Mobile memory dumps, MSAB and MPE+

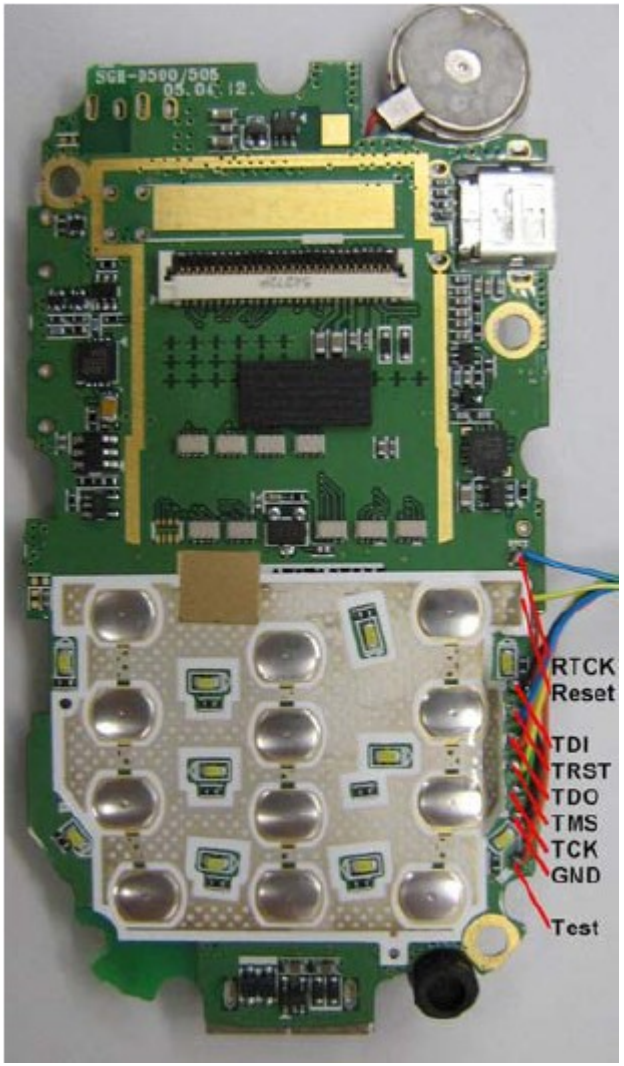
Data collection

Information recovery

Analysis and interpretation of results

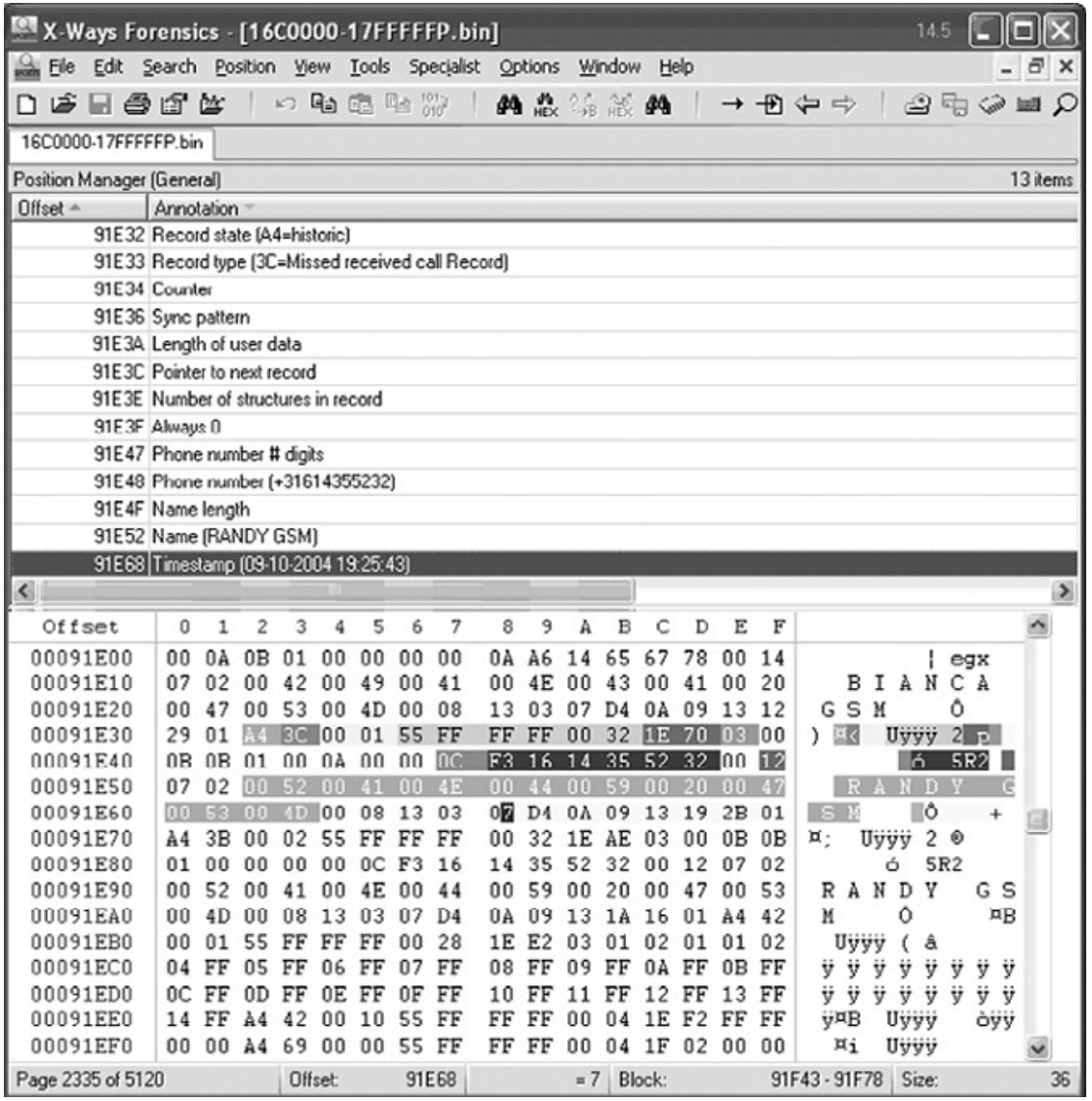
Physical Extraction

- 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



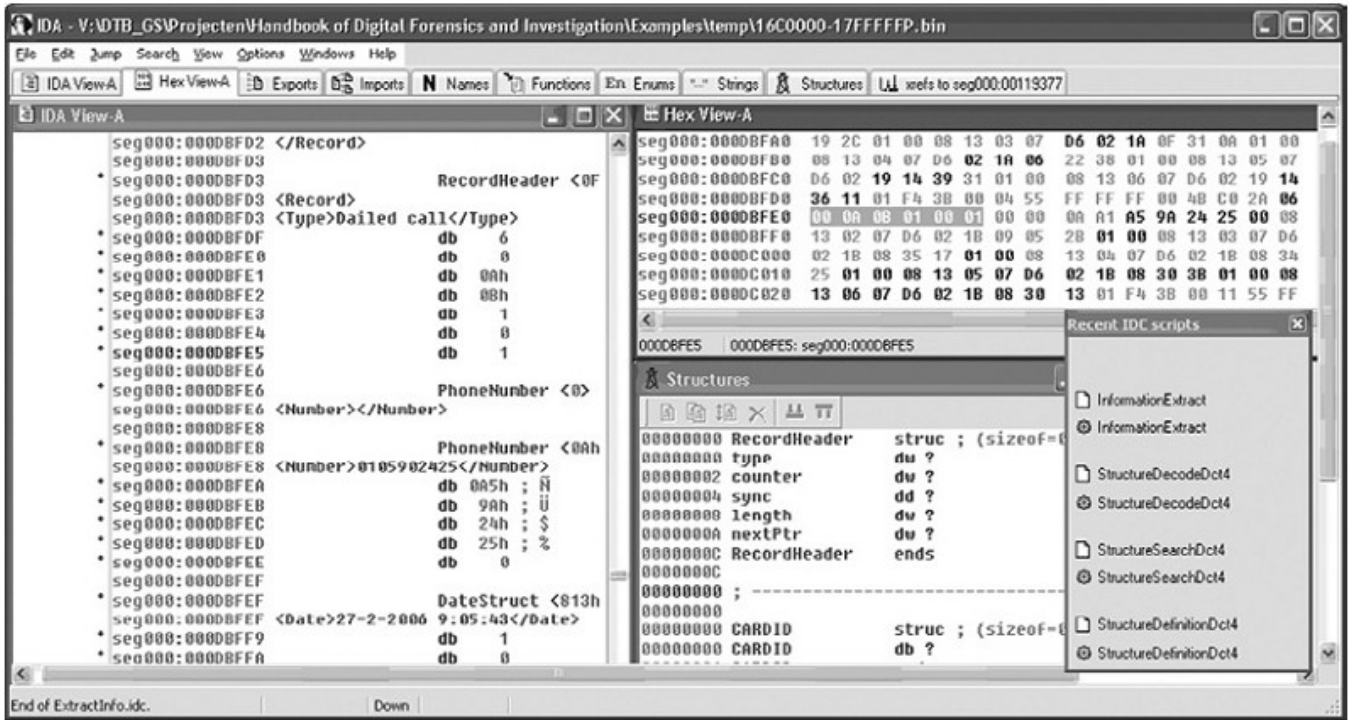
Hex editors - WinHex

- 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

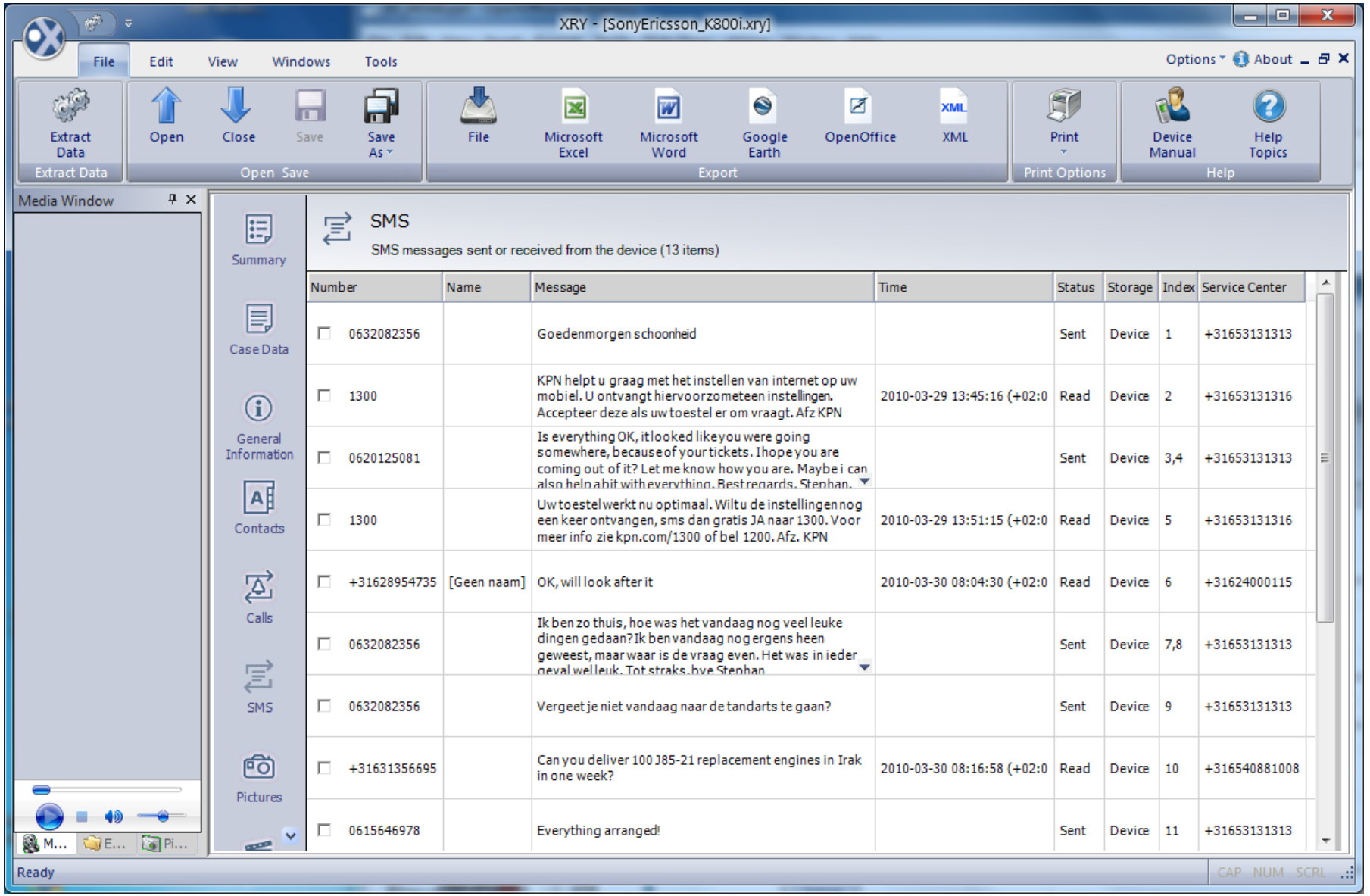
- In IDA Pro using IDC scripts or the plugins framework
  - Could be used to load data from an embedded system memory that contains data encoding functions and to reverse engineer them to reconstruct relevant system and user information
  - A more practical approach is to (ab)use IDA as an advanced hex 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



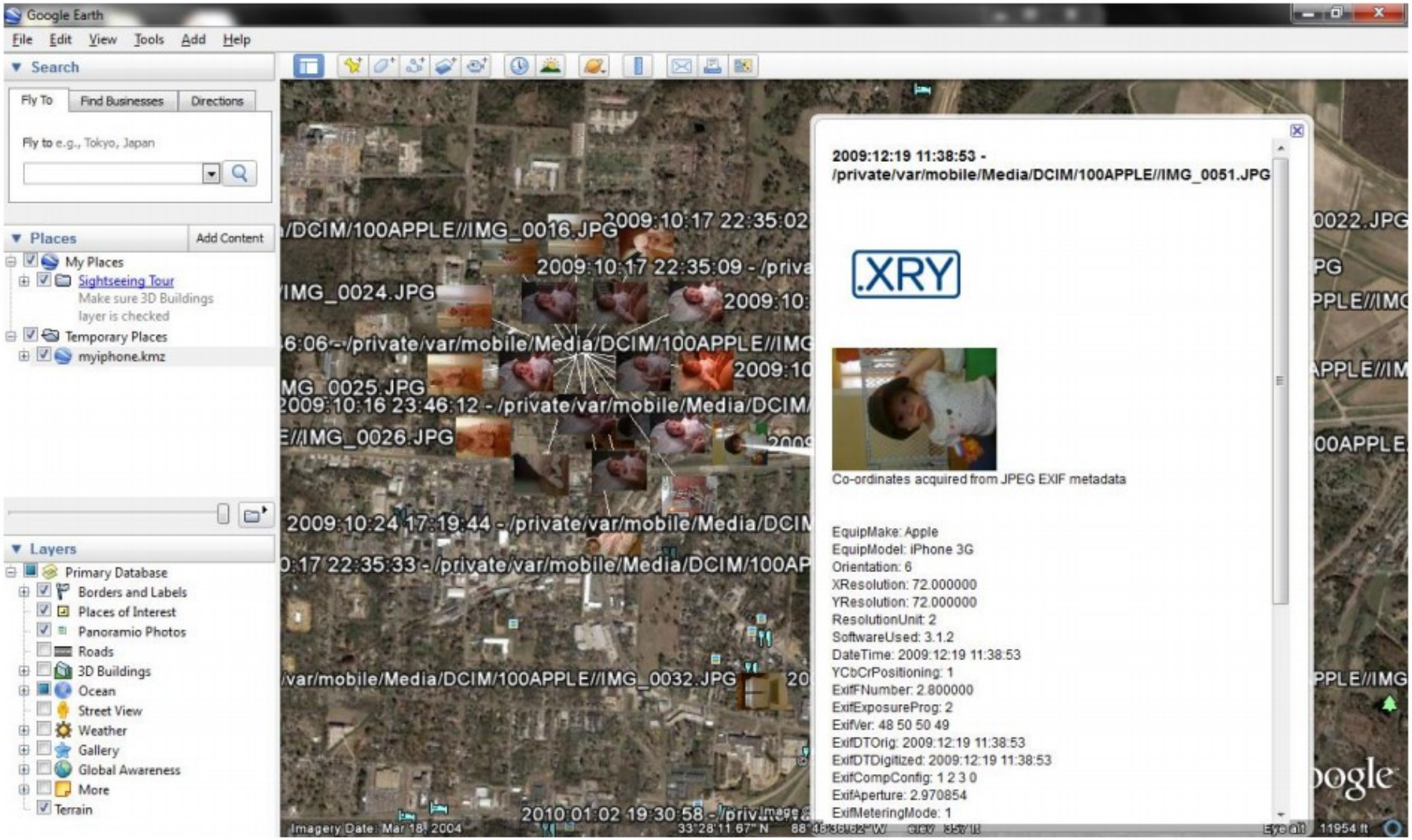
MSAB Forensic Office

- 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!

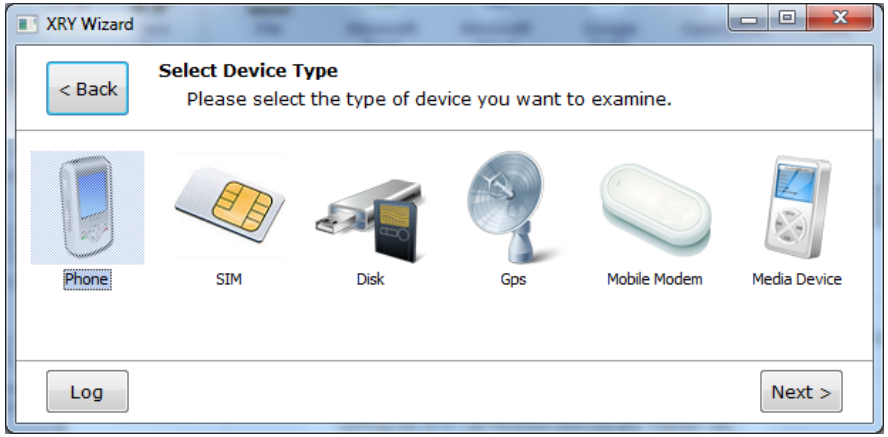
MSAB XRY

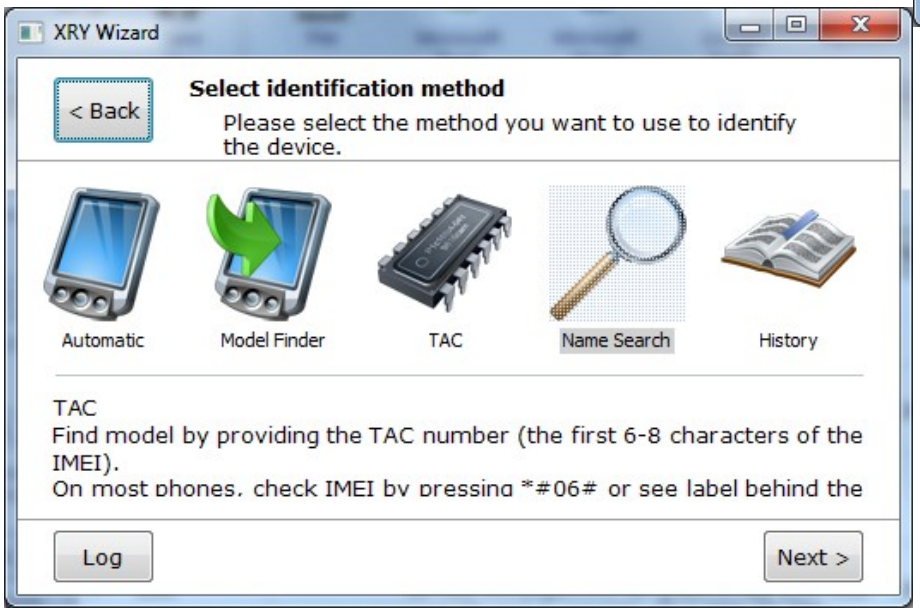

XRY - [SonyEricsson_K800i.xry]
File
Edit
View
Windows
Tools
Options
About
Extract Data
Open
Close
Save
Save As
File
Microsoft Excel
Microsoft Word
Google Earth
OpenOffice
XML
Print
Device Manual
Help Topics
Extract Data
Open Save
Export
Print Options
Help
Media Window
Summary
Case Data
General Information
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 zo meteen 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 wel leuk. Tot straks, bye 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
Ready
CAP
NUM
SCRL

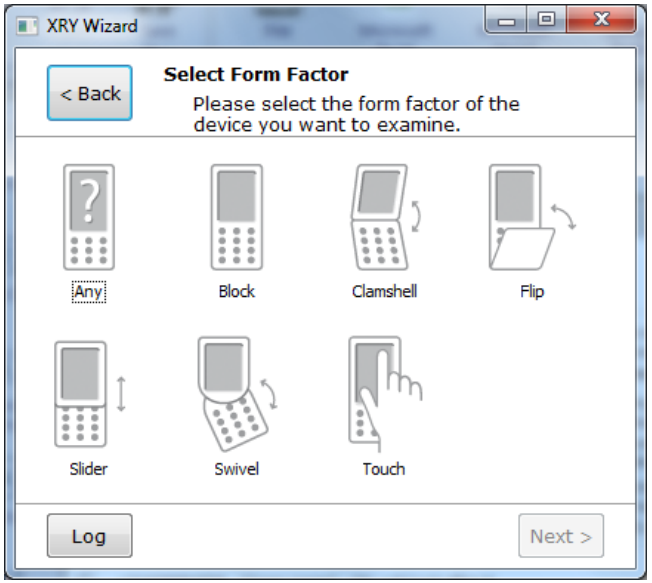
Geocoded Data



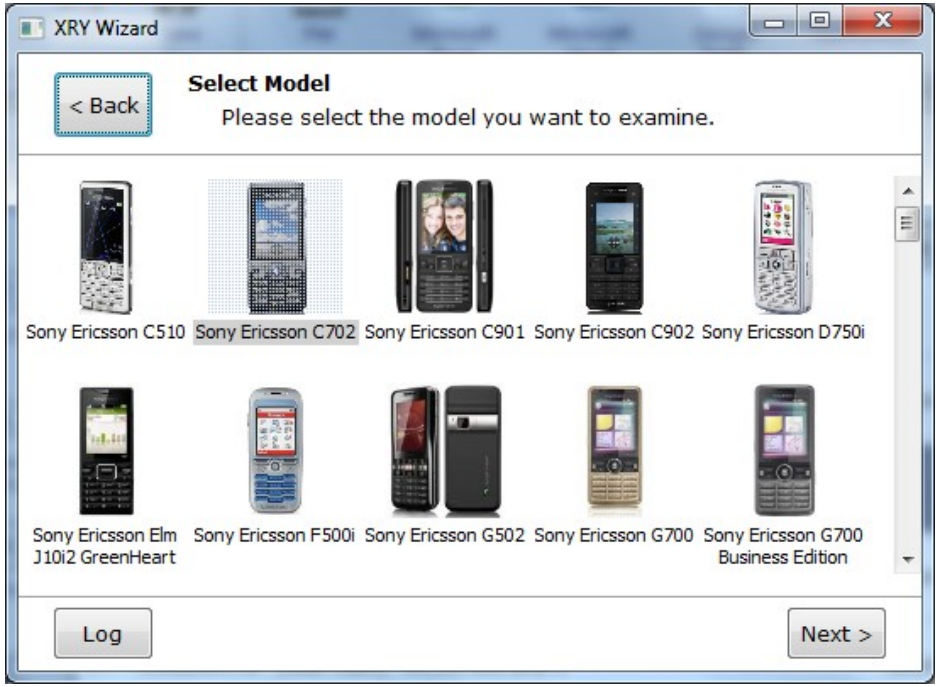
MSAB XRY Wizard 1

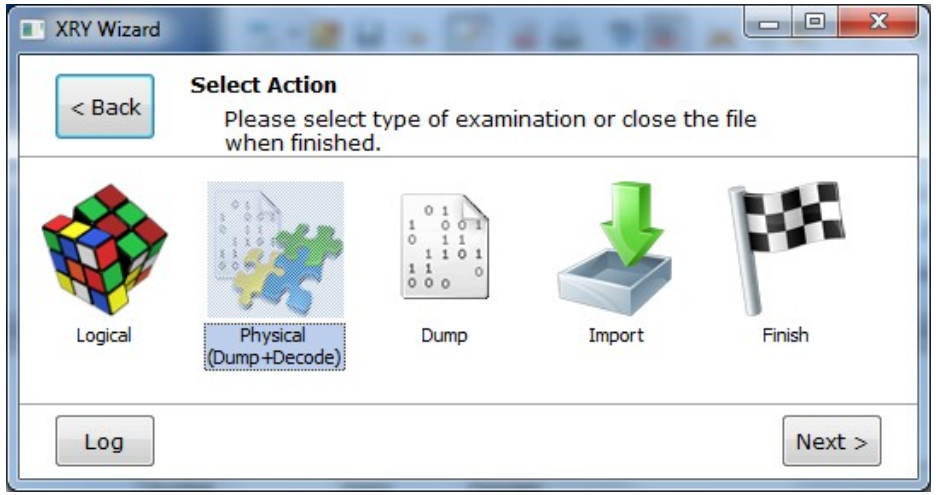


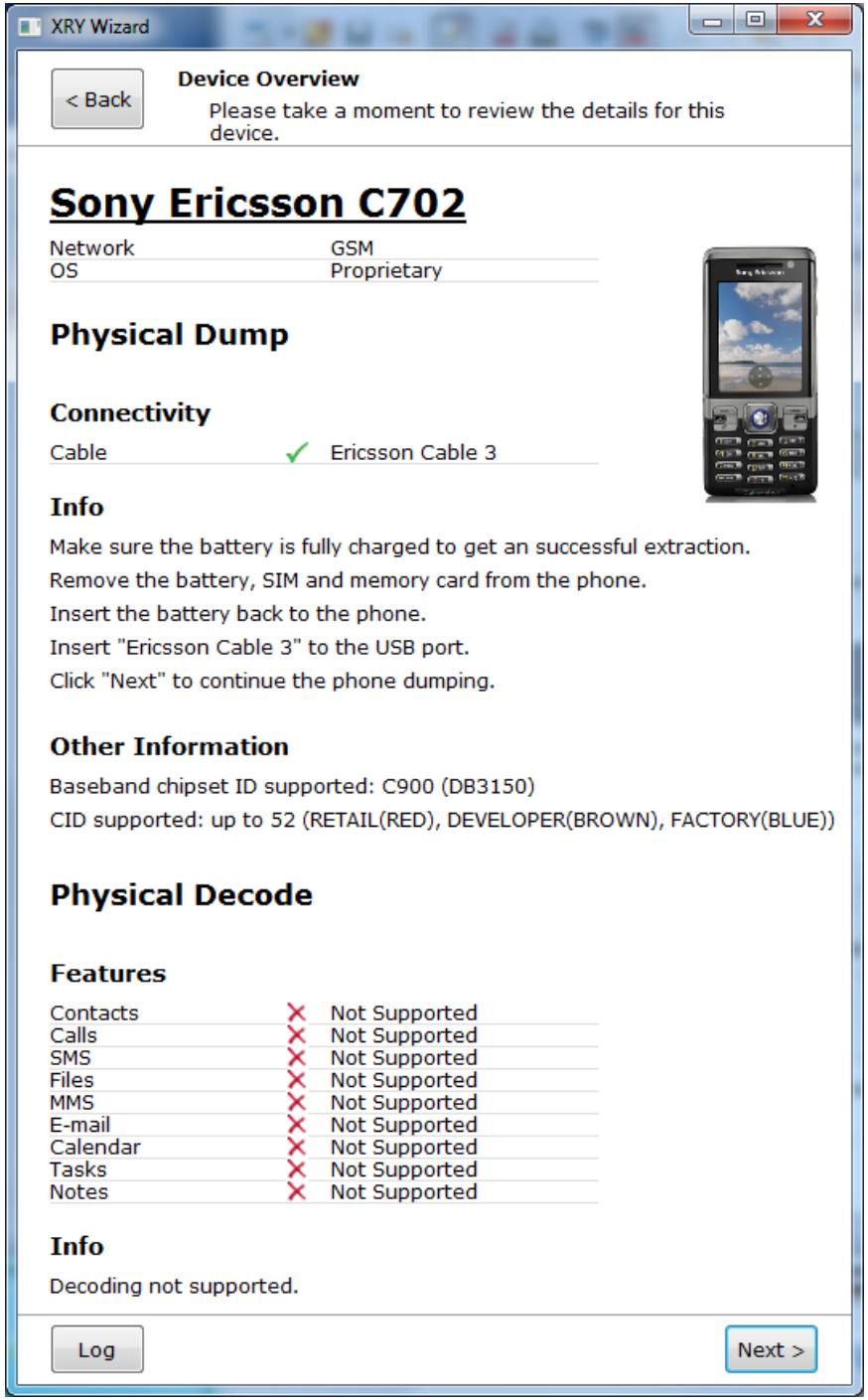




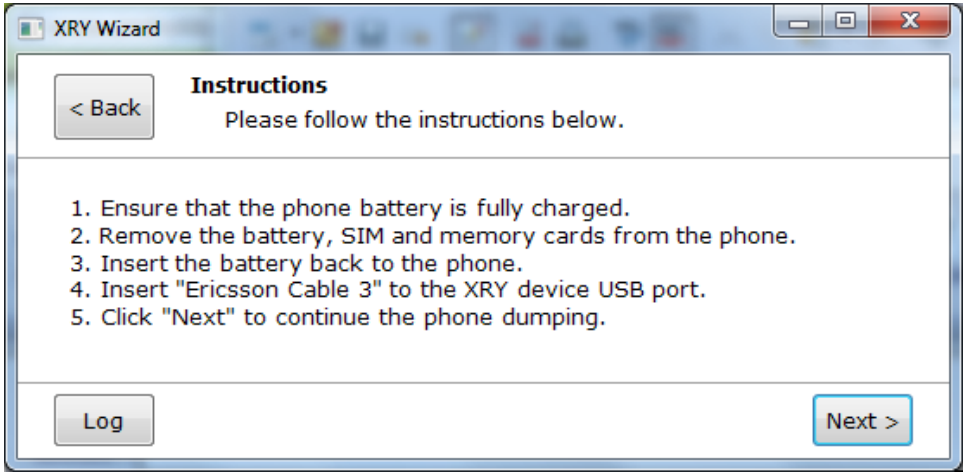
MSAB XRY 2

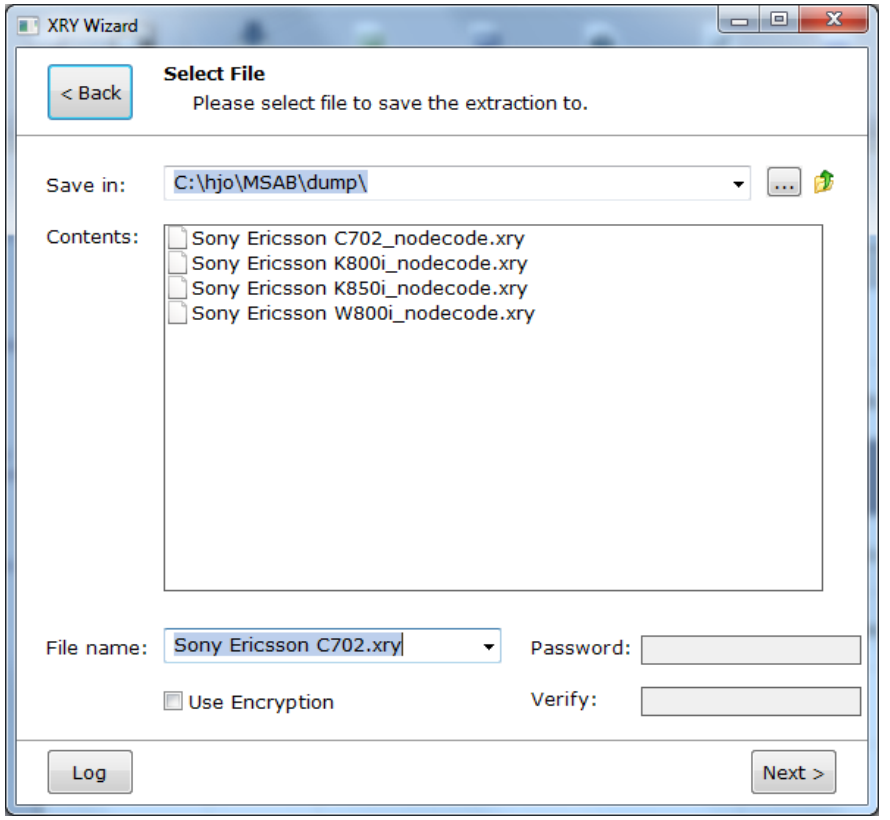

XRY Wizard
< Back
Select Model
Please select the model you want to examine.
Sony Ericsson C510
Sony Ericsson C702
Sony Ericsson C901
Sony Ericsson C902
Sony Ericsson D750i
Sony Ericsson Elm J10i2 GreenHeart
Sony Ericsson F500i
Sony Ericsson G502
Sony Ericsson G700
Sony Ericsson G700 Business Edition
Log
Next >

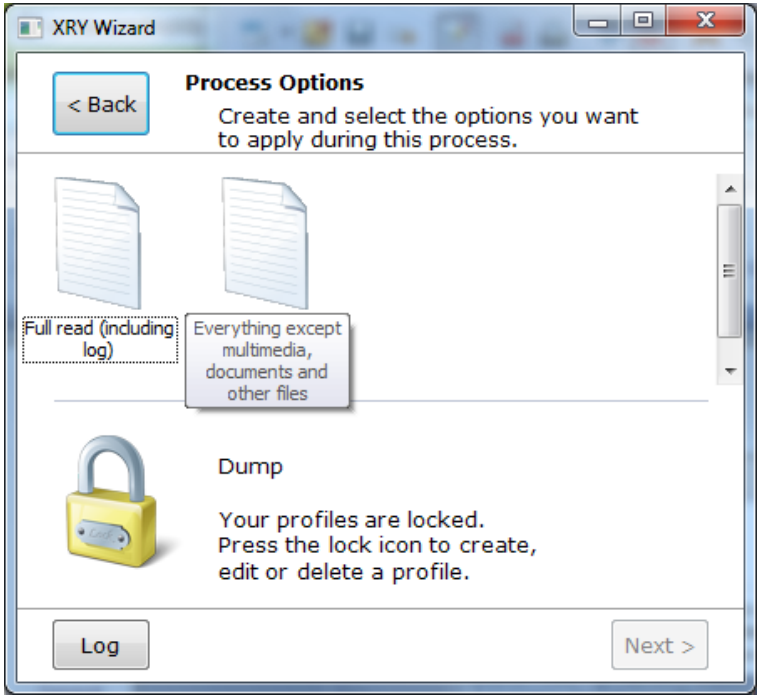

XRY Wizard
< Back
Select Action
Please select type of examination or close the file when finished.
Logical
Physical (Dump+Decode)
Dump
Import
Finish
Log
Next >

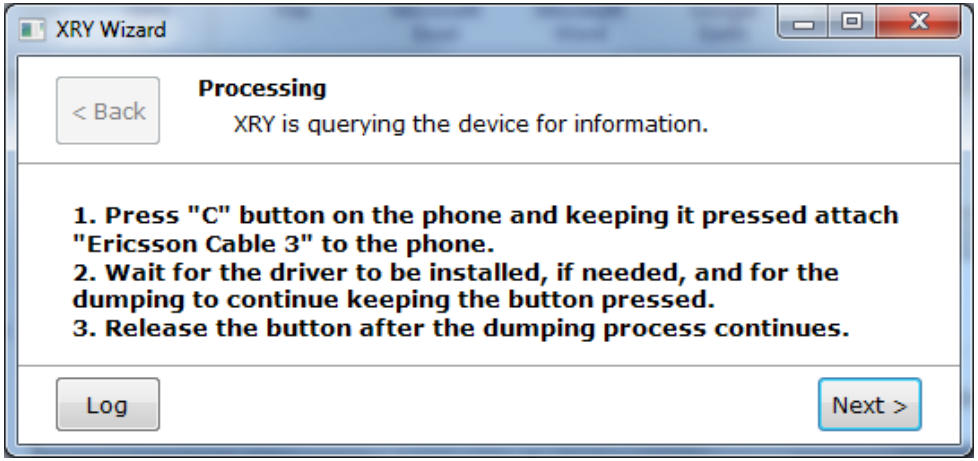

XRY Wizard
< Back
Device Overview
Please take a moment to review the details for this device.
Sony Ericsson C702
Network GSM
OS Proprietary
Physical Dump
Connectivity
Cable Ericsson Cable 3
Info
Make sure the battery is fully charged to get an successful extraction.
Remove the battery, SIM and memory 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 Not Supported
Calls Not Supported
SMS Not Supported
Files Not Supported
MMS Not Supported
E-mail Not Supported
Calendar Not Supported
Tasks Not Supported
Notes Not Supported
Info
Decoding not supported.
Log
Next >

MSAB XRY 3


XRY Wizard
< Back
Instructions
Please follow the instructions below.
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
< Back
Select File
Please select file to save the extraction to.
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
< Back
Process Options
Create and select the options you want to apply during this process.
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 >


XRY Wizard
< Back
Processing
XRY is querying the device for information.
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 >

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.

Micro Systemation AB
Visiting address: Hornsbruksgatan 28

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 thay 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.

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

Cost effective, rewritable SIM cards
SIM id-Cloner Examination cards are re-writeable, 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)

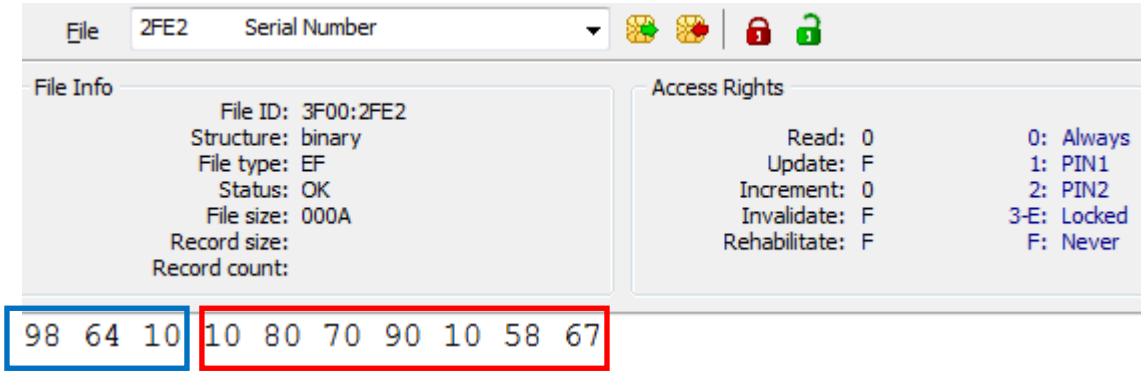
IMSI = MCC + MNC + MSIN

MCC	240	Sweden
MNC	01	Telia
MSIN	1234567890	

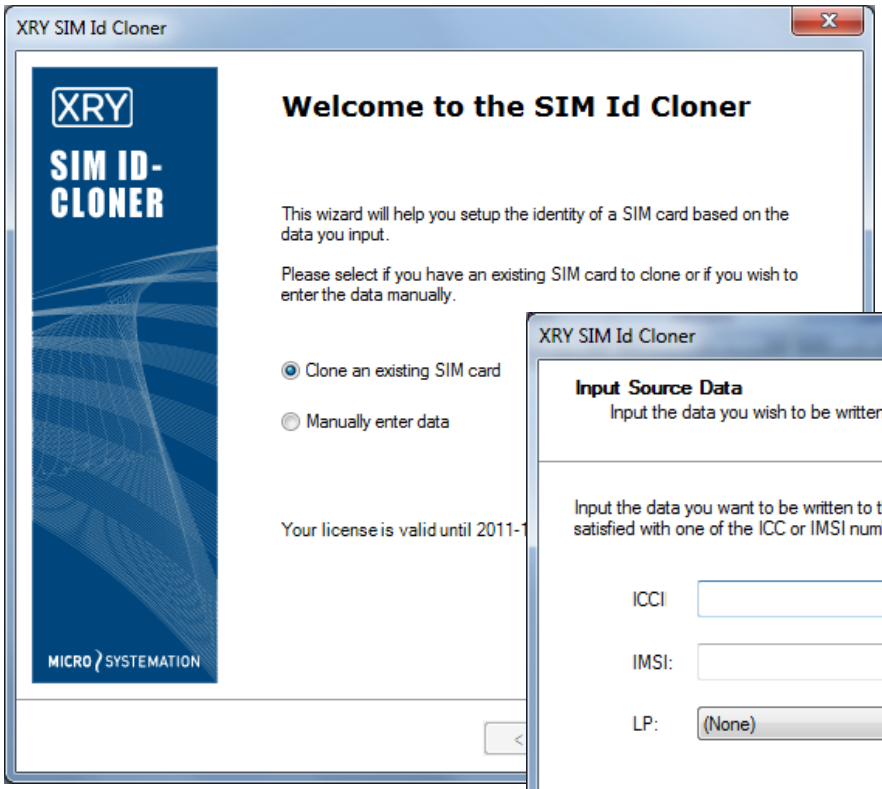
- IMSI analysis
  - The process of examining a subscriber's IMSI to identify which network the IMSI belongs to and whether subscribers from that network are allowed to use a given network

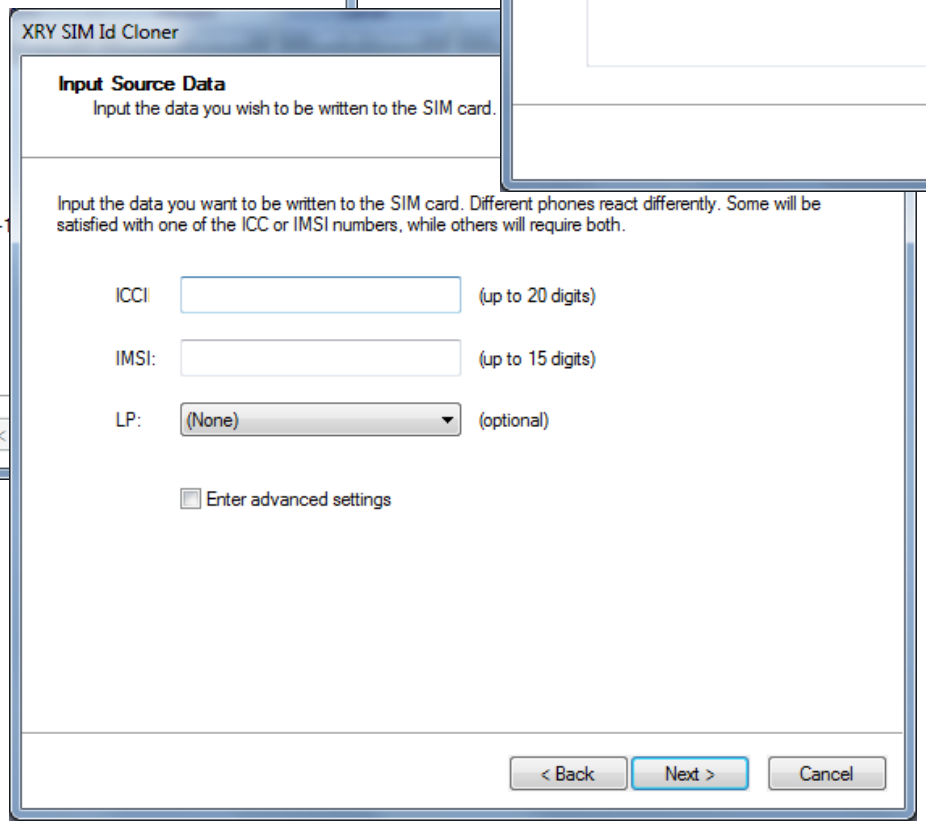
Integrated Circuit Card Identifier

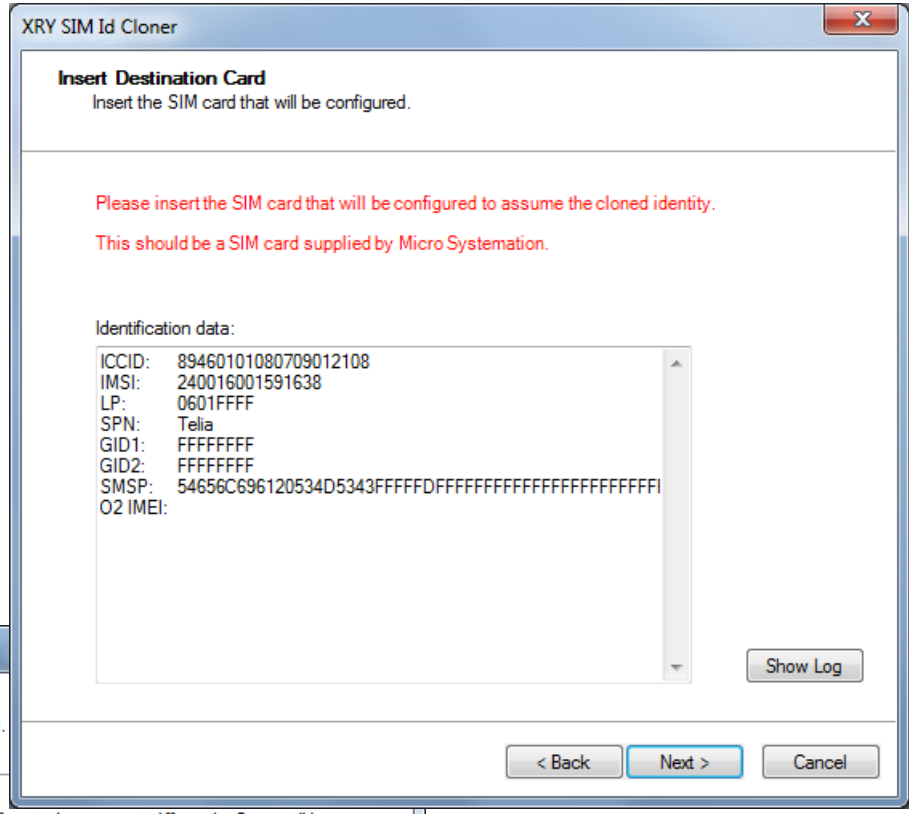
- **ICCID** uniquely identifies the SIM card, one can determine issuing service provider and country code from ICCID
- International Standard ISO/IEC 7812
  - http://en.wikipedia.org/wiki/ISO_7812
  - 19 or 20 digits in length and always stored in the card
  - Normally printed on the outside (may be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



MSAB XRY SIM Id Cloner







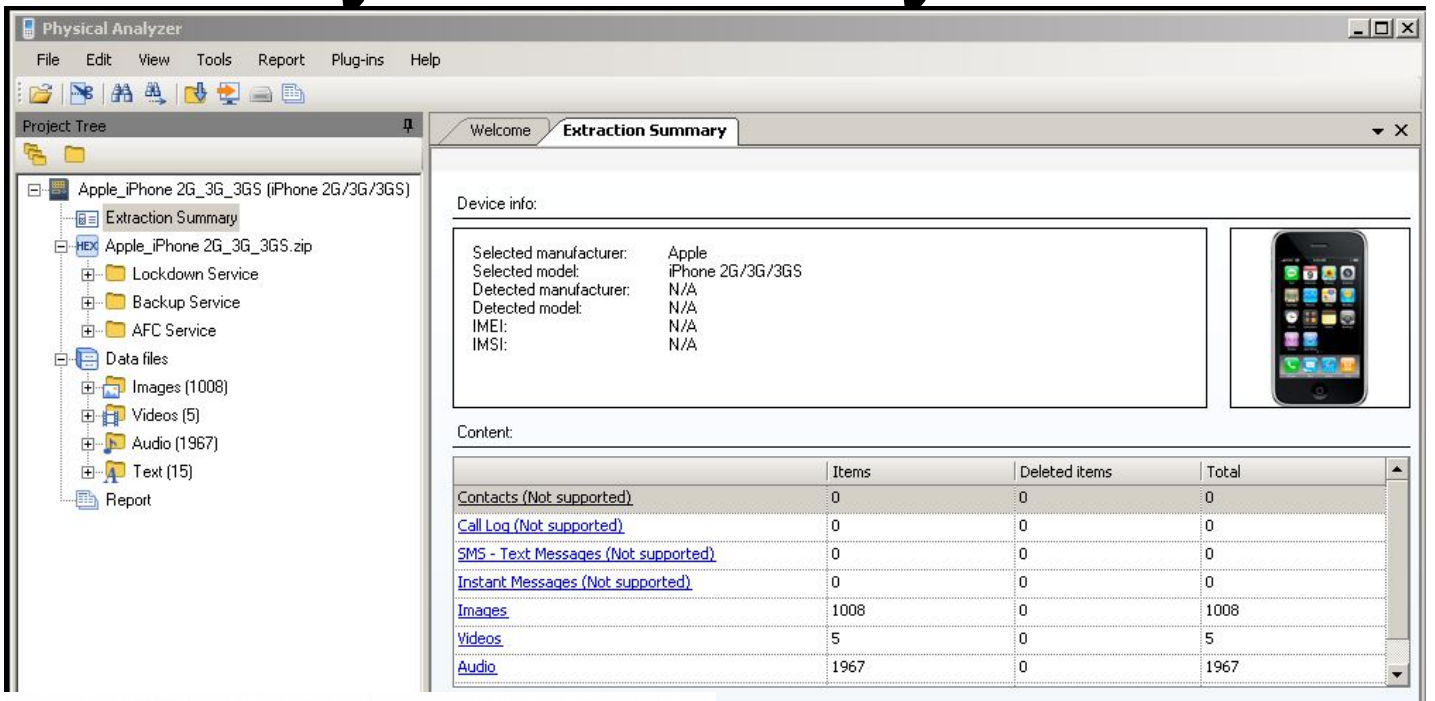
FTS Forensic Telecommunications Services

cellebrite
mobile data secured

- 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

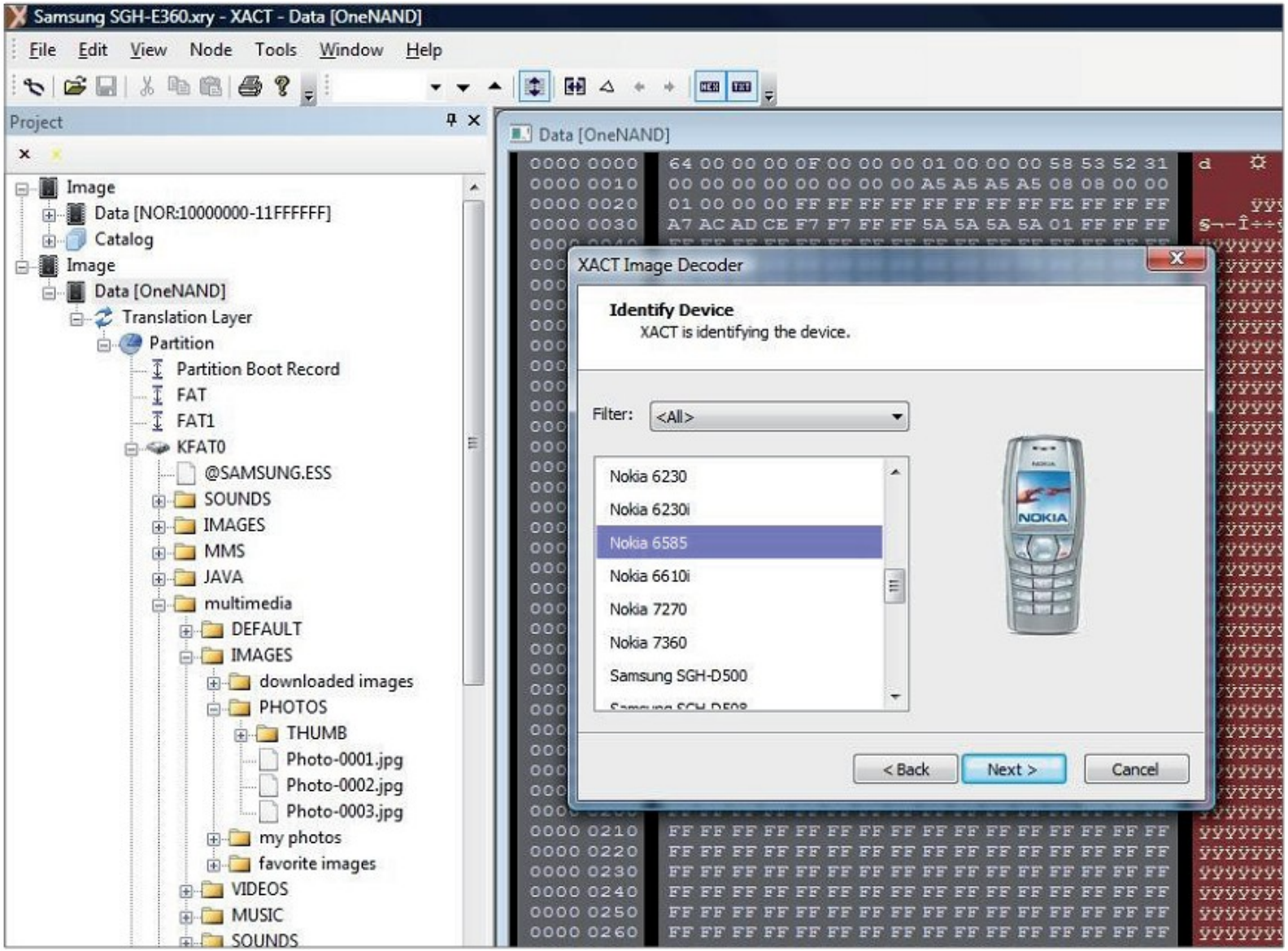
cellebrite
mobile data secured



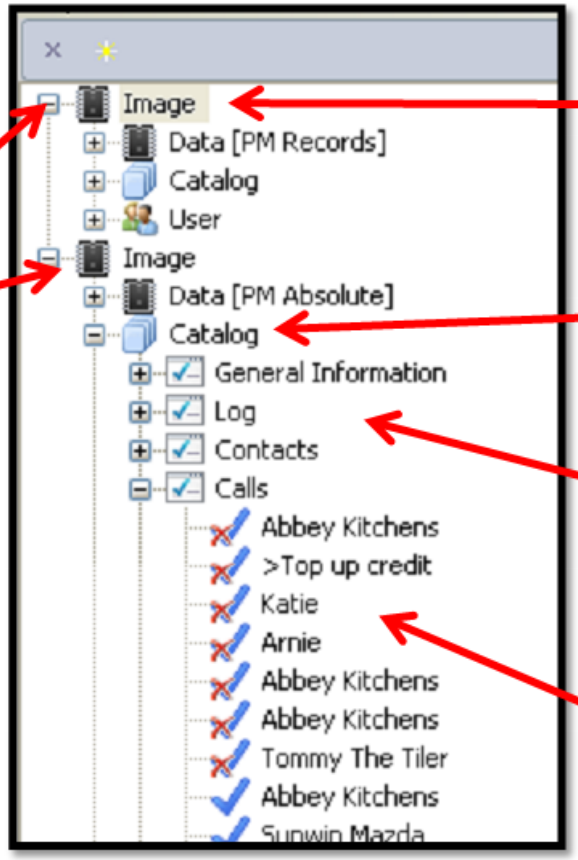
Generate Report

/2010 9:46:19 PM
/2010 12:06:42 PM
[redacted]
.7
e No. 110
e 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
< Back
Next >
Cancel

XACT Project Structure



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

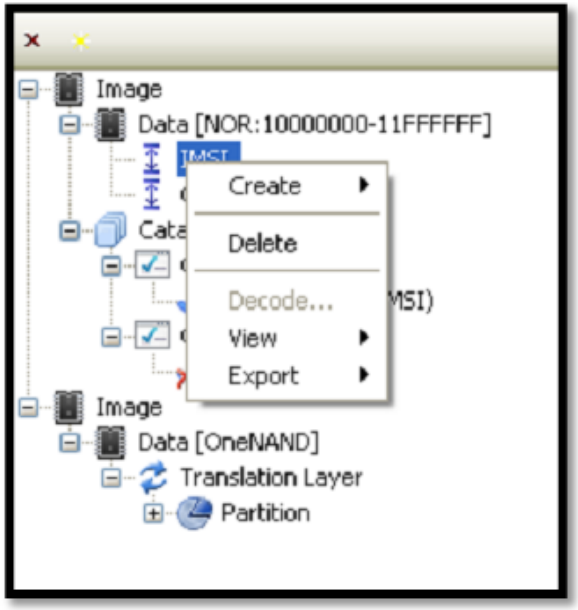
"Image" entries are always at the top level in the XACT Project window

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

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

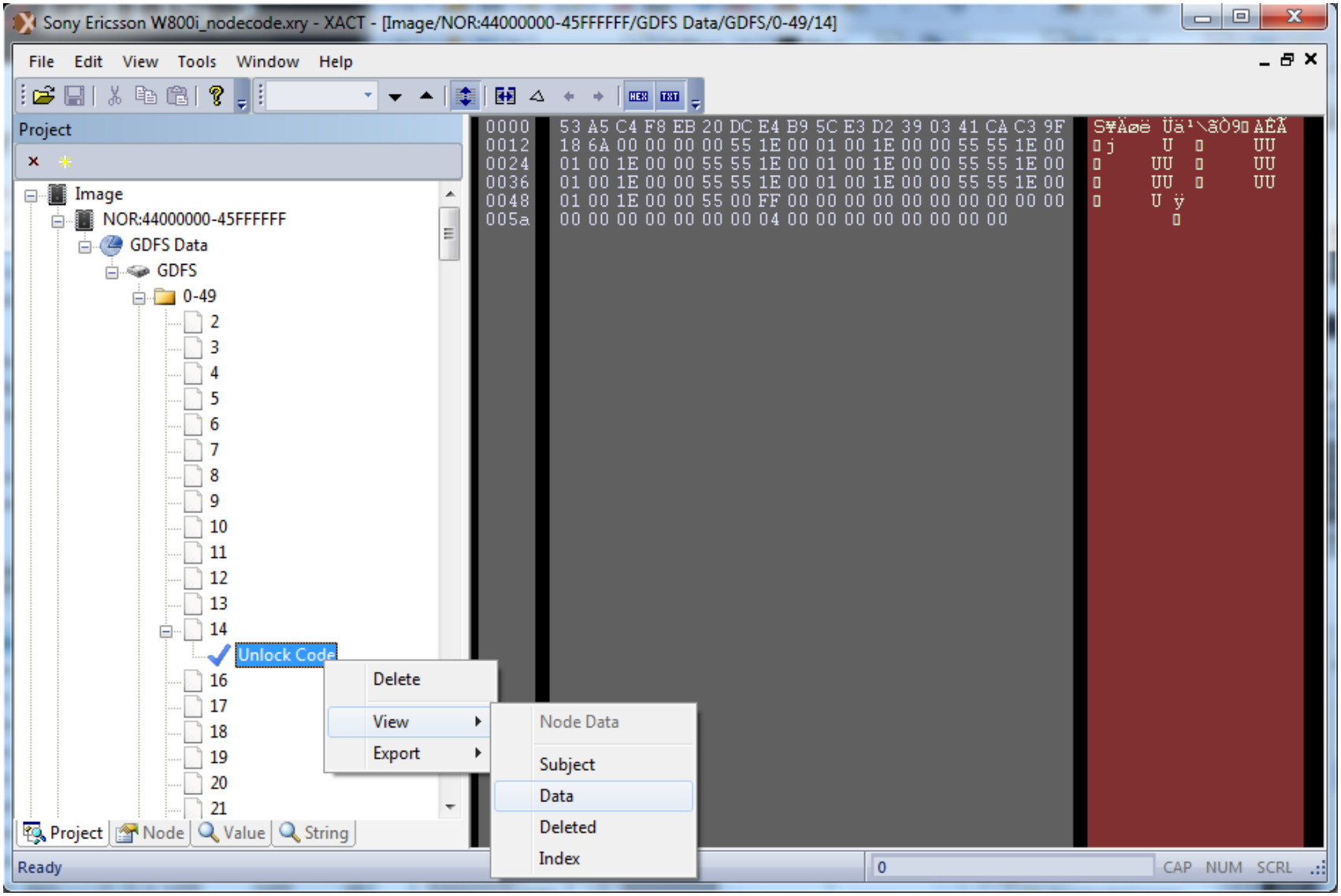
Decoded data "items" the red cross indicates "deleted" or "inactive"

XACT Project Structure

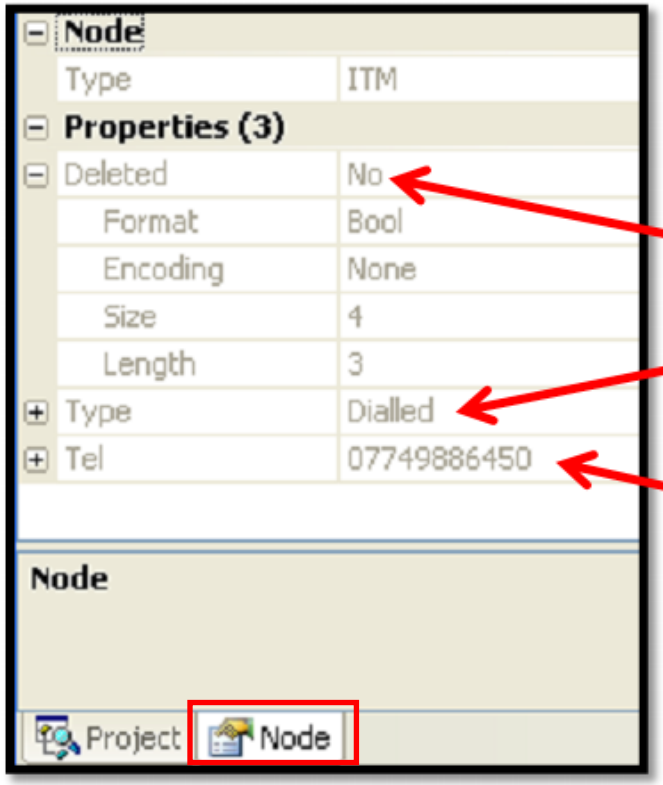


- All entries in the Project window are “nodes”
- Different actions are available for each node type
  - Right click on a node to select an action
- Some node types can be double-clicked to view data in a separate hex viewer window

MSAB XACT 2


Sony Ericsson W800i_nodecode.xry - XACT - [Image/NOR:44000000-45FFFFFF/GDFS Data/GDFS/0-49/14]
File Edit View Tools Window Help
Project
Image
NOR:44000000-45FFFFFF
GDFS Data
GDFS
0-49
2
3
4
5
6
7
8
9
10
11
12
13
14
Unlock Code
16
17
18
19
20
21
Delete
View
Export
Node Data
Subject
Data
Deleted
Index
Project
Node
Value
String
Ready
CAP NUM SCRL

Viewing Item Properties



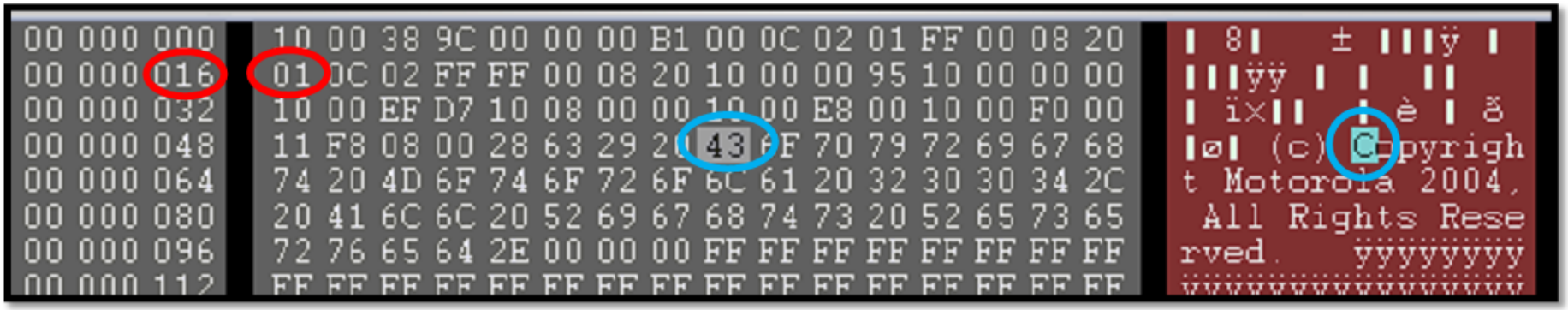
- "Node view" is used to view the contents of a data item

Live (not deleted)

Dialled call

To 07749 886450

XACT Hex Viewer



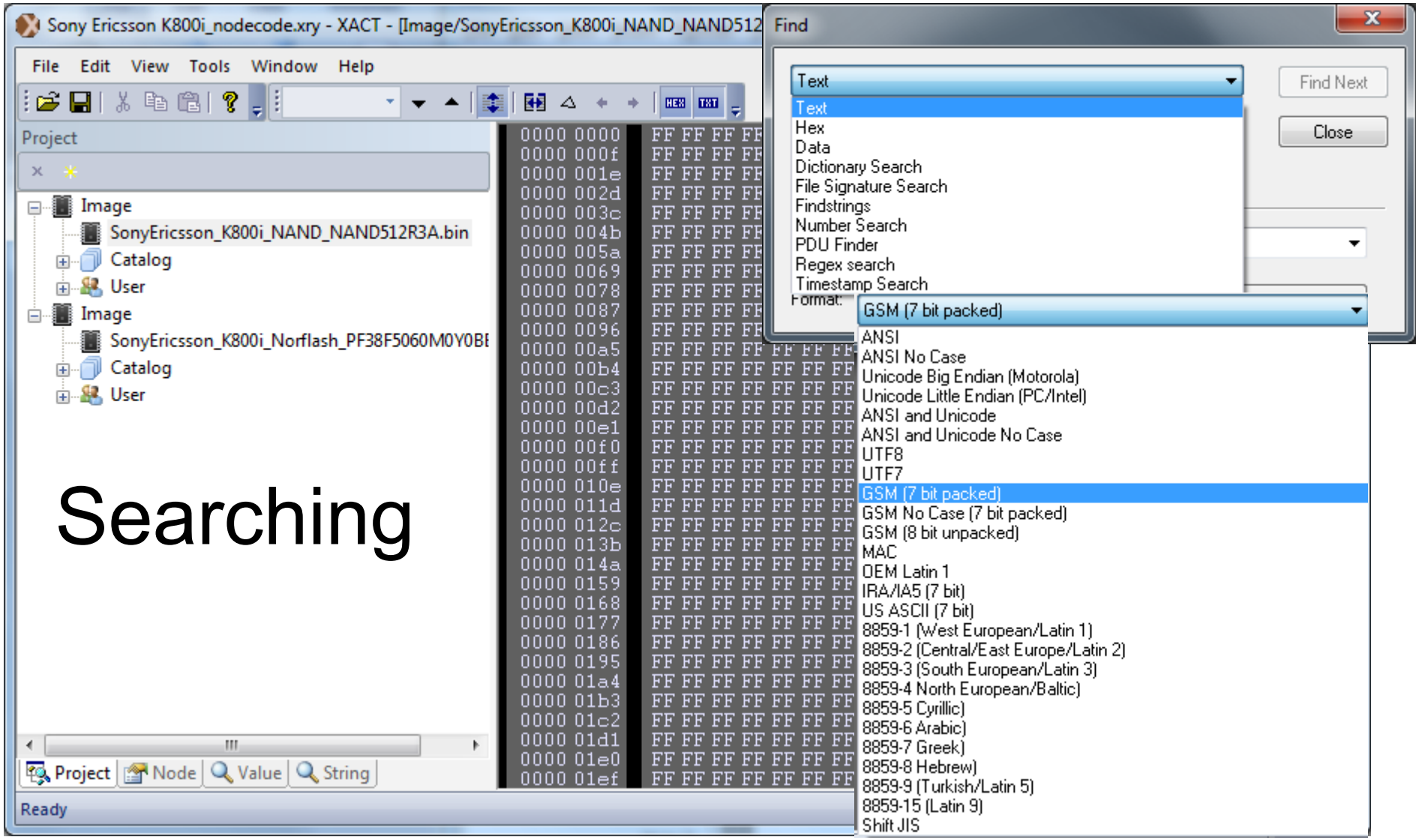
The "016" here tells us the position for the first byte on this line

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)

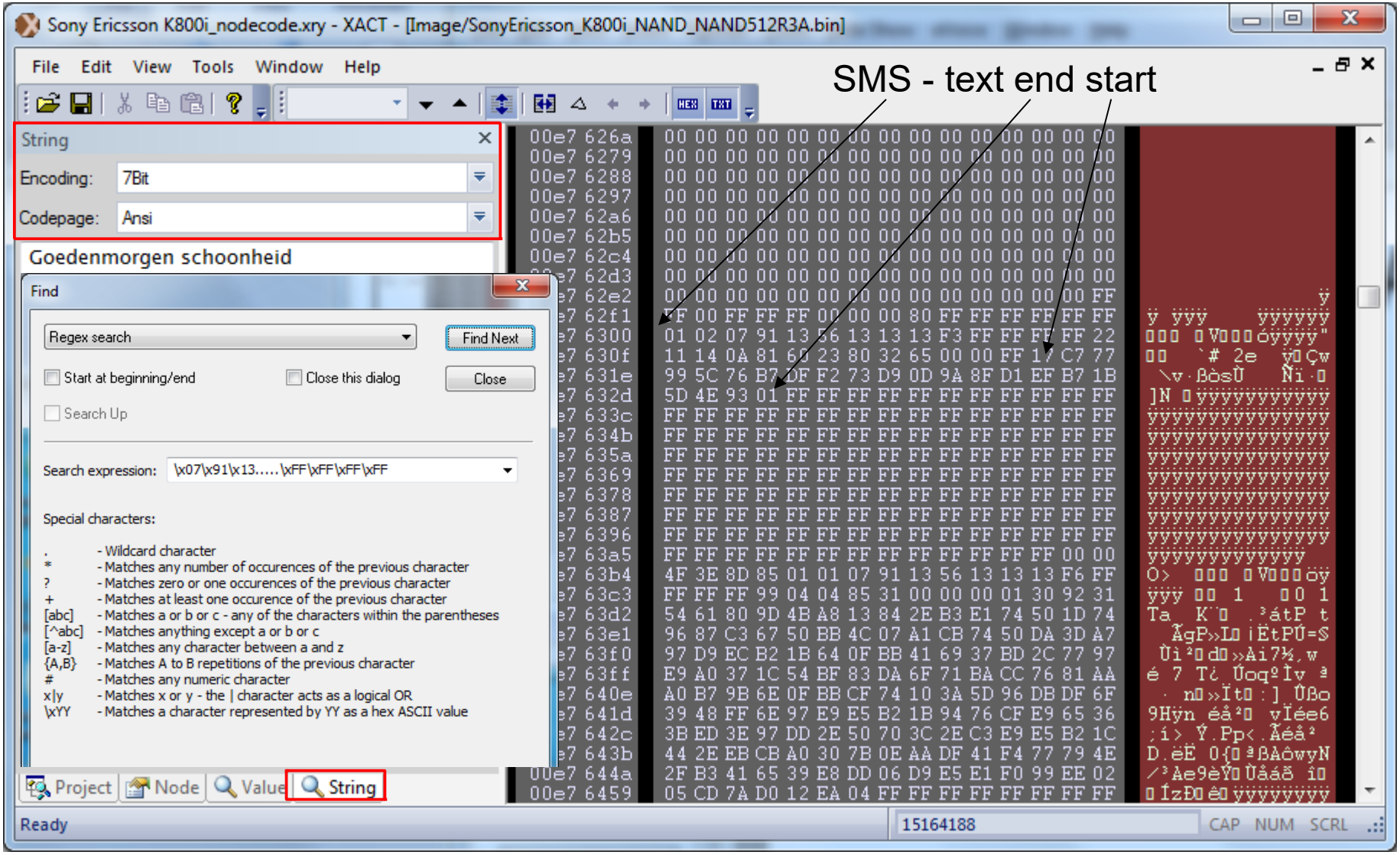
MSAB XACT 3

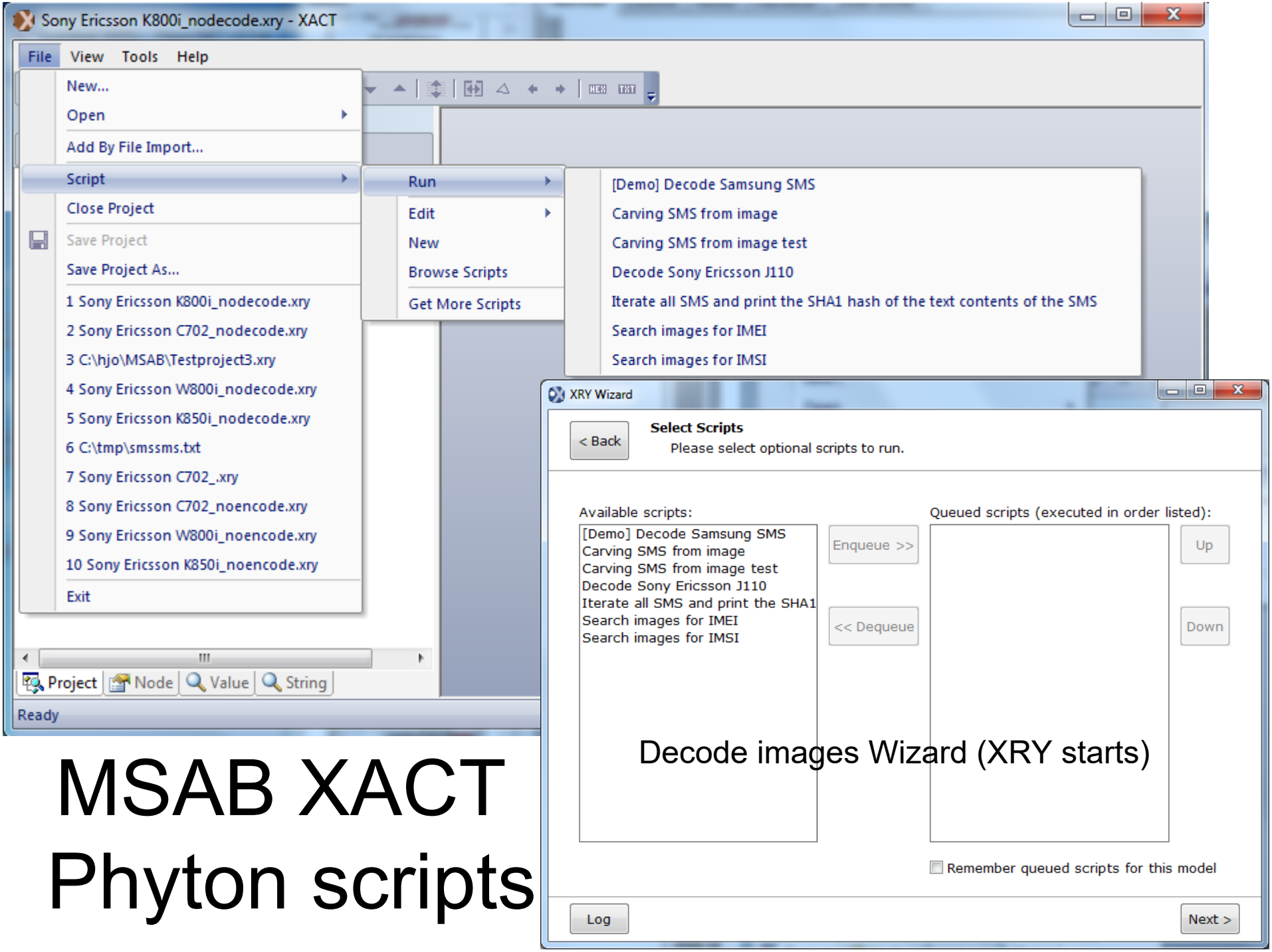


Searching

MSAB XACT 4

SMS 7-bit Encoding



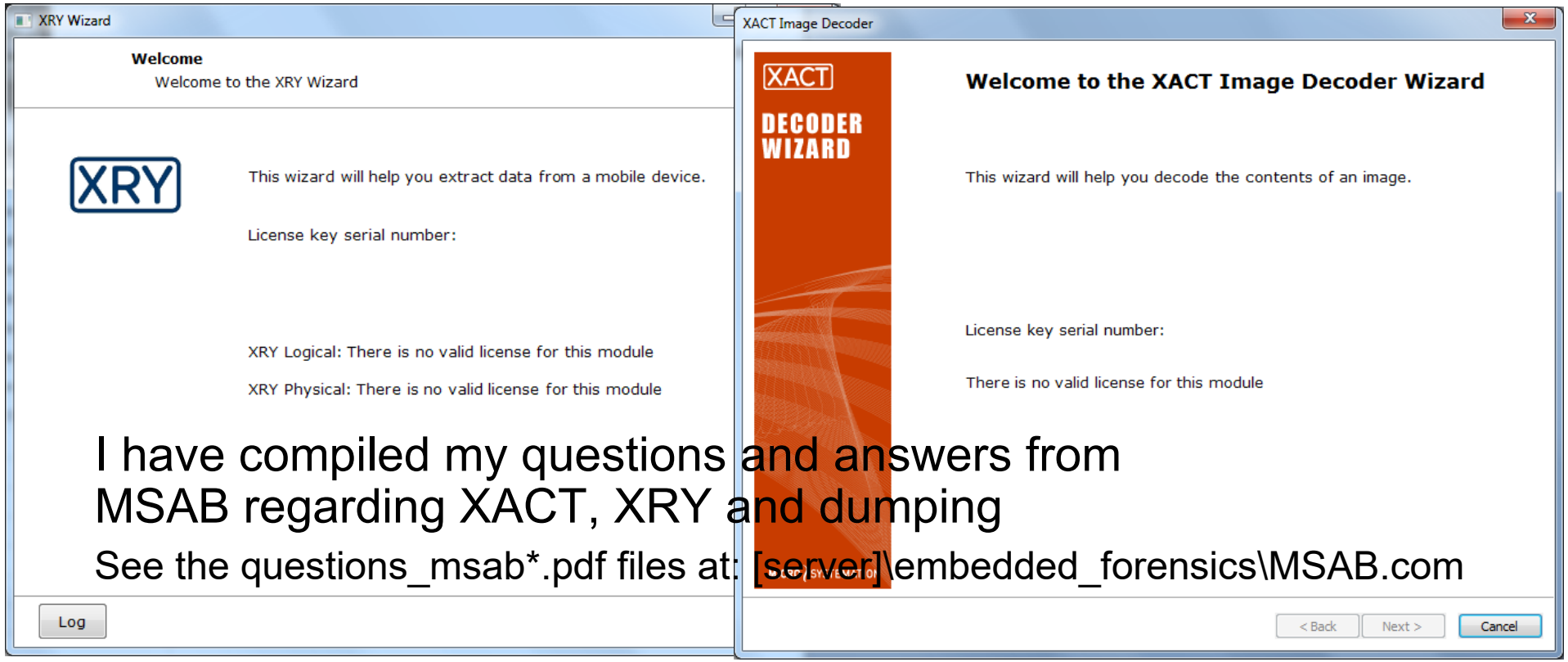


MSAB XACT Phyton scripts

Decode images Wizard (XRY starts)

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

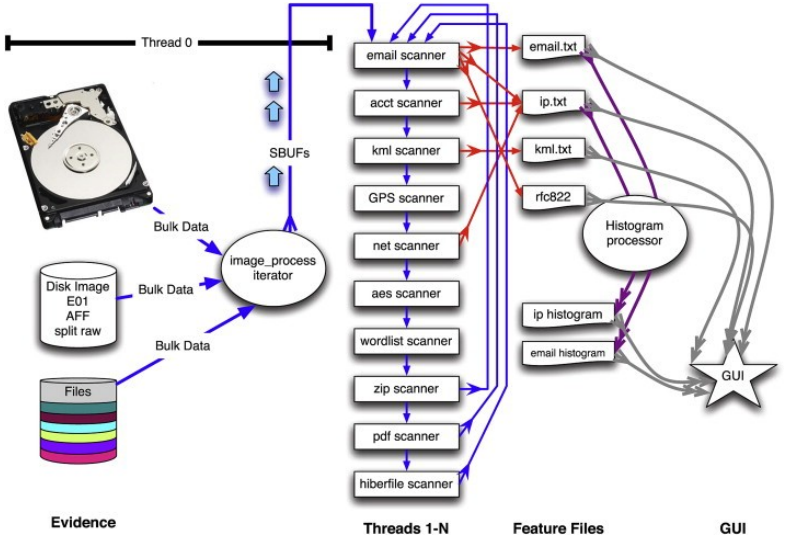
Extracting dump data

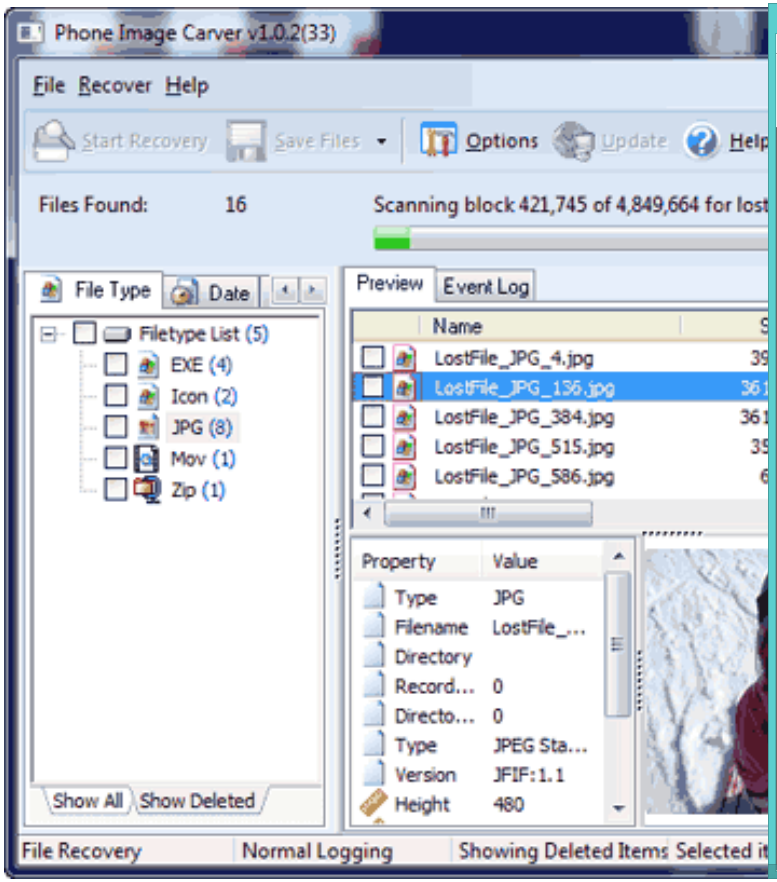
Spare area may or may not be included in MSAB phone dumps!

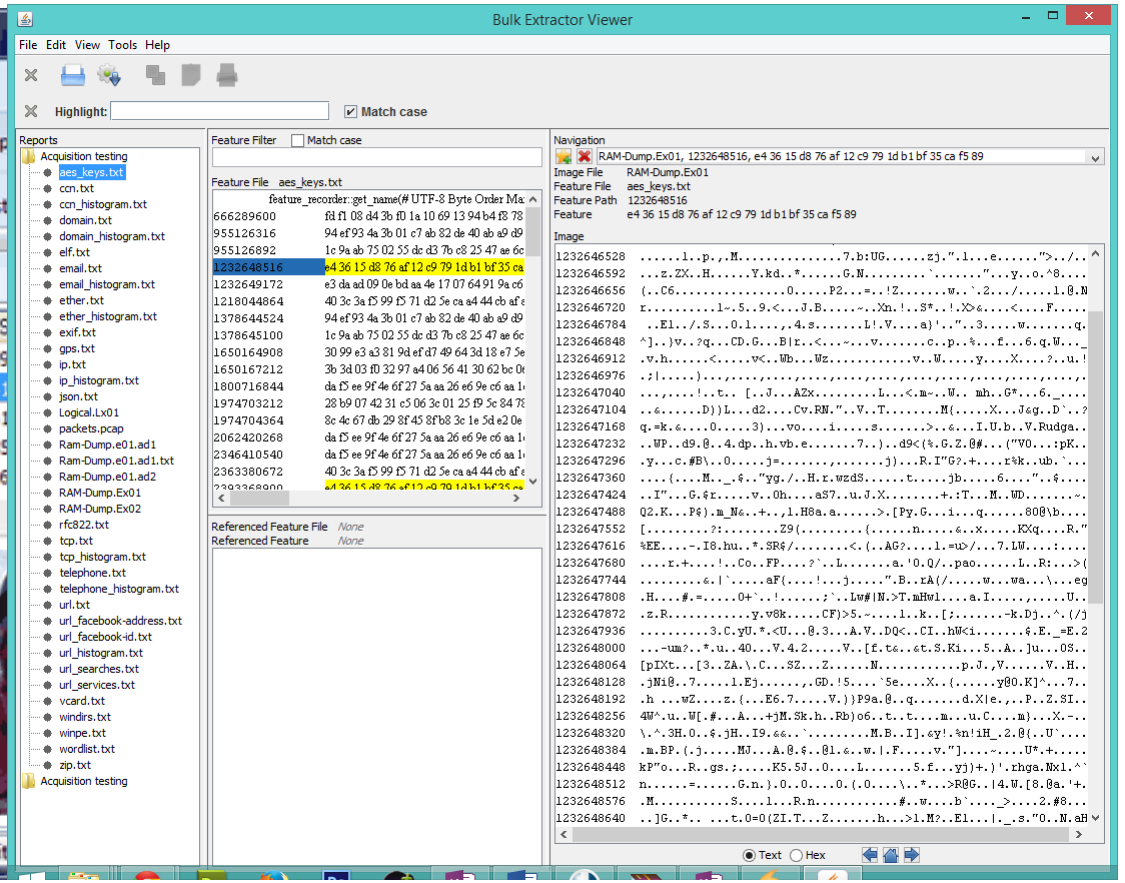
- Non file based
  - Lock keys, IMEI, IMSI, ICCID
  - SMS, time stamps?, call logs?..., etc.
- File based – for best results you need to get rid of the NAND OOB/spare area (present in chip read dumps)
  - MMS, audio files, call logs
  - Videos - 3GP / MP4 with tools as NFI Defraser
  - E-mail, social 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







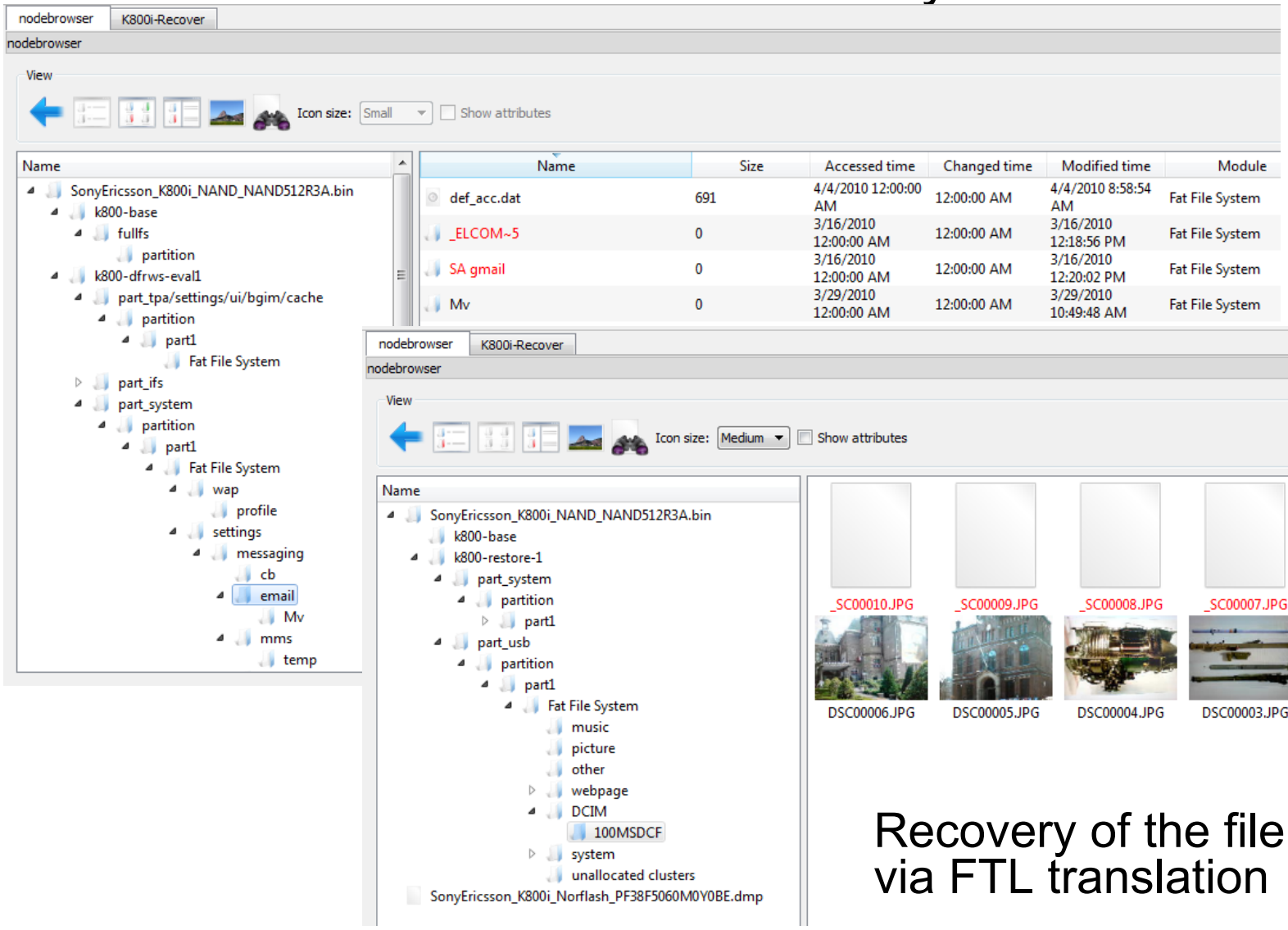
MSAB Building a file system

build_fat_fs.py
from the XACT manual

```
# 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)
```

Digital Forensics Framework

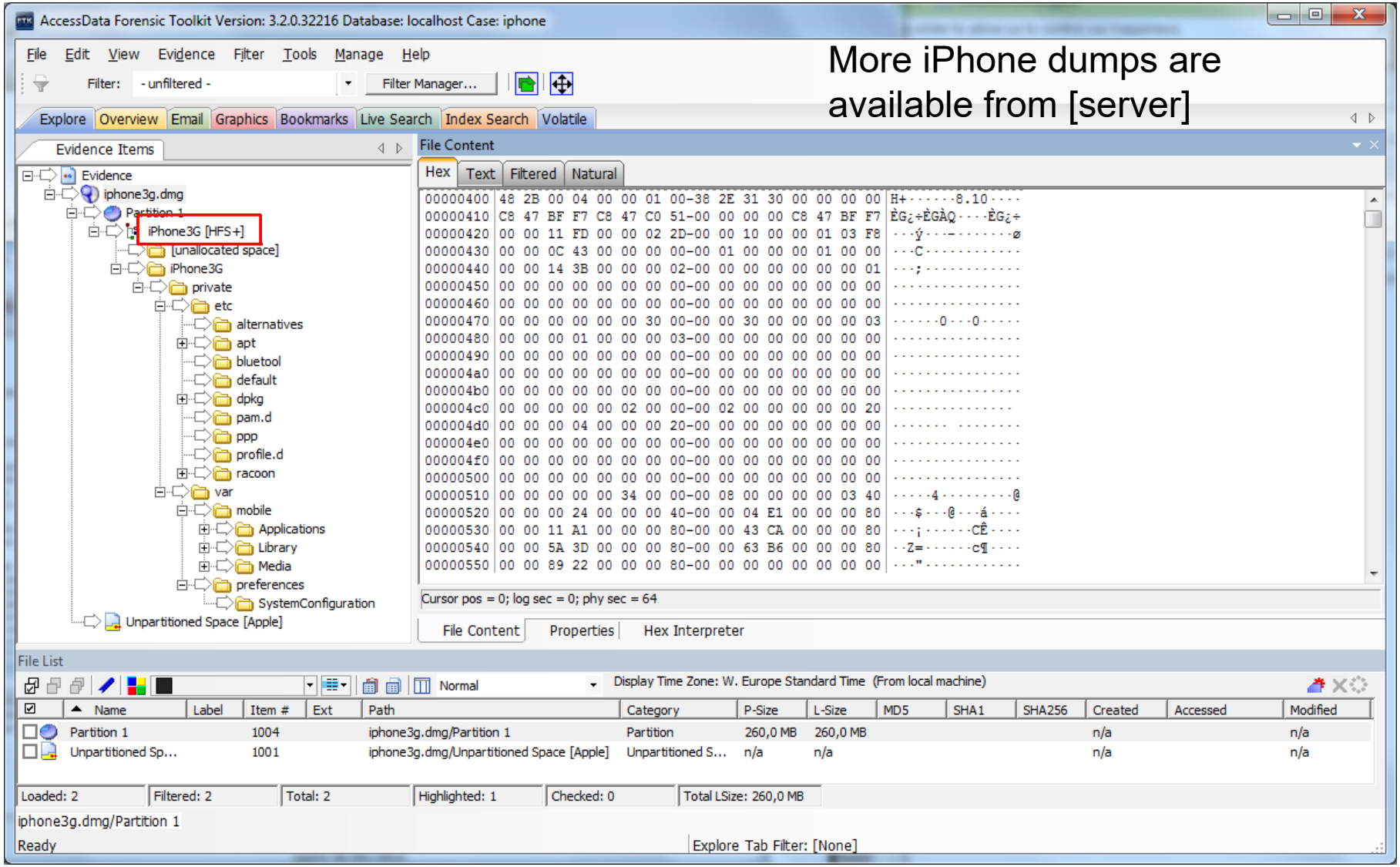
with winner of DFRWS 2010 Python module script



Recovery of the file system via FTL translation

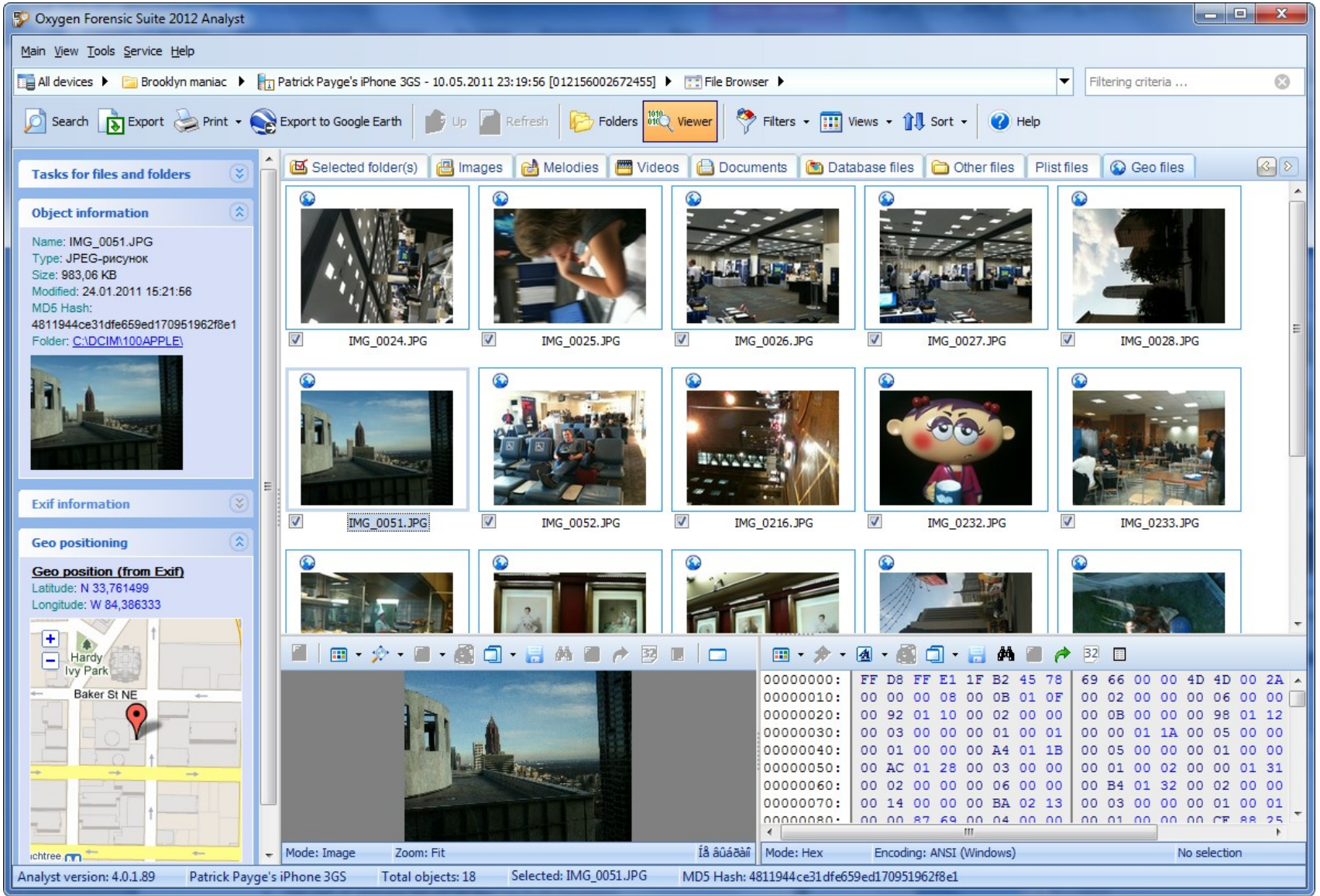
FTK >= 3.2 have YAFFS and Ext4 support

DMG dump from iPhone 3G

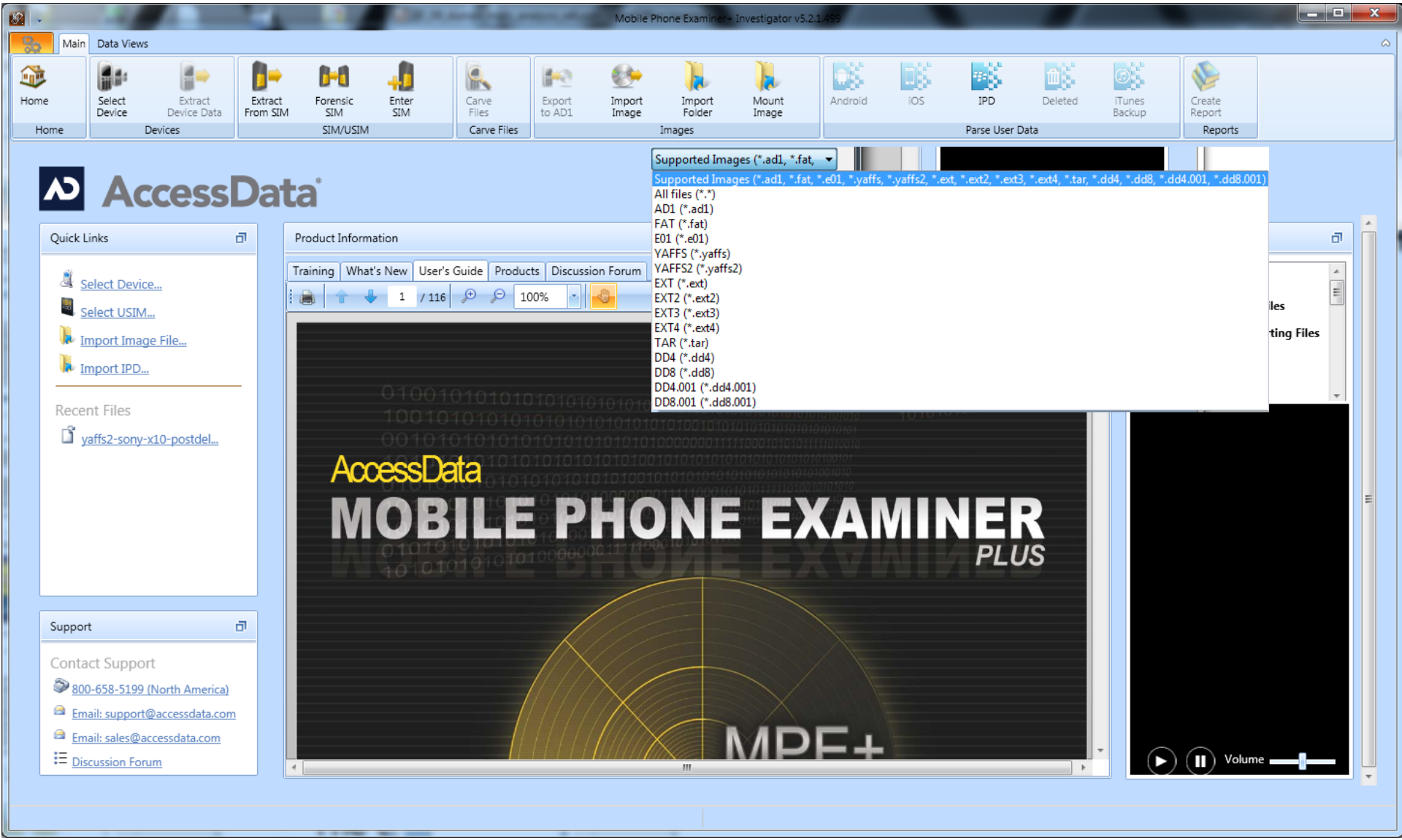


Oxygen Forensic Suite

Oxygen Forensics – many demo dumps on [server]



AccessData MPE+



Time stamps and search terms

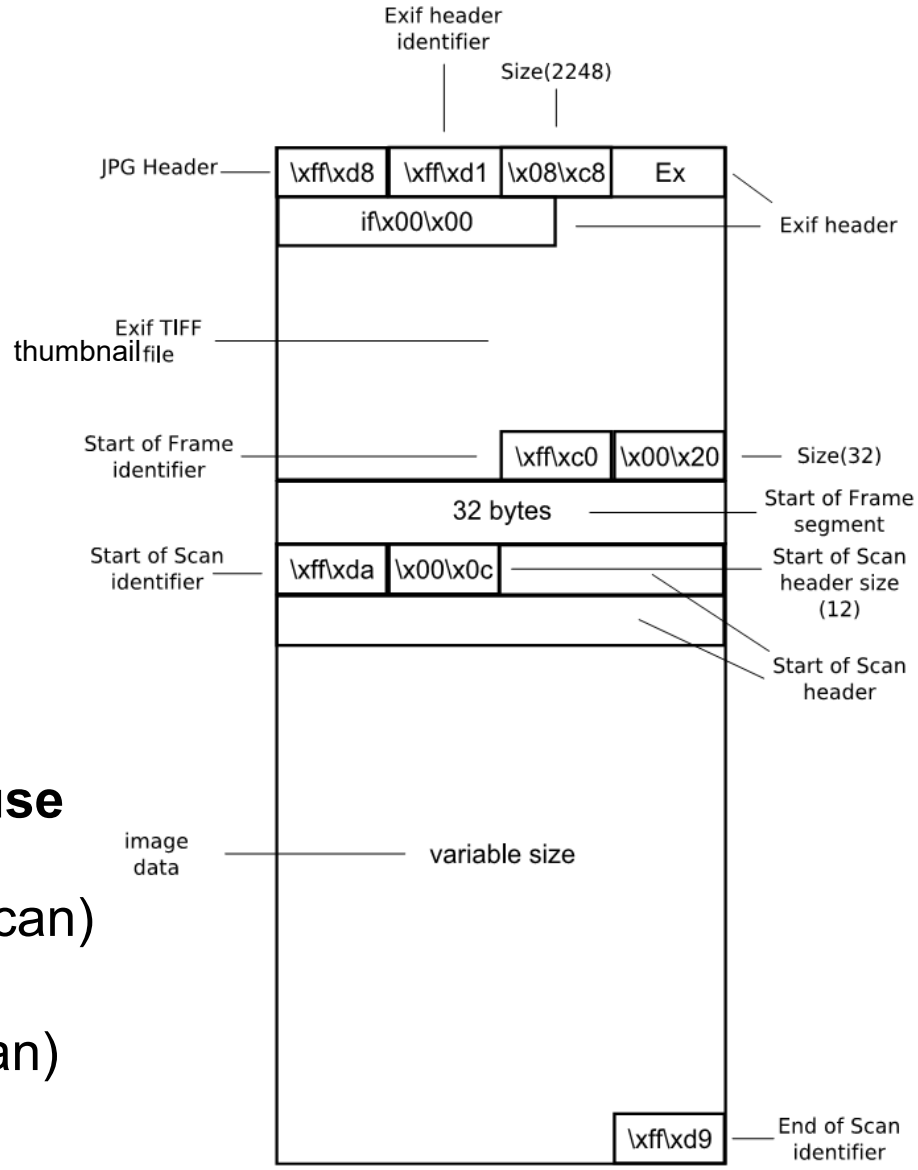
- A wide variety of storage formats are used for storing timestamp data in embedded system memories
- To illustrate - the timestamp "30 April 2008 14:30:59 UTC" is encoded as follows in some formats found in different mobile phone memories:
  - 0x80400341039500 (ETSI SMS)
  - 0xB19E0CA3 (Nokia)
  - 0x07D8041E0E1E3B (Nokia)
  - 0x26041E0E1E3B (Motorola)
  - 0x00E129CB0E8B2EC0 (Symbian)
  - 0x481882A3 (POSIX)

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

- Regular Expressions and Search Terms for Phone Examiners
  - http://www.controlf.net/regexps/
- Remember!
  - Many forensic artifacs are stored in manufacturer-specific or proprietary formats, it can even change between different models and revisions from the same manufacturer!

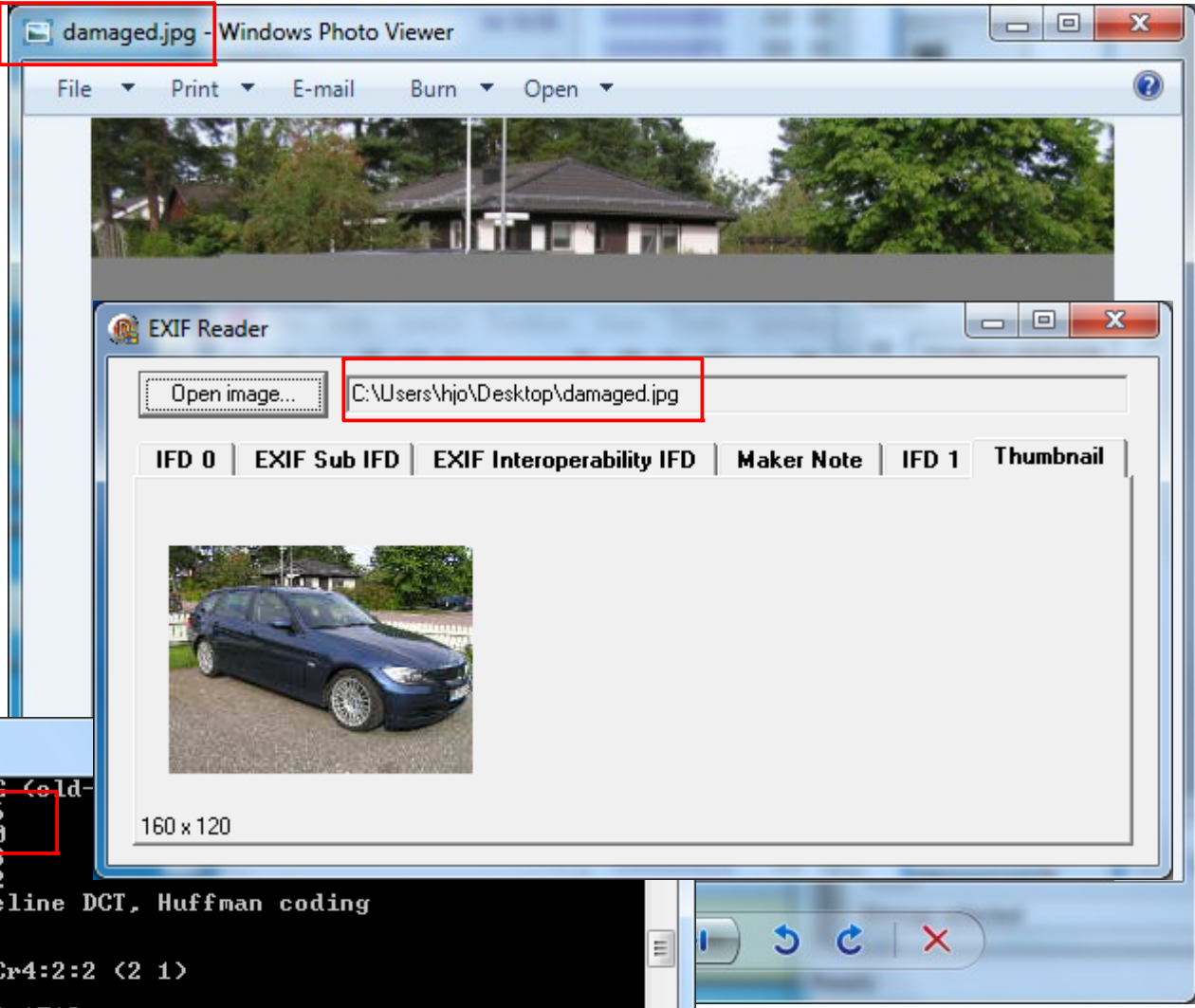
JPG file structure and carving

- 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 extr
act)
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

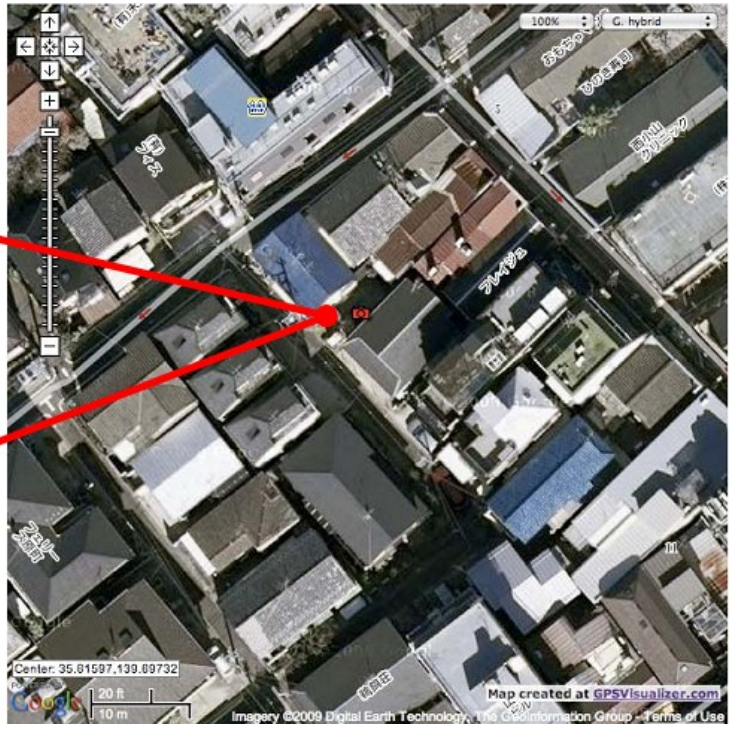
METADATA TAGS USED IN EXIF (JEITA CP-3451)

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

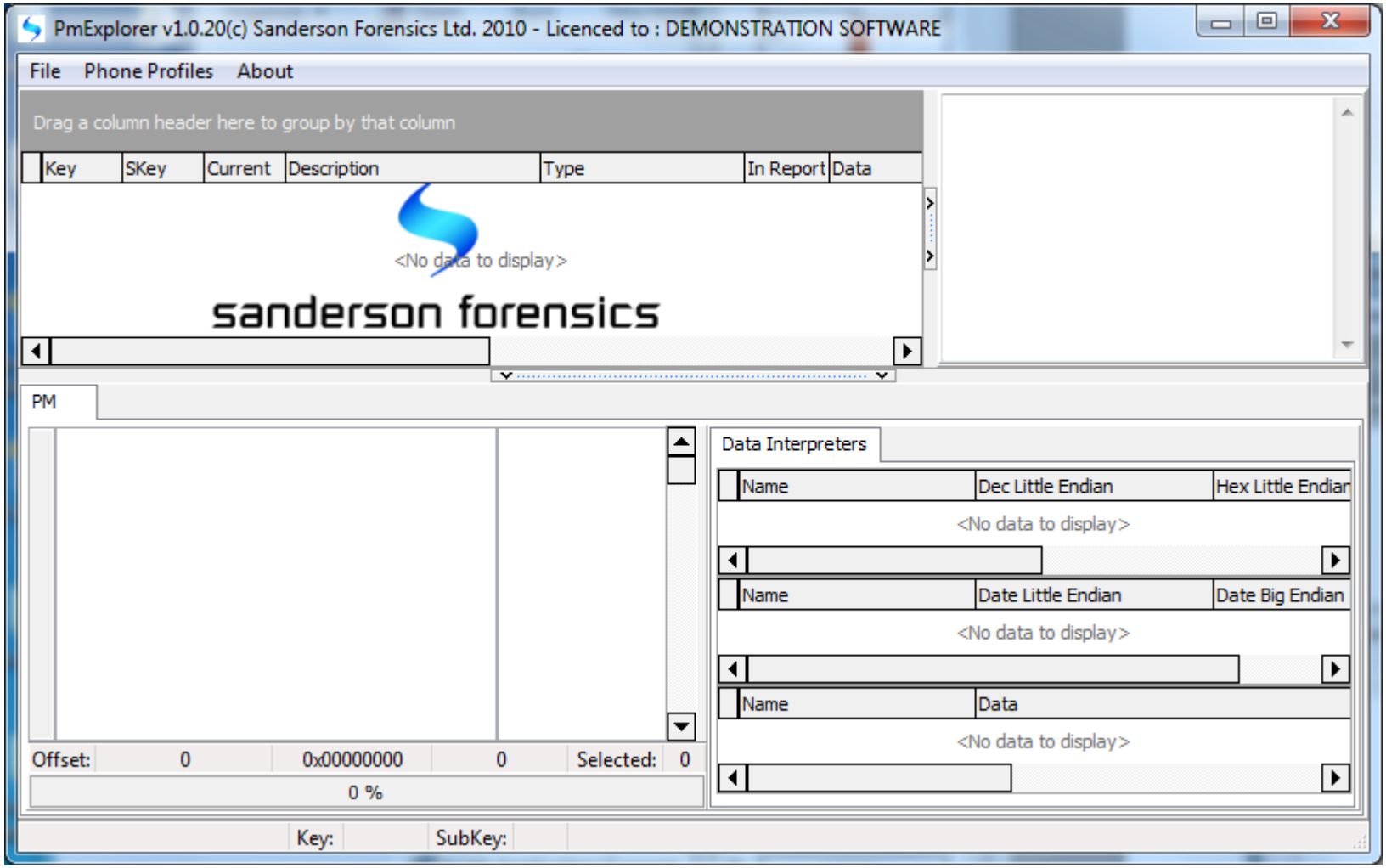
Degrees/Minutes/Seconds
May need conversion

N35 deg 36 '
E139 deg 41'



PmExplorer

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

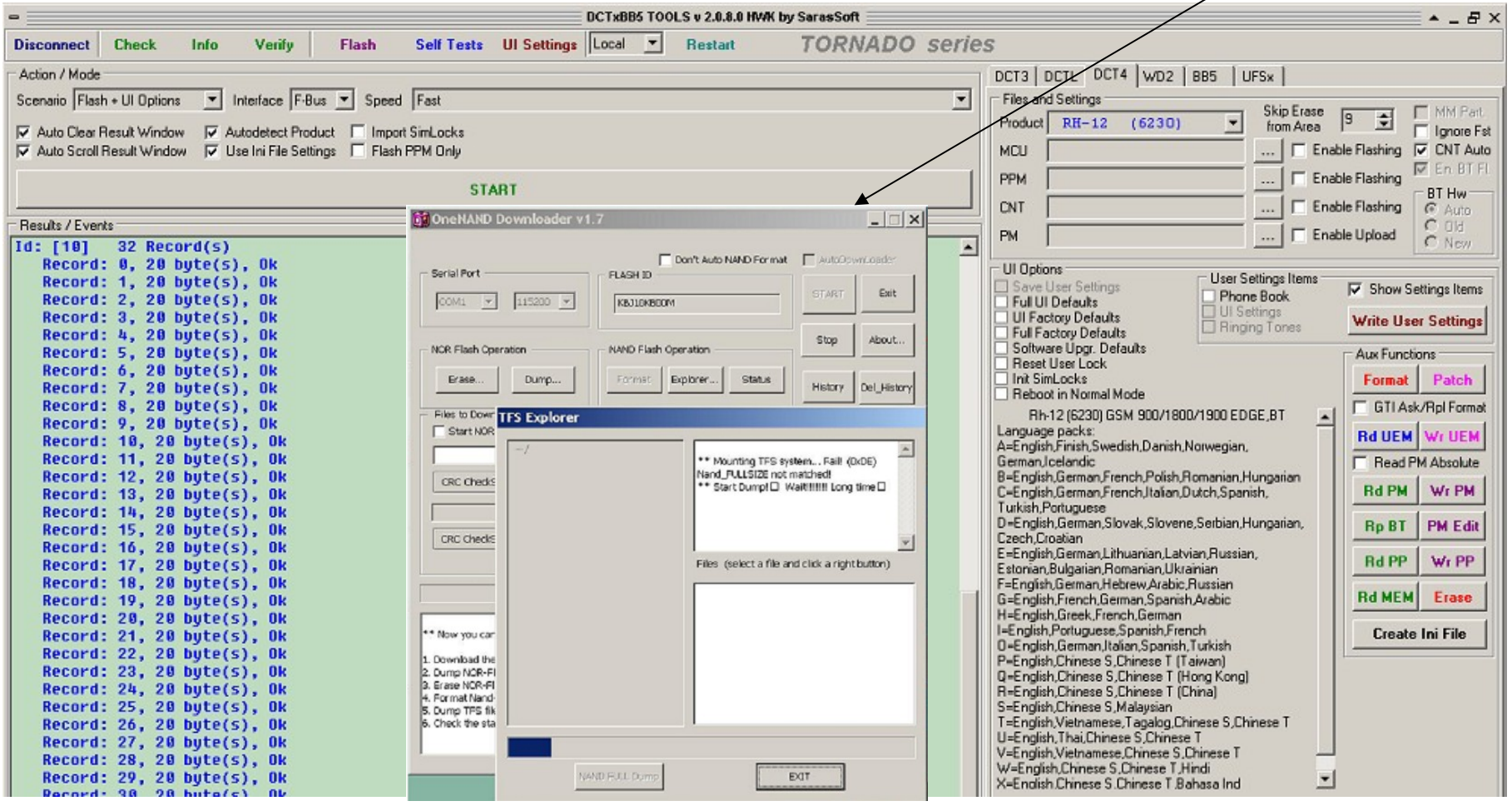


Nokia
PM tables/records

Phone flashers 1

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

Samsung
OneNAND
Downloader

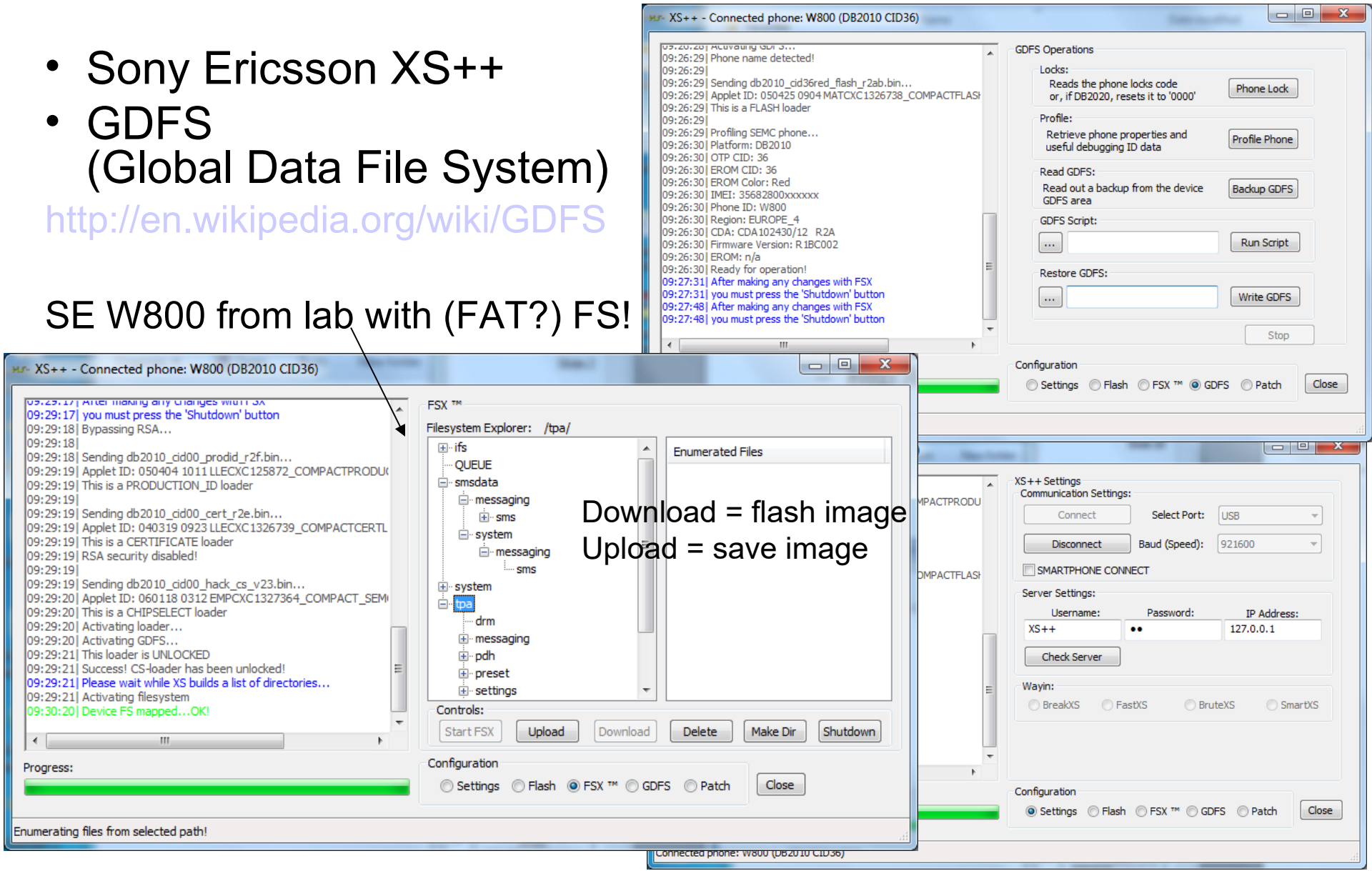


Phone flashers 2

- 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