Digitalna forenzika

Andrej Brodnik

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

Podatki na celičnem telefonu

- Primer (POCKET-DIAL M FOR MURDER):
  Storilec 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*)

Forenzika mobilnih naprav

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

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

Forenzika mobilnih naprav

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

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

Forenzika mobilnih naprav

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

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

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?

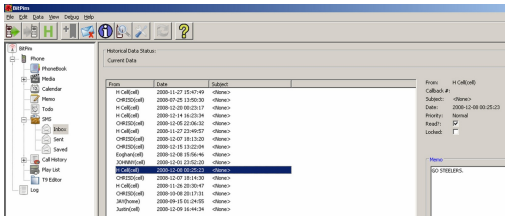
Podatki o napravi

- 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

SMS kot dokazno gradivo

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

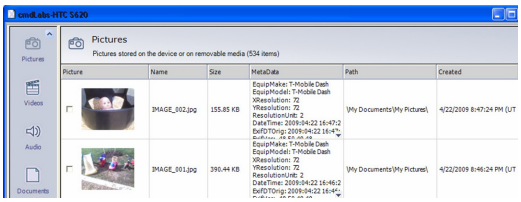
primer vpogleda z orodjem BitPim (http://www.bitpim.org/)



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/)



Dostop do medmrežnih storitev

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

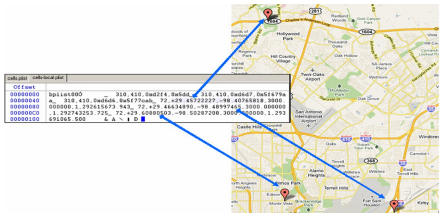
Dostop do medmrežnih storitev

- 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
```

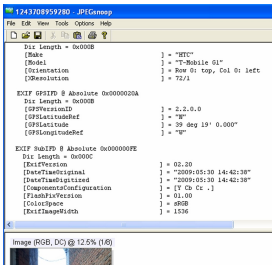
Geografski podatki

- hrani se lahko zgodovina prehodov med baznimi postajami
- GPS naprave lahko hranijo natančne koordinate



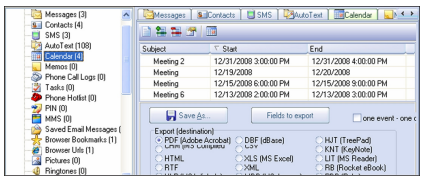
Geografski podatki

- slike lahko hranijo podatke o tem kdaj in kje so bile posnete
  - prim EXIF format
- *Izziv:* poiščite geografske podatke v vašem telefonu.



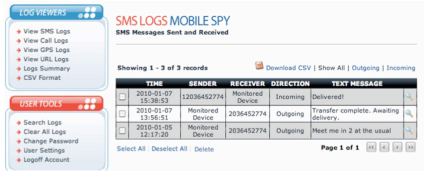
Drugi podatki

- koledar, zapiski, ...
- *Izziv:* poiščite koledarske podatke v vašem telefonu.



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/)
- aplikacija pobira gesla, ...
  - omogoči dostop napadalcu do bančnih računov ...
  - glej MobileSpy (http://www.mobile-spy.com/)



Napadi na mobilne naprave

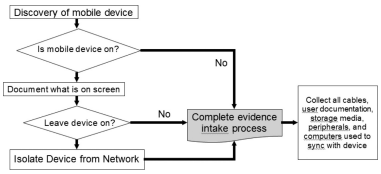
- *Izziv:* Kako deluje MobileSpy?
- *Izziv:* Najdite programje, ki vam lahko škoduje na Android sistemu?
- *Izziv:* Naredite svoj program, ki pobira podatke na Android (iPhone) sistemu. Je lahko to tudi uporabno programje?

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



Rokovanje z napravo

- umakniti pomnilniške module
  - pomnilniški moduli so vedno manjši
- običajno FAT datotečni sistem
- sicer običajni postopki (podpis, dnevnik, ...)

Prid0bivanje podatkov

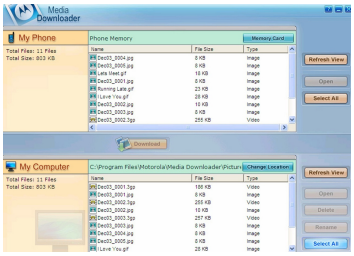
- različni načini dostopa pri različnih modelih
  - nima vsaka naprava USB vodila
- primeri:
  - preko uporabniškega vmesnika
  - preko komunikacijskih vrat
  - notranjega vodila (Nokia F-BUS, *Flash BUS*)
  - preko JTAG (*Joint Test Action Group*) vmesnika
  - preko neposrednega dostopa do čipa

Prid0bivanje 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

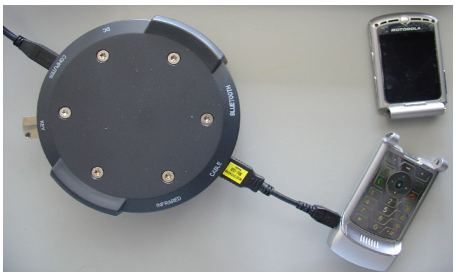
Primeri ...

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



Primeri ...

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

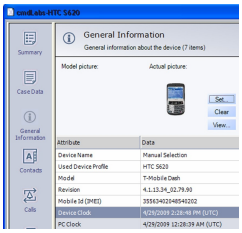


Orodja za mobilne naprave

- 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

Orodja za mobilne naprave

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



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

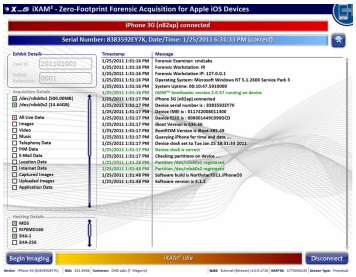
Orodja za mobilne naprave

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

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

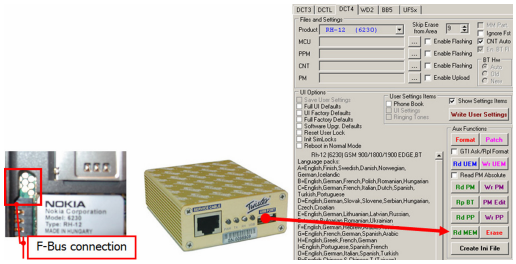
Orodja za mobilne naprave

- iXAM (http://www.ixam-forensics.com/)



Orodja za mobilne naprave

Twister Flasher

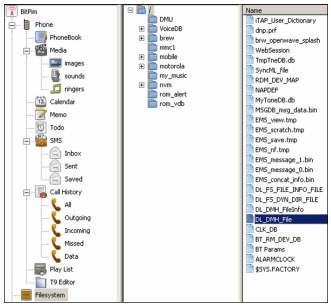


Preiskava – datotečni sistem

- odvisno od naprave
  - posebni
  - vgrajeni v sisteme Qualcomm (BREW, Binary Runtime Environment for Wireless)
  - FAT, ext2, ext3, HSFX, ...
- na voljo različna orodja:

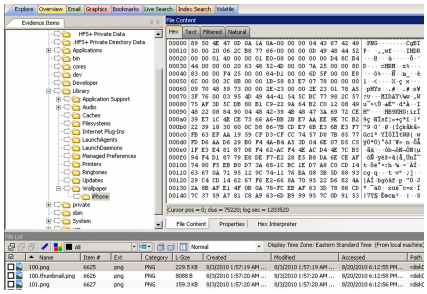
Nekaj osnovnih orodij ...

BitPim (http://www.bitpim.org/) – Motorola CDMA



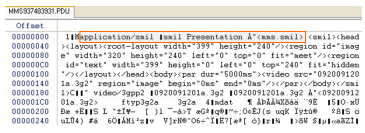
Nekaj osnovnih orodij ...

Forensic Toolkit, FTK (http://accessdata.com/products/computer-forensics/ftk) – iPhone



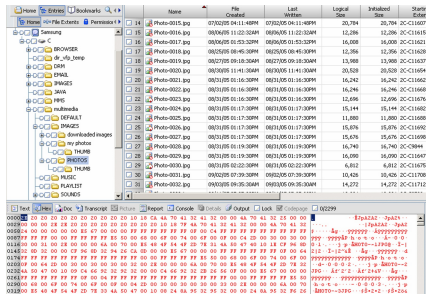
Neceloviti podatki

- četudi nimamo vseh podatkov, lahko iz logičnih podatkov rekunstruiramo delno zbrisane podatke



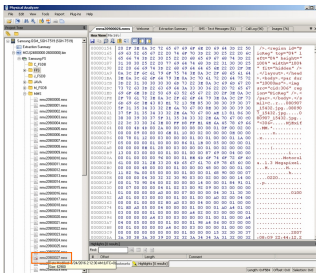
Neceloviti podatki

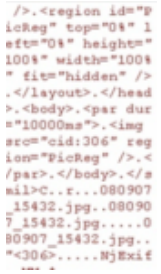
- če je običajen datotečni sistem (FAT, ext2, ext3, HFS, ...) že znana orodja
  - EnCase in izbrisane slike



Neceloviti podatki

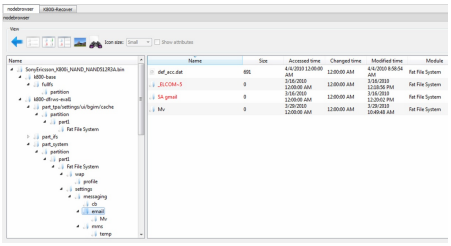
- v primeru sestavljenih datotek (MMS, docx, ...) lahko najdemo dele podatkov





Neceloviti podatki

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



Oblika datoteke SMIL

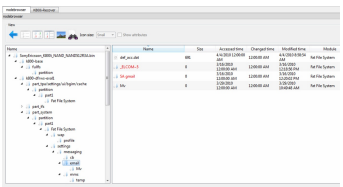
- *Synchronized Multimedia Integration Language*
  - del W3C standarda - http://www.w3.org/AudioVideo/
  - inačice 1, 2 in 3 (http://www.w3.org/TR/SMIL3/)
- vključuje SVG predmete (povečljiva vektorska grafika, *Scalable Vector Graphics*)
- omogoča:
  - animacijo, vključevanje drugih slik, modularizacijo,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

Neceloviti podatki

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

Preiskava – ostali podatki

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



Preiskava – format podatkov

- večinoma standardni formati
- SMS sporočila:
  - 7-bitni standard; GSM 03.38: 160 znakov
  - 16-bitni UCS-2 (*Universal Character Set*, UTF-16): 70 znakov

Basic Character Set[1]

	0x00	0x10	0x20	0x30	0x40	0x50	0x60	0x70
0x00	@	Δ	SP	0	¡	P	¿	p
0x01	£	_	!	1	A	Q	a	q
0x02	$	Φ	"	2	B	R	b	r
0x03	¥	Γ	#	3	C	S	c	s
0x04	è	Λ	¤	4	D	T	d	t
0x05	é	Ω	%	5	E	U	e	u
0x06	ù	Π	&	6	F	V	f	v
0x07	ì	Ψ	'	7	G	W	g	w
0x08	ò	Σ	(	8	H	X	h	x
0x09	Ç	Θ	)	9	I	Y	i	y
0x0A	LF	Ξ	*	:	J	Z	j	z
0x0B	Ø	ESC	+	;	K	Ä	k	ä
0x0C	ø	Æ	,	<	L	Ö	l	ö
0x0D	CR	æ	-	=	M	Ñ	m	ñ
0x0E	Å	ß	.	>	N	Ü	n	ü
0x0F	å	É	/	?	O	§	o	à

Basic Character Set Extension[2]

	0x00	0x10	0x20	0x30	0x40	0x50	0x60	0x70
0x00								
0x01								
0x02								
0x03								
0x04		^						
0x05								€
0x06								
0x07								
0x08			{					
0x09			}					
0x0A	FF							
0x0B		SS2						
0x0C				[				
0x0D	CR2			~				
0x0E				]				
0x0F			\					

Preiskava – format podatkov

- debeli in tanki konec – odvisno od procesorja
  - Motorola – debeli konec
- debeli in tanki košček (*nibble*)
  - številka 12036452577 se shrani kot 2130462577F4 (F je polnilo)

Preiskava – SIM kartica

- SIM (*Subscriber Indenty Module*)
- naprava je last uporabnika, SIM kartica je last operaterja
  - ki dovoli uporabniku shranjevanje določenih podatkov nanjo
- podrobna definicija v:
  - ETSI (*European Telecommunications Standards Institute*): *GSM, Global Mobile Communications*, GSM 11.11, 1995.
  - www.ttfn.net/techno/smartcards/gsm11-11.pdf

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
MSISDN	7F10:6F40
Last Dialed Numbers (LDN)	7F10:6F44
Abbreviated Dial Numbers (ADN)	7F10:6F3A
IMSI	7F20:6F07
LOCI	7F20:6F7E
LOCIGPRS	7F20:6F53

SIM kartica

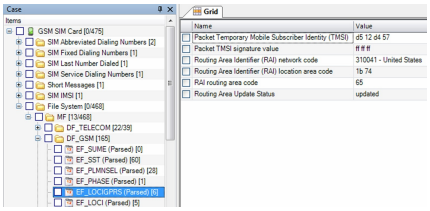
- nekatere datoteke so definirane v standardu
  - 3F00:7F10 (DFTELECOM, *dedicated file*): zapisi o uporabi storitev (npr. poslana SMS sporočila, klicane številke, ...)
  - 3F00:2FE2 (EFICCID, *elementary file*): hrani ICC-ID (*Integrated Circuit Card ID*)
  - 3F00:7F20:6F07 EFIMSI: hrani IMSI (*International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

SIM kartica

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

SIM kartica

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



SIM kartica

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

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