

# Digitalna forenzika

Andrej Brodnik

Andrej Brodnik: Digitalna forenzika

---

---

---

---

---

---

---

---

## Celični (mobilni) telefoni.

*poglavje 20*

- različne tehnologije prenosa podatkov
- včasih predvsem telefoni, danes predvsem računalniki
- bogat vir osebnih podatkov
  - zgodovina klicev (prihodnih, odhodnih in zgrešenih)
  - zgodovina sporočil SMS in MMS (prihodnih in odhodnih)
  - zgodovina podatkov o mestu nahajanja
  - slike, dnevniki, koledarji, ...
  - dostopi do spletnih omrežij – skratka takorekoč vsi podatki, ki se nahajajo tudi na običajnih računalnikih

Andrej Brodnik: Digitalna forenzika

---

---

---

---

---

---

---

---

## Podatki na celičnem telefonu

- Primer (POCKET-DIAL M FOR MURDER):  
*Starilec je imel v žepu telefon, ki je poklical ženin telefon med tem, ko je moril žrtev. Na ženini strani se je sprožila zapisovalna naprava (tajnica), ki je vse skupaj posnela.*
- telefoni postajajo sposobnejši, ker vsebujejo več V/I naprav
  - merilci temperature
  - pospeškometri
  - bralniki kreditnih kartic
  - ...
- uporaba enot je neizmerna; npr. pri določeni temperaturi se sproži akcija
- telefoni so postali celoviti vgrajeni sistemi (*embedded systems*)

Andrej Brodnik: Digitalna forenzika

---

---

---

---

---

---

---

---

### Forenzika mobilnih naprav.

- naprave imajo sposobnejše operacijske sisteme
  - Android
  - iPhone
  - Blackberry
  - Windows Mobile
- in starejše operacijske sistem (SYMBIAN, ...)

Andrej Brodnik: Digitalna forenzika

---

---

---

---

---

---

---

---

### Forenzika mobilnih naprav

- naprave so po definiciji omrežne naprave
  - GPRS, CDMA, UMTS, ...
  - IEEE 802.11
  - IEEE 802.15 (Bluetooth)
  - infrardeča komunikacija
  - ...
- dostop do naprave lahko uniči ali spremeni dokazno gradivo

Andrej Brodnik: Digitalna forenzika

---

---

---

---

---

---

---

---

### Forenzika mobilnih naprav

- podatki so običajno hranjeni v pomnilniških medijih
  - ki jih ni moč brisati, ampak prepisati
  - zaradi omejenega števila zapisovanj zapisovalni algoritmi razpršijo podatke po mediju
  - zato lahko pridobimo precej podatkov, za katere izgleda, kot da so izbrisani

Andrej Brodnik: Digitalna forenzika

---

---

---

---

---

---

---

---

### Forenzika mobilnih naprav

- zajem podatkov iz naprav
  - običajno preko podatkovnega kabla
    - potrebno poznavanje protokola
  - včasih je potreben neposreden zajem iz pomnilniškega medija
    - neposredno branje iz čipa

Andrej Brodnik: Digitalna forenzika

---

---

---

---

---

---

---

---

### Forenzika mobilnih naprav

- naprave sestojajo iz dveh delov
  - naprave kot takšne
  - SIM kartice
- naprava ima enoličen identifikator IMEI (*International Mobile Equipment Identity*)



Andrej

---

---

---

---

---

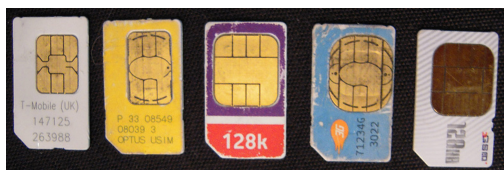
---

---

---

### Forenzika mobilnih naprav

- SIM kartice so računalniki
  - CPU, ROM, RAM
- vsebujejo ICC-ID (*Integrated Circuit Card Identifier*):
  - MCC (*mobile country code*),
  - MNC (*mobile network code*),
  - serijsko številko kartice



Andrej Brodnik: Digitalna forenzika

---

---

---

---

---

---

---

---

## SIM kartice

- Izziv: Katere podatke še vse vsebuje SIM kartica?
- Izziv: Kaj je to LAI in kaj je IMSI?
- Izziv: Kaj vsebuje vaša SIM kartica? Kakšne so vrednosti teh podatkov? Kakšna je identifikacija vaše mobilne naprave?

Andrej Brodnik, Digitalna forenzika

---

---

---

---

---

---

---

---

## Podatki o in na napravi.

- na napravi – odvisno od tipa naprave:
  - osnovni telefon
  - pametni telefon
- kje se še nahajajo podatki:
  - uporabnikov računalnik
  - operater
  - SIM kartica
- na napravi so shranjeni vsaj:
  - naslovi
  - prejeti, oddani in zgrešeni klici
  - prejeti in oddani SMS

Andrej Brodnik, Digitalna forenzika

---

---

---

---

---

---

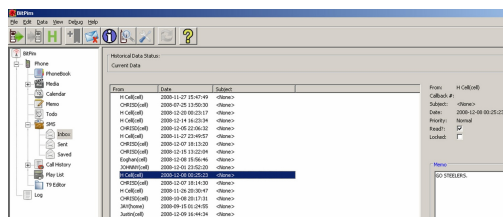
---

---

## SMS kot dokazno gradivo

- celovita informacija: kdaj poslano/prejeto od koga in vsebina
- ni podatka, kdaj prvič prebrano!

primer vpogleda z orodjem BitPim (<http://www.bitpim.org/>)



Andrej Brodnik, Digitalna forenzika

---

---

---

---

---

---

---

---

## Slikovno gradivo

- pametni telefoni imajo kamero
- slikovno gradivo v EXIF zapisu (običajno)  
primer vpogleda v Windows Mobile napravo z orodjem XRY (<http://www.msab.com/>)

Picture	Name	Size	MetaData	Path	Created
	IMAGE_002.jpg	155.85 KB	EquipMake: T-Mobile Dash EquipModel: T-Mobile Dash Resolution: 72 Resolution: 72 DataTime: 2009-04-22 16:47:2 DateTime: 2009-04-22 16:47:2 EquipMake: T-Mobile Dash EquipModel: T-Mobile Dash Resolution: 72	W:\Documents\My Pictures	4/22/2009 8:47:24 PM (LT)
	IMAGE_001.jpg	390.44 KB	EquipMake: T-Mobile Dash EquipModel: T-Mobile Dash Resolution: 72 Resolution: 72 DataTime: 2009-04-22 16:46:2 DateTime: 2009-04-22 16:46:2 EquipMake: T-Mobile Dash EquipModel: T-Mobile Dash Resolution: 72	W:\Documents\My Pictures	4/22/2009 8:46:24 PM (LT)

---

---

---

---

---

---

---

---

---

---

## Dostop do medmrežnih storitev

- mobilne naprave omogočajo dostop do spleta
  - pogosto uporabnik na njih hrani gesla
  - obstaja zgodovina dostopov
  - zabeležke zadnjih dostopov
  - ...
- mobilne naprave omogočajo branje pošte
  - gesla za dostop do nabiralnikov
  - zadnje prejete / poslane pošiljke
  - ...
- druge aplikacije in njihovi podatki

Andrej Brodnik, Digitalna forenzika

---

---

---

---

---

---

---

---

---

---

## Dostop do medmrežnih storitev

- primer podatkov na iPhone

```
F:\tools>sqlite3.exe "iPhone2\Keychains\keychain-2.db"
SQLite version 3.6.16
Enter ".help" for instructions
Enter SQL statements terminated with a ";"
sqlite> select labl,acct,svce from genp;
eric.rooster@yahoo.com|Yahoo-token
erooster@live.com|
erikroost@hotmail.com|
therooster@hotmail.com|
therooster@hotmail.com|com.apple.itunesstored.keychain
erooster|MMODBracketsAccount|
LumosityBrainTrainer|erooster|LumosityBrainTrainer
```

Andrej Brodnik, Digitalna forenzika

---

---

---

---

---

---

---

---

---

---



## Napadi na mobilne naprave

- napadelec naloži svojo kodo na napravo
  - preko omrežja
  - uporabnik naloži aplikacijo, ki sicer izgleda uporabna in prijazna ([http://www.theregister.co.uk/2010/01/11/android\\_phishing\\_app/](http://www.theregister.co.uk/2010/01/11/android_phishing_app/))
- aplikacija pobira gesla, ...
  - omogoči dostop napadalcu do bančnih računov ...
  - glej MobileSpy (<http://www.mobile-spy.com/>)



## Napadi na mobilne naprave

- **Izziv:** Kako deluje MobileSpy?
- **Izziv:** Najdite programje, ki vam lahko škoduje na Android sistemu?
- **Izziv:** Naredite svoj program, ki pobira podatke na Android (iPhone) sistemu. Je lahko to tudi uporabno programje?

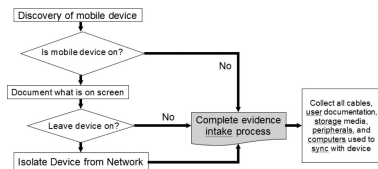
Andrej Brodnik: Digitalna forenzika

## Misli širše

- dodatni podatki:
  - uporabnikov računalnik
  - operater: klicni center in bazne postaje
- naprave, o katerih uporabnik nekaj ve (tranzitivnost)

### Rokovanje z napravo.

- naprava se lahko brezžično poveže s svetom
- onemogočiti
  - umakniti napajanje
  - drugi načini



Andrej Brodnik, Digitalna forenzika

---

---

---

---

---

---

---

---

### Rokovanje z napravo

- umakniti pomnilniške module
  - pomnilniški moduli so vedno manjši
- običajno FAT datotečni sistem
  - iPhone: APFS, Android: Linux zasnova
- sicer običajni postopki (podpis, dnevnik, ...)



Andrej Brodnik, Digitalna forenzika

---

---

---

---

---

---

---

---

### Pridobivanje podatkov.

- različni načini dostopa pri različnih modelih
  - nima vsaka naprava USB vodila
- primeri:
  - preko uporabniškega vmesnika
  - preko komunikacijskih vrat
  - notranjega vodila (Nokia F-BUS, Flash BUS)
  - preko JTAG (Joint Test Action Group) vmesnika
  - preko neposrednega dostopa do čipa

Andrej Brodnik, Digitalna forenzika

---

---

---

---

---

---

---

---



### Pridobivanje podatkov

- nekatere naprave omogočajo agentni dostop
  - ko se naprava zažene, se naloži naš agent, ki prevzame nadzor nad napravo (iPhone)
- včasih lahko prekinemo nalaganje programja in vsilimo našo kodo kot nadaljnje nalaganje
- proizvajalci nudijo programje za arhiviranje podatkov, ki omogoča tudi dostop do zbrisanih in ostalih podatkov

Andrej Brodnik, Digitalna forenzika

---

---

---

---

---

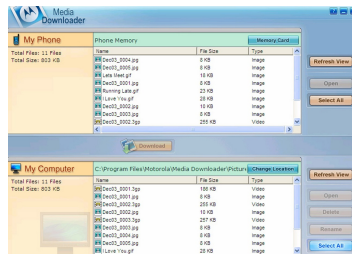
---

---

---

### Primeri ...

- primer analize shranjenih podatkov z arhivom z orodjem XACT (Motorolina naprava)



Andrej Brodnik, Digitalna forenzika

---

---

---

---

---

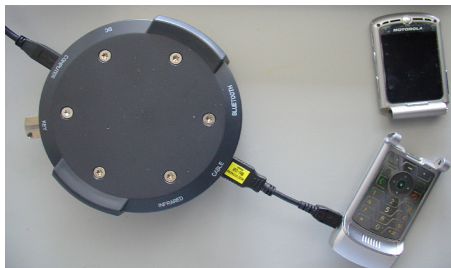
---

---

---

### Primeri ...

- naprava, ki je delno uničena, morda še vedno dovolj deluje



Andrej Brodnik, Digitalna forenzika

---

---

---

---

---

---

---

---

### Orodja za mobilne naprave

- katerokoli orodje omogoča predvsem dostop do pomnilnika naprave (prim. disk)
- pri disku je dostop relativno varen, ker sam po sebi ne more spreminjati vsebine
- pri mobilni napravi to ni nujno res
- posebej pri tujih aplikacijah

Andrej Brodnik, Digitalna forenzika

---

---

---

---

---

---

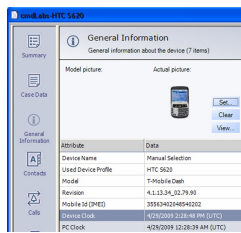
---

---

### Orodja za mobilne naprave

XRY (<http://www.msab.com/>)

Cellebrite UFED (*Universal Forensic Extraction Device*) - <http://www.cellebrite.com/>



Andrej Brodnik, Digitalna forenzika

---

---

---

---

---

---

---

---

### Orodja za mobilne naprave

Logicube CellDEK (<http://www.logicube.com/>)

- MOBILedit! Forensic (<http://mobiledit.com/>)
- programska oprema za analizo



Andrej Brodnik, Digitalna forenzika

---

---

---

---

---

---

---

---





### Neceloviti podatki

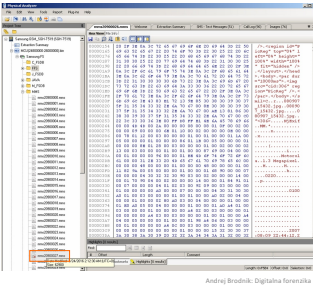
- če je običajen datotečni sistem (FAT, ext2, ext3, APFS, ...) že znana orodja
- EnCase in izbrisane slike

Name	File Offset	File Size	Logical Size	Inherited Size	Date
Prua-0005.jpg	070205 04 14 40PM	070205 06 11 40PM	20,794	20,794	20-11-07
Prua-0014.jpg	080605 11 02 30AM	080605 11 02 30AM	12,286	12,286	20-11-07
Prua-0018.jpg	080505 08 45 30PM	080505 08 45 30PM	12,286	12,286	20-11-07
Prua-0019.jpg	080705 09 16 30PM	080705 09 16 30PM	13,969	13,969	20-11-07
Prua-0020.jpg	080605 11 41 30AM	080605 11 41 30AM	20,528	20,528	20-11-07
Prua-0021.jpg	080705 01 16 30PM	080705 01 16 30PM	16,742	16,742	20-11-07
Prua-0022.jpg	080705 01 16 30PM	080705 01 16 30PM	16,744	16,744	20-11-07
Prua-0023.jpg	080705 01 16 30PM	080705 01 16 30PM	12,696	12,696	20-11-07
Prua-0024.jpg	080705 01 17 30PM	080705 01 17 30PM	15,144	15,144	20-11-07
Prua-0025.jpg	080705 01 17 30PM	080705 01 17 30PM	11,680	11,680	20-11-07
Prua-0026.jpg	080705 01 17 30PM	080705 01 17 30PM	15,676	15,676	20-11-07
Prua-0027.jpg	080705 01 17 30PM	080705 01 17 30PM	15,676	15,676	20-11-07
Prua-0028.jpg	080705 01 19 30PM	080705 01 19 30PM	16,740	16,740	20-08-04
Prua-0029.jpg	080705 01 19 30PM	080705 01 19 30PM	16,680	16,680	20-11-07
Prua-0030.jpg	080705 02 22 30PM	080705 02 22 30PM	6,812	6,812	20-11-07
Prua-0031.jpg	080605 07 39 30PM	080605 07 39 30PM	19,628	19,628	20-11-07
Prua-0032.jpg	080605 08 36 30PM	080605 08 36 30PM	19,272	19,272	20-11-07



### Neceloviti podatki

- v primeru sestavljenih datotek (MMS, docx, ...) lahko najdemo dele podatkov



```

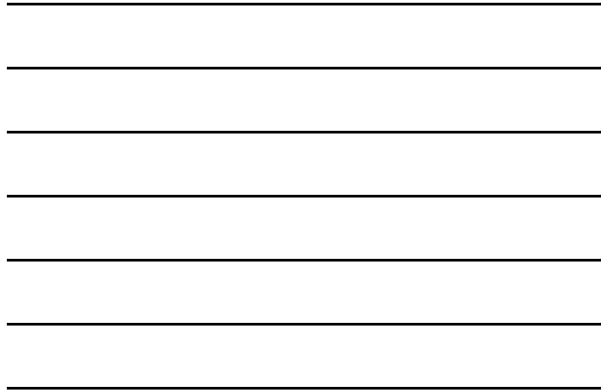
/>.<region id="P
icReg" top="0" l
eft="0" height="
100%" width="100%"
" fit="hidden" />
.</layout.</head
>.<body>.<par dur
="1000ms">..<
/par.</body.</s
mil>C...080907
15432.jpg...08090
7_15432.jpg...0
80907_15432.jpg..
"<306>....NJExif
  
```



### Neceloviti podatki

- primer zajetih podatkov z orodjem DFF (Digital Forensic Framework, <http://www.digital-forensic.org/>)
- Izziv: preučite okolje in kako se ga razširja.

Name	Size	Accessed time	Changed time	Modified time	Metadata
..	4096	120808 AM	120808 AM	6-12-2011 8:56A	File File System
..	4096	120808 AM	120808 AM	6-12-2011 8:56A	File File System
..	4096	120808 AM	120808 AM	6-12-2011 8:56A	File File System
..	4096	120808 AM	120808 AM	6-12-2011 8:56A	File File System



## Oblika datoteke SMIL

- *Synchronized Multimedia Integration Language*
  - del W3C standarda - <http://www.w3.org/AudioVideo/>
  - inačice 1, 2 in 3 (<http://www.w3.org/TR/SMIL3/>)
- vključuje SVG predmete (povečljiva vektorska grafika, *Scalable Vector Graphics*)
- omogoča:
  - animacijo, vključevanje drugih slik, modularizacijo, ...
- **Izziv:** Poiščite SMIL datoteko in jo preučite.
- **Izziv:** Naredite svojo SMIL datoteko ter jo pošljite na forum.

Andrej Brodnik: Digitalna forenzika

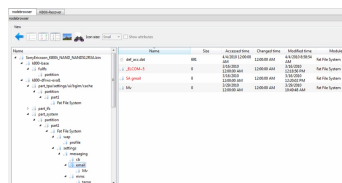
## Neceloviti podatki

- skladiščni medij je SSD
- podatki, ki so v shrambi, a niso strukturirani
  - delno zbrisani podatki
  - podatki v zbranih blokih, ki so razpršeni po enoti
- **Izziv:** pregledajte forenzični izziv in rešitev DRFWS2010 (*Digital Forensic Research Conference*) – <http://www.dfrws.org/2010/challenge/>
  - na voljo primeri datotek z enoto
- **Izziv:** pregledajte forenzični izziv in rešitev DRFWS2011 – <http://www.dfrws.org/2011/challenge/>
- **Izziv:** pregledajte forenzični izziv DRFWS2012 – <http://www.dfrws.org/2012/challenge/>

Andrej Brodnik: Digitalna forenzika

## Preiskava – ostali podatki

- veliko pametnih telefonov hrani svoje podatke v podatkovni bazi
  - SQLite – Android, iPhone, Palm, ...
  - cemail.vol – Windows Mobile



Andrej Brodnik: Digitalna forenzika



## SIM kartica

- preprosta notranja struktura
- sestoji iz datotek, od katerih ima vsaka svojo identifikacijsko dvo-bajtno kodo
- prvi bajt označuje tip datoteke:
  - 3F – glavna datoteka (*Master File*), MF
  - 7F – namenska datoteka (*Dedicated File*), DF
  - 2F – delna datoteka MF
  - 6F – delna datoteka DF

Description	Location
SMS	7F10:6F3C
MS/SDN	7F10:6F40
Last Dialed Numbers (LDN)	7F10:6F44
Abbreviated Dial Numbers (ADN)	7F10:6F3A
IMSI	7F20:6F07
LOCI	7F20:6F7E
LOCI/GPRS	7F20:6F53

Andrej Brodnik: Digitalna forenzika

## SIM kartica

- nekatere datoteke so definirane v standardu
  - 3F00:7F10 (DFTELECOM, *dedicated file*): zapisi o uporabi storitev (npr. poslana SMS sporočila, klicane številke, ...)
  - 3F00:2FE2 (EFICCID, *elementary file*): hrani ICC-ID (*Integrated Circuit Card ID*)
  - 3F00:7F20:6F07 EFIMSI: hrani IMSI (*International Mobile Subscriber Identity*)
  - 7F20:6F7E (EFLOCI): kako se je kartica premikala med operaterji
  - 7F20:6F53 (EFLOCIGPRS): GPRS usmerjevalno področje

Andrej Brodnik: Digitalna forenzika

## SIM kartica

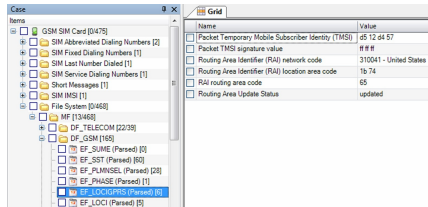
- orodja za pregledovanje SIM kartic:
  - TULP2G: *Netherlands Forensic Institute*
  - <http://tulp2g.sourceforge.net/>
- orodje ni posodobljeno, a za branje SIM kartic je v redu

Andrej Brodnik: Digitalna forenzika



## SIM kartica

- primer pogleda v SIM kartico (*Paraben Device Seizure*)



Andrey Brodnik: Digitalna forenzika

---

---

---

---

---

---

---

---

## SIM kartica

- Izziv: kako bi lahko dostopili do podatkov na vaši SIM kartici?
- Izziv: ali se hrani celotna zgodovina GPRS usmerjanja?
- Izziv: naštejajte EF, v katere lahko piše uporabnik.

Andrey Brodnik: Digitalna forenzika

---

---

---

---

---

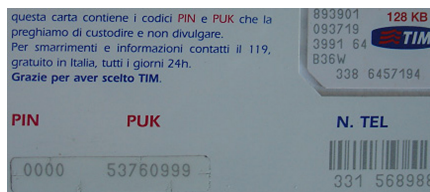
---

---

---

## SIM kartica in varnost

- kartica je zaščitena s PIN (*Personal Identification Number*) kodo
- če se prevečkrat zmotimo (ni možno pregledovanje), se kartica zaklene
- za odklepanje potrebujemo PUK (*PIN Unlock Key*) kodo
  - pogosto jo ima operater



Andrey Brodnik: Digitalna forenzika

---

---

---

---

---

---

---

---