

UČNI NAČRT PREDMETA / COURSE SYLLABUS							
<b>Predmet:</b>		Digitalna forenzika					
<b>Course title:</b>		Digital forensic					
<b>Študijski program in stopnja</b> Study programme and level		<b>Študijska smer</b> Study field		<b>Letnik</b> Academic year		<b>Semester</b> 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	
<b>Vrsta predmeta / Course type</b>				izbirni			
<b>Univerzitetna koda predmeta / University course code:</b>				63530			
<b>Predavanja</b> Lectures	<b>Seminar</b> Seminar	<b>Vaje</b> Tutorial	<b>Klinične vaje</b> work	<b>Druge oblike študija</b>	<b>Samost. delo</b> Individ. work	<b>ECTS</b>	
45		30			105	6	
<b>Nosilec predmeta / Lecturer:</b>		Andrej Brodnik					
<b>Jeziki / Languages:</b>		<b>Predavanja / Lectures:</b> slovenski/Slovene, angleški/English					
		<b>Vaje / Tutorial:</b> slovenski/Slovene, angleški/English					
<b>Pogoji za vključitev v delo oz. za opravljanje študijskih obveznosti:</b>				<b>Prerequisites:</b>			
<b>Vsebina:</b>				<b>Content (Syllabus outline):</b>			
Uvod in pravne osnove:				Introduction and legal basis: introduction			

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

<ul style="list-style-type: none"> <li>- forenzična znanost in omrežja: razpoznavna, dokumentiranje, zbiranje, ohranjanje podatkov, filtriranje in združevanje podatkov</li> <li>- digitalni dokazi na fizični in povezavni plasti</li> <li>- digitalni dokazi na omrežni in prednosti plasti</li> <li>- digitalni dokazi v Internetu: splet, e-pošta, pogovorni programi, uporaba interneta kot preiskovalnega orodja</li> </ul> <p>Preiskovanje računalniškega kriminala:</p> <ul style="list-style-type: none"> <li>- vdori in rekonstrukcija</li> <li>- spolni zločini</li> <li>- nadlegovanje</li> <li>- digitalni dokazi kot alibi</li> </ul>	<p>digital evidences on a physical layer</p> <p>digital evidences on a link layer</p> <p>digital evidences on a network layer</p> <p>digital evidences in Internet: web, e-mail, chats, use of Internet as an investigation tool</p> <p>Investigation of a computer crime:</p> <p>intrusion and reconstruction</p> <p>sexual crimes</p> <p>harassment</p> <p>digital evidence as an alibi</p>
---	---

#### Temeljni literatura in viri / Readings:

- a) Digital Evidence and Computer Crime, Second Edition, Eoghan Casey, Academic Press (2004), ISBN-10: 0121631044, ISBN-13: 978-0121631048
- b) Cyber Crime: The Investigation, Prosecution and Defense of a Computer-Related Crime. 2nd Edition. Edited by Clifford, R., Carolina Academic Press, ISBN 159460150X
- c) Computer Forensics: Incident Response Essentials, Kruse, W., & Heiser, J, Addison Wesley, ISBN 201707195

#### Cilji in kompetence:

Študent se spozna s tem, kako se uporablja računalništvo in informatika v forenzičnih postopkih.

#### Objectives and competences:

Student learns how to use knowledge and skills of Computer Science in forensic procedures.

#### Predvideni študijski rezultati:

Po uspešnem zaključku predmeta bo študent:

- sposoben izkazati razumevanje osnovnih

#### Intended learning outcomes:

After the successful completion of the course the student will be able to:

<p>pojmov forenzike,</p> <p>- sposoben opredeliti v podrobnosti delovanja računalniških sistemov,</p> <p>- znal povezovati obe področji.</p>	<p>- understand basic terms in forensic science,</p> <p>- explain details of computer systems, and</p> <p>- combine knowledge from both areas.</p>
--	--

**Metode poučevanja in učenja:**

Predavanja, vaje, domače naloge, seminarji, konzultacije, laboratorijsko delo.

**Learning and teaching methods:**

Lectures, exercises, lab work, assignments, seminars, consulting.

Delež (v %) /

**Načini ocenjevanja:**

Weight (in %)

**Assessment:**

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

**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]