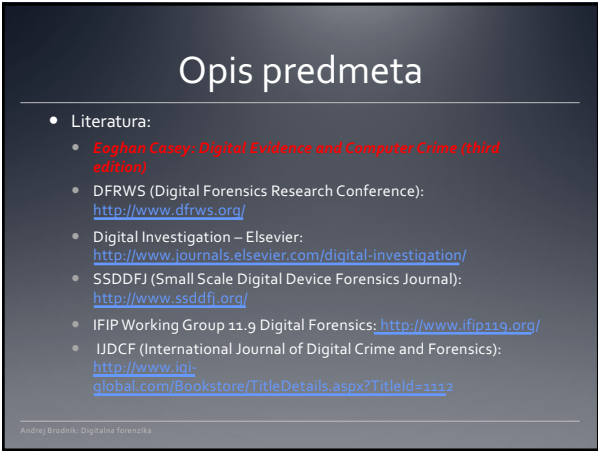




1



2



3

Opis predmeta – nadalj.

- predavanja: vključno z vsaj dvema vabljenima predavanjima
- domače naloge (DN):
 - štiri domače naloge iz vsebine predavanj (!), vaj in knjige
 - za pozitivno: vsaka naloga vsaj 20% in povprečje vsaj 40%
 - DNo in DNn
- laboratorijski nalogi (LN):
 - dve praktični laboratorijski nalogi
 - nalogi postavljeni v učilnici, kamor se tudi oddaja rezultate
 - za pozitivno: vsaka vsaj 20% in povprečje vsaj 50%

Andraž Brodnik, Digitalna forenzika

4

Opis predmeta – nadalj.

- seminarska naloga (SN):
 - Skupina (do trije) bo morala prebrati: znanstveni članek izkonference ali revije, knjige, orodja ali podobno
 - predstavitev (20 minut) in pisni izdelek, ki ga kolegi recenzirajo ter na koncu dokončni izdelek
 - časovni raspored:
 - do 27.2. izbira skupine; do 6.3. vsaka skupina odda predlog teme svoje seminarske naloge, ki se jo potrdi oziroma zavrne vendar najkasneje do 13.3. potrdi;
 - do 18.5. oddana predstavitev; do 8.5. oddana seminarska; do 22.5. recenzija; do 30.5. dokončno besedilo;
 - v maju in juniju predstavitve seminarskih nalog
 - za pozitivno: oddani vsi izdelki in vsaj 40% iz predstavitve ter 40% iz končnega pisnega izdelka ter vsaj 50% iz skupne ocene seminarske naloge

Andraž Brodnik, Digitalna forenzika

5

Opis predmeta – nadalj.

- pisni izpit (PI):
 - samo en pisni izpit in to sredi leta (predvidoma 5. 5.)
 - za pozitivno: vsaj 50%
- skupna ocen predmeta:

$$\frac{1}{3} * PI + \frac{1}{3} * SN + \frac{1}{3} * (\frac{1}{2} * LN + \frac{1}{2} * DN)$$

Andraž Brodnik, Digitalna forenzika

6

Okvirni program

- Uvod in osnove
- Računalniki – strojna oprema
- Operacijski sistemi (MS Windows, Unix/Linux)
- Računalniška omrežja
- Mobilne naprave
- Digitalna forenzika slik
- Zbiranje informacij odprtega tipa in človeški vektorji napada
- Izvajanje digitalne preiskave
- Varstvo pravice do zasebnosti v kazenskem postopku

slike na prosojnicah so iz knjige © 2011: Eoghan Casey: Digital Evidence and Computer Crime (third edition)

Andraž Brodnik, Digitalna forenzika

7

Okvirni program – nadalj.

- vabljeni predavanja:
 - Digitalna forenzika v detektivski agenciji
 - Digitalna forenzika omrežij (SI-CERT)

Andraž Brodnik, Digitalna forenzika

8

Razpored predavanj in vaj

teden	predavanja		E. Casey: Digital Evidence and Computer Crime
1	14.02.22	Uvod in osnove	Introduction and basics
2	21.02.22	Računalnik, operacijski sistem MS Windows	Computer and operating system MS Windows
3	28.02.22	Operacijski sistem Unix	Operating system Unix
4	07.03.22	Računalniška omrežja	Computer networks
5	14.03.22	Mobilne naprave	Mobile devices
6	21.03.22	Digitalna forenzika slik	Digital forensics of images
7	28.03.22	Zbiranje informacij odprtega tipa in človeški vektorji napada	Open source intelligence gathering (OSINT) and human attack vectors
8	04.04.22	Varstvo pravice do zasebnosti v kazenskem postopku	Protection of the right to privacy in criminal procedure
9	11.04.22	Izvajanje digitalne preiskave	Execution of a digital investigation
10	18.04.22	praznik	Holiday
11	25.04.22	Vabljeno predavanje / Digitalna forenzika mrežnih napadov	Invited lecture
12	02.05.22	izpit	exam
13	09.05.22	Vabljeno predavanje / Preiskovalno delo zasebnega detektiva in digitalna forenzika	Invited lecture
14	16.05.22	predstavitve seminarskih nalog	presentation of seminars
15	23.05.22		
16	30.05.22		

Andraž Brodnik, Digitalna forenzika

9

Razpored predavanj in vaj

teden	vaje	DN
1	14.02.22	
2	21.02.22	Predstavitve predmeta, 1. laboratorijska. 1
3	28.02.22	Osnovni ukazi (ls, grep, mount, ps, md5sum)
4	07.03.22	lso, hdd dump, dostop do particij, LVM, RAID, Fsc, fuse, mkisofs,
5	14.03.22	Analiza metapodatkov v slikah 2
6	21.03.22	Windows registry, ReactOS
7	28.03.22	Windows kraja ključev
8	04.04.22	Syslog, linux init sistemi, keylogger
9	11.04.22	Sqlite, Zgodovina v brskalnikih, cache, db 3
10	18.04.22	<i>prazniki</i>
11	25.04.22	Podatki na mobilni telefonu – android
12	02.05.22	Buffer overflow 1
13	09.05.22	Metasploit 4
14	16.05.22	Analiza podatkov v pomnilniku
15	23.05.22	Steganografija
16	30.05.22	

Andrej Brodnik - Digitalna forenzika

10

Razpored predavanj in vaj

teden	laboratorij	seminarske
2	21.02.22	27.02.22 izbira skupine
3	28.02.22	06.03.22 predizbira teme
4	07.03.22	13.03.22 izbira teme
5	14.03.22	
6	21.03.22	
7	28.03.22	
8	04.04.22	LAB1
9	11.04.22	
10	18.04.22	
11	25.04.22	
12	02.05.22	08.05.22 seminarska
13	09.05.22	
14	16.05.22	18.05.22 predstavitev
15	23.05.22	LAB2 22.05.22 recenziji
16	30.05.22	LAB3 30.05.22 končni izdelek

Andrej Brodnik - Digitalna forenzika

11

Uvod in osnove

poglavja 1 – 5

Andrej Brodnik - Digitalna forenzika

12

Osnove digitalne forenzike

poglavje 1

- Kaj je digitalni dokaz?
 - Digitalni dokaz je katerikoli digitalni podatek, ki je shranjen ali prenešen in omogoča dokaz ali zanikanje [kriminalnega] dejanja.
- Kaj je to računalniški sistem?
 - odprti računalniški sistemi
 - komunikacijski sistemi
 - vgrajeni sistemi

Andraž Brodnik: Digitalna forenzika

13

Osnove digitalne forenzike

- za izvajanje forenzične preiskave ni dovolj znanje, ampak se zahteva certificiranost osebja, organizacije, laboratorija, ...

Andraž Brodnik: Digitalna forenzika

14

Principi digitalne forenzike

- uporaba znanosti za potrebe prava
- pomen razlikovanja gotovosti in verjetnosti:

Neobstoje dokaza ni dokaz o neobstoju!

- priprava in hranjenje gradiva za morebitni sodni spor

Andraž Brodnik: Digitalna forenzika

15

Izmenjava dokaza

- prstni odtisi (na tipkovnici)
- e-pošta in zabeležke
- zabeležke o obiskovanih straneh
- komunikacijske sledi
- ...

Izmenjava dokaznega gradiva med žrtvijo in storilcem (ali prizoriščem)
Locardov princip izmenjave

Andraj Brodnik: Digitalna forenzika

16

Dokazi

- dokazi imajo skupne lastnosti (vsi programi te vrste) in posebne lastnosti (konkretne nastavitve)
- da je digitalni dokaz sprejemljiv na sodišču:
 - mora biti pravilno obdelan (zajet) in
 - mora biti hranjen na forenzično pravičen način
- zato je potrebno beležiti vse akcije na prizorišču

Andraj Brodnik: Digitalna forenzika

17

Dokazi

- zagotavljanje avtentičnosti:
 1. vsebina mora biti nespremenjena
 2. vsebina mora izvirati s prizorišča (beleženje vrstnega reda posedovanja dokaza – dokazna veriga)
 3. dodatne informacije o rokovanju z dokazi

cmfLabs Continuity of Possession Form			
Case Number:	2010-05-27-00X	Client/Case Name:	DigiFinger Intrusion
Evidence Type:	hard drive	Evidence Number:	0023
Details: Mac storage <network share>			
Date of Transfer:	Transferred From:	Transferred To:	Location of Transfer:
5/27/10	Sam Spade	Philip Mendonca	DigiFinger HQ
			Libtiscourt MD
			Action Taken by Recipient:
			Collected evidence for examination

Andraj Brodnik: Digitalna forenzika

18

Celovitost dokaza

- sprejeta oblika zagotavljanja celovitosti dokaza je podpisovanje z razpršilno funkcijo
 - MD5, SHA-1, ...

File 1
File 1 (copy)
File 2

MD5

Message Digest 1
Message Digest 2

Andraž Brodnik, Digitalna forenzika

19

Ravnanje z dokazi

- objektivnost dokaza
 - vsebuje interpretacijo in predstavitev dokaza
- ponovljivost analize dokaza

Andraž Brodnik, Digitalna forenzika

20

Izzivi rokovanja z digitalnimi dokazi

- ostanki ali rekonstrukcija ni isto kot celotno gradivo:
 - rekonstruirana datoteka, ki je bila izbrisana, ni isto kot delčki le-te
 - ostanki poslane e-pošte ni isto kot celotna e-pošta
- povezava med (digitalnim) dokazom in storilcem ni vedno očitna
- podatki niso večni
 - podatki o prometu na omrežju

Andraž Brodnik, Digitalna forenzika

21

Izzivi rokovanja z digitalnimi dokazi

- dokazi niso nujno brez napak
 - administrator je že bil poskušal rešiti pobrisano datoteko
 - sistemski administrator je spremenil vsebino, da bi zavaroval sistem
 - prišlo je do napake pri zajemu podatkov (nestandardni postopek)
 - pri zajemu podatkov je bil uporabljen okužen medij
 - medij s shranjenimi podatki se je poškodoval
 - ...

Andraž Brodnik: Digitalna forenzika

22

Digitalni svet ni ločen od realnega

- primer: kupec je preko eBay kupil dobrino
 - *case example: Auction Fraud, 2000; str. 29*
- podatki lahko pridejo iz povsem nepričakovanih mest

The Living Classroom 0° [N] WEATHER
Baltimore, MD 21231



BLGMR 05/27/2010 03:35

Andraž Brodnik: Digitalna forenzika

23

Razvoj jezika raziskave računalniških zločinov

poglavje 2

- na začetku ni bilo računalnikov in zakon je ščitil samo materialne dokaze
- digitalni dokazi vključujejo:
 - računalniška (datotečna) forenzika
 - omrežna forenzika
 - mobilna forenzika
 - slabogramje (*malware*) forenzika
- pomembna razlika med preiskovanjem in analizo podatkov
 - preiskovanje vključuje zajem, organizacijo, ...
 - analiza predstavlja dejansko obravnavo dokazov

Andraž Brodnik: Digitalna forenzika

24

Vloga računalnika

Po Parkerju, 1976, 1983, 1998:

1. predmet (objekt) zločina
 - kraja računalnika ali uničenje
 2. osebek (subjekt) zločina – zločin je bil narejen nad računalnikom
 - okužba računalnika
 3. orodje za pripravo in/ali izvedbo zločina
 - kopiranje dokumentov
 4. uporaba po svojih lastnostih v zločinu (*symbol*)
 - ponujanje storitev ali zmožnosti računalniških storitev: dobitki na borzi, ...
- vir podatkov(!!) – ostanki datotek, e-pošte, ...

Andraž Brodnik, Digitalna forenzika

25

Vloga računalnika

USDOJ (*US Department of Justice*), 1994, 1998:

- strojna oprema kot predmet ali rezultat zločina
- strojna oprema kot instrument
- strojna oprema kot dokaz
- informacija kot predmet ali rezultat zločina
- informacija kot instrument
- informacija kot dokaz

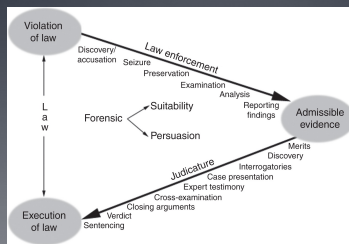
Andraž Brodnik, Digitalna forenzika

26

Digitalni dokaz na sodišču

poglavje 3

digitalni dokaz na sodišču



Andraž Brodnik, Digitalna forenzika

27

Naloge izvedenca

- predstavitev dokaznega gradiva:
 - ne podleči vplivom
 - odklanjati prezgodaj postavljanje teorije
 - raba znanstvene resnice za potrebe pravnega procesa
- ACM Code of ethics
- IEEE Code of ethics

Andraž Brodnik: Digitalna forenzika

28

Sprejemljivost gradiva

- pet osnovnih pravil:
 1. relevantnost gradiva za primer
 2. avtentičnost gradiva (*zajem, sledljivost, ...*)
 3. niso govorice (*dokaz sam niso govorice, če ni govorec prisoten*)
 4. najboljši možen dokaz (*original in kopija*)
 5. dokazno gradivo brez potrebe ne napeljuje na zaključke
- nalog za preiskavo

Andraž Brodnik: Digitalna forenzika

29

Stopnje zanesljivosti

- v beležkah imamo zapis:


```
2009-04-03 02:28:10 W3SVC1 10.10.10.50 GET
/images/snakeoil113.jpg-80-192.168.1.1
Mozilla/4.0+(compatible;+MSIE+6.0;Windows+NT+5.1) 200
0 0
```
- kaj sklepamo iz njega?
- stopnje zanesljivosti:
 - (1) skoraj zagotovo; (2) zelo verjetno; (3) verjetno; (4) zelo možno; (5) možno
 - statistična verjetnost

Andraž Brodnik: Digitalna forenzika

30

Računalniška zakonodaja

poglavje 4

- zakonodaja ZDA
 - 50 zakonodaj
 - zakonodaja Washington DC
 - zvezna zakonodaja

Andraž Brodnik: Digitalna forenzika

31

Računalniška zakonodaja

poglavje 5

- zakonodaja ES (EU)
 - Irska (in Velika Britanija) ločen sistem – *common law*
 - preostale države – *civil law*
- skupna zakonodaja:
 - parlament EU
 - Konvencija o računalniških zločinih (*Convention on Cybercrime*), 1. julij 2004
 - nista ratificirali Irska (in Velika Britanija)
 - Protokol o dejanjih rasizma in ksenofobije, 1. marec 2006
 - GDPR, 2019

Andraž Brodnik: Digitalna forenzika

32

Zločini nad integriteto računalnika

- Dostop do računalnika ni dovoljen, če nam tega ne dovoli lastnik
- Primeri:
 - hekerji
 - kraja podatkov
 - prestrezanje podatkov
 - vplivanje na podatke in/ali sisteme (DOS, virusi)
 - »napačna« ali nenamenska uporaba enote/naprave

Andraž Brodnik: Digitalna forenzika

33

Zločini s pomočjo računalnika

- ponarejanje
- goljufija
- zloraba

Andrej Brodnik: Digitalna forenzika

34

Zločini povezani z vsebino podatkov

- Zločini, ki zadevajo vsebino podatkov
 - otroška pornografija
 - spletno zapeljevanje
 - rasizem in ksenofobija

Andrej Brodnik: Digitalna forenzika

35

Ostali zločini

- kršenje avtorskih pravic
- računalniško izsiljevanje
- ...

Andrej Brodnik: Digitalna forenzika

36
