



Semestar 1		
Politehni?ki specijalisti?ki diplomski studij, Informacijska sigurnost i digitalna forenzika obavezni predmeti		
P:izv. prof. dr. sc. Krunoslav Antoliš P:dr.sc. Damir Delija P:mr.sc. Marinko Žagar viši predavač L: Domagoj Tuličić S:mr.sc. Marinko Žagar viši predavač	Digitalna forenzika	ECTS:6.0
P:Prof. dr. sc. Jana Žiljak Gršić , pročelnica INRO, voditeljica studija Informatike L:Prof. dr. sc. Jana Žiljak Gršić , pročelnica INRO, voditeljica studija Informatike L: Darija Čutić , mag. ing. graph. techn. S:Prof. dr. sc. Jana Žiljak Gršić , pročelnica INRO, voditeljica studija Informatike	Digitalni mediji, sigurnost i zaštita	ECTS:6.0
P:mr.sc. Marinko Žagar viši predavač L: Domagoj Tuličić L: Marin Rak S:mr.sc. Marinko Žagar viši predavač	Informacijska sigurnost	ECTS:6.0
P:dr.sc. Vlatko Mičković prof. P: Goran Sirovatka S: Goran Sirovatka L: Goran Sirovatka	Matematički modeli sigurnosti	ECTS:6.0
P: Sanja Kraljević , dipl.ing., v. pred. L: Sanja Kraljević , dipl.ing., v. pred. S: Sanja Kraljević , dipl.ing., v. pred.	Sigurnost web aplikacija	ECTS:6.0
P:izv. prof. dr. sc. Krunoslav Antoliš L:izv. prof. dr. sc. Krunoslav Antoliš S:izv. prof. dr. sc. Krunoslav Antoliš	Zakonska osnova digitalne forenzike	ECTS:6.0
Politehni?ki specijalisti?ki diplomski studij, Informacijska sigurnost i digitalna forenzika izborni predmeti		
P:Dr. sc. Aleksandar Stojanović	Programiranje za forenziku	ECTS:5.0



Semestar 2		
Politehni?ki specijalisti?ki diplomski studij, Informacijska sigurnost i digitalna forenzika obavezni predmeti		
P:mr.sc. Marinko Žagar viši predavač P: Dino Županović L:mr.sc. Marinko Žagar viši predavač L: Dino Županović S:mr.sc. Marinko Žagar viši predavač S: Dino Županović	Integrirani sustavi informacijske sigurnosti	ECTS:6.0
P:dr.sc. Damir Delija L: Savina Gruičić L: Davorka Topolčić S:dr.sc. Damir Delija	Organizacija i vođenje digitalno forenzičkih analiza	ECTS:6.0
P:dr.sc. Damir Delija L: Vedran Turkalj S: Vedran Turkalj	Sigurnost računalnih mreža	ECTS:6.0
P:mr.sc. Marinko Žagar viši predavač L: Ines Trbojević Košturjak S: Ines Trbojević Košturjak	Upravljanje rizicima i incidentima informacijske sigurnosti	ECTS:6.0
Politehni?ki specijalisti?ki diplomski studij, Informacijska sigurnost i digitalna forenzika izborni predmeti		
P: Aleksandra Bernašek Petrincec L: Aleksandra Bernašek Petrincec	IT Forenzika dokumenata i vrijednosnica	ECTS:6.0
P: Goran Sirovatka P:dr. sc. Roman Domović , prof. L: Goran Sirovatka S: Goran Sirovatka	Primijenjena kriptografija	ECTS:6.0
P:dr.sc. Damir Delija L: Savina Gruičić L:dr.sc. Damir Delija L: Davorka Topolčić L: Krešimir Hausknecht S:dr.sc. Damir Delija	Računalna forenzika	ECTS:5.0



Semestar 3		
Politehnički specijalistički diplomski studij, Informacijska sigurnost i digitalna forenzika obavezni predmeti		
P:dr.sc. Damir Delija S:dr.sc. Damir Delija L: Savina Gručić L: Krešimir Hausknecht	Forenzika računalnih mreža	ECTS:5.0
P:dr.sc. Damir Delija L: Davorka Topolčić L: Savina Gručić S:dr.sc. Damir Delija	Forenzika radne memorije	ECTS:5.0
P:dr.sc. Damir Delija L: Davorka Topolčić L: Savina Gručić S:dr.sc. Damir Delija S: Davorka Topolčić	Forenzika zlonamjernih programa	ECTS:5.0
P:v.pred. Aleksander Radovan , dipl. ing. L:v.pred. Aleksander Radovan , dipl. ing.	Tehnike sigurnog programiranja	ECTS:6.0
P:mr.sc. Marinko Žagar viši predavač L: Ines Trbojević Košturjak S: Ines Trbojević Košturjak	Upravljanje kontinuitetom poslovanja	ECTS:5.0
Politehnički specijalistički diplomski studij, Informacijska sigurnost i digitalna forenzika izborni predmeti		
P:dr.sc. Damir Delija	Digitalna forenzika na otvorenim sustavima	ECTS:5.0
P:mr.sc. Marinko Žagar viši predavač L: Domagoj Tuličić	Etičko hakiranje	ECTS:6.0
P:dr.sc. Damir Delija S:dr.sc. Damir Delija L: Krešimir Hausknecht	Forenzika mobilnih uređaja	ECTS:5.0
P: Goran Sirovatka L: Domagoj Tuličić	Skriptni i objektni jezici za forenziku	ECTS:6.0



Semestar 4

Politehnički specijalistički diplomski studij, Informacijska sigurnost i digitalna forenzika obavezni predmeti

S:mr.sc. Marinko Žagar viši predavač	Diplomski rad	ECTS:20.0
P:mr.sc. Marinko Žagar viši predavač S:mr.sc. Marinko Žagar viši predavač	Metodologija stručnog i istraživačkog rada	ECTS:5.0



Semestar 5



Semestar 6



Šifra WEB/ISVU	24964/173030	ECTS	6.0	Akadska godina	2019/2020
Naziv	Digitalna forenzika				
Status	1. semestar - Politehni?ki specijalisti?ki diplomski studij, Informacijska sigurnost i digitalna forenzika (Izvanredni specijalisti?ki informacijska sigurnost i digitalna forenzika) - Obavezni predmet				
Izvedba nastave	Predavanja + vjezbe (auditorne+laboratorij+seminar+konstrukcijske) Samostalan rad			30+30 (0+15+15+0) 120	
Izvođači	Predavanja:1. izv. prof. dr. sc. Krunoslav Antoliš Predavanja:2. dr.sc. Damir Delija Predavanja:3. mr.sc. Marinko Žagar viši predavač Laboratorijske vjezbe: Domagoj Tuličić Seminarske vjezbe:mr.sc. Marinko Žagar viši predavač				
Cilj predmeta	Stjecanje temeljnih znanja o digitalnoj forenzici i zakonskim osnovama digitalne forenzike				
Ishodi učenja:	1. prezentirati zakonske osnove digitalne forenzike . Razina:6,7 2.kreirati izvještaj o provedenoj digitalno forenzičkoj analizi . Razina:6,7 3.kategorizirati digitalne artefakte. Razina:6 4.identificirati Izdvojiti digitalne tragove . Razina:6 5.razlikovati vrste digitalne forenzike. Razina:6 6.analizirati digitalno forenzičke artefakte. Razina:6 7. usporediti digitalno forenzičke alate . Razina:6,7				
Način izvođenja predavanja	Frontalna, ex cathedra Gost, predavač Analiza primjera, case studies Pitanja - odgovori				
Način izvođenja laboratorijskih vjezbi	Laboratorijske s laboratorijskom opremom Laboratorijske, simulacije na računalima Grupno rješavanje zadanih problema Međusobno zadavanje i rješavanje problema Radionica				
Način izvođenja seminarskih vjezbi	Analiza literature na webu, knowledge mining Pisanje eseja Rasprave, brainstorming Radionica				
Sadržaj predavanja	1.Uvod u digitalnu forenziku, 2h, Ishodi:1 2.Procesi i grane digitalne forenzike, 2h, Ishodi:2 3.Kibernetički kriminal, Protokol konvencije o kibernetičkom kriminalu, 1h, Ishodi:5 4.The European Cybercrime Centre (EUROPOL), 1h, Ishodi:4 5.Četiri principa digitalne forenzike, 2h, Ishodi:3 6.Organizacija digitalno forenzičkog tima, 2h, Ishodi:4 7.Digitalno forenzički istražni proces i faze digitalno forenzičkog procesa, 2h, Ishodi:6 8.Glavni izazovi forenzičkog procesa, ispitivanje dokaza i izvještavanje, 2h, Ishodi:6 9.Modeli digitalno forenzičkih istraga, 2h, Ishodi:4 10.Principi akvizicije i obrade digitalno forenzičkih dokaza, 2h, Ishodi:3 Akvizicija i obrada internet dokaza, 1h, Ishodi:3 Akvizicija i obrada dokaza na računalima, 1h, Ishodi:6 11.Strojno programska oprema za forenzički laboratorij, 2h, Ishodi:7 12.Digitalno forenzički artefakti, 2h, Ishodi:7 13.Artefakti digitalnih dokumenata, 2h, Ishodi:3 14.Windows, Linux i MAC OS artefakti, 2h, Ishodi:2 15.Tehnike antiforenzika, 2h, Ishodi:1				
Sadržaj laboratorijskih vjezbi	1.Uvod u laboratorijske vjezbe i osnovne alate digitalne forenzike, 1h, Ishodi:1 2.Istraživanje i analiza digitalno forenzičkih artefakta, 2h, Ishodi:7 3.Osnove korištenja alata AmpedFive, 2h, Ishodi:2 4.Osnove korištenja alata EnCase, 2h, Ishodi:6 5.Analiza digitalnih zapisa pomoću alata AmpedFive, 2h, Ishodi:7 6.Analiza video zapisa pomoću alata AmpedFive, 2h, Ishodi:3,5 7.Analiza nositelja digitalnih zapisa pomoću alata EnCase, 2h, Ishodi:6,7 8.Izrada izvještaja o provedenim analizama, 2h, Ishodi:5 9.Nema nastave 10.Nema nastave 11.Nema nastave 12.Nema nastave 13.Nema nastave 14.Nema nastave 15.Nema nastave				
Sadržaj seminarskih vjezbi	1.Definiranje teme seminarskog rada, 1h, Ishodi:1 2.Izrada seminarskog rada, 2h, Ishodi:2 3.Izrada seminarskog rada, 2h, Ishodi:3 4.Izrada seminarskog rada, 2h, Ishodi:4 5.Izrada seminarskog rada, 2h, Ishodi:5 6.Izrada seminarskog rada, 2h, Ishodi:2 7.Izrada seminarskog rada, 2h, Ishodi:1				



	8.Izrada seminarskog rada, 2h, Ishodi:1 9.Nema nastave 10.Nema nastave 11.Nema nastave 12.Nema nastave 13.Nema nastave 14.Nema nastave 15.Nema nastave
Materijalni uvjeti za izvedbu predmeta	Namjenski laboratorij Namjenski računalni laboratorij Projektor
Ishodi	6#7
Literatura	1.John Sammons: The Basics of Digital Forensics, Syngress, March 2012 2.Fred Cohen, Challenges to Digital Forensic Evidence,ASP Press, 2008 3.Marinko Žagar, Skripta predavanja - Digitalna forenzika, 2016. 4.K. Antoliš poglavlje u knjizi: Internet Forensics and Combating Terrorism u knjizi: The Dangerous Landscape, ISBN978-954-92521-6-3, nakladnik: Procon Ltd. 2013. 5.K. Antoliš: ICT Identity Theft, Informatologija, 46, 2013., 4, 353-360, UDK:681.3:340:001, ISSN 1330-0067, Zagreb, Hrvatska. 6.David Lilburn Watson Andrew Jones : Digital Forensics Processing and Procedures, 1st Edition Meeting the Requirements of ISO 17020, ISO 17025, ISO 27001 and Best Practice Requirements, David Lilburn Watson Andrew Jones, 2013 7.Jana Žiljak Vujić, Sigurnosna grafika,TVZ,978-953-7048-33-4,2014
Uvjeti za potpis (obaveze studenta)	Prisustvo na nastavi 80% Izrađene laboratorijske vježbe Predan seminarski rad
Provjera znanja u semestru	Kolokvij
Način polaganja ispita nakon semestra	Laboratorijske vježbe ili seminar do 50 bodova Dva kolokvija po 25 bodova (Svaki kolokvij ima popravak) Opcionalni bodovi za zalaganje Ukoliko student ne položi kolokvije ima mogućnost izlaska na usmeni ispit. Ukupno maksimalno 100 bodova 0-49 - nedovoljan 50-61 - dovoljan 62-74 - dobar 75-86 - vrlo dobar 87-100 - izvrstan
Praćenje rada studenta:	Aktivnost ECTS Pohađanje nastave () 1 Pismeni ispit () 1 Seminarski rad () 1 Usmeni ispit () 1 Praktični rad () 2
Napomena	Iz ovog predmeta moguća je izrada završnog/diplomskog rada
Preduvjeti:	Nema preduvjeta
Izradio prijedlog	mr.sc. Marinko Žagar viši predavač, 5.6.2018



Šifra WEB/ISVU	25248/202985	ECTS	5,0	Akadska godina	2019/2020
Naziv	Digitalna forenzika na otvorenim sustavima				
Status	3. semestar - Politehni?ki specijalisti?ki diplomski studij, Informacijska sigurnost i digitalna forenzika (Izvanredni specijalisti?ki informacijska sigurnost i digitalna forenzika) - Izborni predmet				
Izvedba nastave	Predavanja + vje?be (auditorne+laboratorij+seminar+konstrukcijske) Samostalan rad			30+30 (0+30+0+0) 90	
Izvođa?i	Predavanja:1. dr.sc. Damir Delija				
Cilj predmeta	Stjecanje temeljnih znanja o digitalnoj forenzici na otvorenim operacijskim sustavima				
Ishodi u?enja:	1.osmisliiti Osmisliti i upotrijebiti alate za spremanje i analizu digitalnih dokaza na operacijskom sustavu Linux. Razina:6,7 2.napisati Napisati i izraditi izvještaje o provedenoj digitalno forenzi?koj istrazi ra?unala koriste?i Linux . Razina:6,7 3.planirati Planirati i provesti forenzi?ku analizu koriste?i Linux alate . Razina:6,7 4.analizirati Identificirati i analizirati kriptirane podatke Linux alatima. Razina:6 5.osmisliiti Osmisliti i provesti forenzi?ku analizu otovrenog sustava Linux. Razina:6,7 6.organizirati Organizirati samostalno korištenje otvorenog sustava Linux u digitalnoj forenzici. Razina:6,7				
Na?in izvođenja predavanja	Frontalna, ex cathedra Gost, predava?i Analiza primjera, case studies Demonstracije Simulacije Modeliranje Diskusija problema Pitanja - odgovori Seminar, izlaganje studenta s raspravom Izlaganje domaćih zadaća Ostalo, upisati prakti?ni rad				
Na?in izvođenja laboratorijskih vje?bi	Laboratorijske s laboratorijskom opremom Laboratorijske, simulacije na ra?unalima Grupno rješavanje zadanih problema Analiza klasi?ne literature Analiza literature na webu, knowledge mining Pisanje eseja Rasprave, brainstorming Mapiranje pojmova, mind-mapping Ra?unalne simulacije Me?usobno zadavanje i rješavanje problema Radionica Ostalo, upisati prakti?an rad				
Sadržaj predavanja	1.Uvod u Otvorene sustave , 2h, Ishodi:1,4 2.Procesi digitalne forenzike i Linux, 2h, Ishodi:1,4 3.Alati ra?unalne forenzike na Linuxu, 2h, Ishodi:1,3 4.Faze digitalno forenzi?kog procesa i Linux, 2h, Ishodi:1 5.Akvizicija i obrada dokaza na ra?unalima na Linuxu, 2h, Ishodi:2,6 6.Akvizicija i obrada internet dokaza na Linuxu, 2h, Ishodi:2,3 7.Akvizicija i obrada digitalnih fotografija na Linuxu, 2h, Ishodi:2,3 8.Akvizicija digitalnih dokaza iz oblaka na Linuxu, 2h, Ishodi:3 9.Akvizicija digitalnih tragova mobilnih ure?aja na Linuxu, 2h, Ishodi:3 10.Linux i forenzika ?ivih podataka, 2h, Ishodi:4 11.Alati forenzike digitalnih dokumenata, 2h, Ishodi:4 12.Digitalno forenzi?ki artefakti, 2h, Ishodi:3,5 13.Linux artefakti, 2h, Ishodi:1,2,3 14.Linux i artefakti digitalnih dokumenata, 2h, Ishodi:3,5 15.Tehnike antiforenzike i Linux, 2h, Ishodi:1,2,3				
Sadržaj laboratorijskih vje?bi	1.Uvod u laboratorijske vje?be, 2h, Ishodi:1,6 2.Alati digitalne forenzike, 2h, Ishodi:5,6 3.Istra?ivanje i analiza digitalno forenzi?kih artefakta, 2h, Ishodi:2,3,4 4.Napredno korištenja Linuxa, 2h, Ishodi:5,6 5.Detalji gra?e Linuxa, 2h, Ishodi:2,3,4,5 6.Akvizicija podataka na Linux, 2h, Ishodi:2,3,4,5 7.Izrada izvještaja o provedenim analizama, 2h, Ishodi:2,3,4,5 8.Sumarni pregled vje?ni, 2h, Ishodi:1,2,3,4,5,6 9.Prvi kolokvij, 2h, Ishodi:1,2,3,4,5,6 10.Izbor teme za seminare, 2h, Ishodi:1,2,3,4,5,6 11.Izrada seminara , 2h, Ishodi:1,2,3,4,5,6 12.Izrada seminara , 2h, Ishodi:1,2,3,4,5,6 13.Izrada seminara , 2h, Ishodi:1,2,3,4,5,6 14.Izlaganje seminara, 2h, Ishodi:1,2,3,4,6 15.Drugi kolokvij, 2h, Ishodi:1,2,3,4,5,6				



Materijalni uvjeti za izvedbu predmeta	Elementarni: predavaona, ploča, kreda... Namjenski laboratorij Računalni laboratorij opće namjene Namjenski računalni laboratorij Bijela ploča sa flomasterima Projektor Video oprema Alat, navesti
Ishodi	6#7
Literatura	Barry J. Grundy :The Law Enforcmnt and Fornsic Examinrs Introduction to Linux, June 2018 Shiva V.N. Parasram: Digital Forensics with Kali Linux Cameron H. Malin, Eoghan Casey and James M. Aquilina: Malware Forensics Field Guide for Linux Systems Chris Pogue, Cory Altheide and Todd Haverkos: UNIX and Linux Forensic Analysis DVD Toolkit AAaron Walters, Jamie Levy, Andrew Case and Michael Hale Ligh :The Art of Memory Forensics: Detecting Malware and Threats in Windows, Linux, and Mac Memory
Uvjeti za potpis (obaveze studenta)	Prisustvo na nastavi 80% Izrađene laboratorijske vježbe Predan seminarski rad
Provjera znanja u semestru	kolokviranje
Način polaganja ispita nakon semestra	Laboratorijske vježbe ili seminar do 50 bodova Dva kolokvija po 25 bodova (Svaki kolokvij ima popravak) Opcionalni bodovi za zalaganje Ukoliko student ne položi kolokvije ima mogućnost izlaska na usmeni ispit. Ukupno maksimalno 100 bodova 0-49 - nedovoljan 50-61 - dovoljan 62-74 - dobar 75-86 - vrlo dobar 87-100 - izvrstan
Praćenje rada studenta:	Aktivnost ECTS Pohađanje nastave () 1 Praktični rad () 2 Seminarski rad () 1 Pismeni ispit () 1
Napomena	Iz ovog predmeta moguća je izrada završnog/diplomskog rada
Preduvjeti:	Nema preduvjeta
Izradio prijedlog	dr.sc. Damir Delija , 18.7.2019



Šifra WEB/ISVU	25071/185429	ECTS	6.0	Akademski godina	2019/2020
Naziv	Digitalni mediji, sigurnost i zaštita				
Status	1. semestar - Politehnički specijalistički diplomski studij, Informacijska sigurnost i digitalna forenzika (Izvanredni specijalistički informacijska sigurnost i digitalna forenzika) - Obavezni predmet				
Izvedba nastave	Predavanja + vježbe (auditorne+laboratorij+seminar+konstrukcijske) Samostalan rad			30+30 (0+15+15+0) 120	
Izvođači	Predavanja:1. Prof. dr. sc. Jana Žiljak Gršić , pročelnica INRO, voditeljica studija Informatike Laboratorijske vježbe: Darija Čutić , mag. ing. graph. techn. Laboratorijske vježbe:Prof. dr. sc. Jana Žiljak Gršić , pročelnica INRO, voditeljica studija Informatike Seminarske vježbe:Prof. dr. sc. Jana Žiljak Gršić , pročelnica INRO, voditeljica studija Informatike				
Cilj predmeta	Osposobiti studente za prepoznavanje sigurnosnih elemenata dokumenata i vrijednosnica te korištenje alata za provedbu grafičke forenzike.				
Ishodi učenja:	1.analizirati pristup dizajnu dokumenata i vrijednosnica. Razina:6 2. kritički prosuđivati vrste dizajna i elemenata zaštita na dokumentima i vrijednosnicama . Razina:7 3.razlikovati metode i tehnologiju izrade sigurnih elemenata. Razina:6 4.razlikovati uzorke zaštićenih dokumenata i vrijednosnica na instrumentima za digitalnu forenziku . Razina:6 5.analizirati suvremene tehnike zaštita i načine pokušaja krivotvorenja. Razina:6 6. usporediti pojedine elemente zaštite . Razina:6,7				
Način izvođenja predavanja	Frontalna, ex cathedra Gost, predavač Pitanja - odgovori				
Način izvođenja laboratorijskih vježbi	Laboratorijske s laboratorijskom opremom Laboratorijske, simulacije na računalima Grupno rješavanje zadanih problema Analiza klasične literature Analiza literature na webu, knowledge mining Mapiranje pojmova, mind-mapping Računalne simulacije Međusobno zadavanje i rješavanje problema Radionica				
Način izvođenja seminarskih vježbi	Analiza klasične literature Analiza literature na webu, knowledge mining Pisanje eseja Međusobno zadavanje i rješavanje problema				
Sadržaj predavanja	1.Pregled dizajn vrijednosnica i dokumenata kroz povijest, 2h, Ishodi:1 2.Dizajn i analizu dokumenata i vrijednosnica, 2h, Ishodi:1 3.Dizajn sigurnosnih elemenata na dokumentima i vrijednosnicama, 2h, Ishodi:1 4.Sigurnost pojedinih zaštitnih elemenata na dokumentima i vrijednosnicama, 2h, Ishodi:2 5.Karakteristike sigurnosnih boja u sustavu zaštite, 2h, Ishodi:3 6.Sigurnost linijska grafika u sustavu zaštite, 2h, Ishodi:3 7.Suvremeni način krivotvorenja, 2h, Ishodi:1 8.Dizajn u vidljivom, IR i UV, 2h, Ishodi:6 9.Krivotvorine u svakom spektru, 2h, Ishodi:6 10.Sigurnost od ukupnog krivotvorenja dokumenata i vrijednosnica, 2h, Ishodi:4 11.Razlikovanje dizajna krivotvorine dizajnu zaštite, 2h, Ishodi:6 12.Sigurnost dokumenata i razlozi za zaštićenu grafiku, 2h, Ishodi:1 13.Dizajn za pojedini dokument, 2h, Ishodi:1 14.Sigurnosna dostignuća u području krivotvorenja, 2h, Ishodi:2 15.Dizajniranih dokumenata i vrijednosnica sa sustavom suvremene zaštite, 1h, Ishodi:3 Testiranje dizajniranog rješenja na sigurnost od krivotvorenja, 1h, Ishodi:4,6				
Sadržaj laboratorijskih vježbi	1.Analiziranje pojedinih dizajna dokumenata, 1h, Ishodi:1 2.Sigurnosni dizajn zaštita, Ishodi: 1 4., 1h, Ishodi:1,4 3.Dizajn specifičnih vrsta vrijednosnica, 1h, Ishodi:2,6 4.Dizajn osnovnih elemenata na dokumentima i novčanicama: vizualna procjena, 1h, Ishodi:2 5.Proučavanje karakteristika vizualnog spektra, 1h, Ishodi:2 6.Dizajn u ultraljubičastom dijelu spektra, 1h, Ishodi:4 7.Nova rješenja u zaštiti dokumenata i vrijednosnica, 1h, Ishodi:5 8.Analiza krivotvorenih sa originalnim novčanicama, 1h, Ishodi:4 9.Vidljiva autentičnosti dokumenata i vrijednosnica, 1h, Ishodi:4 10.Testiranje na Projektini, 1h, Ishodi:6 11.Metoda stvaranja originala, 1h, Ishodi:3 12.Poznavanje procedure kod otkrivanja krivotvorine, 1h, Ishodi:3 13.Sustav nadogradnje tehnologije, 1h, Ishodi:3 14.Način realizacije dokumenata, 1h, Ishodi:3 15.Svjetski poznate tiskare dokumenata i vrijednosnica i njihovi standardi, 1h, Ishodi:6				
Sadržaj seminarskih vježbi	1.Analiziranje dizajna pojedine vrijednosnice, 2h, Ishodi:2 2.Dizajn grafičkih elemenata na dokumentima i vrijednosnicama, 2h, Ishodi:2 3.Proučavanje pravnih aspekata dizajna, 2h, Ishodi:3 4.Razmatranje osnovnih elemenata na novčanicama kroz 3 spektra: instrumentalna metoda, 2h, Ishodi:2 5.Dizajn za IR i UV izvore svjetla, 2h, Ishodi:3 6.Dizajn u infracrvenom dijelu spektra, 2h, Ishodi:4				



	7.Dizajn sukladno novim tehnologijama u zaštiti dokumenata i vrijednosnica, 2h, Ishodi:5 8.Sigurnost dokumenata i vrijednosnica, 2h, Ishodi:4 9.Analiza krivotvorina i procjena kvalitete, 2h, Ishodi:4 10.Metode snimanja falsifikata, 2h, Ishodi:6 11.Proces izrade dokumenata i vrijednosnica, 2h, Ishodi:3 12.Proces informiranja o krivotvorinama, 2h, Ishodi:6 13.Suvremeni dokumenti na granicama, 2h, Ishodi:5 14.Ovlaštenja proizvođača dokumenata, 2h, Ishodi:3 15.Opremu i metode potrebne za realizaciju i forenziku, 2h, Ishodi:6
Materijalni uvjeti za izvedbu predmeta	Elementarni: predavaona, ploča, kreda... Bijela ploča sa flomasterima Projektor
Ishodi	6#7
Literatura	1.Jana Žiljak Vujić, Sigurnosna grafika, Tehničko veleučilište u Zagrebu, Informatičko - računarski odjel,978-953-7048-33-4, 2014 2.Gordan Mršić, Jasna Galeković, Andrea Ledić, Andrijana Ristović, Nevenka Škavić, Forenzika dokumenata, novca i rukopisa, Hrvatska Sveučilišna Naklada, 978-953-169-286-1, 2014
Uvjeti za potpis (obaveze studenta)	Izrada seminara i vježbi je obvezna za sve studente i uvjet za potpis. Oprema: -Softver za dizajn zaštitnih elemenata i vektorske grafike Adobe -Projektina -UV lampe -fotoaparati sa IR filterom
Provjera znanja u semestru	Laboratorijske vježbe i seminar Ukoliko student ne položi kolokvije ima mogućnost izlaska na usmeni ispit. Ukupno maksimalno 100 bodova 0-49 - nedovoljan 50-61 - dovoljan 62-74 - dobar 75-86 - vrlo dobar 87-100 izvrstan
Način polaganja ispita nakon semestra	ispit
Praćenje rada studenta:	Aktivnost ECTS Pohađanje nastave () 1 Kontinuirana provjera znanja () 3 Praktični rad () 2
Napomena	Iz ovog predmeta moguća je izrada završnog/diplomskog rada
Preduvjeti:	Nema preduvjeta
Izradio prijedlog	Prof. dr. sc. Jana Žiljak Gršić, 8.6.2018



Šifra WEB/ISVU	25243/200668	ECTS	20.0	Akadska godina	2019/2020
Naziv	Diplomski rad				
Status	4. semestar - Politehni?ki specijalisti?ki diplomski studij, Informacijska sigurnost i digitalna forenzika (Izvanredni specijalisti?ki informacijska sigurnost i digitalna forenzika) - Obavezni predmet				
Izvedba nastave	Predavanja + vje?be (auditorne+laboratorij+seminar+konstrukcijske) Samostalan rad			0+120 (0+0+120+0) 480	
Izvođa?i	Seminarske vje?be:1. mr.sc. Marinko ?agar viši predava??				
Cilj predmeta					
Ishodi u?enja:	1.izra?unati izra?unati vrijednosti matemati?kih izraza. Razina: 2. formulirati / oblikovati Rješavanja slo?enih matemati?kih problema. Razina: 3.nacrtati nacrtati graf realne funkcije jedne ili više realnih varijabli. Razina: 4.analizirati napisati jednostavnije ra?unalne skripte/funkcije. Razina: 5.riješiti riješiti (ne)algebarske. Razina: 6.riješiti riješiti obi?ne diferencijalne jedna?be. Razina: 7.identificirati Prepoznati mogu?nosti programskih alata Julia i R. Razina:				
Preduvjeti:	Nema preduvjeta				



Šifra WEB/ISVU	25219/173038	ECTS	6.0	Akadska godina	2019/2020
Naziv	Etičko hakiranje				
Status	3. semestar - Politehnički specijalistički diplomski studij, Informacijska sigurnost i digitalna forenzika (Izvanredni specijalistički informacijska sigurnost i digitalna forenzika) - Izborni predmet				
Izvedba nastave	Predavanja + vježbe (auditorne+laboratorij+seminar+konstrukcijske) Samostalan rad			30+30 (0+20+10+0) 120	
Izvođači	Predavanja:1. mr.sc. Marinko Žagar viši predavač Laboratorijske vježbe: Domagoj Tuličić				
Cilj predmeta	Stjecanje znanja i vještina iz područja etičkog hakiranja. Upoznavanje s osnovnim pojmovima, alatima, tehnikama i metodologijom etičkog hakiranja. Usvojiti teorijska i praktična znanja za primjenu i podizanje informacijske sigurnosti.				
Ishodi učenja:	1.analizirati informacije mrežnih informacijskih sustava. Razina:6 2.izdvojiti prijetnje informacijskom sustavu. Razina:6 3.kategorizirati informacije informacijskih sustava. Razina:6 4. kritički prosuđivati alate i tehnike etičkog hakiranja. Razina:7 5. formulirati / oblikovati ranjivosti informacijskog sustava. Razina:6,7 6. usporediti metodologije etičkog hakiranja. Razina:6,7				
Način izvođenja predavanja	Frontalna, ex cathedra Gost, predavač Analiza primjera, case studies Diskusija problema Seminar, izlaganje studenta s raspravom				
Način izvođenja laboratorijskih vježbi	Laboratorijske s laboratorijskom opremom Laboratorijske, simulacije na računalima Grupno rješavanje zadanih problema Rasprave, brainstorming				
Način izvođenja seminarskih vježbi	Analiza klasične literature Analiza literature na webu, knowledge mining Pisanje eseja				
Sadržaj predavanja	1.Osnovni pojmovi, 2h, Ishodi:1 2.Proces etičkog hakiranja i odgovornosti etičkog hakera, 2h, Ishodi:2,3,5 3.Analiza sustava, 2h, Ishodi:1,3 4.Istraživanje web sjedišta, Korištenje aktivnih/pasivnih metoda, 2h, Ishodi:1,3,4 5.Skeniranje portova, Pronalazak OS, 2h, Ishodi:2,4 6.Iskorištavanje ranjivosti sustava za izvršavanje malicioznog koda, 2h, Ishodi:1,2 7.Upravljanje sjednicama (sesijama) i kolačićima, 2h, Ishodi:1,2 8.Vrste napada, 2h, Ishodi:5,6 9.Alati, Obrambene strategije, 2h, Ishodi:4,5,6 10.Ranjivosti web servera, 2h, Ishodi:2,3,6 11.Otkrivanje korisničkih imena, Otkrivanje lozinki, 2h, Ishodi:3,4 12.Identifikacija procesa, 2h, Ishodi:6 13.Korištenje alata etičkog hakiranja, 2h, Ishodi:4,6 14.Izrada i oblikovanje izvještaja, 2h, Ishodi:4,6 15.Ranjivosti web servera, 2h, Ishodi:2,6				
Sadržaj laboratorijskih vježbi	1.Uvod u vježbe etičkog hakiranja, 2h, Ishodi:1,2 2.Istraživanje (profiliranje) i analiza ciljane organizacije, 2h, Ishodi:2 3.Analiza incidenata, log datoteka, 2h, Ishodi:2,3 4.Korištenje alata (ping, nslookup, nmap, telnet), 2h, Ishodi:4,5,6 5.Korištenje online alata (netcraft, ripe), 2h, Ishodi:4 6.Uvod i korištenje Google Hacking, 2h, Ishodi:4 7.Korištenje alata i tehnika za skeniranje portova, 2h, Ishodi:4,6 8.Istraživanje ranjivosti web aplikacija, sql injection, 2h, Ishodi:4 9.Provjera ranjivosti autentifikacije/autorizacije, 2h, Ishodi:4,6 10.Korištenje proxy-a (Burp Suite), 2h, Ishodi:5,6 11.Nema nastave 12.Nema nastave 13.Nema nastave 14.Nema nastave 15.Nema nastave				
Sadržaj seminarskih vježbi	1.Definiranje teme seminarskog rada, 2h, Ishodi:5,6 2.Izrada seminarskog rada, 6h, Ishodi:4,5,6 3.Prezentacija seminarskog rada, 2h, Ishodi:6 4.Nema nastave, 2h 5.Nema nastave 6.Nema nastave 7.Nema nastave 8.Nema nastave 9.Nema nastave 10.Nema nastave 11.Nema nastave 12.Nema nastave				



	13.Nema nastave 14.Nema nastave 15.Nema nastave												
Materijalni uvjeti za izvedbu predmeta	Elementarni: predavaona, ploča, kreda... Namjenski računalni laboratorij Projektor												
Ishodi	6#7												
Literatura	1.Oriyano Sean-Philip,CEHV8 - Certified Ethical Hacker, John Wiley Sons, Inc., Indianapolis, Indiana, ISBN 978-1-118-64767-7, 2014 2.CARNet CERT, Metodologija penetracijskog testiranja, CARNet CERT, 2008												
Uvjeti za potpis (obaveze studenta)	Pohađanje nastave minimalno 80% Izrada i prezentacija seminarskog rada												
Provjera znanja u semestru	Laboratorijske vježbe ili seminar do 50 bodova #61655;Dva kolokvija po 25 bodova (Svaki kolokvij ima popravak) #61655;Opcionalni bodovi za zalaganje #61655;												
Način polaganja ispita nakon semestra	Ukoliko student ne položi kolokvije ima mogućnost izlaska na usmeni ispit. #61655;Ukupno maksimalno 100 bodova #61655;0-49 - nedovoljan #61655;50-61 - dovoljan #61655;62-74 - dobar #61655;75-86 - vrlo dobar #61655;87-100 - izvrstan												
Praćenje rada studenta:	<table><thead><tr><th>Aktivnost</th><th>ECTS</th></tr></thead><tbody><tr><td>Pohađanje nastave ()</td><td>1</td></tr><tr><td>Seminarski rad ()</td><td>1</td></tr><tr><td>Pismeni ispit ()</td><td>2</td></tr><tr><td>Usmeni ispit ()</td><td>1</td></tr><tr><td>Praktični rad ()</td><td>1</td></tr></tbody></table>	Aktivnost	ECTS	Pohađanje nastave ()	1	Seminarski rad ()	1	Pismeni ispit ()	2	Usmeni ispit ()	1	Praktični rad ()	1
Aktivnost	ECTS												
Pohađanje nastave ()	1												
Seminarski rad ()	1												
Pismeni ispit ()	2												
Usmeni ispit ()	1												
Praktični rad ()	1												
Napomena	Iz ovog predmeta moguća je izrada završnog/diplomskog rada												
Preduvjeti:	Nema preduvjeta												
Izradio prijedlog	mr.sc. Marinko Žagar viši predavač, 17.6.2019												



Šifra WEB/ISVU	25223/173042	ECTS	5.0	Akadska godina	2019/2020
Naziv	Forenzika ra?unalnih mreža				
Status	3. semestar - Politehni?ki specijalisti?ki diplomski studij, Informacijska sigurnost i digitalna forenzika (Izvanredni specijalisti?ki informacijska sigurnost i digitalna forenzika) - Obavezni predmet				
Izvedba nastave	Predavanja + vježbe (auditorne+laboratorij+seminar+konstrukcijske) Samostalan rad			30+20 (0+10+10+0) 100	
Izvođa?i	Predavanja:1. dr.sc. Damir Delija Laboratorijske vježbe: Savina Grui?ić Laboratorijske vježbe: Krešimir Hausknecht Seminarske vježbe:dr.sc. Damir Delija				
Cilj predmeta	Upoznati studente sa metodama, tehnikama i alatima za provođenje analize ra?unalnih mreža na postojanje digitalnih tragova.				
Ishodi u?enja:	1.ispitati ra?unalnu mrežu na postojanje digitalnih tragova. Razina:6 2. kriti?ki prosuđivati alate za monitoring ra?unalnih mreža. Razina:7 3. kriti?ki prosuđivati proces autentifikacije i autorizacije. Razina:7 4. formulirati / oblikovati model topologije ra?unalnih mreža. Razina:6,7 5. izgraditi izvještaje o provedenoj digitalno forenzi?koj istrazi ra?unalnih mreža. Razina:6,7 6.kombinirati model otvorenog sustava ISO OSI. Razina:6,7				
Na?in izvođenja predavanja	Frontalna, ex cathedra Gost, predava?i Analiza primjera, case studies Diskusija problema Pitanja - odgovori				
Na?in izvođenja laboratorijskih vježbi	Laboratorijske, simulacije na ra?unalima Grupno rješavanje zadanih problema Ra?unalne simulacije Međusobno zadavanje i rješavanje problema Radionica				
Na?in izvođenja seminarskih vježbi	Grupno rješavanje zadanih problema Analiza literature na webu, knowledge mining Pisanje eseja Međusobno zadavanje i rješavanje problema				
Sadržaj predavanja	1.Vrste mreža, mrežne tehnologije, uređaji, 2h, Ishodi:4,6 2.Povijest interneta, osnove www, url, html, 2h, Ishodi:3,4,6 3.Otvoreni sustav međusobnog povezivanja Model 7 slojeva, 2h, Ishodi:4,6 4.Transport Control Protocol/Internet Protocol, 2h, Ishodi:4,6 5.Povjerljivosti, integritet i raspoloživosti, autentifikacija, autorizacija i dostupnost, 2h, Ishodi:3 6.Sigurnosni identifikator - SID, Vatrozid, 2h, Ishodi:1,2 7.Otkrivanje upada u sustav, prevencija, 2h, Ishodi:3,4,5 8.Sustav imena domena, mrežni protokoli, 2h, Ishodi:1,2,5,6 9.Mrežni Alati za analizu Log: Splunk, 2h, Ishodi:4,5,6 10.Linux alati za analizu mrežnih prometa, 2h, Ishodi:2,3,4 11.Wireshark mrežno hvatanje i analiza paketa, 2h, Ishodi:2,3,5 12.Studije slu?aja, 3h, Ishodi:2,3,4 13. izgraditi izvještaje o provedenoj digitalno forenzi?koj istrazi ra?unalnih mreža , 3h, Ishodi:5,6 14.Nema nastave, 2h 15.Nema nastave, 2h				
Sadržaj laboratorijskih vježbi	1.Primjenjivanje alata za nadzor mrežnog prometa, 2h, Ishodi:1,2 2.Korištenje alata za analizu mrežnog prometa, 1h, Ishodi:1,2 3.Izvesti analizu ra?unalnih mreža na digitalne tragove, 1h, Ishodi:1,5 4.Ispitati sigurnost ra?unalne mreže na upade, 1h, Ishodi:1,2,3 5.Ispitati mrežne servere na postojanje digitalnih tragova, 1h, Ishodi:1,2,3 6.Primijeniti alate za ispitivanje digitalnih tragova, 1h, Ishodi:1,2,3,4,5,6 7.Primijeniti Linux alate za nadzor mrežnog prometa, 1h, Ishodi:4,5,6 8.Izraditi izvještaje o provedenoj digitalno forenzi?koj analizi mrežnih resursa, 2h, Ishodi:4,5,6 9.Nema nastave, 2h 10.Nema nastave, 2h 11.Nema nastave, 2h 12.Nema nastave, 2h 13.Nema nastave, 2h 14.Nema nastave, 2h 15.Nema nastave, 2h				
Sadržaj seminarskih vježbi	1.Definiranje teme seminarskog rada, 2h, Ishodi:1,2,3,4,5,6 2.Pisanje seminarskog rada, 6h, Ishodi:1,2,3,4,5,6 3.Prezentiranje seminarskog rada, 2h, Ishodi:1,2,5,6 4.Nema nastave, 2h 5.Nema nastave, 2h 6.Nema nastave, 2h 7.Nema nastave, 2h 8.Nema nastave, 2h 9.Nema nastave, 2h				



	10.Nema nastave, 2h 11.Nema nastave, 2h 12.Nema nastave, 2h 13.Nema nastave, 2h 14.Nema nastave, 2h 15.Nema nastave, 2h
Materijalni uvjeti za izvedbu predmeta	Elementarni: predavaona, ploča, kreda... Namjenski laboratorij Računalni laboratorij opće namjene Projektor
Ishodi	6#7
Literatura	1. EC-Council Press,Computer Forensics: Investigating File and Operating Systems, Wireless Networks and Storage, EC-Council Press, 9781305883482, 2016 2. Clint P Garrison i dr.,Digital Forensics for Network, Internet, and Cloud Comp, Syngress, 9781597495370, 2010
Uvjeti za potpis (obaveze studenta)	Pohađanje nastave minimalno 80% Izrada i prezentacija seminarskog rada
Provjera znanja u semestru	Laboratorijske vježbe ili seminar do 50 bodova #61655;Dva kolokvija po 25 bodova (Svaki kolokvij ima popravak) #61655;Opcionalni bodovi za zalaganje
Način polaganja ispita nakon semestra	Ukoliko student ne položi kolokvije ima mogućnost izlaska na usmeni ispit. #61655;Ukupno maksimalno 100 bodova #61655;0-49 - nedovoljan #61655;50-61 - dovoljan #61655;62-74 - dobar #61655;75-86 - vrlo dobar #61655;87-100 - izvrstan
Praćenje rada studenta:	Aktivnost ECTS Pohađanje nastave () 1 Pismeni ispit () 2 Usmeni ispit () 1 Seminarski rad () 1
Napomena	Iz ovog predmeta moguća je izrada završnog/diplomskog rada
Preduvjeti:	Nema preduvjeta
Izradio prijedlog	mr.sc. Marinko Žagar viši predavač, 18.6.2019



Šifra WEB/ISVU	25220/173039	ECTS	5.0	Akademski godina	2019/2020
Naziv	Forenzika mobilnih uređaja				
Status	3. semestar - Politehnički specijalistički diplomski studij, Informacijska sigurnost i digitalna forenzika (Izvanredni specijalistički informacijska sigurnost i digitalna forenzika) - Izborni predmet				
Izvedba nastave	Predavanja + vježbe (auditorne+laboratorij+seminar+konstrukcijske) Samostalan rad			30+20 (0+10+10+0) 100	
Izvođači	Predavanja:1. dr.sc. Damir Delija Laboratorijske vježbe: Krešimir Hausknecht Seminarske vježbe:dr.sc. Damir Delija				
Cilj predmeta	Upoznati studente s forenzikom mobilnih uređaja, alatima, postupcima i izradom izvještaja nakon provedene digitalno forenzičke analize mobilnih uređaja.				
Ishodi učenja:	1.analizirati i kategorizirati digitalne tragove mobilnih uređaja. Razina:6 2.ispitati mobilni uređaj na postojanje digitalnih tragova. Razina:6 3. formulirati / oblikovati izvještaje o provedenoj digitalno forenzičkoj istrazi mobilnih uređaja. Razina:6,7 4. klasificirati digitalne tragove. Razina:6,7 5. odabrati alate za obavljanje osnovnih ekstrakcije podataka sa mobilnog uređaja. Razina:7 6. voditi digitalno forenzičke analize u skladu sa zakonskim smjernicama. Razina:6,7				
Način izvođenja predavanja	Frontalna, ex cathedra Gost, predavač Analiza primjera, case studies Diskusija problema Pitanja - odgovori				
Način izvođenja laboratorijskih vježbi	Laboratorijske, simulacije na računalima Rasprave, brainstorming Računalne simulacije				
Način izvođenja seminarskih vježbi	Analiza literature na webu, knowledge mining Pisanje eseja Radionica				
Sadržaj predavanja	1.Digitalna forenzika i vrste digitalne forenzike, 2h, Ishodi:1,4 2.Digitalno forenzički procesi, digitalni dokazi, prikupljanje i spremanje dokaza, 2h, Ishodi:1,2,4,5 3.Proces trijaže, 2h, Ishodi:1,4 4.Proces prikupljanja dokaza, 2h, Ishodi:1,2,4 5.Mobilni uređaji, proizvođači, platforme, 2h, Ishodi:1 6.Mobilne mreže i tehnologije, 2h, Ishodi:1 7.SIM kartice, kloniranje, mrežna izolacija, 2h, Ishodi:2,5 8.Logička vs fizička ekstrakcija, 2h, Ishodi:3,4 9.Alati, metode, agenti, bootloaders, 2h, Ishodi:1,2,3,4,5 10.Flash memorije, arhitektura (NAND, NOR), 2h, Ishodi:1,2,5 11.Rukovanje s dokazima, 2h, Ishodi:1,4,6 12.iOS, 2h, Ishodi:1 13.Android sustav, 2h, Ishodi:1,5 14.PLists i SQL baza podataka, 2h, Ishodi:1 15.Vođenje digitalno forenzičkih istraga i izrada izvještaja , 2h, Ishodi:1,3				
Sadržaj laboratorijskih vježbi	1.Prepoznavanje vrsta i modela mobilnih uređaja, 1h, Ishodi:2,6 2.Poznavanje operacijskih sustava mobilnih uređaja, 1h, Ishodi:2 3.Poznavanje metodologije rukovanja sa digitalnim dokazima, 1h, Ishodi:3,4 4.Primjenjivanje digitalno forenzičkih alata, 1h, Ishodi:1,5 5.Primjenjivanje alata za ekstrakciju podataka sa mobilnih uređaja, 1h, Ishodi:3,4 6.Rad sa digitalnim dokazima u skladu sa zakonskim odredbama, 1h, Ishodi:2,4 7.Poznavanje arhitekture mobilnih uređaja, 1h, Ishodi:3,5 8.Poznavanje uređaja za pohranu digitalnih dokaza, 1h, Ishodi:4,5 9.Izrađivanje izvještaja o provedenoj istrazi, 2h, Ishodi:4,5 10.Nema nastave 11.Nema nastave 12.Nema nastave 13.Nema nastave 14.Nema nastave 15.Nema nastave				
Sadržaj seminarskih vježbi	1.Definiranje teme seminarskog rada, 2h, Ishodi:1,2 2.Pisanje seminarskog rada, 6h, Ishodi:3,4 3.Prezentiranje seminarskog rada, 2h, Ishodi:1,2,5,6 4.Nema nastave 5.Nema nastave 6.Nema nastave 7.Nema nastave 8.Nema nastave 9.Nema nastave 10.Nema nastave 11.Nema nastave 12.Nema nastave 13.Nema nastave				



	14.Nema nastave 15.Nema nastave
Materijalni uvjeti za izvedbu predmeta	Elementarni: predavaona, ploča, kreda... Namjenski laboratorij Namjenski računalni laboratorij Projektor
Ishodi	6#7
Literatura	1.Devices Eamon P. Doherty,Digital Forensics for Handheld Devices,CRC Press,978-1-4398-9878-9, 2013 2.Angel Alonso-Parrizas, Forensic Analysis On Android: A Practical Case,SANS Institute, 2015 3.CARNet CERT, Wireless forenzika,CARNet CERT, 2008
Uvjeti za potpis (obaveze studenta)	Pohađanje nastave minimalno 80% Izrada i prezentacija seminarskog rada
Provjera znanja u semestru	Laboratorijske vježbe ili seminar do 50 bodova #61655;Dva kolokvija po 25 bodova (Svaki kolokvij ima popravak) #61655;Opcionalni bodovi za zalaganje
Način polaganja ispita nakon semestra	Ukoliko student ne položi kolokvije ima mogućnost izlaska na usmeni ispit. #61655;Ukupno maksimalno 100 bodova #61655;0-49 - nedovoljan #61655;50-61 - dovoljan #61655;62-74 - dobar #61655;75-86 - vrlo dobar #61655;87-100 - izvrstan
Praćenje rada studenta:	Aktivnost ECTS Pohađanje nastave () 1 Seminarski rad () 2 Usmeni ispit () 1 Pismeni ispit () 1
Napomena	Iz ovog predmeta moguća je izrada završnog/diplomskog rada
Preduvjeti:	Nema preduvjeta
Izradio prijedlog	mr.sc. Marinko Žagar viši predavač, 17.6.2019



Šifra WEB/ISVU	25224/173043	ECTS	5,0	Akadska godina	2019/2020
Naziv	Forenzika radne memorije				
Status	3. semestar - Politehni?ki specijalisti?ki diplomski studij, Informacijska sigurnost i digitalna forenzika (Izvanredni specijalisti?ki informacijska sigurnost i digitalna forenzika) - Obavezni predmet				
Izvedba nastave	Predavanja + vje?be (auditorne+laboratorij+seminar+konstrukcijske) Samostalan rad			30+20 (0+10+10+0) 100	
Izvođa?i	Predavanja:1. dr.sc. Damir Delija Laboratorijske vje?be: Savina Grui?ić Laboratorijske vje?be: Davorka Topol?ić Seminarske vje?be:dr.sc. Damir Delija				
Cilj predmeta	Upoznati studente s forenzikom radne memorije, alatima, postupcima i izradom izvještaja nakon provedene digitalno forenzi?ke analize radne memorije uređaja.				
Ishodi u?enja:	1.analizirati radnu memoriju. Razina:6 2.identificirati regularne procese u radnoj memoriji. Razina:6 3.analizirati sadržaj radne memorije na postojanje virusa. Razina:6 4. kombinirati alate za spremanje i analizu radne me. Razina:6,7 5. samoprocijeniti procedure za spremanje podataka iz memorije računala. Razina:7 6. izgraditi izvještaje o provedenoj digitalno forenzi?koj istrazi radne memorije. Razina:6,7 7. prosuditi alate za analizu RAM-a. Razina:7				
Na?in izvođenja predavanja	Frontalna, ex cathedra Gost, predava?i Analiza primjera, case studies Simulacije Pitanja - odgovori				
Na?in izvođenja laboratorijskih vje?bi	Laboratorijske, simulacije na računalima Rasprave, brainstorming Ra?unalne simulacije Međusobno zadavanje i rješavanje problema				
Na?in izvođenja seminarskih vje?bi	Laboratorijske, simulacije na računalima Pisanje eseja Međusobno zadavanje i rješavanje problema				
Sadržaj predavanja	1.Tradicionalna forenzika vs. Forenzika radne memorije, 3h, Ishodi:1,2 2.Razlike u operacijskim sustavima u pogledu promjenjivih podataka (Volatile Data), 3h, Ishodi:1,2,3,4,5,6,7 3.Snimanje mjesta analize, 3h, Ishodi:7 4.Rad sa ugašenim ili upaljenim računalom, 3h, Ishodi:1,2,3 5.Prikupljanje podataka , 3h, Ishodi:1,6,7 6.Rad sa kriptiranim diskom, 3h, Ishodi:3,4,5,6,7 7.Dokumentiranje svih uređaja, 3h, Ishodi:5,6,7 8.Izrada kopija svih nositelja zapisa, 3h, Ishodi:4,5,6,7 9.Dokumentiranje svih koraka, 3h, Ishodi:4,5,7 10.Izraditi izvještaje o provedenoj digitalno forenzi?koj istrazi radne memorije, 3h, Ishodi:7 11.Nema nastave, 2h 12.Nema nastave, 2h 13.Nema nastave, 2h 14.Nema nastave, 2h 15.Nema nastave, 2h				
Sadržaj laboratorijskih vje?bi	1.Upotrebe alata Volatility za analizu radne memorije , 2h, Ishodi:1,2,3,4,5,6,7 2.Korištenje alata za rad sa kriptiranim uređ, 2h, Ishodi:1,2,3 3.Izrada izvještaja o provedenoj digitalno forenzi?koj analizi. 2h, Ishodi:5,6,7 4.Korištenje uređaja za izradu kopija podataka, 2h, Ishodi:5,6,7 5.Korištenja procedura u akviziciji podataka uklju?enih sustava, 2h, Ishodi:1,2,3,4,5,6,7 6.Nema nastave, 2h 7.Nema nastave, 2h 8.Nema nastave, 2h 9.Nema nastave, 2h 10.Nema nastave, 2h 11.Nema nastave, 2h 12.Nema nastave, 2h 13.Nema nastave, 2h 14.Nema nastave, 2h 15.Nema nastave, 2h				
Sadržaj seminarskih vje?bi	1.Definiranje teme seminarskog rada, 2h, Ishodi:1,2,3 2.Pisanje seminarskog rada, 6h, Ishodi:1,2,3,4,5,6,7 3.Prezentiranje seminarskog rada, 2h, Ishodi:5,6,7 4.Nema nastave, 2h 5.Nema nastave, 2h 6.Nema nastave, 2h 7.Nema nastave, 2h 8.Nema nastave, 2h 9.Nema nastave, 2h 10.Nema nastave, 2h				



	11.Nema nastave, 2h 12.Nema nastave, 2h 13.Nema nastave, 2h 14.Nema nastave, 2h 15.Nema nastave, 2h
Materijalni uvjeti za izvedbu predmeta	Elementarni: predavaona, ploča, kreda... Namjenski računalni laboratorij Projektor
Ishodi	6#7
Literatura	1.EC-Council Press,Computer Forensics: Investigating File and Operating Systems, Wireless Networks and Storage, EC-Council Press, 9781305883482, 2016 2.Geetha,Combating Security Breaches and Criminal Activity in the Digital Sphere ,IGI Global, 978-1522501930,2016 3.Dr. Philip Polstra,Windows Forensics,Pentester Academy, 2016 4.1.Cameron H. Malin, Eoghan Casey, James M. Aquilina,Malware Forensics Field Guide for Linux Systems, Syngress, 978-1597494700, 2014
Uvjeti za potpis (obaveze studenta)	Pohađanje nastave minimalno 80% Izrada i prezentacija seminarskog rada
Provjera znanja u semestru	Laboratorijske vježbe ili seminar do 50 bodova #61655;Dva kolokvija po 25 bodova (Svaki kolokvij ima popravak) #61655;Opcionalni bodovi za zalaganje
Način polaganja ispita nakon semestra	Ukoliko student ne položi kolokvije ima mogućnost izlaska na usmeni ispit. #61655;Ukupno maksimalno 100 bodova #61655;0-49 - nedovoljan #61655;50-61 - dovoljan #61655;62-74 - dobar #61655;75-86 - vrlo dobar #61655;87-100 - izvrstan
Praćenje rada studenta:	Aktivnost ECTS Pohađanje nastave () 1 Seminarski rad () 1 Usmeni ispit () 1 Pismeni ispit () 2
Napomena	Iz ovog predmeta moguća je izrada završnog/diplomskog rada
Preduvjeti:	Nema preduvjeta
Izradio prijedlog	mr.sc. Marinko Žagar viši predavač, 18.6.2019



Šifra WEB/ISVU	25222/173041	ECTS	5,0	Akadska godina	2019/2020
Naziv	Forenzika zlonamjernih programa				
Status	3. semestar - Politehni?ki specijalisti?ki diplomski studij, Informacijska sigurnost i digitalna forenzika (Izvanredni specijalisti?ki informacijska sigurnost i digitalna forenzika) - Obavezni predmet				
Izvedba nastave	Predavanja + vjezbe (auditorne+laboratorij+seminar+konstrukcijske) Samostalan rad			30+20 (0+10+10+0) 100	
Izvođači	Predavanja:1. dr.sc. Damir Delija Laboratorijske vjezbe: Savina Gruičić Laboratorijske vjezbe: Davorka Topolčić Seminarske vjezbe:dr.sc. Damir Delija Seminarske vjezbe: Davorka Topolčić				
Cilj predmeta	Upoznati studente za zlonamjernih programima, alatima za analizu zlonamjernih programa, provođenjem analize i pisanjem izvještaja o provedenim analizama zlonamjernih programa.				
Ishodi učenja:	1. kreirati analizu sustava na postojanje zlonamjernih programa. Razina:6,7 2. formulirati / oblikovati izvještaje o provedenoj digitalno forenzičkoj analizi zlonamjernih programa. Razina:6,7 3.voditi postupak analize i identifikacije zlonamjernih programa. Razina:6,7 4.analizirati ponašanje zlonamjernih programa. Razina:6 5.analizirati zlonamjernih programa na Windows platformi. Razina:6 6. kritički prosuđivati zlonamjernih programa na Linux platformi. Razina:7				
Način izvođenja predavanja	Frontalna, ex cathedra Gost, predavač Analiza primjera, case studies Diskusija problema Pitanja - odgovori				
Način izvođenja laboratorijskih vježbi	Laboratorijske s laboratorijskom opremom Laboratorijske, simulacije na računalima Rasprave, brainstorming Međusobno zadavanje i rješavanje problema				
Način izvođenja seminarskih vježbi	Pisanje eseja Međusobno zadavanje i rješavanje problema Radionica				
Sadržaj predavanja	1.Taksonomija zlonamjernih programa, 2h, Ishodi:5,6 2.Prijetnje zlonamjernih programa, 2h, Ishodi:5,6 3.Pravni aspekti, 2h, Ishodi:1,2,3 4.Identifikacija i zaštita od zlonamjernih programa, 2h, Ishodi:1,2,3,4 5.Alati za analizu zlonamjernih programa, 2h, Ishodi:1,3 6.Analiza zlonamjernih progarma prema potpisu datoteka, 2h, Ishodi:1,6 7.Nadziranje računalnih procesa, 2h, Ishodi:4,5 8.Analiza i rad registy-a, 2h, Ishodi:4,5 9.Analiza i nadzor mrežnog prometa, 2h, Ishodi:4,5 10.Ranjivosti PDF i Microsoft Office dokumenata, 2h, Ishodi:3,4,5 11. Ekstrakcija zlonamjernog programa i alati za analizu, 2h, Ishodi:4,5,6 12.Otkrivanje Alternate Data Streams s TSK (SleuthKit), 2h, Ishodi:4,5,6 13.Otkrivanje artefakata u memoriji, 2h, Ishodi:4,5,6 14.Analiza mrežnih artefakata od zlonamjernog programa Zaus, 2h, Ishodi:4,5,6 15.Izrada izvještaja o provedenim analizama, 2h, Ishodi:1,2,3				
Sadržaj laboratorijskih vježbi	1.Izvesti sigurno okruženje za rad s zlonamjernih programima, 2h, Ishodi:1,3,4,5 2.Koristiti alate za analizu zlonamjernih programa, 2h, Ishodi:1,2,4,5 3.Primijeniti statičku i dinamičku analizu zlonamjernih dokumenata, 1h, Ishodi:1,4,5 4.Izvesti analizu mrežnog prometa, 1h, Ishodi:1,2,4,5 5.Primjena alata za analizu registry-a, 1h, Ishodi:1,3,4,5 6.Primjena alata za analizu zlonamjernih programa na Windows platformi, 1h, Ishodi:3,4,5 7.Primjena alata za analizu zlonamjernih programa na Linux platformi, 1h, Ishodi:3,4,5 8.Primjenjivati alate za analizu RAM-a, 1h, Ishodi:2,4,5 9.Nema nastave, 2h 10.Nema nastave, 2h 11.Nema nastave, 2h 12.Nema nastave, 2h 13.Nema nastave, 2h 14.Nema nastave, 2h 15.Nema nastave, 2h				
Sadržaj seminarskih vježbi	1.Definiranje teme seminarskog rada, 2h, Ishodi:1,2 2.Pisanje seminarskog rada, 6h, Ishodi:3,4 3.Prezentiranje seminarskog rada, 2h, Ishodi:1,2,5,6 4.Nema nastave, 2h 5.Nema nastave, 2h 6.Nema nastave, 2h 7.Nema nastave, 2h 8.Nema nastave, 2h 9.Nema nastave, 2h 10.Nema nastave, 2h				



	11.Nema nastave, 2h 12.Nema nastave, 2h 13.Nema nastave, 2h 14.Nema nastave, 2h 15.Nema nastave, 2h
Materijalni uvjeti za izvedbu predmeta	Elementarni: predavaona, ploča, kreda... Namjenski računalni laboratorij Projektor
Ishodi	6#7
Literatura	1.Michael Ligh, Steven Adair, Blake Hartstein, Matthew Richard ,Malware Analyst's Cookbook: Tools and Techniques for Fighting Malicious Code,Wiley,978-0-470-61303-0,2010 2.Open Source,Open Source Cyber Security Learning
Uvjeti za potpis (obaveze studenta)	Pohađanje nastave minimalno 80% Izrada i prezentacija seminarskog rada
Provjera znanja u semestru	Laboratorijske vježbe ili seminar do 50 bodova #61655;Dva kolokvija po 25 bodova (Svaki kolokvij ima popravak) #61655;Opcionalni bodovi za zalaganje
Način polaganja ispita nakon semestra	Ukoliko student ne položi kolokvije ima mogućnost izlaska na usmeni ispit. #61655;Ukupno maksimalno 100 bodova #61655;0-49 - nedovoljan #61655;50-61 - dovoljan #61655;62-74 - dobar #61655;75-86 - vrlo dobar #61655;87-100 - izvrstan
Praćenje rada studenta:	Aktivnost ECTS Pohađanje nastave () 1 Pismeni ispit () 1 Seminarski rad () 2 Usmeni ispit () 1
Napomena	Iz ovog predmeta moguća je izrada završnog/diplomskog rada
Preduvjeti:	Nema preduvjeta
Izradio prijedlog	mr.sc. Marinko Žagar viši predavač, 17.6.2019



Šifra WEB/ISVU	24962/173027	ECTS	6.0	Akadska godina	2019/2020
Naziv	Informacijska sigurnost				
Status	1. semestar - Politehni?ki specijalisti?ki diplomski studij, Informacijska sigurnost i digitalna forenzika (Izvanredni specijalisti?ki informacijska sigurnost i digitalna forenzika) - Obavezni predmet				
Izvedba nastave	Predavanja + vjezbe (auditorne+laboratorij+seminar+konstrukcijske) Samostalan rad			30+30 (0+15+15+0) 120	
Izvođači	Predavanja:1. mr.sc. Marinko Žagar viši predavač Laboratorijske vjezbe: Marin Rak Laboratorijske vjezbe: Domagoj Tuličić Seminarske vjezbe:mr.sc. Marinko Žagar viši predavač				
Cilj predmeta	Upoznavanje studenata sa konceptima, standardima, rizicima i općenito problematikom Informacijske sigurnosti				
Ishodi učenja:	1.prezentirati koncept sigurnost. Razina:6,7 2. kritički prosuđivati implementirane standarde sigurnosti. Razina:7 3.prezentirati standarde i politike sigurnosti. Razina:6,7 4.procijeniti sigurnosne prijetnje i ranjivosti. Razina:6,7 5.analizirati zlonamjerne programe i zaštitu od zlonamjernih programa. Razina:6 6.procijeniti sigurnost aplikacija iz oblaka. Razina:6,7 7. ocijeniti implementirane sigurnosne standarde. Razina:7				
Način izvođenja predavanja	Frontalna, ex cathedra Gost, predavač Analiza primjera, case studies Diskusija problema Pitanja - odgovori				
Način izvođenja laboratorijskih vjezbi	Laboratorijske s laboratorijskom opremom Laboratorijske, simulacije na računalima Rasprave, brainstorming Radionica				
Način izvođenja seminarskih vjezbi	Analiza klasične literature Analiza literature na webu, knowledge mining Pisanje eseja Radionica				
Sadržaj predavanja	1.Uvod u informacijsku sigurnost, 1h, Ishodi:4 2.Kibernetička sigurnost, 1h, Ishodi:6 3.Prijetnje informacijskim sustavima, 1h, Ishodi:4,5,6 Krađa identiteta, 1h, Ishodi:5 Oblici i mjere zaštite, 1h, Ishodi:7 4.Zakonodavni okvir elektroničkog poslovanja, 2h, Ishodi:3 Zakon o informacijskoj sigurnosti, 1h, Ishodi:3 5.ISO standardi informacijske sigurnosti, 2h, Ishodi:3 6.Implementacija sustava upravljanja informacijskom sigurnošću, 2h, Ishodi:1,3,7 7.Infrastruktura javnog ključa (PKI), 2h, Ishodi:2 8.Računalni kriminal, 2h, Ishodi:4,5 9.Zlonamjerni programi, 2h, Ishodi:5 10.Zaštita od zlonamjernih programa, 2h, Ishodi:5 11.Arhitektura web aplikacija, 2h, Ishodi:4 12.Vrste napada na bežične mreže, 2h, Ishodi:4 13.Metode zaštite bežičnih mreža, 2h, Ishodi:1,4 14.Sigurnosni problemi i rizici računalstva u oblaku, 2h, Ishodi:6 15.Sigurnosne preporuke računalstva u oblaku CSA, 2h, Ishodi:6				
Sadržaj laboratorijskih vjezbi	1.Sustav upravljanja informacijskom sigurnošću, 3h, Ishodi:2,7 2.Zakonska usklađenost, 2h, Ishodi:3 3.Usklađenost s normom ISO 27001:2013, 2h, Ishodi:2,3,7 4.Politika sigurnosti, 2h, Ishodi:2,7 5.Analiza sigurnosti IS, 2h, Ishodi:4,6,7 6.Analiza usklađenosti organizacije sa ISO normom 27000, 2h, Ishodi:3,7 7.Uпотреba alata za provjeru ranjivosti i IDS-a, 2h, Ishodi:4,5 8.Nema nastave 9.Nema nastave 10.Nema nastave 11.Nema nastave 12.Nema nastave 13.Nema nastave 14.Nema nastave 15.Nema nastave				
Sadržaj seminarskih vjezbi	1.Definiranje zadatka seminaraskog rada, 3h, Ishodi:1,2,3,4,5,6,7 2.Izrada seminaraskog rada, 2h 3.Izrada seminaraskog rada, 2h 4.Izrada seminaraskog rada, 2h 5.Izrada seminaraskog rada, 2h 6.Izrada seminaraskog rada, 2h 7.Izrada seminaraskog rada, 2h				



	8.Nema nastave 9.Nema nastave 10.Nema nastave 11.Nema nastave 12.Nema nastave 13.Nema nastave 14.Nema nastave 15.Nema nastave, 2h
Materijalni uvjeti za izvedbu predmeta	Elementarni: predavaona, ploča, kreda... Namjenski računalni laboratorij Bijela ploča sa flomasterima Projektor
Ishodi	6#7
Literatura	1.K. Antoliš et all.: Sigurnost informacijskih sustava, Algebra d.o.o., Zagreb ožujak, 2016 2.Vlada Republike Hrvatske, Nacionalna strategija kibernetičke sigurnosti i akcijski plan za provedbu Nacionalne strategije kibernetičke sigurnosti, NN 150/11 i 119/14, 2015. 3.Hrvatski Sabor, Zakona o zaštiti osobnih podataka sa izmjenama i dopunama, NN 103/03; 118/06, 41/08, 130/11, 2012. 4.Hrvatski Sabor, Zakona o Informacijskoj sigurnosti, NN 79/2007, 2007. 5.Hrvatski Sabor, Zakona o elektroničkom potpisu, NN 10/2002, 2002. 6.Marinko Žagar, Skripta predavanja - Informacijska sigurnost , 2016
Uvjeti za potpis (obaveze studenta)	Predani rezultati laboratorijskih vježbi Predan seminarski rad Prisustvo na nastavi min, 80%
Provjera znanja u semestru	Laboratorijske vježbe ili seminar do 50 bodova Dva kolokvija po 25 bodova (Svaki kolokvij ima popravak) Opcionalni bodovi za zalaganje
Način polaganja ispita nakon semestra	Pismeni ispit Usmeni ispit
Praćenje rada studenta:	Aktivnost ECTS Pismeni ispit () 1 Seminarski rad () 1 Usmeni ispit () 1 Eksperimentalni rad () 1 Aktivnost u nastavi () 1 Kontinuirana provjera znanja () 1
Napomena	Iz ovog predmeta moguća je izrada završnog/diplomskog rada
Preduvjeti:	Nema preduvjeta
Izradio prijedlog	mr.sc. Marinko Žagar viši predavač, 4.6.2018



Šifra WEB/ISVU	24966/173033	ECTS	6.0	Akadska godina	2019/2020
Naziv	Integrirani sustavi informacijske sigurnosti				
Status	2. semestar - Politehni?ki specijalisti?ki diplomski studij, Informacijska sigurnost i digitalna forenzika (Izvanredni specijalisti?ki informacijska sigurnost i digitalna forenzika) - Obavezni predmet				
Izvedba nastave	Predavanja + vježbe (auditorne+laboratorij+seminar+konstrukcijske) Samostalan rad			30+30 (0+20+10+0) 120	
Izvođači	Predavanja:1. Dino Županović Predavanja:mr.sc. Marinko Žagar viši predavač Laboratorijske vježbe:mr.sc. Marinko Žagar viši predavač Laboratorijske vježbe: Dino Županović Seminarske vježbe:mr.sc. Marinko Žagar viši predavač Seminarske vježbe: Dino Županović				
Cilj predmeta	Upoznavanje studenata sa integriranim sustavima informacijske sigurnosti				
Ishodi učenja:	1.razlikovati arhitekture sigurnosnih sustava. Razina:6 2.razlikovati sustave integralne sigurnosti. Razina:6 3. izgraditi model informacijske sigurnosti. Razina:6,7 4.dizajnirati integralni sustav sigurnosti. Razina:6 5.procijeniti sustav sigurnosti podataka. Razina:6,7 6.razlikovati sigurnosne sustave za upravljanje pristupu informacijama. Razina:6				
Način izvođenja predavanja	Frontalna, ex cathedra Gost, predavač Analiza primjera, case studies Diskusija problema Pitanja - odgovori				
Način izvođenja laboratorijskih vježbi	Laboratorijske s laboratorijskom opremom Laboratorijske, simulacije na računalima Rasprave, brainstorming Računalne simulacije Međusobno zadavanje i rješavanje problema Radionica				
Način izvođenja seminarskih vježbi	Analiza klasične literature Analiza literature na webu, knowledge mining Pisanje eseja Radionica				
Sadržaj predavanja	1.Informacijska sigurnost, 2h, Ishodi:2,3 2.Prijetnje informacijskoj sigurnosti, 2h, Ishodi:2,3,4 3.Provođenje sigurnosne procjene, 2h, Ishodi:2,3 4.Sigurnosni standardi, politike i procedure, 2h, Ishodi:2 5.Definiranje ciljeva dizajniranog sustava sigurnosti, 2h, Ishodi:3,4 6.Sigurnosna arhitektura (operativnih) sustava, 2h, Ishodi:1,3,4 7.Zaštita nesigurnih podataka, 2h, Ishodi:5,6 8.Upravljanje pravima na pristup informacijama , 2h, Ishodi:5,6 9.Sigurnosna pohrana podataka, 2h, Ishodi:3,5,6 10.Sigurnost baze podataka, 2h, Ishodi:5 11.Sigurnost mrežnih komunikacija i uređaja, 2h, Ishodi:2,3 12.Otkrivanje i sprječavanje sigurnosnih incidenata, 2h, Ishodi:2,3,4,5 13.Upravljanje sigurnosnim operacijama, 2h, Ishodi:2,4 14.Biometrija, 2h, Ishodi:5,6 15.Biometrijske tehnologije, 2h, Ishodi:5,6				
Sadržaj laboratorijskih vježbi	1.Analiza i procjena rizika arhitekture sigurnosti sustava, 2h, Ishodi:1 2.Vježba izrade sigurnosnih kontrola prema standardima, 3h, Ishodi:1,2 3.Vježbe izrade plana implementacije sustava sigurnosti, 2h, Ishodi:2,3 4.Vježba planiranje sustava sigurnosti, 2h, Ishodi:3 5.Vježba primjene zaštite podataka, 2h, Ishodi:6 6.Vježba dizajniranja integralnog sustava sigurnosti, 2h, Ishodi:4 7.Analiziranje i primjena biometrijskih sustava zaštite, 2h, Ishodi:5 8.Nema nastave 9.Nema nastave 10.Nema nastave 11.Nema nastave 12.Nema nastave 13.Nema nastave 14.Nema nastave 15.Nema nastave				
Sadržaj seminarskih vježbi	1.Definiranje zadatka seminarskog rada, 4h, Ishodi:1 2.Izrada seminarskog rada, 2h, Ishodi:2 3.Izrada seminarskog rada, 2h, Ishodi:3 4.Izrada seminarskog rada, 2h, Ishodi:4 5.Izrada seminarskog rada, 2h, Ishodi:5 6.Izrada seminarskog rada, 2h, Ishodi:6 7.Izrada seminarskog rada, 1h, Ishodi:1				



	8.Nema nastave 9.Nema nastave 10.Nema nastave 11.Nema nastave 12.Nema nastave 13.Nema nastave 14.Nema nastave 15.Nema nastave
Materijalni uvjeti za izvedbu predmeta	Elementarni: predavaona, ploča, kreda... Namjenski laboratorij Računalni laboratorij opće namjene Bijela ploča sa flomasterima Projektor
Ishodi	6#7
Literatura	1.Mark Rhodes-Ousley, Information Security: The Complete Reference,MC Graw Hill, 978-0071784351, 2015 2.John R. Vacca, Biometric Technologies and Verification Systems, Elsevier, 978-0-7506-7967-1, 2007 3.Rebeca Wong,Data Security Breaches and Privacy in Europe,Springer, 9781447155850, 2013 4.Ravindra Das,Biometric Technology - Authentication, Biocryptography and Cloud-Based Architecture,CRC Press, 9781466592452, 2015
Uvjeti za potpis (obaveze studenta)	Rad studenata vrednuje se temeljen pohađanja nastave (25 bodova), rješavanja zadataka na vježbama (25 bodova), izradi seminarskog rada (30 bodova), te rezultatu pismenog ispita (20 bodova). Pohađanje i izrada vježbi i seminarskog rada su nužni preduvjeti za dobivanje potpisa i izlazak na pismeni dio ispita. Izvršavajući obveze na kolegiju, student može prikupiti najviše 100 bodova, na temelju čega se formira i konačna ocjena prema slijedećem kriteriju: 0-49 bodova nedovoljan (1) 50-61 bodova dovoljan (2) 62-74 bodova dobar (3) 75-86 bodova - vrlo dobar (4) 87-100 bodova izvrstan (5)
Provjera znanja u semestru	Kratki testovi
Način polaganja ispita nakon semestra	Ako student ima manje od 50% ukupno sakupljenih bodova ili manje od 50% bodova iz pojedinoga kolokvija, predmet može položiti pismenim i usmenim putem na nekom od redovnih ispitnih rokova. 0-49 bodova ocjena nedovoljan (1) 50-59 bodova ocjena dovoljan (2) 60-75 bodova ocjena dobar (3) 76-89 bodova ocjena vrlo dobar (4) 90-100 bodova ocjena izvrstan (5)
Praćenje rada studenta:	Aktivnost ECTS Pohađanje nastave () 1 Pismeni ispit () 2 Seminarski rad () 2 Usmeni ispit () 1
Napomena	Iz ovog predmeta moguća je izrada završnog/diplomskog rada
Preduvjeti:	Nema preduvjeta
Izradio prijedlog	mr.sc. Marinko Žagar viši predavač, 14.6.2018



Šifra WEB/ISVU	25093/185565	ECTS	6.0	Akadska godina	2019/2020
Naziv	IT Forenzika dokumenata i vrijednosnica				
Status	2. semestar - Politehni?ki specijalisti?ki diplomski studij, Informacijska sigurnost i digitalna forenzika (Izvanredni specijalisti?ki informacijska sigurnost i digitalna forenzika) - Izborni predmet				
Izvedba nastave	Predavanja + vje?be (auditorne+laboratorij+seminar+konstrukcijske) Samostalan rad			30+30 (0+30+0+0) 120	
Izvođa?i	Predavanja:1. Aleksandra Bernašek Petrincec Laboratorijske vje?be: Aleksandra Bernašek Petrincec				
Cilj predmeta	Osposobiti studente za korištenje alata te ovladavanje znanjima potrebnim za provedbu forenzike dokumenata i vrijednosnica				
Ishodi u?enja:	1.analizirati osnovne grafi?ke forenzike. Razina:6 2. kriti?ki prosuđivati vrste zaštita na dokumentima i vrijednosnicama. Razina:7 3.razlikovati osnovne metode i tehnologiju. Razina:6 4. izmjeriti uzorke zaštićenih vrijednosnica na instrumentu za digitalnu forenziku. Razina:7 5.analizirati nove tehnologije . Razina:6 6.upravljati i provoditi forenzi?ke analize . Razina:6,7				
Na?in izvođenja predavanja	Frontalna, ex cathedra Analiza primjera, case studies Demonstracije Diskusija problema Pitanja - odgovori Seminar, izlaganje studenta s raspravom Ostalo, upisati Snimanje uzoraka na instrumentu za digitalnu forenziku te upotreba kamera sa IR filterom i UV lampi za prepoznavanje pojedinih zaštita.				
Na?in izvođenja laboratorijskih vje?bi	Laboratorijske s laboratorijskom opremom Grupno rješavanje zadanih problema Analiza literature na webu, knowledge mining Rasprave, brainstorming Ostalo, upisati Docucenter 4500 sa softverom PIA 7000, ?ita? dokumenata, UV lampe i fotoaparati s IR filterom.				
Sadržaj predavanja	1.Pregled vrijednosnica i dokumenata kroz povijest, 2h, Ishodi:1 2.Uvod u forenzi?ku analizu dokumenata i vrijednosnica, 2h, Ishodi:1 3.Vrijednosnice, 2h, Ishodi:1 4.Zaštitni elementi na nov?anicama, 2h, Ishodi:2 5.Osnove o bojama, 2h, Ishodi:3 6.Bojila kao zaštita, 2h, Ishodi:3 7.Suvremena postignuća u zaštiti vrijednosnica i dokumenata, 2h, Ishodi:5 8.Krivotvorine, 2h, Ishodi:1 9.Pokušaji i na?ini krivotvorenja, 2h, Ishodi:4 10.Kriminalisti?ka istra?ivanja, 2h, Ishodi:6 11.Papiri i ostale supstance za izradu dokumenata i vrijednosnica, 2h, Ishodi:3 12.Procedure i procesi ispitivanja izvornosti dokumenata, 2h, Ishodi:6 13.Primjena biometrijske tehnologije u zaštiti dokumenata, 2h, Ishodi:5 14.Tehnike izrade dokumenata i vrijednosnica, 2h, Ishodi:3 15.Forenzi?ka analiza rukopisa, 2h, Ishodi:4,6				
Sadržaj laboratorijskih vje?bi	1.Analiziranje razvijanja dokumenata i vrijednosnica kroz povijest, 2h, Ishodi:1 2.Analiza grafi?kih forenzi?kih metoda, 2h, Ishodi:1 3.Prou?avanje zaštitnih elemenata na dokumentima i vrijednosnicama, 2h, Ishodi:2 4.Identificirati konvencionalne i bez kontaktne tehnike tiska, 2h, Ishodi:3 5.Klasificirati papire, 2h, Ishodi:3 6.Analiza sinteti?kih supstanci za izradu dokumenata i vrijednosnica, 2h, Ishodi:3 7.Prou?avanje karakteristika vizualnog spektra, 2h, Ishodi:2 8.Mjerenje u ultraljubi?astom dijelu spektra, 2h, Ishodi:4 9.Mjerenje u infracrvenom dijelu spektra, 2h, Ishodi:4 10.Uspoređivanje krivotvorenih s originalnim nov?anicama, 2h, Ishodi:4 11.Analiziranje krivotvorenih dokumenata i vrijednosnica, 2h, Ishodi:4 12.Analizirati sustav upravljanja identitetom, 2h, Ishodi:3 13.Analiziranje biometrijskih dokumenata (putovnice), 2h, Ishodi:5 14.Utvrđivanje autenti?nosti potpisa i ?iga, 2h, Ishodi:4 15.Analiziranje izvornosti autorstva rukopisa, 2h, Ishodi:6				
Materijalni uvjeti za izvedbu predmeta	Namjenski laboratorij Ra?unalni laboratorij op?e namjene Bijela plo?a sa flomasterima Projektor Posebna oprema, navesti Docucenter 4500 sa softverom PIA 7000, ?ita? dokumenata, UV lampe i fotoaparati s IR filterom.				
Ishodi	6#7				
Literatura	1. Gordan Mršić, Jasna Galeković, Andrea Ledić, Andrijana Ristović, Nevenka Škavić, Forenzika dokumenata, novca i rukopisa, Hrvatska Sveučilišna Naklada, 978-953-169-286-1, 2014				



	2. Jana Žiljak Vujić, Sigurnosna grafika, Tehničko veleučilište u Zagrebu, Informatičko - računarski odjel, 978-953-7048-33-4, 2014														
Uvjeti za potpis (obaveze studenta)	Pohađanje nastave, vježbi i seminar.														
Provjera znanja u semestru	Praktični rad.														
Način polaganja ispita nakon semestra	Izlaganje seminarskog rada i usmeni ispit.														
Praćenje rada studenta:	<table><thead><tr><th>Aktivnost</th><th>ECTS</th></tr></thead><tbody><tr><td>Pohađanje nastave ()</td><td>1</td></tr><tr><td>Aktivnost u nastavi ()</td><td>1</td></tr><tr><td>Seminarski rad ()</td><td>1</td></tr><tr><td>Praktični rad ()</td><td>1</td></tr><tr><td>Istraživanje ()</td><td>1</td></tr><tr><td>Usmeni ispit ()</td><td>1</td></tr></tbody></table>	Aktivnost	ECTS	Pohađanje nastave ()	1	Aktivnost u nastavi ()	1	Seminarski rad ()	1	Praktični rad ()	1	Istraživanje ()	1	Usmeni ispit ()	1
Aktivnost	ECTS														
Pohađanje nastave ()	1														
Aktivnost u nastavi ()	1														
Seminarski rad ()	1														
Praktični rad ()	1														
Istraživanje ()	1														
Usmeni ispit ()	1														
Napomena	Iz ovog predmeta moguća je izrada završnog/diplomskog rada														
Preduvjeti:	Nema preduvjeta														
Izradio prijedlog	Aleksandra Bernašek Petrinec , 14.6.2018														



Šifra WEB/ISVU	24963/173028	ECTS	6.0	Akadska godina	2019/2020
Naziv	Matematički modeli sigurnosti				
Status	1. semestar - Politehnički specijalistički diplomski studij, Informacijska sigurnost i digitalna forenzika (Izvanredni specijalistički informacijska sigurnost i digitalna forenzika) - Obavezni predmet				
Izvedba nastave	Predavanja + vježbe (auditorne+laboratorij+seminar+konstrukcijske) Samostalan rad			30+30 (0+15+15+0) 120	
Izvođači	Predavanja:1. Goran Sirovatka Predavanja:dr.sc. Vlatko Mičković prof. Laboratorijske vježbe: Goran Sirovatka Seminarske vježbe: Goran Sirovatka				
Cilj predmeta	Program obuhvaća niz različitih tema koje se odnose na matematičko definiranje osnovnih pojmova i operacija diskretne matematike koji se koriste u teoriji informacija i informacijskoj sigurnosti Program obuhvaća teme matematike i matematičkog programiranja, kao podlogu za usvajanje sadržaja inforamcijske sigurnosti i računalne forenzike Cilj predmeta je je osposobiti diplomirane studente primjeni matematičkih alata kako bi mogli dalje pratiti razvoj novih model informacijske sigurnosti te ih primjenjivati. Očekuje se da studenti budu sposobni razumjeti i razviti algoritme temeljem usvojenih znanja. Zahtijeva se samostalan rad studenata.				
Ishodi učenja:	1. pripremiti Primijeniti diskretne matematičke strukture u analizi informacijske sigurnosti. Razina:6,7 2. formulirati / oblikovati Primijeniti algoritme teorije grafova na forenziku društvenih mreža. Razina:6,7 3. sastaviti (prijedlog / rješenje) Razumije i primjenjuje regularne izraze primijeniti ih u digitalnoj forenzici. Razina:6,7 4. razviti Razumjeti modele za kontrolu toka informacija. Razina:6,7 5. razviti Primijeniti logičke modele na dokaze korektnosti programa. Razina:6,7 6. planirati Organizirati matematičke modele informacijske sigurnosti. Razina:6,7				
Način izvođenja predavanja	Frontalna, ex cathedra Gost, predavač Analiza primjera, case studies Simulacije Diskusija problema				
Način izvođenja laboratorijskih vježbi	Laboratorijske s laboratorijskom opremom Laboratorijske, simulacije na računalima Grupno rješavanje zadanih problema Rasprave, brainstorming Računalne simulacije Radionica				
Način izvođenja seminarskih vježbi	Laboratorijske s laboratorijskom opremom Laboratorijske, simulacije na računalima Pisanje eseja Računalne simulacije Radionica				
Sadržaj predavanja	1.Osnovne operacija s cijelim brojevima, Ishodi: 1, 2h, Ishodi:1 2.Boolova algebra, Ishodi: 1, 2h, Ishodi:1 3.Indukcija i rekuzija, Ishodi: 1,5, 2h, Ishodi:1,5 4.Kriptografija i teorija brojeva, Ishodi: 1, 2h, Ishodi:1 5.HASH funkcija, Ishodi: 1, 2h, Ishodi:1 6.Grafovi i Stabla, Ishodi: 2, 2h, Ishodi:2 7.Teorija podudaranja i Bojanja , Ishodi: 2, 2h, Ishodi:2 8.Formalni jezici, Ishodi:1, 3, 2h, Ishodi:1,3 9.Regularni skupovi i izrazi, Ishodi: 3, 2h, Ishodi:3 10.Automati , Ishodi: 3, 2h, Ishodi:3 11.Algoritmi za randomizaciju, Ishodi: 4, 2h, Ishodi:4 12.Algoritmi za validaciju programskog koda Ishod 4, 2h, Ishodi:4 13.Vjerojatnost, Ishodi: 4, 2h, Ishodi:4 14.Logički iskazi i Dokazi, Ishodi: 5, 2h, Ishodi:5 15.Poopćavanje i generalizacija modela sigurnosti , Ishodi: 5, 6, 2h, Ishodi:4,5				
Sadržaj laboratorijskih vježbi	1.Vježbe iz teorije brojeva , Ishodi: 1, 1h, Ishodi:1 2.Vježbe iz matematičke logike , Ishodi: 1 i 5, 1h, Ishodi:1,5 3.Vježbe Kako pretvoriti rekurzivni algoritam u linearani algoritam i obrnuto Ishod 1, 1h, Ishodi:1 4.Vježba prosti brojevi Ishod 1,4, 1h, Ishodi:1,4 5.Vježbe izrade kriptografskih algoritama, Ishodi: 1, 1h, Ishodi:1 6.Vježbe izrade hash algoritma i njegove validacije, Ishodi: 1, 1h, Ishodi:1 7.Vježbe iz teorije grafova i rješavanja NP problema , Ishodi: 2, 1h, Ishodi:2 8.Vježbe - regularni izrazi u digitalnoj forenzici, Ishodi: 3, 1h, Ishodi:3 9.Vježbe - konačni automati , Ishodi: 3, 1h, Ishodi:3 10.Vježbe - logičke operacije u digitalnoj forenzici, Ishodi: 4, 1h, Ishodi:4 11.Vježbe izrade i validacija algoritama za pseudo randomizaciju Ishod 4, 1h, Ishodi:4 12.Vježbe modeliranja informacijskog sustava sigurnosti , Ishodi: 5, 1h, Ishodi:5 13.Vježbe provođenja računa složenih logičkih izraza Ishod 5, 1h, Ishodi:5 14.Vježbe matematički postupak provođenja dokaza Ishod 5, 1h, Ishodi:5 15.Vježbe izrade modela informacijske sigurnosti , Ishodi: 5, 6, 1h, Ishodi:5,6				
Sadržaj seminarskih vježbi	1.Vježbe iz teorije brojeva , Ishodi: 1, 1h, Ishodi:1 2.Vježbe iz matematičke logike , Ishodi: 1 i 5, 1h, Ishodi:1,5 3.Vježbe Kako pretvoriti rekurzivni algoritam u linearani algoritam i obrnuto Ishod 1, 1h, Ishodi:1				



	4.Vježba prosti brojevi Ishod 1,4 Vježbe izrade kriptografskih algoritama, Ishodi: 1, 1h, Ishodi:1 5.Vježbe izrade hash algoritma i njegove validacije, Ishodi: 1, 1h, Ishodi:1 6.1.kolokvij, 1h 7.Vježbe iz teorije grafova i rješavanja NP problema , Ishodi: 2, 1h, Ishodi:2 8.Vježbe - regularni izrazi u digitalnoj forenzici, Ishodi: 3, 1h, Ishodi:2 9.Vježbe - konačni automati , Ishodi: 3, 1h, Ishodi:3 10.Vježbe - logičke operacije u digitalnoj forenzici, Ishodi: 4, 1h, Ishodi:4 11.Vježbe izrada i validacija algoritama za pseudo randomizaciju Ishod 4, 1h, Ishodi:4 12.Vježbe modeliranja informacijskog sustava sigurnosti , Ishodi: 5, 1h, Ishodi:5 13.Vježbe provođenja računa složenih logičkih izraza Ishod 5 Vježbe matematički postupak provođenja dokaza Ishod 5, 1h, Ishodi:5 14.5 Vježbe matematički postupak provođenja dokaza i izrade modela informacijske sigurnosti , Ishodi: 5, 6, 1h, Ishodi:4,5 15.2. kolokvij, 1h
Materijalni uvjeti za izvedbu predmeta	Elementarni: predavaona, ploča, kreda... Računalni laboratorij opće namjene Bijela ploča sa flomasterima Projektor
Ishodi	6#7
Literatura	1.Dujela, Diskretna matematika, skripta 2.Haggard all, Dicrete mathematics for Computer Science, Thompson, ISBN 0-534-49501-X 3.Kenneth Rosen, Discrete mathematics and its Application, McGraw Hill, ISBN 978-0-07-338309-5 1.Čirić, Diskretna matematika OSNOVE KOMBINATORIKE I TEORIJE GRAFOVA, skripta 2007 2.EC-Council Press,Computer Forensics: Investigating File and Operating Systems, Wireless Networks and Storage, EC-Council Press, 9781305883482, 2016 3.S. Geetha,Combating Security Breaches and Criminal Activity in the Digital Sphere ,IGI Global,978-1522501930, 2016 4.Dr. Philip Polstra,Windows Forensics,Pentester Academy, 2016
Uvjeti za potpis (obaveze studenta)	Izrada seminara i vježbi je obvezna za sve studente i uvjet za potpis
Provjera znanja u semestru	Laboratorijske vježbe ili seminar do 50 bodova Dva kolokvija po 25 bodova (Svaki kolokvij ima popravak)
Način polaganja ispita nakon semestra	Ukoliko student ne položi kolokvije ima mogućnost izlaska na usmeni ispit. 0-49 - nedovoljan 50-61 - dovoljan 62-74 - dobar 75-86 - vrlo dobar 87-100 - izvrstan
Praćenje rada studenta:	Aktivnost ECTS Pohadanje nastave () 1 Kontinuirana provjera znanja () 1 Esej () 1 Pismeni ispit () 2 Istraživanje () 1
Napomena	Iz ovog predmeta moguća je izrada završnog/diplomskog rada
Preduvjeti:	Nema preduvjeta
Izradio prijedlog	Goran Sirovatka , 6.6.2018



Šifra WEB/ISVU	25245/173046	ECTS	5.0	Akadska godina	2019/2020
Naziv	Metodologija stručnog i istraživačkog rada				
Status	4. semestar - Politehnički specijalistički diplomski studij, Informacijska sigurnost i digitalna forenzika (Izvanredni specijalistički informacijska sigurnost i digitalna forenzika) - Obavezni predmet				
Izvedba nastave	Predavanja + vježbe (auditorne+laboratorij+seminar+konstrukcijske) Samostalan rad			30+30 (0+0+30+0) 90	
Izvođači	Predavanja:1. mr.sc. Marinko Žagar viši predavač Seminarske vježbe:mr.sc. Marinko Žagar viši predavač				
Cilj predmeta	Osposobiti studente za izradu i provedbu kvalitetnog stručnog i istraživačkog rada				
Ishodi učenja:	1. formulirati / oblikovati istraživačke hipoteze okvire rješenja problema i predmeta istraživanja. Razina:6,7 2. generirati rješenje stručnog i znanstvenog problema putem istraživanja.. Razina:6,7 3. valorizirati pravila i postupke metodologije stručnog i istraživačkog rada.. Razina:7 4. izabrati opciju postupaka za transformaciju kvalitetne ideje u kvalitetan stručni rad.. Razina:7 5. odabrati metode pri izradi stručnog rada.. Razina:7 6. prezentirati rezultate rada ciljanoj publici.. Razina:6,7				
Način izvođenja predavanja	Frontalna, ex cathedra Analiza primjera, case studies Diskusija problema Pitanja - odgovori				
Način izvođenja seminarskih vježbi	Analiza literature na webu, knowledge mining Pisanje eseja Radionica				
Sadržaj predavanja	1.Uvod u stručni i istraživački rad. Stručna, istraživačka i znanstvena djelatnost. Pojam i vrste znanstvenog djela. Pojam i vrste stručnog djela., 4h, Ishodi:1,2 2.Metodologija stručnog istraživačkog rada. Pojam i klasifikacija stručnih i znanstvenih metoda., 4h, Ishodi:5,6 3.Tehnologija stručnog i znanstvenog istraživanja. Odabir teme istraživanja. Planiranje i organizacija istraživačkog rada., 4h, Ishodi:3 4.Istraživanje i razvoj. Pisanje i tehnička obrada stručnog rada. Korištenje literature i citiranje; dijelovi rada i istraživačka dokumentacija., 4h, Ishodi:3 5.Plagijat. Stručni i znanstveni časopisi i publikacije. Pretraživanje baza podataka. Radovi za stjecanje stručnih i znanstvenih zvanja., 6h, Ishodi:1 6.Postupak kontrole izvornosti završnih i diplomskih radova odabranim računalnim programom., 8h, Ishodi:4 7.Nema nastave, 2h 8.Nema nastave, 2h 9.Nema nastave, 2h 10.Nema nastave, 2h 11.Nema nastave, 2h 12.Nema nastave, 2h 13.Nema nastave, 2h 14.Nema nastave, 2h 15.Nema nastave, 2h				
Sadržaj seminarskih vježbi	1.u dogovoru s mentorom, 2h, Ishodi:2 2.u dogovoru s mentorom, 2h, Ishodi:2 3.u dogovoru s mentorom, 2h, Ishodi:2 4.u dogovoru s mentorom, 2h, Ishodi:2 5.u dogovoru s mentorom, 2h, Ishodi:2 6.u dogovoru s mentorom, 2h, Ishodi:2 7.u dogovoru s mentorom, 2h, Ishodi:2 8.u dogovoru s mentorom, 2h, Ishodi:2 9.u dogovoru s mentorom, 2h, Ishodi:2 10.u dogovoru s mentorom, 2h, Ishodi:2 11.u dogovoru s mentorom, 2h, Ishodi:2 12.u dogovoru s mentorom, 2h, Ishodi:2 13.u dogovoru s mentorom, 2h, Ishodi:2 14.u dogovoru s mentorom, 2h, Ishodi:2 15.u dogovoru s mentorom, 2h, Ishodi:2				
Materijalni uvjeti za izvedbu predmeta	Elementarni: predavaona, ploča, kreda... Računalni laboratorij opće namjene Projektor				
Ishodi	6#7				
Literatura	1. M.Žugaj, K.Dumičić, V.Dušak: Temelji znanstvenoistraživačkog rada- Metodologija i metodika, FOI, Varaždin, 2006.g. 2. R. Zelenika: Metodologija i tehnologija izrade znanstvenog i stručnog djela. Ekonomski fakultet, Rijeka, 2000.g. 3. Lj. Baban, K. Ivić, S. Jelinić, M. Lamza-Maronić, A. Šundalić: Primjena metodologije stručnog i znanstvenog istraživanja.Ekonomski fakultet, Osijek, 2000. 4. R. Zelenika: Tehnologija znanstvenog i razvojnog istraživanja. IQ plus d.o.o.Rijeka 2016. ISBN: 978-953-95705-9-8				
Uvjeti za potpis (obaveze studenta)	Pohađanje nastave i aktivnost na predavanjima				
Provjera znanja u semestru	Usmeni ispit i seminarski rad				



Način polaganja ispita nakon semestra	Seminarski rad Bodovi 0-50 nedovoljno 51-63 dovoljno 64-77 dobro 78-90 vrlo dobro 91-100 izvrsno
Praćenje rada studenta:	Aktivnost ECTS Seminarski rad () 2 Pismeni ispit () 2 Pohađanje nastave () 1
Napomena	Iz ovog predmeta moguća je izrada završnog/diplomskog rada
Preduvjeti:	Nema preduvjeta
Izradio prijedlog	mr.sc. Marinko Žagar viši predavač, 18.7.2019



Šifra WEB/ISVU	25094/185566	ECTS	6.0	Akadska godina	2019/2020
Naziv	Organizacija i vođenje digitalno forenzičkih analiza				
Status	2. semestar - Politehnički specijalistički diplomski studij, Informacijska sigurnost i digitalna forenzika (Izvanredni specijalistički informacijska sigurnost i digitalna forenzika) - Obavezni predmet				
Izvedba nastave	Predavanja + vježbe (auditorne+laboratorij+seminar+konstrukcijske) Samostalan rad			30+30 (0+15+15+0) 120	
Izvođači	Predavanja:1. dr.sc. Damir Delija Laboratorijske vježbe: Savina Gruičić Laboratorijske vježbe: Davorka Topolčić Seminarske vježbe:dr.sc. Damir Delija				
Cilj predmeta	Upoznavanje studenata sa organizacijom digitalno forenzičkih timova, istražnih timova, organizacije laboratorija, alata za provođenje digitalno forenzičkih analiza kao i procesa analiza.				
Ishodi učenja:	<ol style="list-style-type: none"> 1. organizirati digitalno forenzički laboratorij. Razina:6,7 2. kritički prosuđivati procese prikupljanja, analize digitalnih dokaza. Razina:7 3.voditi digitalno forenzičke analize u skladu sa zakonskim smjernicama. Razina:6,7 4. kritički prosuđivati Razumjeti procese provođenja digitalnih analiza. Razina:7 5. kritički prosuđivati svrhe i ciljeve digitalno forenzičkog laborat. Razina:7 6. prosuditi alate i opremu za provođenje digitalno forenzičkih analiza. Razina:7 7. voditi procese prikupljanja i obrade dokaza u skladu sa zakonima i standardima. Razina:6,7 				
Način izvođenja predavanja	Frontalna, ex cathedra Gost, predavač Analiza primjera, case studies Demonstracije Simulacije Diskusija problema Pitanja - odgovori Seminar, izlaganje studenta s raspravom				
Način izvođenja laboratorijskih vježbi	Laboratorijske s laboratorijskom opremom Laboratorijske, simulacije na računalima Grupno rješavanje zadanih problema Analiza literature na webu, knowledge mining Računalne simulacije Radionica				
Način izvođenja seminarskih vježbi	Laboratorijske s laboratorijskom opremom Laboratorijske, simulacije na računalima Analiza literature na webu, knowledge mining Računalne simulacije Radionica				
Sadržaj predavanja	<ol style="list-style-type: none"> 1.Uloga računala u kriminalu, Ishodi, Vrste i tipovi uređaja i sustava koji zahtijevaju analizu, 2h, Ishodi:1,3,4,5,6,7 2.Računalo, mrežno računalo, ručni uređaj, Analiza na uređajima koji su uključeni,, 2h, Ishodi:2,7 3.Razlozi za pokretanje analize, Visoko-tehnološki kriminal,, 2h, Ishodi:2,4,6 4.Oprema digitalno forenzičkog laboratorija (HWSW), Oprema za pohranu digitalnih dokaza, 2h, Ishodi:1,2 5.Oprema za izlazak na teren, Procedure,, 2h, Ishodi:6 6.Definiranje opsega rada laboratorija, Izrada poslovnog plana, 2h, Ishodi:1,4 7.Definiranje opsega rada laboratorija, Izrada poslovnog plana, 2h, Ishodi:1,6 8.Lokacija laboratorija, Izbor i selekcija kadrova, 2h, Ishodi:1,6 9.Potrebne kvalifikacije i iskustva, Edukacija i specijalizacija,, 2h, Ishodi:1,4,5,7 10.Zakonske odredbe i praksa, IStandardi (ISO 17025) i najbolja praksa,, 2h, Ishodi:1,4,7 11.Procesi prikupljanja dokaza, Zbirka dokaza: , 2h, Ishodi:1,2,4,6 12.Procesi analize dokaza u laboratoriju, Upravljanje skladištem dokaza,, 2h, Ishodi:1,2,4,5 13.Upravljanje i održavanje arhivskih skladišta, Osiguranje kvalitete, , 2h, Ishodi:1 14.Izazovi upravljanja, Certifikati laboratorija i osoblja,, 2h, Ishodi:1,4,6 15.Organizacijski modeli DFL, Utjecaj promjena na proces analize, 2h, Ishodi:1,4,7 				
Sadržaj laboratorijskih vježbi	<ol style="list-style-type: none"> 1.Analiziranje i opisivanje procesa digitalno forenzičkih analiza, 2h, Ishodi:4,5 2.Analiziranje trendova kibernetičkog kriminala, 2h, Ishodi:1,5 3.Izrađivanje izvještaja o provedenim analizama, 2h, Ishodi:3,5 4.Korištenje alata i opreme za digitalno forenzičke analize, 2h, Ishodi:5,7 5.Upravljanje digitalno forenzičkim laboratorijem, 2h, Ishodi:6 6.Primjenjivati procese u provođenju digitalno forenzičkih analiza, 2h, Ishodi:2,4,5,7 7.Primjenjivanje zakonskih procedura u vođenju digitalno forenzičkih analiza, 2h, Ishodi:3,7 8.Izrada poslovnih i operativnih planova digitalno forenzičkog laboratorija, 1h, Ishodi:1 9.nema nastave 10.nema nastave 11.nema nastave 12.nema nastave 13.nema nastave 14.nema nastave 15.nema nastave 				
Sadržaj seminarskih vježbi	<ol style="list-style-type: none"> 1.Definiranje teme seminarskog rada, 1h, Ishodi:1,2,3,4,5,6,7 2.Pisanje seminarskog rada, 2h, Ishodi:1 3.Pisanje seminarskog rada, 2h, Ishodi:1 				



	4.Pisanje seminarskog rada, 2h, Ishodi:1 5.Pisanje seminarskog rada, 2h, Ishodi:1 6.Pisanje seminarskog rada, 2h, Ishodi:1 7.Pisanje seminarskog rada, 2h, Ishodi:1 8.nema nastave, 2h 9.nema nastave, 2h 10.nema nastave, 2h 11.nema nastave, 2h 12.nema nastave, 2h 13.nema nastave, 2h 14.nema nastave, 2h 15.nema nastave, 2h
Materijalni uvjeti za izvedbu predmeta	Elementarni: predavaona, ploča, kreda... Namjenski laboratorij Računalni laboratorij opće namjene Namjenski računalni laboratorij Bijela ploča sa flomasterima Projektor Potrošni materijal, navesti
Ishodi	6#7
Literatura	Andrew Jones, Craig Valli, Building a Digital Forensic Laboratory: Establishing and Managing a Successful Facility, Butterworth Heinemann and Syngress Publishing Inc., 978-1856175104, 2015 The European Union Agency for Network and Information Security (ENISA), Electronic evidence - a basic guide for First Responders, The European Union Agency for Network and Information Security (ENISA), 978-92-9204-111-3, 2014 Karen Kent, Suzanne Chevalier, Tim Grance, Hung Dang, Guide to Integrating Forensic Techniques into Incident Response, Computer Security Division, Information Technology Laboratory, National Institute of Standards and, 2006 David Lilburn Watson Andrew Jones : Digital Forensics Processing and Procedures, 1st Edition Meeting the Requirements of ISO 17020, ISO 17025, ISO 27001 and Best Practice Requirements, David Lilburn Watson Andrew Jones, 2013
Uvjeti za potpis (obaveze studenta)	Izrada seminara i vježbi je obvezna za sve studente
Provjera znanja u semestru	Dva kolokvija po 25 bodova (Svaki kolokvij ima popravak)
Način polaganja ispita nakon semestra	Ukoliko student ne položi kolokvije ima mogućnost izlaska na usmeni ispit. Ukupno maksimalno 100 bodova 0-49 - nedovoljan 50-61 - dovoljan 62-74 - dobar 75-86 - vrlo dobar 87-100 - izvrstan
Praćenje rada studenta:	Aktivnost ECTS Pohadanje nastave () 1 Pismeni ispit () 1 Usmeni ispit () 1 Seminarski rad () 1 Istraživanje () 1 Praktični rad () 1
Napomena	Iz ovog predmeta moguća je izrada završnog/diplomskog rada
Preduvjeti:	Nema preduvjeta
Izradio prijedlog	dr.sc. Damir Delija, 14.6.2018



Šifra WEB/ISVU	24968/173035	ECTS	6.0	Akadska godina	2019/2020
Naziv	Primijenjena kriptografija				
Status	2. semestar - Politehni?ki specijalisti?ki diplomski studij, Informacijska sigurnost i digitalna forenzika (Izvanredni specijalisti?ki informacijska sigurnost i digitalna forenzika) - Izborni predmet				
Izvedba nastave	Predavanja + vjezbe (auditorne+laboratorij+seminar+konstrukcijske) Samostalan rad			30+30 (0+15+15+0) 120	
Izvoa?i	Predavanja:1. dr. sc. Roman Domović , prof. Predavanja: Goran Sirovatka Laboratorijske vjezbe: Goran Sirovatka Seminarske vjezbe: Goran Sirovatka				
Cilj predmeta	Primijenjena kriptografija				
Ishodi u?enja:	1.razlikovati kriptografske algoritme i sustave. Razina:6 2.identificirati prijetnje po sigurnost povjerljivih podataka i posljedice koje mogu nastati realizacijom tih prijetnji. Razina:6 3.predvidjeti poteško?e koje mogu nastati pri rukovanju povjerljivim podacima. Razina:6,7 4.upravljati alatima i opremom za stvaranje okruženja za sigurno rukovanje povjerljivim podacima. Razina:6,7 5.kombinirati kriptografska rješenja u prakti?nim sustavima. Razina:6,7 6. prosuditi koje je rješenje najbolje za sigurnost povjerljivih podataka pri odre?enoj svrsi u odre?enom okruženju. Razina:7				
Na?in izvo?enja predavanja	Frontalna, ex cathedra Gost, predava? Analiza primjera, case studies Demonstracije Simulacije Pitanja - odgovori				
Na?in izvo?enja laboratorijskih vjezbi	Laboratorijske s laboratorijskom opremom Laboratorijske, simulacije na ra?unalima Rasprave, brainstorming Radionica				
Na?in izvo?enja seminarskih vjezbi	Analiza klasi?ne literature Analiza literature na webu, knowledge mining Pisanje eseja Rasprave, brainstorming				
Sadržaj predavanja	1.Uvod u kriptografiju, 2h, Ishodi:1 2.Simetri?na kriptografija, 2h, Ishodi:1,2 3.Asimetri?na kriptografija, 2h, Ishodi:1,2 4.Jednosmjerne funkcije sažimanja, 2h, Ishodi:1,2,3 5.Digitalni potpis, 2h, Ishodi:2,3,4 6.Sigurnost lozinki, 2h, Ishodi:2,3,4 7.Prvi kolokvij, 2h, Ishodi:1,2,3,4 8.Dužina klju?a, 2h, Ishodi:2,3,4,5 9.Upravljanje klju?evima, 2h, Ishodi:2,3,4,5 10.Matemati?ka podloga kriptografskih algoritama, 2h, Ishodi:1,2,3,4 11.Napredne blokne šifre i njihovo kombiniranje, 2h, Ishodi:3,4,5,6 12.Napredni algoritmi javnoga klju?a, 2h, Ishodi:3,4,5,6 13.Specijalni algoritmi za protokole, 2h, Ishodi:5,6 14.Standardi i regulativa, 2h, Ishodi:5,6 15.Drugi kolokvij, 2h, Ishodi:1,2,3,4,5,6				
Sadržaj laboratorijskih vjezbi	1.Stagenografija, 1h, Ishodi:1,2 2.AES i IDEA algoritmi, 1h, Ishodi:1,2 3.RSA algoritam, 1h, Ishodi:1,2 4.Jednosmjerne funkcije sažimanja i njihova primjena, 1h, Ishodi:1,2,3 5.Digitalni potpis, 1h, Ishodi:2,3,4 6.Probijanje lozinki, 1h, Ishodi:2,3,4 7.Prvi kolokvij, 1h, Ishodi:1,2,3,4 8.Upravljanje klju?evima, 1h, Ishodi:2,3,4,5 9.PGP, 1h, Ishodi:2,3,4,5 10.Faktorizacija i prosti brojevi, 1h, Ishodi:2,3 11.Korištenje kriptografskih algoritama, 1h, Ishodi:4,5 12.Višestruka enkripcija, 1h, Ishodi:4,5 13.Kriptosustavi na temelju elipti?nih krivulja, 1h, Ishodi:3,4,5 14.Ostali algoritmi s javnim klju?em, 1h, Ishodi:3,4,5,6 15.Drugi kolokvij, 1h, Ishodi:1,2,3,4,5,6				
Sadržaj seminarskih vjezbi	1.Steganografija, 1h, Ishodi:1,2 2.Crypt soft, 1h, Ishodi:3,4,5 3.Bitlocker, True Crypt, 1h, Ishodi:3,4,5 4.Kali Linux dekripcija, 1h, Ishodi:3,4,5 5.Kali Linux probijanje WiFi lozinki, 1h, Ishodi:3,4,5 6.Wireshark, 1h, Ishodi:3,4,5 7.Pronalaženje i korištenje razli?itih kriptografskih alata, 1h, Ishodi:3,4,5 8.Sigurnost klijenata za e-poštu, 1h, Ishodi:3,4,5				



	9.Mreža TOR, 1h, Ishodi:4,5 10.Odabir seminara, 1h, Ishodi:4,5,6 11.Predaja seminara i diskusija, 1h, Ishodi:4,5,6 12.Prezentacija seminara, 1h, Ishodi:5 13.Prezentacija seminara, 1h, Ishodi:5 14.Prezentacija seminara, 1h, Ishodi:5 15.Prezentacija seminara, 1h, Ishodi:5
Materijalni uvjeti za izvedbu predmeta	Elementarni: predavaona, ploča, kreda... Računalni laboratorij opće namjene Namjenski računalni laboratorij Bijela ploča sa flomasterima Projektor
Ishodi	6#7
Literatura	1. Domović, Roman.; Sirovatka, Goran. Nastavne skripte. 2. Paar, Christopher; Pelzl, Jan. Understanding Cryptography: A Textbook for Students and Practitioners. Springer Berlin Heidelberg, 2011. 3. Menezes J. Alfred; Katz, Jonathan; van Oorschot C. Paul; Vanstone A. Scott. Handbook of Applied Cryptography, CRC Press, 1996. 4. Schneier, Bruce. Applied Cryptography: Protocols, Algorithms and Source Code in C. Wiley, 2017. 5. Katz, Jonathan; Lindell, Yehuda. Introduction to Modern Cryptography, Second Edition, CRC Press, 2014. 6. O'Connor, T.J. Violent Python: A Cookbook for Hackers, Forensic Analysts, Penetration Testers and Security Engineers, Elsevier Science, 2012. 7. Sweigart, Al. Cracking Codes with Python: An Introduction to Building and Breaking Ciphers, No Starch Press, 2018. 8. Douglas R. Stinson, Maura B. Paterson - Cryptography. Theory and Practice-CRC Press (2019).
Uvjeti za potpis (obaveze studenta)	Predan i pozitivno ocijenjen seminar.
Provjera znanja u semestru	Dvije provjere znanja i vještina
Način polaganja ispita nakon semestra	Ako student ima manje od 50% ukupno sakupljenih bodova ili manje od 50% bodova iz pojedinoga kolokvija, predmet može položiti pismenim i usmenim putem na nekom od redovnih ispitnih rokova. 0-49 bodova ocjena nedovoljan (1) 50-59 bodova ocjena dovoljan (2) 60-75 bodova ocjena dobar (3) 76-89 bodova ocjena vrlo dobar (4) 90-100 bodova ocjena izvrstan (5)
Praćenje rada studenta:	Aktivnost ECTS Seminarski rad () 2 Pismeni ispit () 2 Praktični rad () 2
Napomena	Iz ovog predmeta moguća je izrada završnog/diplomskog rada
Preduvjeti:	Nema preduvjeta
Izradio prijedlog	dr. sc. Roman Domović, viši predavač



Šifra WEB/ISVU	25247/202958	ECTS	5.0	Akadska godina	2019/2020
Naziv	Programiranje za forenziku				
Status	1. semestar - Politehni?ki specijalisti?ki diplomski studij, Informacijska sigurnost i digitalna forenzika (Izvanredni specijalisti?ki informacijska sigurnost i digitalna forenzika) - Izborni predmet				
Izvedba nastave	Predavanja + vjezbe (auditorne+laboratorij+seminar+konstrukcijske) Samostalan rad			30+30 (0+30+0+0) 90	
Izvođači	Predavanja:1. Dr. sc. Aleksandar Stojanović				
Cilj predmeta	Savladati napredne tehnike programiranja u programskom jeziku Java				
Ishodi učenja:	1.napisati osnovni program. Razina:6,7 2.raščlaniti program na više modula. Razina:6 3.napisati složeniji program za rad s datotekama. Razina:6,7 4.napisati složeniji program upotrebom mrežnih modula. Razina:6,7 5.napisati program upotrebom naprednih mogućnosti Pythona. Razina:6,7				
Način izvođenja predavanja	Frontalna, ex cathedra Analiza primjera, case studies Demonstracije Simulacije Modeliranje Diskusija problema Pitanja - odgovori Seminar, izlaganje studenta s raspravom Izlaganje domaćih zadaća				
Način izvođenja laboratorijskih vježbi	Grupno rješavanje zadanih problema				
Sadržaj predavanja	1.Uvod u Python, 2h, Ishodi:1 2.Ugrađene strukture podataka: Liste, ntorke, mape i skupovi, 2h, Ishodi:1 3.Rad s datotekama, 2h, Ishodi:3 4.Iznimke, moduli i paketi, 2h, Ishodi:5 5.Klase, 2h, Ishodi:2,5 6.Obrada teksta i regularni izrazi, 2h, Ishodi:1,2,3,4,5 7.Standardni mrežni i internetski moduli, 2h, Ishodi:4 8.Izrada sučelja modulom tkinter, 2h, Ishodi:5 9.Funkcije višeg reda, iteratori i generatori, 2h, Ishodi:5 10.Konkurentno izvršavanje programa, 2h, Ishodi:5 11.Nema nastave, 2h 12.Nema nastave, 2h 13.Nema nastave, 2h 14.Nema nastave, 2h 15.Nema nastave, 2h				
Sadržaj laboratorijskih vježbi	1.Uvod u Python: Riješavanje problema, 2h, Ishodi:1 2.Ugrađene strukture podataka: Liste, ntorke, mape i skupovi: Riješavanje problema, 2h, Ishodi:1 3.Rad s datotekama: Riješavanje problema, 2h, Ishodi:2 4.Iznimke, moduli i paketi: Riješavanje problema, 2h, Ishodi:5 5.Klase: Riješavanje problema, 2h, Ishodi:2,5 6.Obrada teksta i regularni izrazi: Riješavanje problema, 2h, Ishodi:1,2,3,4,5 7.Standardni mrežni i internetski moduli: Riješavanje problema, 2h, Ishodi:4 8.Izrada sučelja modulom tkinter: Riješavanje problema, 2h, Ishodi:5 9.Funkcije višeg reda, iteratori i generatori: Riješavanje problema, 2h, Ishodi:5 10.Konkurentno izvršavanje programa: Riješavanje problema, 2h, Ishodi:5 11.Nema nastave, 2h 12.Nema nastave, 2h 13.Nema nastave, 2h 14.Nema nastave, 2h 15.Nema nastave, 2h				
Materijalni uvjeti za izvedbu predmeta	Elementarni: predavaona, ploča, kreda... Računalni laboratorij opće namjene Bijela ploča sa flomasterima Projektor				
Ishodi	6#7				
Literatura	1. A. Stojanović: Elementi računalnih programa s primjerima u Pythonu i Scali, Element, 2012. 2. M. Lutz: Learning Python, O'Reilly, 2013.				
Uvjeti za potpis (obaveze studenta)	Odslušana predavanja				
Provjera znanja u semestru	Dva kolokvija				
Način polaganja ispita nakon semestra	Ispit				
Praćenje rada studenta:	Aktivnost Pohađanje nastave ()		ECTS 1		



	Pismeni ispit ()	4
Napomena	Iz ovog predmeta moguća je izrada završnog/diplomskog rada	
Preduvjeti:	Nema preduvjeta	
Izradio prijedlog	mr.sc. Aleksandar Stojanović , 18.7.2019	



Šifra WEB/ISVU	24967/173034	ECTS	5.0	Akadska godina	2019/2020
Naziv	Računalna forenzika				
Status	2. semestar - Politehnički specijalistički diplomski studij, Informacijska sigurnost i digitalna forenzika (Izvanredni specijalistički informacijska sigurnost i digitalna forenzika) - Izborni predmet				
Izvedba nastave	Predavanja + vježbe (auditorne+laboratorij+seminar+konstrukcijske) Samostalan rad			30+20 (0+10+10+0) 100	
Izvođači	Predavanja:1. dr.sc. Damir Delija Laboratorijske vježbe:dr.sc. Damir Delija Laboratorijske vježbe: Savina Gruić Laboratorijske vježbe: Krešimir Hausknecht Laboratorijske vježbe: Davorka Topolčić Seminarske vježbe:dr.sc. Damir Delija				
Cilj predmeta	Naučiti osnove računalne forenzike, postupke rada sa digitalnim dokazima, pronalaženje i interpretiranje i prezentiranje digitalnih dokaza računalne forenzike.				
Ishodi učenja:	1.izdvojiti dokaze sa mjesta zlocina. Razina:6 2.voditi analizu racunala. Razina:6,7 3.identificirati i analizirati kriptirane podatke. Razina:6 4. složiti izvjestaje o provedenoj digitalno forenzickoj istrazi racunala. Razina:6,7 5. generirati forenzicku kopiju racunala. Razina:6,7 6. valorizirati alate za spremanje i analizu digitalnih dokaza. Razina:7 7. prosuditi procedure za spremanje podataka iz racunala. Razina:7				
Način izvođenja predavanja	Frontalna, ex cathedra Gost, predavač Analiza primjera, case studies Demonstracije Simulacije Diskusija problema Pitanja - odgovori Seminar, izlaganje studenta s raspravom				
Način izvođenja laboratorijskih vježbi	Laboratorijske s laboratorijskom opremom Grupno rješavanje zadanih problema Analiza literature na webu, knowledge mining Rasprave, brainstorming Računalne simulacije Radionica				
Način izvođenja seminarskih vježbi	Laboratorijske s laboratorijskom opremom Laboratorijske, simulacije na računalima Grupno rješavanje zadanih problema Analiza literature na webu, knowledge mining Rasprave, brainstorming Računalne simulacije Radionica				
Sadržaj predavanja	1.Uvod u digitalnu forenziku (ključne komponente, principi, podjela digitalne forenzike) ,Dijelovi računala (komponente i arhitektura), 2h, Ishodi:1,2,3,4 2.Digitalni dokazi (izvori i vrste),Mjesto istrage , 2h, Ishodi:2,3,5,6 3.Postupci sa ugašenim ili upaljenim računalom,Dokumentiranje svih uređaja, 2h, Ishodi:1,2,3,5 4.Postupci izrade kopija svih nositelja zapisa ,Pakiranje i spremanje svih komponenti , 2h, Ishodi:1,2,3,4,7 5.Dokumentiranje svih koraka ,Brojevni sustav i računala., 2h, Ishodi:2,4 6.Radna memorija, Boot procesi računala, 2h, Ishodi:1,2,6,7 7.Osnove datotečnih sustava FAT datotečni sustav, 2h, Ishodi:1,2,3,4,6 8.NTFS datotečni sustav Ostali datotečni sustavi, 2h, Ishodi:1,3,5 9.Datoteke i njihove forenzičke karakteristike , 2h, Ishodi:1,2,3,5 10.Povrat obrisanih datoteka i data carving, Složene datoteke, 2h, Ishodi:2,4,5 11.Hash funkcije , Akvizicija i verifikacija dokaza , 2h, Ishodi:1,2,3 12.Artefakti u Windows operativnom sustavu Internet artefakti , 2h, Ishodi:1,2,3,4 13.Enkripcija , 2h, Ishodi:1,2,5,7 14.Artefakti elektroničke pošte i el. komunikacije, 2h, Ishodi:1,2,4,5,7 15.Digitalna forenzika i nadolazeće tehnologije, Izrada izvještaja, 2h, Ishodi:1,2,3,4,5,6,7				
Sadržaj laboratorijskih vježbi	1.Vježbe prikupljanja digitalnih dokaza sa mjesta zločina, 2h, Ishodi:1,2,3,4 2.Primjena raznih alata za računalnu forenziku , 2h, Ishodi:1,2,5 3.Primjena alata za analizu radne memorije, 2h, Ishodi:1,2,5,6 4.Korištenje alata za rad sa kriptiranim uređajima, 2h, Ishodi:2,3,4,7 5.Korištenje uređaja za izradu kopija podataka, 2h, Ishodi:2,3,6 6.Vježba korištenja procedura u akviziciji podataka, 2h, Ishodi:3,4,5 7.Izrada izvještaja o provedenoj digitalno forenzičkoj analizi , 2h, Ishodi:1,2,3,4,5,6,7 8.nema nastave, 2h 9.nema nastave, 2h 10.nema nastave, 2h 11.nema nastave, 2h 12.nema nastave, 2h 13.nema nastave, 2h 14.nema nastave, 2h				



	15.nema nastave, 2h												
Sadržaj seminarских vježbi	1.Priprema izrade seminarског rada, 1h, Ishodi:1,2,3,4,5,6,7 2.Izrada seminarског rada, 2h 3.Izrada seminarског rada, 2h 4.Izrada seminarског rada, 2h 5.Izrada seminarског rada, 2h 6.Izrada seminarског rada, 2h 7.Izrada seminarског rada, 2h 8.nema nastave 9.nema nastave 10.nema nastave 11.nema nastave 12.nema nastave 13.nema nastave 14.nema nastave 15.nema nastave												
Materijalni uvjeti za izvedbu predmeta	Elementarni: predavaona, ploča, kreda... Namjenski laboratorij Računalni laboratorij opće namjene Namjenski računalni laboratorij Bijela ploča sa flomasterima Projektor Video oprema Potrošni materijal, navesti												
Ishodi	6#7												
Literatura	John Sammons, The Basics of Digital Forensics, 2nd Edition, 2014 Nelson B., Philips A., Steuart C., Guide to computer forensics and investigation, 5th Edition, Cengage Learning 2016. Philipp A., Cowen D., Davis C., Hacking exposed computer Forensics, 2nd Edition, Mc Graw Hill 2010 Brian Carrier: File System Forensic Analysis, 2005												
Uvjeti za potpis (obaveze studenta)	Pohađanje nastave, izrada seminara i vježbi je obvezna za sve studente i uvjet za potpis.												
Provjera znanja u semestru	Dva kolokvija po 25 bodova												
Način polaganja ispita nakon semestra	Ukoliko student ne položi kolokvije ima mogućnost izlaska na usmeni ispit. Ukupno maksimalno 100 bodova 0-49 - nedovoljan 50-61 - dovoljan 62-74 - dobar 75-86 - vrlo dobar 87-100 - izvrstan												
Praćenje rada studenta:	<table><thead><tr><th>Aktivnost</th><th>ECTS</th></tr></thead><tbody><tr><td>Pohađanje nastave ()</td><td>1</td></tr><tr><td>Pismeni ispit ()</td><td>1</td></tr><tr><td>Usmeni ispit ()</td><td>1</td></tr><tr><td>Praktični rad ()</td><td>1</td></tr><tr><td>Seminarski rad ()</td><td>1</td></tr></tbody></table>	Aktivnost	ECTS	Pohađanje nastave ()	1	Pismeni ispit ()	1	Usmeni ispit ()	1	Praktični rad ()	1	Seminarski rad ()	1
Aktivnost	ECTS												
Pohađanje nastave ()	1												
Pismeni ispit ()	1												
Usmeni ispit ()	1												
Praktični rad ()	1												
Seminarski rad ()	1												
Napomena	Iz ovog predmeta moguća je izrada završnog/diplomskog rada												
Preduvjeti:	Nema preduvjeta												
Izradio prijedlog	dr.sc. Damir Delija , 14.6.2018												



Šifra WEB/ISVU	24970/173037	ECTS	6.0	Akadska godina	2019/2020
Naziv	Sigurnost računalnih mreža				
Status	2. semestar - Politehnički specijalistički diplomski studij, Informacijska sigurnost i digitalna forenzika (Izvanredni specijalistički informacijska sigurnost i digitalna forenzika) - Obavezni predmet				
Izvedba nastave	Predavanja + vježbe (auditorne+laboratorij+seminar+konstrukcijske) Samostalan rad			30+30 (0+15+15+0) 120	
Izvođači	Predavanja:1. dr.sc. Damir Delija Laboratorijske vježbe: Vedran Turkalj Seminarske vježbe: Vedran Turkalj				
Cilj predmeta	Stjecanje temeljnih znanja o sigurnosti računalnih mreža.				
Ishodi učenja:	1. formulirati / oblikovati sigurnosnu politiku sigurnosnim tehnologijama, proizvodima i rješenjima. Razina:6,7 2.izgraditi sigurnu računalno-komunikacijsku infrastrukturu. Razina:6,7 3. opravdati stav o važnosti uspostave odgovarajućeg sigurnosnog sustava prema upravi. Razina:7 4.kreirati napredne konfiguracije i sigurnosne postavke mrežnih uređaja. Razina:6,7 5.razviti detaljno razumijevanje principa mrežne sigurnosti. Razina:6,7 6.klasificirati vrste prijetnji na Internetu. Razina:6,7				
Način izvođenja predavanja	Frontalna, ex cathedra Gost, predavač Analiza primjera, case studies Demonstracije Pitanja - odgovori Seminar, izlaganje studenta s raspravom				
Način izvođenja laboratorijskih vježbi	Laboratorijske s laboratorijskom opremom Laboratorijske, simulacije na računalima Rasprave, brainstorming Međusobno zadavanje i rješavanje problema Radionica				
Način izvođenja seminarskih vježbi	Analiza klasične literature Analiza literature na webu, knowledge mining Pisanje eseja				
Sadržaj predavanja	1.Definiranje i provođenje sigurnosne politike, 4h, Ishodi:1 2.Projektiranje, instalacija, konfiguracija i održavanje mrežnog vatrozida (firewall), 4h, Ishodi:2,6 3.Primjena sustava za provjeru identiteta i prava korisnika (AAA) na preklopnima, bežičnim mrežama i udaljenom pristupu (NAC Network Admission Control, 4h, Ishodi:5 4.Dizajn i implementacija VPN (Virtual Private Networks) povezivanja , 3h, Ishodi:2 5.Prikupljane i obrada log zapisa (SIEM), 3h, Ishodi:3 6.Sigurnost bežičnih mreža , 3h, Ishodi:6 7.Sigurnost IoT (Internet of Things), 3h, Ishodi:4 8.Sigurnost uz pomoć strojnog učenja (machine learning), 4h, Ishodi:2 9.Nema nastave 10.Nema nastave 11.Nema nastave 12.Nema nastave 13.Nema nastave 14.Nema nastave 15.Nema nastave				
Sadržaj laboratorijskih vježbi	1.Uvod u laboratorijske vježbe kolegija Sigurnost računalnih mreža, 1h, Ishodi:2 2.Konfiguracija mrežnog vatrozida, 2h, Ishodi:4 3.Konfiguracija Cisco ISE AAA poslužitelja, 2h, Ishodi:4 4.Povezivanje dvaju usmjerivača IPSec tunelom (policy based VPN), 1h, Ishodi:4 5.Povezivanje dvaju usmjerivača IPSec tunelom (tunnel based VPN), 2h, Ishodi:4 6.Implementacija udaljenog pristupa pomoću Cisco AnyConnect tehnologije, 2h, Ishodi:1 7.Implementacija sigurnosti na bežičnim mrežama, 2h, Ishodi:2 8.Implementacija (Network Admission Control) za pristup mreži preko preklopnika, 1h, Ishodi:5 9.Implementacija (Network Admission Control) za pristup mreži preko bežične mreže, 1h, Ishodi:5 10.Implementacija (Network Admission Control) za pristup mreži preko udaljenog pristupa, 1h, Ishodi:5 11.Nema nastave 12.Nema nastave 13.Nema nastave 14.Nema nastave 15.Nema nastave				
Sadržaj seminarskih vježbi	1.Definiranje teme seminarskog rada, 3h, Ishodi:1 2.Izrada seminarskog rada, 2h, Ishodi:2 3.Izrada seminarskog rada, 2h, Ishodi:3 4.Izrada seminarskog rada, 2h, Ishodi:4 5.Izrada seminarskog rada, 2h, Ishodi:5 6.Izrada seminarskog rada, 2h, Ishodi:6 7.Izrada seminarskog rada, 2h, Ishodi:1 8.Nema nastave 9.Nema nastave 10.Nema nastave				



	11.Nema nastave 12.Nema nastave 13.Nema nastave 14.Nema nastave 15.Nema nastave												
Materijalni uvjeti za izvedbu predmeta	Elementarni: predavaona, ploča, kreda... Namjenski laboratorij Namjenski računalni laboratorij Projektor												
Ishodi	6#7												
Literatura	1.Patrick Engebretson,The Basics of Hacking and Penetration Testing,Syngress, 9780124116443, 2013 2.Cisco,CBT Nuggets Video Cisco CCNA Security 210-260 IINS,Cisco, 2015 3.Adam Gordon,Official (ISC)2 Guide to the CISSP CBK,Auerbach Publications, 9781482262759, 2015												
Uvjeti za potpis (obaveze studenta)	Laboratorijske vježbe ili seminar do 50 bodova.												
Provjera znanja u semestru	Dva kolokvija po 25 bodova (Svaki kolokvij ima popravak) Opcionalni bodovi za zalaganje Praktični dio ispita sadrži jedan problem iz prakse na temelju savladanog gradiva. Ukoliko student ne položi kolokvije ima mogućnost izlaska na usmeni ispit. Ukupno maksimalno 100 bodova 0-49 - nedovoljan 50-61 - dovoljan 62-74 - dobar 75-86 - vrlo dobar 87-100 - izvrstan												
Način polaganja ispita nakon semestra	Pismeni ispit usmeni ispit.												
Praćenje rada studenta:	<table><thead><tr><th>Aktivnost</th><th>ECTS</th></tr></thead><tbody><tr><td>Pohađanje nastave ()</td><td>1</td></tr><tr><td>Pismeni ispit ()</td><td>1</td></tr><tr><td>Usmeni ispit ()</td><td>1</td></tr><tr><td>Seminarski rad ()</td><td>2</td></tr><tr><td>Praktični rad ()</td><td>1</td></tr></tbody></table>	Aktivnost	ECTS	Pohađanje nastave ()	1	Pismeni ispit ()	1	Usmeni ispit ()	1	Seminarski rad ()	2	Praktični rad ()	1
Aktivnost	ECTS												
Pohađanje nastave ()	1												
Pismeni ispit ()	1												
Usmeni ispit ()	1												
Seminarski rad ()	2												
Praktični rad ()	1												
Napomena	Iz ovog predmeta moguća je izrada završnog/diplomskog rada												
Preduvjeti:	Nema preduvjeta												
Izradio prijedlog	mr.sc. Marinko Žagar viši predavač, 14.6.2018												



Šifra WEB/ISVU	24965/173031	ECTS	6.0	Akademski godina	2019/2020
Naziv	Sigurnost web aplikacija				
Status	1. semestar - Politehnički specijalistički diplomski studij, Informacijska sigurnost i digitalna forenzika (Izvanredni specijalistički informacijska sigurnost i digitalna forenzika) - Obavezni predmet				
Izvedba nastave	Predavanja + vježbe (auditorne+laboratorij+seminar+konstrukcijske) Samostalan rad			30+30 (0+15+15+0) 120	
Izvođači	Predavanja:1. Sanja Kraljević , dipl.ing., v. pred. Laboratorijske vježbe: Sanja Kraljević , dipl.ing., v. pred. Seminarske vježbe: Sanja Kraljević , dipl.ing., v. pred.				
Cilj predmeta	Osposobljavanje studenata za projektiranje i izgradnju sigurnih aplikacija te prepoznavanje ranjivosti i prijetnja postojećim aplikacijama. Vrednovanje i ugradnja sustava za upravljanje bazama podataka s aspekta informacijske sigurnosti.				
Ishodi učenja:	1. vrjednovati sigurnost web aplikacija. Razina:7 2. kritički prosuđivati implementirane standarde sigurnosti. Razina:7 3.klasificirati napade na web aplikacije. Razina:6,7 4. razviti sigurni softver u skladu s prijetnjama u obliku napada na softver. Razina:6,7 5. prosuditi kvalitetu implementacije rješenja za sigurnost informacijskih sustava. Razina:7 6.predložiti rješenje za sustav upravljanja bazama podataka te njihovu sigurnu ugradnju. Razina:6,7 7.upravljati alatima za detektiranje razine ranjivosti aplikacija. Razina:6,7				
Način izvođenja predavanja	Frontalna, ex cathedra Analiza primjera, case studies Simulacije Diskusija problema Seminar, izlaganje studenta s raspravom				
Način izvođenja laboratorijskih vježbi	Laboratorijske, simulacije na računalima Rasprave, brainstorming Računalne simulacije				
Način izvođenja seminarskih vježbi	Analiza klasične literature Analiza literature na webu, knowledge mining Pisanje eseja Radionica				
Sadržaj predavanja	1.Arhitektura aplikacije na webu i sigurnosni protokoli, 2h, Ishodi:1 2.Sigurno kodiranje, 2h, Ishodi:2,4,5 3.Napadi vezani za autentikaciju i autorizaciju, 2h, Ishodi:3,4 4.Napadi vezani uz izvršavanje naredbi, 2h, Ishodi:3,4 5.Otkrivanje povjerljivih informacija i logički napadi, 2h, Ishodi:4 6.Sigurnost baza podataka ovlasti nad podatcima i integritet podataka, 2h, Ishodi:6 7.Sigurnost baza podataka kontrola pristupa podatcima, 2h, Ishodi:6 8.Prvi kolokvij, 2h, Ishodi:6 9.Sigurnosne prijetnje, SQL injekcija, problem zaključivanja, 2h, Ishodi:5 10.Maskiranje i šifriranje podataka, 2h, Ishodi:6 11.Pohrana šifriranih podataka, 2h, Ishodi:5,7 12.Testiranje ranjivosti, 2h, Ishodi:7 13.Alati za aplikacijsku sigurnost, 2h 14.Alati za aplikacijsku sigurnost, 2h 15.Drugi kolokvij, 2h				
Sadržaj laboratorijskih vježbi	1.Arhitektura aplikacije na webu i sigurnosni protokoli, 2h, Ishodi:2 2.Sigurno kodiranje, 2h, Ishodi:4 3.Napadi vezani za autentikaciju i autorizaciju, 2h, Ishodi:3 4.Napadi vezani uz izvršavanje naredbi, otkrivanje povjerljivih informacija i logički napadi, 2h, Ishodi:1,3 5.Sigurnost baza podataka ovlasti nad podatcima i integritet podataka, kontrola pristupa podatcima, 2h, Ishodi:6 6.Sigurnosne prijetnje, SQL injekcija, problem zaključivanja, maskiranje i šifriranje podataka, 2h, Ishodi:2,4,6 7.Testiranje ranjivosti, alati za aplikacijsku sigurnost, 2h, Ishodi:7 8.Nema nastave (seminar) 9.Nema nastave (seminar) 10.Nema nastave (seminar) 11.Nema nastave (seminar) 12.Nema nastave (seminar) 13.Nema nastave (seminar) 14.Nema nastave (seminar) 15.Nema nastave (seminar)				
Sadržaj seminarskih vježbi	1.Nema nastave (lab. vježbe) 2.Nema nastave (lab. vježbe) 3.Nema nastave (lab. vježbe) 4.Nema nastave (lab. vježbe) 5.Nema nastave (lab. vježbe) 6.Nema nastave (lab. vježbe) 7.Nema nastave (lab. vježbe) 8.Arhitektura aplikacije na webu i sigurnosni protokoli, 2h, Ishodi:2 9.Sigurno kodiranje, 2h, Ishodi:4 10.Napadi vezani za autentikaciju i autorizaciju, 2h, Ishodi:3				



	11.Napadi vezani uz izvršavanje naredbi, otkrivanje povjerljivih informacija i logički napadi, 2h, Ishodi:1,3 12.Sigurnost baza podataka ovlasti nad podacima i integritet podataka, kontrola pristupa podacima, 2h, Ishodi:6 13.Sigurnosne prijetnje, SQL injekcija, problem zaključivanja, maskiranje i šifriranje podataka, 2h, Ishodi:2,4,6 14.Testiranje ranjivosti, alati za aplikacijsku sigurnost, 2h, Ishodi:7 15.Prezentacije radova, 2h, Ishodi:1,2,3,4,5,6,7
Materijalni uvjeti za izvedbu predmeta	Elementarni: predavaona, ploča, kreda... Računalni laboratorij opće namjene Namjenski računalni laboratorij Bijela ploča sa flomasterima Projektor
Ishodi	6#7
Literatura	Kraljević, S., Skripte s predavanja - Sigurnost web aplikacija
Uvjeti za potpis (obaveze studenta)	Odrađene laboratorijske vježbe ili seminar (projekt)
Provjera znanja u semestru	- 50% - laboratorijske vježbe ili seminar (projekt) - 25% - prvi kolokvij - 25% - drugi kolokvij
Način polaganja ispita nakon semestra	- 50% - laboratory exercises or seminar paper (project) - 50% - ispit
Praćenje rada studenta:	Aktivnost ECTS Pismeni ispit () 2 Projekt () 2 Kontinuirana provjera znanja () 2
Napomena	Iz ovog predmeta moguća je izrada završnog/diplomskog rada
Preduvjeti:	Nema preduvjeta
Izradio prijedlog	Sanja Kraljević, dipl.ing., 12.6.2018.



Šifra WEB/ISVU	25225/173044	ECTS	6.0	Akadska godina	2019/2020
Naziv	Skriptni i objektni jezici za forenziku				
Status	3. semestar - Politehnički specijalistički diplomski studij, Informacijska sigurnost i digitalna forenzika (Izvanredni specijalistički informacijska sigurnost i digitalna forenzika) - Izborni predmet				
Izvedba nastave	Predavanja + vježbe (auditorne+laboratorij+seminar+konstrukcijske) Samostalan rad			30+30 (0+30+0+0) 120	
Izvođači	Predavanja:1. Goran Sirovatka Laboratorijske vježbe: Domagoj Tuličić				
Cilj predmeta	Osposobiti polaznika za korištenje skriptnog jezika za automatizaciju poslova, i proširenje mogućnosti alata za digitalnu forenziku				
Ishodi učenja:	1.pripremiti Primijeniti gotove skripte u forenzici. Razina:6,7 2. kreirati Izraditi skriptu koristeći regularne izraze. Razina:6,7 3. klasificirati Poznavati osnovnu sintaksu i elemente skriptnog jezika. Razina:6,7 4. kreirati Napisati kod u skriptnom jeziku za automatizaciju čestih poslova. Razina:6,7 5. izabrati opciju Pronaći i modificirati forenzičke skripte. Razina:7 6. sastaviti (prijedlog / rješenje) Modificirati skripte za različite forenzičke alate 1.4. Sadržaj. Razina:6,7				
Način izvođenja predavanja	Frontalna, ex cathedra Gost, predavač Analiza primjera, case studies Demonstracije Diskusija problema Pitanja - odgovori Seminar, izlaganje studenta s raspravom				
Način izvođenja laboratorijskih vježbi	Laboratorijske, simulacije na računalima Analiza literature na webu, knowledge mining Pisanje eseja Radionica				
Sadržaj predavanja	1.Repozitoriji forenzičkih skripti i njihovo korištenje, 2h, Ishodi:1 2.Modificiranje forenzičkih skripti, 2h, Ishodi:1,5,6 3.Varijable i operacija,, 2h, Ishodi:3 4.String, lista, tuple, 2h, Ishodi:3 5.Metode, klase, nasljeđivanje,, 2h, Ishodi:3 6.Metode, klase, nasljeđivanje,, 2h, Ishodi:3,4,5,6 7.Objektne strukture u forenzici - primjeri, 2h, Ishodi:3,5 8.Objektne strukture u forenzici - primjeri, 2h, Ishodi:3,5 9.Izrada skripti za pretraživanje, 2h, Ishodi:2 10.Izrada skripti za pretraživanje, 2h, Ishodi:2 11.Skripte u mobilnoj forenzici, 2h, Ishodi:2,4,5 12.Skripte u mobilnoj forenzici, 2h, Ishodi:5,6 13.Skripte u alatima za forenziku računala, 2h, Ishodi:1,2,5,6 14.Skripte u alatima za forenziku računala, 2h, Ishodi:1,2,5 15.Rekapitulacija i ponavljanje s primjerima iz prakse, 2h, Ishodi:1,2,3,4,5,6				
Sadržaj laboratorijskih vježbi	1.Uvod u skriptni jezik, 2h, Ishodi:3 2.Varijable i operatori, 2h, Ishodi:3 3.Strukture IF i repetitivne strukture ,, 2h, Ishodi:3,4 4.Složene strukture podataka, 2h, Ishodi:3 5.Složene strukture podataka, 2h, Ishodi:3 6.Modificiranje forenzičkih skripti s objektnim strukturama, 2h, Ishodi:6 7.Modificiranje forenzičkih skripti s objektnim strukturama, 2h, Ishodi:6 8.1. kolokvij, 2h, Ishodi:2,3,4 9.Modificiranje forenzičkih skripti s objektnim strukturama, 2h, Ishodi:6 10.Regularni izrazi u digitalnoj forenzici,, 2h, Ishodi:2 11.Pisanje skripti za forenzički alat za mobilnu forenziku, 2h, Ishodi:6 12.logičke operacije u digitalnoj forenzici, 2h, Ishodi:2 13.Pisanje i modificiranje skripti u forenzičkom alatu za forenziku računala, 2h, Ishodi:5,6 14.Pisanje i modificiranje skripti u forenzičkom alatu za forenziku računala, 2h, Ishodi:5,6 15.2 kolokvij, 2h, Ishodi:1,4,5,6				
Materijalni uvjeti za izvedbu predmeta	Elementarni: predavaona, ploča, kreda... Računalni laboratorij opće namjene Bijela ploča sa flomasterima Projektor				
Ishodi	6#7				
Literatura	Hans Petter Langtangen,Python Scripting for Computinal Science ,Springer,978-3-540-73915-9, 2008 2. Guidance Ltd,ENScript Language ,Guidance Ltd, 2012 3. Chet Hosmer,Python Forensics,Elsevier,978-0-12-418676-7, 2014 TJ. OConnor - A Cookbook for Hackers,Forensic Analysts, Penetration Testers and Security Engineers,Violent Python,Elsevier,ISBN: 978-1-59749-957-6, 2014 2. Al Sweigart,Hacking Secret Ciphers with Python,Al Sweigart, 978-1482614374, 2013 3. Chet Hosmer,Python Forensics,Elsevier, 978-0-12-418676-7, 2014				
Uvjeti za potpis	Izrada seminara i vježbi je obvezna za sve studente su i uvjet za potpis				



(obaveze studenta)	Vježbe se izvode na programskom jeziku Python i powershell sa konkretnim zadacima kojima je cilj usvojiti vještine izrade skripti, programa kojim se mogu dobiti detaljniji uvodi u digitalne sadržaje/digitalni dokazi (povijest pozivam, Geo lokacija i sl.)												
Provjera znanja u semestru	Laboratorijske vježbe ili seminar do 50 bodova #61623; Dva kolokvija po 25 bodova (Svaki kolokvij ima popravak) #61623; Opcionalni bodovi za zalaganje #61623; Ukoliko student ne položi kolokvije ima mogućnost izlaska na usmeni ispit. #61623; Ukupno maksimalno 100 bodova 0-49 - nedovoljan 50-61 - dovoljan 62-74 - dobar 75-86 - vrlo dobar 87-100 - izvrstan												
Način polaganja ispita nakon semestra	Pismeni 50% i usmeni ispit 50% s provjerom svih ishoda učenja. 0-49 - nedovoljan 50-61 - dovoljan 62-74 - dobar 75-86 - vrlo dobar 87-100 - izvrstan												
Praćenje rada studenta:	<table><tr><td>Aktivnost</td><td>ECTS</td></tr><tr><td>Pohađanje nastave ()</td><td>1</td></tr><tr><td>Aktivnost u nastavi ()</td><td>1</td></tr><tr><td>Kontinuirana provjera znanja ()</td><td>1</td></tr><tr><td>Praktični rad ()</td><td>1</td></tr><tr><td>Eksperimentalni rad ()</td><td>2</td></tr></table>	Aktivnost	ECTS	Pohađanje nastave ()	1	Aktivnost u nastavi ()	1	Kontinuirana provjera znanja ()	1	Praktični rad ()	1	Eksperimentalni rad ()	2
Aktivnost	ECTS												
Pohađanje nastave ()	1												
Aktivnost u nastavi ()	1												
Kontinuirana provjera znanja ()	1												
Praktični rad ()	1												
Eksperimentalni rad ()	2												
Napomena	Iz ovog predmeta moguća je izrada završnog/diplomskog rada												
Preduvjeti:	Nema preduvjeta												
Izradio prijedlog	mr.sc. Marinko Žagar viši predavač, 17.6.2019												



Šifra WEB/ISVU	25226/173045	ECTS	6.0	Akadska godina	2019/2020
Naziv	Tehnike sigurnog programiranja				
Status	3. semestar - Politehni?ki specijalisti?ki diplomski studij, Informacijska sigurnost i digitalna forenzika (Izvanredni specijalisti?ki informacijska sigurnost i digitalna forenzika) - Obavezni predmet				
Izvedba nastave	Predavanja + vjezbe (auditorne+laboratorij+seminar+konstrukcijske) Samostalan rad			30+30 (0+30+0+0) 120	
Izvođači	Predavanja:1. v.pred. Aleksander Radovan , dipl. ing. Laboratorijske vjezbe:v.pred. Aleksander Radovan , dipl. ing.				
Cilj predmeta	Upoznavanje sa standardima i tehnikama sigurnog programiranja te korištenje istih prilikom implementacija desktop, web i mobilnih aplikacija. Analiza naj?ešćih sigurnosnih problema i upoznavanje tehnika za njihovo sprečavanje.				
Ishodi učenja:	1.izdvojiti opciju korištenja koncepata defenzivnog programiranja radi zaštite sigurnosnih aspekata aplikacije. Razina:6 2. procijeniti rizike korištenja pojedine HTTP metode. Razina:6,7 3.dizajnirati sustav otporan na naj?ešće sigurnosne rizike. Razina:6 4. izabrati opciju implementacije modula za prijavu u aplikaciju koji će smanjiti rizik ugrožavanja osjetljivih podataka radnim napadima kao što su brute force attack. Razina:7 5. odabrati načine implementacije aplikacije koji sprečavaju SQL Injection napad na aplikacijske resurse. Razina:7 6.usporediti načine za rad s datotekama koji će spriječiti neovlašteno korištenje podataka koji se nalaze u njima. Razina:6,7 7. preporučiti korištenje održavanja životnog ciklusa sigurnog programiranja svih članova razvojnog tima. Razina:7				
Način izvođenja predavanja	Frontalna, ex cathedra Gost, predavač Analiza primjera, case studies Demonstracije Pitanja - odgovori Izlaganje domaćih zadaća				
Način izvođenja laboratorijskih vjezbi	Laboratorijske, simulacije na računalima Rasprave, brainstorming Računalne simulacije Međusobno zadavanje i rješavanje problema				
Sadržaj predavanja	1.Sigurnosne prijetnje, 2h, Ishodi:2 2.Sigurnosne tehnologije, 2h, Ishodi:5 3.Sigurnosni skeneri Web aplikacija, 2h, Ishodi:3 4.Penetracijsko tesiranje, 2h, Ishodi:2,3 5.CERT inicijativa sigurnog kodiranja, 2h, Ishodi:3 6.OWASP preporuke sigurnog kodiranja, 2h, Ishodi:5 7.NASA 10 pravila za razvoj sigurnog kritičnog koda, 2h, Ishodi:3 8.Principi zaštite osjetljivih podataka, 2h, Ishodi:6 9.Implementacija restriktivnih politika, 2h, Ishodi:4,6 10.Zaštita klijentske strane, 2h, Ishodi:3,6 11.Postavljanje korisničkih ograničenja, 2h, Ishodi:1 12.Principi rada sa datotekama, 2h, Ishodi:6 13.Defenzivni dizajn programskog koda, 2h, Ishodi:3 14.Ofenzivno programiranje, 2h, Ishodi:2,3 15.Tehnike sigurnog programiranja, 2h, Ishodi:4,7				
Sadržaj laboratorijskih vjezbi	1.Osnovne sigurnosti web aplikacij, 2h, Ishodi:1,6 2.Zaštita osjetljivih podataka, 2h, Ishodi:6 3.Siguran rad s datotekama, 2h, Ishodi:6 4.Upravljanje pristupom, 2h, Ishodi:4 5.Autentifikacija i upravljanje sesijom, 2h, Ishodi:2,4 6.Defenzivno programiranje, 2h, Ishodi:1 7.Obrana od Cross-Site Scripting napada, 2h, Ishodi:3 8.Obrana od SQL Injection napada, 2h, Ishodi:3,5 9.Praćenje i detekcija uljeza, 2h, Ishodi:4 10.Životni ciklus održavanja sigurnog programiranja, 2h, Ishodi:7 11.Nema nastave, 2h 12.Nema nastave, 2h 13.Nema nastave, 2h 14.Nema nastave, 2h 15.Nema nastave, 2h				
Materijalni uvjeti za izvedbu predmeta	Elementarni: predavaona, ploča, kreda... Računalni laboratorij opće namjene Projektor				
Ishodi	6#7				
Literatura	1.Jim Manico, August Detlefsen,Iron-Clad Java: Building Secure Web Applications,Oracle press, 978-0-07-183588-6, 2014 2.Fred Long i dr.,Java Coding Guidelines: 75 Recommendations for Reliable and Secure Programs (SEI Series in Software Engineering),,Addison-Wesley, 978-0-321-93315-7, 2013 3.Fred Long i dr.,The CERT Oracle Secure Coding Standard for Java (SEI Series in Software Engineering),Addison-Wesley, 978-0-321-80395-5, 2012				
Uvjeti za potpis (obaveze studenta)	Izrada vjezbi je obavezna za sve studente i uvjet za potpis. Predaja i kolokviranje svih vjezbi je preduvjet za ostvarivanja prava na izlazak na ispit.				



Provjera znanja u semestru	Laboratorijske vježbe do 60% Kontrolne zadaće (2) 40%																
Način polaganja ispita nakon semestra	Pismeni/usmeni ispit (ako student ne zadovolji na kontrolnim zadaćama) 40%																
Praćenje rada studenta:	<table><thead><tr><th></th><th>ECTS</th></tr></thead><tbody><tr><td>Aktivnost</td><td></td></tr><tr><td>Pohađanje nastave ()</td><td>1</td></tr><tr><td>Pismeni ispit ()</td><td>1</td></tr><tr><td>Usmeni ispit ()</td><td>1</td></tr><tr><td>Seminarski rad ()</td><td>1</td></tr><tr><td>Praktični rad ()</td><td>1</td></tr><tr><td>Aktivnost u nastavi ()</td><td>1</td></tr></tbody></table>		ECTS	Aktivnost		Pohađanje nastave ()	1	Pismeni ispit ()	1	Usmeni ispit ()	1	Seminarski rad ()	1	Praktični rad ()	1	Aktivnost u nastavi ()	1
	ECTS																
Aktivnost																	
Pohađanje nastave ()	1																
Pismeni ispit ()	1																
Usmeni ispit ()	1																
Seminarski rad ()	1																
Praktični rad ()	1																
Aktivnost u nastavi ()	1																
Napomena	Iz ovog predmeta moguća je izrada završnog/diplomskog rada																
Preduvjeti:	Nema preduvjeta																
Izradio prijedlog	mr.sc. Marinko Žagar viši predavač, 18.6.2019																



Šifra WEB/ISVU	25221/173040	ECTS	5.0	Akadska godina	2019/2020
Naziv	Upravljanje kontinuitetom poslovanja				
Status	3. semestar - Politehni?ki specijalisti?ki diplomski studij, Informacijska sigurnost i digitalna forenzika (Izvanredni specijalisti?ki informacijska sigurnost i digitalna forenzika) - Obavezni predmet				
Izvedba nastave	Predavanja + vje?be (auditorne+laboratorij+seminar+konstrukcijske) Samostalan rad			30+20 (0+10+10+0) 100	
Izvođa?i	Predavanja:1. mr.sc. Marinko ?agar viši predava? Laboratorijske vje?be: Ines Trbojevi? Košturjak Seminarske vje?be: Ines Trbojevi? Košturjak				
Cilj predmeta	Upoznavanje s problematikom upravljanja kontinuitetom poslovanja, va?nošću za organizacije te primjenom procesa upravljanja kontinuitetom poslovanja.				
Ishodi u?enja:	1. kriti?ki prosuđivati koncept održavanja i upravljanja kontinuitetom poslovanja. Razina:7 2.planirati razvoj i održavanje plana kontinuiteta poslovanja. Razina:6,7 3.razlikovati Razlikovati korake i faze kao i strateške aktivnosti koncepta upravljanja kontinuitetom poslovanja. Razina:6 4.analizirati utjecaja na poslovanje, procjenu prihvatljive razine rizika. Razina:6 5. pripremiti testiranje kontinuiteta poslovanja. Razina:6,7 6. procijeniti rizike koji ugro?avaju resurse, te na vrijeme implementirati kontrole koje će zaustaviti prijetnju ili smanjiti potencijalnu štetu. Razina:6,7 7.planirati oporavak poslovnih procesa i organizacije. Razina:6,7				
Na?in izvođenja predavanja	Frontalna, ex cathedra Gost, predava? Analiza primjera, case studies Simulacije Modeliranje Pitanja - odgovori				
Na?in izvođenja laboratorijskih vje?bi	Laboratorijske, simulacije na ra?unalima Međusobno zadavanje i rješavanje problema Radionica				
Na?in izvođenja seminarskih vje?bi	Laboratorijske, simulacije na ra?unalima Grupno rješavanje zadanih problema Međusobno zadavanje i rješavanje problema Radionica				
Sadržaj predavanja	1.Osnove o upravljanju kontinuitetom poslovanja (BCM), 2h, Ishodi:1,3,6 2.O?ekivanja od upravljanja kontinuitetom poslovanja (BCM), 2h, Ishodi:1,3,6 3.Identifikacija mogućih prijetnji i rizika, 2h, Ishodi:1,2,3,6 4.Uzroci prekida poslovanja, 2h, Ishodi:1,3 5.Utjecaj na organizaciju, 2h, Ishodi:4,6,7 6.Kako procijeniti rizike koji proizlaze iz prekida poslovanja, 2h, Ishodi:4,6 7.Identifikacija ključnih poslovnih procesa i procjena utjecaja na poslovanje (eng. Business Impact Assesment), 2h, Ishodi:5,6,7 8.Strateška analiza prioriteta i opcija oporavka poslovanja, 2h, Ishodi:4,7 9.Definiranje BCM strategije, 2h, Ishodi:1,6,7 10.Koraci i faze izrade analize utjecaja na poslovanje, 2h, Ishodi:6,7 11.Procjena financijskih i operativnih učinaka (štete) poslovnih procesa povezanih s prekidom poslovanja, 2h, Ishodi:6,7 12.Testiranje plana kontinuiteta i plana oporavka, 2h, Ishodi:1,6,7 13.Planiranje i upravljanje izvanrednim situacijama, 2h, Ishodi:2,3,6,7 14.Oporavak poslovanja, 2h, Ishodi:6,7 15.Norme i alati za izradu plana upravljanja kontinuitetom poslovanja, 2h, Ishodi:2,3				
Sadržaj laboratorijskih vje?bi	1.Analiza organizacije, procesa i rizika, 2h, Ishodi:1,4,7 2.Procijeniti rizike koji proizlaze iz prekida poslovanja, 1h, Ishodi:5,6,7 3.Identificirati rizike i izraditi matricu rizika, 1h, Ishodi:2,3,4,5 4.Procijeniti financijski i operativni učinak prekida poslovanja, 1h, Ishodi:6,7 5.Primjenjivanje norme ISO 22301, 1h, Ishodi:1,3 6.Izrađivanje plana kontinuiteta poslovanja, 1h, Ishodi:1,5 7.Primjenjivati alate za izradu plana upravljanja kontinuitetom poslovanja, 1h, Ishodi:1,5,6,7 8.Korištenje alata za procjenu rizika koji ugro?avaju poslovanje, 1h, Ishodi:1,6,7 9.Upravljanje poslovanjem u izvanrednim situacijama, 1h, Ishodi:1,5,6,7 10.Nema nastave, 2h 11.Nema nastave, 2h 12.Nema nastave, 2h 13.Nema nastave, 2h 14.Nema nastave, 2h 15.Nema nastave, 2h				
Sadržaj seminarskih vje?bi	1.Definiranje teme seminarskog rada, 2h, Ishodi:1,2 2.Pisanje seminarskog rada, 6h, Ishodi:1,2,3,4,5,6,7 3.Prezentiranje seminarskog rada, 2h, Ishodi:4,5,6 4.Nema nastave, 2h 5.Nema nastave, 2h 6.Nema nastave, 2h 7.Nema nastave, 2h 8.Nema nastave, 2h				



	9.Nema nastave, 2h 10.Nema nastave, 2h 11.Nema nastave, 2h 12.Nema nastave, 2h 13.Nema nastave, 2h 14.Nema nastave, 2h 15.Nema nastave, 2h
Materijalni uvjeti za izvedbu predmeta	Elementarni: predavaona, ploča, kreda... Računalni laboratorij opće namjene Bijela ploča sa flomasterima Projektor
Ishodi	6#7
Literatura	1. Jim Burtles, Principles and Practice of Business Continuity, Philip Jan Rothestein,978-1931332392, 2007 2. Michael Wallace, The Disaster Recovery Handbook: A Step-by-Step Plan to Ensure Business Continuity and Protect Vital Operations, Facilities, and Assets, 978-0814437841 ,2010 3. Centar informacijske sigurnosti, Upravljanje kontinuitetom poslovnih procesa, Centar informacijske sigurnosti, 2011 4. mr.sc. Antonio Valčić, Upravljanje kontinuitetom poslovanja u financijskoj industriji, Hrvatska Narodna Banka, 2013
Uvjeti za potpis (obaveze studenta)	Pohađanje nastave minimalno 80% Izrada i prezentacija seminarskog rada
Provjera znanja u semestru	Laboratorijske vježbe ili seminar do 50 bodova #61655;Dva kolokvija po 25 bodova (Svaki kolokvij ima popravak) #61655;Opcionalni bodovi za zalaganje
Način polaganja ispita nakon semestra	Ukoliko student ne položi kolokvije ima mogućnost izlaska na usmeni ispit. #61655;Ukupno maksimalno 100 bodova #61655;0-49 - nedovoljan #61655;50-61 - dovoljan #61655;62-74 - dobar #61655;75-86 - vrlo dobar #61655;87-100 - izvrstan
Praćenje rada studenta:	Aktivnost ECTS Pohađanje nastave () 1 Seminarski rad () 1 Pismeni ispit () 2 Usmeni ispit () 1
Napomena	Iz ovog predmeta moguća je izrada završnog/diplomskog rada
Preduvjeti:	Nema preduvjeta
Izradio prijedlog	mr.sc. Marinko Žagar viši predavač, 17.6.2019



Šifra WEB/ISVU	24969/173036	ECTS	6.0	Akadska godina	2019/2020
Naziv	Upravljanje rizicima i incidentima informacijske sigurnosti				
Status	2. semestar - Politehni?ki specijalisti?ki diplomski studij, Informacijska sigurnost i digitalna forenzika (Izvanredni specijalisti?ki informacijska sigurnost i digitalna forenzika) - Obavezni predmet				
Izvedba nastave	Predavanja + vje?be (auditorne+laboratorij+seminar+konstrukcijske) Samostalan rad			30+20 (0+10+10+0) 130	
Izvođači	Predavanja:1. mr.sc. Marinko ?agar viši predava? Laboratorijske vje?be: Ines Trbojevi? Košturjak Seminarske vje?be: Ines Trbojevi? Košturjak				
Cilj predmeta	Steći znanje potrebno za planiranje, implementaciju i održavanje sustava upravljanja rizicima				
Ishodi učenja:	1. organizirati Organizirati implementaciju, održavanje i upravljanje programom upravljanja rizicima informacijske sigurnosti. Razina:6,7 2. prezentirati Prezentirati najbolju praksu u upravljanju rizicima informacijske sigurnosti. Razina:6,7 3.analizirati Analizirati koncepte, pristupe, standarde, metode i tehnike za efektivno upravljanje rizicima. Razina:6 4.analizirati Analizirati odnos između sustava informacijske sigurnosti, sigurnosnih kontrola te zakonskih/regulatornih odredbi vezanih uz upravljanje rizicima. Razina:6 5. pripremiti Primijeniti postupak procjene rizika i obradu rizika unutar organizacije. Razina:6,7 6.identificirati Identificirati koncepte, pristupe, metode i tehnike koji omogućavaju efektivno upravljanje rizicima. Razina:6 7.identificirati Identificirati i vršiti procjene rizika. Razina:6				
Način izvođenja predavanja	Frontalna, ex cathedra Gost, predava? Simulacije Seminar, izlaganje studenta s raspravom				
Način izvođenja laboratorijskih vje?bi	Laboratorijske s laboratorijskom opremom Laboratorijske, simulacije na računalima Rasprave, brainstorming Računalne simulacije Radionica				
Način izvođenja seminarskih vje?bi	Laboratorijske s laboratorijskom opremom Laboratorijske, simulacije na računalima Rasprave, brainstorming Računalne simulacije Radionica				
Sadržaj predavanja	1.Osnovni pojmovi, Resursi, Prijetnje, Ranjivosti, Rizik, 2h, Ishodi:1,2 2.Koncepti i definicije koje se odnose na upravljanje rizicima, 2h, Ishodi:1,5,7 3.Norme, standardi i metodologije u upravljanju rizicima, 2h, Ishodi:1,4 4.Prepoznavanje prijetnji i ranjivosti, 2h, Ishodi:6 5.Karakterizacija sustava, 2h, Ishodi:3,5 6.Analiza kontrola, 2h, Ishodi:3,5 7.Određivanje vjerojatnosti, 2h, Ishodi:3 8.Analiza utjecaja, 2h, Ishodi:3,5 9.Određivanje i ublažavanje rizika, 2h, Ishodi:3,7 10.Strategija za smanjenje rizika, 2h, Ishodi:3 11.Rukovanje s rizicima, 2h, Ishodi:1,3,7 12.Prepoznavanje rizika i procjena prema ISO 27005 normi, 2h, Ishodi:5,6 13.Zakonska regulativa RH, 2h, Ishodi:4 14.HANFA Smjernice za primjereno upravljanje rizicima informacijskih sustava, 2h, Ishodi:1,3 15.Sustav upravljanje informacijskom sigurnošću (ISMS), 2h, Ishodi:5 Praćenje i pregled čimbenika rizika, 2h, Ishodi:7 Nadzor upravljanja rizicima, 2h, Ishodi:4,6 Metode analize rizika (CRAM, EBIOS, MEHARI,OCTAVE), 2h, Ishodi:1,2,3 Microsoft Security Risk Management, 2h, Ishodi:2,3 Sigurnosni incidenti i postupci u slučaju sigurnosnih incidenata, 2h, Ishodi:7				
Sadržaj laboratorijskih vje?bi	1.-, 2h 2.-, 2h 3.-, 2h 4.Identifikacija rizika informacijske sigurnosti, 1h, Ishodi:1,3 5.Izvesti analizu i vrednovanje rizika, 1h, Ishodi:2,3,6 6.Korištenje alata za procjenu rizika, 1h, Ishodi:3,6 7.Korištenje metodologije za upravljanje rizicima, 1h, Ishodi:5,6 8.Primjena postupaka za obradu rizika, 1h, Ishodi:1,5,6 9.Korištenje programa za upravljanje rizicima, 1h, Ishodi:5,6 10.Primjena zakonskih normi i regulatornih kontrola vezanih uz upravljanje rizicima, 2h, Ishodi:4,5,6 11.Primjenjivati mjere za smanjenje rizika informacijske sigurnosti, 2h, Ishodi:2,3 12.-, 2h 13.-, 2h 14.-, 2h 15.-, 2h				
Sadržaj seminarskih vje?bi	1.-, 2h 2.-, 2h				



	3.-, 2h 4. Identifikacija rizika informacijske sigurnosti, 1h, Ishodi:2,3 5. Izvesti analizu i vrednovanje rizika, 1h, Ishodi:2,3,6 6. Korištenje alata za procjenu rizika, 1h, Ishodi:3,6 7. Korištenje metodologije za upravljanje rizicima, 1h, Ishodi:5,6 8. Primjena postupaka za obradu rizika, 1h, Ishodi:1,5,6 9. Korištenje programa za upravljanje rizicima, 1h, Ishodi:5,6 10. Primjena zakonskih normi i regulatornih kontrola vezanih uz upravljanje rizicima, 2h, Ishodi:4,5,6 11. Primjenjivati mjere za smanjenje rizika informacijske sigurnosti, 2h, Ishodi:2,3 12.-, 2h 13.-, 2h 14.-, 2h 15.-, 2h																
Materijalni uvjeti za izvedbu predmeta	Elementarni: predavaona, ploča, kreda... Namjenski računalni laboratorij Bijela ploča sa flomasterima Projektor																
Ishodi	6#7																
Literatura	1. Atle Refsdal, Bj#248;rnar Solhaug, Ketil St#248;len, Cyber-Risk Management, Springer, 978-3-319-23569-1, 2015 2. CERT, Upravljanje sigurnosnim incidentima, CARNet CERT, 2009 3. Steve Elky, An Introduction to Information System Risk Management SANS 2007																
Uvjeti za potpis (obaveze studenta)	Maksimalni dozvoljeni broj izostanaka sa predavanja: ne više od 50%																
Provjera znanja u semestru	Dva kolokvija po 25 bodova (Svaki kolokvij ima popravak) Opcionalni bodovi za zalaganje Ukoliko student ne položi kolokvije ima mogućnost izlaska na usmeni ispit.																
Način polaganja ispita nakon semestra	Vježbe i seminar sa prezentacijom do 50 bodova Dva kolokvija po 25 bodova (Svaki kolokvij ima popravak) Opcionalni bodovi za zalaganje Ukoliko student ne položi kolokvije ima mogućnost izlaska na usmeni ispit. Ukupno maksimalno 100 bodova Pragovi ocjena: 0-49 - nedovoljan (1) 50-61 - dovoljan (2) 62-74 - dobar (3) 75-86 - vrlo dobar (4) 87-100 - izvrstan (5)																
Praćenje rada studenta:	<table><thead><tr><th></th><th>ECTS</th></tr></thead><tbody><tr><td>Aktivnost</td><td></td></tr><tr><td>Pohađanje nastave ()</td><td>1</td></tr><tr><td>Pismeni ispit ()</td><td>1</td></tr><tr><td>Usmeni ispit ()</td><td>1</td></tr><tr><td>Aktivnost u nastavi ()</td><td>1</td></tr><tr><td>Kontinuirana provjera znanja ()</td><td>1</td></tr><tr><td>Seminarski rad ()</td><td>1</td></tr></tbody></table>		ECTS	Aktivnost		Pohađanje nastave ()	1	Pismeni ispit ()	1	Usmeni ispit ()	1	Aktivnost u nastavi ()	1	Kontinuirana provjera znanja ()	1	Seminarski rad ()	1
	ECTS																
Aktivnost																	
Pohađanje nastave ()	1																
Pismeni ispit ()	1																
Usmeni ispit ()	1																
Aktivnost u nastavi ()	1																
Kontinuirana provjera znanja ()	1																
Seminarski rad ()	1																
Napomena	Iz ovog predmeta moguća je izrada završnog/diplomskog rada																
Preduvjeti:	Nema preduvjeta																
Izradio prijedlog	Doc. dr. sc. Marko Horvat v. pred., 13.6.2018.																



Šifra WEB/ISVU	25070/185428	ECTS	6.0	Akadska godina	2019/2020
Naziv	Zakonska osnova digitalne forenzike				
Status	1. semestar - Politehni?ki specijalisti?ki diplomski studij, Informacijska sigurnost i digitalna forenzika (Izvanredni specijalisti?ki informacijska sigurnost i digitalna forenzika) - Obavezni predmet				
Izvedba nastave	Predavanja + vjezbe (auditorne+laboratorij+seminar+konstrukcijske) Samostalan rad			30+30 (0+15+15+0) 120	
Izvođači	Predavanja:1. izv. prof. dr. sc. Krunoslav Antoliš Laboratorijske vjezbe:izv. prof. dr. sc. Krunoslav Antoliš Seminarske vjezbe:izv. prof. dr. sc. Krunoslav Antoliš				
Cilj predmeta	Usvojiti znanja o zakonskoj osnovi te zakonitom postupanju u domeni digitalne forenzike				
Ishodi učenja:	<p>1.analizirati 7.Studenti će naučiti zakonito postupati prilikom procese prikupljanja, obrade i analize digitalnih dokaza, stvaranja izvješća o digitalno forenzičkoj istrazi, te postupanju pri pohrani i čuvanju digitalnih dokaza, a također biti će i osposobljeni za donošenje ekspertnih prosudbi o digitalno forenzičnim materijalima u skladu sa normativnim aktima. Razina:6</p> <p>2.analizirati 6.Studenti će biti u stanju objediniti i povezati, rezultate digitalne forenzične istrage u funkciji rekonstrukcije, te utvrđivanja njezine utemeljenosti na konvencijama, zakonima i uredbama u cilju zaključivanja o zakonitosti postupanja i validnosti dokaza. Razina:6</p> <p>3.analizirati 5.Studenti će znati odabirati i uporabiti adekvatne zakonske norme u funkciji preventivne i kurativne zaštite od informacijskih napada, a biti će također i osposobljeni za odabir i uporabu, odgovarajućih PKI koncepata zaštite baziranih na tehnikama i metodama kriptiranja, te digitalnom potpisu i digitalnim certifikatima. Razina:6</p> <p>4.analizirati 4.Studenti će ovladati znanjima iz zakonske regulative u svezi sa sigurnosti poslovne suradnje te biti u stanju ekspertno pomoći u postupanju pri dobivanju certifikata poslovne sigurnosti, te sklapanja ugovora koji sadrže klasificirane podatke i informacije. Razina:6</p> <p>5.analizirati 3.Studenti će biti osposobljeni za prepoznavanje prijetnji i analizu rizika te sa načinima zaključivanja o posljedicama koje mogu nastati iz realizacije tih prijetnji i to posebice kada je riječ o klasificiranim podacima. Razina:6</p> <p>6.analizirati 2.Studenti će sukladno EU direktivama znati zaštititi temeljna prava i slobode pojedinca u svezi s obradom podataka kao i kako se osigurava slobodan protok osobnih podataka između država članica.. Razina:6</p> <p>7.analizirati 1.Studenti će biti osposobljeni razumjeti važnost i spoznati ulogu zakonske regulative te će moći ocijeniti i interpretirati rad sa digitalnim podacima i informacijama nastalim digitalnom forenzičkom analizom u skladu sa normativnim aktima. Razina:6</p>				
Način izvođenja predavanja	Frontalna, ex cathedra Gost, predavač Analiza primjera, case studies Demonstracije Simulacije Modeliranje Diskusija problema Pitanja - odgovori Seminar, izlaganje studenta s raspravom Izlaganje domaćih zadaća				
Način izvođenja laboratorijskih vježbi	Laboratorijske s laboratorijskom opremom Laboratorijske, simulacije na računalima Grupno rješavanje zadanih problema Analiza klasične literature Analiza literature na webu, knowledge mining Pisanje eseja Rasprave, brainstorming Mapiranje pojmova, mind-mapping Računalne simulacije Međusobno zadavanje i rješavanje problema Radionica				
Način izvođenja seminarskih vježbi	Laboratorijske s laboratorijskom opremom Laboratorijske, simulacije na računalima Grupno rješavanje zadanih problema Analiza klasične literature Analiza literature na webu, knowledge mining Pisanje eseja Rasprave, brainstorming Mapiranje pojmova, mind-mapping Računalne simulacije Međusobno zadavanje i rješavanje problema Radionica Ostalo, upisati UFED				
Sadržaj predavanja	<p>1.Međunarodni i nacionalni., strateški i zakonski okvir, 1h, Ishodi:1 Konvencija o kibernetičkom kriminalitetu VE, , 1h, Ishodi:1,4,5,6</p> <p>2.Konvencija o sprječavanju terorizma VE, 1h, Ishodi:1,3,4,6</p> <p>Uredba (EU) 2016/679 Europskog parlamenta I Vijeća o zaštiti pojedinaca u vezi s obradom osobnih podataka i o slobodnom kretanju takvih podataka, 1h, Ishodi:1,2</p> <p>3.Zakon o zaštiti osobnih podataka, 2h, Ishodi:1,2,5</p> <p>4.Autorska i srodna pravila u virtualnom okruženju, 2h, Ishodi:2</p> <p>5.Zakon o tajnosti podataka, 2h, Ishodi:3</p> <p>6.Pravilnik o tajnosti obrade podataka, 1h, Ishodi:3</p>				



	<p>Nacionalne strategije kibernetičke sigurnosti, , 1h, Ishodi:3 7.Nacionalna strategija za prevenciju i suzbijanje terorizma, 1h, Ishodi:3 Zakon o sigurnosno obavještajnom sustavu RH, , 1h, Ishodi:3,5,7 8.Zakon o informacijskoj sigurnosti, 2h, Ishodi:3,5,7 9.Uloga i zadaća UVNS, ZSIS, Nacionalni CERT u sustavu informacijske sigurnosti RH, , 2h, Ishodi:3,7 10.Sigurnosna politika i upravljanje informacijskim rizikom, 1h, Ishodi:3 Kazneno procesni okvir, 1h, Ishodi:3,5,6,7 11.Kazneni zakon glava 25, 1h, Ishodi:3,5,7 Zakon o kaznenom postupku, , 1h, Ishodi:3,5,7 12.Pravilnik o načinu provođenja posebnih dokaznih radnji, 1h, Ishodi:7 Prepoznavanje i postupanje prilikom izuzimanja digitalnih dokaza, 1h, Ishodi:7 13.Prijenos i čuvanje digitalnih dokaza, 1h, Ishodi:7 Pretraga nositelja digitalnih dokaza, 1h, Ishodi:7 14.Rekonstrukcija na bazi digitalnih dokaza, 1h, Ishodi:6,7 Struktura, sadržaj i izgled izvješća nastalog digitalnom forenzičkom analizom, 1h, Ishodi:7 15.Ekspertna prosudba materijala nastalih digitalnom forenzikom, 1h, Ishodi:7 Vještačenje i digitalna forenzika, 1h, Ishodi:3,5,7</p>
Sadržaj laboratorijskih vježbi	<p>1.Metode i tehnike digitalne forenzike, 1h, Ishodi:1,7 2.Informacijske ugroze i analizu rizika, 1h, Ishodi:3 3.Sigurnost infrastrukture javnog ključa, 1h, Ishodi:5 4.Tehnike i metode kriptiranja, 1h, Ishodi:5 5.Digitalni potpis, Digitalni certifikati, , 1h, Ishodi:5 6.Prikupljanje digitalnih dokaza, , 1h, Ishodi:7 7.Obrada i analiza digitalnih dokaza, , 1h, Ishodi:7 8.Stvaranja izvješća o digitalno forenzičkoj istrazi, , 1h, Ishodi:7 9.Postupanja pri pohrani i čuvanju digitalnih dokaza, 1h, Ishodi:7 10.Digitalna forenzika i rekonstrukcija događaja, 1h, Ishodi:6 11.Metodologija zaključivanja o zakonitosti postupanja kod digitalne forenzične istrage, 1h, Ishodi:6 12.Informacijske prijetnje i načini zaštite klasificiranih podataka, 1h, Ishodi:3 13.Postupanja prilikom zahtjeva za dobivanje sigurnosti poslovne suradnje, , 1h, Ishodi:4 14.Sklapanje ugovora koji sadrže klasificirane podatke i informacije, 1h, Ishodi:4 15.Primjena EU direktiva u zaštiti temeljna prava i slobode pojedinca, , 1h, Ishodi:2</p>
Sadržaj seminarskih vježbi	<p>1.Informacijska sigurnost, 1h, Ishodi:1 2.Računalna sigurnost, 1h, Ishodi:1 3.Digitalna forenzika zakonske osnove, 1h, Ishodi:2 4.Digitalna forenzika tehnički aspekti, 1h, Ishodi:3 5.Računalne ugroze, 1h, Ishodi:5 6.Analiza rizika, 1h, Ishodi:4 7.Mjere i standardi informacijske sigurnosti, 1h, Ishodi:6 8.Sigurnost podataka, 1h, Ishodi:7 9.Sigurnost informacijskih sustava, 1h, Ishodi:7 10.Zloupotreba naprava, 1h, Ishodi:4 11.Neovlašteni pristup, 1h, Ishodi:6 12.Ometanje rada računalnog sustava, 1h, Ishodi:3 13.Oštećenje računalnih podataka, 1h, Ishodi:5 14.Računalno krivotvorenje, 1h, Ishodi:7 15.Računalna prijevarama, 1h, Ishodi:6</p>
Materijalni uvjeti za izvedbu predmeta	<p>Elementarni: predavaona, ploča, kreda... Namjenski laboratorij Računalni laboratorij opće namjene Namjenski računalni laboratorij Bijela ploča sa flomasterima Projektor Grafoskop Video oprema Maketa Alat, navesti Potrošni materijal, navesti Posebna oprema, navesti UFED</p>
Ishodi	6#7
Literatura	<p>1. K. Antoliš et all.: Sigurnost informacijskih sustava, ISBN 978-953-7390-92-1, nakladnik: Algebra d.o.o., Zagreb ožujak, 2016. 2. Dujella A., Maretić M.: Kriptografija, Element, Zagreb, 2007. 3. K. Antoliš et all.: Sigurnost računalnih mreža, ISBN 978-953-322-170-0, priručnik, nakladnik: Algebra d.o.o., Zagreb srpanj, 2014. 4.K. Antoliš et all.: Sigurnost elektroničkog poslovanja, ISBN 978-953-322-155-7, priručnik, nakladnik: Algebra d.o.o., Zagreb srpanj, 2013 5.K. Antoliš poglavlje u knjizi:The Darknet as a Safe Haven for Violent Extremists, str. 77.-87. U knjizi Violent Extremism and Radicalization Processes as Driving Factors to Terrorism Threats,CIP: 323.285(082), ISBN 978-961-94011-1-8, Institut for Corporative Security Studies, May 2018, Ljubljana, Slovenija, 6.K. Antoliš, P. Mišević, A. Miličević: VULNERABILITIES OF NEW TECHNOLOGIES AND THE PROTECTION OF CNI, Media, culture and public relations, ISSN 1333-6371, Vol. 6. No.1, INFO-84, 1, UDK: 004.521.39:004.7:001, Authors Review/ Pregledni rad, 6, 2015, Zagreb,</p>



	7.K. Antoliš: ICT Identity Theft, Informatologija, 46, 2013., 4, 353-360, UDK:681.3:340:001, Authors Review/Pregledni rad, ISSN 1330-0067, Zagreb, Hrvatska.												
Uvjeti za potpis (obaveze studenta)	Seminar je obavezan i sastoji se od eseja, prezentacije i javne obrane do 30 bodova Opcionalni bodovi za zalaganje 15 bodova												
Provjera znanja u semestru	Dva kolokvija po 20 bodova Ukoliko student ne položi kolokvije ima obvezu izlaska na pismeni ispit.												
Način polaganja ispita nakon semestra	Ocjene: 0-49 - nedovoljan 50-61 - dovoljan 62-74 - dobar 75-86 - vrlo dobar 87-100 izvrstan												
Praćenje rada studenta:	<table><thead><tr><th>Aktivnost</th><th>ECTS</th></tr></thead><tbody><tr><td>Esej ()</td><td>1</td></tr><tr><td>Usmeni ispit ()</td><td>2</td></tr><tr><td>Pohađanje nastave ()</td><td>1</td></tr><tr><td>Seminarski rad ()</td><td>1</td></tr><tr><td>Pismeni ispit ()</td><td>1</td></tr></tbody></table>	Aktivnost	ECTS	Esej ()	1	Usmeni ispit ()	2	Pohađanje nastave ()	1	Seminarski rad ()	1	Pismeni ispit ()	1
Aktivnost	ECTS												
Esej ()	1												
Usmeni ispit ()	2												
Pohađanje nastave ()	1												
Seminarski rad ()	1												
Pismeni ispit ()	1												
Napomena	Iz ovog predmeta moguća je izrada završnog/diplomskog rada												
Preduvjeti:	Nema preduvjeta												
Izradio prijedlog	izv. prof. dr. sc. Krunoslav Antoliš , 8.6.2018												