

Digitalna forenzika

Andrej Brodnik

Andrej Brodnik: Digitalna forenzika

---

---

---

---

---

---

---

---

Izvajanje digitalne preiskave

*poglavje 6*

- (digitalna) preiskava se izvaja po točno določenih korakih
- koraki so definirani v priročnikih, navodilih, ...

Andrej Brodnik: Digitalna forenzika

---

---

---

---

---

---

---

---

Koraki v digitalni preiskavi

1. *priprava*: priprava načrta preiskave
2. *pregled/identifikacija*: kaj je potrebno zajeti in kako
3. *shranjevanje*: forenzično korektno zajetega gradiva
4. *raziskava (examination) in analiza*: zajeto gradivo se ustrezno pripravi za analizo, ki temelji na ustreznih znanstvenih metodah
5. *predstavitve gradiva*: izsledke preiskave se ustrezno namenu predstavi (sodišče, v podjetju, vojska, ...)

Andrej Brodnik: Digitalna forenzika

---

---

---

---

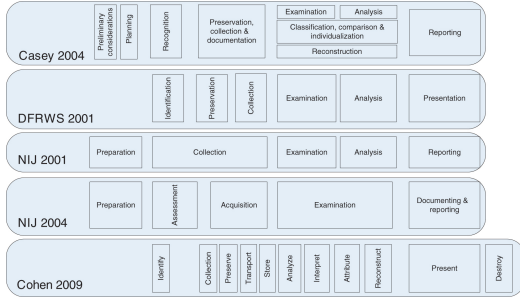
---

---

---

---

### Koraki v digitalni preiskavi



Andrej Brodnik, Digitalna forenzika

---

---

---

---

---

---

---

---

### Procesni modeli preiskave – fizični model

- model, ki izhaja iz klasičnega pristopa (Carrier, 2003)

	Phase Goals (Physical)	Phase Goals (Digital)
Crime scene preservation	Securing entrances and exits and preventing physical changes to evidence	[Redacted]
Crime scene survey	Walking through scene, identifying obvious and fragile physical evidence	
Crime scene documentation	Photographs, sketches, maps of evidence, and crime scene	
Crime scene search and collection	In-depth search for physical evidence	
Crime scene reconstruction	Developing theories based on analysis results and testing against evidence	

Andrej Brodnik, Digitalna forenzika

---

---

---

---

---

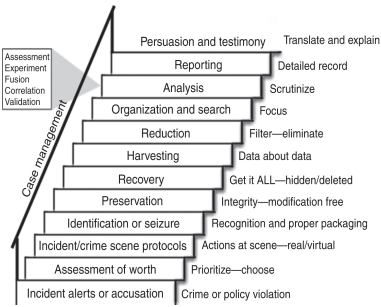
---

---

---

### Procesni modeli preiskave – stopničasti model

- Casey & Palmer, 2004
- odvetniki in preiskovalci delujejo skupaj
- ni enosmeren tok, ampak se lahko vračamo na prejšnje faze



Andrej Brodnik, Digitalna forenzika

---

---

---

---

---

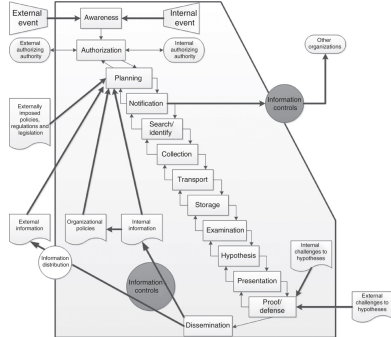
---

---

---

### Procesni modeli preiskave – model toka podatkov

- Ó Ciardhuáin, 2004
- celovit proces od zavarovanja do sodišča
- celotna veriga dogodkov




---

---

---

---

---

---

---

---

### Procesni modeli preiskave – (pod)fazni model

- Beebe & Clark, 2005
- proces je razdeljen na faze, od katerih ima vsaka točno določene cilje / namen
- osnovne faze so (prim. nazaj):
  1. priprava
  2. odziv na prijavo
  3. zbiranje gradiva
  4. analiza gradiva (podatkov)
  5. predstavitev izsledkov
  6. zaključek primera

Andrej Brodnik: Digitalna forenzika

---

---

---

---

---

---

---

---

### Procesni modeli preiskave – (pod)fazni model

- primer: cilji analize datotečnega sistema
 

1. zmanjšanje količine podatkov za analizo	9. pridobitev relevantne e-pošte s prilonkami
2. ocena znanja osumljenca	10. pridobitev relevantnih drugih podatkov (koledar, adresar, zaznamki, ...)
3. pridobitev izbranih datotek	11. iskanje natisnenih podatkov
4. iskanje relevantnih skritih podatkov	12. identifikacija relevantnega programja
5. ugotovitev zaporedja dejavnosti z datoteko	13. iskanje dokazil o neavtoriziranih dostopih ( <i>malware</i> )
6. pridobitev relevantnih ASCII podatkov	14. rekonstrukcija omrežnih dogodkov
7. pridobitev relevantnih ne-ASCII podatkov	
8. ocena spletne (e-pošta, brskanje) dejavnosti	

Andrej Brodnik: Digitalna forenzika

---

---

---

---

---

---

---

---

## Procesni modeli preiskave – model vlog in odgovornosti

- leong, 2006
- FORZA – vsak udeleženec ima določeno vlogo in dolžnosti v procesu

Table 2 – A high-level view of the FORZA framework

	Why (motivation)	What (data)	How (function)	Where (network)	Who (people)	When (time)
Case leader (conceptual investigation layer)	Investigation objectives	Event nature	Requested initial investigation	Investigation geography	Initial participants	Investigation timeline
System owner (if any) (conceptual layer)	Business objectives	Business and event nature	Business and system process model	Business geography	Organization and participants relationship	Business and incident timeline
Legal advisor (legal advisory layer)	Legal objectives	Legal background and preliminary issues	Legal procedures for further investigation	Legal geography	Legal entities and participants	Legal timeframe
Security/system architect/auditor (conceptual security layer)	System/security control objectives	System information and security control model	Security mechanisms	Security domain and network infrastructure	Core and security entity model	Security timing and sequencing
Digital forensic specialist (technical preparation layer)	Forensics investigation strategy objectives	Forensics data model	Forensics strategy design	Forensics data geography	Forensics entity model	Hypothetical forensics event timeline
Forensics investigator/system administrator/organizer (data acquisition layer)	Forensics acquisition objectives	On-site forensics data observation	Forensics acquisition/seizure procedures	Site network forensics data acquisition	Participants interviewing and hearing	Forensics acquisition timeline
Forensics investigator/forensics analyst (data analysis layer)	Forensics examination objectives	Event data reconstruction	Forensics analysis procedures	Network address extraction and analysis	Entity and evidence relationship analysis	Event timeline reconstruction
Legal prosecutor (legal presentation layer)	Legal presentation objectives	Legal presentation attributes	Legal presentation procedures	Legal jurisdiction location	Entities in litigation procedures	Timeline of the entire event for presentation

Andrej Brodnik, Digitalna forenzika

---

---

---

---

---

---

---

---

---

---

---

## Zbiranje podatkov

- začetna točka je obtožba ali obvestilo o dogodku
- sledi avtorizacija za izvedbo preiskave
  - avtorizacija na podlagi napotila
  - (sodni) nalog za preiskavo
- triaža primera – odločitev, ali so dokazi zadovoljivi
- prenašanje in delo z dokaznim gradivom – dnevniški zapisi
- preverjanje zaseženega gradiva
- vodenje primera – vključuje ostale udeležence

Andrej Brodnik, Digitalna forenzika

---

---

---

---

---

---

---

---

---

---

---

## Metodologija dela v digitalni preiskavi

- delo mora sloneti na znanstvenih metodah
  - oblikovanje in preverjanje hipotez
- koraki:
  - priprava na digitalno preiskavo
  - pregled mesta zločina
  - shranjevanje podatkov
  - raziskovanje podatkov
  - analiza
  - poročanje in pričanje

Andrej Brodnik, Digitalna forenzika

---

---

---

---

---

---

---

---

---

---

---

### Znanstveni pristop

1. opazovanje (*brskalnik se je sesul in takoj za tem se je pognal antivirusni program*)
2. oblikovanje hipotez
3. prepostavka, kje so dokazi za potrditev hipotez
4. preverjanje hipotez
5. zaključek

Primer: zaposleni je obtožen kraje podatkov ob tem, ko je zapustil službo

Andrej Brodnik: Digitalna forenzika

---

---

---

---

---

---

---

---

- **Izziv:** zamislite si primer vključno z izvedbo zločina in ga zapišite v datoteko. Datoteka naj vsebuje tudi opis mesta nahajanja podatkov oziroma opis prizorišča. Na forum zapišite obtožbo in ostali naj raziskujejo primer. Delajte skupinsko!

Andrej Brodnik: Digitalna forenzika

---

---

---

---

---

---

---

---

### Priprava na digitalno preiskavo

1. *opazovanje:* število sistemov, kakšni so sistemi, ...
  2. *oblikovanje hipotez:* sistemi uporabljajo ATA in SATA diskovna vodila
  3. *preverjanje hipotez:* pregledovanje računalnikov
  4. *zaključek:* načrt kako natančno zajeti podatke vključno s potrebno opremo in postopki
- šele po zaključku lahko pričnemo z zbiranjem samega gradiva – *ad hoc* postopki niso zaželjeni

Andrej Brodnik: Digitalna forenzika

---

---

---

---

---

---

---

---

### Pregled mesta zločina

1. *opazovanje*: pregled mesta zločina
2. *oblikovanje hipotez*: nenavadnosti – zakaj nekaj manjka ali je nekaj prisotno; omejevanje količine gradiva
3. *prepostavka, kje so dokazi za potrditev hipotez*: hipoteza o pomembnosti podatka in nato predpostavka, kje se nahajajo dokazi
4. *preverjanje hipotez*: preverjanje hipoteze o relevantnosti podatka in njegovem mestu nahajanja
5. *zaključek*: zbiranje dokaznega gradiva se izvede

Andrej Brodnik: Digitalna forenzika

---

---

---

---

---

---

---

---

### Shranjevanje podatkov

- odvisno od oblike podatkov
  - primer: e-pošta je shranjena na strežniku vključno s 30 dnevnim arhivom
1. *opazovanje*: ...
  2. *oblikovanje hipotez*: ...
  3. *prepostavka, kje so dokazi za potrditev hipotez*: ...
  4. *preverjanje hipotez*: ...
  5. *zaključek*: ...

Andrej Brodnik: Digitalna forenzika

---

---

---

---

---

---

---

---

### Raziskovanje podatkov

- običajne faze:
  - pregled in triaža podatkov
  - predhodno raziskovanje
  - temeljito raziskovanje
- faze se seveda lahko ponovijo na istih podatkih
- vključuje: pripravo na raziskavo, ogled, forenzično raziskavo, pridobivanje podatkov, izločanje zanimivih podatkov, temeljita raziskava

Andrej Brodnik: Digitalna forenzika

---

---

---

---

---

---

---

---

### Raziskovanje podatkov

- primer:
- 1. *opazovanje*: trdi disk vsebuje obilico dokumentov, ki so zanimivi za raziskavo
- 2. *oblikovanje hipotez*: dokumenti so v .doc obliki
- 3. *prepostavka, kje so dokazi za potrditev hipotez*: če pridobimo vse .doc datoteke, bomo pridobili vse gradivo
- 4. *preverjanje hipotez*: pridobimo sicer vse .doc datoteke, a najdemo še .pdf in .tiff
- 5. *zaključek*: ko pridobimo vse dokumente smo naredili zaddovoljivo in celovito raziskavo

Andrej Brodnik: Digitalna forenzika

---

---

---

---

---

---

---

---

### Analiza

- dejansko znanstveno utemeljen odgovor na vprašanja ( $k^5z^1$ ): kdo, kaj, kje, kdaj, kako in zakaj
- upoštevamo, da imajo podatki vsebinsko in kontekstualno vrednost
- 1. *opazovanje*: osumljenec je bil zabeležen na kameri pri dvigu gotovine na avtomatu v bližini mesta zločina neposredno po zločinu. Zločinec je kmalu po zločinu dvignil denar z žrtvinega računa.
- 2. *oblikovanje hipotez*: ...
- 3. *prepostavka, kje so dokazi za potrditev hipotez*: ...
- 4. *preverjanje hipotez*: ...
- 5. *zaključek*: ...

Andrej Brodnik: Digitalna forenzika

---

---

---

---

---

---

---

---

### Poročanje in pričanje

- sodišče običajno ni izkušeno o strokovni materiji
- poročanje mora biti natančno in verodostojno ter transparentno
  - pri opisu postopkov
  - pri posredovanju zaključkov

Andrej Brodnik: Digitalna forenzika

---

---

---

---

---

---

---

---

- Izziv: primer v knjigi preberite in preučite podrobnosti postopka.  
*In this case, Jill observes unusually high numbers of failed logon attempts to a server that contains plans and details of Corporation X's newest product, code named Fastjet . She contacts the system administrator for the system and, after a quick review of recent system logs, he confirms that there has been unauthorized use of the administrator account on the system. There is a strong indication that a security breach has occurred.*  
 Komentarji na forum.

Andrej Brodnik: Digitalna forenzika

---

---

---

---

---

---

---

---

### Delo na mestu digitalnega zločina

- digitalni so dokazi, zločin je lahko povsem fizičen
- obstajajo priročniki, ki opisujejo postopke za delo na mestu zločina (ali za prikrito opazovanje)

Andrej Brodnik: Digitalna forenzika

---

---

---

---

---

---

---

---

### Delo na mestu digitalnega zločina

poglavje 7

- priročniki o ravnanju na mestu zločina:
  - *The Good Practice Guide for Computer Based Evidence, (ACPO guide, Association of Chief Police Officers)*
  - <http://www.afentis.com/forensic-science-articles/acpo-guide-electronic-evidence>
  - [http://7safe.com/electronic\\_evidence/index.html#](http://7safe.com/electronic_evidence/index.html#)

Andrej Brodnik: Digitalna forenzika

---

---

---

---

---

---

---

---



## Osnovni principi

1. z nobenim dejanjem se naj ne spreminjajo ali neposredno dostopamo do podatkov na napravi
2. če že dostopamo, potem moramo biti sposobni razumeti in predvideti posledice le-tega
3. obstajati mora zapis o vseh dejavnostih, ki jih mora biti tretja stran sposobna preveriti
4. vodja preiskave je odgovoren, da se zakon in ta pravila spoštujejo
  - primer: vključevanje naprave, ...

Andrej Brodnik: Digitalna forenzika

---

---

---

---

---

---

---

---

## Osnovni principi

The UK authorities, in consultation with industry experts, have created a 'GUIDE FOR COMPUTER BASED EVIDENCE' which defines minimum levels of standard for the preservation and analysis of electronic evidence exhibits. The ACPO Guide Electronic Evidence is built upon four (4) main principles:

- PRINCIPLE 1: No action taken by Police or their agents should change data held on a computer or other media which may subsequently be relied upon in Court;
- PRINCIPLE 2: In exceptional circumstances where a person finds it necessary to access original data held on a target computer that person must be competent to do so and to give evidence explaining the relevance and the implications of their actions;
- PRINCIPLE 3: An audit trail or other record of all processes applied to computer based evidence should be created and preserved. An independent third party should be able to examine those processes, assess an exhibit, and achieve the same result;
- PRINCIPLE 4: The Officer in charge of the case is responsible for ensuring that the law and these principles are adhered to. This applies to the possession of and access to, information contained in a computer.

[http://www.7safe.com/electronic\\_evidence/ACPO\\_guidelines\\_computer\\_evidence.pdf](http://www.7safe.com/electronic_evidence/ACPO_guidelines_computer_evidence.pdf)

Andrej Brodnik: Digitalna forenzika

---

---

---

---

---

---

---

---

## Avtorizacija za preiskavo

- raziskavo delamo po navodilu ali naročilu
  - sodišče, tožilstvo; vodja oddelka, ...
- navodilo ali naročilo mora natančno opredeljevati, kaj raziskujemo in katere podatke smemo zbrati
- primer:
  - preverite, ali je oseba A poslala e-pošto osebi B
  - to navodilo dovoljuje samo zbiranje podatkov o poslani pošti in ne zbiranje vsebine te pošte
  - podobno pri klicih (telefonskih, VoIP, ...)

Andrej Brodnik: Digitalna forenzika

---

---

---

---

---

---

---

---

### Avtorizacija za preiskavo

- sodišče (naredbodajalec) mora / naj bi skrbel za to, da se pri zbiranju podatkov ščiti zasebnost
- osumljenec ni kriv dokler ni pravnomočno obsojen
  - in še tedaj se mora spoštovati njegova zasebnost

Andrej Brodnik: Digitalna forenzika

---

---

---

---

---

---

---

---

### Priprava za delo na mestu digitalnega zločina

- pripravimo načrt dela na mestu zločina
- priprava je izredno pomembna, saj le ustrezna priprava lahko zaščiti dokazno gradivo

Andrej Brodnik: Digitalna forenzika

---

---

---

---

---

---

---

---

### Priprava za delo na mestu digitalnega zločina – ACPO priporočila

- upoštevanje tehničnega znanja osumljenca
- vključevanje ustreznih orodij in metod
- upoštevanje ranljivosti podatkov: brezžične in omrežne naprave, delujoče naprave (računalniki), ...



Andrej Brodnik: Digitalna forenzika

---

---

---

---

---

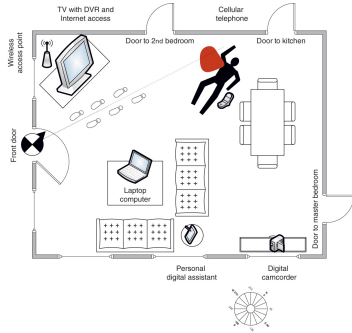
---

---

---

### Ogled mesta digitalnega zločina

- digitalni dokazi se lahko najdejo na različnih mestih – pomembna sistematičnost ogleda
- V/I enote, priročniki za strojno in programsko opremo, ...



Andrej Brodnik: Digitalna forenzika

---

---

---

---

---

---

---

---

### Ogled mesta digitalnega zločina

- izklop naprav
- zapis o izklopu naprave



Andrej Brodnik: Digitalna forenzika

---

---

---

---

---

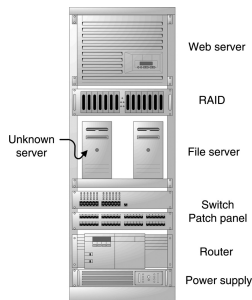
---

---

---

### Ogled mesta digitalnega zločina

- natančen popis naprav in njihova vloga
- gesla za dostop in za enkripcijo
- zapisovanje posegov v skladu z načrtom



Andrej Brodnik: Digitalna forenzika

---

---

---

---

---

---

---

---

### Zavarovanje mesta digitalnega zločina

- nadzor dostopov na mesto zločina:
  - video kamere ipd.: ugasniti sistem, da se ohranjajo podatki
  - (brezžična) omrežja: ugasniti oziroma odklopiti, da ne pride do nehotenega ali drugega dostopa
- zamrznitev mesta zločina
  - dokaze prepíšemo z ustreznimi napravami ter jih podpišemo in shranimo
  - zavarovanje oddaljenih podatkov
  - zavarovanje nedigitalnih dokazov (prstni ali drugi biološki dokazi)

Andrej Brodnik: Digitalna forenzika

---

---

---

---

---

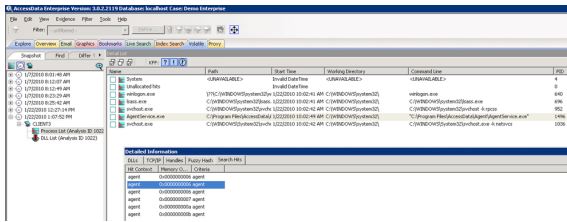
---

---

---

### Zavarovanje mesta digitalnega zločina

- priprava načrta za zavarovanje podatkov
- oddaljeno zavarovanje



Andrej Brodnik: Digitalna forenzika

---

---

---

---

---

---

---

---

### Zavarovanje mesta digitalnega zločina

- kaj pa pri delujočih napravah?
- običajno težko ohranimo vsebino glavnega pomnilnika (RAM)
- vendar:
  - trenutno izvajajoči procesi povedo kaj o vdoru v sistem
  - zakriptirani datotečni sistem je priklopljen in geslo vnešeno
  - odklenjeni dostopi do oddaljenih mest oziroma storitev
  - ...

Andrej Brodnik: Digitalna forenzika

---

---

---

---

---

---

---

---

