercises and complete the test task in lectures.

STUDENT’S WORKLOAD

L. p.	**Forms of activity**	**Average number of hours required for realization of activity**
1. Contact hours with teacher		
1.1	Lectures	30

1.2	Tutorials	
1.3	Laboratory	45
1.4	Seminar	
1.5	Project	
1.6	Examination	
Total number of contact hours with teacher:		75
2. Student’s individual work		
2.1	Preparation for tutorials and tests	15
2.2	Preparation for laboratory exercises, writing reports on laboratories	30
2.3	Preparation of project	
2.4	Preparation for final lecture assessment	10
2.5	Preparation for examination	
2.6	Individual study of literature	10
Total number of hours of student’s individual work:		65
Overall student’s workload:		140
Overall number of ECTS credits for the module		5
Number of ECTS points that student receives in classes requiring teacher’s supervision:		3
Number of **ECTS** credits acquired during practical classes including laboratory exercises and projects:		2

BASIC AND SUPPLEMENTARY RESOURCE MATERIALS

1. Ward B., Linux., Helion, 2005.
2. Osetek S., Pytel K.,Operating systems, WSiP 2013.
3. Wantoch-Rekowski R., Android, PWN, Warszawa, 2019.
4. E-learning platform PCz Moodle.
5. Nihad Hassan, Digital Forensic Basics, Apress, 2019
6. Harlan Carvey, Windows Forensic Analysis Toolkit, Syngres, Elsevier, 2018

MODULE COORDINATOR (NAME, SURNAME, E-MAIL ADDRESS)

dr hab. eng. Janusz Bobulski, januszb@icis.pcz.pl