



Mobile memory dumps, MSAB and MPE+

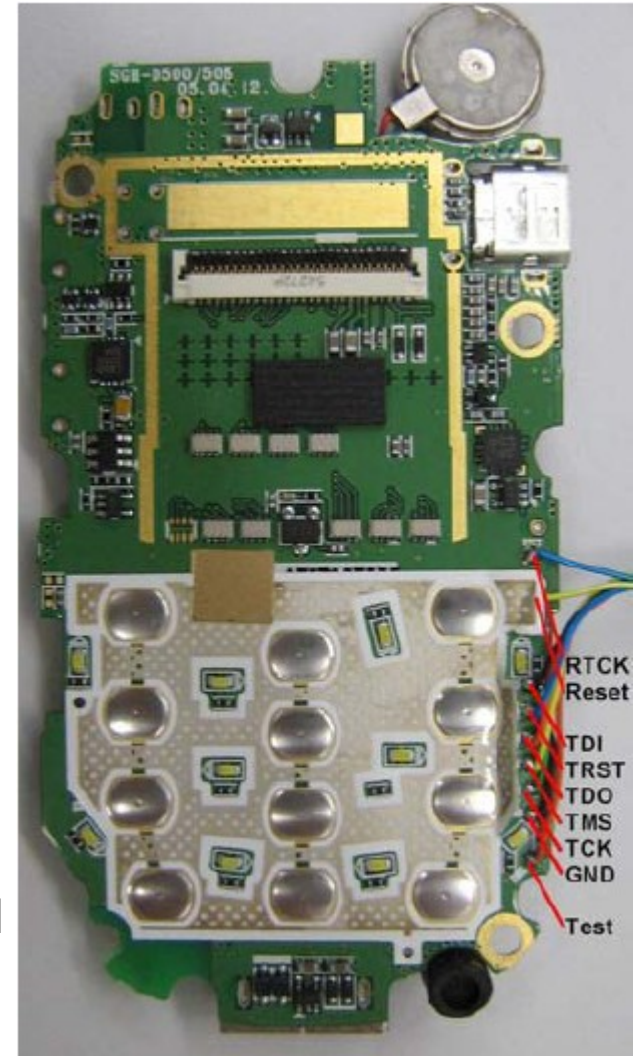
Data collection

Information recovery

Analysis and interpretation of results

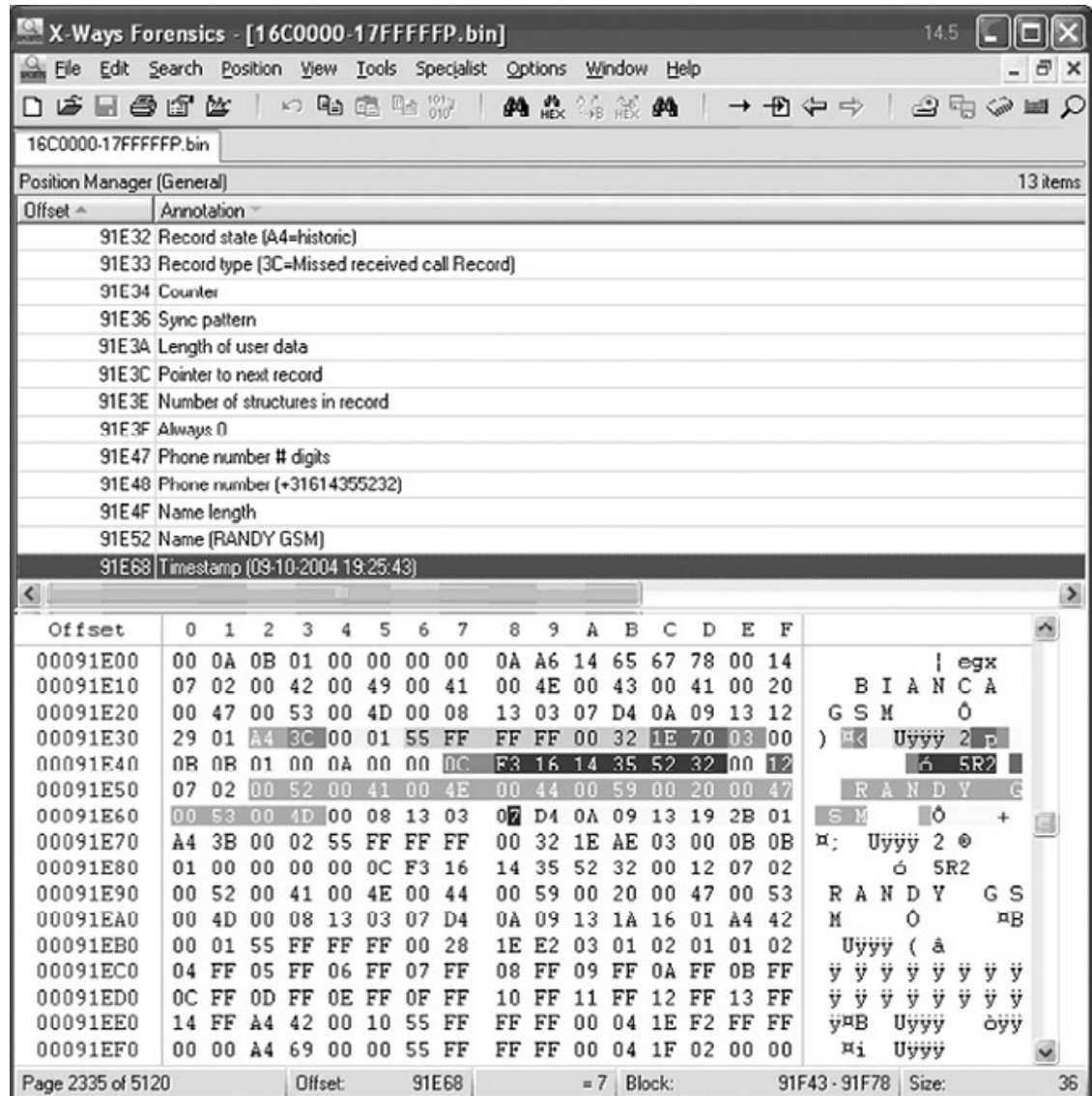
Physical Extraction

- Physical extraction involves either
 - Removing chips from circuit board and “dumping” contents (destructive)
 - Via a data cable (e.g. service ports on many Nokias)
- Data is supplied in a “raw” form
 - Interpretation requires time and specialist knowledge
 - Provides a lot of data including deleted handset information
- JTAG test and debug access port
 - A complete forensic image can be produced
 - The risk of changing data is minimized
 - Not all embedded systems are JTAG enabled
 - <http://en.wikipedia.org/wiki/Jtag>



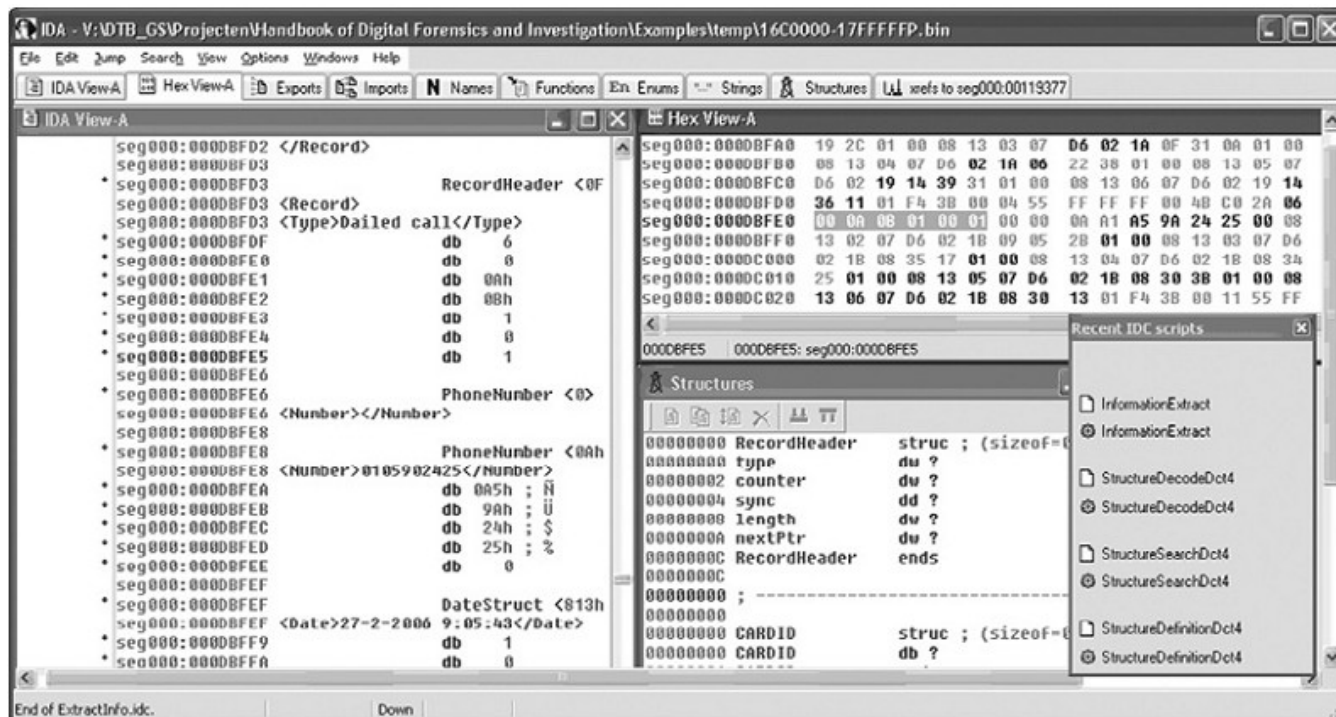
Hex editors - WinHex

- Color mappings
- Bookmarks
- Structure definitions
- Using the bookmark functionality of WinHex to dissect a deleted missed call record of a partial NOR flash copy from a Nokia 1600 phone



Hex editors – IDA Pro

- In IDA Pro using IDC scripts or the plugins framework
 - Could be used to load data from an embedded system memory that contains data encoding functions and to reverse engineer them to reconstruct relevant system and user information
 - A more practical approach is to (ab)use IDA as an advanced hex editor with additional functionality for repeated decoding of memory data
 - Do the following examining the dump in 4 steps with scripts:
 - StructureDefinition.idc, StructureSearch.idc, StructureDecode.idc, InformationExtract.idc



MSAB Forensic Office





- We can extract the data through the phone by talking to the operating system, using a set of various software tools and techniques.
- It is the fastest (cheapest) way to examine a phone.
- It is the best way for 80% of all examinations
- It will not reveal deleted data.
- All visible data may not be possible to extract!

MSAB XRY

The screenshot displays the MSAB XRY software interface. The main window title is "XRY - [SonyEricsson_k800i.xry]". The menu bar includes File, Edit, View, Windows, Tools, Options, About, and Help. The toolbar contains various icons for file operations (Extract Data, Open, Close, Save, Save As), file types (File, Microsoft Excel, Microsoft Word, Google Earth, OpenOffice, XML), and other functions (Print, Device Manual, Help Topics).

The "Media Window" is open, showing a summary of SMS messages. The summary indicates "SMS messages sent or received from the device (13 items)". The messages are listed in a table with columns: Number, Name, Message, Time, Status, Storage, Index, and Service Center.

Number	Name	Message	Time	Status	Storage	Index	Service Center
<input type="checkbox"/> 0632082356		Goedenmorgen schoonheid		Sent	Device	1	+31653131313
<input type="checkbox"/> 1300		KPN helpt u graag met het instellen van internet op uw mobiel. U ontvangt hiervoor zometeen instellingen. Accepteer deze als uw toestel er om vraagt. Afz KPN	2010-03-29 13:45:16 (+02:0)	Read	Device	2	+31653131316
<input type="checkbox"/> 0620125081		Is everything OK, it looked like you were going somewhere, because of your tickets. I hope you are coming out of it? Let me know how you are. Maybe i can also help a bit with everything. Best regards. Stenhan.		Sent	Device	3,4	+31653131313
<input type="checkbox"/> 1300		Uw toestel werkt nu optimaal. Wilt u de instellingen nog een keer ontvangen, sms dan gratis JA naar 1300. Voor meer info zie kpn.com/1300 of bel 1200. Afz. KPN	2010-03-29 13:51:15 (+02:0)	Read	Device	5	+31653131316
<input type="checkbox"/> +31628954735	[Geen naam]	OK, will look after it	2010-03-30 08:04:30 (+02:0)	Read	Device	6	+31624000115
<input type="checkbox"/> 0632082356		Ik ben zo thuis, hoe was het vandaag nog veel leuke dingen gedaan? Ik ben vandaag nog ergens heen geweest, maar waar is de vraag even. Het was in ieder geval wel leuk. Tot straks. hve Stenhan		Sent	Device	7,8	+31653131313
<input type="checkbox"/> 0632082356		Vergeet je niet vandaag naar de tandarts te gaan?		Sent	Device	9	+31653131313
<input type="checkbox"/> +31631356695		Can you deliver 100 J85-21 replacement engines in Irak in one week?	2010-03-30 08:16:58 (+02:0)	Read	Device	10	+316540881008
<input type="checkbox"/> 0615646978		Everything arranged!		Sent	Device	11	+31653131313


The interface also shows a sidebar with navigation options: Summary, Case Data, General Information, Contacts, Calls, SMS, and Pictures. The system tray at the bottom left shows the "Ready" status and system icons. The bottom right corner displays "CAP NUM SCRL" and a scroll bar.

Geocoded Data

The screenshot displays the Google Earth interface with a map of a city area. Numerous small photo thumbnails are scattered across the map, each labeled with a file path and timestamp, such as `/private/var/mobile/Media/DCIM/100APPLE//IMG_0016.JPG` and `2009:10:17 22:35:02`. A central cluster of these photos is highlighted with a starburst effect. On the left, the 'Places' and 'Layers' panels are visible. The 'Layers' panel includes options like 'Primary Database', 'Borders and Labels', 'Places of Interest', 'Panoramio Photos', 'Roads', '3D Buildings', 'Ocean', 'Street View', 'Weather', 'Gallery', 'Global Awareness', 'More', and 'Terrain'. A metadata window is open on the right, showing the following information:

2009:12:19 11:38:53 -
`/private/var/mobile/Media/DCIM/100APPLE//IMG_0051.JPG`

.XRY

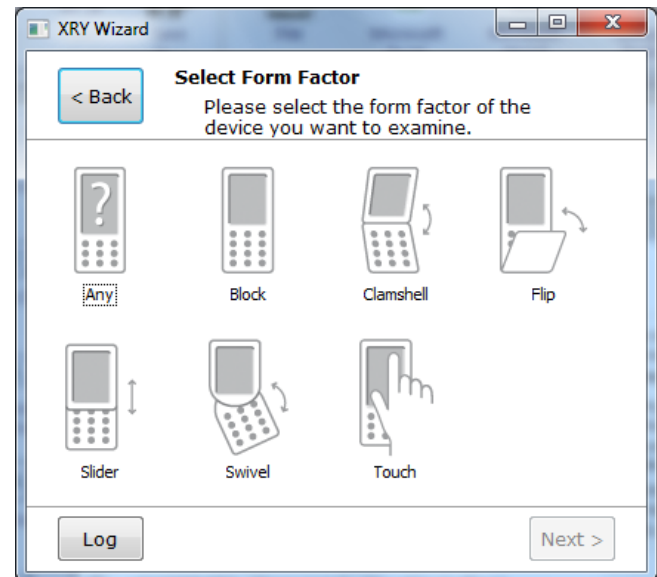
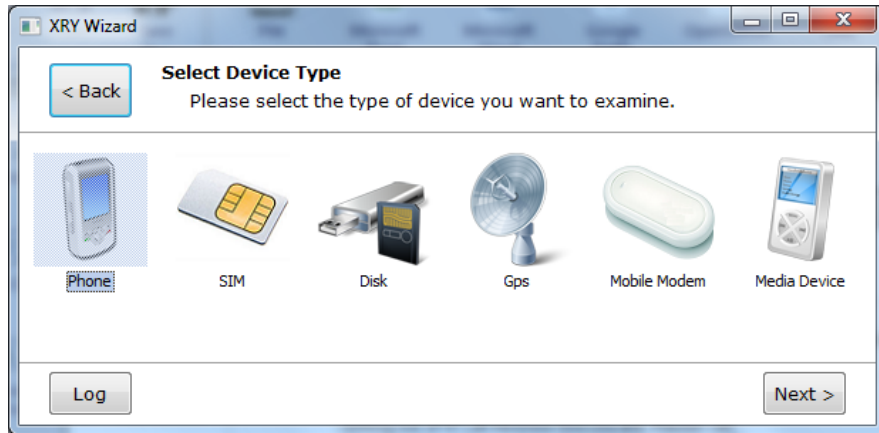


Co-ordinates acquired from JPEG EXIF metadata

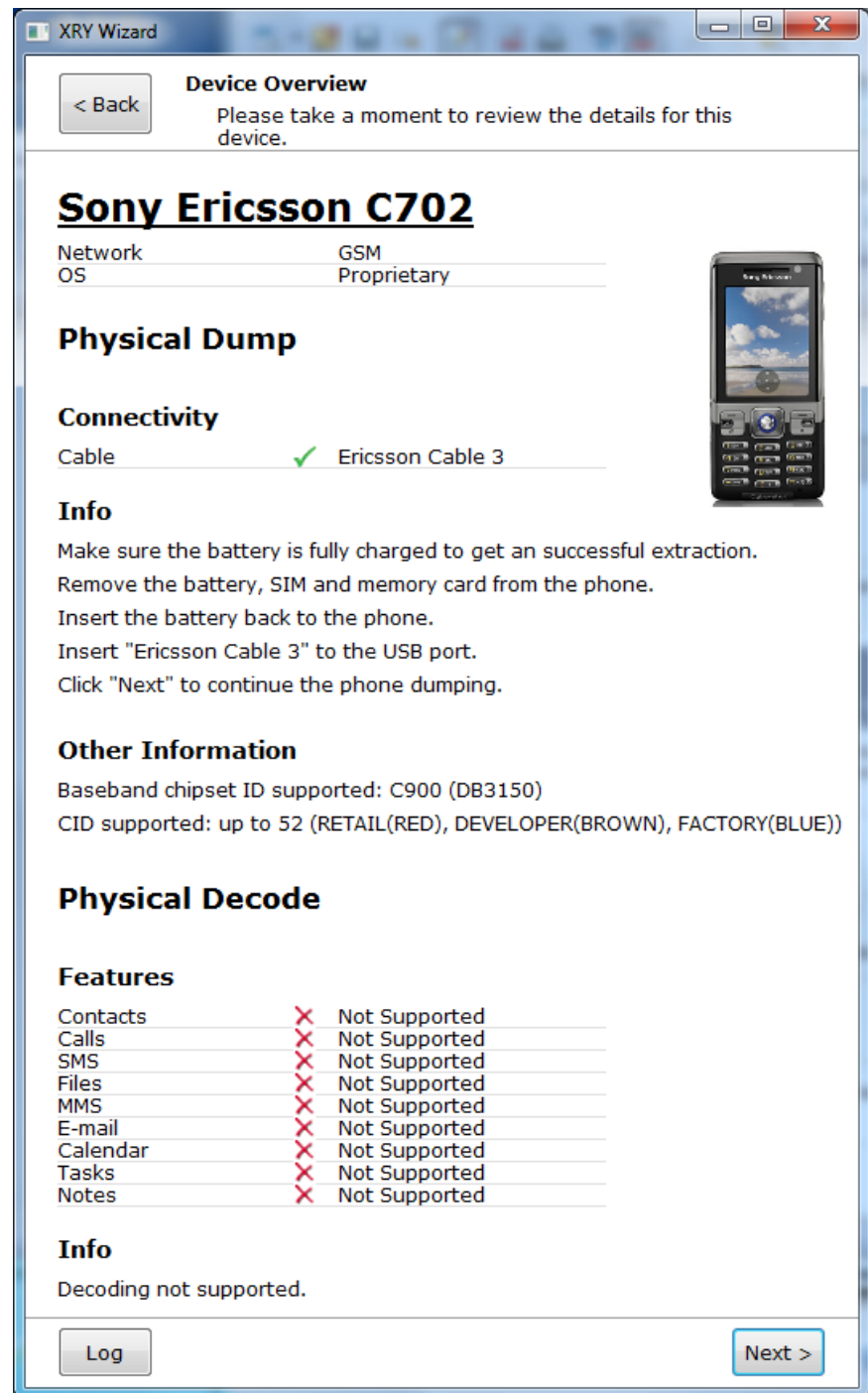
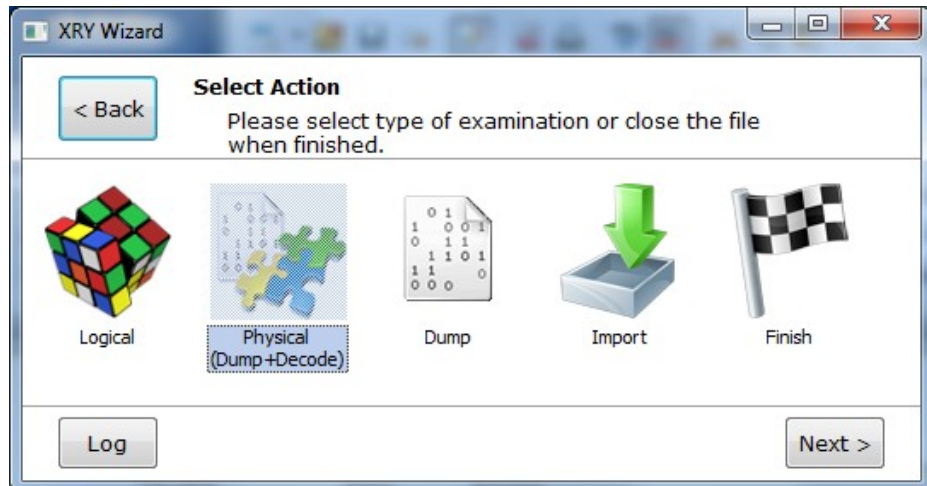
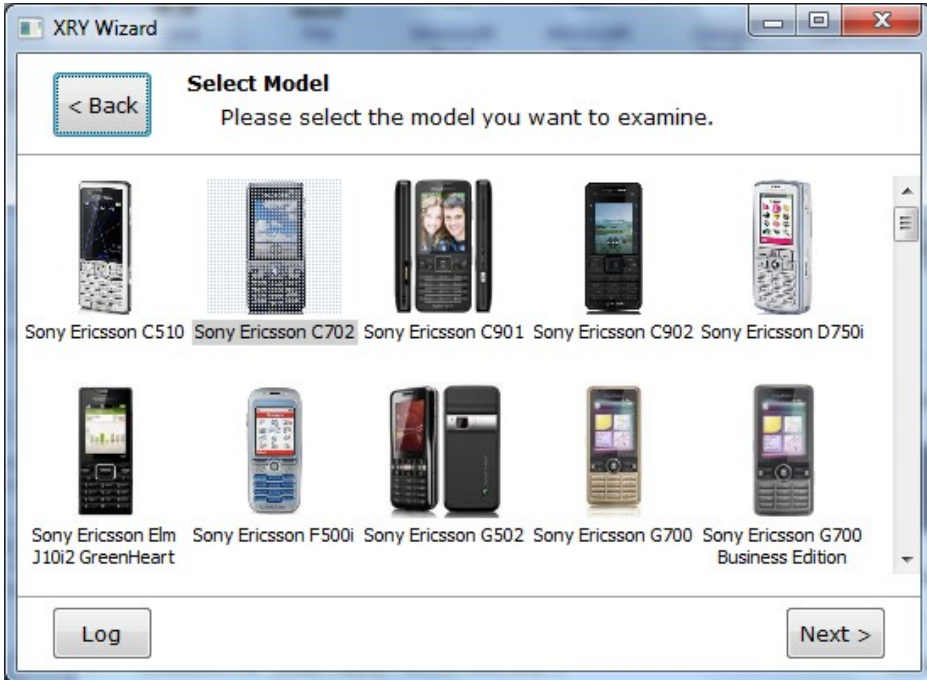
EquipMake: Apple
EquipModel: iPhone 3G
Orientation: 6
XResolution: 72.000000
YResolution: 72.000000
ResolutionUnit: 2
SoftwareUsed: 3.1.2
DateTime: 2009:12:19 11:38:53
YCbCrPositioning: 1
ExifNumber: 2.800000
ExifExposureProg: 2
ExifVer: 48 50 50 49
ExifDTOrig: 2009:12:19 11:38:53
ExifDTDigitized: 2009:12:19 11:38:53
ExifCompConfig: 1 2 3 0
ExifAperture: 2.970854
ExifMeteringMode: 1

At the bottom of the map, the following information is displayed: Imagery Date: Mar 18, 2004; Coordinates: 33° 28' 11.87" N, 88° 48' 38.82" W; Elevation: 857 ft; Eye Alt: 11954 ft.

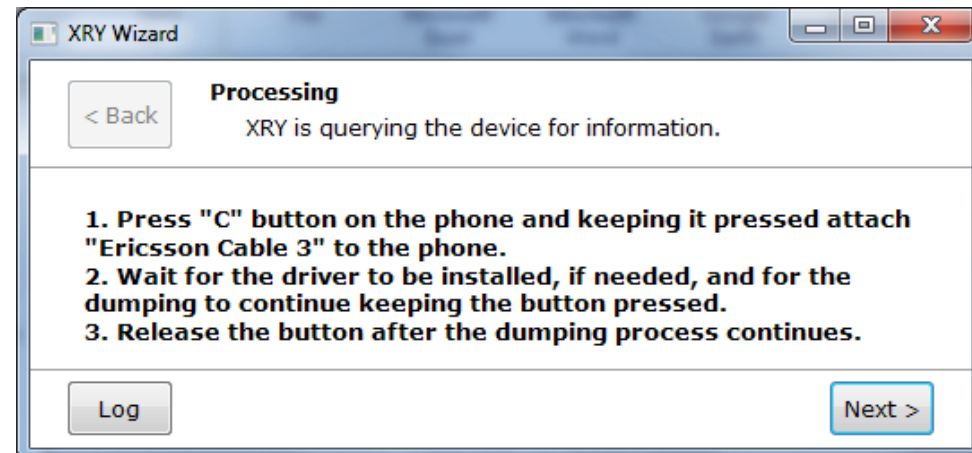
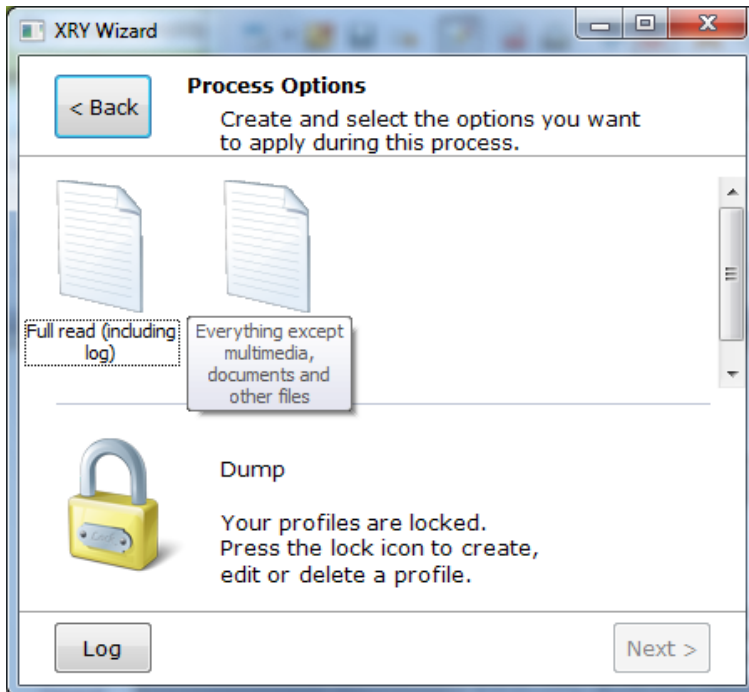
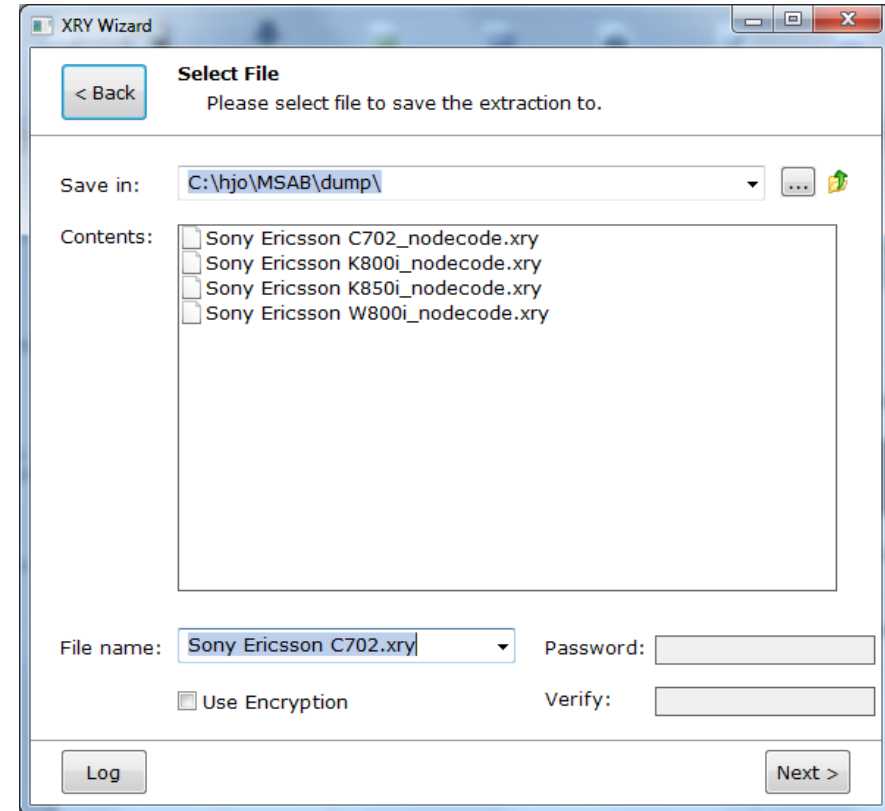
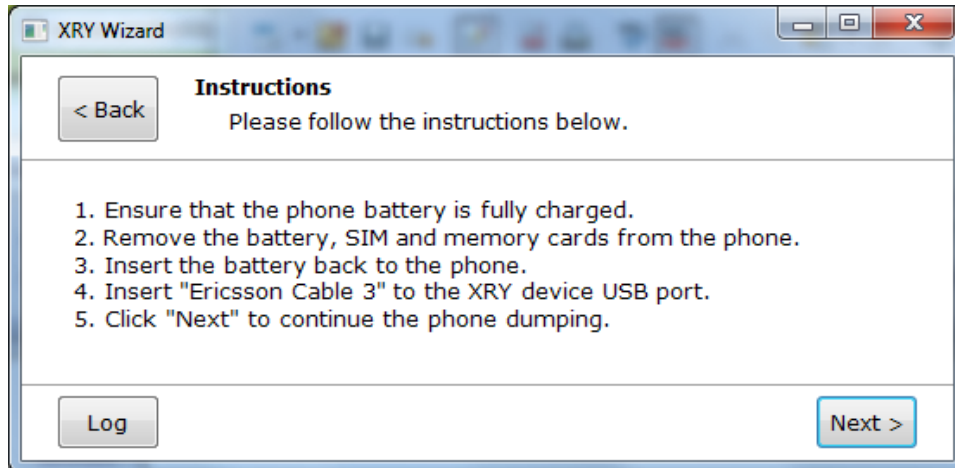
MSAB XRY Wizard 1



MSAB XRY 2



MSAB XRY 3



MSAB XRY SIM Id Cloner

SIM_id-Cloner.pdf

Do you need a tool that helps you in these situations?

- ▶ Examine a mobile phone without the original SIM card
- ▶ Examine a mobile phone with a PIN locked SIM card
- ▶ Examine a mobile phone without connecting to the mobile network

If so, SIM id-Cloner is the ideal solution.

Examine a mobile phone without the original SIM card

With SIM id-Cloner the examiner can create a SIM card, which gives access to the phone without destroying the call list.

NOTE: The examiner needs either ICCID or IMSI, which normally requires a contact with the mobile network operator.

Examine a mobile phone with a PIN locked SIM card

There is a SIM card in the phone which is PIN locked, and it is difficult at short notice to get information from the mobile network provider (e.g. PUK code). With the SIM id-Cloner the examiner can create SIM card, which gives access to the phone without destroying the call list.

NOTE: This is suitable for phones where only ICCID is needed. In some cases it is possible also to retrieve IMSI from the phone memory.

Examine a mobile phone without connecting to the mobile network

The SIM card is available and not PIN locked, but the examiner needs to do the mobile phone examination without any connection to the mobile network. The reason for that is to avoid incoming calls or text messages to the mobile phone during the examination. With SIM id-Cloner the examiner can create a SIM card that allows you to do the examination during radio silence and without destroying the call list.



Other benefits with SIM id-Cloner

Tested with many different mobile phones and SIM cards

Our SIM id-Cloner Examination card has been tested with many different phone models and SIM cards and it's specified to work with almost all phones. For a detailed description for each phone model, see the SIM id-Cloner manual.

The SIM id-Cloner manual includes all the information you need.

Read the SIM id-Cloner manual and you will understand how to create a SIM id-Clone for the individual phone model that you need to examine based on our testing of each individual phone model.

Full support through phone and email when you need assistance

If you have questions or need technical advice for a certain phone or SIM card we are available to assist you.

Well integrated with .XRY

SIM id-Cloner is well integrated in .XRY. If you don't have an .XRY license you can run SIM id-Cloner with .XRY Reader, available at no charge. If you have an .XRY license then you can use the same SIM Card Reader as .XRY.

NOTE: You need a separate license for SIM id-Cloner.

Cost effective, rewritable SIM cards

SIM id-Cloner Examination cards are rewritable, which means that you don't need one for every examination

International Mobile Subscriber Identity

<http://en.wikipedia.org/wiki/IMSI>

<http://pt.com/page/tutorials/gsm-tutorial>

- **IMSI** uniquely identifies a subscriber
 - Always provisioned in the phone/SIM (GSM), USIM (3G) or CSIM (CDMA)
 - Usually 15 digits in length
- Ex. IMSI: 240011234567890
 - The first 3 digits are the Mobile Country Code (MCC)
 - Followed by the Mobile Network Code (MNC)
 - Either 2 digits (EU standard) or 3 digits (North American standard)
 - The remaining digits are the Mobile Station Identification Number (MSIN)

IMSI = MCC + MNC + MSIN

MCC	240	Sweden
MNC	01	Telia
MSIN	1234567890	

- IMSI analysis
 - The process of examining a subscriber's IMSI to identify which network the IMSI belongs to and whether subscribers from that network are allowed to use a given network

Integrated Circuit Card Identifier

- **ICCID** uniquely identifies the SIM card, one can determine issuing service provider and country code from ICCID
- International Standard ISO/IEC 7812
 - http://en.wikipedia.org/wiki/ISO_7812
 - 19 or 20 digits in length and always stored in the card
 - Normally printed on the outside (may be abbreviated)
- **Issuer Identification Number (IIN)**
 - Major Industry Identifier (MII), 2 digits, 89 for telecommunication purposes
 - Country code, 1-3 digits, as defined by ITU-T recommendation E.164.
 - Issuer identifier 1-4 digits, (Total all 6 digits including the MII)
- **Individual account identification**
 - Max 12 digits plus
 - Parity check digit

File: 2FE2 Serial Number

File Info

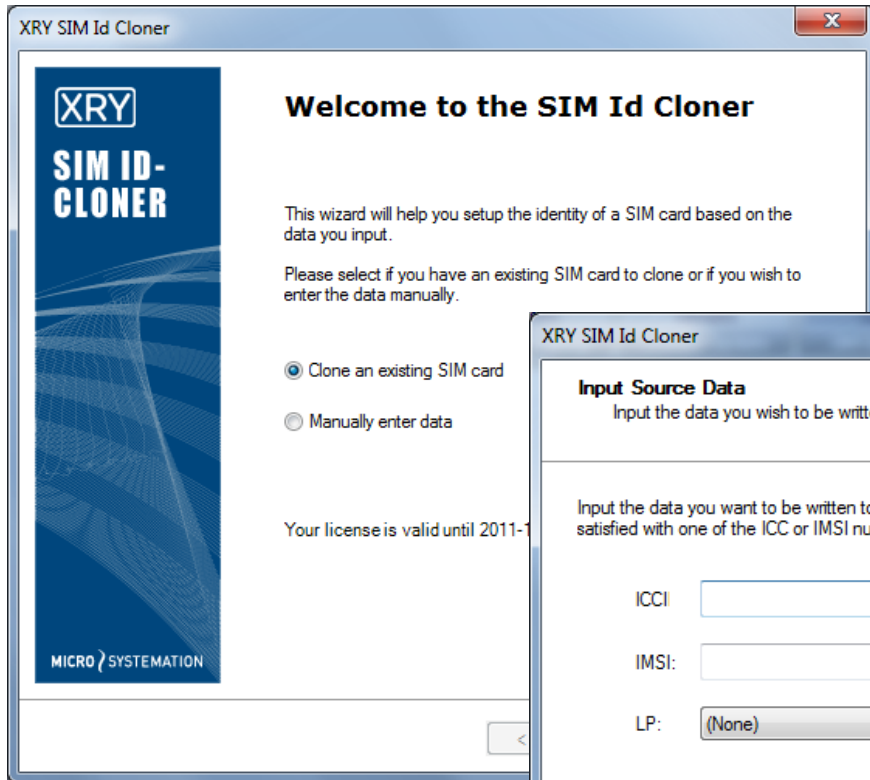
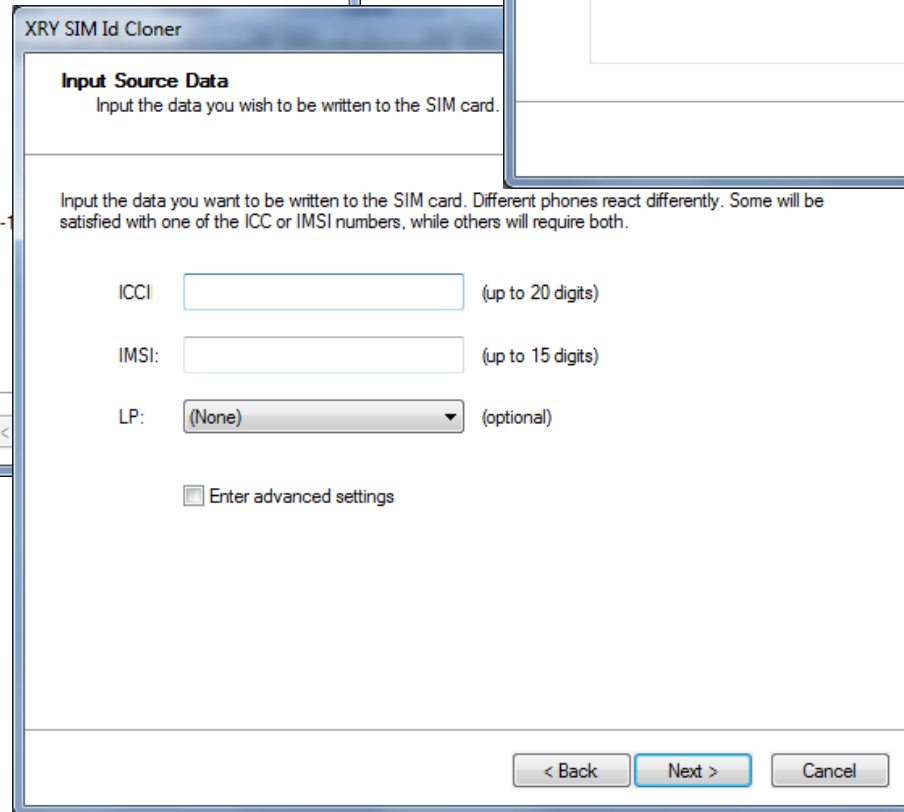
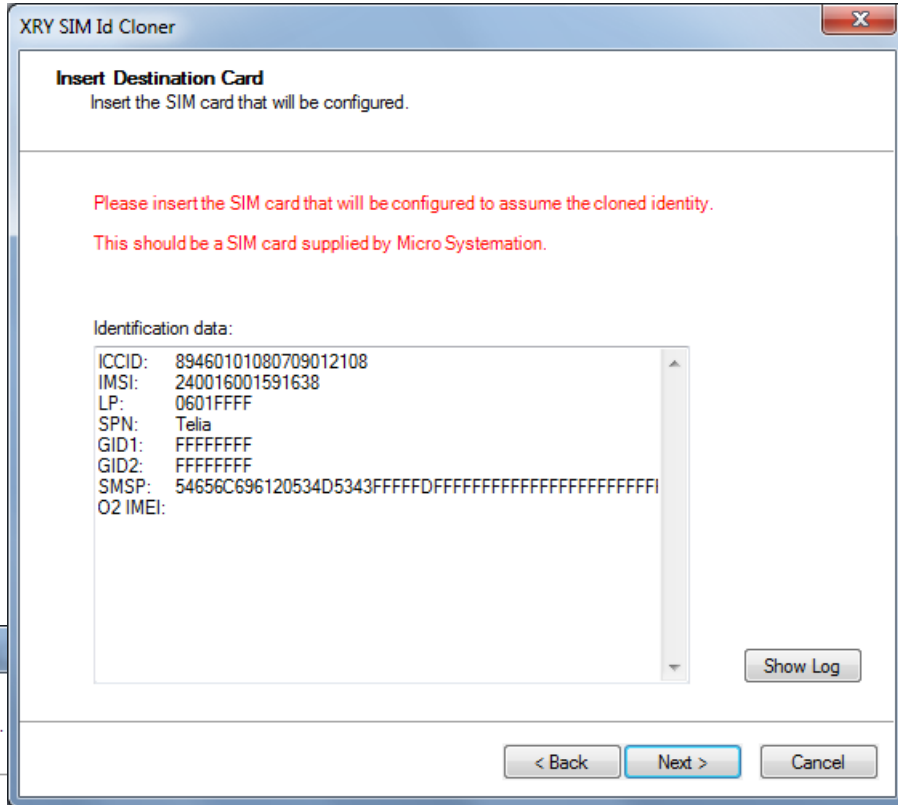
File ID: 3F00:2FE2
Structure: binary
File type: EF
Status: OK
File size: 000A
Record size:
Record count:

Access Rights

Read: 0 0: Always
Update: F 1: PIN1
Increment: 0 2: PIN2
Invalidate: F 3-E: Locked
Rehabilitate: F F: Never

98 64 10 10 80 70 90 10 58 67

MSAB XRY SIM Id Cloner

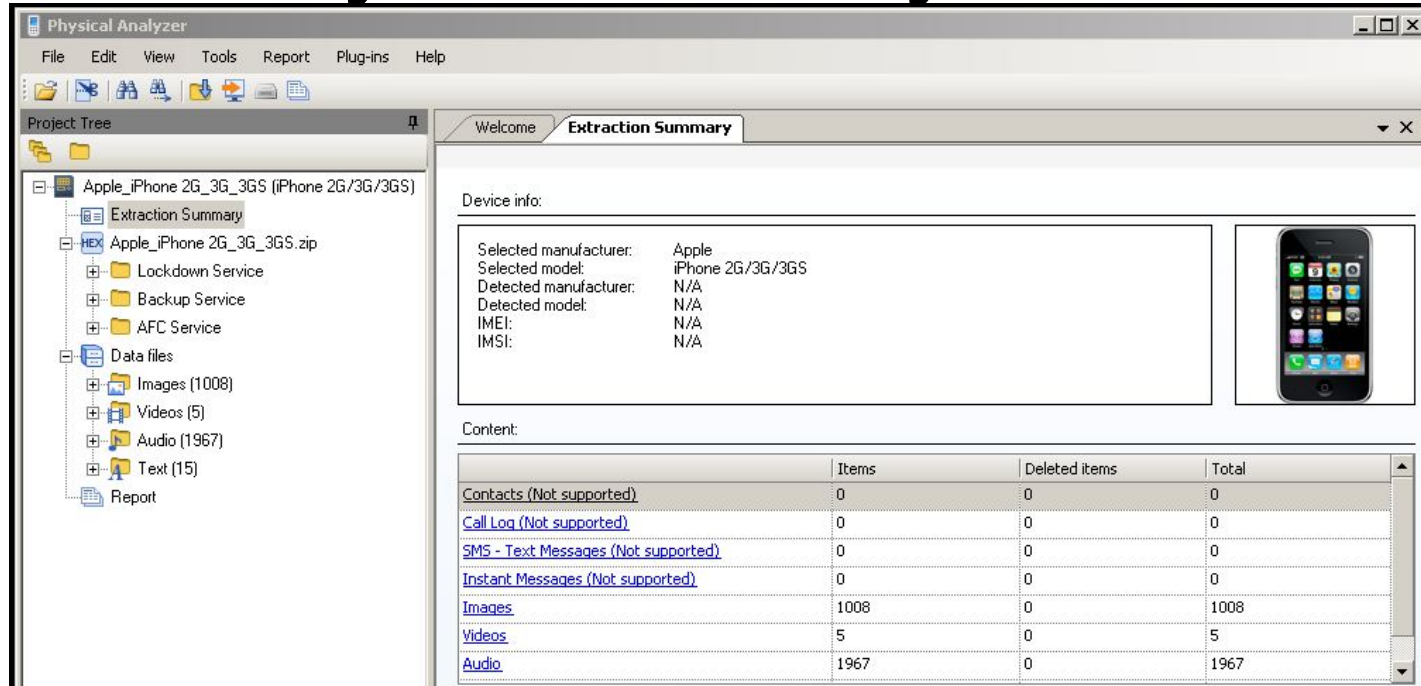




- Phones without a SIM Card
- Phones with PIN Locked SIM cards
- Phones with the security lock set
- To recover deleted evidence
- Where SIM cards have been swapped
 - Automatic erasure of call lists when SIM card is changed is a standard feature in most phones
- Possible on handsets with minor damage
- Forensic tools like XRY, UFED and FTS Hex use flash loader techniques for forensic acquisition of data
 - Instead of directly using the built-in boot loader functionality they use the primary boot loader to transfer custom executable code to one of the writable device memories and start executing that code producing a "dd" dump

UFED Physical Analyzer

cellebrite
mobile data secured



The screenshot shows the 'Physical Analyzer' software window. The 'Project Tree' on the left lists the device 'Apple_iPhone 2G_3G_3GS (iPhone 2G/3G/3GS)' and its contents: 'Extraction Summary', 'Apple_iPhone 2G_3G_3GS.zip', 'Lockdown Service', 'Backup Service', 'AFC Service', 'Data files' (including 1008 Images, 5 Videos, 1967 Audio, and 15 Text), and a 'Report'. The main window displays the 'Extraction Summary' for the device, including a 'Device info' section with the following details:

Selected manufacturer:	Apple
Selected model:	iPhone 2G/3G/3GS
Detected manufacturer:	N/A
Detected model:	N/A
IMEI:	N/A
IMSI:	N/A

A small image of the iPhone is shown to the right. Below this is a 'Content' table:

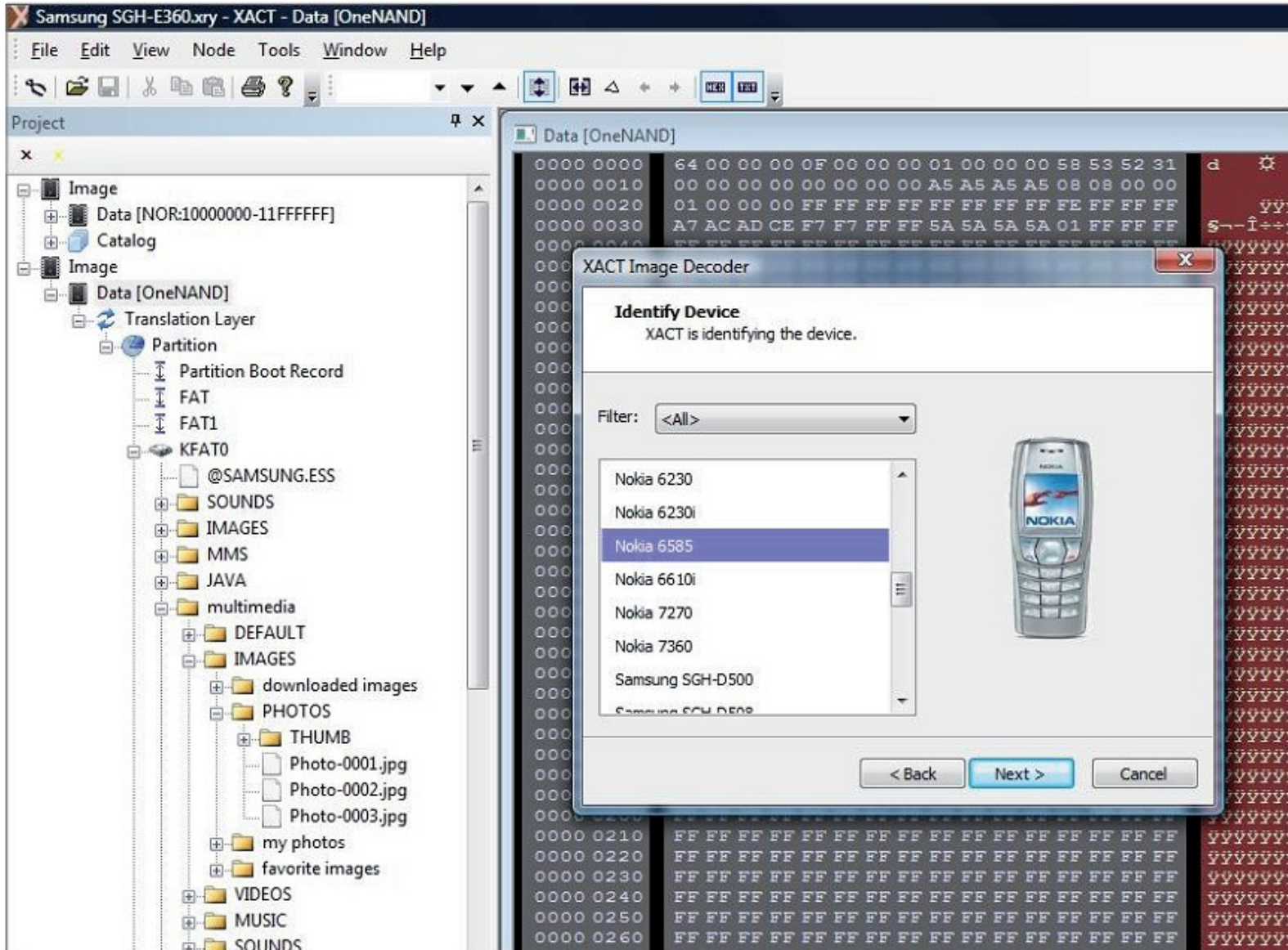
	Items	Deleted items	Total
Contacts (Not supported)	0	0	0
Call Log (Not supported)	0	0	0
SMS - Text Messages (Not supported)	0	0	0
Instant Messages (Not supported)	0	0	0
Images	1008	0	1008
Videos	5	0	5
Audio	1967	0	1967

Generate Report

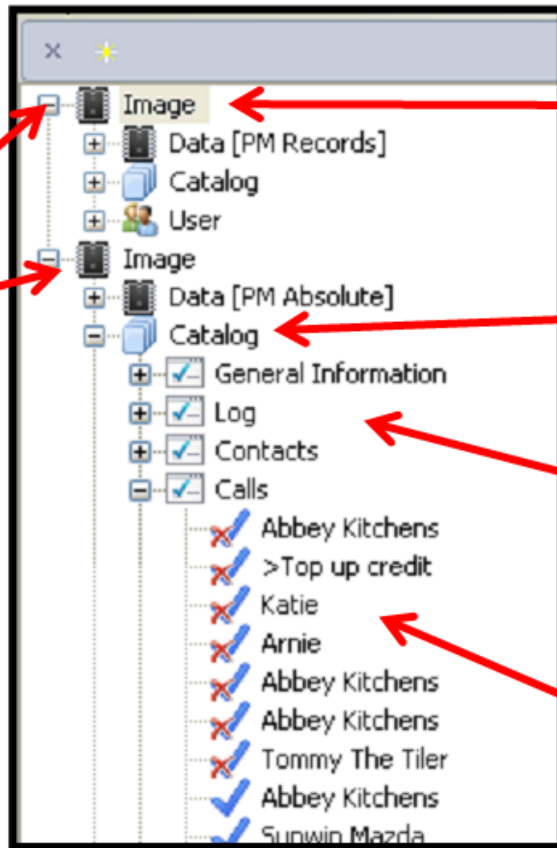
/2010 9:46:19 PM
/2010 12:06:42 PM
>
.7
: No. 110
: iPhone 2G_3G_3GS.zip



MSAB XACT 1



XACT Project Structure



“Image” entries are always at the top level in the XACT Project window

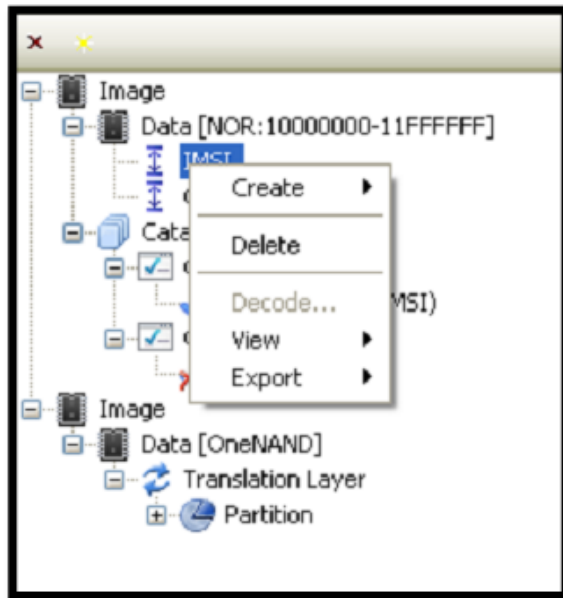
“Catalog” provides a home for decoded calls, calendar etc.

Decoded data is grouped into “Views” (e.g. Calls etc.)

Decoded data “items” the red cross indicates “deleted” or “inactive”

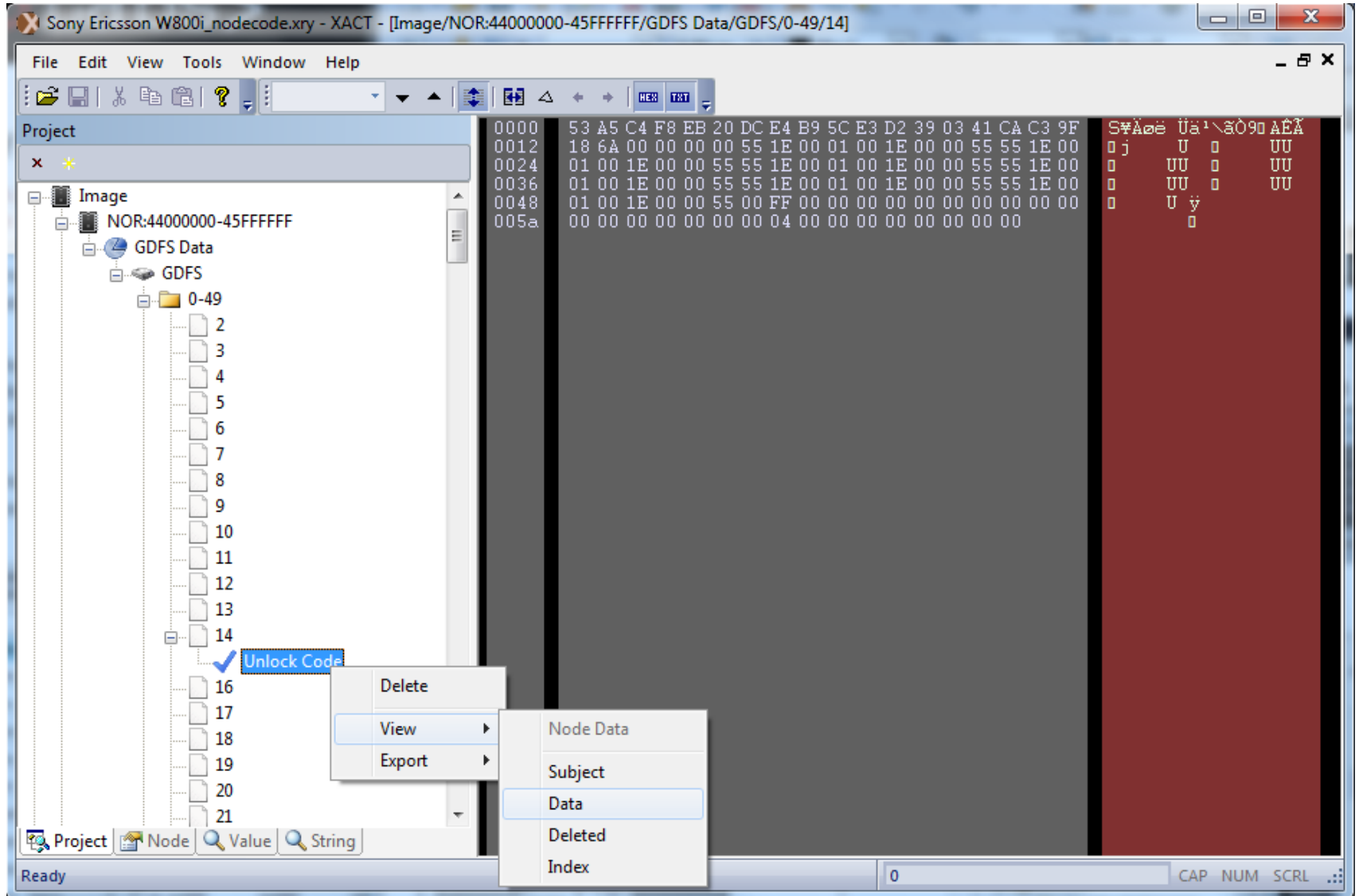
An XACT project may contain more than one image (memory dump)

XACT Project Structure



- All entries in the Project window are “nodes”
- Different actions are available for each node type
 - Right click on a node to select an action
- Some node types can be double-clicked to view data in a separate hex viewer window

MSAB XACT 2



```
0000 53 A5 C4 F8 EB 20 DC E4 B9 5C E3 D2 39 03 41 CA C3 9F
0012 18 6A 00 00 00 00 55 1E 00 01 00 1E 00 00 55 55 1E 00
0024 01 00 1E 00 00 55 55 1E 00 01 00 1E 00 00 55 55 1E 00
0036 01 00 1E 00 00 55 55 1E 00 01 00 1E 00 00 55 55 1E 00
0048 01 00 1E 00 00 55 00 FF 00 00 00 00 00 00 00 00 00 00
005a 00 00 00 00 00 00 00 04 00 00 00 00 00 00 00 00 00
```

```
S#Åæë Üa¹\ãÖ90 ÅEÄ
0 j U 0 UU
0 UU 0 UU
0 UU 0 UU
0 U ý
0 0
```

- Unlock Code
- Delete
- View
 - Node Data
- Export
 - Subject
 - Data
 - Deleted
 - Index

Project Node Value String

Ready

0 CAP NUM SCRL

Viewing Item Properties



- “Node view” is used to view the contents of a data item

[-] Node	Type	ITM
[-] Properties (3)	Deleted	No
	Format	Bool
	Encoding	None
	Size	4
	Length	3
[+] Type	Dialled	
[+] Tel	07749886450	

Node

Project Node

Live (not deleted)

Dialled call

To 07749 886450

MSAB XACT 3

The screenshot displays the MSAB XACT 3 interface. The main window shows a hex editor with memory addresses from 0000 to 01ef and their corresponding hexadecimal values. A search dialog is open, showing a list of search formats. The 'Format' dropdown is set to 'GSM (7 bit packed)'. The search results list includes various encoding formats such as ANSI, UTF8, and GSM variants.

Project: SonyEricsson_K800i_NAND_NAND512R3A.bin

Search Dialog:

- Text
- Hex
- Data
- Dictionary Search
- File Signature Search
- Findstrings
- Number Search
- PDU Finder
- Regex search
- Timestamp Search
- Format: GSM (7 bit packed)

Search Results:

- ANSI
- ANSI No Case
- Unicode Big Endian (Motorola)
- Unicode Little Endian (PC/Intel)
- ANSI and Unicode
- ANSI and Unicode No Case
- UTF8
- UTF7
- GSM (7 bit packed)
- GSM No Case (7 bit packed)
- GSM (8 bit unpacked)
- MAC
- DEM Latin 1
- IRA/IA5 (7 bit)
- US ASCII (7 bit)
- 8859-1 (West European/Latin 1)
- 8859-2 (Central/East Europe/Latin 2)
- 8859-3 (South European/Latin 3)
- 8859-4 North European/Baltic)
- 8859-5 Cyrillic)
- 8859-6 Arabic)
- 8859-7 Greek)
- 8859-8 Hebrew)
- 8859-9 (Turkish/Latin 5)
- 8859-15 (Latin 9)
- Shift JIS

Hex Editor Content:

0000	0000	FF	FF	FF	FF
0000	000f	FF	FF	FF	FF
0000	001e	FF	FF	FF	FF
0000	002d	FF	FF	FF	FF
0000	003c	FF	FF	FF	FF
0000	004b	FF	FF	FF	FF
0000	005a	FF	FF	FF	FF
0000	0069	FF	FF	FF	FF
0000	0078	FF	FF	FF	FF
0000	0087	FF	FF	FF	FF
0000	0096	FF	FF	FF	FF
0000	00a5	FF	FF	FF	FF
0000	00b4	FF	FF	FF	FF
0000	00c3	FF	FF	FF	FF
0000	00d2	FF	FF	FF	FF
0000	00e1	FF	FF	FF	FF
0000	00f0	FF	FF	FF	FF
0000	00ff	FF	FF	FF	FF
0000	010e	FF	FF	FF	FF
0000	011d	FF	FF	FF	FF
0000	012c	FF	FF	FF	FF
0000	013b	FF	FF	FF	FF
0000	014a	FF	FF	FF	FF
0000	0159	FF	FF	FF	FF
0000	0168	FF	FF	FF	FF
0000	0177	FF	FF	FF	FF
0000	0186	FF	FF	FF	FF
0000	0195	FF	FF	FF	FF
0000	01a4	FF	FF	FF	FF
0000	01b3	FF	FF	FF	FF
0000	01c2	FF	FF	FF	FF
0000	01d1	FF	FF	FF	FF
0000	01e0	FF	FF	FF	FF
0000	01ef	FF	FF	FF	FF

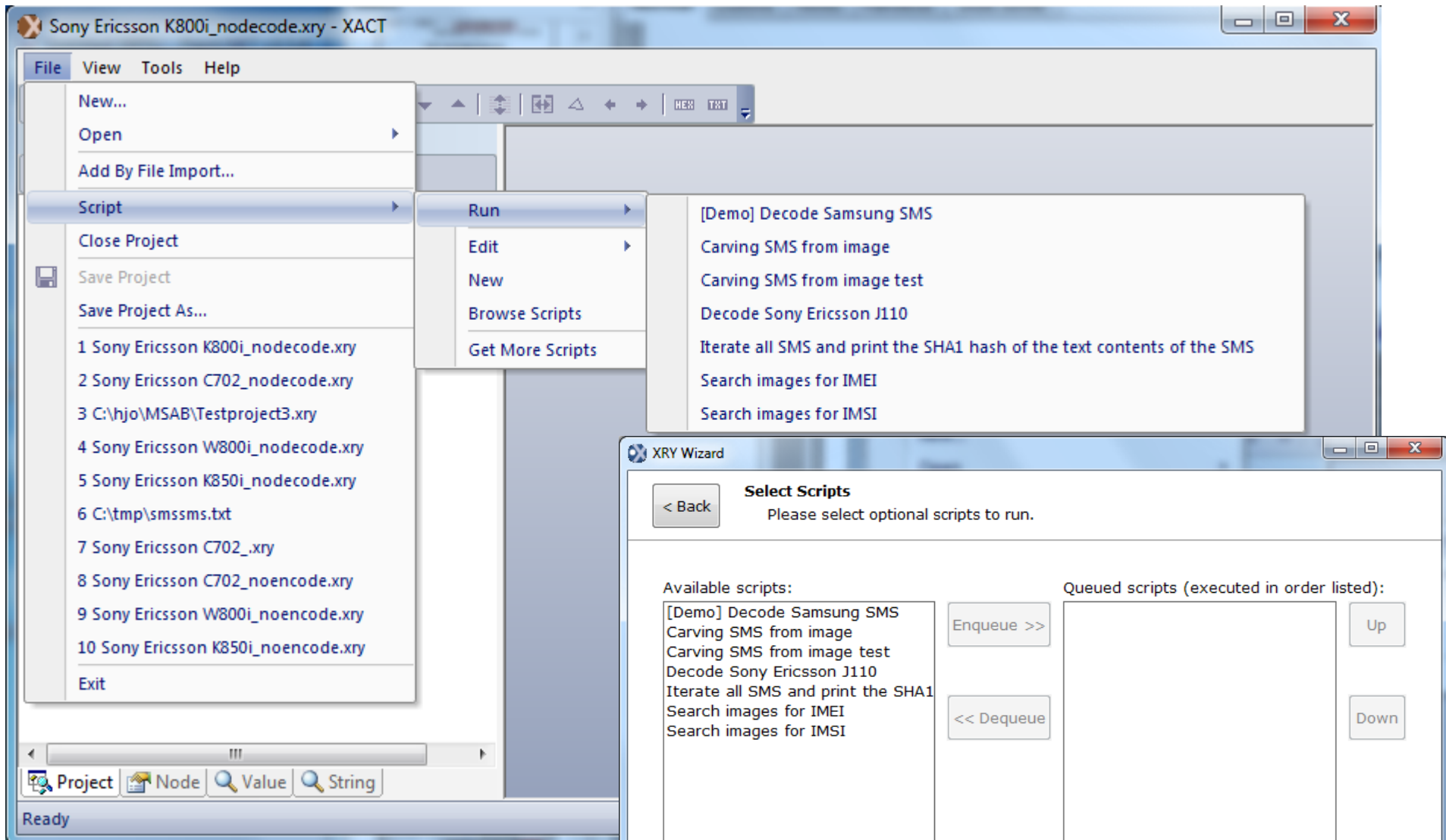
Searching

MSAB XACT 4

SMS 7-bit Encoding

The screenshot displays the MSAB XACT 4 interface with the following components:

- String Panel:** A red box highlights the 'String' panel where 'Encoding' is set to '7Bit' and 'Codepage' is set to 'Ansi'.
- Find Dialog:** A 'Find' dialog box is open, showing a 'Regex search' mode with the search expression `\x07\x91\x13.....\xFF\xFF\xFF\xFF`. A red box highlights the 'String' button in the bottom toolbar.
- Hex View:** The main window shows a hex dump of the file `SonyEricsson_K800i_NAND_NAND512R3A.bin`. The hex data is displayed in columns, with corresponding ASCII characters shown to the right.
- Annotations:** Two arrows labeled 'SMS - text end start' point to the beginning and end of a text block in the hex view.
- Text Content:** The text on the left reads 'Goedenmorgen schoonheid'. The text on the right is a block of 7-bit encoded characters, including 'y yyy yyyyyy', '000 0W000öyyyyy"', '00 `# 2e y0Çw', '\v·BòsÜ Ni·0', and 'JN 0 yyyyyyyyyyyyyy'.



MSAB XACT Phyton scripts

Decode images Wizard (XRY starts)

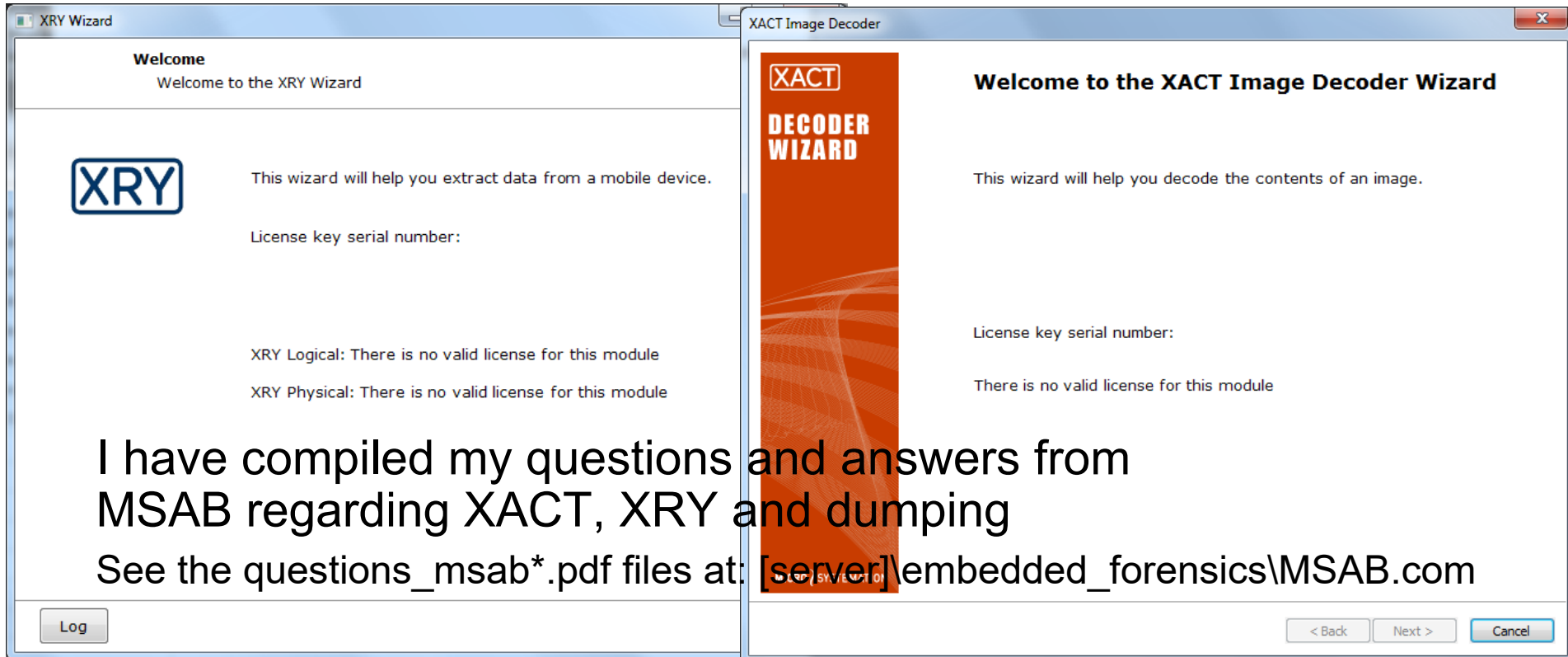
Remember queued scripts for this model

Log

Next >

MSAB no-license limitations

- XRY - cannot do data extraction or create new .xry projects
 - SIM cloning is not possible without license
- XACT - cannot do image decoding or run MSAB Python scripts
 - Can be done with your own tools if they are good



I have compiled my questions and answers from MSAB regarding XACT, XRY and dumping

See the questions_msab*.pdf files at: [\[server\]embedded_forensics\MSAB.com](http://[server]embedded_forensics\MSAB.com)

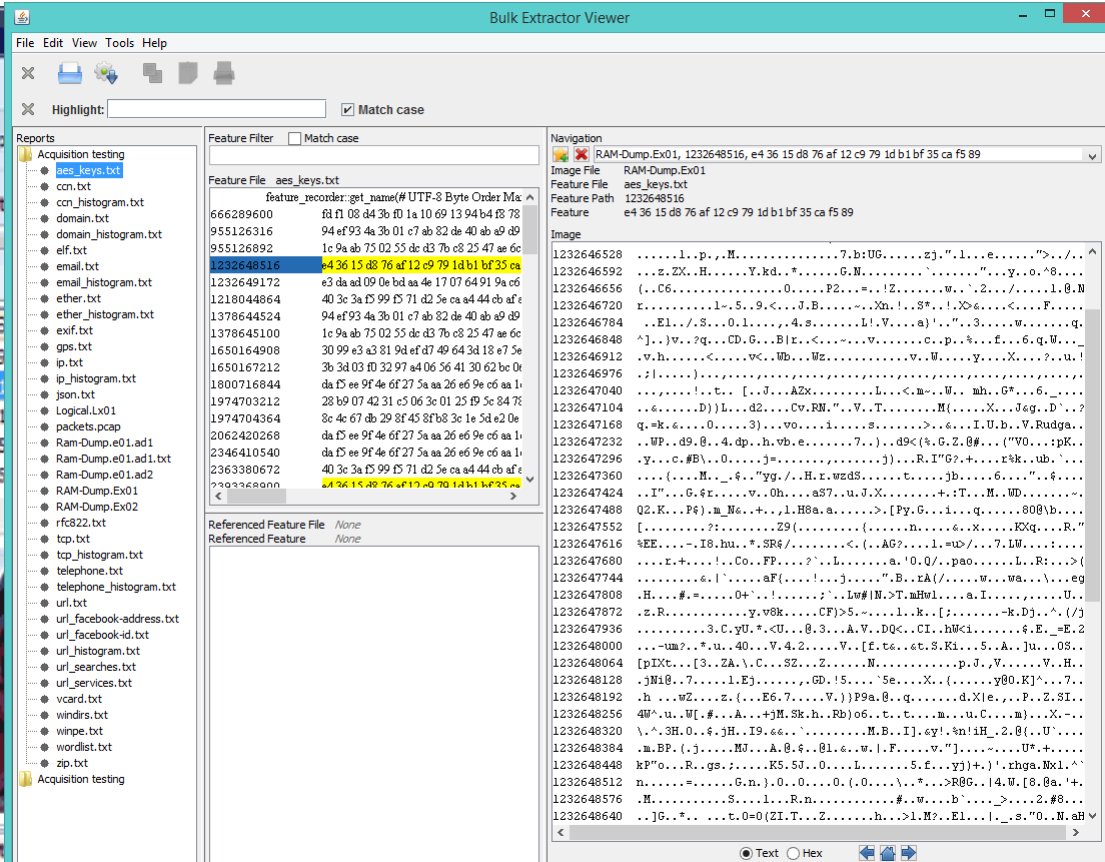
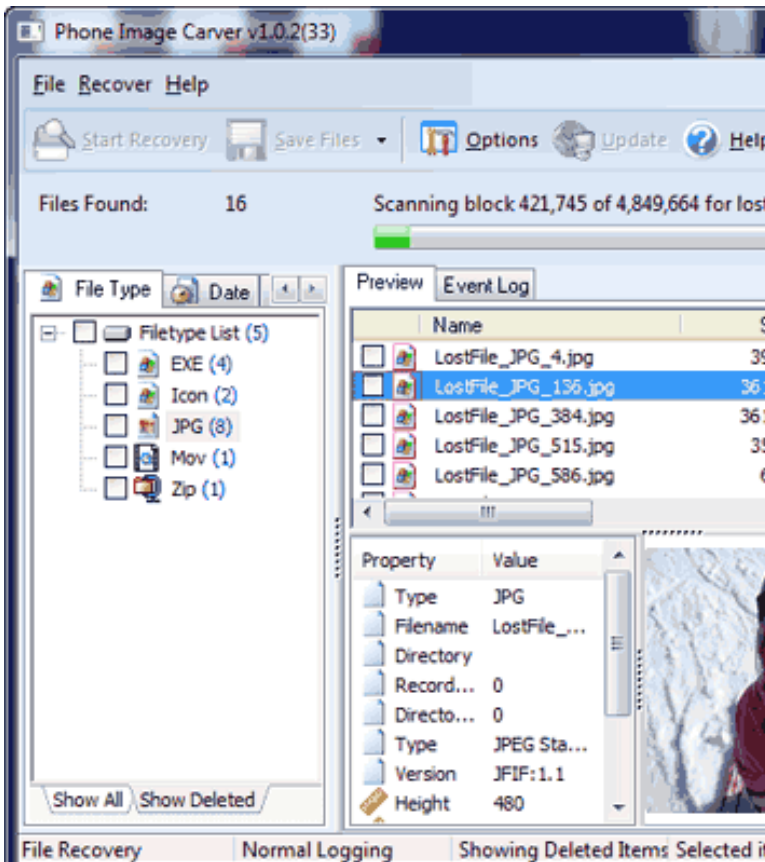
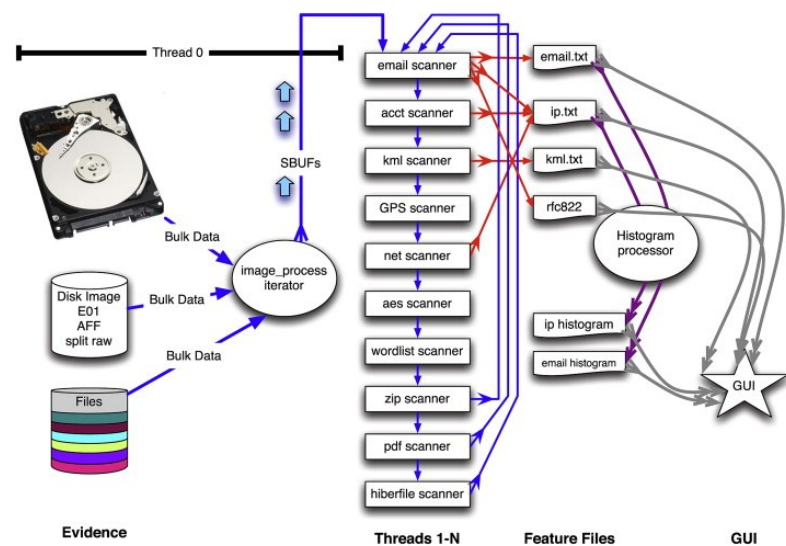
Extracting dump data

Spare area may or may not be included in MSAB phone dumps!

- Non file based
 - Lock keys, IMEI, IMSI, ICCID
 - SMS, time stamps?, call logs?..., etc.
- File based – for best results you need to get rid of the NAND OOB/spare area (present in chip read dumps)
 - MMS, audio files, call logs
 - Videos - 3GP / MP4 with tools as NFI Defraser
 - E-mail, social data
 - Pictures, if damaged, the exif info may be intact (thumbnail)
 - Contacts, notes, calendar, positions, ..., etc. everything!
- Recover the file system if possible via FTL translation
 - If format is raw read from memory (chip physical)
 - If dumped via software it "should" be easier creating a filesystem
- Check out all the submissions to the DFRWS 2010 challenge for tools and ideas
 - <http://www.dfrws.org/2010/challenge/results.shtml>

Carving dump data tools

- Phone Image Carver
- Bulk Extractor



MSAB Building a file system

```
# Building a file system
# In this example we'll build a FAT file system on a memory which has 512 bytes of data
# and 16 bytes of spare area. The memory contains 1024 of these pages so the memory is
# 540672 bytes in total size. Our goal is to filter out these 16 bytes and keep the rest
# as data and remap this data into a linear partition so that the FAT file system parser
# can work with it.
import xact

__contact__ = "hjo@du.se"
__version__ = "0.1.0"
__description__ = "FAT Sample"

# Entry point
def main(images):
    # For each image which has the type set to "NAND:10000" we'll create a FAT
    # file system. The type is arbitrary and not based on any phone in particular.
    for image in filter(lambda i: i.type == "NAND:10000", images):

        # Generate a list of tuples which will be the offset of each page
        # and then the size of each page minus the spare area. See documentation
        # for xact.Image.add_partition.
        segments = list(zip(range(0, 540672, 528), [512] * 1024))

        # The add_partition will automatically parse the FAT file system and
        # generate the volumes.
        partition = image.add_partition("FAT partition", segments, xact.PARTITION_FAT)

        # Log informational message with the name of each FAT partition.
        for volume in partition.volumes:
            print("Decoded FAT partition:", volume.name)
```

build_fat_fs.py
from the XACT manual

Digital Forensics Framework

with winner of DFRWS 2010 Python module script

The image displays two screenshots of the NodeBrowser interface. The top screenshot shows a file list with columns for Name, Size, Accessed time, Changed time, Modified time, and Module. The bottom screenshot shows a directory tree on the left and a grid of recovered files on the right, including several JPEG images and a MOV file.

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

Recovered files shown in the bottom screenshot:

- DSC00006.JPG
- DSC00005.JPG
- DSC00004.JPG
- DSC00003.JPG
- ._SC00010.JPG
- ._SC00009.JPG
- ._SC00008.JPG
- ._SC00007.JPG
- MOV00002.3GP
- DSC00007.JPG

Recovery of the file system
via FTL translation

FTK >= 3.2 have YAFFS and Ext4 support DMG dump from iPhone 3G

AccessData Forensic Toolkit Version: 3.2.0.32216 Database: localhost Case: iphone

File Edit View Evidence Filter Tools Manage Help

Filter: -unfiltered- Filter Manager...

Explore Overview Email Graphics Bookmarks Live Search Index Search Volatile

Evidence Items File Content

Evidence
iphone3g.dmg
Partition 1
iPhone3G [HFS+] (highlighted in red)
[unallocated space]
iPhone3G
private
etc
alternatives
apt
bluetooth
default
dpkg
pam.d
ppp
profile.d
racocon
var
mobile
Applications
Library
Media
preferences
SystemConfiguration
Unpartitioned Space [Apple]

File Content

Hex	Text	Filtered	Natural
00000400	48 2B 00 04 00 00 01 00-38 2E 31 30 00 00 00 00		H+.....8.10...
00000410	C8 47 BF F7 C8 47 C0 51-00 00 00 00 C8 47 BF F7		ÈGz+ÈGÀQ...ÈGz+
00000420	00 00 11 FD 00 00 02 2D-00 00 10 00 00 01 03 F8		...ý.....ø
00000430	00 00 0C 43 00 00 00 00-00 01 00 00 00 01 00 00		...C.....
00000440	00 00 14 3B 00 00 00 02-00 00 00 00 00 00 00 01		...;.....
00000450	00 00 00 00 00 00 00 00-00 00 00 00 00 00 00 00	
00000460	00 00 00 00 00 00 00 00-00 00 00 00 00 00 00 00	
00000470	00 00 00 00 00 00 30 00-00 00 30 00 00 00 03	0...0.....
00000480	00 00 00 01 00 00 03-00 00 00 00 00 00 00 00	
00000490	00 00 00 00 00 00 00 00-00 00 00 00 00 00 00	
000004a0	00 00 00 00 00 00 00 00-00 00 00 00 00 00 00	
000004b0	00 00 00 00 00 00 00 00-00 00 00 00 00 00 00	
000004c0	00 00 00 00 02 00 00-00 02 00 00 00 00 00 20	
000004d0	00 00 00 04 00 00 20-00 00 00 00 00 00 00 00	
000004e0	00 00 00 00 00 00 00 00-00 00 00 00 00 00 00	
000004f0	00 00 00 00 00 00 00 00-00 00 00 00 00 00 00	
00000500	00 00 00 00 00 00 00 00-00 00 00 00 00 00 00	
00000510	00 00 00 00 34 00 00-00 08 00 00 00 03 40	4.....@
00000520	00 00 00 24 00 00 40-00 00 04 E1 00 00 00 80		...\$...@...á...
00000530	00 00 11 A1 00 00 80-00 00 43 CA 00 00 00 80		...j.....CÈ...
00000540	00 00 5A 3D 00 00 80-00 00 63 B6 00 00 00 80		...Z=.....cŸ...
00000550	00 00 89 22 00 00 80-00 00 00 00 00 00 00 00		...".

Cursor pos = 0; log sec = 0; phy sec = 64

File Content Properties Hex Interpreter

File List

Name	Label	Item #	Ext	Path	Category	P-Size	L-Size	MD5	SHA1	SHA256	Created	Accessed	Modified
Partition 1		1004		iphone3g.dmg/Partition 1	Partition	260,0 MB	260,0 MB				n/a		n/a
Unpartitioned Sp...		1001		iphone3g.dmg/Unpartitioned Space [Apple]	Unpartitioned S...	n/a	n/a				n/a		n/a

Loaded: 2 Filtered: 2 Total: 2 Highlighted: 1 Checked: 0 Total LSize: 260,0 MB

iphone3g.dmg/Partition 1

Ready

Explore Tab Filter: [None]

Oxygen Forensic Suite

Oxygen Forensics – many demo dumps on [server]

The screenshot displays the Oxygen Forensic Suite 2012 Analyst interface. The main window shows a grid of image thumbnails from a folder named 'Patrick Payge's iPhone 3GS - 10.05.2011 23:19:56'. The selected file is 'IMG_0051.JPG'. The interface includes a menu bar (Main, View, Tools, Service, Help), a toolbar with various actions like Search, Export, Print, and a 'Viewer' button. On the left, there is a sidebar with 'Tasks for files and folders', 'Object information', 'Exif information', and 'Geo positioning'. The 'Geo positioning' section shows a map with a red pin at the location of the image. The bottom right corner features a hex editor displaying the raw data of the selected image file.

Object information

Name: IMG_0051.JPG
Type: JPEG-рисунок
Size: 983,06 KB
Modified: 24.01.2011 15:21:56
MD5 Hash:
4811944ce31dfe659ed170951962f8e1
Folder: C:\DCIM\100APPLE

Exif information

Geo positioning

Geo position (from Exif)
Latitude: N 33,761499
Longitude: W 84,386333

Hex Editor

00000000:	FF D8 FF E1 1F B2 45 78	69 66 00 00 4D 00 00 2A
00000010:	00 00 00 08 00 0B 01 0F	00 02 00 00 00 06 00 00
00000020:	00 92 01 10 00 02 00 00	00 0B 00 00 00 00 98 01 12
00000030:	00 03 00 00 00 01 00 01	00 00 01 1A 00 05 00 00
00000040:	00 01 00 00 00 A4 01 1B	00 05 00 00 00 01 00 00
00000050:	00 AC 01 28 00 03 00 00	00 01 00 02 00 00 01 31
00000060:	00 02 00 00 00 06 00 00	00 B4 01 32 00 02 00 00
00000070:	00 14 00 00 00 BA 02 13	00 03 00 00 00 01 00 01
00000080:	00 00 87 69 00 04 00 00	00 01 00 00 00 00 CF 88 25

Analyst version: 4.0.1.89 Patrick Payge's iPhone 3GS Total objects: 18 Selected: IMG_0051.JPG MD5 Hash: 4811944ce31dfe659ed170951962f8e1

AccessData MPE+

Mobile Phone Examiner+ Investigator v5.2.1.499

Supported Images (*.ad1, *.fat, ...)

Supported Images (*.ad1, *.fat, *.e01, *.yaffs, *.yaffs2, *.ext, *.ext2, *.ext3, *.ext4, *.tar, *.dd4, *.dd8, *.dd4.001, *.dd8.001)

All files (*.*)

AD1 (*.ad1)

FAT (*.fat)

E01 (*.e01)

YAFFS (*.yaffs)

YAFFS2 (*.yaffs2)

EXT (*.ext)

EXT2 (*.ext2)

EXT3 (*.ext3)

EXT4 (*.ext4)

TAR (*.tar)

DD4 (*.dd4)

DD8 (*.dd8)

DD4.001 (*.dd4.001)

DD8.001 (*.dd8.001)

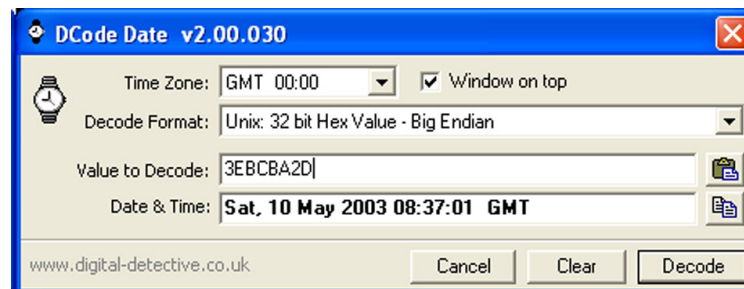
AccessData
MOBILE PHONE EXAMINER
PLUS

MPE+

800-658-5199 (North America)
Email: support@accessdata.com
Email: sales@accessdata.com
Discussion Forum

Time stamps and search terms

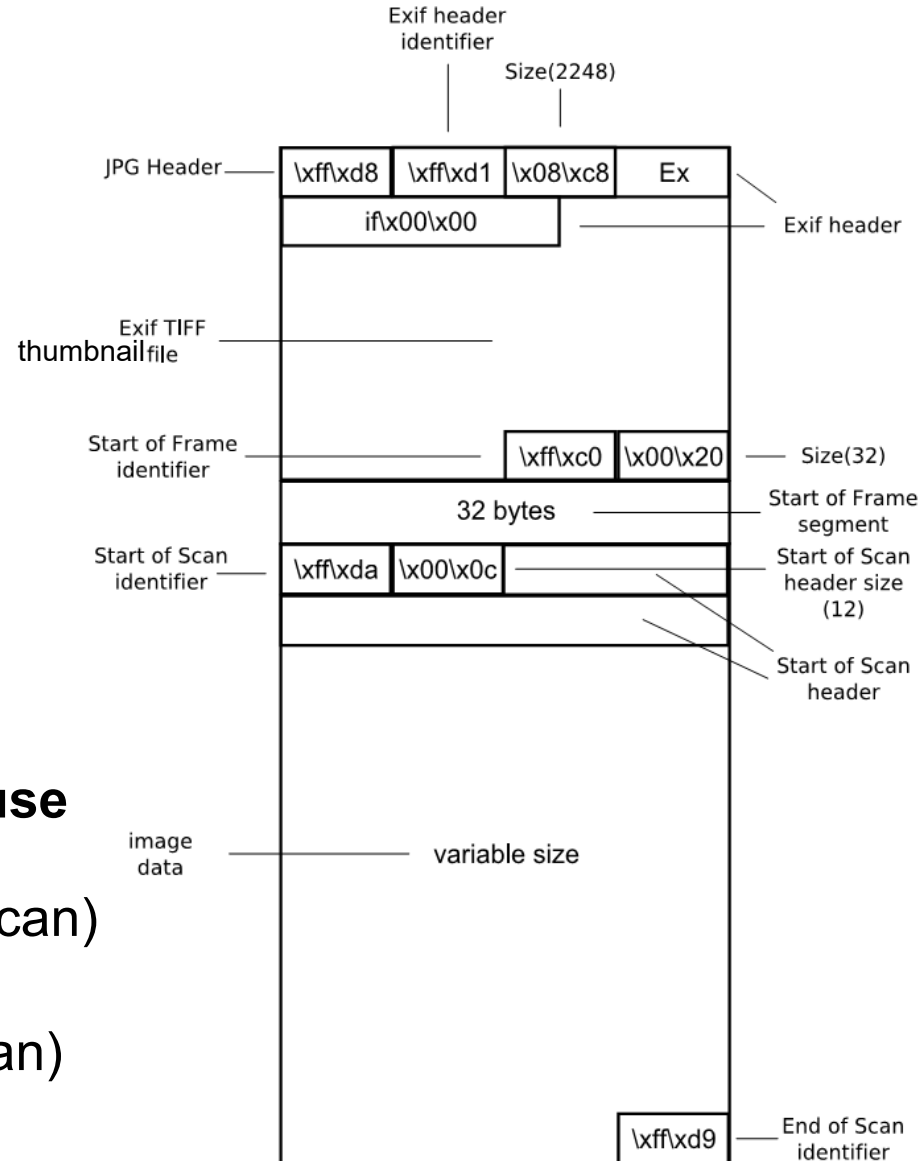
- A wide variety of storage formats are used for storing timestamp data in embedded system memories
- To illustrate - the timestamp "30 April 2008 14:30:59 UTC" is encoded as follows in some formats found in different mobile phone memories:
 - 0x80400341039500 (ETSI SMS)
 - 0xB19E0CA3 (Nokia)
 - 0x07D8041E0E1E3B (Nokia)
 - 0x26041E0E1E3B (Motorola)
 - 0x00E129CB0E8B2EC0 (Symbian)
 - 0x481882A3 (POSIX)
- Regular Expressions and Search Terms for Phone Examiners
 - <http://www.controlf.net/regexps/>
- Remember!
 - Many forensic artifacts are stored in manufacturer-specific or proprietary formats, it can even change between different models and revisions from the same manufacturer!



<http://www.digital-detective.co.uk/>

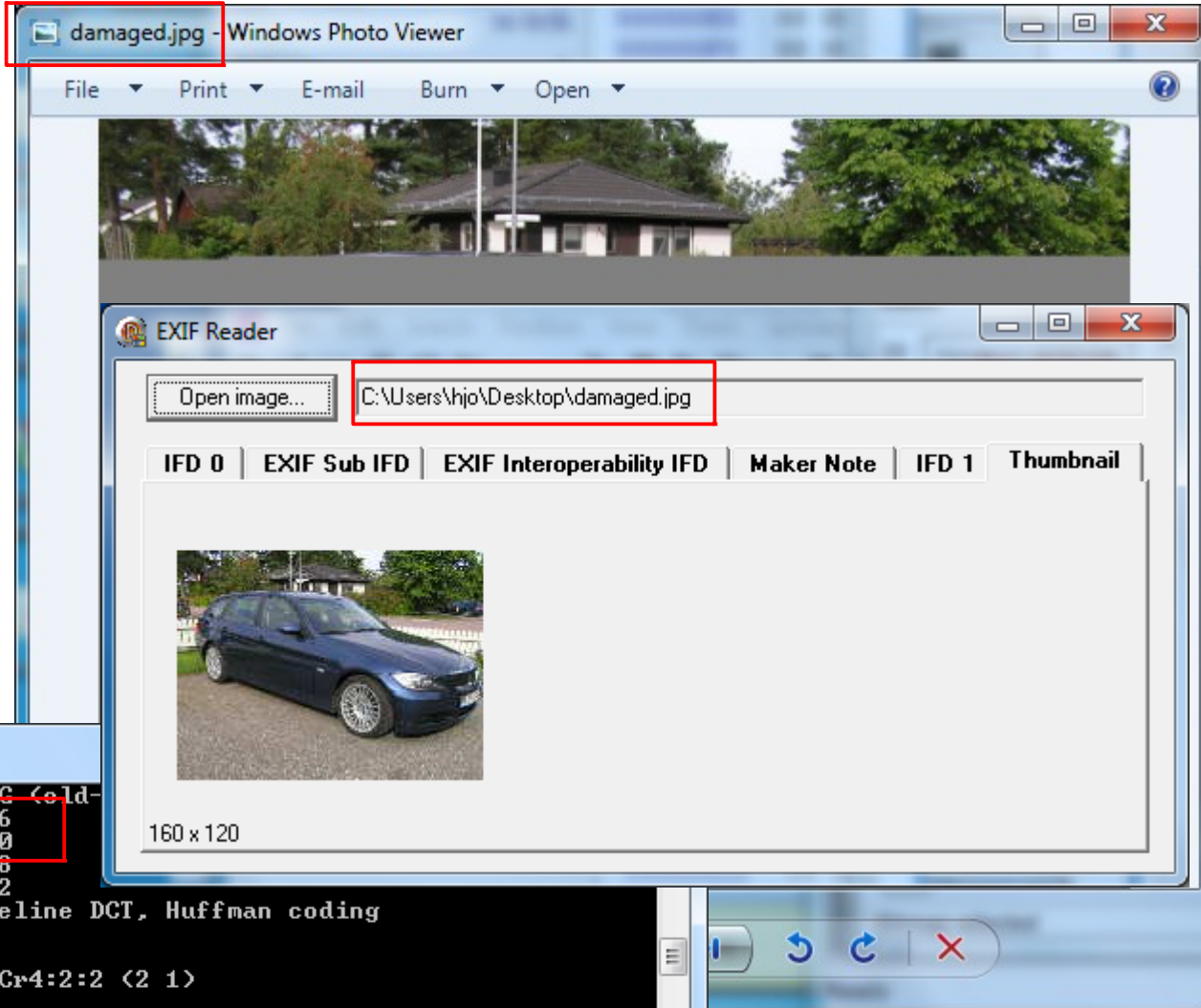
JPG file structure and carving

- Scalpel/Photorec etc.
- JFIF = 0xFFD8FFE0
- Exif = 0xFFD8FFE1
- Beware of Samsung JPG header 0xFFD8FFE3
- JPEG file structure
 - JPEG header
 - Exif header identifier
 - Exif header
 - Exif TIFF data
 - **Exif JPEG Thumbnail (may use a JFIF header and footer)**
 - Start of image data (Start of scan)
 - Image data
 - End of image data (End of scan)



Exif JPEG Thumbnail

exiftool



```
C:\utils\exiftool\exiftool(-k).exe
Compression      : JPEG (old-
Thumbnail Offset : 4096
Thumbnail Length : 5130
Image Width      : 2288
Image Height     : 1712
Encoding Process : Baseline DCT, Huffman coding
Bits Per Sample  : 8
Color Components  : 3
Y Cb Cr Sub Sampling : YCbCr4:2:2 (2 1)
Aperture         : 4.0
Image Size       : 2288x1712
Scale Factor To 35 mm Equivalent: 6.0
Shutter Speed    : 1/4000
Thumbnail Image   : <Binary data 5130 bytes, use -b option to extract>
Circle Of Confusion : 0.005 mm
Field Of View     : 50.6 deg
Focal Length      : 6.3 mm (35 mm equivalent: 38.1 mm)
Hyperfocal Distance : 2.00 m
Light Value       : 13.3
-- press any key --
```

Position artifacts

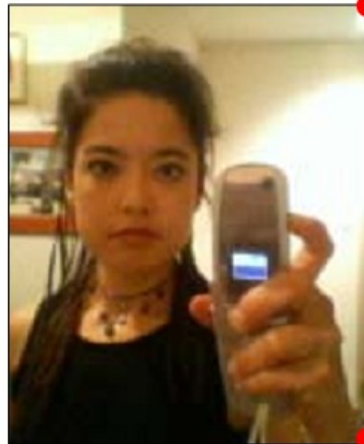
- Cached map queries
 - Traffic/navigation or social networking applications
 - GPS coordinates embedded in Exif

METADATA TAGS USED IN EXIF (JEITA CP-3451)

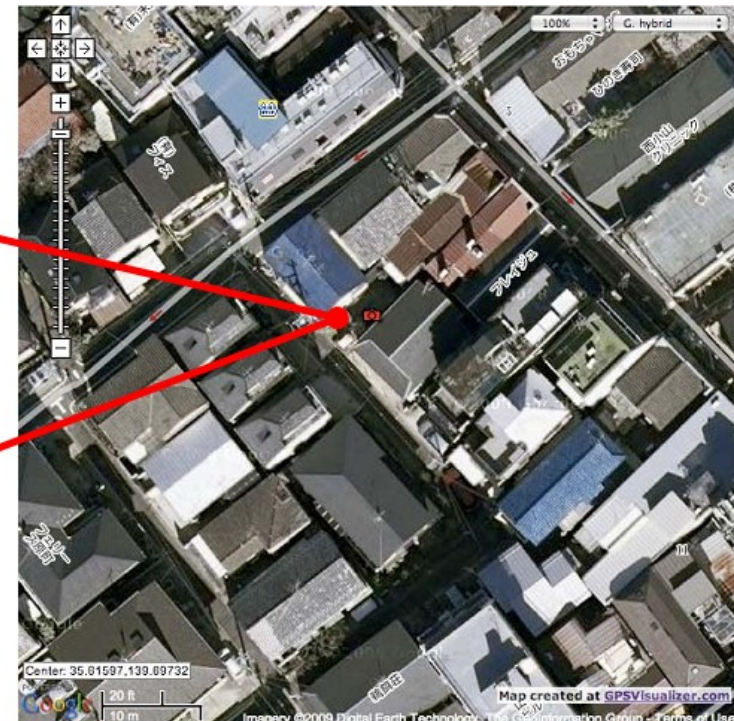
GPS IFD
Tags Relating to GPS
GPSVersionID
GPSLatitudeRef
GPSLatitude
GPSLongitudeRef
GPSLongitude
GPSAltitude
GPSTimeStamp
GPSSatellites
GPSStatus
GPSMeasureMode
GPSDOP
GPSSpeedRef
GPSTrackRef
GPSTrackRef
GPSImgDirectionRef
GPSImgDirectionRef
GPSMapDatum
GPSDestLatitudeRef
GPSDestLatitude
GPSDestLongitudeRef
GPSDestLongitude
GPSDestBearingRef
GPSDestBearing
GPSDestDistanceRef
GPSDestDistanceRef
GPSProcessingMethod
GPSAreaInformation
GPSDateStamp
GPSDifferential

Digital Still Camera Forensics - SSDDFJ_V1_1_Cohen.pdf

Degrees/Minutes/Seconds
May need conversion

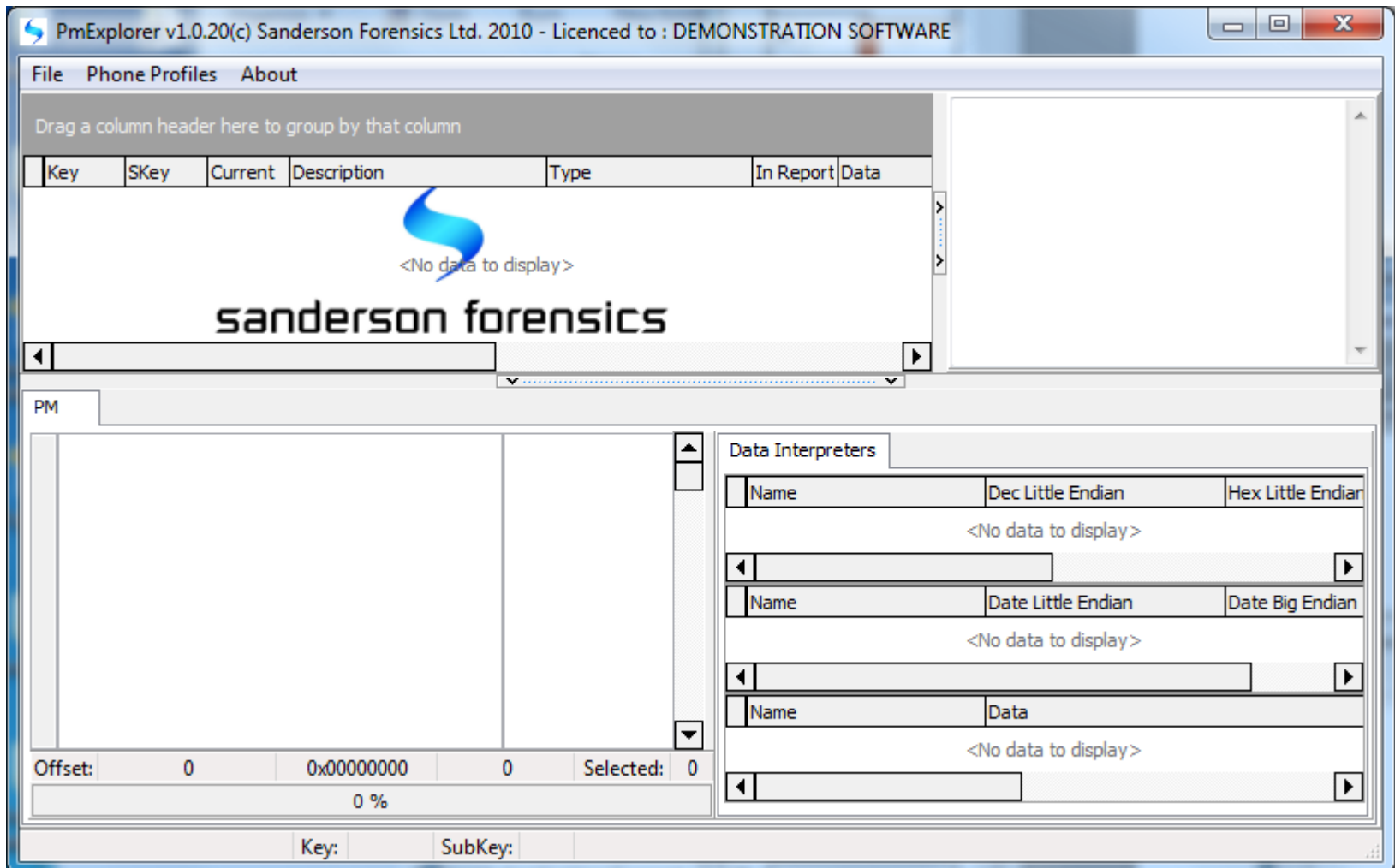


N35 deg 36 '
E139 deg 41'



PmExplorer

- View Nokia PM tables/records (dumps), as SE GDFS?



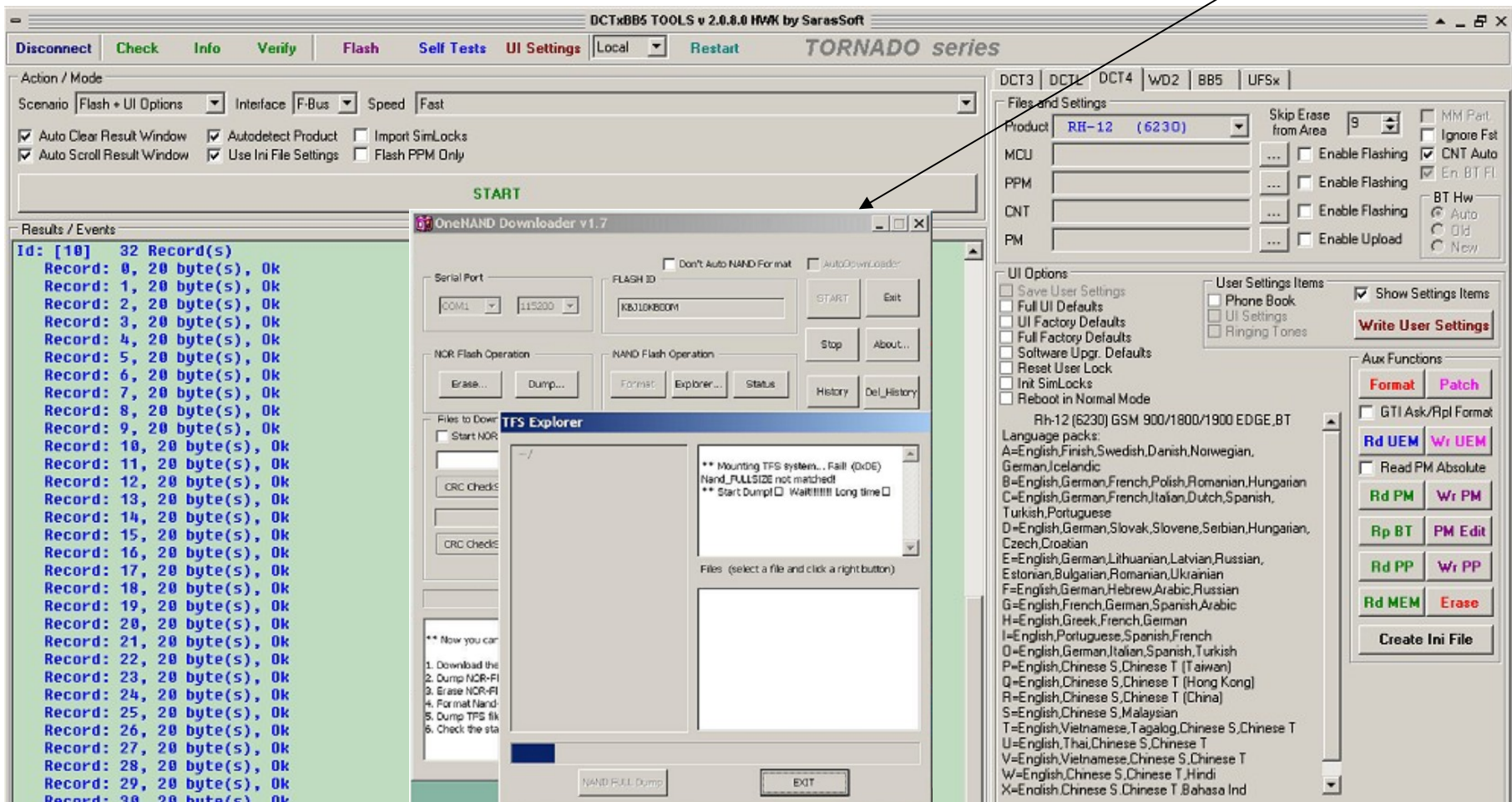
Nokia

PM tables/records

Phone flashers 1

- Designed to update firmware (flash memory)
- Usually a flash memory backup can be made

Samsung
OneNAND
Downloader

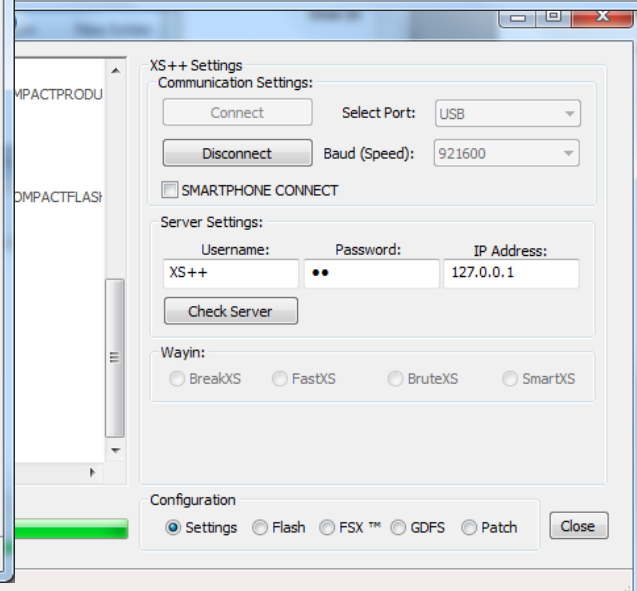
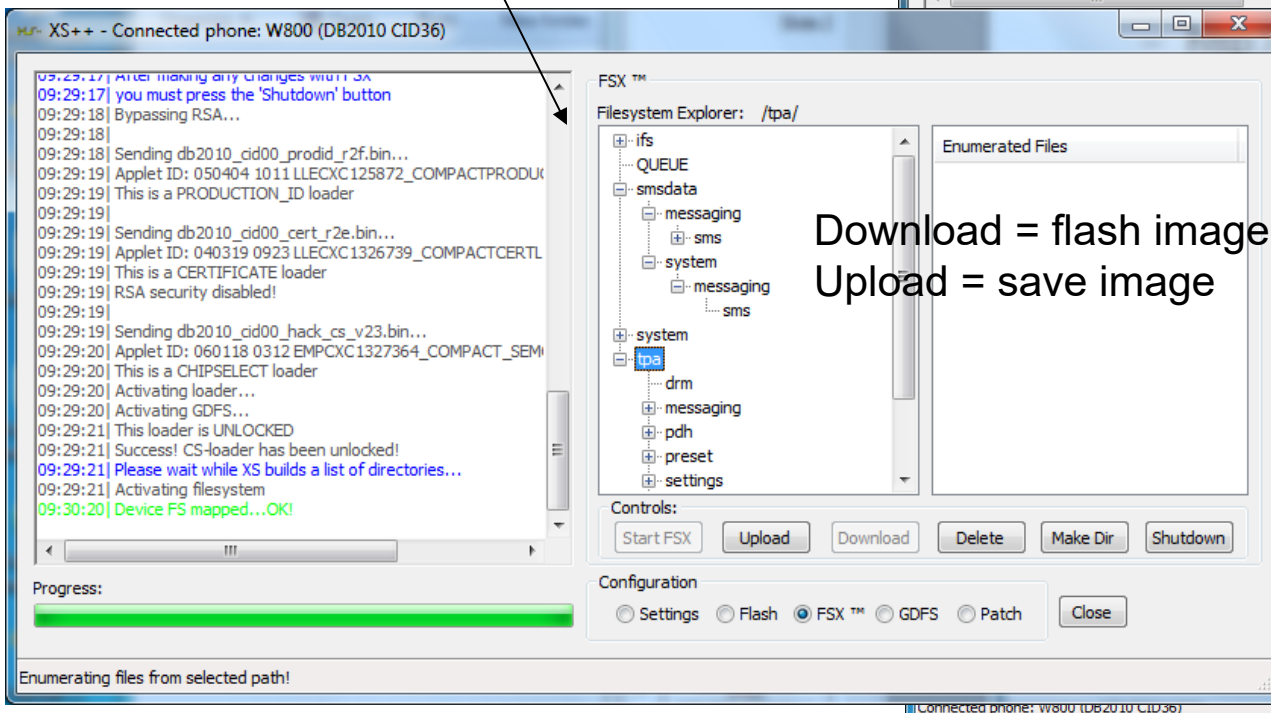
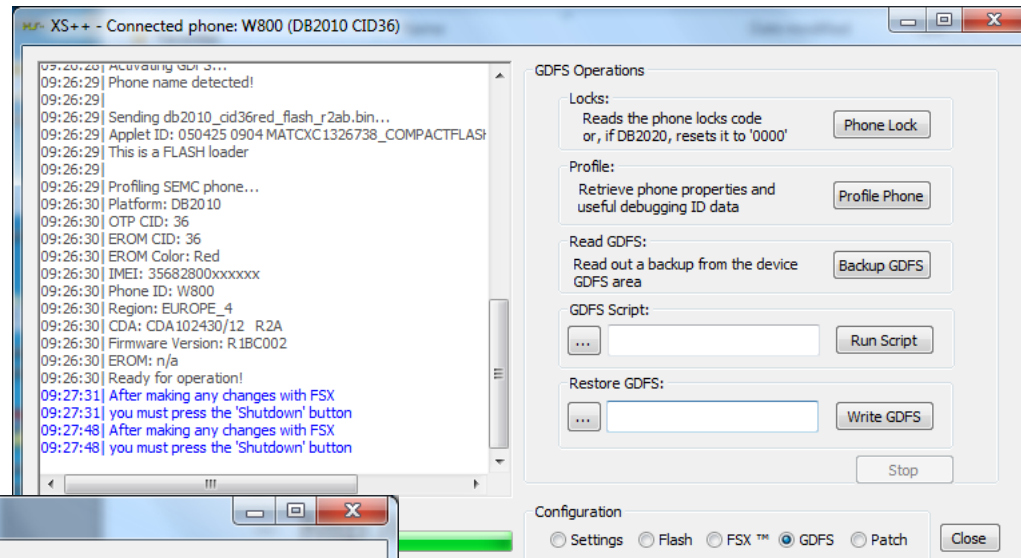


Phone flashers 2

- Sony Ericsson XS++
- GDFS (Global Data File System)

<http://en.wikipedia.org/wiki/GDFS>

SE W800 from lab with (FAT?) FS!



Flasher boxes

- Designed to update flash memory
 - Twister
 - HWK
 - UFS3
 - SHU box
 - JAF box



Simple imaging and analyze of phones

- Some handsets can be attached in off mode and automatically enter a special "file transfer" mode
- Windows may detect the memory (no memory card should be present) as a storage device with a FAT file system
- Use FTK imager or similar to make an image!
- Analyze with existing forensic tools
- Paper describing the method
 - RECOVERING DELETED DATA FROM FAT PARTITIONS WITHIN MOBILE PHONE HANDSETS USING TRADITIONAL IMAGING TECHNIQUES
- Another useful method if it is hard to interpret data is to use an emulator to analyze and interpret the data
 - Extract image or database etc. from an examined phone
 - Boot up the development emulator using this data

Simpler analysis of phone dumps

- If it is possible to create a filesystem of the phone image one should export this dump to an forensic image and use a familiar advanced tool as FTK or Autopsy etc.
- This is especially true if it is a smartphone since it shares a lot of technology with ordinary computers which will ease the investigation a lot
- It can also be beneficial doing this with files in a folder
- Example: <http://computer-forensics.sans.org/blog/2010/09/22/digital-forensics-quick-cellebrite-ufed-extract-phone-data-file-system-dump/>
 - Using a dump from a iPhone 3G IOS 4.02
- Viewing all familiar file types including SQLite files and plist (property list) files etc. setting bookmarks and so on...
 - iPhone .plist files are usually storing serialized objects as user settings or application information in a binary XML format
 - http://en.wikipedia.org/wiki/Property_list