

Digitalna forenzika

Andrej Brodnik

Digitalna forenzika

- predavanja: dr. Andrej Brodnik
- vaje: Aleks Huč, dr. Gašper Fele-Žorž
- e-viri: učilnica



FORUM

Opis predmeta

- Literatura:

- **Eoghan Casey: Digital Evidence and Computer Crime (third edition)**
- DFRWS (Digital Forensics Research Conference): <http://www.dfrws.org/>
- Digital Investigation – Elsevier: <http://www.journals.elsevier.com/digital-investigation/>
- SSDDFJ (Small Scale Digital Device Forensics Journal): <http://www.ssddfj.org/>
- IFIP Working Group 11.9 Digital Forensics: <http://www.ifip119.org/>
- IJDCF (International Journal of Digital Crime and Forensics): <http://www.igi-global.com/Bookstore/TitleDetails.aspx?TitleId=1112>

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%

Opis predmeta – nadalj.

• seminarska naloga (SN):

- Skupina (do trije) bo morala prebrati: znanstveni članek izkonference ali revije, knjige, orodja ali podobno
- predstavitve (20 minut) in pisni izdelek, ki ga kolegi recenzirajo ter na koncu dokončni izdelek

~~• časovni raspored:~~

- ~~• do 1.3. izbira skupine; do 8. 3. vsaka skupina odda predlog teme svoje seminarske naloge, ki se jo potrdi oziroma zavrne vendar najkasneje do 15. 3. potrdi;~~
- ~~• do 19.5. oddana predstavitve; do 3.5. oddana seminarska; do 17.5. recenzija; do 1.6. 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~~

Opis predmeta – nadalj.

- pisni izpit (PI):

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

6,5

- skupna ocen predmeta:

$$\left[\frac{1}{3} * PI + \frac{1}{3} * SN + \frac{1}{3} * \left(\frac{1}{2} * LN + \frac{1}{2} * DN \right) \right] / 10$$






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 cloveski 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)***

Okvirni program – nadalj.

- vabljeni predavanja:

- Digitalna forenzika v Policiji (Policija) 
- Digitalna forenzika v detektivski agenciji 
- Varovanje osebnih podatkov (Informacijska pooblaščenka)
- Digitalna forenzika omrežij (SI-CERT) 

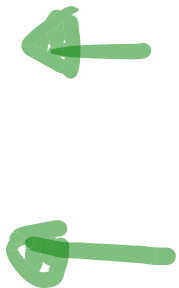
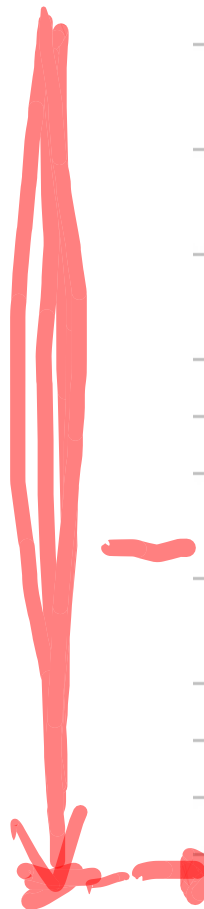
 V A Š A P R E D S T A V I T V E

Razpored predavanj in vaj

	<u>teden</u>	<u>predavanja</u>	E. Casey: Digital Evidence and Computer Crime
1	15.02.21	<u>Uvod in osnove</u>	1, 2, 3, 4, 5
2	22.02.21	<u>Računalnik, operacijski sistem MS Windows</u>	15, 17
3	01.03.21	<u>Operacijski sistem Unix</u>	18
4	08.03.21	<u>Računalniška omrežja</u>	21
5	15.03.21	<u>Mobilne naprave</u>	20
6	22.03.21	<u>Digitalna forenzika slik</u>	
7	29.03.21	<u>Zbiranje informacij odprtega tipa in človeški vektorji napada</u>	
8	05.04.21	<u>Varstvo pravice do zasebnosti v kazenskem postopku</u>	
9	12.04.21	<u>Izvajanje digitalne preiskave</u>	6, 7
10	19.04.21	<u>Vabljeni predavanje</u>	
11	26.04.21	<u>Vabljeni predavanje</u>	
12	03.05.21	izpit	
13	10.05.21	<u>Vabljeni predavanje</u>	
14	17.05.21	<u>predstavitve seminarских nalog</u>	
15	24.05.21		
16	31.05.21		

	teden	vaje	DN
1	15.02.21		
2	22.02.21		
		Predstavitev predmeta, 1. laboratorijska.	
3	01.03.21		
		Osnovni ukazi (ls, grep, mount, ps, md5sum)	
4	08.03.21	Iso, hdd dump, dostop do particij, LVM, RAID, Fscck, fuse, mkisofs,	1
5	15.03.21	Analiza metapodatkov v slikah	
6	22.03.21	Windows registry, ReactOS	
7	29.03.21		
		Windows kraja ključev	
8	05.04.21		2
		Syslog, linux init sistemi, keylogger	
9	12.04.21	Sqlite, Zgodovina v brskalnikih, cache, db	
10	19.04.21		
			<i>prazniki</i>
11	26.04.21	Podatki na mobitelu – android	
12	03.05.21	Buffer overflow 1	3
13	10.05.21	Metasploit	
14	17.05.21	Analiza podatkov v pomnilniku	
15	24.05.21	Steganografija	
16	31.05.21		4

	teden	laboratorij	seminarske	
1	15.02.21			
2	22.02.21		28.02.21	izbira skupine
3	01.03.21		07.03.21	predizbira teme
4	08.03.21		14.03.21	izbira teme
5	15.03.21			
6	22.03.21			
7	29.03.21			
8	05.04.21	LAB1		
9	12.04.21			
10	19.04.21			
11	26.04.21			
12	03.05.21		09.05.21	seminarska
13	10.05.21			
14	17.05.21		19.05.21	predstavitev
15	24.05.21	LAB2	23.05.21	recenziji
16	31.05.21	LAB3	31.05.21	končni izdelek



EAS & CHAIR

Uvod in osnove

poglavja 1 – 5

"COMPUTERS"

DIGITAL FORENSICS

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

Osnove digitalne forenzike

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

UL FRI

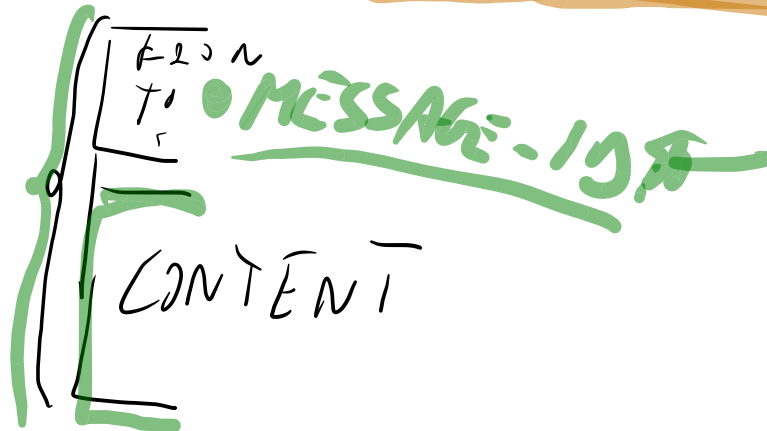
Principi digitalne forenzike

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

Neobstoja dokaza ni dokaz o neobstoju!

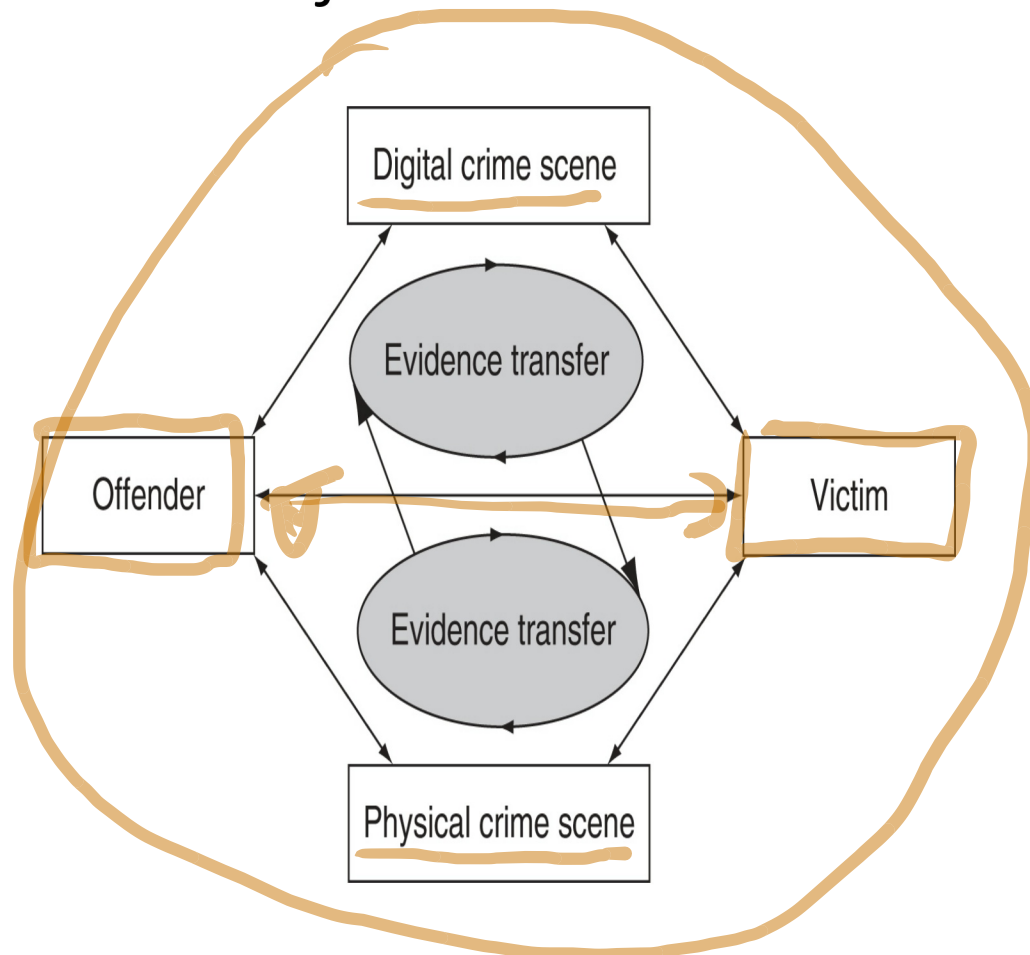
- priprava in hranjenje gradiva za morebitni sodni spor

e-mail:



10%
possi/probleq

Izmenjava dokaza



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

Izmenjava dokaznega gradiva med žrtvijo in storilcem (ali prizoriščem)

Locardov princip izmenjave

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 ~~zajet~~
 - mora biti hranjen na forenzično pravilen način
- zato je potrebno beležiti vse akcije na prizorišču

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

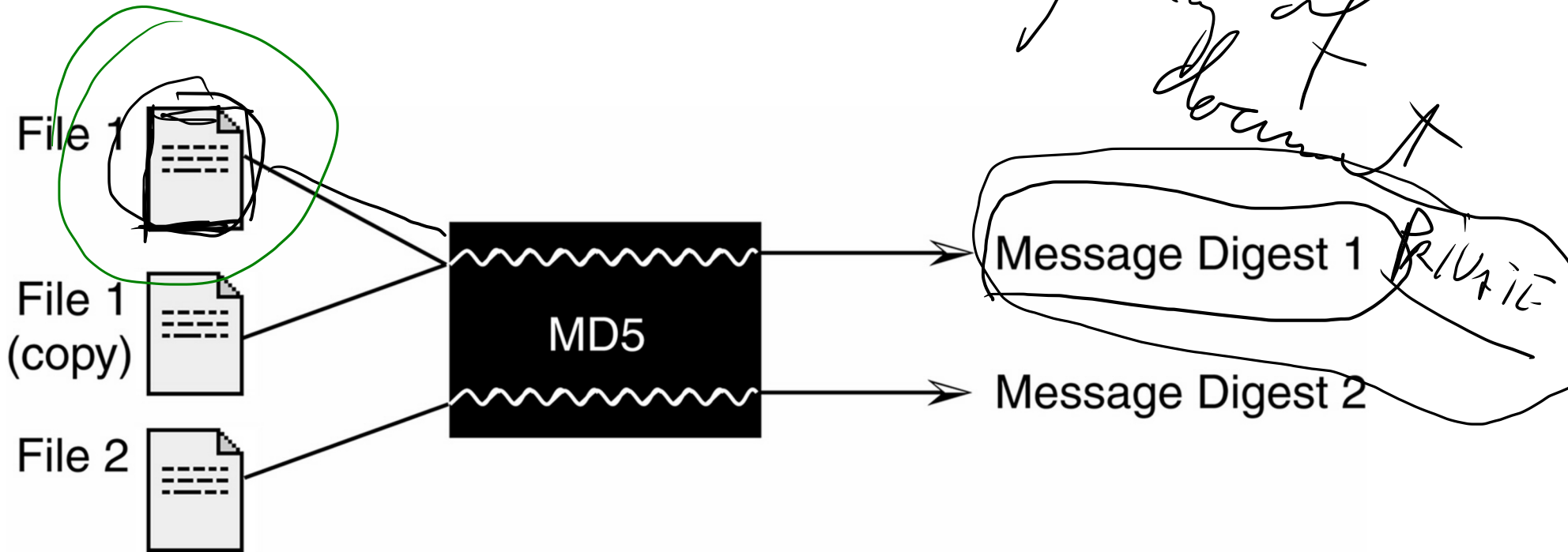
cmdLabs Continuity of Possession Form				
Case Number:	2010-05-27-00X		Client/Case Name:	Digifinger intrusion
Evidence Type:	hard drive		Evidence Number:	0023
Details:	<u>Mac storage <network share></u>			
Date of Transfer	Transferred From	Transferred To	Location of Transfer	Action Taken by Recipient
5/27/10	<small>signature</small> [Signature] <small>print name</small> Sam Spade	<small>signature</small> [Signature] <small>print name</small> Philip Marlowe	Digifinger HQ Linthicum MD	Collected evidence for examination
	<small>signature</small> <small>print name</small>	<small>signature</small> <small>print name</small>		

Celovitost dokaza

Integrity proof

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

Signing of document



Ravnanje z dokazi

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

Izzivi rokovanja z digitalnimi dokazi

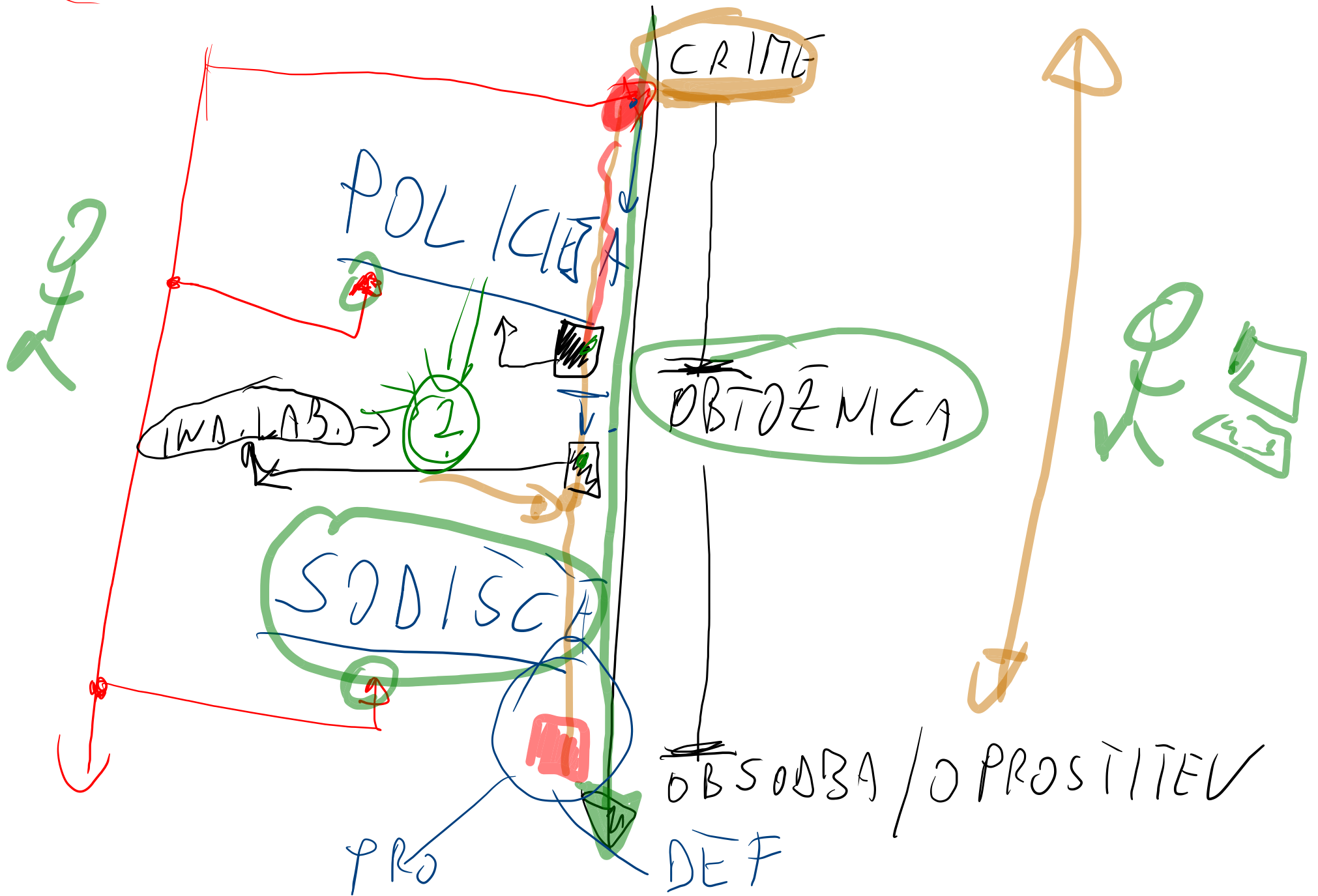
- ostanki ali rekonstrukcija ni isto kot celotno gradivo:
 - rekonstruirana datoteka, ki je bila izbrisana, ni isto kot delčki le-te
 - ostanki poslane e-pošte ni isto kot celotna e-pošta
- povezava med (digitalnim) dokazom in storilcem ni vedno očitna
- podatki niso večni
 - podatki o prometu na omrežju

CONSTR
E-MAIL

Quick collect

foren 214

time



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
- ...

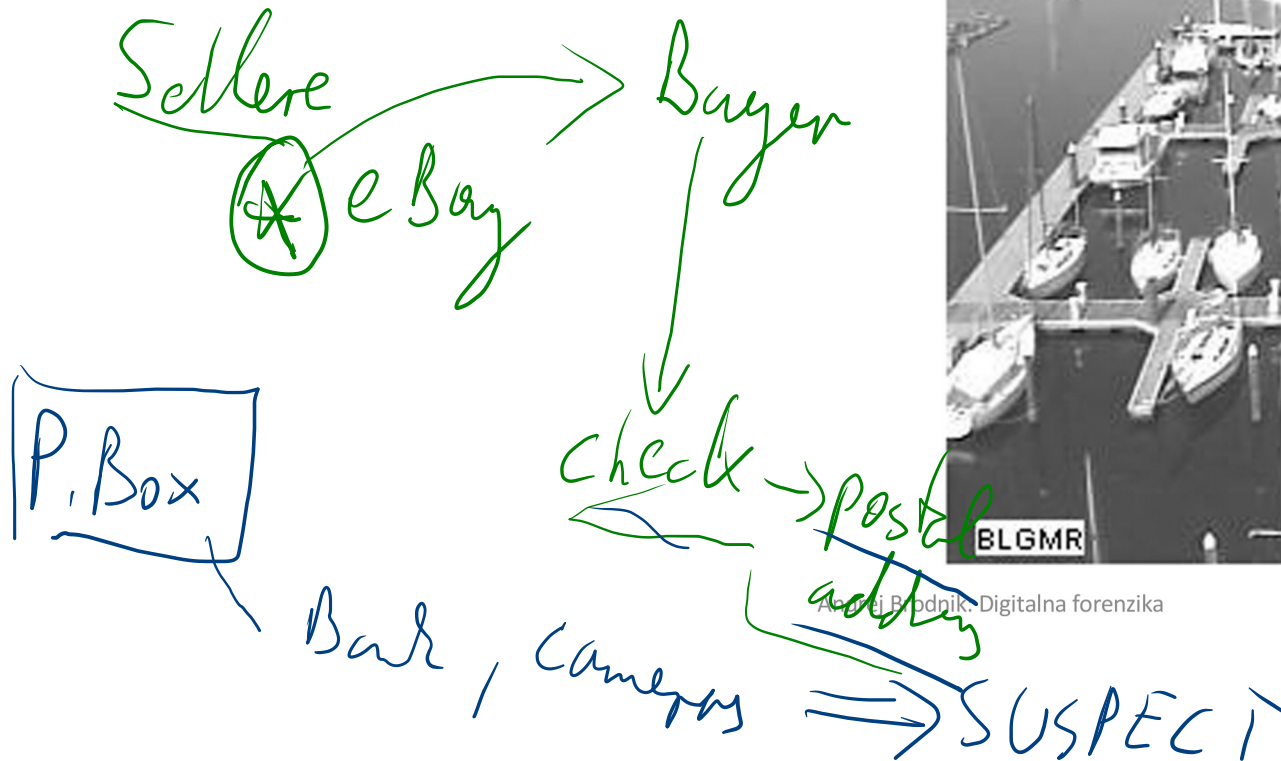
PROFESSIONAL QUALITY

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
Baltimore, MD 21231

0° [N]
WEATHER



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

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, ...

Vloga računalnika

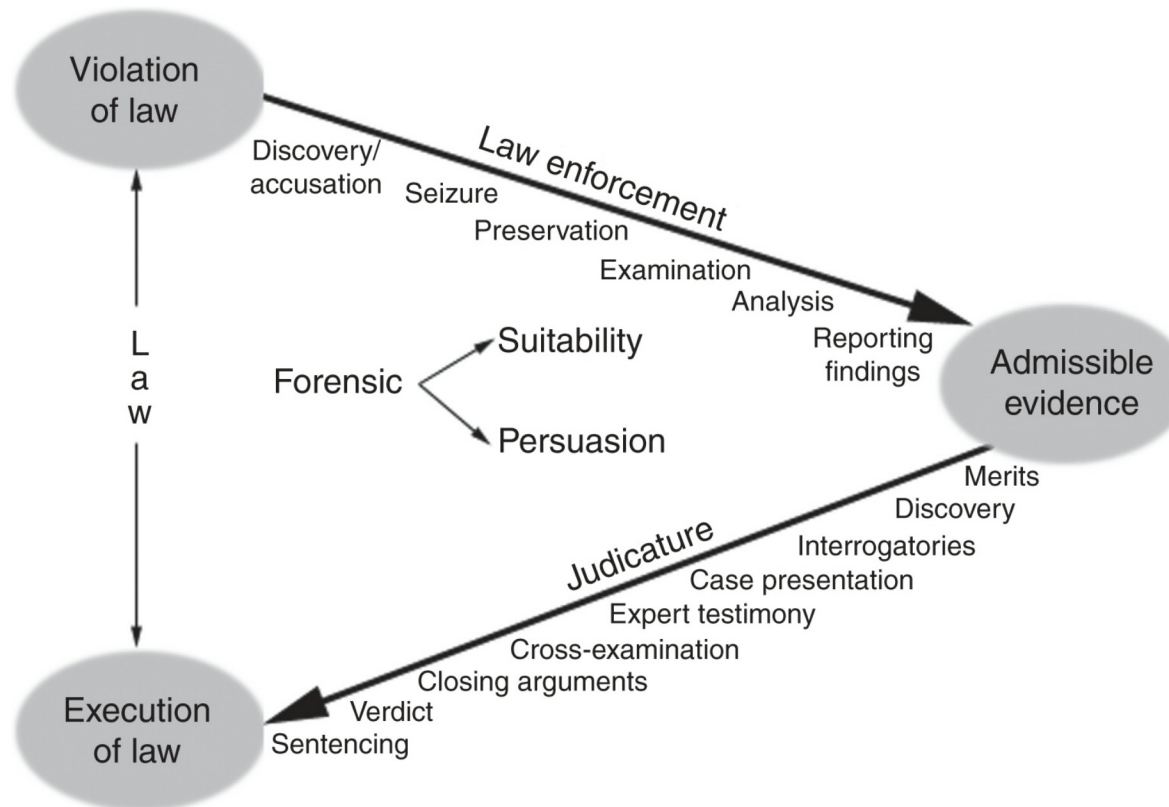
USDOJ (*US Department of Justice*), 1994, 1998:

- 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

Digitalni dokaz na sodišču

poglavje 3

digitalni dokaz na sodišču



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

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

Stopnje zanesljivosti

- v beležkah imamo zapis:

```
2009-04-03 02:28:10 W3SVC1 10.10.10.50 GET  
/images/snakeoil13.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

Računalniška zakonodaja

poglavje 4

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

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

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

Zločini s pomočjo računalnika

- ponarejanje
- goljufija
- zloraba

Zločini povezani z vsebino podatkov

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

Ostali zločini

- kršenje avtorskih pravic
- računalniško izsiljevanje
- ...