UČNI NAČRT PREDMETA / COURSE SYLLABUS (leto / year 2017/18)			
Predmet:	Računalniška forenzika		
Course title:	Digital forensic		
Študijski program in stopnja Study programme and level	**Študijska smer Study field**	**Letnik Academic year**	**Semester Semester**
Interdisciplinarni magistrski študijski program Računalništvo in matematika	ni smeri	1 ali 2	drugi
Interdisciplinary Master's study programme Computer Science and Mathematics	none	1 or 2	second

Vrsta predmeta / Course type	izbirni / elective
Univerzitetna koda predmeta / University course code:	63530

Predavanja Lectures	**Seminar Seminar**	**Vaje Tutorial**	**Klinične vaje work**	**Druge oblike študija**	**Samost. delo Individ. work**	**ECTS**
45		**30**			**105**	**6**

Nosilec predmeta / Lecturer:	doc. dr. Andrej Brodnik

Jeziki / Languages:	**Predavanja / Lectures:**	slovenski / Slovene, angleški / English
	Vaje / Tutorial:	slovenski / Slovene, angleški / English

Pogoji za vključitev v delo oz. za opravljanje študijskih obveznosti:	**Prerequisites:**
Vpis v letnik študija.	Enrolment in the programme.
Vsebina:	**Content (Syllabus outline):**

Uvod in pravne osnove: uvod digitalni dokazi in računalniški kriminal tehnologija in pravo: evropska perspektiva, ameriška perspektiva preiskovalni proces in rekonstrukcija modus operandi, motivi in tehnologija digitalni dokazi na sodišču Računalniki: osnove: delovanje, predstavitev podatkov, datotečni sistemi, enkripcija forenzična znanost in računalniki: avtorizacija, razpoznava, dokumentiranje, zbiranje in ohranjanje, preiskava in analiziranje, rekosntrukcija forenzična analiza sistemov Windows: datotečni sistem, pridobivanje podatkov iz računalnika, register, zabeležke (log), sledi datotek, omrežno dostopanje, programi forenzična analiza sistemov Unix: datotečni sistem, pridobivanje podatkov iz računalnika, register, zabeležke (log), sledi datotek, omrežno dostopanje, programi forenzična analiza sistemov Macintosh: datotečni sistem, pridobivanje podatkov iz računalnika, register, zabeležke (log), sledi datotek, omrežno dostopanje, programi forenzična analiza dlančnih sistemov: pomnilnik, Palm OS, Windows CE, RIM Blackberry, mobilni telefoni	Introduction and legal basis: introduction digital evidence and computer crime technology and legal framework: European perspective, North American perspective investigating procedure and reconstruction modus operandi, motifs and technology a digital evidence and a court of law Computers: basics: operation, data representation, file systems, encryption forensic science and computers: authorization, recognition, documentation, collecting and saving data, investigation and analysis, reconstruction forensic analysis of Windows systems: file system, collecting data from the computer, registry, logs, traces of files, network access, programs forensic analysis of Unix systems: file system, collecting data from the computer, registry, logs, traces of files, network access, programs forensic analysis of Mac computers: file system, collecting data from the computer, registry, logs, traces of files, network access, programs forensic analysis of palm computers: memory, Palm OS, Windows CE, RIM Blackberry, mobile phones Networks:

Omrežja: osnove: plasti in njihove storitve ter protokoli forenzična znanost in omrežja: razpoznava, dokumentiranje, zbiranje, ohranjanje podatkov, filtriranje in združevanje podatkov digitalni dokazi na fizični in povezavni plasti digitalni dokazi na omrežni in prenosti plasti digitalni dokazi v Internetu: splet, e-pošta, pogovorni programi, uporaba interneta kot preiskovalnega orodja Preiskovanje računalniškega kriminala: vdori in rekonstrukcija spolni zločini nadlegovanje digitalni dokazi kot alibi	basics: layers and their services with protocols forensic science and networks: recognition, documentation, collecting and saving data, data filtering and event matching digital evidences on a physical layer digital evidences on a link layer digital evidences on a network layer digital evidences in Internet: web, e-mail, chats, use of Internet as an investigation tool Investigation of a computer crime: intrusion and reconstruction sexual crimes harassment digital evidence as an alibi

Temeljni literatura in viri / Readings:

Digital Evidence and Computer Crime, Second Edition, Eoghan Casey, Academic Press (2004), ISBN-10: 0121631044, ISBN-13: 978-0121631048

Cyber Crime: The Investigation, Prosecution and Defense of a Computer-Related Crime. 2nd Edition. Edited by Clifford, R., Carolina Academic Press, ISBN 159460150X

Computer Forensics: Incident Response Essentials, Kruse, W., &, Heiser, J, Addison Wesley, ISBN 201707195

Cilji in kompetence:	**Objectives and competences:**

Študent se spozna s tem, kako se uporablja računalništvo in informatika v forenzičnih postopkih.	Student learns how to use knowledge and skills of Computer Science in forensic procedures.

Predvideni študijski rezultati:	**Intended learning outcomes:**
Znanje in razumevanje: Študent razume osnovne pojme forenzike in v podrobnosti delovanje računalniških sistemov ter je sposoben povezaovati obe področji. Uporaba: Sposoben je problem, poiskati, ga opredeliti iz strokovnega in forenzičnega kota ter ga rešiti. Refleksija: Spoznavanje, razumevanje in zavedanje dvojnosti problematike pri forenzičnih postopkih – stroka in forenzika. Prenosljive spretnosti - niso vezane le na en predmet: Teoretične osnove za inženirsko reševanje različnih praktičnih problemov, ki se pojavljajo v forenzičnih problemih.	Knowledge and understanding: Student understands basic terms in forensic science and details of computer systems, and then can combine knowledge from both areas. Application: Capable to find the problem, define it from professional and forensic point of view and solve it. Reflection: Learning and understanding of duality in forensic procedures – profession of computer and forensic science. Transferable skills: Theoretical and engineering skills for solving various practical problems appearing in digital forensic.

Metode poučevanja in učenja:	**Learning and teaching methods:**
Predavanja, vaje, domače naloge, seminarji, konzultacije, laboratorijsko delo.	Lectures, exercises, lab work, assignments, seminars, consulting.

Načini ocenjevanja:	Delež (v %) / Weight (in %)	**Assessment:**
Način (pisni izpit, ustno izpraševanje, naloge, projekt):		Type (examination, oral, coursework, project):Continuing (homework, midterm exams, project work)Final (written and oral exam)

Sprotno preverjanje (domače naloge, kolokviji in projektno delo) Končno preverjanje (pisni in ustni izpit) Ocene: 6-10 pozitivno, 1-5 negativno (v skladu s Statutom UL)	 50% 50%	Grading: 6-10 pass, 1-5 fail (according to the rules of University of Ljubljana)

Reference nosilca / Lecturer's references:

ZADRAVEC, Mirko, BRODNIK, Andrej, MANNILA, Markus, WANNE, Merja, ŽALIK, Borut. A practical approach to the 2D incremental nearest-point problem suitable for different point distributions. Pattern recognition, ISSN 0031-3203. [Print ed.], feb. 2008, vol. 41, iss. 2, str. 646-653. [COBISS.SI-ID 11580182]

BRODNIK, Andrej, CARLSSON, Svante, FREDMAN, Michael L., KARLSSON, Johan, MUNRO, J. Ian. Worst case constant time priority queue. The Journal of Systems and Software, ISSN 0164-1212. [Print ed.], 2005, vol. 78, no. 3, str. 249-256. [COBISS.SI-ID 13758553]

JOHANSSON, Olof, CARLSSON, Svante, LINDHOLM, Joel, SUNDSTRÖM, Mikael, BRODNIK, Andrej. Firewall apparatus and method of controlling network data packet traffic between internal and external networks : United States Application 20020016826. 02.07.2002. [COBISS.SI-ID 13760089]

BERGLUND, Tomas, BRODNIK, Andrej, JONSSON, Håkan, STAFFANSON, Mats, SÖDERKVIST, Inge. Planning smooth and obstacle-avoiding B-spline paths for autonomous mining vehicles. IEEE transactions on automation science and engineering, ISSN 1545-5955. [Print ed.], Jan. 2010, vol. 7, no. 1, str. 167-172, ilustr. [COBISS.SI-ID 7730260]

Andrej Brodnik: