

1.	Course Title	Digital Forensics
2.	Code	F18L3S093
3.	Study program	Software engineering and information systems
4.	Study Program Organizer	Faculty of Computer Science and Engineering
5.	Degree (first, second, third cycle)	first cycle
6.	Academic year / semester 3 / summer / optional	7. ECTS credits 6
8.	Teacher	associate professor Vesna Dimitrova
9.	Course enrollment prerequisites	Информациска безбедност
10.	<p>Course program goals (competencies): After finishing the course student will know the fundamental principles and techniques needed to carry out digital forensic investigation. Student will obtain practical knowledge to work with different forensic tools for different operating systems.</p>	
11.	<p>Course program content: (1) Digital forensics fundamentals, analysis and managing the situation after a cyber attack (1) File system forensics, forensic plan and Linux and Android technologies (1) Memory forensics under Windows and Windows forensics tools (1) Windows file system forensic tools (1) Data acquisition in Windows/Linux systems (1) Forensics analysis in Windows using registers and other artefacts. (1) Rootkits kernel modules (1) Techniques for structuring forensic data and data visualization (1) Tools and techniques for discovering money laundry, fraud detection and cyber criminal (1) Blockchain technology and Eterhium (1) Using the blockchain technology in forensic applications (1) Using chain analysis for integrity protection of the digital assets</p>	
12.	<p>Learning methods: Lectures using presentations, interactive lectures, exercises (using equipment and software packages), teamwork, case studies, invited guest lecturers, independent preparation and defense of a project assignment and seminar work.</p>	
13.	Total available time	6 ECTS x 30 hours = 180 hours
14.	Distribution of the available time	30 + 45 + 15 + 15 + 75 = 180 hours

15.	Teaching activity forms	15.1.	Lectures – theoretical teaching	30 hours
		15.2.	Exercises (laboratory, auditory), seminar papers, teamwork	45 hours
16.	Other activity forms	16.1.	Project Tasks	15 hours
		16.2.	Independent Learning Tasks	15 hours
		16.3.	Home learning	75 hours
17.	Assessment methodology			
	17.1.	Tests		10 points
	17.2.	Seminar paper/project (presentation: written and oral)		10 points
	17.3.	Activity and learning		10 points
	17.4.	Final exam		70 points
18.	Assessment criteria (points/grade)		up to 50 points	5 (five) (F)
			51 to 60 points	6 (six) (E)
			61 to 70 points	7 (seven) (D)
			71 to 80 points	8 (eight) (C)
			81 to 90 points	9 (nine) (B)
			91 to 100 points	10 (ten) (A)
19.	Course completion and final exam requirements	Realized activities 15.1 and 15.2		
20.	Teaching Language	Macedonian and English		
21.	Teaching quality evaluation method	Internal evaluation mechanisms and questionnaires		
22.	Course Material			
	22.1.	Mandatory course material		

No	Author	Title	Publisher	Year
1	John Sammons	The Basics of Digital Forensics, Second Edition: The Primer for Getting Started in Digital Forensics	Elsevier	2014
2	Mark Gates	Blockchain: Ultimate guide to understanding blockchain, bitcoin, cryptocurrencies, smart contracts and the future of money	Amazon Digital Services LLC	2017
3	Michael K Robinson	Digital Forensics Workbook: Hands-on Activities in Digital Forensics	CreateSpace Independent Publishing Platform	2015
22.2.	Additional course material			
No.	Author	Title	Publisher	Year