

# Digital forensics

Andrej Brodnik

# Cell (mobile) phones

*chapter 20*

- various technologies of data transfer
- sometimes mostly phones, today mostly computers
- rich source of personal data
  - call history (incoming, outgoing and missed)
  - SMS and MMS history (received and sent)
  - history of location data
  - images, journals, calendars, ...
  - access to the web networks – shortly, all the data which is also found on usual computers

# Data on the cell phone

- Example (POCKET-DIAL M FOR MURDER):  
*The perpetrator had a phone in his pocket during the crime, which has pocket-dialed cellphone of his wife, who was the victim of the crime. On the wife's phone, the call went to voicemail and it was recorded.*
- Computational power of mobile devices is increasing because they contain much more I/O devices
  - thermometers
  - accelerometers
  - credit card scanners
  - ...
  - use of these units went beyond the manufacturer's intentions; e.g. at certain temperature some action is triggered
- phones became one type of *embedded systems*

# Mobile device forensics

- devices have more capable operation systems
  - Android
  - iPhone
  - Blackberry
  - Windows Mobile
- and older operation systems (SYMBIAN, ...)

# Mobile device forensics

- devices are by the definition network devices
  - GPRS, CDMA, UMTS, ...
  - IEEE 802.11
  - IEEE 802.15 (Bluetooth)
  - Infrared communication
  - ...
- access to the device may destroy or modify the evidence material

# Mobile device forensics

- data is usually saved in storage media
  - it cannot be deleted, but it can be copied
  - due to the limited number of writes, writing algorithms spread data across storage media
  - that is why we can get a lot of data that seems to be deleted

# Mobile device forensics

- data acquiring from device
  - usually using cable connected to the data port
    - protocol knowledge needed
  - sometimes a direct capture from the storage media is required
    - direct reading from chip

# Mobile device forensics

- devices are made from two parts
  - device itself
  - SIM cards
- device has unique identification number  
IMEI (*International Mobile Equipment Identity*)





# Mobile device forensics

- SIM cards are computers
  - CPU, ROM, RAM
- contain ICC-ID (*Integrated Circuit Card Identifier*):
  - MCC (*mobile country code*),
  - MNC (*mobile network code*),
  - serial number of card



# SIM cards

- *Challenge: Which data SIM card also contains?*
- *Challenge: What is LAI and what is IMSI?*
- *Challenge: What your SIM card has? What are the values of this data? What is the identification of your mobile device?*

# Data about and on the device

- on device – depends on the type of the device:
  - baseline phone
  - smart phone
- where the data is also stored:
  - user's computer
  - operator
  - SIM card
- on device are at least stored:
  - titles
  - incoming, outgoing and missed calls
  - received and sent SMS

# SMS as digital evidence

- full information: when is sent/received, from who and content
- no record of when messages were first read

example of data acquired using BitPim (<http://www.bitpim.org/>)

The screenshot shows the BitPim software interface. On the left is a tree view of phone data categories: Phone, PhoneBook, Media, Calendar, Memo, Todo, SMS (with sub-items: Inbox, Sent, Saved), Call History, Play List, T9 Editor, and Log. The main window displays a table of SMS messages under 'Current Data'. The selected message is highlighted in blue.

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>

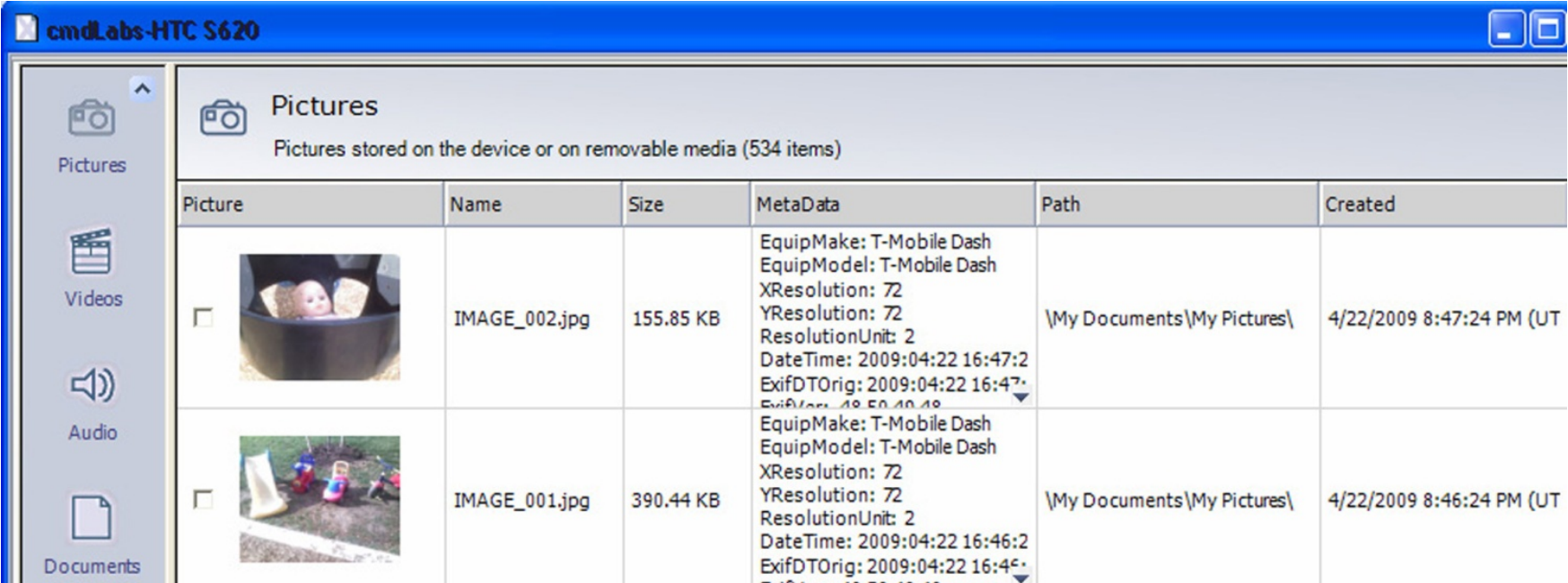
From: H Cell(cell)  
Callback #:   
Subject: <None>  
Date: 2008-12-08 00:25:23  
Priority: Normal  
Read?:   
Locked:



Memo  
GO STEELERS.

# Image data

- smart phones have cameras
- Image data is in EXIF record (usually)

Example of data acquired from Windows Mobile device using 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 XResolution: 72 YResolution: 72 ResolutionUnit: 2 DateTime: 2009:04:22 16:47:2 ExifDOrig: 2009:04:22 16:47:2 ExifDate: 2009:04:22 16:47:2	\\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 ExifDate: 2009:04:22 16:46:2	\\My Documents\\My Pictures\\	4/22/2009 8:46:24 PM (UT)

# Access to the Internet services

- mobile devices enable access to the web
  - often user saves passwords there
  - there is history of entries
  - logs of the last entries
  - ...
- mobile devices enable e-mail reading
  - passwords to access mailboxes
  - last received / sent mails
  - ...
- other applications and their data

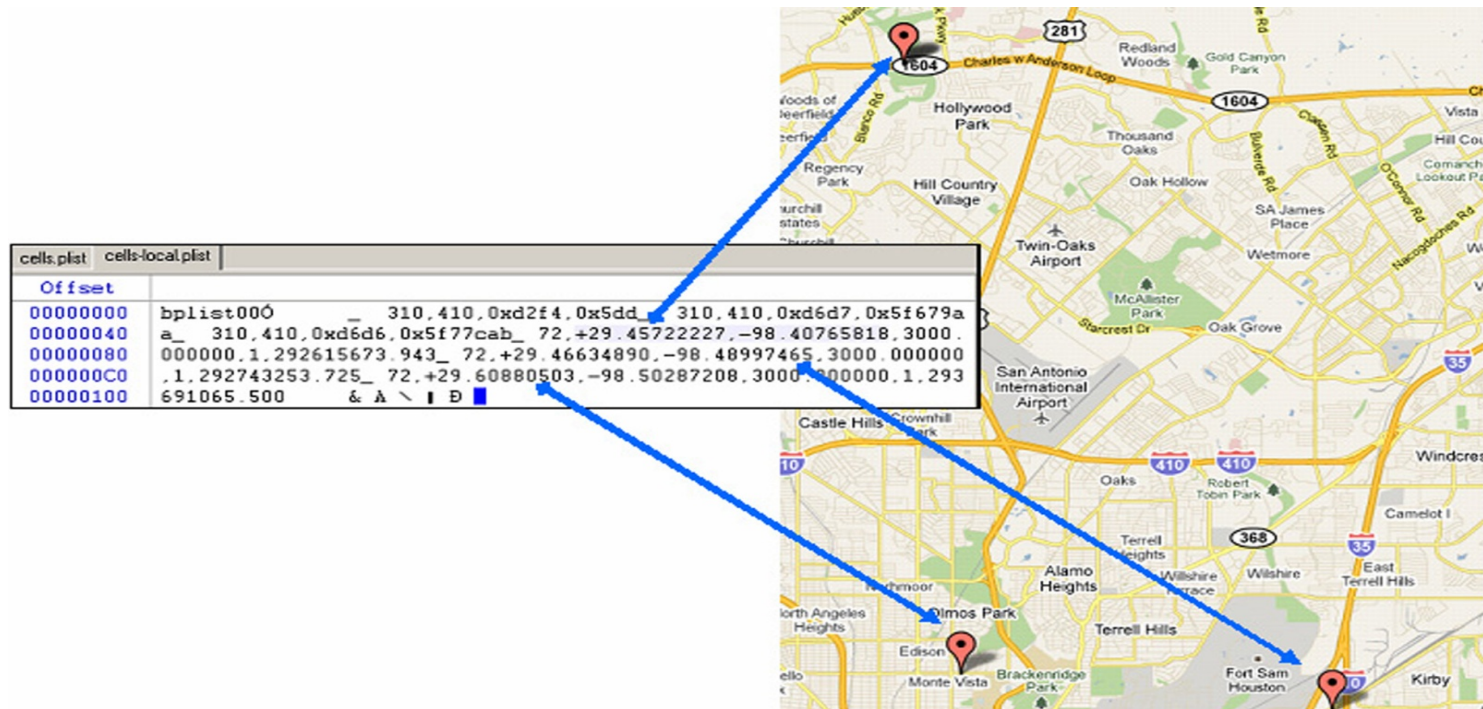
# Access to the Internet services

- example of data on an 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
```

# Location Information

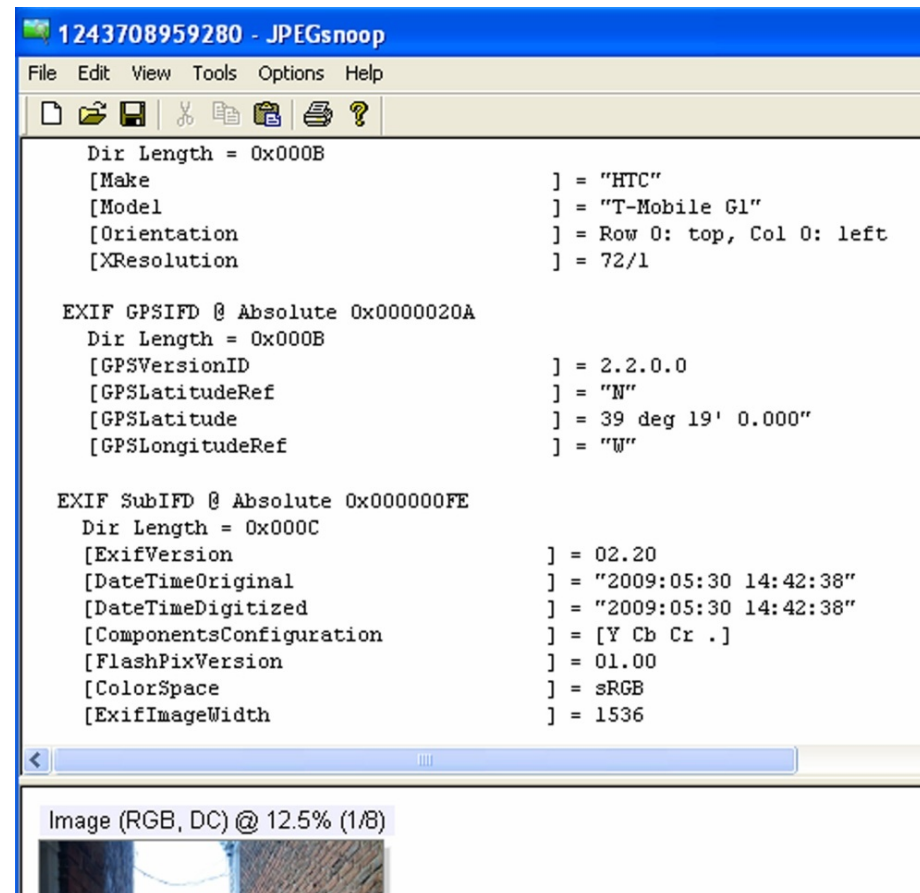
- history of moving between cellular towers can be saved
- GPS devices can save exact coordinates





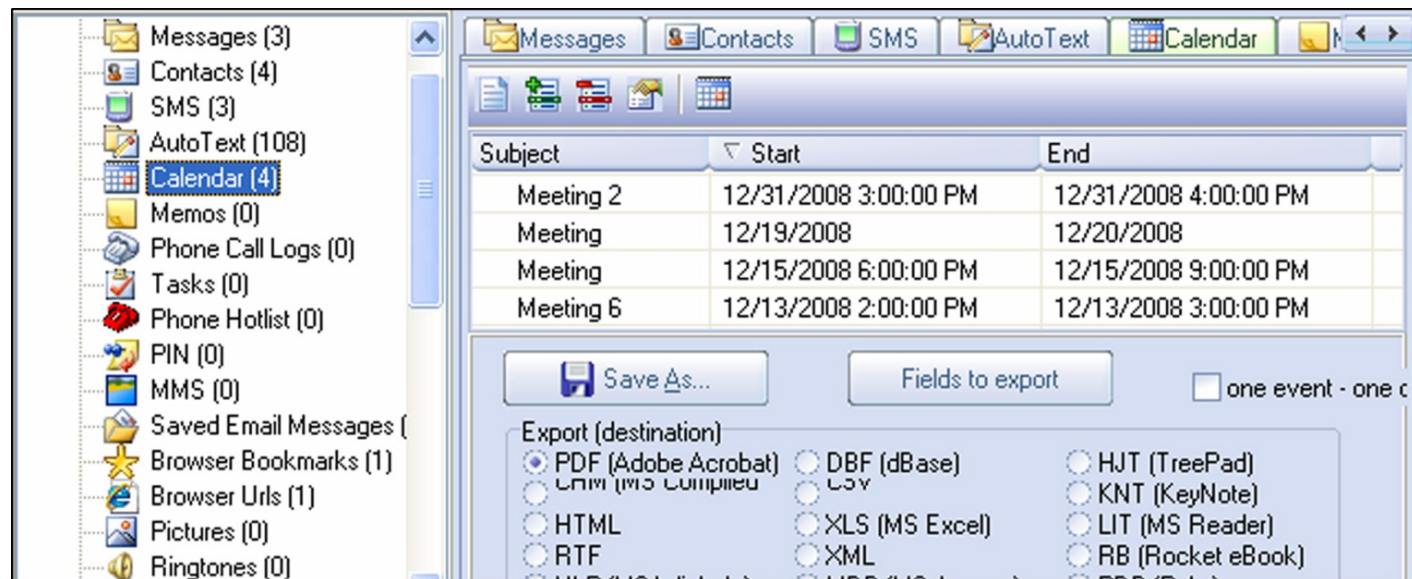
# Location Information

- images can save information such as when and where they were taken
  - e.g. EXIF format
- *Challenge: search for location information in your phone.*



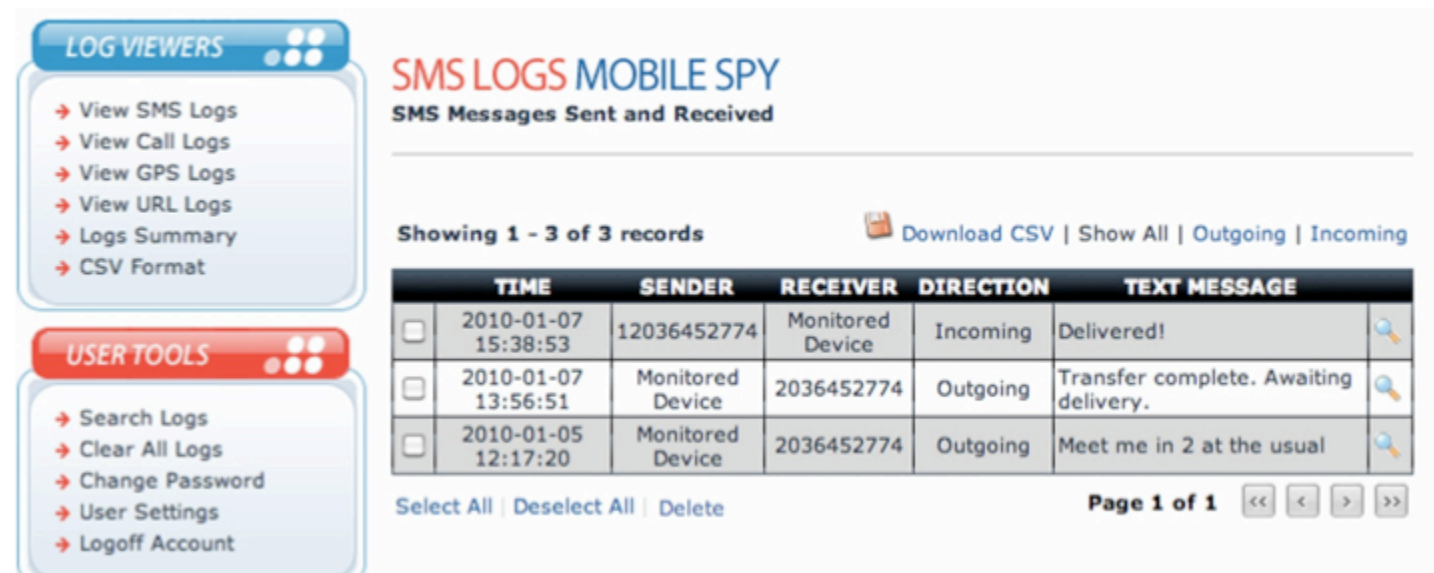
# Other data

- calendar, notes, ...
- *Challenge: search for calendar data in your phone.*



# Attacks on mobile devices

- the attacker loads his code on the device
  - through the network
  - the user uploads an application that seems useful and friendly ([http://www.theregister.co.uk/2010/01/11/android\\_phishing\\_app/](http://www.theregister.co.uk/2010/01/11/android_phishing_app/))
- the application reads passwords, ...
  - allows the attacker to access to bank accounts ...
  - see MobileSpy (<http://www.mobile-spy.com/>)



The screenshot displays the 'SMS LOGS MOBILE SPY' 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 controls for 'Select All', 'Deselect All', and 'Delete', and a pagination bar showing 'Page 1 of 1'.

**LOG VIEWERS**

- View SMS Logs
- View Call Logs
- View GPS Logs
- View URL Logs
- Logs Summary
- CSV Format

**USER TOOLS**

- Search Logs
- Clear All Logs
- Change Password
- User Settings
- Logoff Account

**SMS LOGS MOBILE SPY**  
SMS Messages Sent and Received

Showing 1 - 3 of 3 records [Download CSV](#) | [Show All](#) | [Outgoing](#) | [Incoming](#)

	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	

[Select All](#) | [Deselect All](#) | [Delete](#) Page 1 of 1

# Attacks on mobile devices

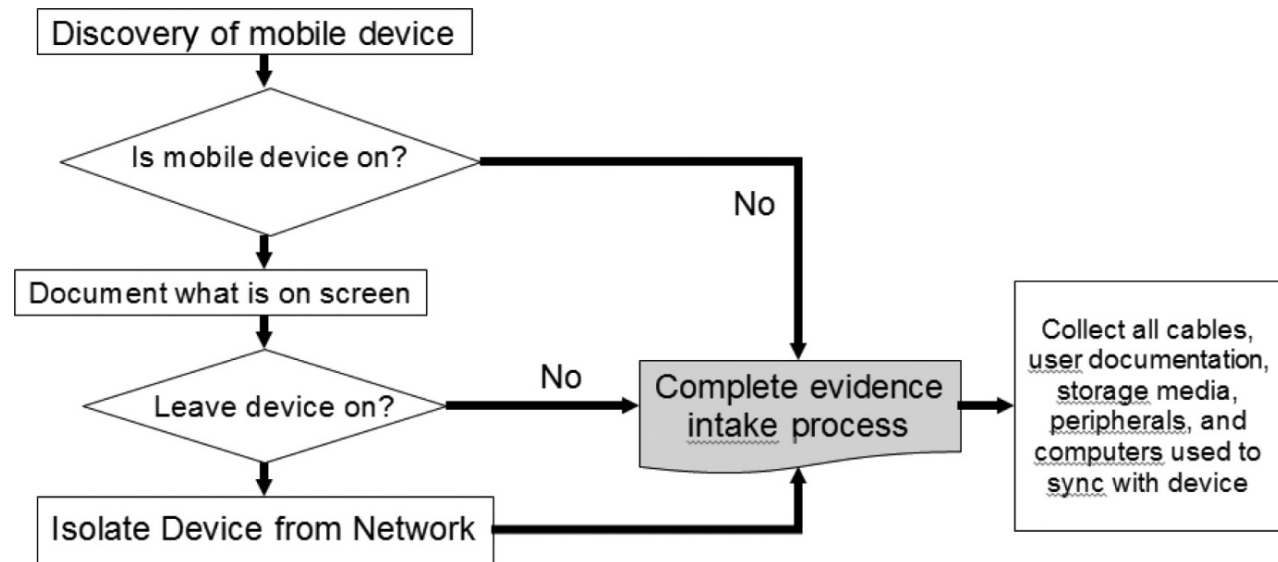
- *Challenge:* How does the MobileSpy work?
- *Challenge:* Find the software that can harm your Android system?
- *Challenge:* Make your own program that reads data on Android (iPhone) system. Can this also be useful software?

# Thinking Outside of the Device

- additional data:
  - user's computer
  - operator: call center and base stations
- devices, user knows something about (transitivity)

# Handling Mobile Devices

- the device can wirelessly connect with world
- disable
  - remove power
  - other ways



# Handling Mobile Devices

- remove storage module
  - storage modules are always smaller
- usually FAT file system
  - iPhone: APFS, Android: Linux design
- otherwise usual procedures (signature, journals, ...)



# Accessing the data

- different methods of accessing with different types
  - not every device has USB guide
- examples:
  - via user interface
  - via communication port
  - property interface (Nokia F-BUS, *Flash BUS*)
  - via JTAG (*Joint Test Action Group*) interface
  - via direct memory chip access

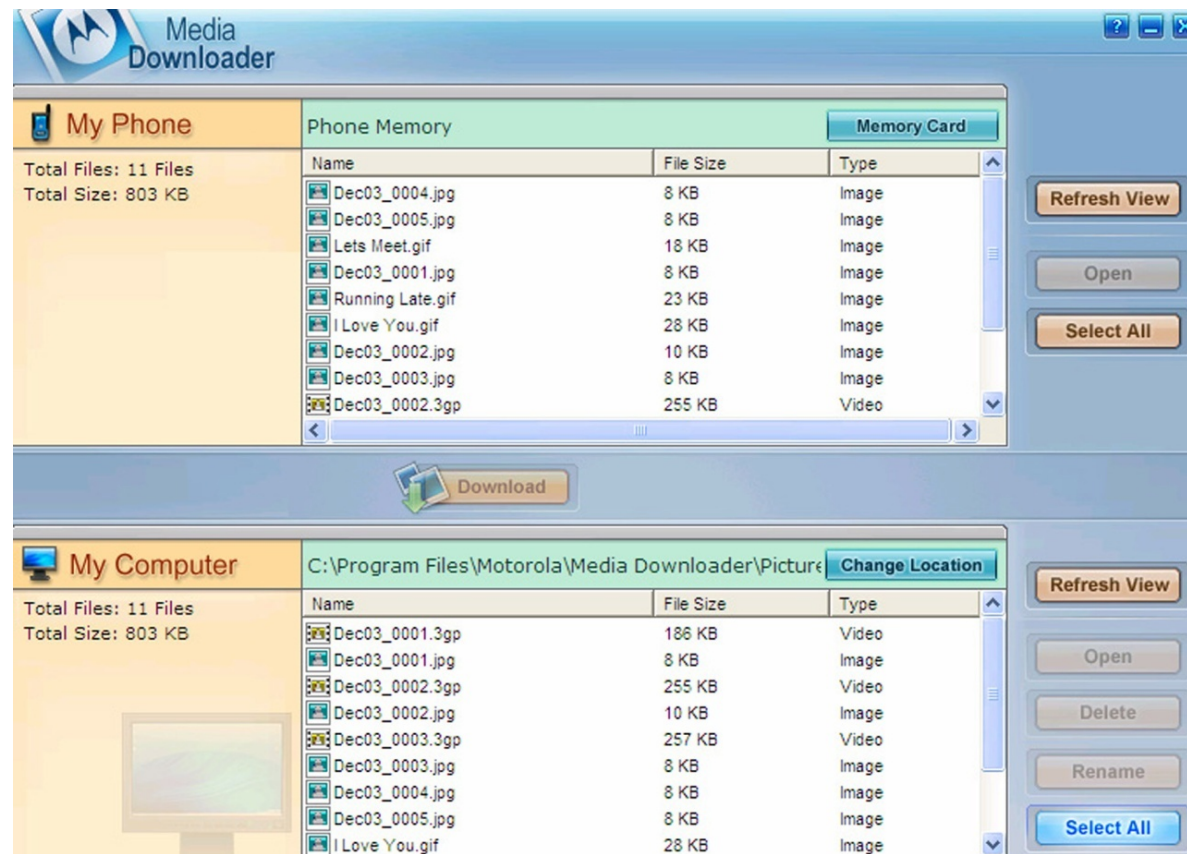


# Accessing the data

- some devices provide agent access
  - when device is on, it runs the agent which takes over control of the device (iPhone)
- sometimes we can stop software launching and put our code as further upload
- manufacturers offer data archiving software which also provides access to deleted and other data

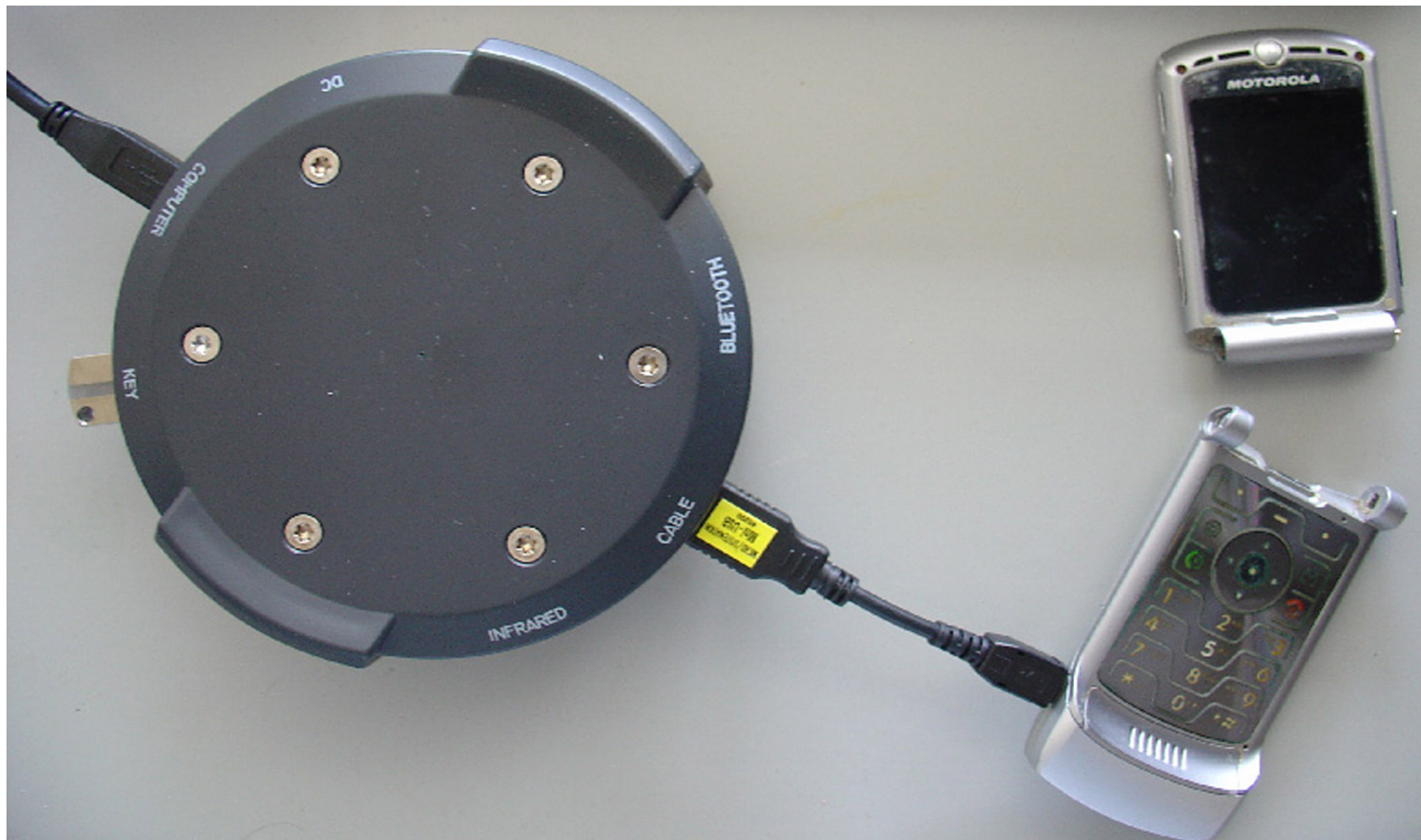
# Examples ...

- example of stored data with an archive using XACT (Motorola device)



# Examples ...

- device, which is partly broken, it may still work well enough



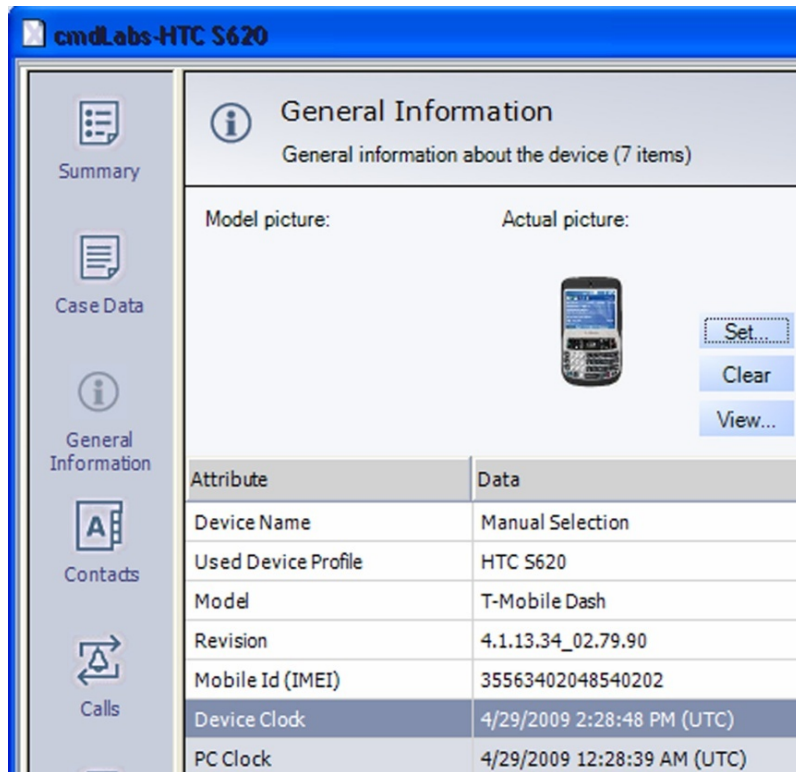
# Mobile Device Forensics Tools

- any tool allows access to the device memory (for example disk)
- in the case of a disk, access is relatively safe because it cannot change content by itself
- in case of mobile device that is not necessarily true

# Mobile Device Forensics Tools

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

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



The screenshot shows the cmdLabs-HTC S620 software interface. The title bar reads "cmdLabs-HTC S620". The left sidebar contains navigation 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)



# Mobile Device Forensics Tools

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

- MOBILedit! Forensic  
(<http://mobiledit.com/>)
- programming equipment  
for analysis



# Mobile Device Forensics Tools

- 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)".

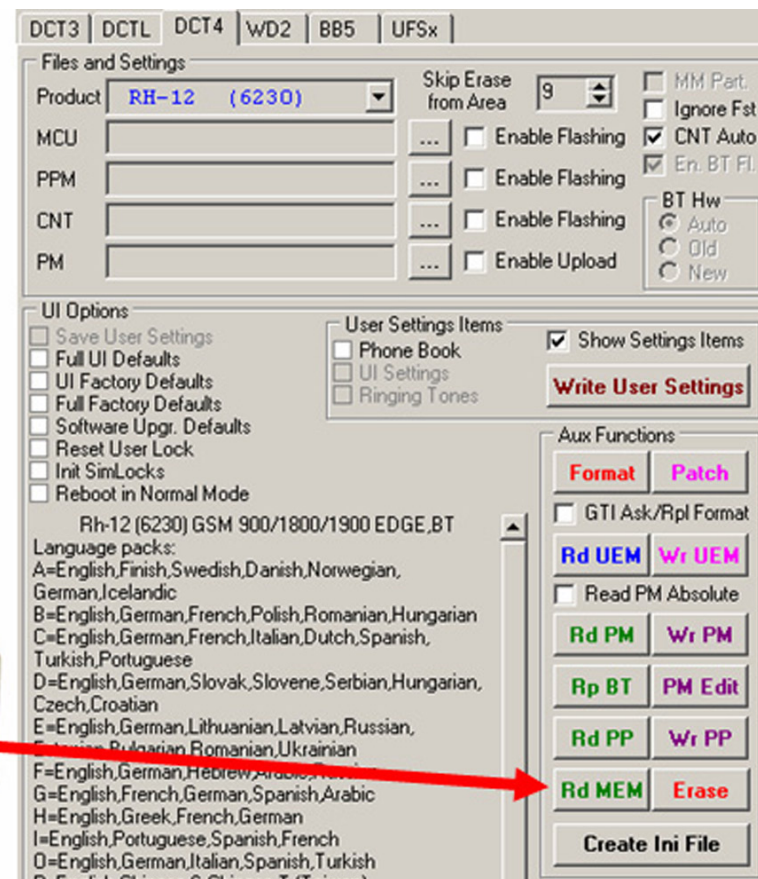
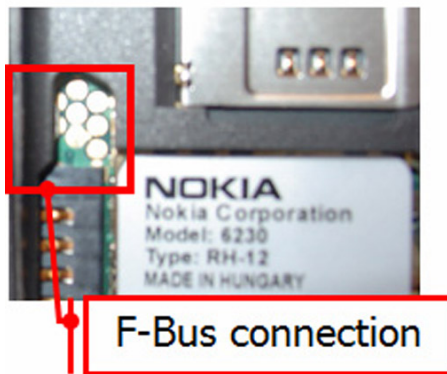
The interface is divided into several sections:

- Exhibit Details:** Case ID: 201101001, Exhibit Reference: 0001.
- Acquisition Details:**  /dev/rdisk0s1 (500.00MB),  /dev/rdisk0s2 (14.64GB). A list of data categories includes:  All Live Data,  Images,  Video,  Music,  Telephony Data,  PIM Data,  E-Mail Data,  Location Data,  Internet Data,  Captured Images,  Uploaded Images,  Application Data.
- Hashing Details:**  MD5,  RIPMD160,  SHA-1,  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", "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".

# Mobile Device Forensics Tools

## Twister Flasher





# File System Examination

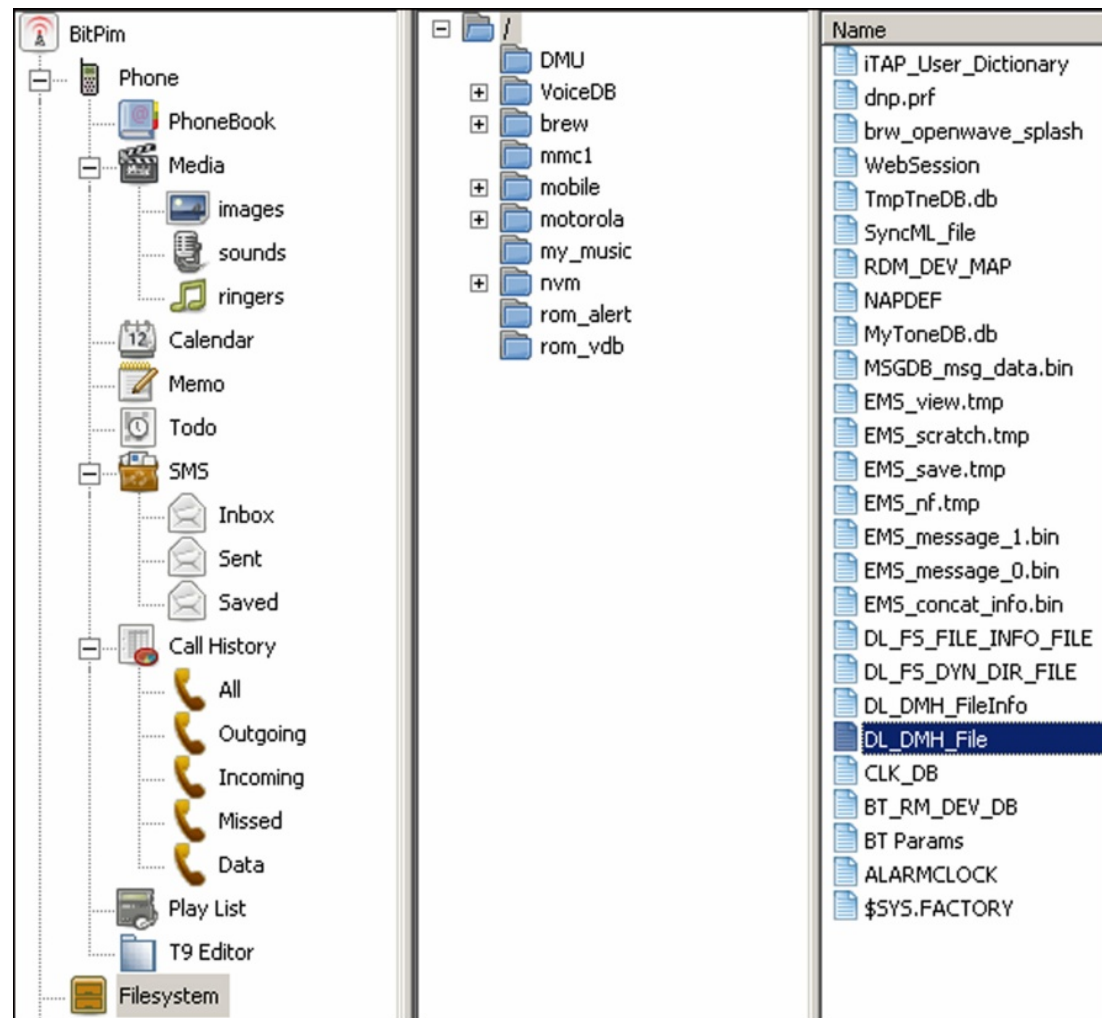
- depends on device
  - unique
  - built in systems Qualcomm (BREW, Binary Runtime Environment for Wireless)
  - FAT, ext2, ext3, HSFx, APFS, ...
- various tools are available:

# Some basic tools ...

BitPim

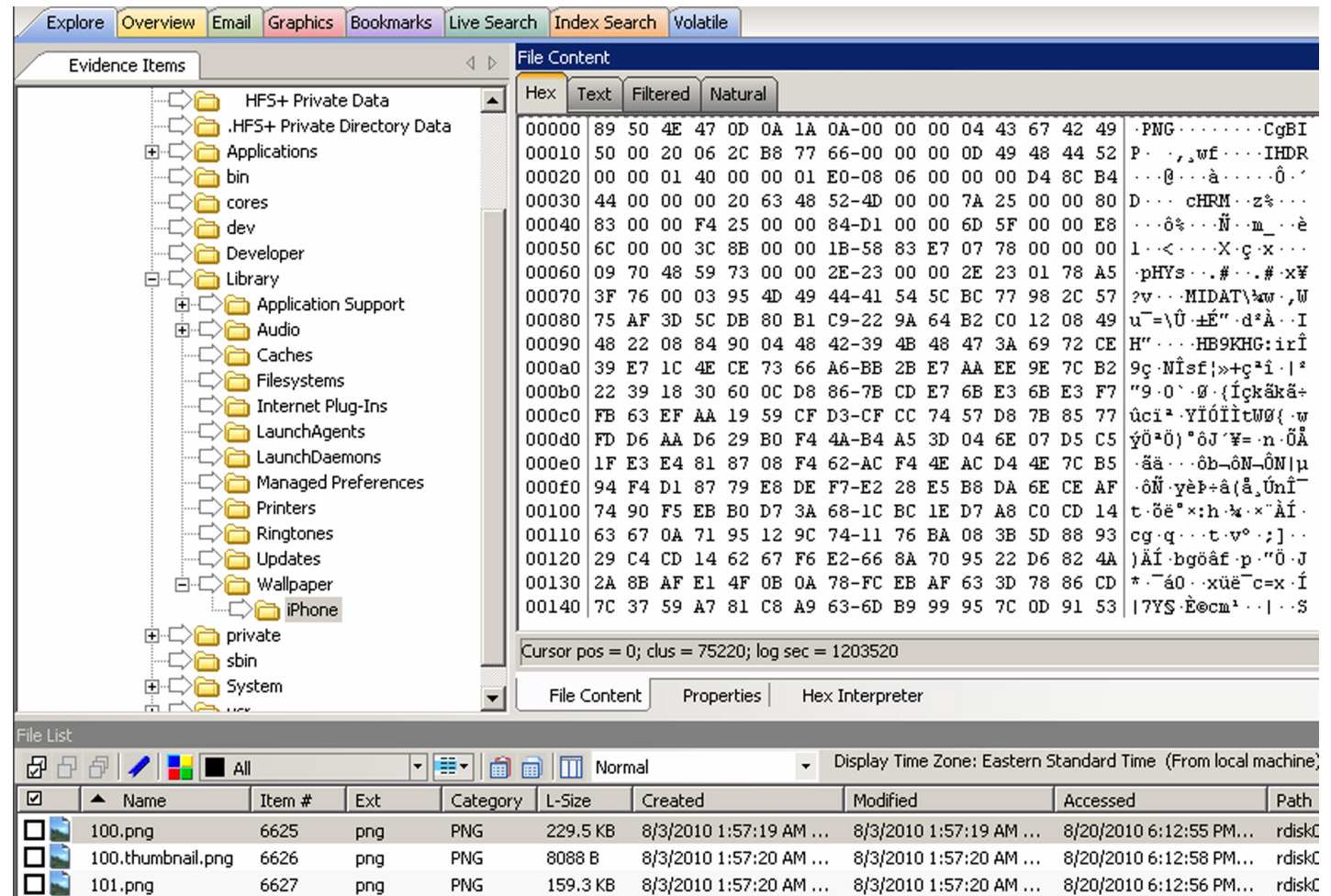
(<http://www.bitpim.org/>) –

Motorola CDMA



# Some basic tools ...

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



# Data recovery

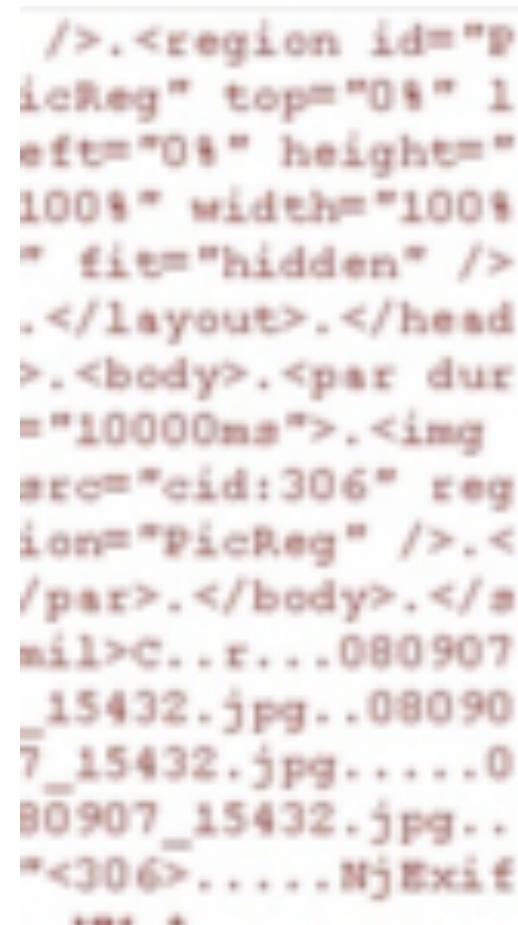
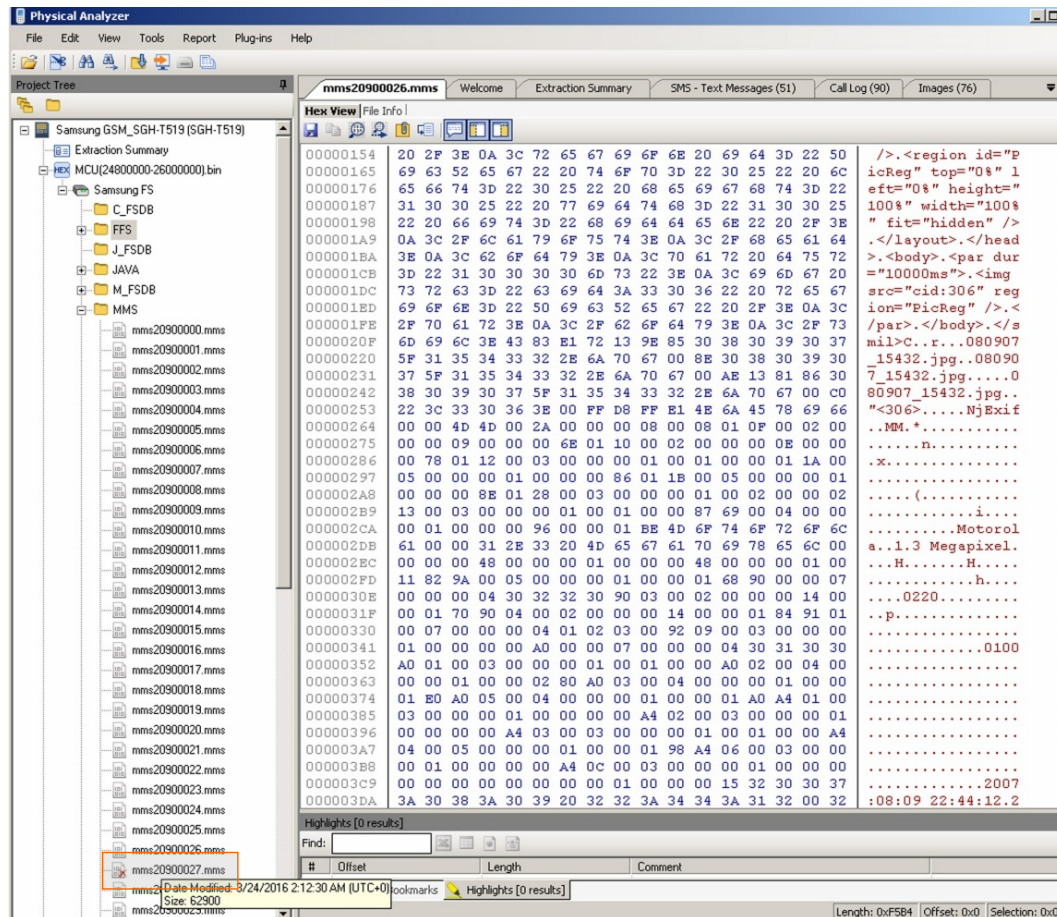
- even if we don't have all the data we can recover partly deleted data from logical data

MMS937483931.PDU	
Offset	
00000000	1  Application/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 4 mdat ¶ ÅpÅÅX8áä "9È  5 0-xÜ
00000200	Ðæ +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  >ðW S p «aãZ



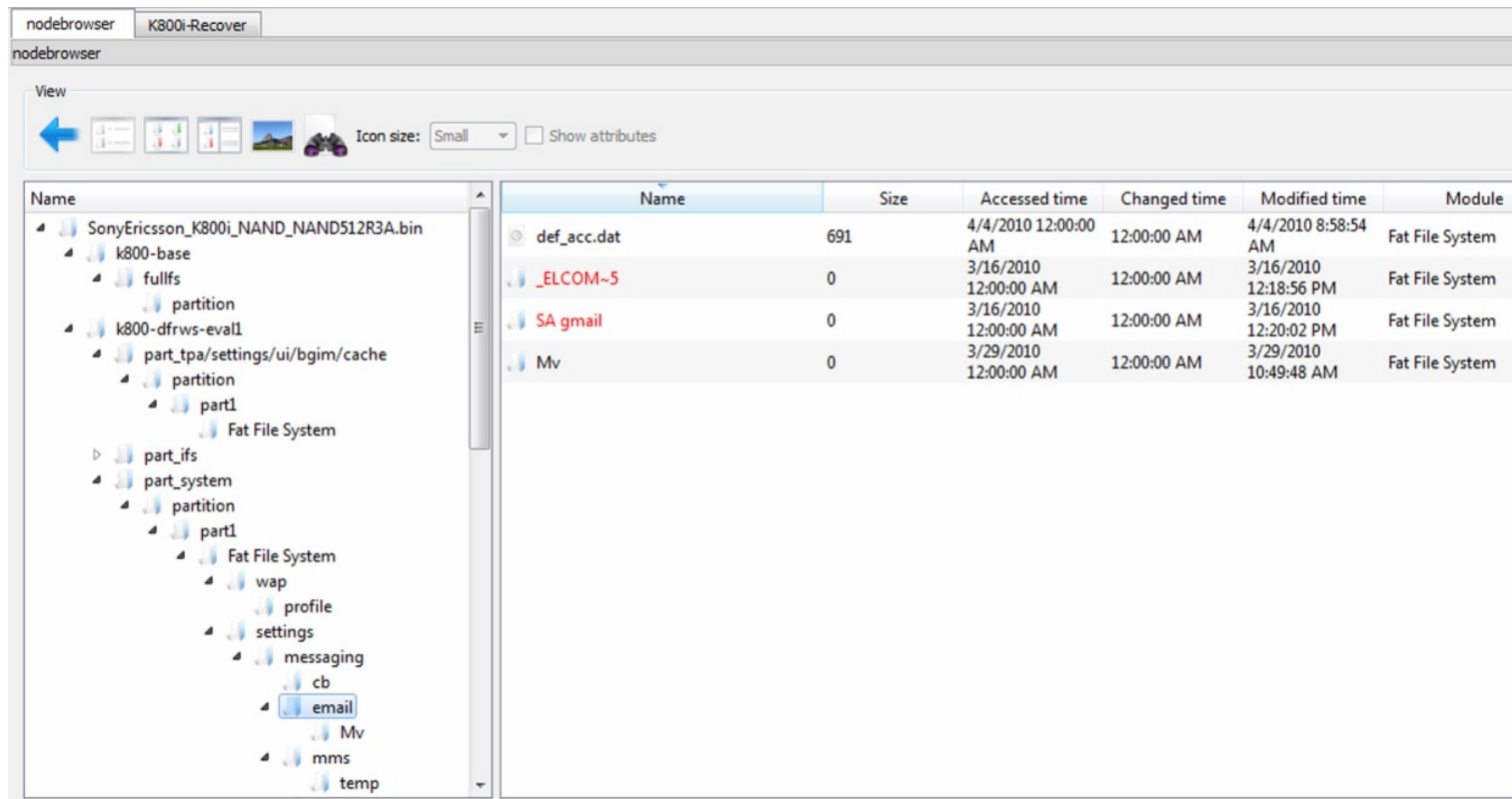
# Data recovery

- In this example of composite files (MMS, docx, ...) we can find parts of data



# Data recovery

- Example of data captured using DFF (*Digital Forensic Framework*, <http://www.digital-forensic.org/>)
- *Challenge: Study the enironment and how it is spread*



The screenshot shows the nodebrowser interface for a SonyEricsson\_K800i NAND. The left pane displays a tree view of the file system, including folders like 'k800-base', 'k800-dfrws-eval1', and 'part\_system'. The right pane shows a table of files with columns for Name, Size, Accessed time, Changed time, Modified time, and Module.

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

# Data Format SMIL

- *Synchronized Multimedia Integration Language*
  - part of W3C standard - <http://www.w3.org/AudioVideo/>
  - versions 1, 2 in 3 (<http://www.w3.org/TR/SMIL3/>)
- includes SVG items (enhanced vector graphics, *Scalable Vector Graphics*)
- allows:
  - animation, integration of other images, modularization, ...
- *Challenge: Find SMIL file and study it.*
- *Challenge: Make your SMIL file and send it to the forum.*

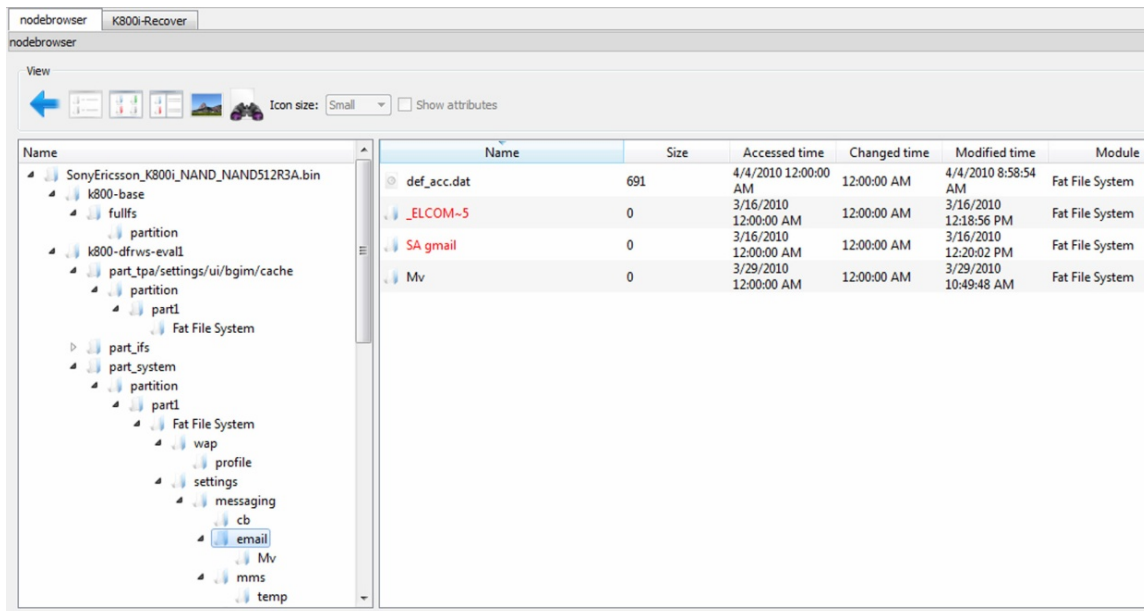


# Data recovery

- SSD is used as storage
- Data, which are in storage, but not structured
  - Partly deleted data
  - Data in deleted blocks which are scattered per unit
- *Challenge: look up forensic challenge and solution DRFWS2010 (Digital Forensic Research Conference) – <http://www.dfrws.org/2010/challenge/>*
  - Examples of files with the unit are available
- *Challenge: look up forensic challenge and solution DRFWS2011 – <http://www.dfrws.org/2011/challenge/>*
- *Challenge: look up forensic challenge DRFWS2012 – <http://www.dfrws.org/2012/challenge/>*

# Examination – other data

- A lot of smart phones saves their data in data base
  - SQLite – Android, iPhone, Palm, ...
  - cemail.vol – Windows Mobile



# Examination – data formats

- mostly standard formats:
  - 7-bit standard; GSM 03.38: 160 characters
  - 16-bit UCS-2 (*Universal Character Set*, UTF-16): 70 characters

**Basic Character Set<sup>[2]</sup>**

	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	Ø	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<sup>[2]</sup>**

	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			\					

# Examination – data formats

- big and little endian – depending on the processor
  - Motorola – big-endian format
- **debeli in tanki košček (*nibble*)**
  - number 12036452774 is saved as 2130462577F4 (F is filler)

# Examination – SIM card

- SIM (*Subscriber Identity Module*)
- device is property of user, SIM card is owned by the operator
  - which allows the user to store certain data on it
- detailed definition in:
  - ETSI (*European Telecommunications Standards Institute*): *GSM, Global Mobile Communications*, GSM 11.11, 1995.
  - [www.ttfn.net/techno/smartcards/gsm11-11.pdf](http://www.ttfn.net/techno/smartcards/gsm11-11.pdf)

# SIM card

- very simple interior structure
- it consists of files and each file has its own identification 2-byte code
- first byte represents type of file:
  - 3F –Master File MF
  - 7F –Dedicated File, DF
  - 2F – partial file MF
  - 6F – partial file 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 card

- Some files are defined in the standard
  - 3F00:7F10 (DFTELECOM, *dedicated file*): records on the use of services (i.e. sent SMS, dialed numbers, ...)
  - 3F00:2FE2 (EFICCID, *elementary file*): saves ICC-ID (*Integrated Circuit Card ID*)
  - 3F00:7F20:6F07 EFIMSI: saves IMSI (*International Mobile Subscriber Identity*)
  - 7F20:6F7E (EFLOCI): how the card was moving between operators
  - 7F20:6F53 (EFLOCIGPRS): GPRS routing area

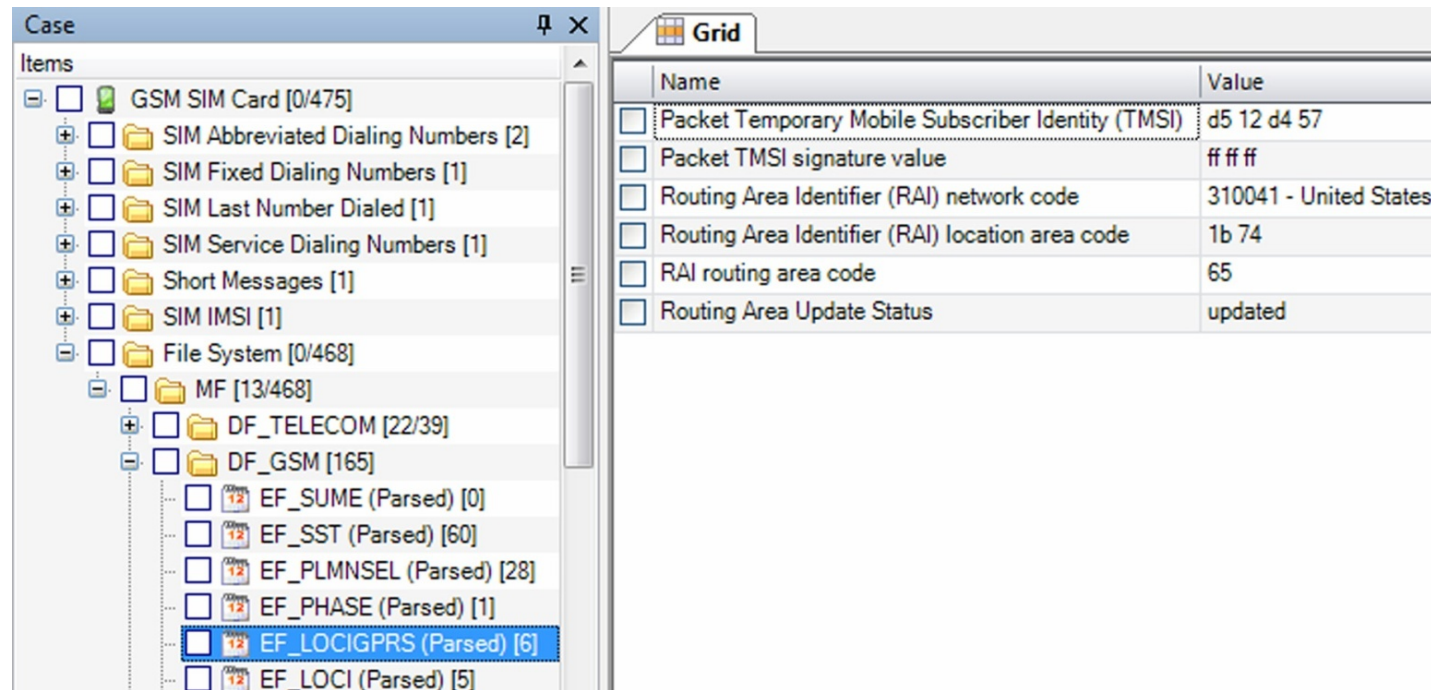
# SIM card

- tools for examining SIM card:
  - TULP2G: *Netherlands Forensic Institute*
  - <http://tulp2g.sourceforge.net/>
  - tool is not updated but it is fine for reading of the SIM card



# SIM card

- example of information from SIM card (*Paraben Device Seizure*)



The screenshot displays a forensic analysis tool interface. On the left, a tree view under 'Case' shows a hierarchy of items. The 'GSM SIM Card [0/475]' folder is expanded, showing sub-folders like 'SIM Abbreviated Dialing Numbers [2]', 'SIM Fixed Dialing Numbers [1]', 'SIM Last Number Dialed [1]', 'SIM Service Dialing Numbers [1]', 'Short Messages [1]', 'SIM IMSI [1]', and 'File System [0/468]'. Under 'File System', there is an 'MF [13/468]' folder containing 'DF\_TELECOM [22/39]' and 'DF\_GSM [165]'. Under 'DF\_GSM', several files are listed, including 'EF\_SUME (Parsed) [0]', 'EF\_SST (Parsed) [60]', 'EF\_PLMNSEL (Parsed) [28]', 'EF\_PHASE (Parsed) [1]', 'EF\_LOCIGPRS (Parsed) [6]' (which is selected), and 'EF\_LOCI (Parsed) [5]'. On the right, a 'Grid' pane shows the details for the selected item. The grid has two columns: 'Name' and 'Value'. The data is as follows:

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 card

- *Challenge:* How can I access the data on your SIM card?
- *Challenge:* Is the entire GPRS history saved?
- *Challenge:* naštejajte **EF**, v katere lahko piše uporabnik. List the EF in which user can write.

# SIM card and security

- card is protected with PIN (*Personal Identification Number*) code
- if you make too many mistakes (cannot be checked), the card locked itself
- for unlocking we need PUK (*PIN Unlock Key*) code
  - often operator has it

