

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 četrty
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-2025-01-17

Predavanja Lectures	Seminar Seminar	Vaje Tutorial	Klinične vaje work	Druge oblike študija	Samost. delo Individ. work	ECTS
30	-	20	-	-	100	5

Nosilec predmeta / Lecturer: izr. prof. dr. Blaž Rodič, izr. prof. dr. Igor Bernik

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

Pogoji za vključitev v delo oz. za opravljanje študijskih obveznosti:

Študent/študentka mora pred pristopom k izpitu opraviti sprotne naloge in seminarsko nalogo.

Prerequisites:

Prior to the exam, the student has to complete the coursework and the seminar paper.

Vsebina:

- 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

Content (Syllabus outline):

- 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

- uporaba odprtokodnega orodja v računalniški forenziki
- predstavitev rezultatov
- zaključna razmišljanja

- the use of open source tools in computer forensics
- presentation of results
- concluding thoughts

Temeljni literatura in viri / Readings:

- Nelson B., Phillips A. and Steuart C.: Guide To Computer Forensics and Investigations, 6th ed., 2018, Cengage.
- Carvey H.: Windows Registry Forensics: Advanced Digital Forensic Analysis of the Windows Registry 2nd Edition, 2016, Syngress.
- Årnes A. (Editor): Digital Forensics, 1st Edition, 2017, Wiley.

Cilji in kompetence:

Učna enota prispeva k razvoju naslednjih splošnih in predmetno specifičnih kompetenc:

- uporaba metodoloških orodij, tj. izvajanje, koordiniranje in organiziranje raziskav, uporaba raznih raziskovalnih metod in tehnik ter ocenitev njihove uporabnosti
- zmožnost za prepoznavanje in izkoriščanje priložnosti, ki se ponujajo v delovnem in družbenem okolju (ki se izkazujejo kot podjetniški duh in aktivno državljanstvo)
- poznavanje in razumevanje interakcij med informacijsko komunikacijsko tehnologijo in sodobno družbo
- poglobljeno razumevanje in kritično razmišljanje o zmožnostih in omejitvah informacijsko komunikacijskih tehnologij
- poznavanje varnostnih vidikov elektronskega poslovanja
- poznavanje konceptov in metodologij za analizo velikih količin podatkov

Objectives and competences:

The instructional unit contributes to the development of the following general and subject-specific competences:

- use of methodological tools, i.e. implementation, coordination and organisation of research, use of various research methods and techniques and to evaluate their usefulness
- the ability to recognise and take advantage of the opportunities, arising in work and social environment (and shown as the entrepreneurial spirit and active citizenship)
- knowledge and understanding of interactions between the information and communication technology and the contemporary society in-depth understanding and critical thinking regarding the possibilities and limitations of information and communication technologies
- knowledge of the security aspects of e – business
- knowledge of the concepts and methodologies for the analysis of large amounts of data

Predvideni študijski rezultati:

<p>Znanje in razumevanje:</p> <ul style="list-style-type: none"> • 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

Intended learning outcomes:

<p>Knowledge and understanding:</p> <ul style="list-style-type: none"> • 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:

<ul style="list-style-type: none"> • <i>predavanja</i> (20 ur) in <i>e-predavanja</i> (10 ur) (razlaga, diskusija, vprašanja, primeri, reševanje primerov) • <i>vaje</i> (15 ur) in <i>e-vaje</i> (5 ur) • individualne in skupinske <i>konzultacije</i> (diskusija, dodatna razlaga, obravnava specifičnih vprašanj)

Learning and teaching methods:

<ul style="list-style-type: none"> • <i>lectures</i> (20 hours) and <i>e-lectures</i> (10 hours) (explanation, discussion, questions, examples, problem solving) • <i>tutorials</i> (15 hours) and <i>e-tutorials</i> (5 hours) • individual and group consultations (discussion, additional explanation, consideration of specific issues)

Načini ocenjevanja:

<p>Način (pisni izpit, ustno izpraševanje, naloge, projekt):</p> <ul style="list-style-type: none"> • pisni izpit • sprotne naloge • seminarska naloga

Delež (v %) /
Weight (in %)

30
50
20

Assessment:

<p>Type (examination, oral, coursework, project):</p> <ul style="list-style-type: none"> • written exam • coursework • seminar paper

Reference nosilca / Lecturer's references:

<p>izr. prof. dr. Blaž Rodič:</p> <ul style="list-style-type: none"> • RODIČ, Blaž. Industry 4.0 and the new simulation modelling paradigm. Organizacija : revija za management, informatiko in kadre, ISSN 1318-5454. [Tiskana izd.], aug. 2017, vol. 50, no. 3, str. 193-207, ilustr., doi: 10.1515/orga-2017-0017

- BRELIH, Marjan, RAJKOVIČ, Uroš, RUŽIČ, Tomaž, RODIČ, Blaž, KOZELJ, Daniel. Modelling decision knowledge for the evaluation of water management investment projects. *Central European Journal of Operations Research*, ISSN 1435-246X, 2018, vol., iss. , str. <https://link.springer.com/content/pdf/10.1007%2Fs10100-018-0600-5.pdf>, doi: 10.1007/s10100-018-0600-5.
- KANDUČ, Tadej, RODIČ, Blaž. Optimisation of machine layout using a force generated graph algorithm and simulated annealing. *International journal of simulation modelling*, ISSN 1726-4529, 2016, vol. 15, no. 2, str. 275-287.
- RODIČ, Blaž, BAGGIA, Alenka. Dynamic airport ground crew scheduling using a heuristic scheduling algorithm. *International journal of applied mathematics and informatics*, ISSN 2074-1278, 2013, vol. 7, iss. 4, str. 153-163.
- RODIČ, Blaž. Mobile agents for distributed decision support systems. *The International Scientific Journal of Management Information Systems*, ISSN 1452-774X, 2011, vol. 6, no. 1, str. 20-27.
- RODIČ, Blaž, KLJAJIĆ, Miroljub. Accessing distributed data sources with mobile agents and XML. V: JAŠKOVÁ, Mária (ur.). *ECON '05 : [selected research papers]*, (Research works proceedings, ISSN 0862-7908, Vol. 12, 2005). Ostrava: Technical University of Ostrava, Faculty of Economics. 2005, str. 280-287.
- RODIČ, Blaž, KLJAJIĆ, Miroljub. Integracija simulacijskih orodij v e-poslovni informacijski sistem. V: GRIČAR, Jože (ur.). *Izboljšanje konkurenčnosti regije z e-poslovanjem*, (Organizacija, ISSN 1318-5454, Letn. 37, 2004, št. 3). Kranj: Moderna organizacija. 2004, str. 162-167.
- ŠKRABA, Andrej, BAGGIA, Alenka, RODIČ, Blaž. Application of a group decision support system in the reform of study programmes. V: DONDON, Philippe (ur.). *Recent advances in education and modern educational technologies*, (Educational technologies series, 9). [S. l.: s. n.]. 2013, str. 128-134.
- RODIČ, Blaž. Issues of e-collaboration and knowledge management in media industries. V: LUGMAYR, Artur (ur.), et al. *Information systems and management in media and entertainment industries*, (International series on computer entertainment and media technology (Online), ISSN 2364-9488). Cham: Springer. cop. 2016.

prof. dr. Igor Bernik:

- BERNIK, Igor. *Cybercrime and cyberwarfare*, (Focus series). London: ISTE; Hoboken: Wiley, 2014. IX, 165 str., graf. prikazi. ISBN 978-1-84821-671-6.
- BERNIK, Igor, PRISLAN, Kaja. Measuring information security performance with 10 by 10 model for holistic state evaluation. *PloS one*, ISSN 1932-6203, 2016, vol. 11, no. 9, 33 str., graf. prikazi. <http://journals.plos.org/plosone/article/asset?id=10.1371/journal.pone.0163050.PDF>, <https://dk.um.si/lzpisGradiva.php?id=66283>.
- CHOI, SeEun, MARTINS, Jorge Tiago, BERNIK, Igor. Information security : listening to the perspective of organisational insiders. *Journal of information science*, ISSN 1741-6485. [Online ed.], 2018, 16 str. <http://journals.sagepub.com/doi/full/10.1177/0165551517748288>.