



Mobile memory dumps, MSAB and MPE+

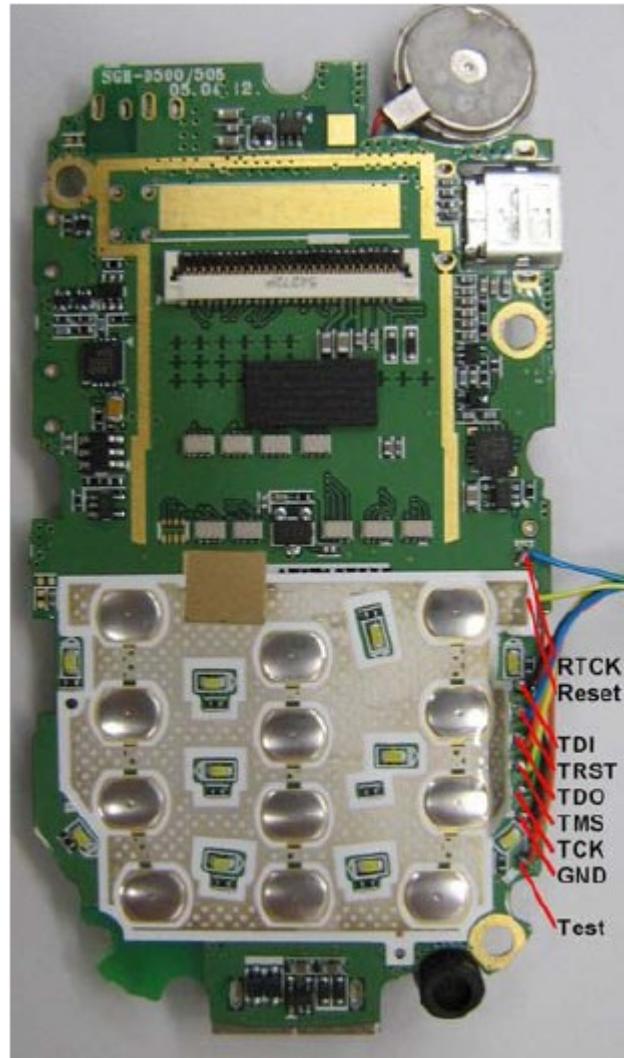
Data collection

Information recovery

Analysis and interpretation of results

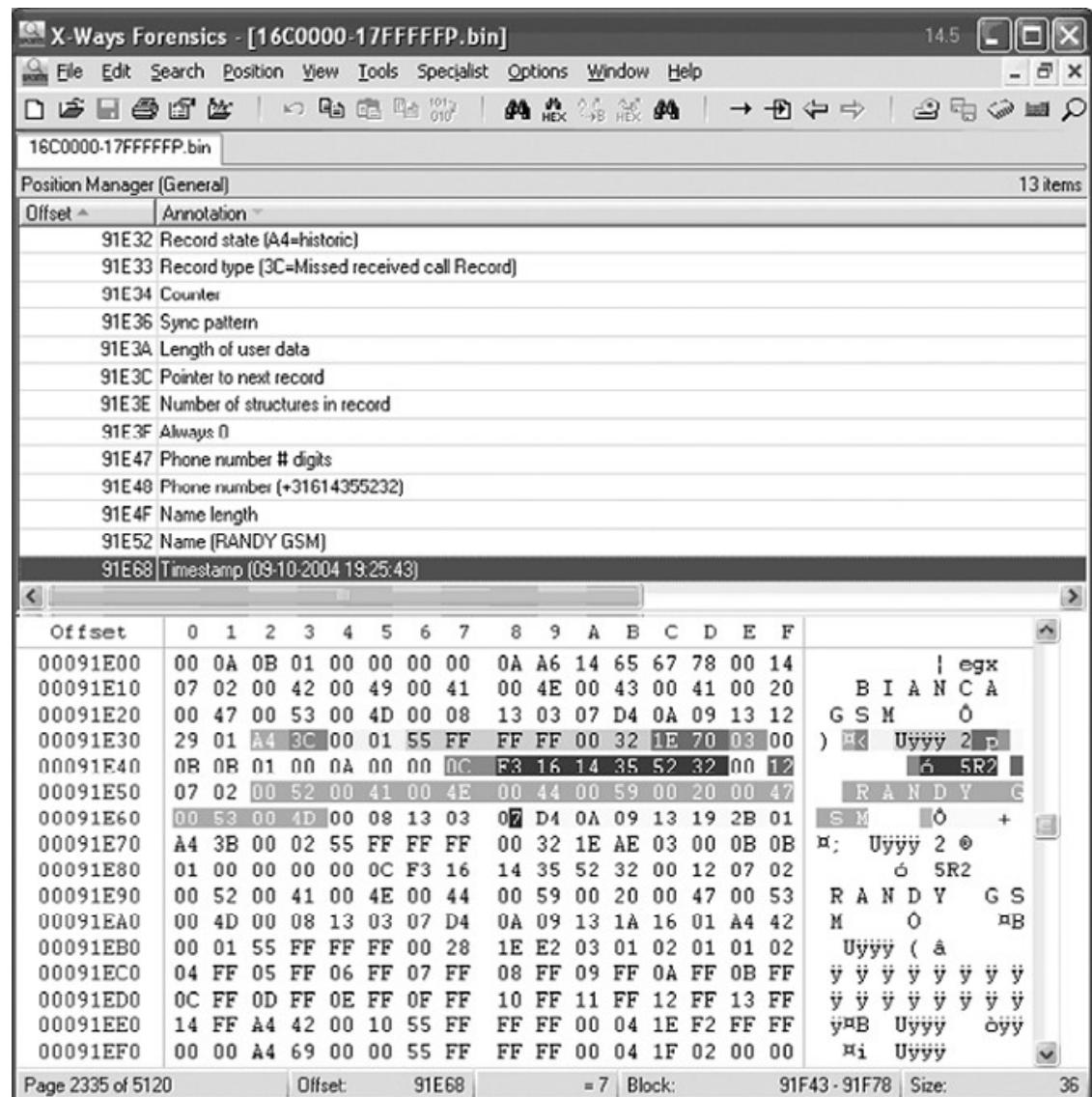
Physical Extraction

- 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>



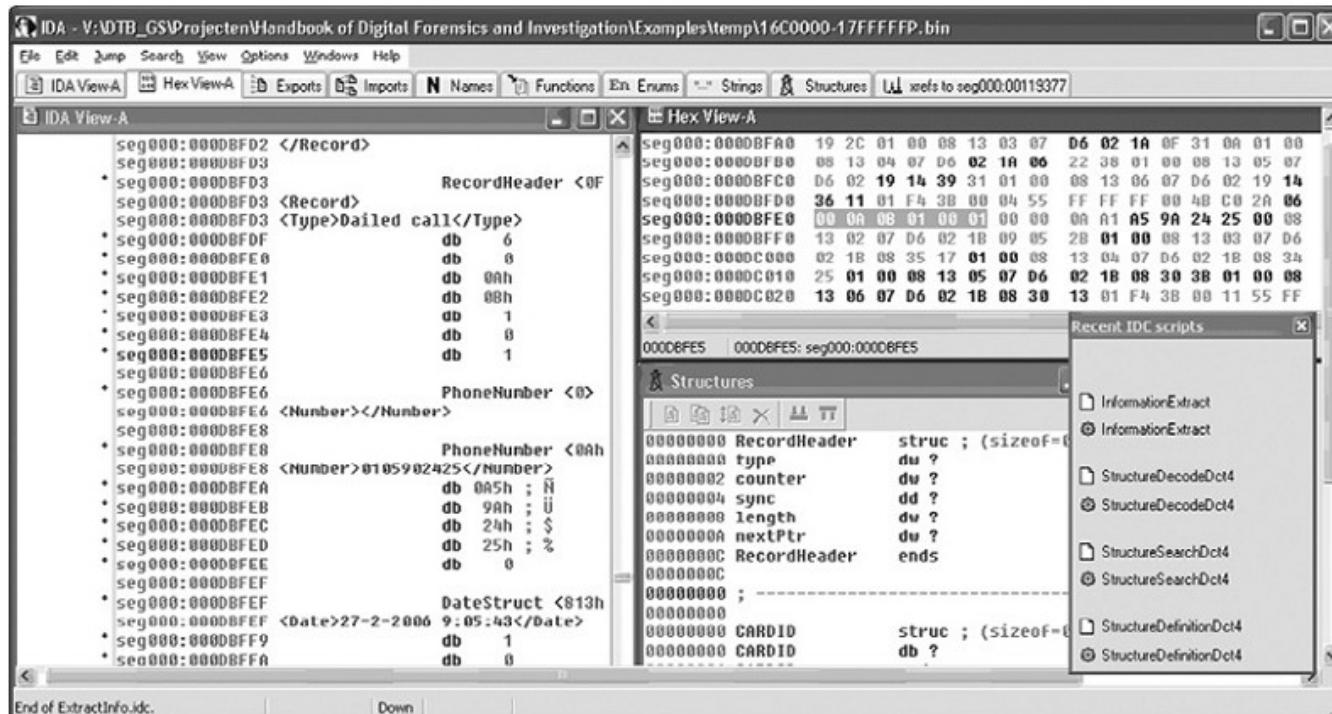
Hex editors - WinHex

- 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

XRY - [SonyEricsson_K800i.xry]

File Edit View Windows Tools Options About

Extract Data Open Close Save Save As File Microsoft Excel Microsoft Word Google Earth OpenOffice XML Print Print Options Device Manual Help Topics

Open Save Export

Media Window

Summary Case Data General Information Contacts Calls SMS Pictures

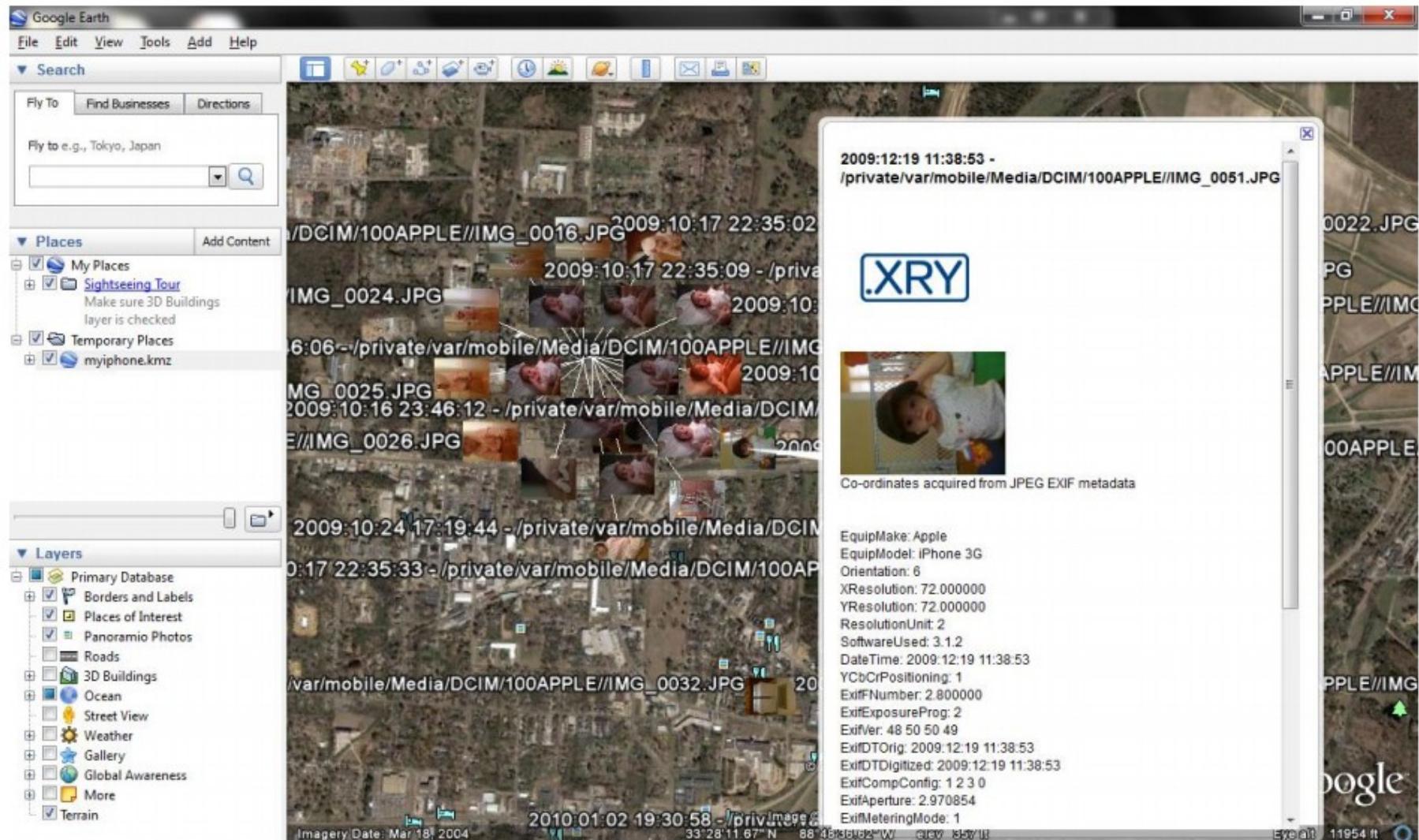
SMS

SMS messages sent or received from the device (13 items)

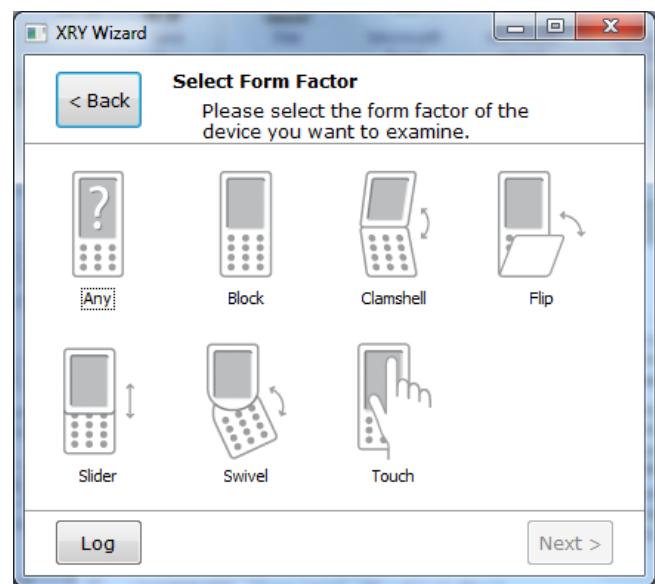
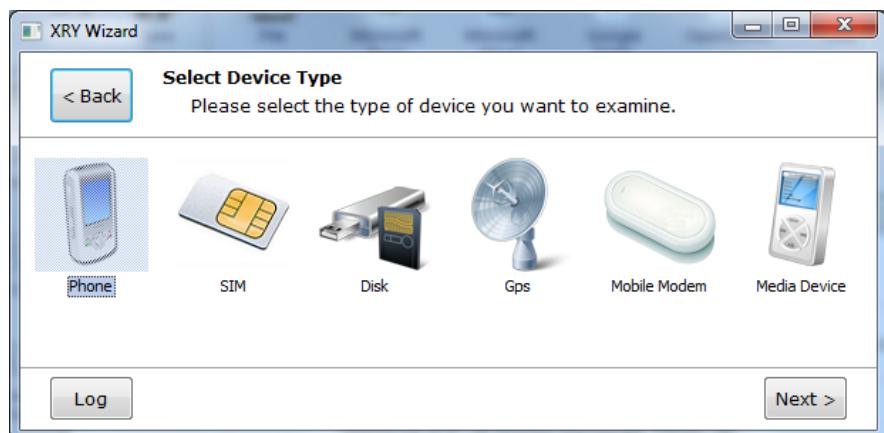
Number	Name	Message	Time	Status	Storage	Index	Service Center
0632082356		Goedenmorgen schoonheid		Sent	Device	1	+31653131313
1300		KPN helpt u graag met het instellen van internet op uw mobiel. U ontvangt hiervoor zometeen instellingen. Accepteer deze als uw toestel er om vraagt. Afz KPN	2010-03-29 13:45:16 (+02:0)	Read	Device	2	+31653131316
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, Stephan.		Sent	Device	3,4	+31653131313
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
+31628954735	[Geen naam]	OK, will look after it	2010-03-30 08:04:30 (+02:0)	Read	Device	6	+31624000115
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 welleuk. Tot straks. hve Stephan		Sent	Device	7,8	+31653131313
0632082356		Vergeet je niet vandaag naar de tandarts te gaan?		Sent	Device	9	+31653131313
+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
0615646978		Everything arranged!		Sent	Device	11	+31653131313

M... E... Pi... Ready CAP NUM SCR

Geocoded Data



MSAB XRY Wizard 1



MSAB XRY 2

XRY Wizard

Select Model

Please select the model you want to examine.

< Back

Sony Ericsson C510 Sony Ericsson C702 Sony Ericsson C901 Sony Ericsson C902 Sony Ericsson D750i

Sony Ericsson Elm J10i2 GreenHeart Sony Ericsson F500i Sony Ericsson G502 Sony Ericsson G700 Sony Ericsson G700 Business Edition

Log

Next >

XRY Wizard

Select Action

Please select type of examination or close the file when finished.

< Back

Logical Physical (Dump+Decode) Dump Import Finish

Log

Next >

XRY Wizard

Device Overview

< Back

Please take a moment to review the details for this device.

Sony Ericsson C702

Network GSM
OS Proprietary

Physical Dump

Connectivity

Cable Ericsson Cable 3

Info

Make sure the battery is fully charged to get an successful extraction.
Remove the battery, SIM and memory card from the phone.
Insert the battery back to the phone.
Insert "Ericsson Cable 3" to the USB port.
Click "Next" to continue the phone dumping.

Other Information

Baseband chipset ID supported: C900 (DB3150)
CID supported: up to 52 (RETAIL(RED), DEVELOPER(BROWN), FACTORY(BLUE))

Physical Decode

Features

Contacts	<input checked="" type="checkbox"/> Not Supported
Calls	<input checked="" type="checkbox"/> Not Supported
SMS	<input checked="" type="checkbox"/> Not Supported
Files	<input checked="" type="checkbox"/> Not Supported
MMS	<input checked="" type="checkbox"/> Not Supported
E-mail	<input checked="" type="checkbox"/> Not Supported
Calendar	<input checked="" type="checkbox"/> Not Supported
Tasks	<input checked="" type="checkbox"/> Not Supported
Notes	<input checked="" type="checkbox"/> Not Supported

Info

Decoding not supported.

Log

Next >



MSAB XRY 3

XRY Wizard

Instructions

Please follow the instructions below.

< Back

1. Ensure that the phone battery is fully charged.
2. Remove the battery, SIM and memory cards from the phone.
3. Insert the battery back to the phone.
4. Insert "Ericsson Cable 3" to the XRY device USB port.
5. Click "Next" to continue the phone dumping.

Log

Next >

XRY Wizard

Select File

Please select file to save the extraction to.

< Back

Save in: C:\hjo\MSAB\dump\

Contents:

- Sony Ericsson C702_nodecode.xry
- Sony Ericsson K800i_nodecode.xry
- Sony Ericsson K850i_nodecode.xry
- Sony Ericsson W800i_nodecode.xry

File name: Sony Ericsson C702.xry

Password:

Use Encryption

Verify:

Log

Next >

XRY Wizard

Processing

XRY is querying the device for information.

< Back

1. Press "C" button on the phone and keeping it pressed attach "Ericsson Cable 3" to the phone.
2. Wait for the driver to be installed, if needed, and for the dumping to continue keeping the button pressed.
3. Release the button after the dumping process continues.

Log

Next >

XRY Wizard

Process Options

Create and select the options you want to apply during this process.

< Back

Full read (including log)

Everything except multimedia, documents and other files

Dump

Your profiles are locked.
Press the lock icon to create, edit or delete a profile.

Log

Next >

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 advise 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.

XRY

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

Cost effective, rewritable SIM cards

SIM id-Cloner Examination cards are re-writable, 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)

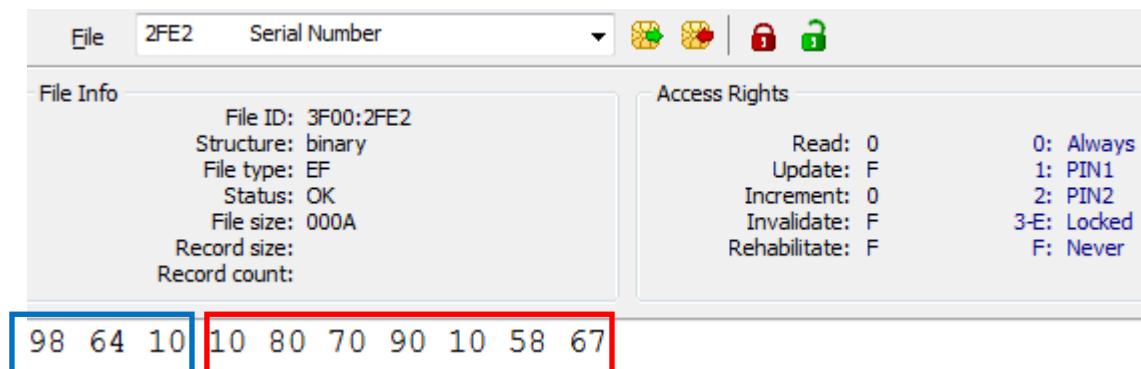
$$\text{IMSI} = \text{MCC} + \text{MNC} + \text{MSIN}$$

MCC	240	<u>Sweden</u>
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

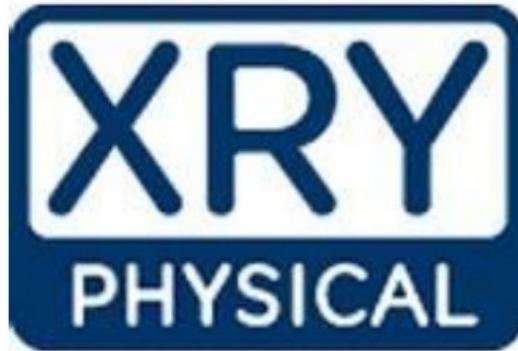
- **ICCID** uniquely identifies the SIM card, one can determine issuing service provider and country code from ICCID
- International Standard ISO/IEC 7812
 - http://en.wikipedia.org/wiki/ISO_7812
 - 19 or 20 digits in length and always stored in the card
 - Normally printed on the outside (may be abbreviated)
- **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



MSAB XRY SIM Id Cloner

The image shows three windows of the XRY SIM Id Cloner software:

- Welcome to the SIM Id Cloner**: This window is the initial setup screen. It features a blue background with abstract white lines. On the left, there's a vertical bar with the "XRY SIM ID-CLONER" logo and "MICRO SYSTEMATION" text. The main area contains a title "Welcome to the SIM Id Cloner", a brief description of the wizard's purpose, and two radio button options: "Clone an existing SIM card" (selected) and "Manually enter data". A note about the license validity until 2011-1 is also present.
- XRY SIM Id Cloner**: This is the main configuration window. It has a title bar "XRY SIM Id Cloner" and a sub-section "Input Source Data" with the instruction "Input the data you wish to be written to the SIM card.". It includes fields for "ICCI" (up to 20 digits), "IMSI" (up to 15 digits), and "LP" (a dropdown menu set to "(None)" with "(optional)" note). There's also a checkbox for "Enter advanced settings". At the bottom are buttons for "< Back", "Next >", and "Cancel".
- XRY SIM Id Cloner**: This is a configuration dialog titled "Insert Destination Card". It has the instruction "Insert the SIM card that will be configured." and a note "Please insert the SIM card that will be configured to assume the cloned identity. This should be a SIM card supplied by Micro Systemation." It displays "Identification data:" followed by a list of parameters with their values:
 - ICCID: 89460101080709012108
 - IMSI: 240016001591638
 - LP: 0601FFFF
 - SPN: Telia
 - GID1: FFFFFFFF
 - GID2: FFFFFFFF
 - SMSP: 54656C696120534D5343FFFFFFFFFFFFFFF
 - O2 IMEI: FFFFFFFFA "Show Log" button is located at the bottom right of this dialog.



- 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 UFED Physical Analyzer software interface. The main window title is "Physical Analyzer". The menu bar includes File, Edit, View, Tools, Report, Plug-ins, and Help. The toolbar contains icons for file operations like Open, Save, Extract, and Import. The "Project Tree" panel on the left shows a project named "Apple_iPhone 2G_3G_3GS (iPhone 2G/3G/3GS)". Inside the project tree, there is an "Extraction Summary" node which contains a "HEX" file named "Apple_iPhone 2G_3G_3GS.zip" and several service nodes: Lockdown Service, Backup Service, and AFC Service. Below these are "Data files" containing Images (1008), Videos (5), Audio (1967), and Text (15). A "Report" node is also present. The "Extraction Summary" tab is selected in the top right. The "Device info:" section displays the following information:

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

The "Content:" section shows a table of extracted items:

	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

A small image of an iPhone is shown in the top right corner of the software interface.



The screenshot shows a report generated by the UFED Physical Analyzer. The report includes a timestamped log and a file list.

Log entries:

- /2010 9:46:19 PM
- /2010 12:06:42 PM
- [REDACTED]
- .7
- No. 110

File list:

- : iPhone 2G_3G_3GS.zip

MSAB XACT 1

Samsung SGH-E360.xry - XACT - Data [OneNAND]

File Edit View Node Tools Window Help

Project

Image
Data [NOR:10000000-11FFFFFF]
Catalog
Image
Data [OneNAND]
Translation Layer
Partition
Partition Boot Record
FAT
FAT1
KFAT0
@SAMSUNG.ESS
SOUNDS
IMAGES
MMS
JAVA
multimedia
DEFAULT
IMAGES
downloaded images
PHOTOS
THUMB
Photo-0001.jpg
Photo-0002.jpg
Photo-0003.jpg
my photos
favorite images
VIDEOS
MUSIC
SOUNDS

Data [OneNAND]

XACT Image Decoder

Identify Device
XACT is identifying the device.

Filter: <All>

Nokia 6230
Nokia 6230i
Nokia 6585
Nokia 6610i
Nokia 7270
Nokia 7360
Samsung SGH-D500
Samsung SCH-R300

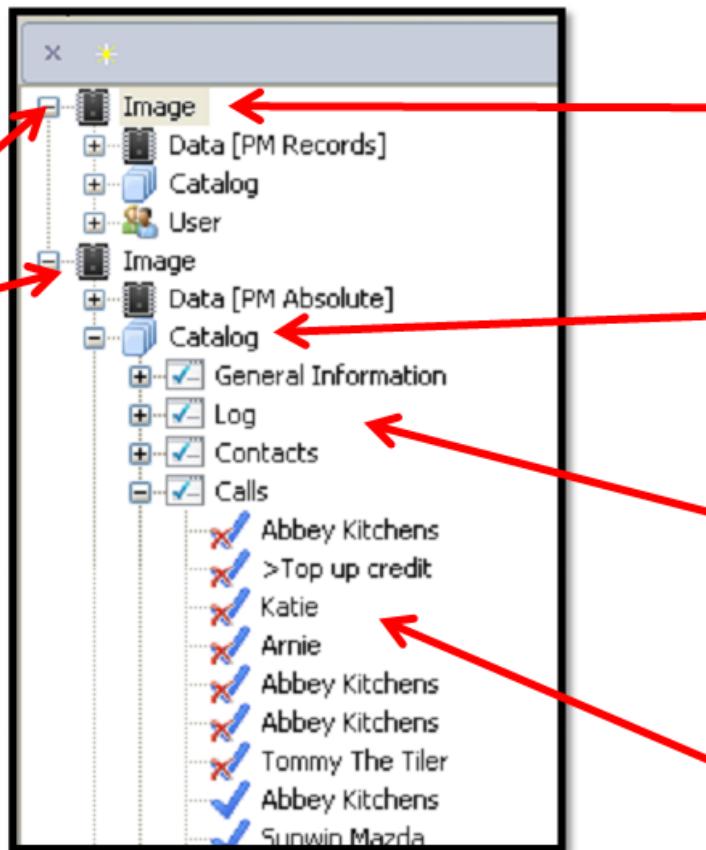
< Back Next > Cancel

0000 0000 64 00 00 00 0F 00 00 00 01 00 00 00 58 53 52 31
0000 0010 00 00 00 00 00 00 00 A5 A5 A5 A5 08 08 00 00
0000 0020 01 00 00 FF FF FF FF FF FF FF FE FF FF FF
0000 0030 A7 AC AD CE F7 F7 FF FF 5A 5A 5A 5A 01 FF FF FF
0000 0040 FF
0000 0050 FF
0000 0060 FF
0000 0070 FF
0000 0080 FF
0000 0090 FF
0000 00A0 FF
0000 00B0 FF
0000 00C0 FF
0000 00D0 FF
0000 00E0 FF
0000 00F0 FF
0000 0100 FF
0000 0110 FF
0000 0120 FF
0000 0130 FF
0000 0140 FF
0000 0150 FF
0000 0160 FF
0000 0170 FF
0000 0180 FF
0000 0190 FF
0000 01A0 FF
0000 01B0 FF
0000 01C0 FF
0000 01D0 FF
0000 01E0 FF
0000 01F0 FF
0000 0200 FF
0000 0210 FF
0000 0220 FF
0000 0230 FF
0000 0240 FF
0000 0250 FF
0000 0260 FF FF



XACT Project Structure

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



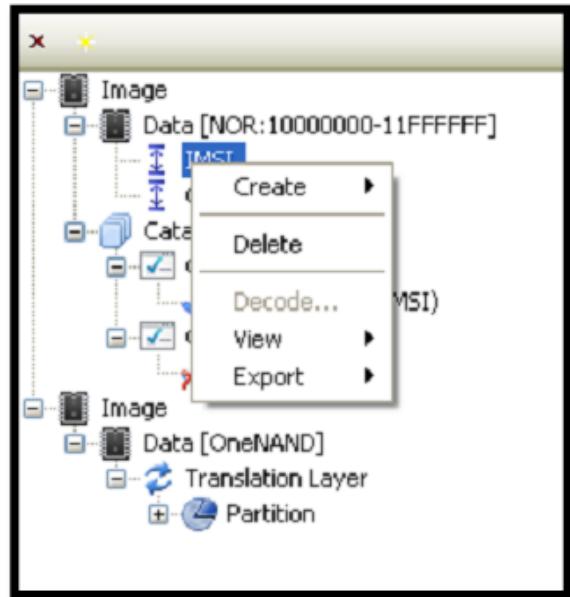
"Image" entries are always at the top level in the XACT Project window

"Catalog" provides a home for decoded calls, calendar etc.

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

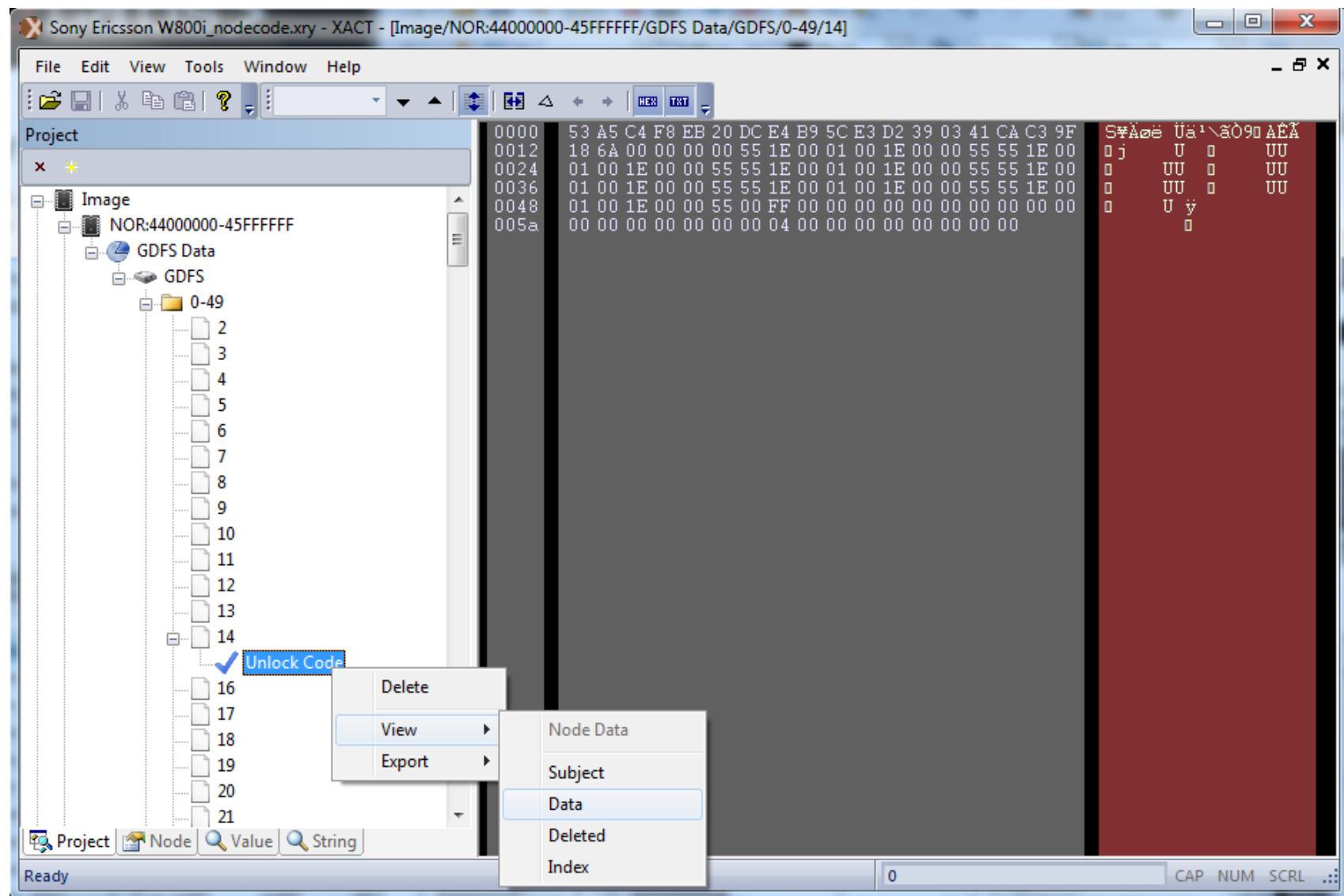
Decoded data "items" the red cross indicates "deleted" or "inactive"

XACT Project Structure



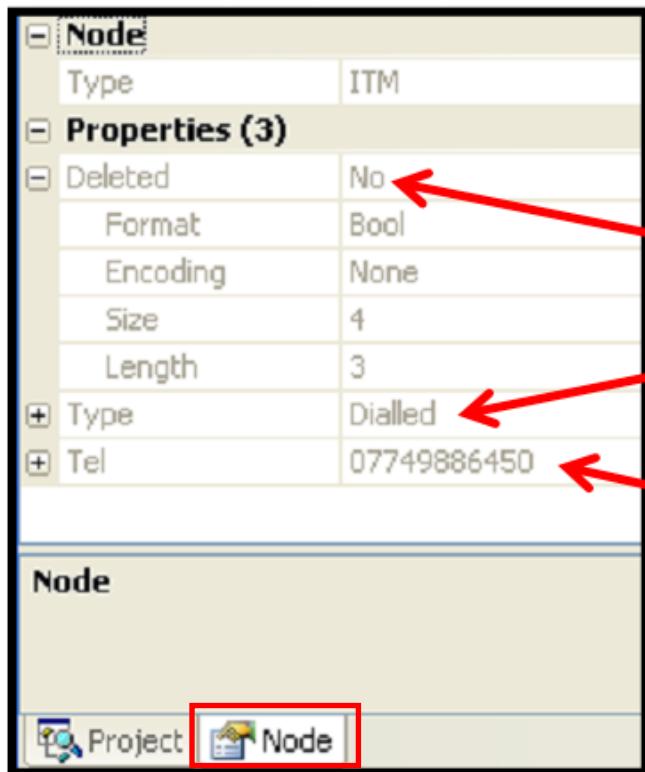
- All entries in the Project window are “nodes”
- Different actions are available for each node type
 - Right click on a node to select an action
- Some node types can be double-clicked to view data in a separate hex viewer window

MSAB XACT 2



Viewing Item Properties

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

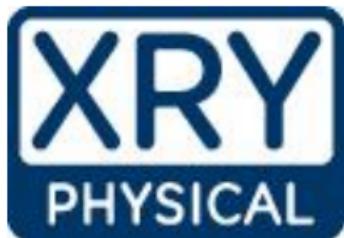


Live (not deleted)

Dialled call

To 07749 886450

XACT Hex Viewer



00 000 000	10 00 38 9C 00 00 00 B1 00 0C 02 01 FF 00 08 20	I 8 ± yy
00 000 016	01 DC 02 FF FF 00 08 20 10 00 00 95 10 00 00 00	yy
00 000 032	10 00 EF D7 10 08 00 00 10 00 E8 00 10 00 F0 00	i× è
00 000 048	11 F8 08 00 28 63 29 20 43 FF 70 79 72 69 67 68	0 (c) C
00 000 064	74 20 4D 6F 74 6F 72 6F 6C 61 20 32 30 30 34 2C	Copyright Motorola 2004,
00 000 080	20 41 6C 6C 20 52 69 67 68 74 73 20 52 65 73 65	All Rights Rese
00 000 096	72 76 65 64 2E 00 00 00 FF FF FF FF FF FF FF FF FF	rved. yyyy yyyy
00 000 112	FF	vvvvvvvvvvvvvvvvv

The “016” here tells us the position for the first byte on this line

By default the viewer displays rows of 16 bytes (until stretched or shrunk by the user)

Note that two hex digits (0x43) are required to represent one ASCII character (C)

Each hex digit is equivalent to a nibble (half a byte)

MSAB XACT 3

The screenshot shows the MSAB XACT 3 application window. On the left, there's a project tree with two main entries: 'Image' and 'SonyEricsson_K800i_NAND_NAND512R3A.bin'. Below these are 'Catalog' and 'User' entries for both categories. The main pane displays a hex dump of memory starting at address 0000 0000, with all bytes showing FF FF FF FF. A 'Find' dialog box is open on the right, containing a 'Text' input field with 'Text' selected, a 'Format' dropdown set to 'GSM (7 bit packed)', and a list of encoding options. The 'GSM (7 bit packed)' option is highlighted with a blue selection bar. At the bottom of the interface, there are tabs for 'Project', 'Node', 'Value', and 'String', with 'String' currently active.

Sony Ericsson K800i_nodecode.xry - XACT - [Image/SonyEricsson_K800i_NAND_NAND512R3A.bin]

File Edit View Tools Window Help

Project

Image

- SonyEricsson_K800i_NAND_NAND512R3A.bin

Catalog

User

Image

- SonyEricsson_K800i_Norflash_PF38F5060M0Y0B1E

Catalog

User

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 FF FF FF FF
0000 00b4 FF FF FF FF FF FF FF FF
0000 00c3 FF FF FF FF FF FF FF FF
0000 00d2 FF FF FF FF FF FF FF FF
0000 00e1 FF FF FF FF FF FF FF FF
0000 00f0 FF FF FF FF FF FF FF FF
0000 00ff FF FF FF FF FF FF FF
0000 010e FF FF FF FF FF FF FF FF
0000 011d FF FF FF FF FF FF FF FF
0000 012c FF FF FF FF FF FF FF FF
0000 013b FF FF FF FF FF FF FF FF
0000 014a FF FF FF FF FF FF FF FF
0000 0159 FF FF FF FF FF FF FF FF
0000 0168 FF FF FF FF FF FF FF FF
0000 0177 FF FF FF FF FF FF FF FF
0000 0186 FF FF FF FF FF FF FF FF
0000 0195 FF FF FF FF FF FF FF FF
0000 01a4 FF FF FF FF FF FF FF FF
0000 01b3 FF FF FF FF FF FF FF FF
0000 01c2 FF FF FF FF FF FF FF FF
0000 01d1 FF FF FF FF FF FF FF FF
0000 01e0 FF FF FF FF FF FF FF FF
0000 01ef FF FF FF FF FF FF FF FF

Find

Text

Text

Hex

Data

Dictionary Search

File Signature Search

Findstrings

Number Search

PDU Finder

Regex search

Timestamp Search

Format:

- GSM (7 bit packed)
- 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
- OEM 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

Find Next

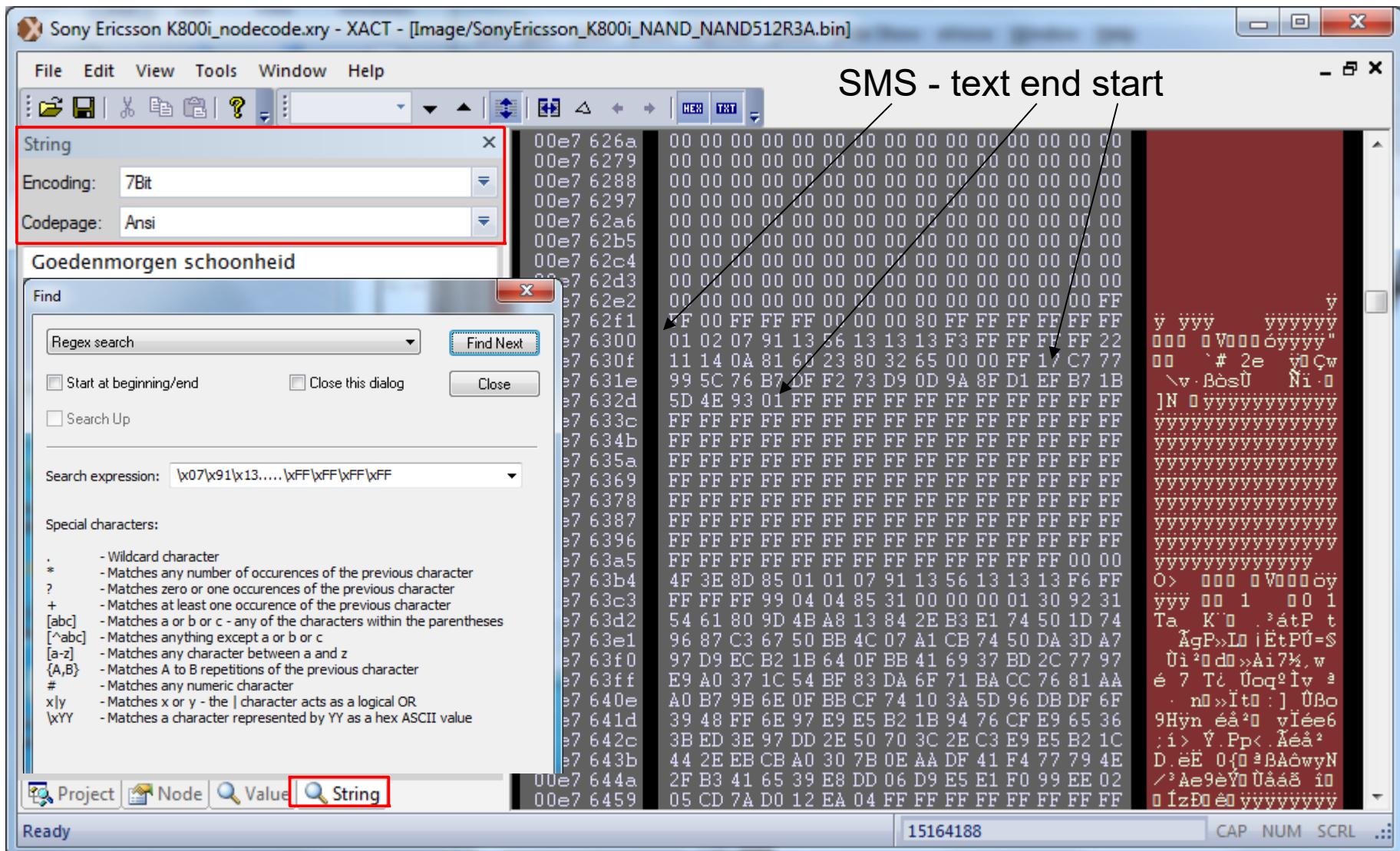
Close

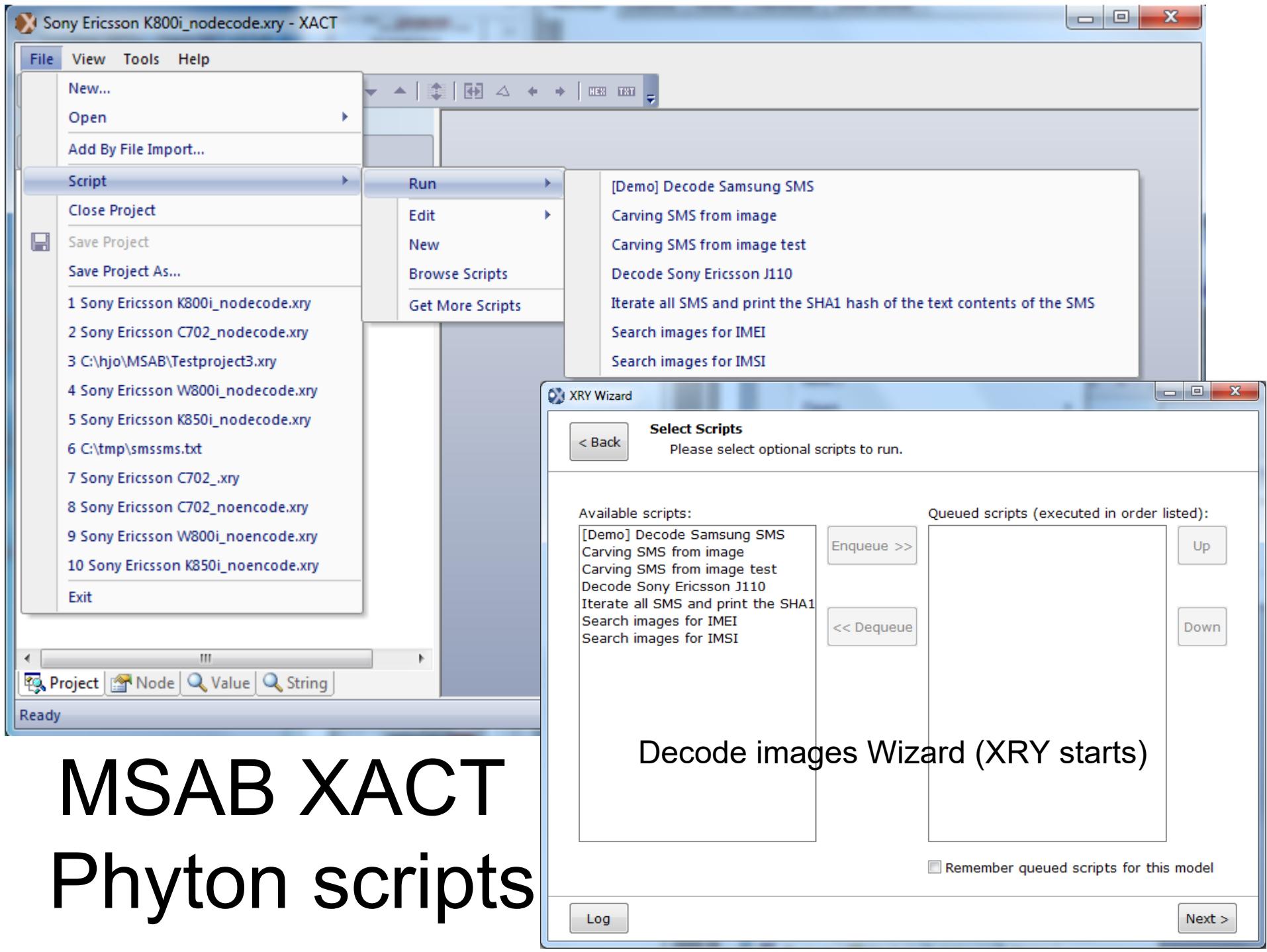
Project Node Value String

Ready

MSAB XACT 4

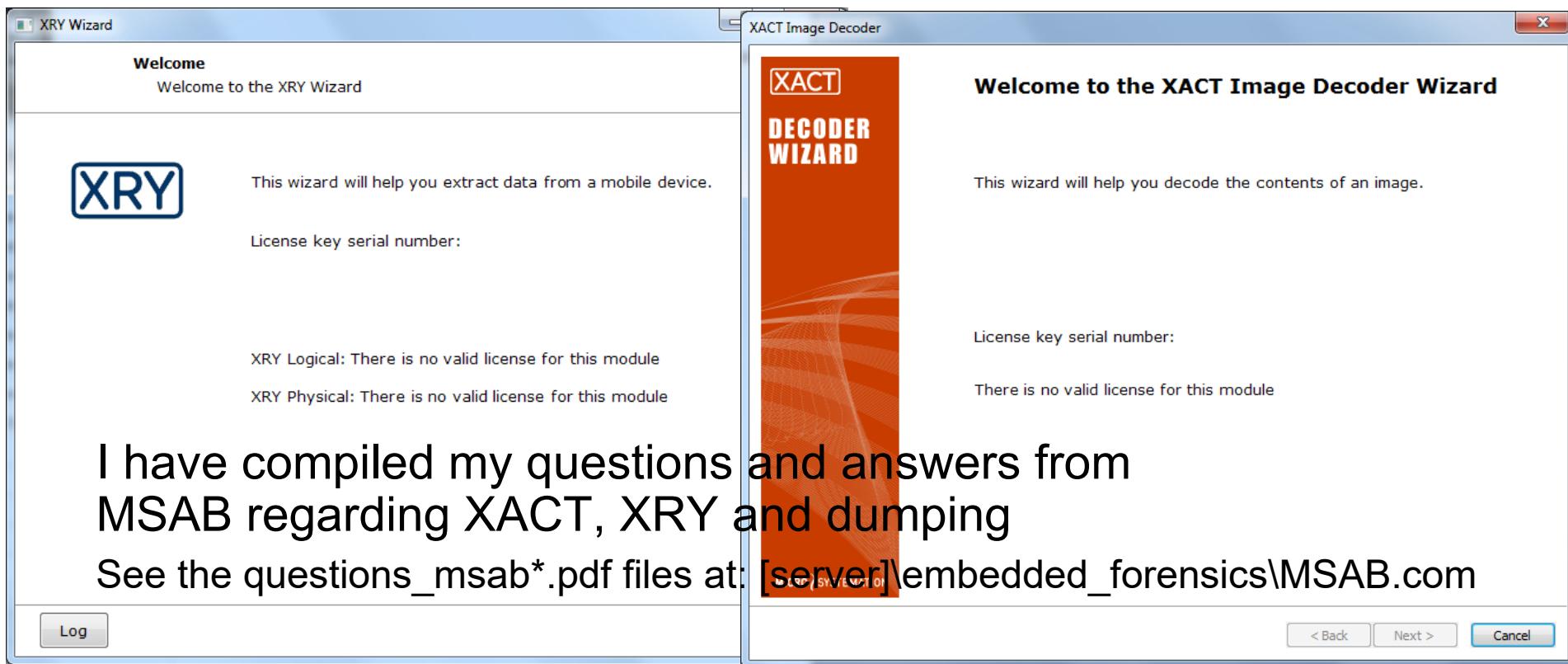
SMS 7-bit Encoding





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

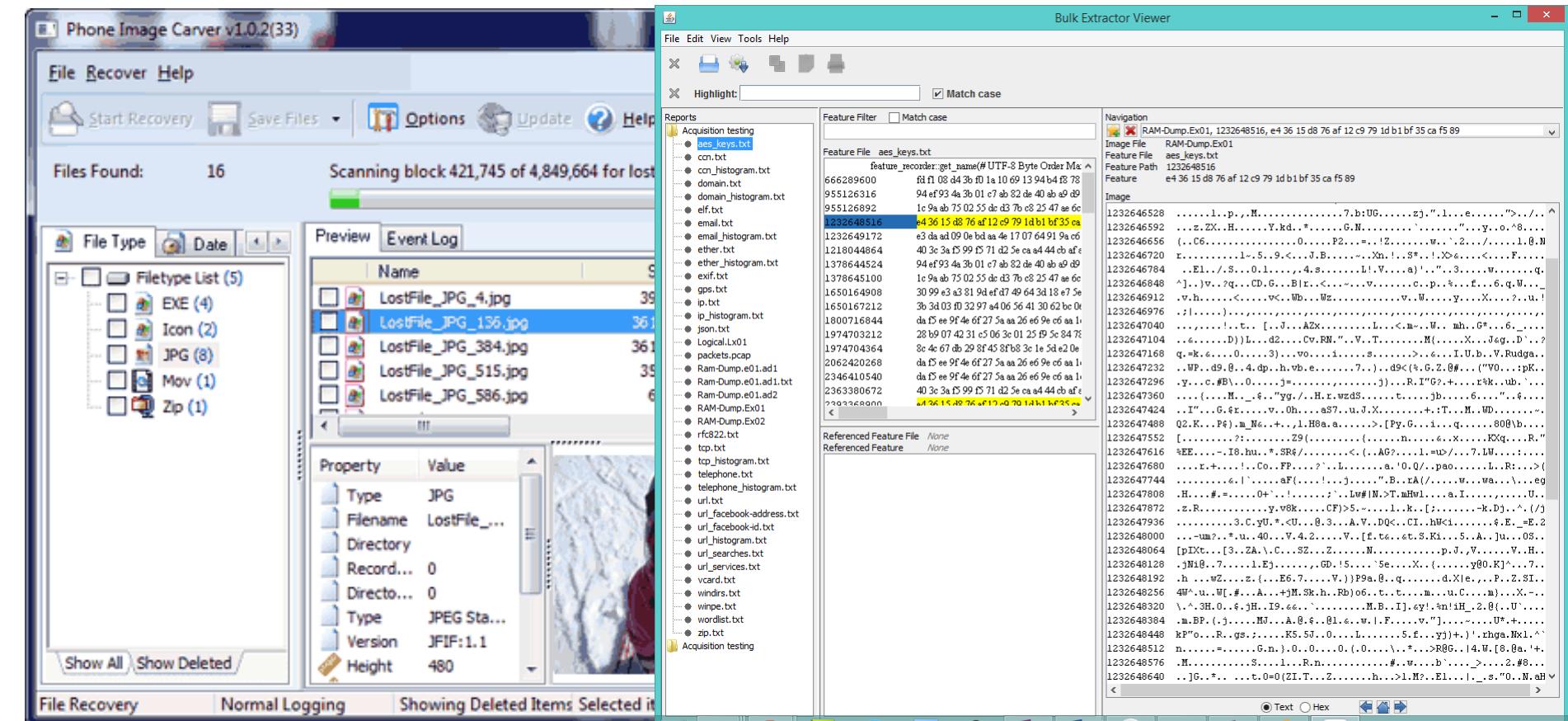
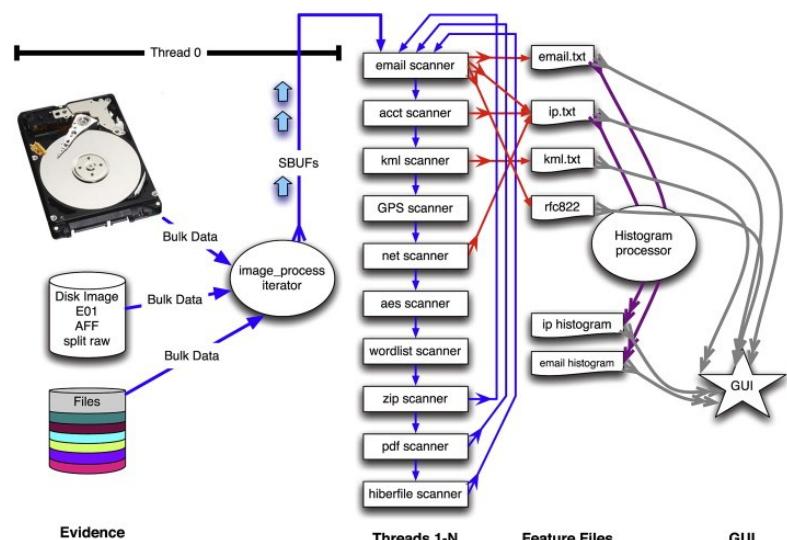
See the questions_msab*.pdf files at: [server]\embedded_forensics\MSAB.com

Extracting dump data

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

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 screenshot displays a digital forensics framework interface with two main panes. The left pane shows a hierarchical tree view of files and folders, including a large SonyEricsson_K800i_NAND_NAND512R3A.bin file and various partitions like k800-base, part_tp, and part_ifs. The right pane shows a detailed table of recovered files and a preview pane displaying recovered images.

Recovered Files Table:

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 Images Preview:

The preview pane shows several recovered images, including:

- DSC00006.JPG
- DSC00005.JPG
- DSC00004.JPG
- DSC00003.JPG
- DSC00010.JPG
- DSC00009.JPG
- DSC00008.JPG
- DSC00007.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

More iPhone dumps are available from [server]

iPhone3g.dmg

Partition 1

iPhone3G [HFS+]

[unallocated space]

iPhone3G

private

etc

alternatives

apt

bluetooth

default

dpkg

pam.d

ppp

profile.d

racoon

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 ÈG+ÈGÀQ...ÈGz+
00000420 00 00 11 FD 00 00 02 2D-00 00 10 00 00 01 03 F8 ..ý.....ø
00000430 00 00 OC 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 00 030...0..
00000480 00 00 00 01 00 00 00 03-00 00 00 00 00 00 00 00 ..0...0..
00000490 00 00 00 00 00 00 00 00-00 00 00 00 00 00 00 00 ..0...0..
000004a0 00 00 00 00 00 00 00 00-00 00 00 00 00 00 00 00 ..0...0..
000004b0 00 00 00 00 00 00 00 00-00 00 00 00 00 00 00 00 ..0...0..
000004c0 00 00 00 00 02 00 00 00-00 02 00 00 00 00 00 20 ..0...0..
000004d0 00 00 00 04 00 00 00 20-00 00 00 00 00 00 00 00 ..0...0..
000004e0 00 00 00 00 00 00 00 00-00 00 00 00 00 00 00 00 ..0...0..
000004f0 00 00 00 00 00 00 00 00-00 00 00 00 00 00 00 00 ..0...0..
00000500 00 00 00 00 00 00 00 00-00 00 00 00 00 00 00 00 ..0...0..
00000510 00 00 00 00 00 34 00 00-00 08 00 00 00 00 03 40 ..-4.....@
00000520 00 00 24 00 00 00 40-00 00 04 E1 00 00 00 80 ..\$...@..á..
00000530 00 00 11 A1 00 00 00 80-00 00 43 CA 00 00 00 80 ..i...-CÉ..
00000540 00 00 5A 3D 00 00 00 80-00 00 63 B6 00 00 00 80 ..Z=...-c¶..
00000550 00 00 89 22 00 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

Normal

Display Time Zone: W. Europe Standard Time (From local machine)

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	n/a	n/a	n/a
Unpartitioned Sp...	1001			iphone3g.dmg/Unpartitioned Space [Apple]	Unpartitioned S...	n/a	n/a		n/a	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]

Oxygen Forensic Suite 2012 Analyst

Main View Tools Service Help

All devices > Brooklyn maniac > Patrick Payne's iPhone 3GS - 10.05.2011 23:19:56 [012156002672455] > File Browser > Filtering criteria ...

Search Export Print Export to Google Earth Up Refresh Folders Viewer Filters Views Sort Help

Tasks for files and folders Selected folder(s) Images Melodies Videos Documents Database files Other files Plist files Geo files

Object information

Name: IMG_0051.JPG
Type: JPEG-картинка
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

IMG_0024.JPG IMG_0025.JPG IMG_0026.JPG IMG_0027.JPG IMG_0028.JPG

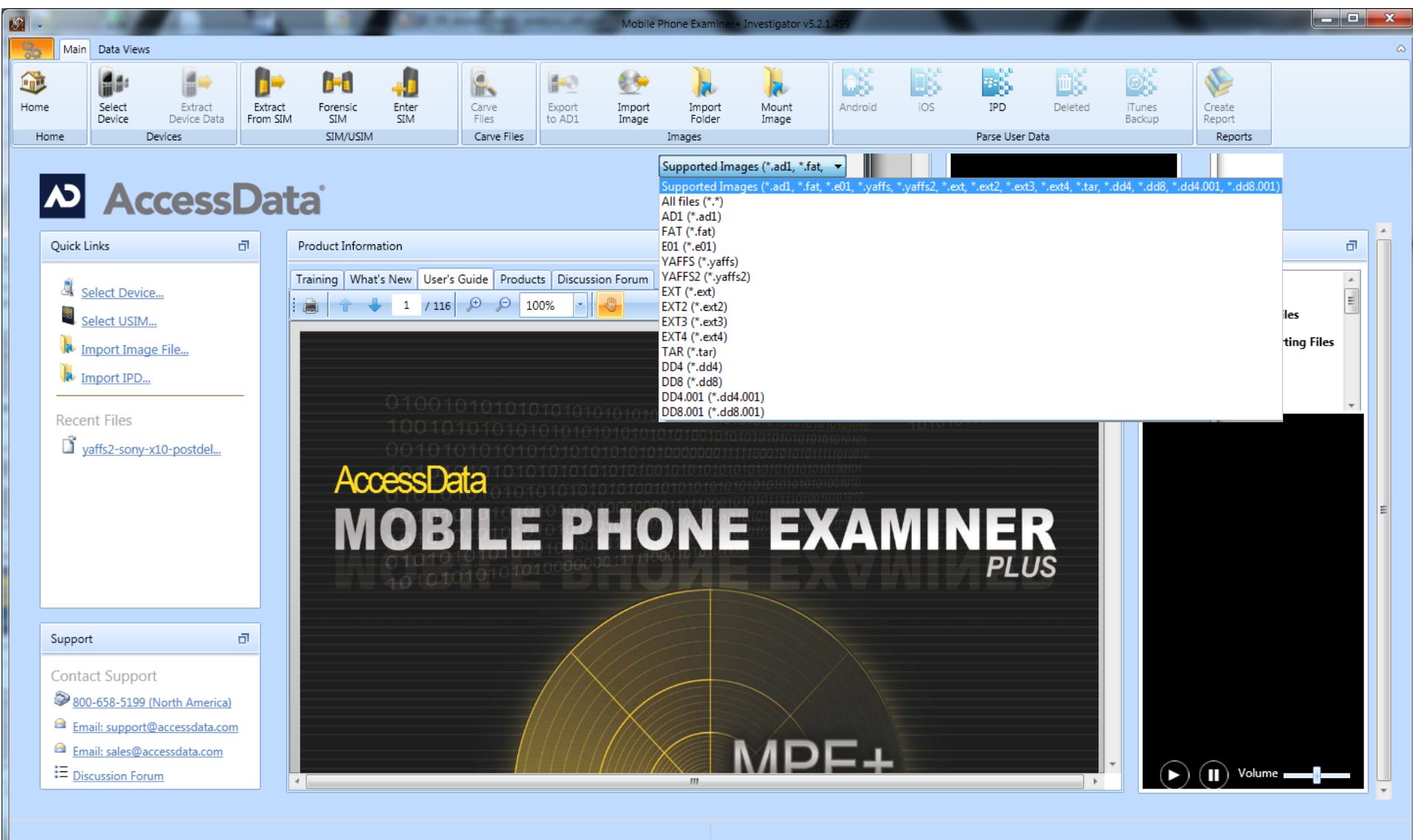
IMG_0051.JPG IMG_0052.JPG IMG_0216.JPG IMG_0232.JPG IMG_0233.JPG

IMG_0053.JPG IMG_0054.JPG IMG_0055.JPG IMG_0056.JPG

Mode: Image Zoom: Fit Mode: Hex Encoding: ANSI (Windows) No selection

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

AccessData MPE+



Time stamps and search terms

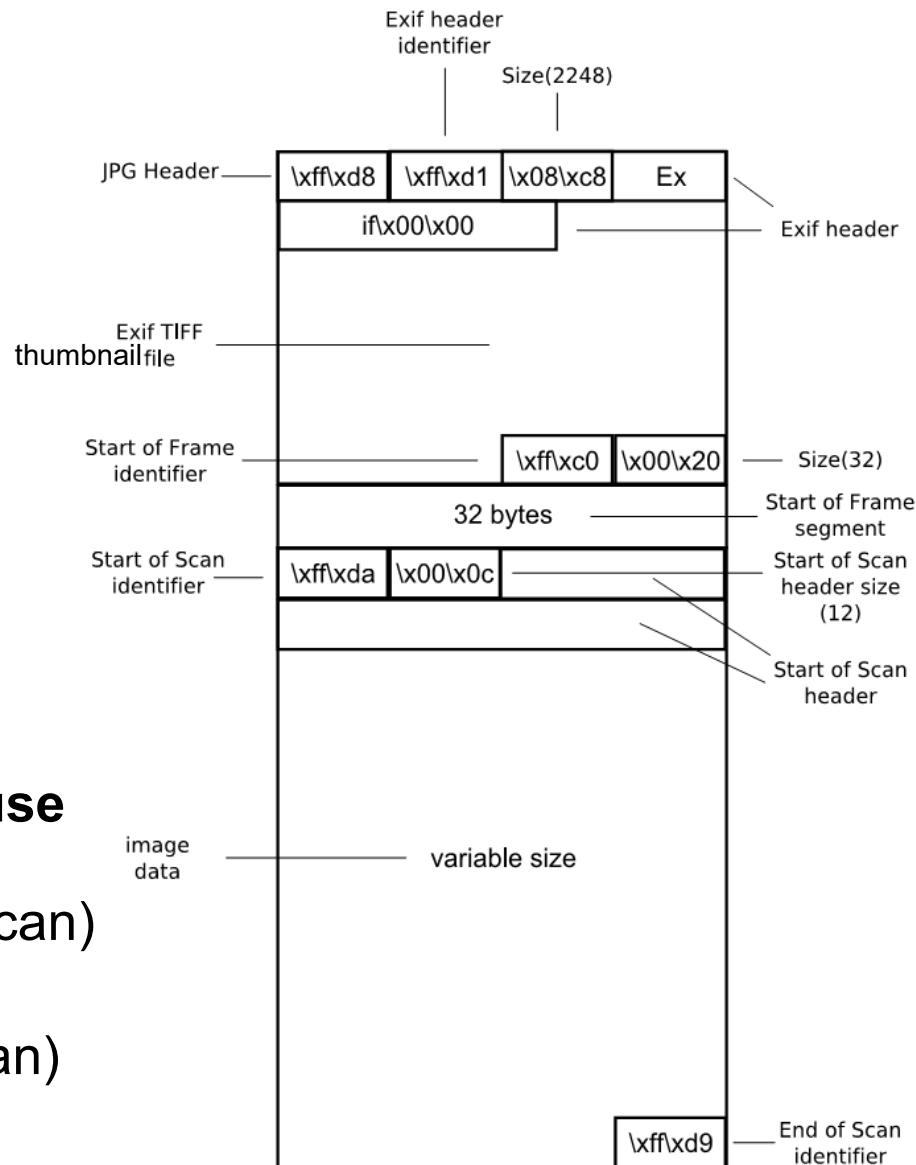
- A wide variety of storage formats are used for storing timestamp data in embedded system memories
- To illustrate - the timestamp "30 April 2008 14:30:59 UTC" is encoded as follows in some formats found in different mobile phone memories:
 - 0x80400341039500 (ETSI SMS)
 - 0xB19E0CA3 (Nokia)
 - 0x07D8041E0E1E3B (Nokia)
 - 0x26041E0E1E3B (Motorola)
 - 0x00E129CB0E8B2EC0 (Symbian)
 - 0x481882A3 (POSIX)
- Regular Expressions and Search Terms for Phone Examiners
 - <http://www.controlf.net/regexprs/>
- 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/>

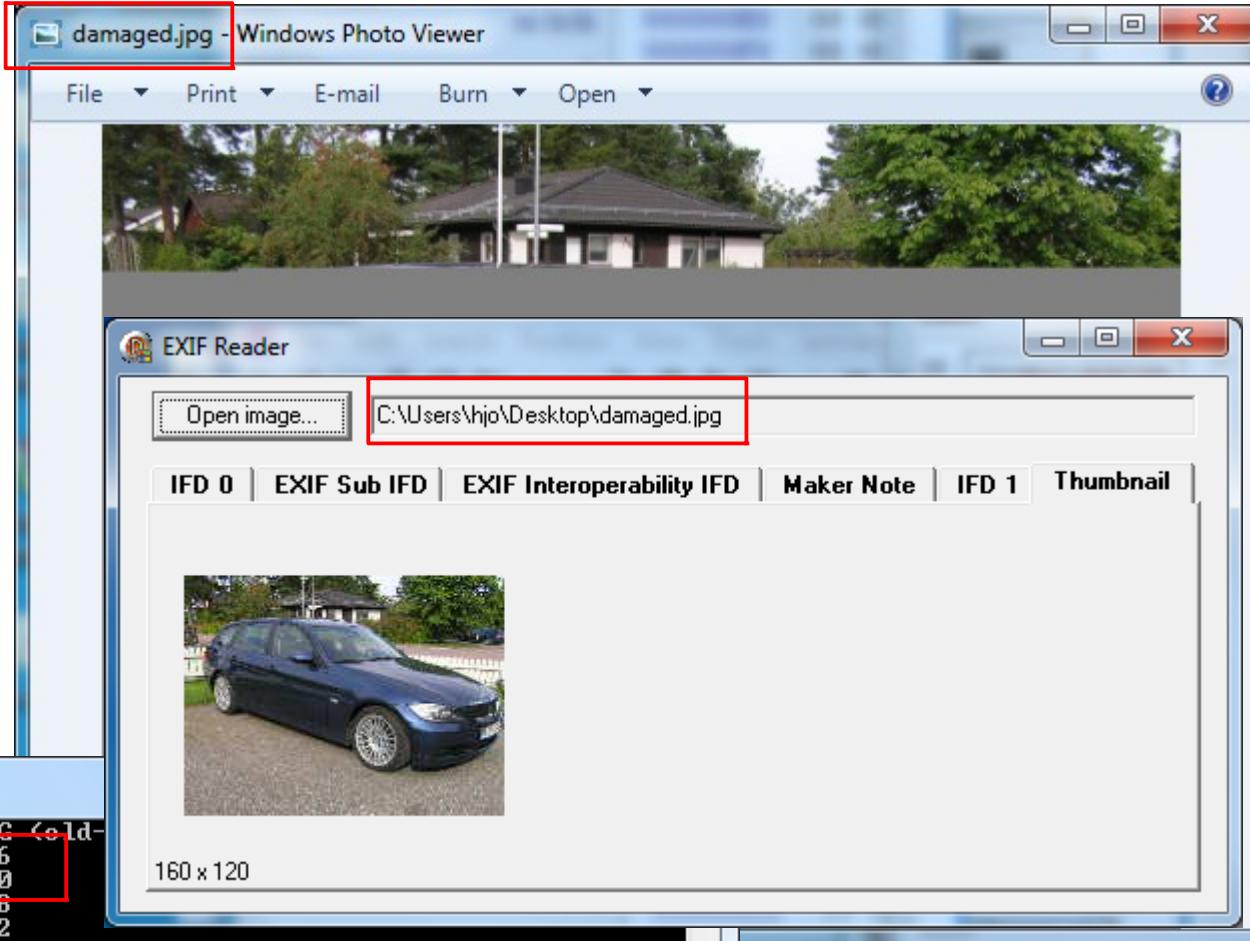
JPG file structure and carving

- 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 : 1/400
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)

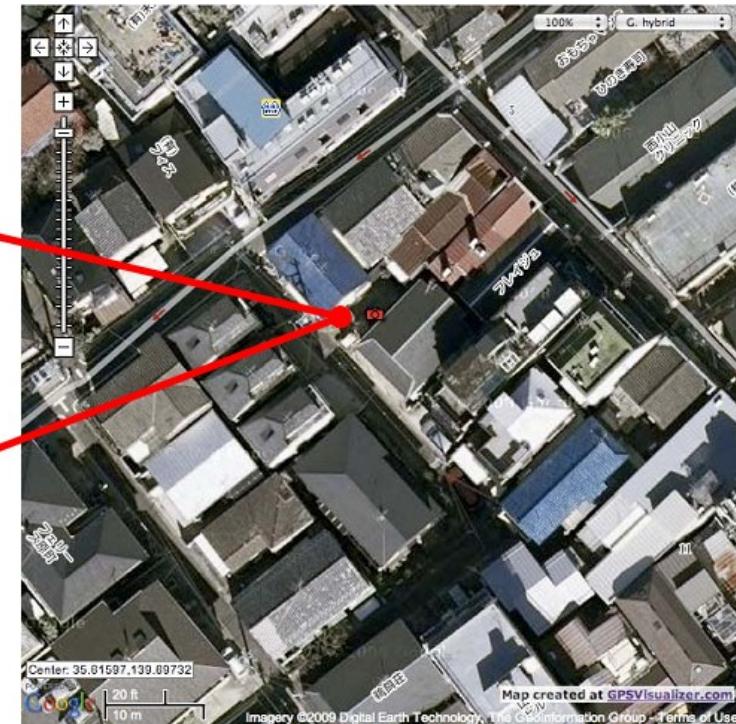
GPS IFD
Tags Relating to GPS
GPSVersionID
GPSLatitudeRef
GPSLatitude
GPSLongitudeRef
GPSLongitude
GPSAltitude
GPSTimeStamp
GPSSatellites
GPSStatus
GPSMeasureMode
GPSDOP
GPSSpeedRef
GPSTrackRef
GPSTrackRef
GPSImgDirectionRef
GPSImgDirectionRef
GPSMapDatum
GPSDestLatitudeRef
GPSDestLatitude
GPSDestLongitudeRef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

Digital Still Camera Forensics - SSDDFJ V1 1 Cohen.pdf

Degrees/Minutes/Seconds
May need conversion

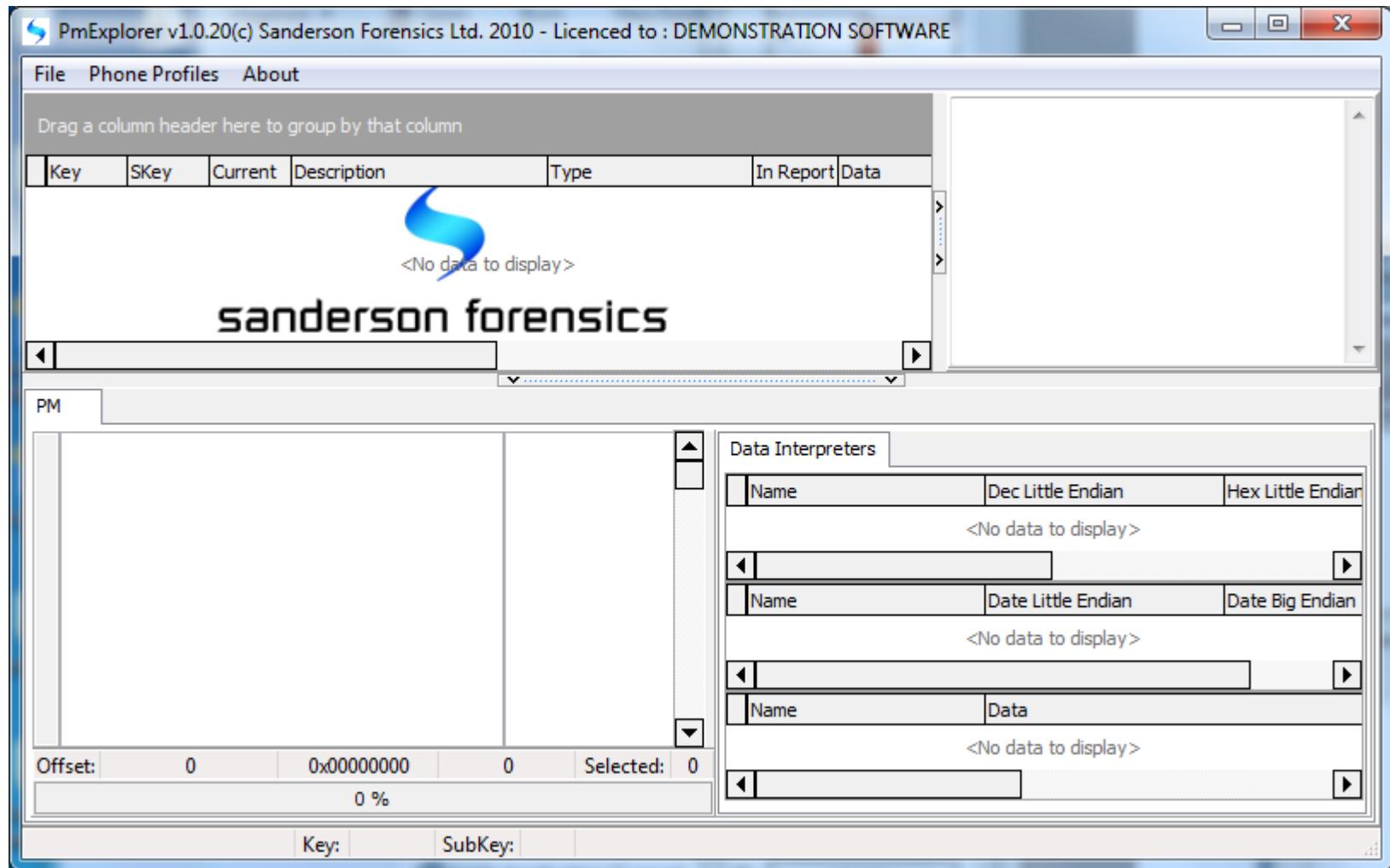


N35 deg 36 '
E139 deg 41'



PmExplorer

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

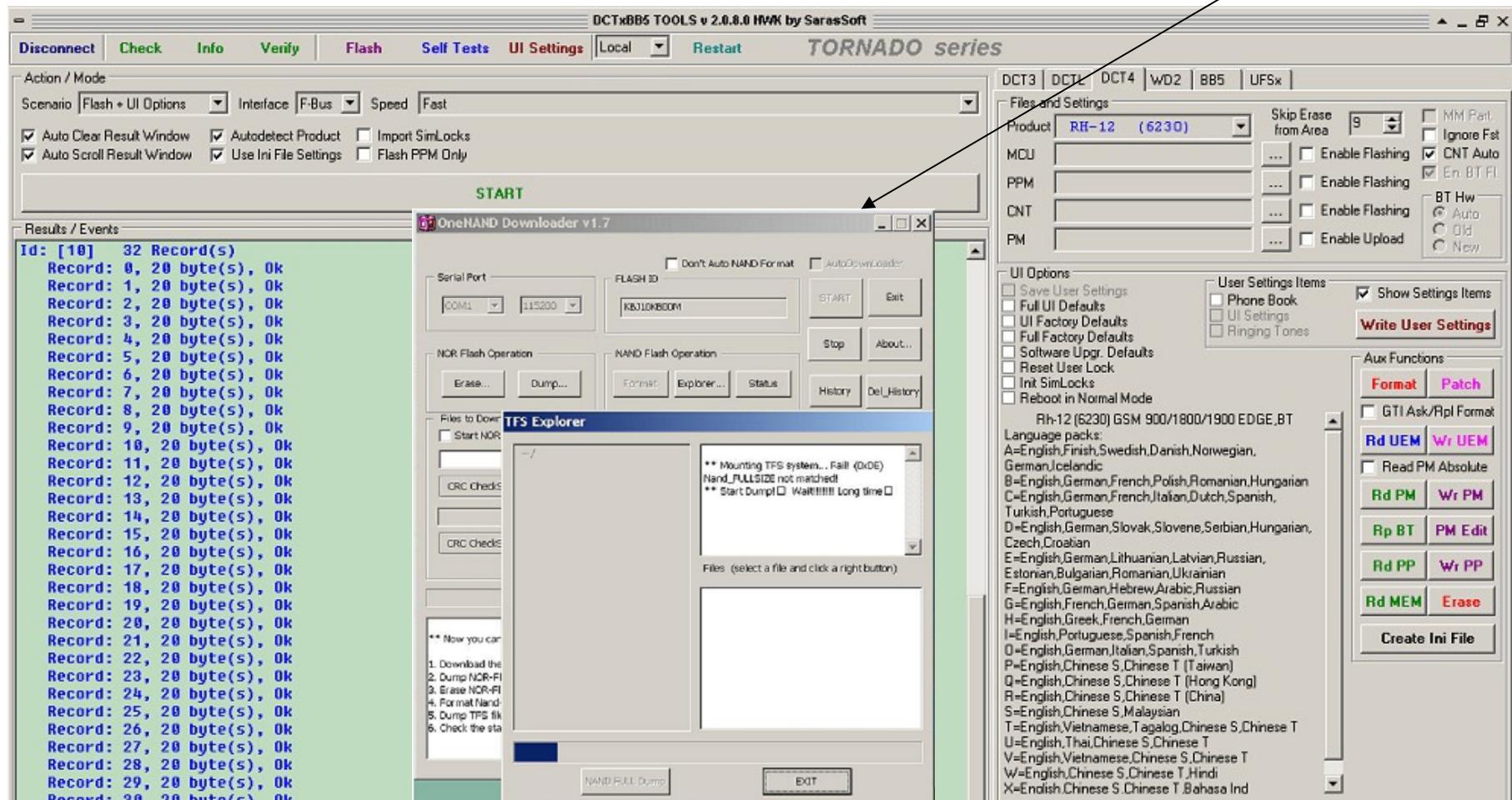


Nokia
PM tables/records

Phone flashers 1

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

Samsung
OneNAND
Downloader

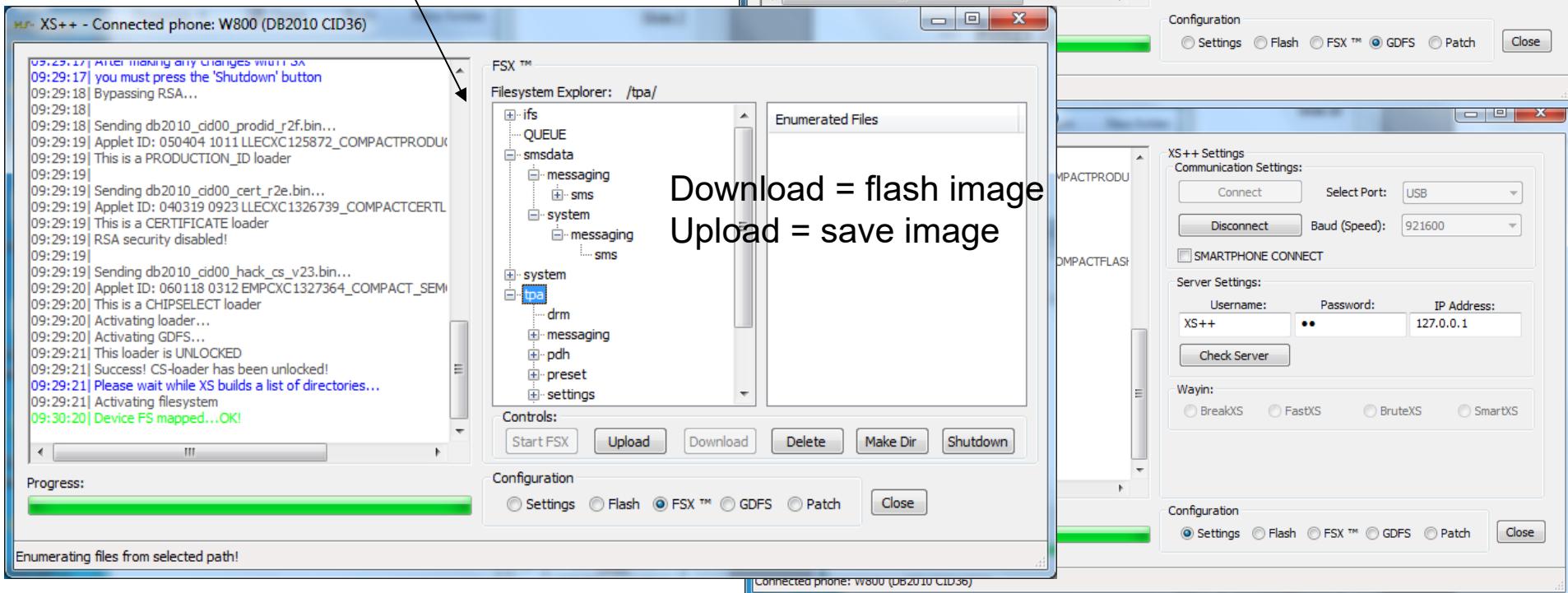


Phone flashers 2

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

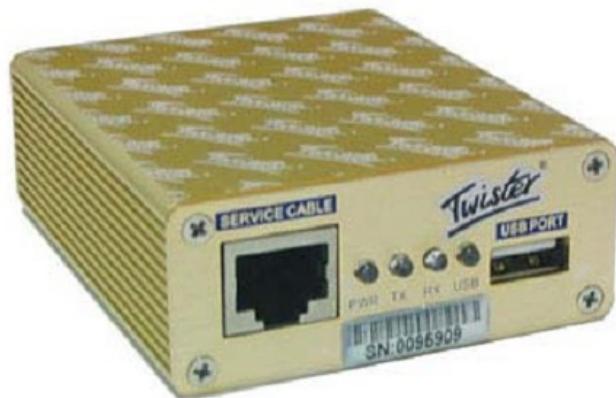
<http://en.wikipedia.org/wiki/GDFS>

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-celebrite-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