

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 določenih temperaturi se sproži akcija
- telefoni so postali celoviti vgrajeni sistemi (*embedded systems*)

Forenzika mobilnih naprav.

- naprave imajo sposobnejše operacijske sisteme
 - Android
 - iPhone
 - Blackberry
 - 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 števila 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 sestojijo 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?

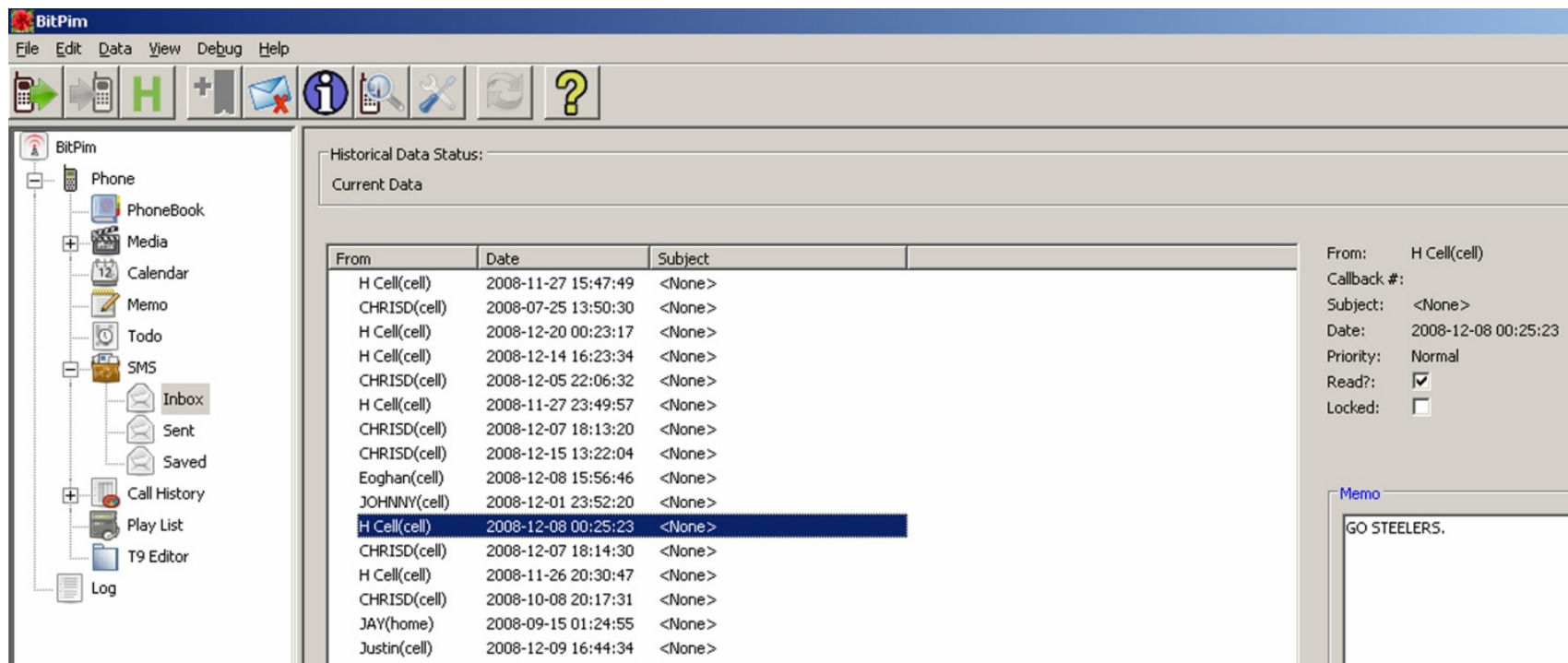
Podatki o in na napravi.

- 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

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/>)



BitPim

File Edit Data View Debug Help

Historical Data Status:
Current Data

From	Date	Subject
H Cell(cell)	2008-11-27 15:47:49	<None>
CHRISD(cell)	2008-07-25 13:50:30	<None>
H Cell(cell)	2008-12-20 00:23:17	<None>
H Cell(cell)	2008-12-14 16:23:34	<None>
CHRISD(cell)	2008-12-05 22:06:32	<None>
H Cell(cell)	2008-11-27 23:49:57	<None>
CHRISD(cell)	2008-12-07 18:13:20	<None>
CHRISD(cell)	2008-12-15 13:22:04	<None>
Eoghan(cell)	2008-12-08 15:56:46	<None>
JOHNNY(cell)	2008-12-01 23:52:20	<None>
H Cell(cell)	2008-12-08 00:25:23	<None>
CHRISD(cell)	2008-12-07 18:14:30	<None>
H Cell(cell)	2008-11-26 20:30:47	<None>
CHRISD(cell)	2008-10-08 20:17:31	<None>
JAY(home)	2008-09-15 01:24:55	<None>
Justin(cell)	2008-12-09 16:44:34	<None>

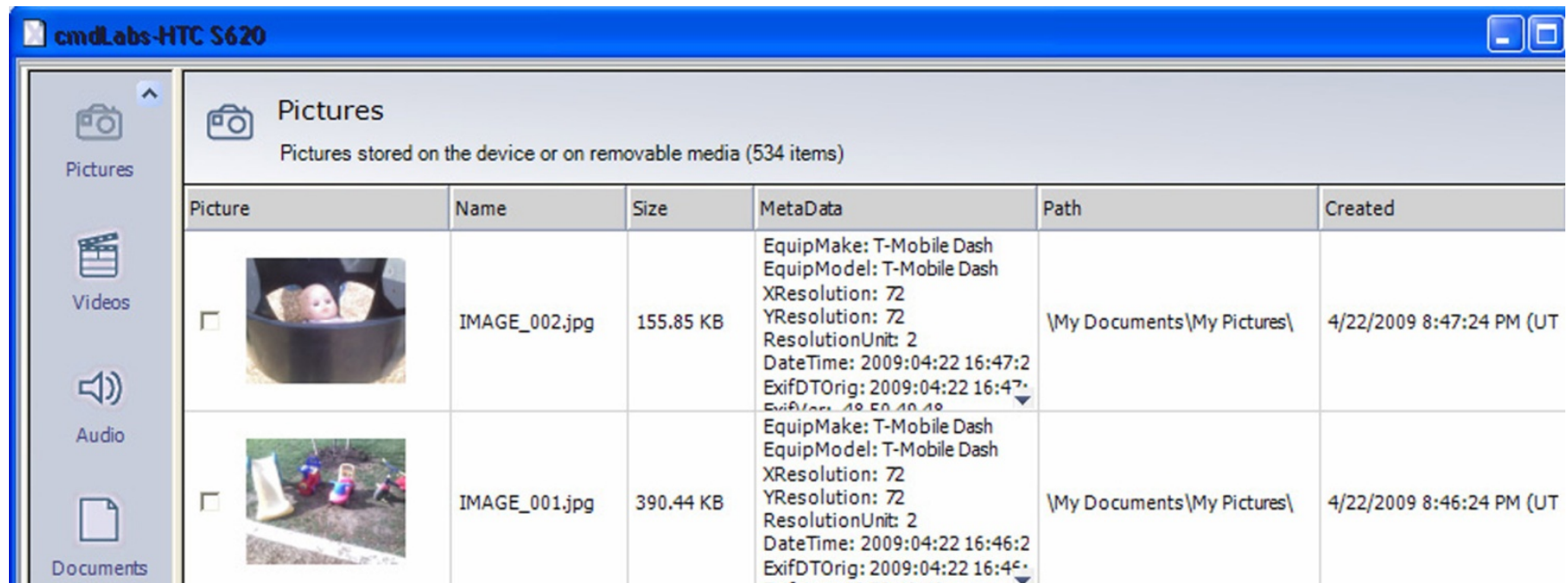
From: H Cell(cell)
Callback #:
Subject: <None>
Date: 2008-12-08 00:25:23
Priority: Normal
Read?:
Locked:

Memo
GO STEELERS.



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/>)



The screenshot shows a Windows Mobile interface for a device named 'cmdLabs-HTC S620'. The 'Pictures' folder is selected, showing 534 items. A table lists two image files with their EXIF metadata.

Picture	Name	Size	MetaData	Path	Created
	IMAGE_002.jpg	155.85 KB	EquipMake: T-Mobile Dash EquipModel: T-Mobile Dash XResolution: 72 YResolution: 72 ResolutionUnit: 2 DateTime: 2009:04:22 16:47:2 ExifDOrig: 2009:04:22 16:47:2 ExifUser: 18 50 40 48	\\My Documents\\My Pictures\\	4/22/2009 8:47:24 PM (UT)
	IMAGE_001.jpg	390.44 KB	EquipMake: T-Mobile Dash EquipModel: T-Mobile Dash XResolution: 72 YResolution: 72 ResolutionUnit: 2 DateTime: 2009:04:22 16:46:2 ExifDOrig: 2009:04:22 16:46:2 ExifUser: 18 50 40 48	\\My Documents\\My Pictures\\	4/22/2009 8:46:24 PM (UT)

Dostop do medmrežnih storitev

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

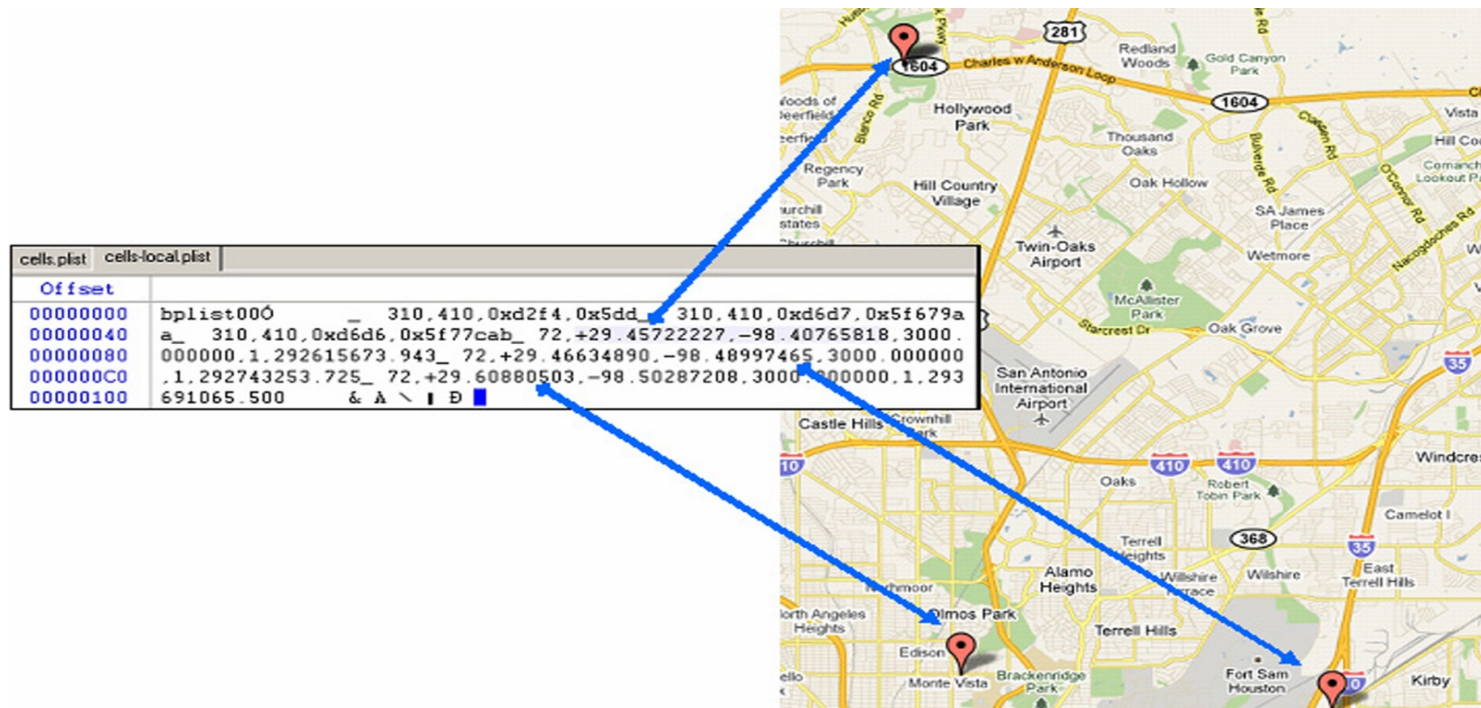
Dostop do medmrežnih storitev

- 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
```

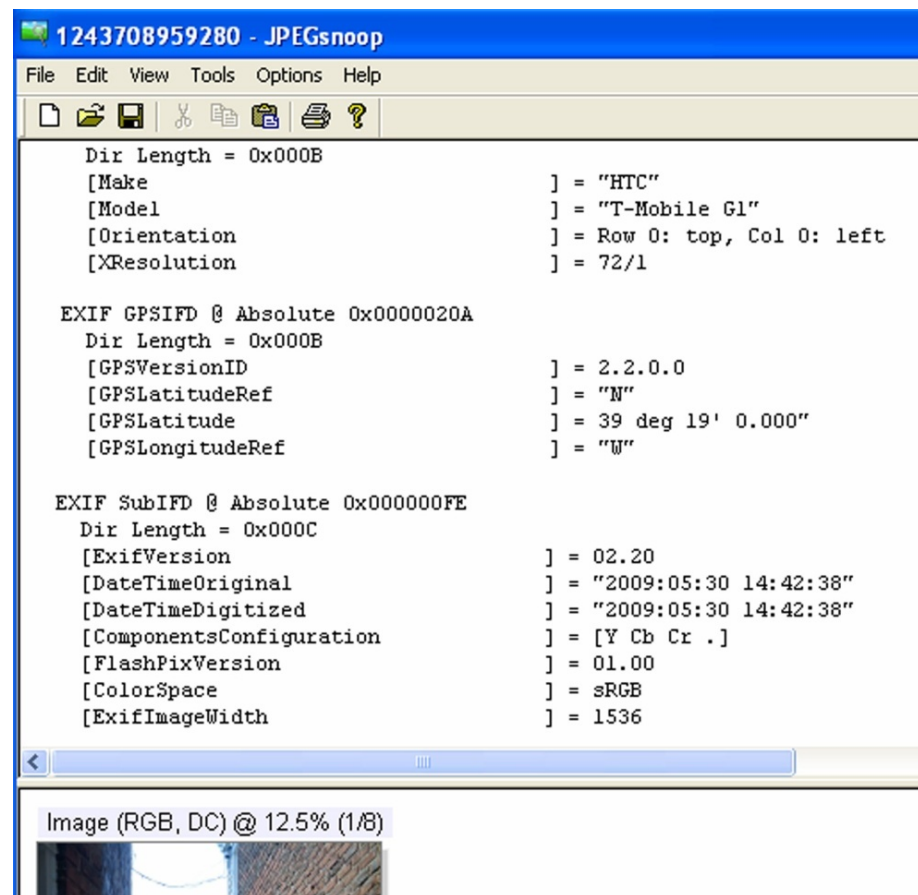
Geografski podatki

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



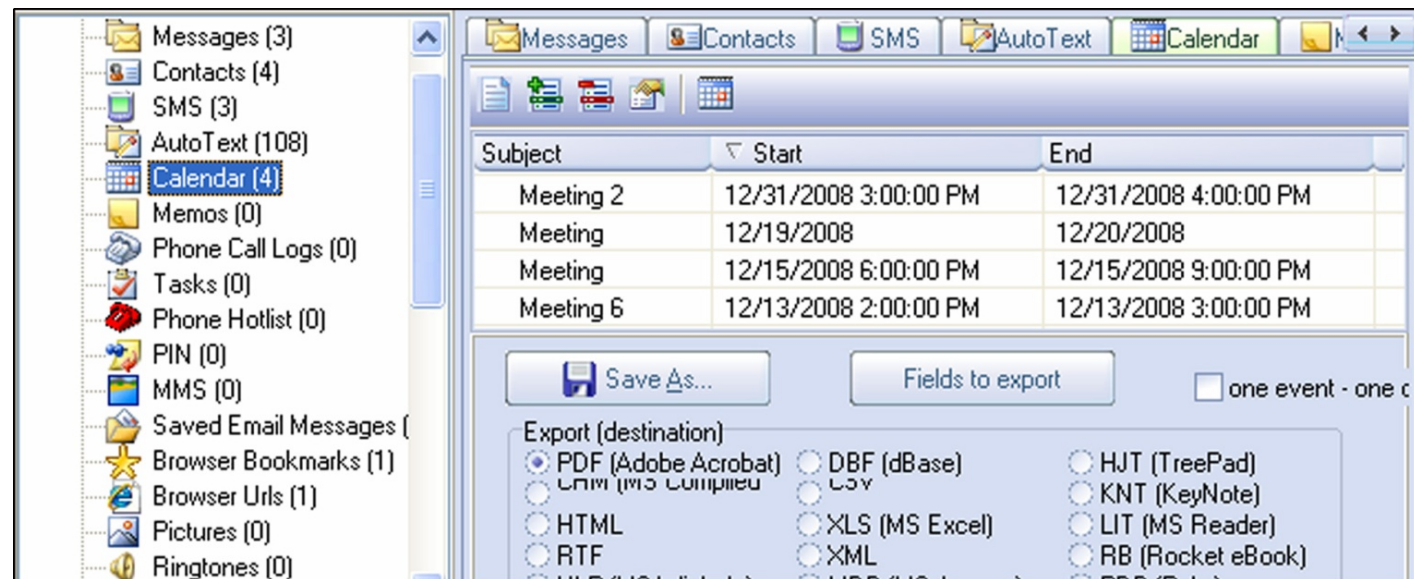
Geografski podatki

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



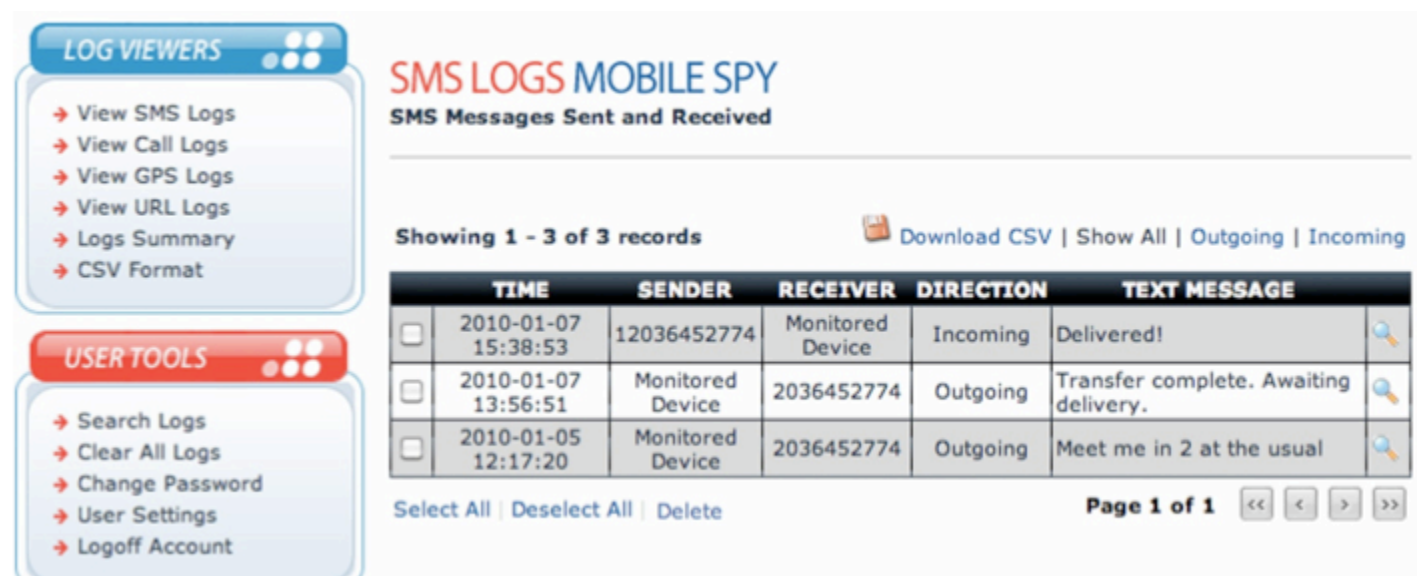
Drugi podatki

- 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/>)



The screenshot displays the 'SMS LOGS MOBILE SPY' web interface. On the left, there are two panels: 'LOG VIEWERS' with options like 'View SMS Logs', 'View Call Logs', 'View GPS Logs', 'View URL Logs', 'Logs Summary', and 'CSV Format'; and 'USER TOOLS' with options like 'Search Logs', 'Clear All Logs', 'Change Password', 'User Settings', and 'Logoff Account'. The main area shows a table of SMS messages with columns for TIME, SENDER, RECEIVER, DIRECTION, and TEXT MESSAGE. Below the table are navigation controls for 'Showing 1 - 3 of 3 records', 'Download CSV', 'Show All', 'Outgoing', 'Incoming', 'Select All', 'Deselect All', 'Delete', and 'Page 1 of 1'.

	TIME	SENDER	RECEIVER	DIRECTION	TEXT MESSAGE	
<input type="checkbox"/>	2010-01-07 15:38:53	12036452774	Monitored Device	Incoming	Delivered!	
<input type="checkbox"/>	2010-01-07 13:56:51	Monitored Device	2036452774	Outgoing	Transfer complete. Awaiting delivery.	
<input type="checkbox"/>	2010-01-05 12:17:20	Monitored Device	2036452774	Outgoing	Meet me in 2 at the usual	

Napadi na mobilne naprave

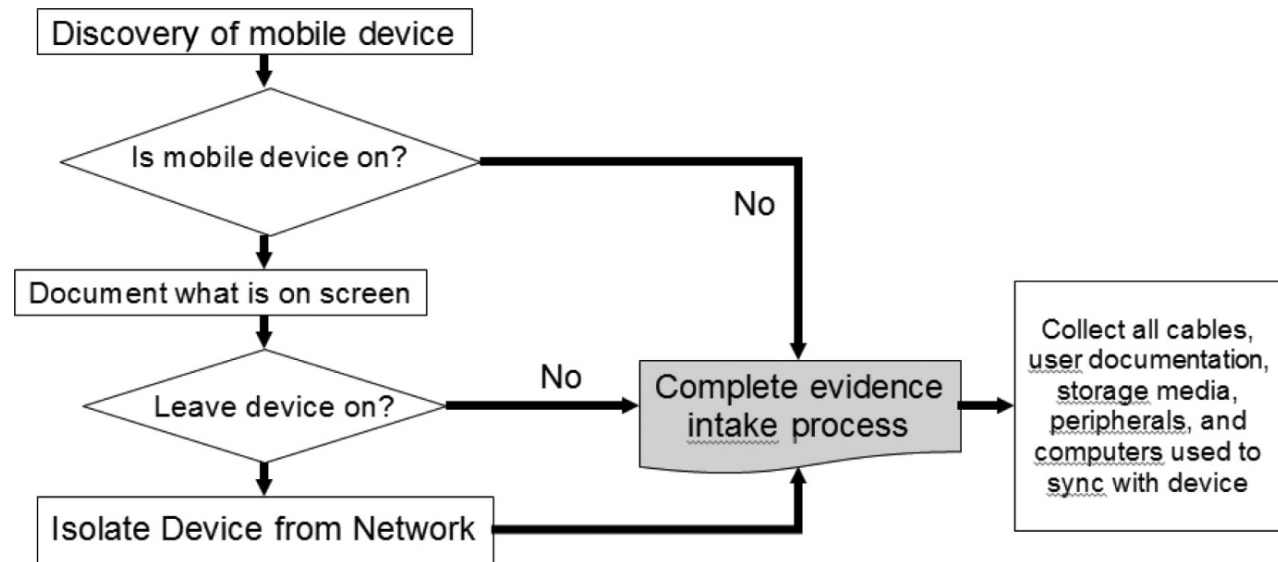
- *Izziv:* Kako deluje MobileSpy?
- *Izziv:* Najdite programje, ki vam lahko škoduje na Android sistemu?
- *Izziv:* Naredite svoj program, ki pobira podatke na Android (iPhone) sistemu. Je lahko to tudi uporabno programje?

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
 - iPhone: APFS, Android: Linux zasnova
- sicer običajni postopki (podpis, dnevnik, ...)



Pridobivanje podatkov.

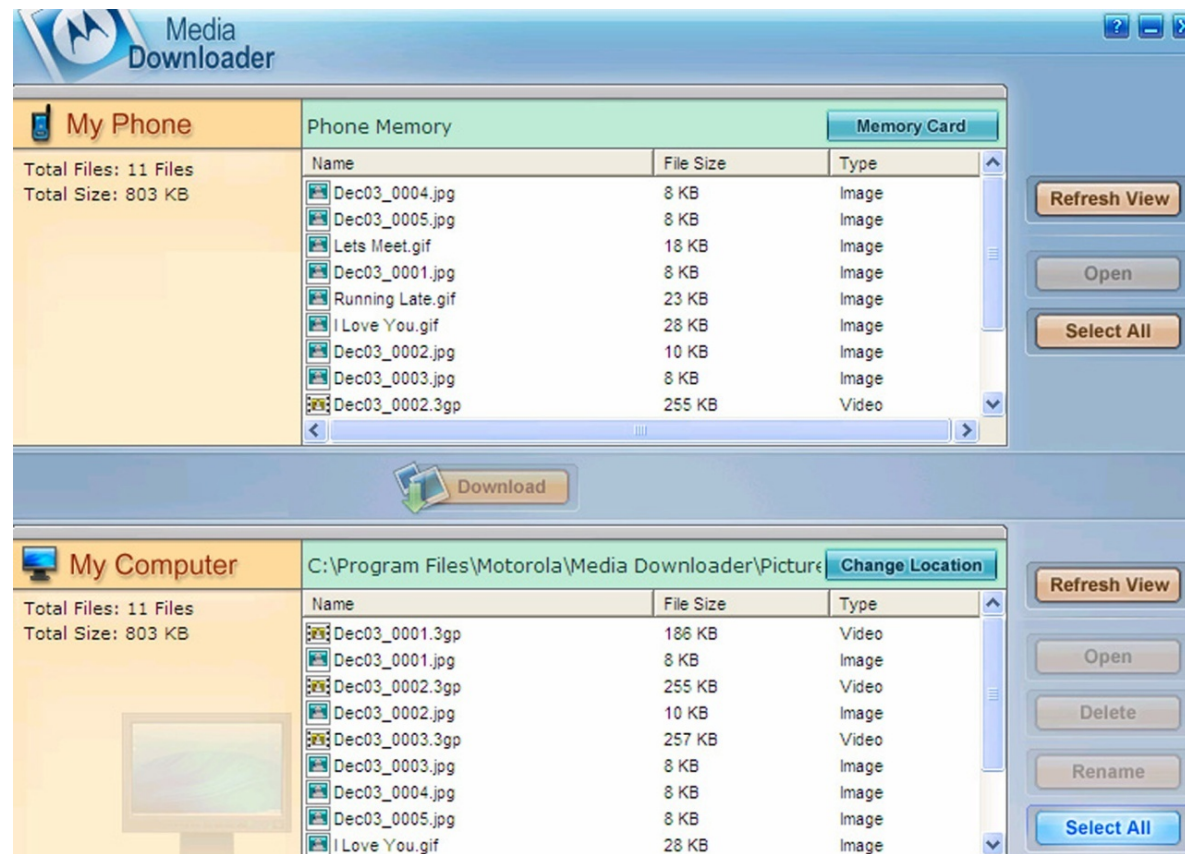
- različni načini dostopa pri različnih modelih
 - nima vsaka naprava USB vodila
- primeri:
 - preko uporabniškega vmesnika
 - preko komunikacijskih vrat
 - notranjega vodila (Nokia F-BUS, *Flash BUS*)
 - preko JTAG (*Joint Test Action Group*) vmesnika
 - preko neposrednega dostopa do čipa

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 zbranih in ostalih podatkov

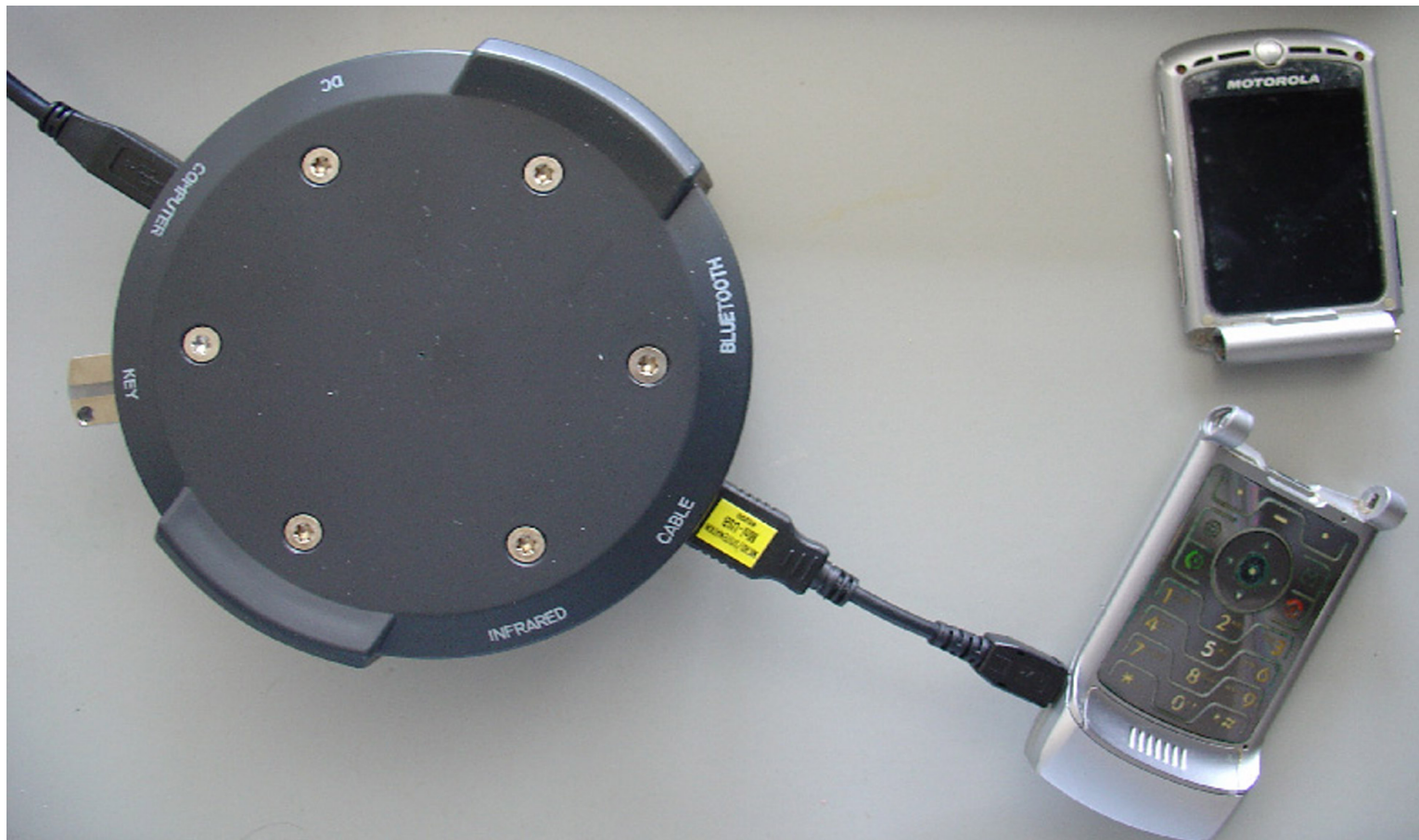
Primeri ...

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



Primeri ...

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



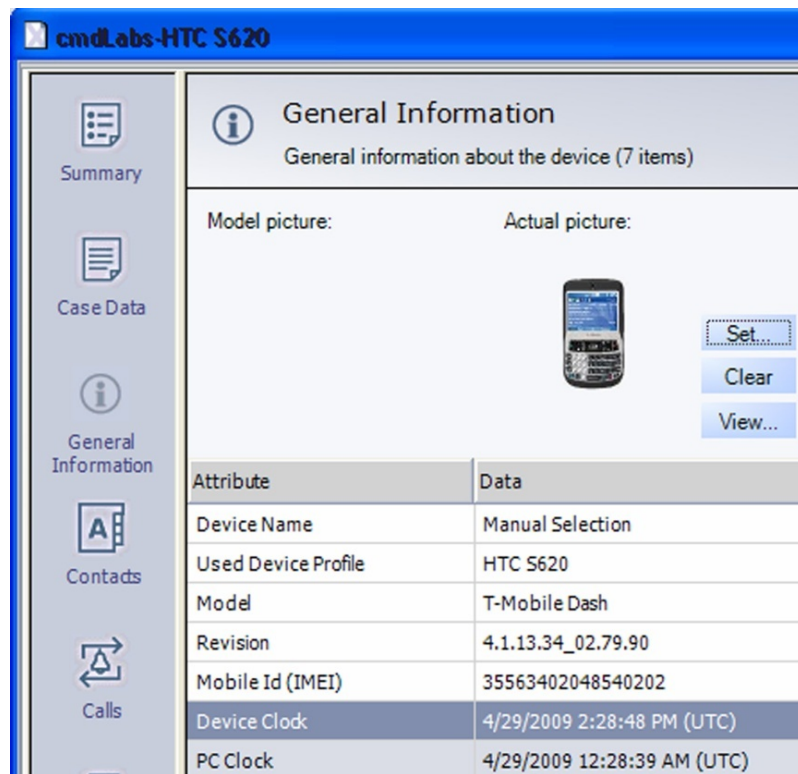
Orodja za mobilne naprave

- 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/>



The screenshot shows the 'cmdLabs-HTC S620' software interface. On the left is a navigation menu with icons for Summary, Case Data, General Information, Contacts, and Calls. The main area displays 'General Information' for the device, including a 'Model picture' and 'Actual picture' section with a small image of the phone and buttons for 'Set...', 'Clear', and 'View...'. Below this is a table of attributes and data.

Attribute	Data
Device Name	Manual Selection
Used Device Profile	HTC S620
Model	T-Mobile Dash
Revision	4.1.13.34_02.79.90
Mobile Id (IMEI)	35563402048540202
Device Clock	4/29/2009 2:28:48 PM (UTC)
PC Clock	4/29/2009 12:28:39 AM (UTC)



Orodja za mobilne naprave

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

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



Orodja za mobilne naprave

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

The screenshot displays the iXAM² software interface for forensic acquisition. The title bar reads "iXAM² - Zero-Footprint Forensic Acquisition for Apple iOS Devices". A red status bar indicates "iPhone 3G (n82ap) connected". Below this, a blue bar shows "Serial Number: 8383592EY7K, Date/Time: 1/25/2011 6:31:33 PM (correct)".

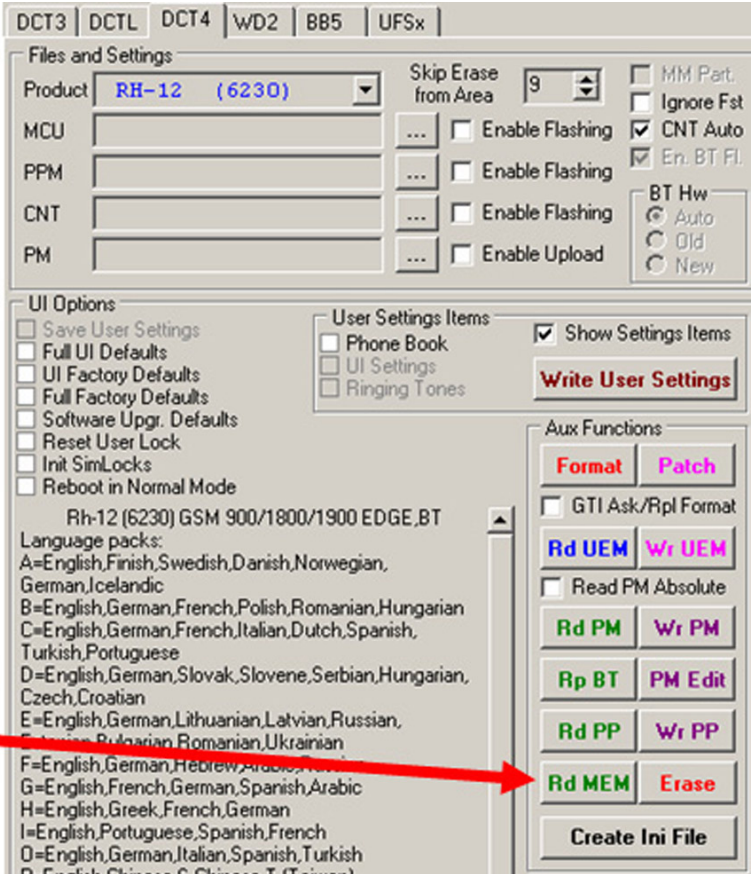
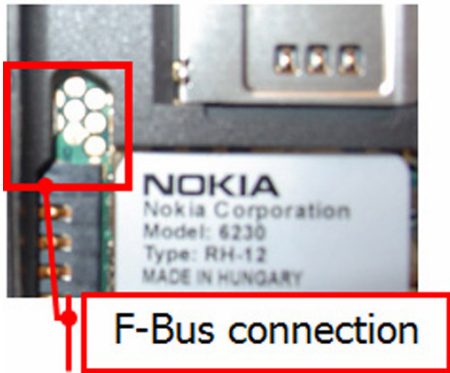
The interface is divided into several sections:

- Exhibit Details:** Case ID: 201101001, Exhibit Reference: 0001.
- Acquisition Details:** Two disks are selected for acquisition: /dev/rdisk0s1 (500.00MB) and /dev/rdisk0s2 (14.64GB). A list of data types is shown with checkboxes: All Live Data (checked), Images, Video, Music, Telephony Data, PIM Data, E-Mail Data, Location Data, Internet Data, Captured Images, Uploaded Images, and Application Data.
- Hashing Details:** MD5 (checked), R1PEMD160, SHA-1 (checked), and SHA-256.
- Message Log:** A table with columns for Timestamp and Message. The messages include: "Forensic Examiner: cmdLabs", "Forensic Workstation: IR", "Forensic Workstation IP: 127.0.0.1", "Operating System: Microsoft Windows NT 5.1.2600 Service Pack 3", "System Uptime: 00:10:47.5910000", "iXAM²® bootloader version 2.0.57 running on device", "iPhone 3G (n82ap) connected", "Device serial number is : 8383592EY7K", "Device IMEI is : 011742008011300", "Device ECID is : 000001449C090DCD", "iBoot Version is 636.66", "BootROM Version is iBoot-385.49", "Querying iPhone for time and date ...", "Device clock set to Tue Jan 25 18:31:33 2011", "Device clock is correct", "Checking partitions on device ...", "Partition /dev/rdisk0s1 registered", "Partition /dev/rdisk0s2 registered", "Software build is Northstar7D11.iPhoneOS", and "Software version is 3.1.2".

At the bottom, there are buttons for "Begin Imaging", "iXAM² Idle", and "Disconnect". The status bar at the very bottom shows: "Device: iPhone 3G (8383592EY7K) | Disk: 152.29GB | Customer: CMD Labs (T. Maguire) | Build: External (Release) v2.0.5.1720 | HASPID: 1770050135 | License Type: Perpetual".

Orodja za mobilne naprave

Twister Flasher



Preiskava – datotečni sistem.

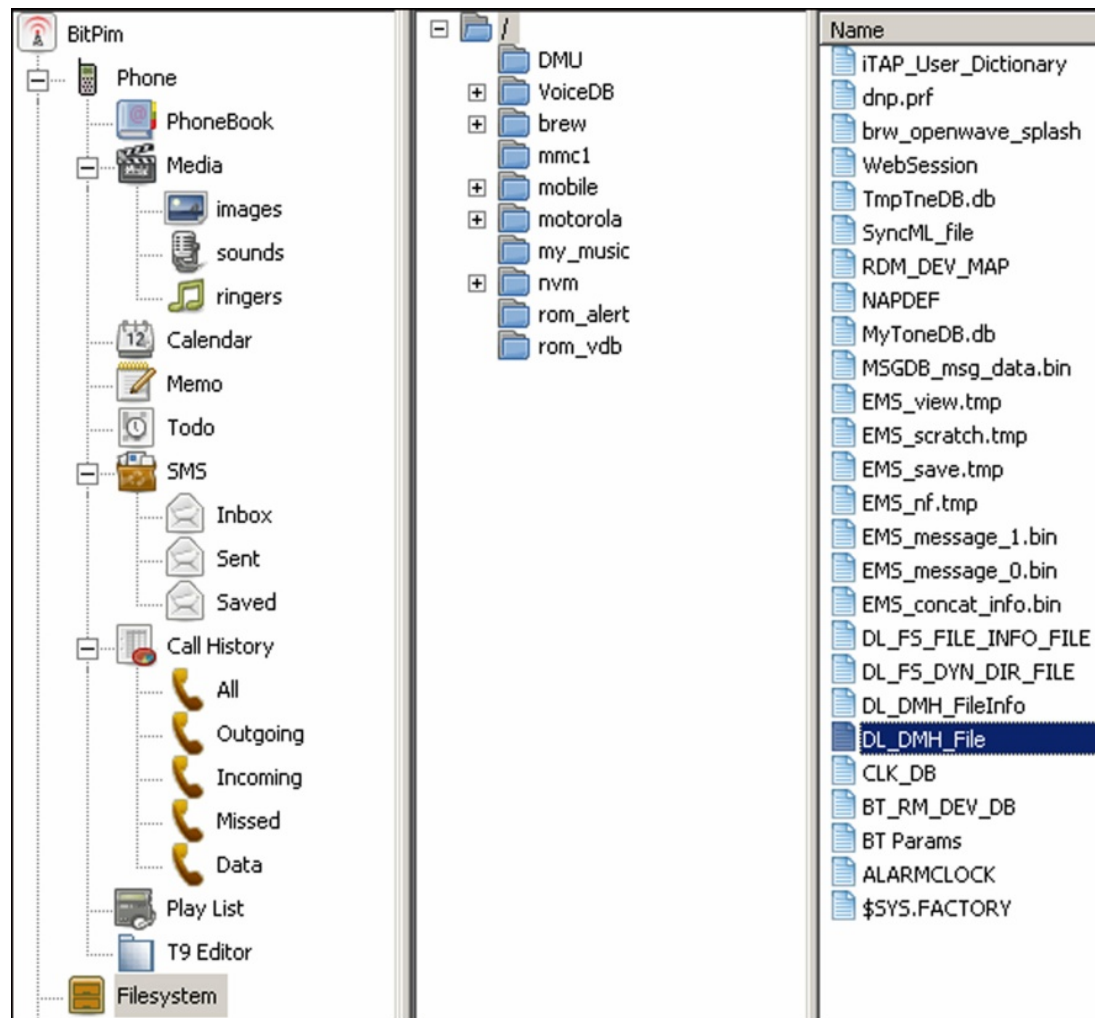
- odvisno od naprave
 - posebni
 - vgrajeni v sisteme Qualcomm (BREW, Binary Runtime Environment for Wireless)
 - FAT, ext2, ext3, HSFx, APFS, ...
- na voljo različna orodja:

Nekaj osnovnih orodij ...

BitPim

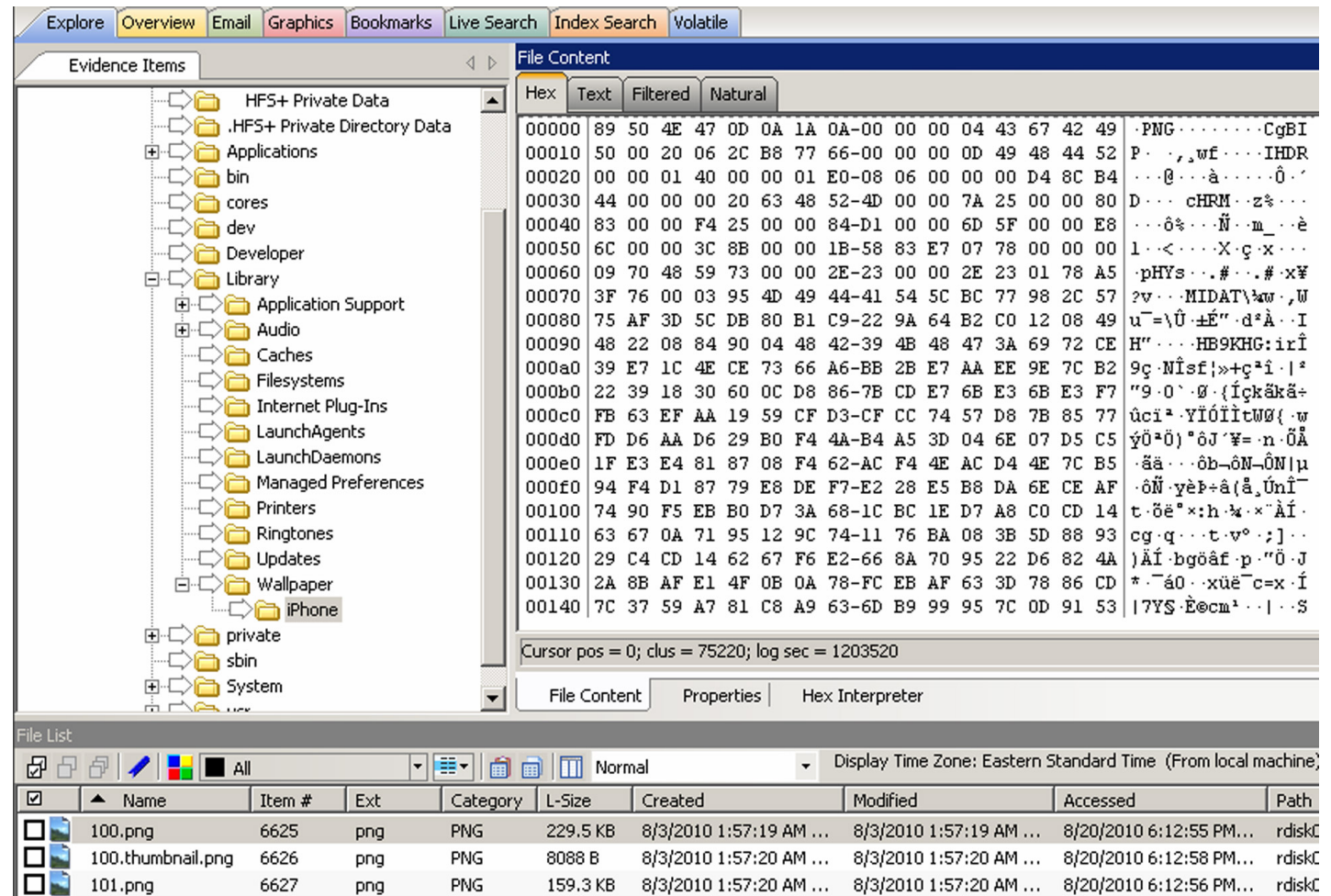
(<http://www.bitpim.org/>) –

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 rekonstruiramo delno zbrisane podatke

MMS937483931.PDU	
Offset	
00000000	1Application/smil smil Presentation Å<mms.smil> <smil><head
00000040	><layout><root-layout width="399" height="240"/><region id="imag
00000080	e" width="320" height="240" left="0" top="0" fit="meet"/><region
000000C0	id="text" width="399" height="0" left="0" top="240" fit="hidden
00000100	"></layout></head><body><par dur="5000ms"><video src="092009120
00000140	1a.3g2" region="image" begin="0ms" end="0ms"/></par></body></smi
00000180	l>C" video/3gpp2 0920091201a.3g2 0920091201a.3g2 Å<09200912
000001C0	01a.3g2> ftyp3g2a 3g2a 4mdat ÅpÅÅX8ää "9È 5 O-xÜ
00000200	Đæ +È S L "±Í#- [)l -à>T æG³ q@ ~+:ÖcÈJ(s uqK İytú@ 9B S ö
00000240	uLÜ4) #á 6Ö ÁMi²z v V]rN@°06÷^İ È?[æ³[ó} r ¼ >8W S p «ažZ

Neceloviti podatki

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

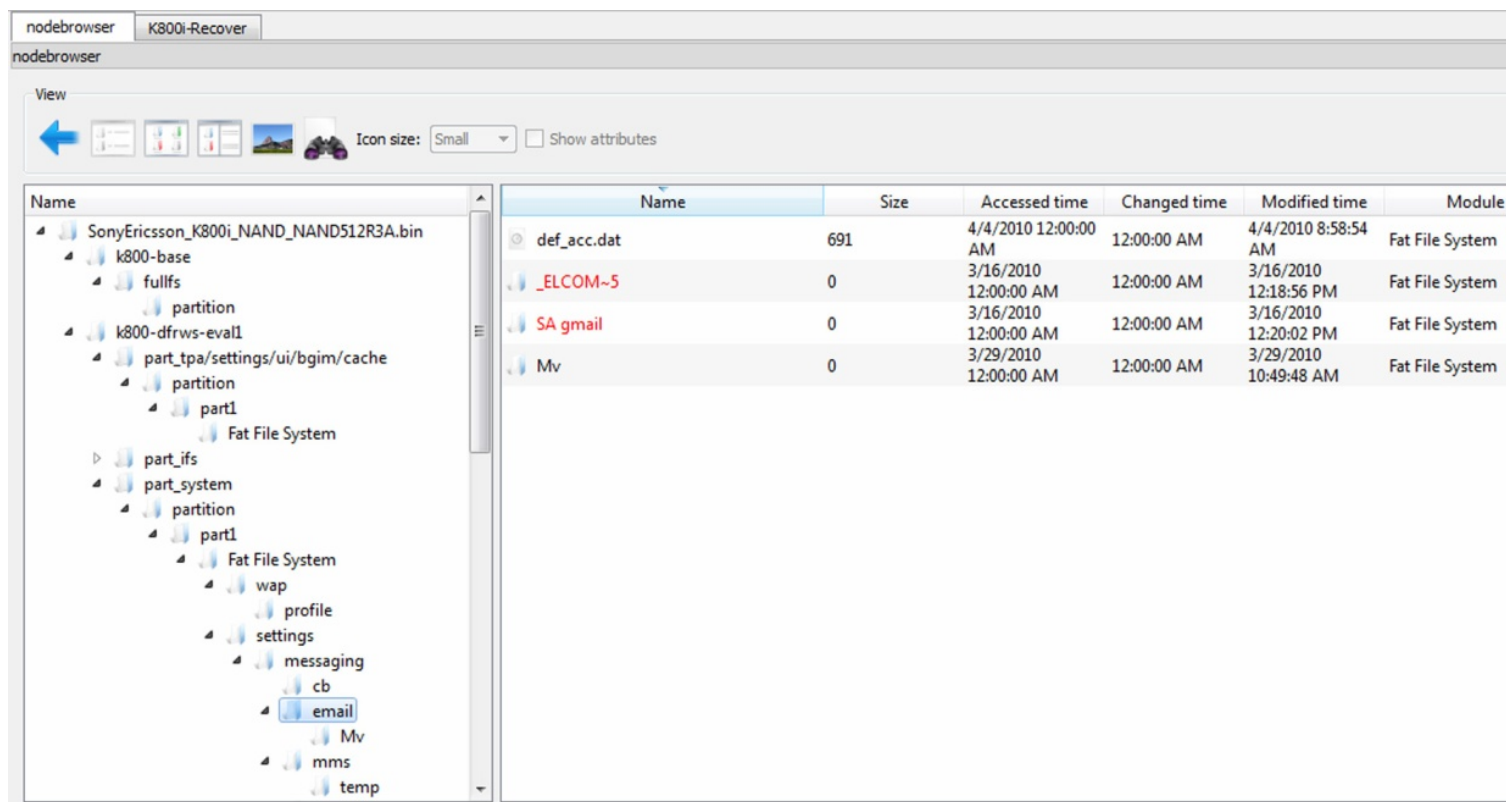
The image shows a file explorer window displaying a directory of photos. The files are listed in a table with columns for Name, File Created, Last Written, Logical Size, Initialized Size, and Startir Extir.

Name	File Created	Last Written	Logical Size	Initialized Size	Startir Extir
Photo-0015.jpg	07/02/05 04:11:48PM	07/02/05 04:11:48PM	20,784	20,784	2C-C11607
Photo-0016.jpg	08/06/05 11:22:32AM	08/06/05 11:22:32AM	12,286	12,286	2C-C11615
Photo-0017.jpg	08/06/05 01:53:32PM	08/06/05 01:53:32PM	16,008	16,008	2C-C11621
Photo-0018.jpg	08/25/05 08:45:30PM	08/25/05 08:45:30PM	12,356	12,356	2C-C11628
Photo-0019.jpg	08/27/05 09:18:30AM	08/27/05 09:18:30AM	13,988	13,988	2C-C11637
Photo-0020.jpg	08/30/05 11:41:30AM	08/30/05 11:41:30AM	20,528	20,528	2C-C11654
Photo-0021.jpg	08/31/05 01:16:30PM	08/31/05 01:16:30PM	16,242	16,242	2C-C11662
Photo-0022.jpg	08/31/05 01:16:30PM	08/31/05 01:16:30PM	16,246	16,246	2C-C11668
Photo-0023.jpg	08/31/05 01:16:30PM	08/31/05 01:16:30PM	12,696	12,696	2C-C11676
Photo-0024.jpg	08/31/05 01:17:30PM	08/31/05 01:17:30PM	15,144	15,144	2C-C11682
Photo-0025.jpg	08/31/05 01:17:30PM	08/31/05 01:17:30PM	11,880	11,880	2C-C11688
Photo-0026.jpg	08/31/05 01:17:30PM	08/31/05 01:17:30PM	15,876	15,876	2C-C11692
Photo-0027.jpg	08/31/05 01:17:30PM	08/31/05 01:17:30PM	15,676	15,676	2C-C11698
Photo-0028.jpg	08/31/05 01:19:30PM	08/31/05 01:19:30PM	16,740	16,740	2C-C9844
Photo-0029.jpg	08/31/05 01:19:30PM	08/31/05 01:19:30PM	16,090	16,090	2C-C11647
Photo-0030.jpg	08/31/05 02:22:30PM	08/31/05 02:22:30PM	6,812	6,812	2C-C11675
Photo-0031.jpg	09/02/05 07:39:30PM	09/02/05 07:39:30PM	10,426	10,426	2C-C11708
Photo-0032.jpg	09/03/05 09:35:30AM	09/03/05 09:35:30AM	14,272	14,272	2C-C11712

Below the file explorer, a hex editor window is open, showing the raw data of a file. The hex editor displays a sequence of bytes in hexadecimal and their corresponding ASCII characters. The data appears to be a corrupted or partially decoded image file, with recognizable patterns like 'JpA2A2' and 'h-o-t-o' visible in the ASCII column.

Neceloviti podatki

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



The screenshot shows the nodebrowser interface for a SonyEricsson_K800i device. The left pane displays a hierarchical file system tree, and the right pane displays a table of files.

Name	Size	Accessed time	Changed time	Modified time	Module
def_acc.dat	691	4/4/2010 12:00:00 AM	12:00:00 AM	4/4/2010 8:58:54 AM	Fat File System
_ELCOM-5	0	3/16/2010 12:00:00 AM	12:00:00 AM	3/16/2010 12:18:56 PM	Fat File System
SA gmail	0	3/16/2010 12:00:00 AM	12:00:00 AM	3/16/2010 12:20:02 PM	Fat File System
Mv	0	3/29/2010 12:00:00 AM	12:00:00 AM	3/29/2010 10:49:48 AM	Fat File System

Oblika datoteke SMIL

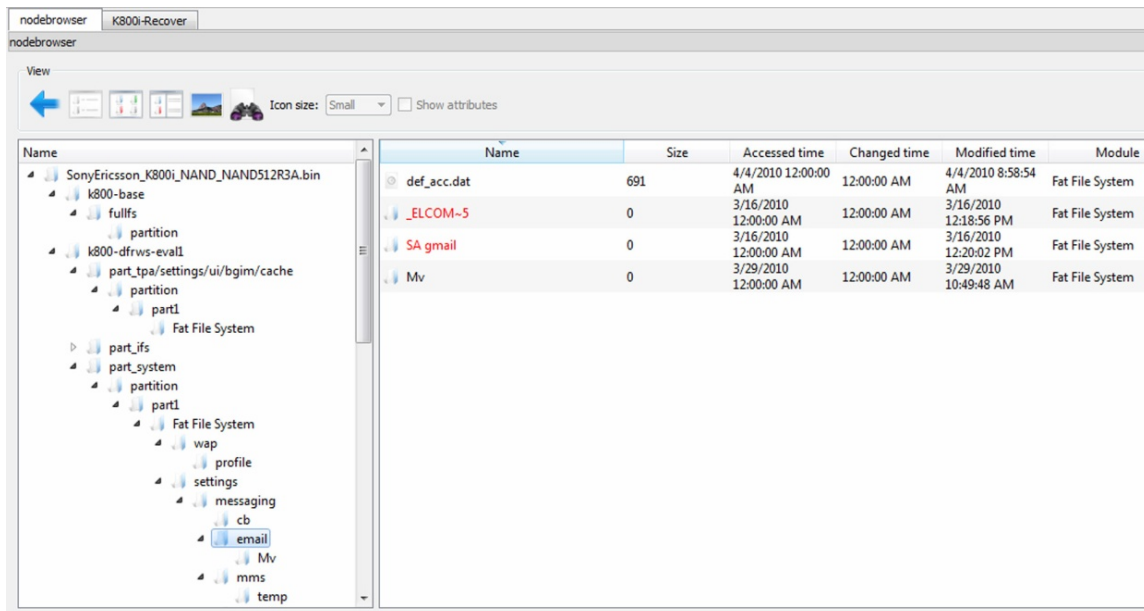
- *Synchronized Multimedia Integration Language*
 - del W3C standarda - <http://www.w3.org/AudioVideo/>
 - inačice 1, 2 in 3 (<http://www.w3.org/TR/SMIL3/>)
- vključuje SVG predmete (povečljiva vektorska grafika, *Scalable Vector Graphics*)
- omogoča:
 - animacijo, vključevanje drugih slik, modularizacijo,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

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^[2]

	0x00	0x10	0x20	0x30	0x40	0x50	0x60	0x70
0x00	@	Δ	SP	0	i	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	≡	*	:	J	Z	j	z
0x0B	∅	ESC	+	;	K	Ä	k	ä
0x0C	ø	Æ	,	<	L	Ö	l	ö
0x0D	CR	æ	-	=	M	Ñ	m	ñ
0x0E	Å	β	.	>	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 12036452774 se shrani kot 2130462577F4 (F je polnilo)

Preiskava – SIM kartica.

- SIM (*Subscriber Identity 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

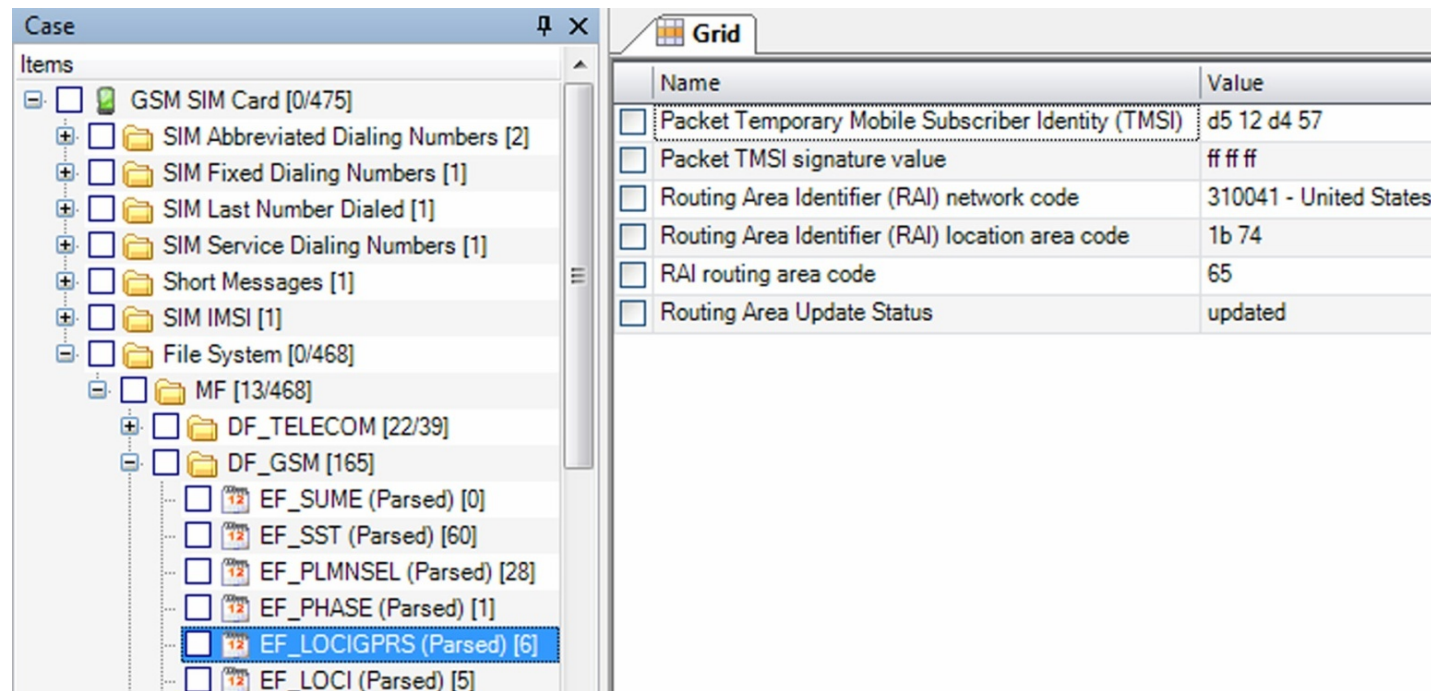
- nekatere datoteke so definirane v standardu
 - 3F00:7F10 (DFTELECOM, *dedicated file*): zapisi o uporabi storitev (npr. poslana SMS sporočila, klicane številke, ...)
 - 3F00:2FE2 (EFICCID, *elementary file*): hrani ICC-ID (*Integrated Circuit Card ID*)
 - 3F00:7F20:6F07 EFIMSI: hrani IMSI (*International 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 posodablano, a za branje SIM kartic je v redu

SIM kartica

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



The screenshot displays a forensic analysis interface. On the left, a tree view titled 'Case' shows a file system structure. The 'GSM SIM Card' folder is expanded, revealing sub-folders for dialing numbers, short messages, and IMSI. The 'File System' folder is also expanded, showing a 'MF' folder containing several 'DF' folders, with 'DF_GSM' further expanded to show 'EF' files. The 'EF_LOCI (Parsed) [6]' file is selected. On the right, a 'Grid' window displays a table of data extracted from the selected file.

Name	Value
Packet Temporary Mobile Subscriber Identity (TMSI)	d5 12 d4 57
Packet TMSI signature value	ff ff ff
Routing Area Identifier (RAI) network code	310041 - United States
Routing Area Identifier (RAI) location area code	1b 74
RAI routing area code	65
Routing Area Update Status	updated

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.

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

