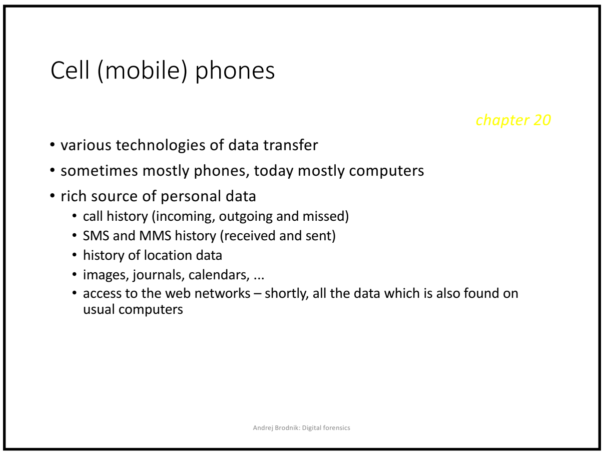
Digital forensics

Andrej Brodnik

Andrej Brodnik: Digital forensics

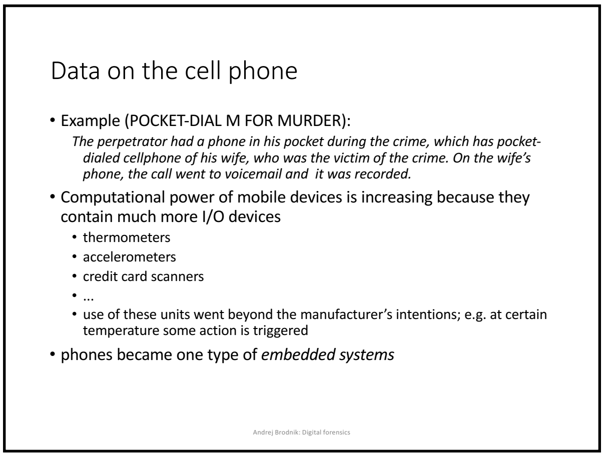


Cell (mobile) phones

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

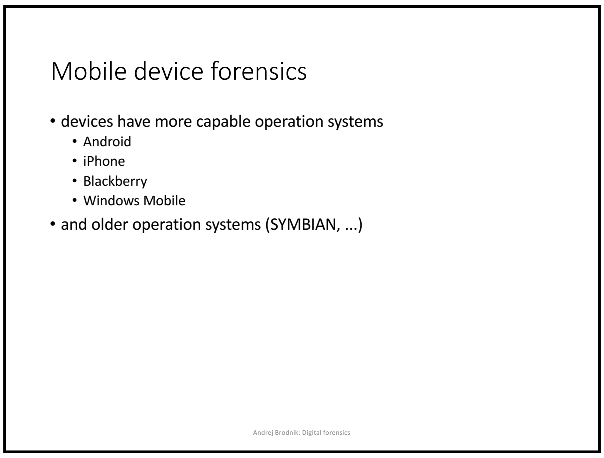
Andrej Brodnik: Digital forensics



Data on the cell phone

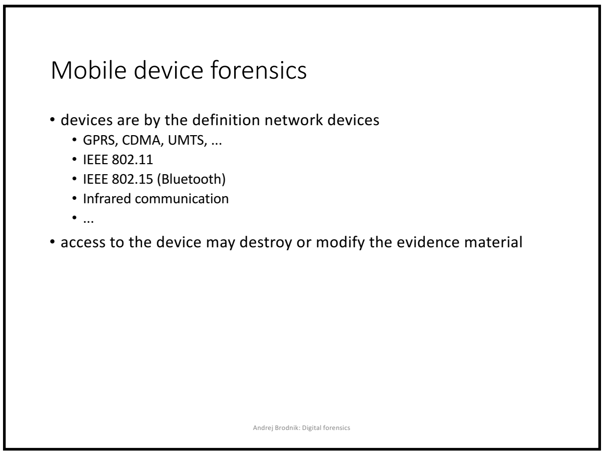
- Example (POCKET-DIAL M FOR MURDER):
  The perpetrator had a phone in his pocket during the crime, which has pocket-dialed cellphone of his wife, who was the victim of the crime. On the wife's phone, the call went to voicemail and it was recorded.
- Computational power of mobile devices is increasing 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*

Andrej Brodnik: Digital forensics



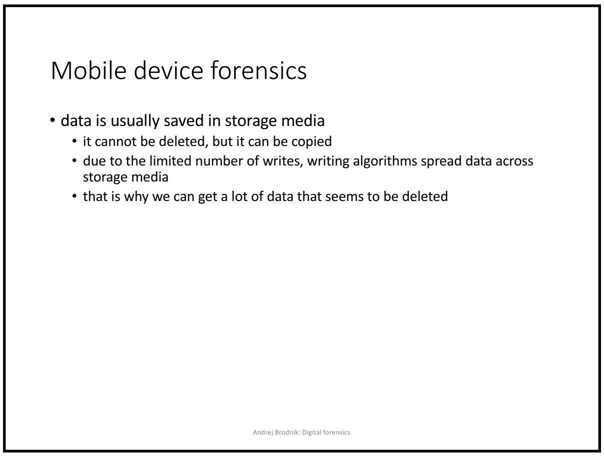
Mobile device forensics

- 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

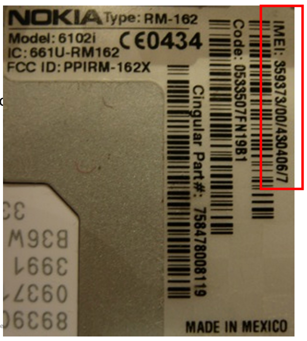
- data is usually saved in storage media
  - it cannot be deleted, but it can be copied
  - due to the limited number of writes, writing algorithms spread data across storage media
  - that is why we can get a lot of data that seems to be deleted

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 identificatio 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?

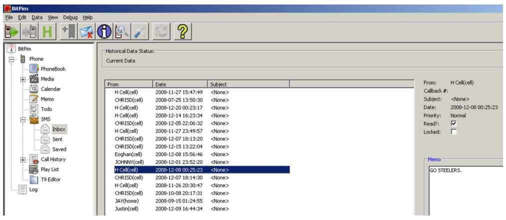
Data about and on the device

- 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/)



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>

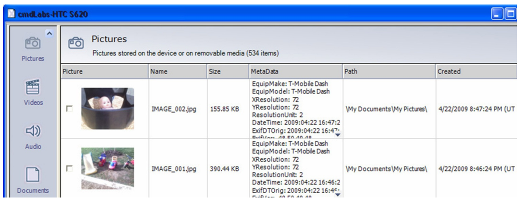
From: H Cell(cell)
Callback #:
Subject: <None>
Date: 2008-12-08 00:25:23
Priority: Normal
Read?: ☑
Locked: □

Memo
GO STEELERS.

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/)



cmdLabs-HTC S620

Pictures

Pictures stored on the device or on removable media (534 items)

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 ExifDTOrig: 2009:04:22 16:47	\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 ExifDTOrig: 2009:04:22 16:46	\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

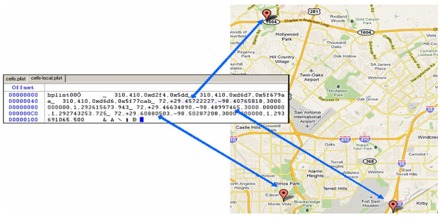
Access to the Internet services

- 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

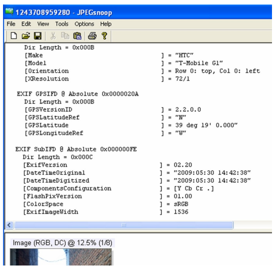
- history of moving between cellular towers can be saved
- GPS devices can save exact coordinates



```
cells.plist  cells-local.plist
Offset
00000000  bplist00Ó       _   310,410,0xd2f4,0x5dd_  310,410,0xd6d7,0x5f679a
00000040  a_  310,410,0xd6d6,0x5f77cab_ 72,+29.45722227,-98.40765818,3000.
00000080  000000,1,292615673.943_ 72,+29.46634890,-98.48997465,3000.000000
000000C0  ,1,292743253.725_ 72,+29.60880503,-98.50287208,3000.000000,1,293
00000100  691065.500      & À \ ▮ Đ █
```

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.*



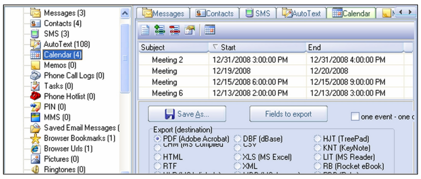
```
    Dir Length = 0x000B
    [Make                                ] = "HTC"
    [Model                               ] = "T-Mobile G1"
    [Orientation                         ] = Row 0: top, Col 0: left
    [XResolution                         ] = 72/1

  EXIF GPSIFD @ Absolute 0x0000020A
    Dir Length = 0x000B
    [GPSVersionID                        ] = 2.2.0.0
    [GPSLatitudeRef                      ] = "N"
    [GPSLatitude                         ] = 39 deg 19' 0.000"
    [GPSLongitudeRef                     ] = "W"

  EXIF SubIFD @ Absolute 0x000000FE
    Dir Length = 0x000C
    [ExifVersion                         ] = 02.20
    [DateTimeOriginal                    ] = "2009:05:30 14:42:38"
    [DateTimeDigitized                   ] = "2009:05:30 14:42:38"
    [ComponentsConfiguration             ] = [Y Cb Cr .]
    [FlashPixVersion                     ] = 01.00
    [ColorSpace                          ] = sRGB
    [ExifImageWidth                      ] = 1536
```

Other data

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

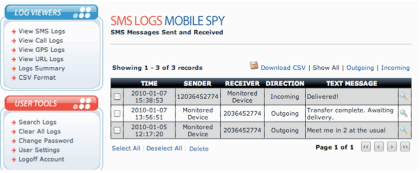


Subject	Start	End
Meeting 2	12/31/2008 3:00:00 PM	12/31/2008 4:00:00 PM
Meeting	12/19/2008	12/20/2008
Meeting	12/15/2008 6:00:00 PM	12/15/2008 9:00:00 PM
Meeting 6	12/13/2008 2:00:00 PM	12/13/2008 3:00:00 PM

Export (destination)
● PDF (Adobe Acrobat) ○ DBF (dBase) ○ HJT (TreePad)
○ CHM (MS Compiled ○ CSV ○ KNT (KeyNote)
○ HTML ○ XLS (MS Excel) ○ LIT (MS Reader)
○ RTF ○ XML ○ RB (Rocket eBook)

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/)
- the application reads passwords, ...
  - allows the attacker to access to bank accounts ...
  - see MobileSpy (http://www.mobile-spy.com/)



SMS LOGS MOBILE SPY

SMS Messages Sent and Received

Showing 1 - 3 of 3 records

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

Attacks on mobile devices

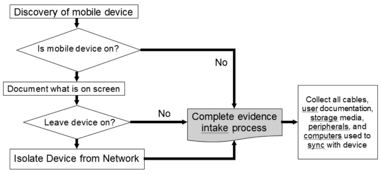
- *Challenge:* How does the MobileSpy work?
- *Challenge:* Find the software that can harm your Android system?
- *Challenge:* Make your own program that reads data on Android (iPhone) system. Can this also be useful software?

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



Discovery of mobile device

Is mobile device on?

No

Document what is on screen

Leave device on?

No

Complete evidence intake process

Collect all cables, user documentation, storage media, peripherals, and computers used to sync with device

Isolate Device from Network

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

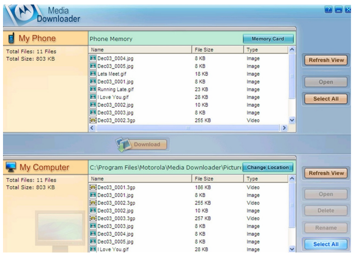
- different methods of accessing with different types
  - not every device has USB guide
- examples:
  - via user interface
  - via communication port
  - property interface (Nokia F-BUS, *Flash BUS*)
  - via JTAG (*Joint Test Action Group*) interface
  - via direct memory chip access

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)



My Phone

Total Files: 11 Files
Total Size: 803 KB

Phone Memory | Memory Card

Name	File Size	Type
Dec03_0004.jpg	8 KB	Image
Dec03_0005.jpg	8 KB	Image
Lets Meet.gif	18 KB	Image
Dec03_0001.jpg	8 KB	Image
Running Late.gif	23 KB	Image
I Love You.gif	28 KB	Image
Dec03_0002.jpg	10 KB	Image
Dec03_0003.jpg	8 KB	Image
Dec03_0002.3gp	255 KB	Video

My Computer

Total Files: 11 Files
Total Size: 803 KB

C:\Program Files\Motorola\Media Downloader\Picture

Name	File Size	Type
Dec03_0001.3gp	186 KB	Video
Dec03_0001.jpg	8 KB	Image
Dec03_0002.3gp	255 KB	Video
Dec03_0002.jpg	10 KB	Image
Dec03_0003.3gp	257 KB	Video
Dec03_0003.jpg	8 KB	Image
Dec03_0004.jpg	8 KB	Image
Dec03_0005.jpg	8 KB	Image
I Love You.gif	28 KB	Image

Examples ...

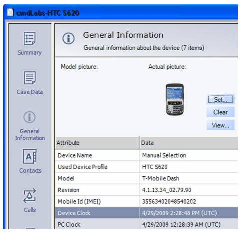
- device, which is partly broken, it may still work well enough

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/)



General Information

General information about the device (7 items)

Model picture:

Actual picture:

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)	355634020485402O2
Device Clock	4/29/2009 2:28:48 PM (UTC)
PC Clock	4/29/2009 12:28:39 AM (UTC)

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

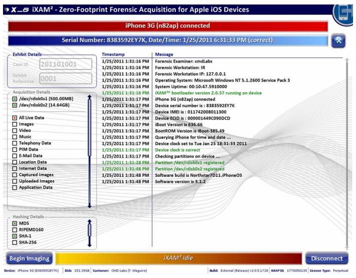
Mobile Device Forensics Tools

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

- MOBILedit! Forensic (http://mobiledit.com/)
- progamming equipment for analysis

Mobile Device Forensics Tools

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



iXAM² - Zero-Footprint Forensic Acquisition for Apple iOS Devices

iPhone 3G (n82ap) connected

Serial Number: 8383592EY7K, Date/Time: 1/25/2011 6:31:33 PM (correct)

Exhibit Details

Case ID: 201101001

Exhibit Reference: 0001

Acquisition Details

☒ /dev/rdisk0s1 (500.00MB)
☒ /dev/rdisk0s2 (14.64GB)

☒ 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

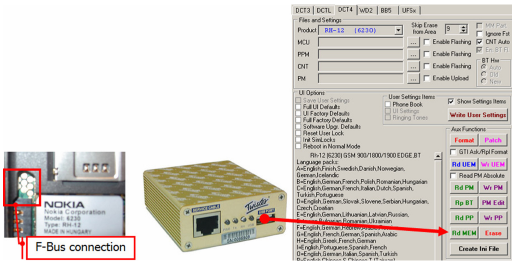
☒ MD5
☐ RIPEMD160
☒ SHA-1
☐ SHA-256

```
Timestamp              Message
1/25/2011 1:31:16 PM   Forensic Examiner: cmdLabs
1/25/2011 1:31:16 PM   Forensic Workstation: IR
1/25/2011 1:31:16 PM   Forensic Workstation IP: 127.0.0.1
1/25/2011 1:31:16 PM   Operating System: Microsoft Windows NT 5.1.2600 Service Pack 3
1/25/2011 1:31:16 PM   System Uptime: 00:10:47.5910000
1/25/2011 1:31:16 PM   iXAM²ᴰ bootloader version 2.0.57 running on device
1/25/2011 1:31:17 PM   iPhone 3G (n82ap) connected
1/25/2011 1:31:17 PM   Device serial number is : 8383592EY7K
1/25/2011 1:31:17 PM   Device IMEI is : 011742008011300
1/25/2011 1:31:17 PM   Device ECID is : 000001449C090DCD
1/25/2011 1:31:17 PM   iBoot Version is 636.66
1/25/2011 1:31:17 PM   BootROM Version is iBoot-385.49
1/25/2011 1:31:17 PM   Querying iPhone for time and date ...
1/25/2011 1:31:17 PM   Device clock set to Tue Jan 25 18:31:33 2011
1/25/2011 1:31:17 PM   Device clock is correct
1/25/2011 1:31:17 PM   Checking partitions on device ...
1/25/2011 1:31:28 PM   Partition /dev/rdisk0s1 registered
1/25/2011 1:31:48 PM   Partition /dev/rdisk0s2 registered
1/25/2011 1:31:48 PM   Software build is Northstar7D11.iPhoneOS
1/25/2011 1:31:48 PM   Software version is 3.1.2
```

Device: iPhone 3G (8383592EY7K) | Disk: 152.29GB | Customer: CMD Labs (T. Maguire) | Build: External (Release) v2.0.5.1720 | HASP ID: 1770050135 | License Type: Perpetual

Mobile Device Forensics Tools

Twister Flasher



Product: RH-12 (6230)

Skip Erase from Area: 9

☐ Enable Flashing
☐ Enable Flashing
☐ Enable Flashing
☐ Enable Upload

☐ MM Part.
☐ Ignore Fst
☑ CNT Auto
☑ En. BT Fl.

BT Hw: ● Auto ○ Old ○ New

UI Options

☐ Save User Settings
☐ Full UI Defaults
☐ UI Factory Defaults
☐ Full Factory Defaults
☐ Software Upgr. Defaults
☐ Reset User Lock
☐ Init SimLocks
☐ Reboot in Normal Mode

User Settings Items

☐ Phone Book
☐ UI Settings
☐ Ringing Tones

☑ Show Settings Items

☐ GTI Ask/Rpl Format
☐ Read PM Absolute

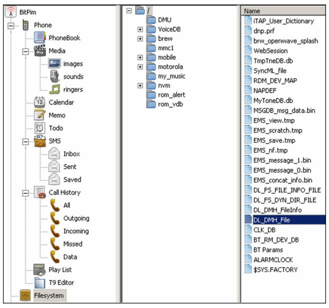
Rh-12 (6230) GSM 900/1800/1900 EDGE,BT
Language packs:
A=English,Finish,Swedish,Danish,Norwegian,German,Icelandic
B=English,German,French,Polish,Romanian,Hungarian
C=English,German,French,Italian,Dutch,Spanish,Turkish,Portuguese
D=English,German,Slovak,Slovene,Serbian,Hungarian,Czech,Croatian
E=English,German,Lithuanian,Latvian,Russian,Estonian,Bulgarian,Romanian,Ukrainian
F=English,German,Hebrew,Arabic,Russian
G=English,French,German,Spanish,Arabic
H=English,Greek,French,German
I=English,Portuguese,Spanish,French
O=English,German,Italian,Spanish,Turkish
P=English,Chinese S,Chinese T (Taiwan)

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:

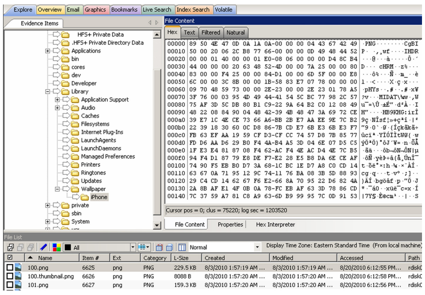
Some basic tools ...

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



Some basic tools ...

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



```
00000 89 50 4E 47 0D 0A 1A 0A-00 00 00 04 43 67 42 49 ·PNG········CgBI
00010 50 00 20 06 2C B8 77 66-00 00 00 0D 49 48 44 52 P· ·,¸wf····IHDR
00020 00 00 01 40 00 00 01 E0-08 06 00 00 00 D4 8C B4 ···@···à·····Ô·´
00030 44 00 00 00 20 63 48 52-4D 00 00 7A 25 00 00 80 D··· cHRM··z%···
00040 83 00 00 F4 25 00 00 84-D1 00 00 6D 5F 00 00 E8 ···ô%···Ñ··m_··è
00050 6C 00 00 3C 8B 00 00 1B-58 83 E7 07 78 00 00 00 l··<····X·ç·x···
00060 09 70 48 59 73 00 00 2E-23 00 00 2E 23 01 78 A5 ·pHYs···.#···.#·x¥
00070 3F 76 00 03 95 4D 49 44-41 54 5C BC 77 98 2C 57 ?v···MIDAT\¼w·,W
00080 75 AF 3D 5C DB 80 B1 C9-22 9A 64 B2 C0 12 08 49 u¯=\Û·±É"·d²À··I
00090 48 22 08 84 90 04 48 42-39 4B 48 47 3A 69 72 CE H"····HB9KHG:irÎ
000a0 39 E7 1C 4E CE 73 66 A6-BB 2B E7 AA EE 9E 7C B2 9ç·NÎsf¦»+çªî·|²
000b0 22 39 18 30 60 0C D8 86-7B CD E7 6B E3 6B E3 F7 "9·0`·Ø·{Íçkãkã÷
000c0 FB 63 EF AA 19 59 CF D3-CF CC 74 57 D8 7B 85 77 ûcïª·YÏÓÏÌtWØ{·w
000d0 FD D6 AA D6 29 B0 F4 4A-B4 A5 3D 04 6E 07 D5 C5 ýÖªÖ)°ôJ´¥=·n·ÕÅ
000e0 1F E3 E4 81 87 08 F4 62-AC F4 4E AC D4 4E 7C B5 ·ãä···ôb¬ôN¬ÔN|µ
000f0 94 F4 D1 87 79 E8 DE F7-E2 28 E5 B8 DA 6E CE AF ·ôÑ·yèÞ÷â(å¸ÚnÎ¯
00100 74 90 F5 EB B0 D7 3A 68-1C BC 1E D7 A8 C0 CD 14 t·õë°×:h·¼·×¨ÀÍ·
00110 63 67 0A 71 95 12 9C 74-11 76 BA 08 3B 5D 88 93 cg·q···t·vº·;]··
00120 29 C4 CD 14 62 67 F6 E2-66 8A 70 95 22 D6 82 4A )ÄÍ·bgöâf·p·"Ö·J
00130 2A 8B AF E1 4F 0B 0A 78-FC EB AF 63 3D 78 86 CD *·¯áO··xüë¯c=x·Í
00140 7C 37 59 A7 81 C8 A9 63-6D B9 99 95 7C 0D 91 53 |7Y§·È©cm¹··|··S
```

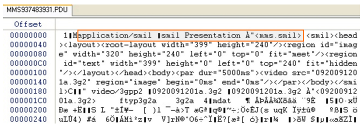
Cursor pos = 0; clus = 75220; log sec = 1203520

Display Time Zone: Eastern Standard Time (From local machine)

☑	Name	Item #	Ext	Category	L-Size	Created	Modified	Accessed	Path
□	100.png	6625	png	PNG	229.5 KB	8/3/2010 1:57:19 AM ...	8/3/2010 1:57:19 AM ...	8/20/2010 6:12:55 PM...	rdiskC
□	100.thumbnail.png	6626	png	PNG	8088 B	8/3/2010 1:57:20 AM ...	8/3/2010 1:57:20 AM ...	8/20/2010 6:12:58 PM...	rdiskC
□	101.png	6627	png	PNG	159.3 KB	8/3/2010 1:57:20 AM ...	8/3/2010 1:57:20 AM ...	8/20/2010 6:12:56 PM...	rdiskC

Data recovery

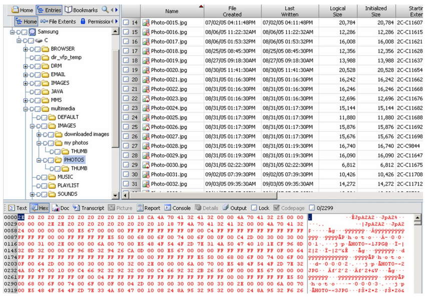
- even if we don't have all the data we can recover partly deleted data from logical data



```
Offset
00000000  1▮Mapplication/smil ▮smil Presentation À"<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 À"<09200912
000001C0 01a.3g2>     ftyp3g2a    3g2a  4▮mdat   ¶ ÀÞÅÅ¾Xõâä ¨9È  ▮5▮O·xÜ
00000200 Ðæ +Ë▮▮S L "±Í¥–  [ )l ¯–à>T æGª▮q®▮~÷;Ö¢ÊJ(s uqK Ïÿ±û®   ºß▮S ö
00000240 uLÛ4) #á  6Ö▮ÁMì²z▮v  V]rN®˚O6÷^Ï▮Ë?[æª[ ó}▮r▮¼  ▮>õW Š▮µ▮«aãZÌ▮
```

Data recovery

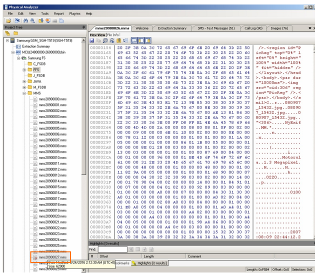
- if it is usual file system (FAT, ext2, ext3, APFS, ...) already known tools
  - EnCase and deleted images

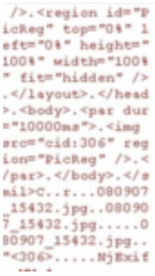


	Name	File Created	Last Written	Logical Size	Initialized Size	Starting Extent
14	Photo-0015.jpg	07/02/05 04:11:48PM	07/02/05 04:11:48PM	20,784	20,784	2C-C11607
15	Photo-0016.jpg	08/06/05 11:22:32AM	08/06/05 11:22:32AM	12,286	12,286	2C-C11615
16	Photo-0017.jpg	08/06/05 01:53:32PM	08/06/05 01:53:32PM	16,008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

Data recovery

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

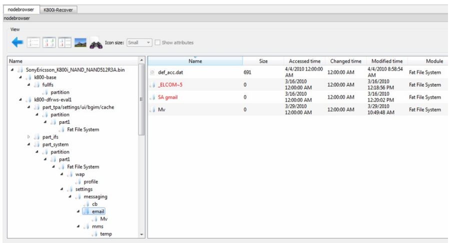




```
/>.<region id="P
icReg" top="0%" l
eft="0%" height="
100%" width="100%
" fit="hidden" />
.</layout>.</head
>.<body>.<par dur
="10000ms">.<img
src="cid:306" reg
ion="PicReg" />.<
/par>.</body>.</s
mil>C..r...080907
_15432.jpg..08090
7_15432.jpg.....0
80907_15432.jpg..
"<306>.....NjExif
```

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



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

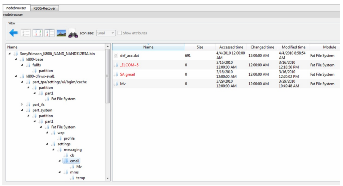
- *Synchronized Multimedia Integration Language*
  - part of W3C standard - http://www.w3.org/AudioVideo/
  - versions 1, 2 in 3 (http://www.w3.org/TR/SMIL3/)
- includes SVG items (enhanced vector graphics, *Scalable Vector Graphics*)
- allows:
  - animation, integration of other images, modularization, ...
- *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

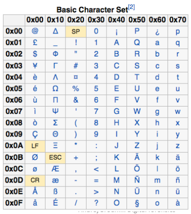


```
Name
SonyEricsson_K800i_NAND_NAND512R3A.bin
  k800-base
    fullfs
      partition
  k800-dfrws-eval1
    part_tpa/settings/ui/bgim/cache
      partition
        part1
          Fat File System
    part_ifs
    part_system
      partition
        part1
          Fat File System
            wap
              profile
            settings
              messaging
                cb
                email
                  Mv
                mms
                  temp
```

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

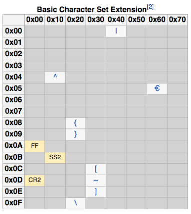
Examination – data formats

- 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[2]

	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			\					

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)

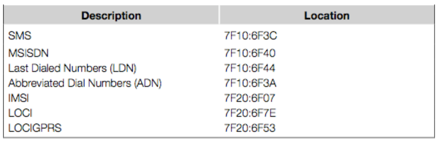
Examination – SIM card

- SIM (*Subscriber Indenty 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

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

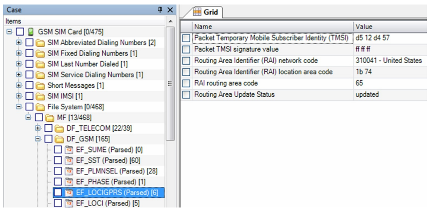
- Some files are defined in the standard
  - 3F00:7F10 (DFTELECOM, *dedicated file*): records on the use of services (i.e. sent SMS, dialed numbers, ...)
  - 3F00:2FE2 (EFICCID, *elementary file*): saves ICC-ID (*Integrated Circuit Card ID*)
  - 3F00:7F20:6F07 EFIMSI: saves IMSI (*International Mobile 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*)



```
⊟ □ GSM SIM Card [0/475]
   ⊞ □ 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]
   ⊟ □ File System [0/468]
      ⊟ □ MF [13/468]
         ⊞ □ DF_TELECOM [22/39]
         ⊟ □ DF_GSM [165]
               □ EF_SUME (Parsed) [0]
               □ EF_SST (Parsed) [60]
               □ EF_PLMNSEL (Parsed) [28]
               □ EF_PHASE (Parsed) [1]
               □ EF_LOCIGPRS (Parsed) [6]
               □ EF_LOCI (Parsed) [5]
```

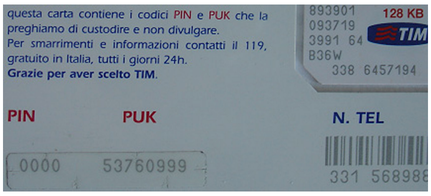
	Name	Value
□	Packet Temporary Mobile Subscriber Identity (TMSI)	d5 12 d4 57
□	Packet TMSI signature value	ff ff ff
□	Routing Area Identifier (RAI) network code	310041 - United States
□	Routing Area Identifier (RAI) location area code	1b 74
□	RAI routing area code	65
□	Routing Area Update Status	updated

SIM card

- *Challenge:* How can I access the data on your SIM card?
- *Challenge:* Is the entire GPRS history saved?
- *Challenge:* naštejtejte 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



questa carta contiene i codici PIN e PUK che la preghiamo di custodire e non divulgare. Per smarrimenti e informazioni contatti il 119, gratuito in Italia, tutti i giorni 24h. **Grazie per aver scelto TIM.**