UČNI NAČRT PREDMETA / COURSE SYLLABUS

Predmet:	Digitalna forenzika II
Course title:	Digital Forensics II

Študijski program in stopnja **Study programme and level**	**Modul** **Module**	**Letnik** **Academic year**	**Semester** **Semester**
Informacijske in komunikacijske tehnologije, 3. stopnja	Napredne internetne tehnologije	1	1
Information and Communication Technologies, 3^{rd} cycle	Advanced Internet Technologies	1	1

Vrsta predmeta / Course type	Izbirni / Elective
Univerzitetna koda predmeta / University course code:	IKT3-666

Predavanja **Lectures**	**Seminar** **Seminar**	**Sem. vaje** **Tutorial**	**Lab. vaje** **Laboratory work**	**Druge oblike**	**Samost. delo** **Individ. work**	**ECTS**
15	**15**			**15**	**105**	**5**

**Navedena porazdelitev ur velja, če je vpisanih vsaj 15 študentov. Drugače se obseg izvedbe kontaktnih ur sorazmerno zmanjša in prenese v samostojno delo. / This distribution of hours is valid if at least 15 students are enrolled. Otherwise the contact hours are linearly reduced and transfered to individual work.*

Nosilec predmeta / Lecturer:	Doc. dr. Tomaž Klobučar

Jeziki / **Languages:**	**Predavanja / Lectures:**	slovenščina, angleščina / Slovenian, English
	Vaje / Tutorial:	

Pogoji za vključitev v delo oz. za opravljanje študijskih obveznosti:	**Prerequisites:**
Zaključen študij druge stopnje s področja informacijskih ali komunikacijskih tehnologij ali zaključen študij druge stopnje na drugih področjih z znanjem osnov s področja predmeta. Potrebna so tudi osnovna znanja matematike, računalništva in informatike.	Completed second cycle studies in information or communication technologies or completed second cycle studies in other fields with knowledge of fundamentals in the field of this course. Basic knowledge of mathematics, computer science and informatics is also requested.

Vsebina:	**Content (Syllabus outline):**
Uvod: definicija osnovnih pojmov, forenzična tehnologija Digitalna forenzika: metodologije digitalne forenzike; digitalna forenzika in operacijski sistemi, pomnilniške naprave, prenosni sistemi, aplikacije in mrežni sistemi Napredna orodja digitalne forenzike: mobilni forenzični sistemi; komercialna in odprtokodna orodja za analizo datotečnih	Introduction: definition of basic concepts, digital forensics technology Digital forensics: digital evidence, digital forensics methodologies, technology and legalization interrelations; digital forensic and operating systems, storage, mobile systems, applications and networked systems Advanced digital forensics tools: digital forensic laboratory, mobile digital forensic systems; commercial and open source forensic

sistemov, živih sistemov, mobilnih naprav, aplikacij in omrežnih sistemov; zanesljivost orodij digitalne forenzike

Izbrana poglavja iz digitalne forenzike (npr. forenzika v oblaku)

Praktični vidiki in smernice razvoja:
praktični primeri postopkov digitalne forenzike; raziskovalno-tehnološki trendi informacijskih sistemov, nova tržišča; izzivi digitalne forenzike

tools for analyses of file, live, mobile and network systems, and applications; tools dependability.

Selected topics in digital forensics (e.g. cloud computing forensics)

Practical aspects and future trends:
practical examples of digital forensic investigations; Information systems research and technology trends, new markets; digital forensics research issues

Temeljna literatura in viri / Readings:

Izbrana poglavja iz naslednjih knjig: / Selected chapters from the following books:

- E. Casey (Ed.), *Handbook of Digital Forensics and Investigation*. Elsevier Academic Press, 2009, ISBN: 978-0-12-374267-4
- S. Davidoff and J. Ham, *Network Forensics: tracking hackers through cyberspace*. Prentice Hall, 2012, ISBN-13: 978-0132564717
- K. J. Jones, R. Bejtlich and C. W. Rose, *Real Digital Forensics: Computer Security and Incident Response*. Addison Wesley, 2005, ISBN: 0321240693
- B. Carrier, *File System Forensic Analysis*. Addison Wesley, 2005, ISBN: 0-321-26817-2

Izbrani znanstveni članki s področja digitalne forenzike, objavljeni npr. v Digital Investigation, IEEE Security and Privacy, IEEE Network Security, International Journal of Digital Evidence, International Journal of Electronic Security and Digital Forensics, Journal of Digital Forensic Practice.

Cilji in kompetence:

Namen predmeta je študentom predstaviti napredne vidike digitalne forenzike.

Študenti bi morali biti sposobni:

- Uporabiti metodologije digitalne forenzike
- Izbrati in uporabiti ustrezna orodja digitalne forenzike
- Upoštevati zahteve in probleme digitalne forenzike v specifičnih okoljih, na primer v oblaku ali mobilnih sistemih
- Nadaljevati raziskovalno-razvojno delo na področju digitalne forenzike

Objectives and competences:

The main objective of this course is to present advanced issues of digital forensics.

Students should be able to:

- Apply digital forensics methodology
- Select and use appropriate digital forensics tools
- Take into account the requirements and problems of digital forensics in specific environments, e.g. in cloud computing or mobile systems
- Continue research and development work in the area of digital forensics

Predvideni študijski rezultati:

Študenti bodo z uspešno opravljenimi obveznostmi tega predmeta pridobili:

- Poznavanje metodologij digitalne forenzike
- Poznavanje naprednih orodij digitalne forenzike
- Poznavanje zahtev in problemov digitalne forenzike v specifičnih okoljih, na primer v oblaku ali mobilnih sistemih
- Poznavanje smernic raziskav in razvoja na

Intended learning outcomes:

Students successfully completing this course will acquire:

- Apply digital forensics methodology
- Select and use appropriate digital forensics tools
- Know requirements and problems of digital forensics in specific environments, e.g. in cloud computing or mobile systems
- Know future trends of digital forensics research and development

področju digitalne forenzike • Sposobnost priprave znanstvenih rezultatov na področju	• Ability to provide research results in the field

Metode poučevanja in učenja:	**Learning and teaching methods:**
Predavanja, seminar, konzultacije, individualno delo	Lectures, seminar, consultancy, individual work

Načini ocenjevanja:	Delež (v %) / Weight (in %)	**Assessment:**
Seminarska naloga	25 %	Seminar work
Ustni zagovor	25 %	Oral defense
Ustni ali pisni izpit	50 %	Oral or written exam

Reference nosilca / Lecturer's references:

- V. Jovanovikj, D. Gabrijelčič and **T. Klobučar**, “A conceptual model of security context,” *International journal of information security*, ISSN 1615-5262, vol. 13, no. 6, pp. 571-581, 2014
- B. Ivanc and **T. Klobučar**, “Attack modeling in the critical infrastructure = Modeliranje napadov v kritični infrastrukturi,” *Elektrotehniški vestnik*, ISSN 0013-5852. [Slovenska tiskana izd.], vol. 81, no. 5, pp. 285-292, 2014
- **T. Klobučar**, D. Gabrijelčič and V. Pagon, “Cross-border e-learning and academic services based on eIDs: case of Slovenia” in *eChallenges 2014: 29-30 October, 2014 Belfast, Ireland*. Dublin: IIMC: = International Information Management Corporation, 8 pages, 2014
- P. Cigoj and **T. Klobučar**, “Cloud security and OpenStack,” in R. Trobec (Ed.), *Proceedings of the 1st International Conference on CLoud Assisted ServiceS, Bled, Slovenia, October 22 -25: CLASS*. 1st ed. Ljubljana: Univerza v Ljubljani, pp. 20-27, 2012
- V. Jovanovikj, D. Gabrijelčič and **T. Klobučar**, “Access control in BitTorrent P2P networks using the enhanced closed swarms protocol” in Netware 2011: August 21-27, 2011, Nice - Saint Laurent du Var, France. [S. l.], pp. 97-102, 2011