UČNI NAČRT PREDMETA / COURSE SYLLABUS	
Predmet:	Digitalna 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 in 2	drugi
Interdisciplinary Masters study programme Computer Science and Mathematics	none	1 in 2	second

Vrsta predmeta / Course type	izbirni
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:	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:**
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, rekonstrukcija 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 Omrežja:	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: basics: layers and their services with protocols forensic science and networks: recognition,

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 prednosti 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	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:**

Po uspešnem zaključku predmeta bo študent: sposoben izkazati razumevanje osnovnih pojmov forenzike, sposoben opredeliti v podrobnosti delovanja računalniških sistemov, znal povezovati obe področji.	After the successful completion of the course the student will be able to: understand basic terms in forensic science, explain details of computer systems, and combine knowledge from both areas.

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): Sprotno preverjanje (domače naloge, kolokviji in projektno delo) Končno preverjanje (pisni in ustni izpit) Ocene: 6-10 pozitivno, 5 negativno (v skladu s Statutom UL).	50% 50%	Type (examination, oral, coursework, project): Continuing (homework, midterm exams, project work) Final (written and oral exam) Grading: 6-10 pass, 5 fail (according to the rules of University of Ljubljana).

Reference nosilca / Lecturer's references:

Andrej Brodnik:

– KRIŽAJ, Dejan, BRODNIK, Andrej, BUKOVEC, Boris. A tool for measurement of innovation newness and adoption in tourism firms. International journal of tourism research, ISSN 1522-1970, 2014, vol. 16, no. 2, str. 113-125. [COBISS.SI-ID 1500126]

– BRODNIK, Andrej, IACONO, John. Unit-time predecessor queries on massive data sets. Lect. notes comput. sci., part 1, str. 133-144. [COBISS.SI-ID 8178260]

– TRČEK, Denis, BRODNIK, Andrej. Hard and soft security provisioning for computationally weak pervasive computing systems in e-health. IEEE wireless communications, ISSN 1536-1284. [Print ed.], Aug. 2013, vol. 20, no. 4, 8 str., ilustr. [COBISS.SI-ID 10091092]

– BRODAL, Gerth Stølting, BRODNIK, Andrej, DAVOODI, Pooya. The encoding complexity of two dimensional range minimum data structures. 21st Annual European Symposium: proceedings, (Lecture notes in computer science, ISSN 0302-9743, Theoretical computer science and general issues, 8125). [COBISS.SI-ID 10148692]

– BRODNIK, Andrej, GRGUROVIČ, Marko. Speeding up shortest path algorithms. V: 23rd international symposium, 23rd international symposium, ISAAC 2012, (Lecture notes in computer science, ISSN 0302-9743, 7676), 2012, str. 156-165. [COBISS.SI-ID 1024498772]