

Vanja Korać
Dragan Prlja
Andrej Diligenski

DIGITALNA FORENZIKA

Vanja Korać
Dragan Prlja
Andrej Diligenski

DIGITALNA FORENZIKA

Beograd, 2016.

Vanja Korać
Dragan Prlja
Andrej Diligenski
DIGITALNA FORENZIKA

Izdavači

Centar za nove tehnologije Viminacium
Arheološki Institut Beograd
Institut za uporedno pravo

Za izdavače

dr Miomir Korać, direktor
dr Jovan Ćirić, direktor

Recenzenti

Prof. dr Stevan Lilić
Prof. dr Gojko Grubor
Prof. dr Žarko Mijajlović

Urednik

dr Miomir Korać

Dizajn korica

dipl. inž. arh. Tijana Milanović

Dizajn i tehničko uređenje

Digital Art Company, Beograd

Štampa

Digital Art Company, Beograd

ISBN

978-86-87271-34-0

Tiraž

300

© Centar za nove tehnologije Viminacium, Beograd, 2016.

Sva prava zadržana. Nije dozvoljeno da bilo koji deo ove knjige bude snimljen, emitovan ili reprodukovan na bilo koji način, uključujući, ali ne ograničavajući se na fotokopiranje, fotografiju, magnetni upis ili bilo koji drugi vid zapisa, bez prethodne dozvole izdavača.

SADRŽAJ

UVOD.....	11
1. SAJBER KRIMINAL.....	15
1.1. Visokotehnoški kriminal - sajber kriminal - računarski kriminal.....	17
1.2. Tipovi visokotehnoškog kriminala.....	22
1.3. Zakonska regulativa sajber kriminala.....	35
1.4. Visokotehnoški kriminal - primeri iz prakse.....	44
2. DIGITALNA FORENZIKA I POSTUPAK ISTRAGE.....	57
2.1. Uloga računara u kriminalnim aktivnostima.....	60
2.1.1. Hardver kao instrument kriminalne aktivnosti.....	63
2.1.2. Hardver kao zabranjeni materijal ili plod kriminalne aktivnosti.....	64
2.1.3. Hardver kao dokaz kriminalne aktivnosti.....	64
2.1.4. Informacija kao instrument kriminalne aktivnosti.....	64
2.1.5. Informacija kao zabranjeni materijal ili plod kriminalne aktivnosti.....	65
2.1.6. Informacija kao dokaz.....	65
2.2. Digitalna forenzička istraga.....	68
2.2.1. Istražne metodologije - modeli.....	78
2.2.1.1. The DFRWS model.....	78
2.2.1.2. America's department of justice - DOJ model.....	80
2.2.1.3. Model "Odgovor na incident".....	81
2.2.1.4. Eoghan Casey model.....	82
2.2.1.5. Carrier i Spafford model.....	92
2.3. Digitalni dokazi.....	100
2.4. Prikupljanje podataka.....	106
2.5. Analiza prikupljenih podataka.....	117
2.6. Prihvatljivost digitalnog dokaza.....	124
2.7. Izveštavanje.....	126
2.8. Digitalna forenzika u virtuelnom okruženju.....	135

2.8.1. Virtuelno okruženje kao mesto krivičnog dela.....	137
2.8.2. Servisi u virtuelnom okruženju.....	138
2.8.3. Mreže u virtuelnom okruženju.....	140
2.8.4. Dokaz postojanja hardvera koji podržava virtuelizaciju.....	141
2.8.5. Dokazivanje vremena.....	142
2.8.6. Obezbeđivanje mesta krivičnog dela u virtuelnom okruženju.....	143
2.8.7. Pristup RAM-u.....	143
2.8.8. Virtuelni hard disk.....	144
2.8.9. Slike stanja virtuelnih mašina.....	146
2.8.10. Forenzičke kopije virtuelnih mašina.....	146
2.8.11. Migracija virtuelne mašine.....	147
2.8.12. Upotreba dokaza dobijenih iz virtuelnog okruženja u digitalno forenzičkoj analizi.....	148

3. DIGITALNA FORENZIKA WINDOWS I

LINUX RAČUNARSKIH SISTEMA.....	153
--------------------------------	-----

3.1. Forenzički odgovor na nedozvoljenu / incidentnu aktivnost “uživo” na Windows platformi.....

3.1.1. Podaci od značaja privremenog karaktera na Windows-u - datum i vreme.....	162
3.1.2. Podaci od značaja privremenog karaktera na Windows-u - logovani korisnici na sistemu i sesije.....	163
3.1.3. Podaci od značaja privremenog karaktera na Windows-u - dump memorijskog procesa i kompletan dump memorije....	167
3.1.4. Podaci od značaja privremenog karaktera na Windows-u - otvoreni fajlovi na sistemu.....	178
3.1.5. Podaci od značaja privremenog karaktera na Windows-u - informacije o mreži.....	179
3.1.6. Podaci od značaja privremenog karaktera na Windows-u - status mreže i konekcije.....	181
3.1.7. Podaci od značaja privremenog karaktera na Windows-u - interna tabela rutiranja.....	186
3.1.8. Podaci od značaja privremenog karaktera na Windows-u - startovani procesi i servisi.....	187
3.1.9. Podaci od značaja privremenog karaktera na Windows-u - mapirani portovi od strane procesa.....	192
3.1.10. Podaci od značaja privremenog karaktera na Windows-u - sadržaj privremene memorije.....	198
3.1.11. Podaci od značaja privremenog karaktera na Windows-u - istorija pokrenutih komandi.....	200

3.1.12. Podaci od značaja privremenog karaktera na Windows-u - mapirani drajvovi i deljeni resursi.....	201
3.1.13. Podaci od značaja privremenog karaktera na Windows-u - privremeni fajlovi.....	203
3.1.14. Postojani podaci od značaja na Windows-u - vremenski pečati fajl sistema.....	204
3.1.15. Postojani podaci od značaja na Windows-u - informacije o računarskom sistemu, verzija OS i nivo ažuriranosti paketa.....	206
3.1.16. Postojani podaci od značaja na Windows-u - setovanja registra baze.....	209
3.1.17. Postojani podaci od značaja na Windows-u - tačka za oporavak sistema.....	216
3.1.18. Postojani podaci od značaja na Windows-u - logovi na sistemu.....	219
3.1.19. Postojani podaci od značaja na Windows-u - Recycle bin i obrisani fajlovi.....	225
3.1.20. Postojani podaci od značaja na Windows-u - print spooler fajlovi.....	229
3.1.21. Postojani podaci od značaja na Windows-u - fajlovi linkova i najčešće korišćeni fajlovi.....	230
3.1.22. Postojani podaci od značaja na Windows-u - fajlovi internet aktivnosti.....	235
3.1.23. Postojani podaci od značaja na Windows-u - fajlovi aktivnosti elektronske pošte.....	241
3.2. Forenzički odgovor na nedozvoljenu / incidentnu aktivnost „uživo“ na Linux platformi.....	247
3.2.1. Podaci od značaja privremenog karaktera na Linux-u -sistemsko vreme i datum.....	252
3.2.2. Podaci od značaja privremenog karaktera na Linux-u - postojeće mrežne konekcije.....	252
3.2.3. Podaci od značaja privremenog karaktera na Linux-u - otvoreni TCP i UDP portovi.....	253
3.2.4. Podaci od značaja privremenog karaktera na Linux-u - izvršni fajlovi koji otvaraju TCP i UDP portove.....	254
3.2.5. Podaci od značaja privremenog karaktera na Linux-u - pokrenuti procesi i servisi.....	255
3.2.6. Podaci od značaja privremenog karaktera na Linux-u - otvoreni fajlovi.....	257
3.2.7. Podaci od značaja privremenog karaktera na Linux-u - interna tabela rutiranja i keš tablele.....	258
3.2.8. Podaci od značaja privremenog karaktera	

na Linux-u - učitani moduli u kernel LKM.....	260
3.2.9. Podaci od značaja privremenog karaktera na Linux-u - dump memorije i memorijskih procesa.....	261
3.2.10. Podaci od značaja privremenog karaktera na Linux-u - montirani fajl sistemi.....	264
3.2.11. Postojani podaci od značaja na Linux-u - verzija OS i nivo ažuriranosti paketa.....	265
3.2.12. Postojani podaci od značaja na Linux-u - vremenski pečati fajl sistema.....	266
3.2.13. Postojani podaci od značaja na Linux-u - checksum fajl sistema.....	268
3.2.14. Postojani podaci od značaja na Linux-u - ulogovani korisnici na sistem.....	269
3.2.15. Postojani podaci od značaja na Linux-u - istorija logovanja na Linux sistem.....	270
3.2.16. Postojani podaci od značaja na Linux-u - logovi na sistemu.....	271
3.2.17. Postojani podaci od značaja na Linux-u - TCP Wrappers.....	275
3.2.18. Postojani podaci od značaja na Linux-u - korisnički nalozi.....	276
3.2.19. Postojani podaci od značaja na Linux-u - korisnički fajl sa istorijom izvršenih komandi.....	277
3.2.20. Postojani podaci od značaja na Linux-u - fajlovi sa SUID, SGID, sticky bitovi i prava nad fajlovima.....	280
3.2.21. Postojani podaci od značaja na Linux-u - sumnjivi fajlovi.....	280
3.3. Softverski forenzički alati za inicijalni odgovor i alati za oporavak podataka i particija.....	281
3.3.1 Alati inicijalnog odgovora za Windows sisteme.....	281
3.3.2. Windows alati za oporavak podataka.....	286
3.3.3. Linux alati za inicijalni odgovor.....	295
3.3.4. Linux alati za oporavak podataka.....	297
3.3.5. Oporavak obrisanih Windows i Linux particija.....	297
3.4. Digitalno forenzički kompleti alata za Windows i Linux sisteme...	300
3.4.1. ENCASE forensic.....	301
3.4.2. ILOOK Investigator.....	303
3.4.3. The Sleuth kit, Autopsy forensic browser.....	304
3.4.4. AccessData Forensic Toolkit (FTK) i Ultimate Toolkit (UTK)...	306
3.4.5. Penguin Sleuth.....	307

3.4.6. The Coroner's Toolkit (TCT).....	309
3.4.7. Helix Live CD.....	309
3.4.8. Knoppix-STD 0.1.....	311
3.4.9. LiveWire Investigator.....	313
3.4.10. The ProDiscover Family.....	314
3.4.11. X-ways Forensics.....	315
4. DIGITALNA FORENZIKA I MERE ZAŠTITE	
U ORGANIZACIJAMA.....	317
4.1. Primeri ranjivosti i načini	
zlonamernog iskorišćavanja sistema.....	323
4.1.1. Opšte ranjivosti.....	324
4.1.2. Ranjivosti na Windows sistemima.....	336
4.1.3. Ranjivosti na Linux sistemima.....	344
4.2. Najčešći načini zlonamernog iskorišćavanja sistema.....	351
4.2.1 Upad na sistem sa ciljem dobijanja pristupa.....	351
4.2.2. Dobijanje privilegija na sistemu.....	355
4.2.3. Napadi sa ciljem onemogućavanja servisa.....	356
4.2.4. Napad tipa man-in-the middle.....	356
4.2.5 Rizici koje nosi korišćenje TOR mreže.....	356
4.3. Zaštita u okviru organizacije i odgovori na	
nedozvoljene ili incidentne aktivnosti.....	362
4.3.1. Detektovanje incidentnih odnosno	
nedozvoljenih aktivnosti.....	364
4.3.2. Indikatori incidentnih odnosno	
nedozvoljenih aktivnosti.....	372
4.3.3. Odluke koje se odnose na rešavanje	
incidentne odnosno nedozvoljene aktivnosti.....	373
4.3.4. Forenzički odgovor na incidentnu/nedozvoljenu aktivnost....	375
4.3.5. Politika bezbednosti.....	379
4.3.6. Formulisanje strategije odgovora.....	383
4.3.7. Nedostaci forenzičkog odgovora „uživo“	
i najčešće forenzičke greške.....	384
5. ZAKLJUČAK.....	387
6. REČNIK POJMOVA I IZRAZA.....	391
7. LITERATURA.....	401
8. BIOGRAFIJE AUTORA.....	415