# Digitalna forenzika

Andrej Brodnik



## Digitalna forenzika

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



## 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
  - naloge v učilnici
  - oddati PDF datoteko
  - *za pozitivno: vsaka naloga vsaj 20% in povprečje vsaj 40%*
- 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 bo morala prebrati: znanstveni članek iz revije ali konference, knjige, orodja ali podobno
  - predstavitev (20 minut) in pisni izdelek, ki ga kolegi recenzirajo ter na koncu dokončni izdelek
  - časovni razpored:
    - do 7.3. izbira skupine; do 14. 3. vsaka skupina odda predlog teme svoje seminarske naloge, ki se jo potrdi oziroma zavrne vendar najkasneje do 21. 3. potrdi;
    - do 2.5. oddana predstavitev; do 9.5. oddana seminarska; do 23.5. recenzija; do 6.6. 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 v tednu 2. 5.)
  - *za pozitivno: vsaj 50%*
- skupna ocen predmeta:

$$1/3 * PI + 1/3 * SN + 1/3 * (½ * LN + ½ * DN)$$

## Okvirni program

- Uvod in osnove
- Preiskava elektronske naprave z uvodom v kazenski postopek
- Računalniki – strojna oprema
- Operacijski sistemi (MS Windows, Unix/Linux)
- Računalniška omrežja
- Mobilne naprave
- Izvajanje digitalne preiskave
- Digitalna forenzika slik

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



## Okvirni program – nadlj.

- vabljena predavanja:
  - Digitalna forenzika v Policiji (Policija)
  - Varovanje osebnih podatkov (Informacijska pooblaščenka)
  - Digitalna forenzika omrežij (SI-CERT)



## Uvod in osnove

poglavja 1 – 5

## 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, ...



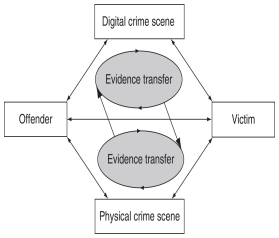
## Principi digitalne forenzike

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

**Neobstoj dokaza ni dokaz o neobstoju!**

- priprava in hranjenje gradiva za morebitni sodni spor

## 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



## Dokazi

- dokazi imajo skupne lastnosti (vsi programi te vrste) in posebne lastnosti (konkretne nastavite)
- da je digitalni dokaz sprejemljiv na sodišču:
  - mora biti pravilno obdelan (zajet) in
  - 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

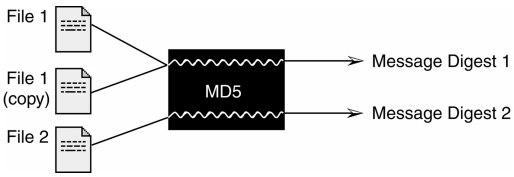
**cmdLabs**
Continuity of Possession Form

| Case Number: | 2010-05-27-00X | Client/Case Name: | Digifinger Intrusion |
|---|---|---|---|
| Evidence Type: | hard drive | Evidence Number: | 0023 |
| Details: | Mac storage <network share> | | |

| Date of Transfer | Transferred From | Transferred To | Location of Transfer | Action Taken by Recipient |
|---|---|---|---|---|
| 5/27/10 | Sam Spade | Philip Marlowe | Digifinger HQ Hunnicum MD | Collected evidence for examination |
| | | | | |

## Celovitost dokaza

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






## 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

## 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
  - ...



## 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




## 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:

1. predmet (objekt) zločina
   - kraja računalnika ali uničenje
2. osebek (subjekt) zločina – zločin je bil narejen s pomočjo računalnika
   - 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*):

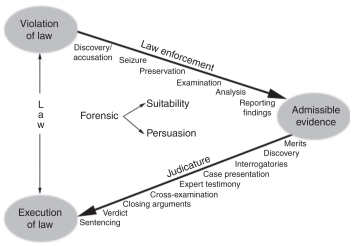
- strojna oprema kot predmet ali rezultat zločina
- strojna oprema kot instrument
- strojna oprema kot dokaz
- informacija kot predmet ali rezultat zločina
- informacija kot instrument
- informacija kot dokaz



## Digitalni dokaz na sodišču

*poglavje 3*

digitalni dokaz na sodišču



## Naloge izvedenca

- predstavitev dokaznega gradiva:
  - ne podleči vplivom
  - odklanjati prezgodaj postavljane 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 Washingon 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



## 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 s vsebino podatkov

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



## Ostali zločini

- kršenje avtorskih pravic
- računalniško izsiljevanje
- …