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-2016-10-01

Predavanja Lectures	**Seminar Seminar**	**Vaje Tutorial**	**Klinične vaje work**	**Druge oblike študija**	**Samost. delo Individ. work**	**ECTS**
30	-	10	-	10	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:

- Networking Series, Vacca R J *Computer Forensic*, 2005.
- Syngress, Aquilina et al *Malware Forensics*, 2008.
- Syngress, Carvey W *Windows Forensic Analysis*, 2009.
- Volonino et al *Computer Forensics*, 2006.
- Altheide, C., Carvey, H. *Digital Forensic with Open Source Tools*, Syngress, 2011.
- Garrison CP *Digital Forensic for Networking, Internet and Cloud Computing*, Syngress, 2010.
- Pogue et al *Unix and Linux Forensic Analysis*, Syngress, 2008.

Cilji in kompetence:	**Objectives and competences:**
Učna enota prispeva k razvoju naslednjih splošnih in predmetno specifičnih kompetenc: • osnovna IT znanja in spretnosti, potrebne za delo z modeli in orodji računalniške forenzike • poznavanje osnovnih delov računalnikov in operacijskega sistema ter dela s podatki, vse skupaj z zornega kota računalniške forenzike; poseben poudarek je na obravnavi konkretnih primerov, vključno z morebitnimi kršitvami in zločini – vsebina je strukturirana na način, ki zagotavlja celovit pregled najpomembnejših elementov računalniške forenzike • razvoj računalniških omrežij je omejen s pogoji za razvoj, razvojem samim in povezljivostjo v Internet, kar predstavlja en vidik tega predmeta, v povezavi z analizo tako poslovnega kot zasebnega okolja in posredovanja v primeru nevarnosti; večina podjetij je še vedno slabo obveščenih o računalniški forenziki in njeni uporabi, kar pomeni, da izobraževanje o tematiki pomeni tako dvig ravni znanja posameznika kot tudi dvig splošne ozaveščenosti • predmet je usmerjen h končnemu uporabniku v omrežnem okolju	*The instructional unit contributes to the development of the following general and subject-specific competences:* • basic ICT knowledge and skills needed to work with the models and tools of computer forensics • Knowledge of basic computer components, the operating system and work with the data from computer forensics point of view; special emphasis is on an examination of actual cases, including possible violations and crimes - the content is structured in a way that provides a comprehensive overview of the most important elements of the computer forensics • development of computer networks is limited by the conditions for development, by the development itself and connectivity to the Internet, which is one aspect of this course, in conjunction with an analysis of both business and private environment and intervention in case of emergency; most companies are still poorly informed about computer forensics and its usage, which means that the education about it represents the raising of knowledge as well as raising the general awareness • the subject is directed to the end user in a networked environment

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:

- *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)

Learning and teaching methods:

- *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