UČNI NAČRT PREDMETA / COURSE SYLLABUS	
Predmet:	Računalniška forenzika
Course title:	Computer Forensics

Študijski program in stopnja Study programme and level	Študijska smer Study field	Letnik Academic year	Semester Semester
Informatika v sodobni družbi, magistrski študijski program druge stopnje	-	Prvi ali drugi	Drugi ali četrti
Informatics in Contemporary Society, second cycle Masters Study Programme	-	First or second	Second or fourth

Vrsta predmeta / Course type	Izbirni / Elective
Univerzitetna koda predmeta / University course code:	1-ISD-MAG-IP-RF-2019-05-13

Predavanja Lectures	Seminar Seminar	Vaje Tutorial	Klinične vaje work	Druge oblike študija	Samost. delo Individ. work	ECTS
30	-	20	-	-	100	5

Nosilec predmeta / Lecturer:	
Jeziki / Languages: Predavanja / Lectures:	slovenski, angleški / Slovene, English
Vaje / Tutorial:	slovenski, angleški / Slovene, English

Pogoji za vključitev v delo oz. za opravljanje študijskih obveznosti:	Prerequisits:
Študent/študentka mora pred pristopom k izpitu pripraviti in zagovarjati seminarsko nalogo.	Prior to the exam, the student has to prepare and present seminar work.

Vsebina:	Content (Syllabus outline):
• računalniška forenzika • pregled tehnologije • digitalni dokazi • računalniški dokazi in njihovo zbiranje • forenzična analiza Windows sistemov • forenzična analiza Linux sistemov • forenzika malware-a • forenzika GSM in mobilnih naprav • forenzika mrež, Interneta in računalništva v oblaku	• computer forensics • technology overview • digital evidence • computer evidence and their collection • forensic analysis of Windows systems • forensic analysis of Linux systems • forensics of malware-a • forensics of GSM and mobile devices • forensics of networks, internet and cloud computing • the use of open source tools in

• uporaba odprtokodnega orodja v računalniški forenziki • predstavitev rezultatov • zaključna razmišljanja	computer forensics • presentation of results • concluding thoughts

Temeljni literatura in viri / Readings:

- Nelson B., Phillips A. and Steuart C.: Guide To Computer Forensics and Investigations, 6th ed., 2018, Cengage.
- Carvey H.: Windows Registry Forensics: Advanced Digital Forensic Analysis of the Windows Registry 2nd Edition, 2016, Syngress.
- Årnes A. (Editor): Digital Forensics, 1st Edition, 2017, Wiley.

Cilji in kompetence:	**Objectives and competences:**
Učna enota prispeva k razvoju naslednjih splošnih in predmetno specifičnih kompetenc: • uporaba metodoloških orodij, tj. izvajanje, koordiniranje in organiziranje raziskav, uporaba raznih raziskovalnih metod in tehnik ter ocenitev njihove uporabnosti • zmožnost za prepoznavanje in izkoriščanje priložnosti, ki se ponujajo v delovnem in družbenem okolju (ki se izkazujejo kot podjetniški duh in aktivno državljanstvo • poznavanje in razumevanje interakcij med informacijsko komunikacijsko tehnologijo in sodobno družbo • poglobljeno razumevanje in kritično razmišljanje o zmožnostih in omejitvah informacijsko komunikacijskih tehnologij • poznavanje varnostnih vidikov elektronskega poslovanja • poznavanje konceptov in metodologij za analizo velikih količin podatkov	*The instructional unit contributes to the development of the following general and subject-specific competences:* • use of methodological tools, i.e. implementation, coordination and organisation of research, use of various research methods and techniques and to evaluate their usefulness • the ability to recognise and take advantage of the opportunities, arising in work and social environment (and shown as the entrepreneurial spirit and active citizenship) • knowledge and understanding of interactions between the information and communication technology and the contemporary societyin-depth understanding and critical thinking regarding the possibilities and limitations of information and communication technologies • knowledge of the security aspects of e – business • knowledge of the concepts and methodologies for the analysis of large amounts of data

Predvideni študijski rezultati:	**Intended learning outcomes:**
Znanje in razumevanje: • poiskati in ohraniti digitalne dokaze • samostojna izvedba osnovne forenzične analize živega sistema • samostojna izvedba kriminalistično-tehnične analize post-mortem sistemov • samostojna izvedba forenzične analize mobilnih in PDA naprav • izvedba analize malware-a • izvedba ocene orodij za izvajanje računalniške forenzike • predložitev in predstavitev poročila o spremljanju poslovanja	Knowledge and understanding: • locate and preserve digital evidence • independent implementation of basic forensic analysis of living systems • independent implementation of forensic analysis of post-mortem systems • independent implementation of forensic analysis of mobile and PDA devices • analyzing a malware • performance assessment tools for implementation of computer forensics • submission and presentation of a monitoring operations report

Metode poučevanja in učenja:	**Learning and teaching methods:**
• *predavanja* z aktivno udeležbo študentov (razlaga, diskusija, vprašanja, primeri, reševanje primerov) • *vaje in laboratorijske vaje* • individualne in skupinske *konzultacije* (diskusija, dodatna razlaga, obravnava specifičnih vprašanj)	• *lectures* with active participation of students (explanation, discussion, questions, examples, problem solving) • *exercises and lab work* • individual and group consultations (discussion, additional explanation, consideration of specific issues)

Načini ocenjevanja:	Delež (v %) / Weight (in %)	**Assessment:**
Način (pisni izpit, ustno izpraševanje, naloge, projekt):		Type (examination, oral, coursework, project):
• pisni/ustni izpit	50	• written/oral exam
• seminarska naloga s poročili seminarskega dela in eksperimentalnih vaj ter predstavitev naloge	50	• seminar work