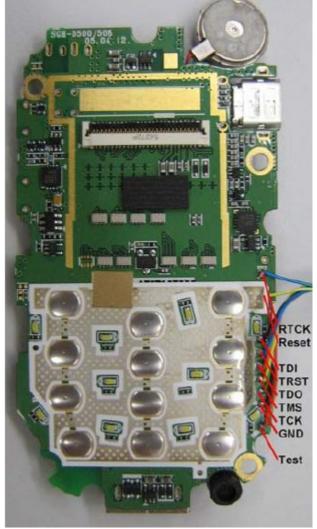


Mobile memory dumps, MSAB and MPE+ Data collection Information recovery Analysis and interpretation of results

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

🕮 X-Ways Fo	rensi	cs -	[16	C00	00-1	17FI	FFFI	FP.b	in]											14	.5		
🔒 Eile Edit 🖻	earch	Pos	sition	⊻ie	W]	Lools	Sp	ecijalis	t Op	tions	<u>W</u>	ndow	/ H	elp								-	8
0 16 1 8	a"	凶	1	5				01-3 10	44	HEX	2,5	HEX	44	1	→	Ð	¢-	⇒	1	2	-	500	inti y
16C0000-17FFFF	FP.bir																						
Position Manager	(Gene	ral)																				1	3 iter
Offset A	Annol	ation	*																				
91E32	Recor	d sta	te (A	4=his	toric)																		
91E33	Recor	d typ	e (30	=Mis	sed re	eceiv	ed ca	al Red	cord)														
91E34	Count	er																					
91E36	Sync	patter	m																				
91E3A	Lengt	h of u	iser d	lata																			
91E3C					1																		
91E3E	Numb	er of	struc	tures	in rec	broc																	
91E3F	Alway	s 0																					
91E47	Phone	num	iber ‡	‡ digi	s																		
91E48	Phone	num	iber (+316	1435	5232)																
91E4F	Name	leng	th																				
91E52	Name	(RAN	DY	GSM)																		
91E68	Times	tamp	(09-1	0-20	04 19	25:4	13)																
<									_														6
Offset	0	1	2	3	4	5	6	7	8	9	A	в	С	D	Е	F							~
00091E00	00	0A	0B	01	00	00	00	00	0A	A6	14	65	67	78	00	14				1	eg	jх	
00091E10	07	02	00	42	00	49	00	41	00	4E	00	43	00	41	00	20		_	_	A N	С	A	
00091E20	00	47	00	53	00	4D	00	80	13	03	07	D4	0A	09	13	12	G	s	М		Ô		
00091E30	29	01	A4	3C	00	01	55	FF	FF	FF	00	32	112	70	03	00		¤<	U	yyy	2	P.	
00091E40	0B	0B	01	00	0A	00	00	0C	F3	16	14	35	52	32	00	12				Ó	_5F	_	
00091E50	07	02	C.C.		_		00	_	_	44	00		00		00			_	A	ND		G	
	111	53	0.0	4D	-	08	13	03	07	D4	0 V	09	13	19	2B	01	S	-		Ô		+	3
00091E60	h-m-m													00	0B	0B	¤:	U	Jvv	ÿ 2	•		
00091E70	À4	3B	00	02			FF	FF	00	32	1E	AE	03										
00091E70 00091E80	À4 01	00	00	00	00	0C	F3	16	14	35	52	32	00	12	07	02			ć		R2		
00091E70 00091E80 00091E90	À4 01 00	00	00	00	00	0C 4E	F3 00	16 44	14 00	35 59	52 00	32 20	00	12 47	07 00	02 53	R	A		DY		GS	
00091E70 00091E80 00091E90 00091EA0	À4 01 00 00	00 52 4D	00 00 00	00 41 08	00 00 13	0C 4E 03	F3 00 07	16 44 D4	14 00 0A	35 59 09	52 00 13	32 20 1A	00 00 16	12 47 01	07 00 À4	02 53 42	RM	A	N	DY		G S ¤B	
00091E70 00091E80 00091E90 00091EA0 00091EB0	À4 01 00 00 00	00 52 4D 01	00 00 00 55	00 41 08 FF	00 00 13 FF	0C 4E 03 FF	F3 00 07 00	16 44 D4 28	14 00 0A 1E	35 59 09 E2	52 00 13 03	32 20 1A 01	00 00 16 02	12 47 01 01	07 00 À4 01	02 53 42 02	RM	A	N N	D 7 0 (â		¤Β	
00091E70 00091E80 00091E90 00091EA0 00091EB0 00091EC0	A4 01 00 00 00 04	00 52 4D 01 FF	00 00 00 55 05	00 41 08 FF FF	00 00 13 FF 06	0C 4E 03 FF FF	F3 00 07 00 07	16 44 D4 28 FF	14 00 0A 1E 08	35 59 09 E2 FF	52 00 13 03 09	32 20 1A 01 FF	00 00 16 02 0A	12 47 01 01 FF	07 00 À4 01 0B	02 53 42 02 FF	R M ÿ	A Uÿÿ ÿ	N Ŋ ÿ	D Y 0 (â ÿ ÿ	ÿ	¤B ÿÿ	
00091E70 00091E80 00091E90 00091EA0 00091EB0 00091EC0 00091ED0	A4 01 00 00 00 04 0C	00 52 4D 01 FF FF	00 00 00 55 05 0D	00 41 08 FF FF FF	00 00 13 FF 06 0E	0C 4E 03 FF FF FF	F3 00 07 00 07 07 0F	16 44 D4 28 FF FF	14 00 0A 1E 08 10	35 59 09 E2 FF FF	52 00 13 03 09 11	32 20 1A 01 FF FF	00 00 16 02 0A 12	12 47 01 01 FF FF	07 00 À4 01 0B 13	02 53 42 02 FF FF	R M ÿ	A Uÿş ÿ ÿ	N ÿ ÿ	D Y 0 (â ÿ ÿ ÿ ÿ	ÿ	¤B ÿÿ ÿÿ	
00091E70 00091E80 00091E90 00091E80 00091EB0 00091EC0 00091ED0 00091EE0	A4 01 00 00 00 04 0C 14	00 52 4D 01 FF FF	00 00 55 05 0D Å4	00 41 08 FF FF FF 42	00 00 13 FF 06 0E 00	0C 4E 03 FF FF FF 10	F3 00 07 00 07 07 0F 55	16 44 D4 28 FF FF	14 00 0A 1E 08 10 FF	35 59 09 E2 FF FF FF	52 00 13 03 09 11 00	32 20 1A 01 FF FF 04	00 00 16 02 0A 12 1E	12 47 01 01 FF FF F2	07 00 A4 01 0B 13 FF	02 53 42 02 FF FF FF	R M ÿ ÿ	A Uÿÿ ÿ ÿ	N ÿ ÿ	D Y O (â ÿ ÿ ÿ ÿ	ÿ	¤B ÿÿ	
00091E70 00091E80 00091E90 00091EA0 00091EB0 00091EC0 00091ED0	A4 01 00 00 00 04 0C 14 00	00 52 4D 01 FF FF	00 00 55 05 0D Å4	00 41 08 FF FF FF 42	00 00 13 FF 06 0E 00 00	0C 4E 03 FF FF FF 10	F3 00 07 00 07 0F 55 55	16 44 D4 28 FF FF	14 00 0A 1E 08 10 FF	35 59 09 E2 FF FF	52 00 13 03 09 11	32 20 1A 01 FF FF 04 04	00 00 16 02 0A 12 1E	12 47 01 01 FF FF	07 00 A4 01 0B 13 FF	02 53 42 02 FF FF FF 00	R M ÿ ÿ	A Uÿÿ ÿ ¤B ¤i	N ÿ ÿ U U	D Y 0 (â ÿ ÿ ÿ ÿ	ÿÿ	¤B ÿÿ ÿÿ	3

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

Edit Jump Search View Options Windows Help DA View A 때 Hex View A 한 Exports D을 Imports N Names 한 Functions	Po	Course 1		R	Charles		Cost.				0.001	10077	1						
					5000	tures	04	xrers	10.54	oguu	.001	13377		_	_	_	_	_	
A View-A	×																		
seg800:000DBFD2 seg808:000DBFD3				00BFA0 00BFB0		2C 13	81 84				03 18		D6 0			31 88	0A 13	81 85	81
* seg000:000DBFD3 RecordHeader <0	F			OBFCO		02	19	14 :	39	31	81	88	88 1	3 80	5 87	Dő	82	19	-
seg000:000DBFD3 <record></record>		seq88	8:88	BOBFDB	36	11	81	F4 :	3B		84 !		FF F	F FI	: 00	48	03	2A	8
seg000:000DBFD3 <type>Dailed call</type>	11			ODBFEO		0A	08	01	-		00		OA A	1 85	5 9A	24	25	00	_
* seg000:000DBFDF db 6				OBFFO		82	87	D6			89		28 0	1 8	0 08	13	63	07	D
* seg000:000DBFE0 db 0	11			0000000		1B	08				00			4 07		02		08	_
* seg000:000DBFE1 db 0Ah				8DC 818				68					02 1						-
* seg000:000DBFE2 db 0Bh		seg00	0:00	0DC 02 0	13	86	07	D6	82	1B	08	30	13 0	1 F	4 3B	00	11	55	F
* seg000:000DBFE3 db 1	11	<											Director I		C scri	-			8
* seg000:000DBFE4 db 0		OCCORFE	-					~					Recto	11.10	L SUI	pts	_	_	
* seg000:000DBFE5 db 1	111	UUUUBHE	:5	000DBFE5	: segu	00:00	UUBH	15	_	_	_	_							
seg000:000DBFE6		& Str	uctur	ine .															
* seg000:000DBFE6 PhoneNumber <0>		Di Sili	uctur	6.9		_	_	_	-	-	_		D.	deren 1	tionEx				
seg000:000DBFE6 <nunber></nunber>			商超	XI	4 11								-						
seg000:000DBFE8		A		Record		_					1 20	of=1	01	nforma	NionEx	dract			
* seg000:000DBFE8 PhoneNunber <0A		00000			неац	er		in ?	ς,	()	126	011							
seg000:000D8FE8 <nunber>0105902425</nunber>				counte				lu ?					D s	in sets	reDec	odeD	140		
* seg000:000DBFEA db 0A5h ; Ñ		00000			r			Id ?											
* seg888:88800BFEB db 9Ah ; Ü				length				IU ?					0 5	tructu	reDec	odeD	ct4		
* seg000:000DBFEC db 24h ; \$				nextPt				lu ?											
* seg888:8880BFED db 25h ; %				Record									Do	hachi	reSea	chDe	-14		
* seg000:000DBFEE db 0		00000		necoro	neau	er.		ends					-						
seg000:000DBFEF		00000											O S	tructu	reSea	rchDo	:14		
* seg000:000DBFEF DateStruct <813		00000		,															
seg000:0000BFEF <date>27-2-2006 9:05:43</date>				CARDID				*****			1.70	of=	ms	Inachu	reDefi	nition	Dct4		
* seg888:8880BFF9 db 1										(3	126	01-1	1 -						
* seo888:8800BFFA db 8		00000	000	CARDID				1b ?					0 9	buctu	reDefi	nition	Dct4		

MSAB Forensic Office



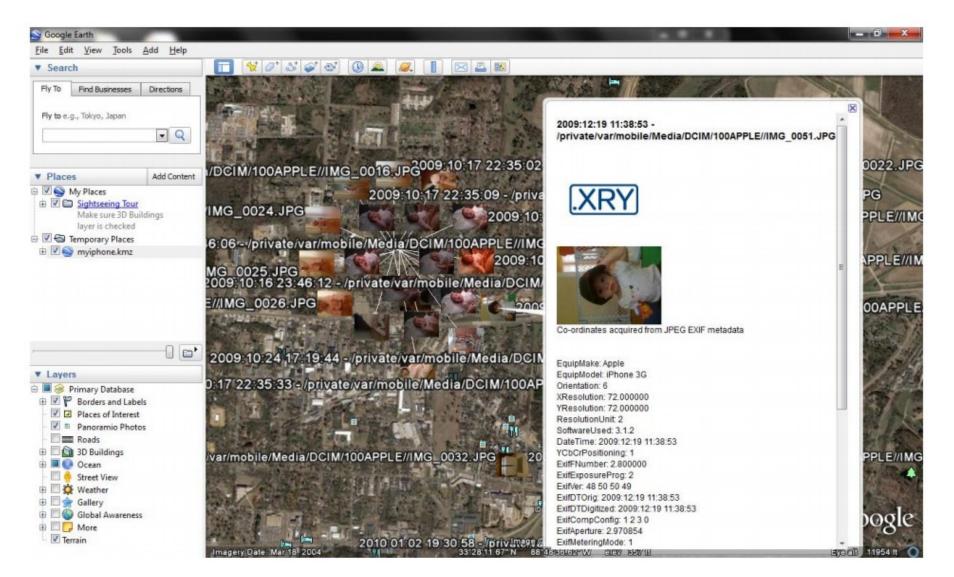


- We can extract the data through the phone by talking to the operating system, using a set of various software tools and techniques.
- It is the fastest (cheapest) way to examine a phone.
- It is the best way for 80% of all examinations
- It will not reveal deleted data.
- All visible data may not be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

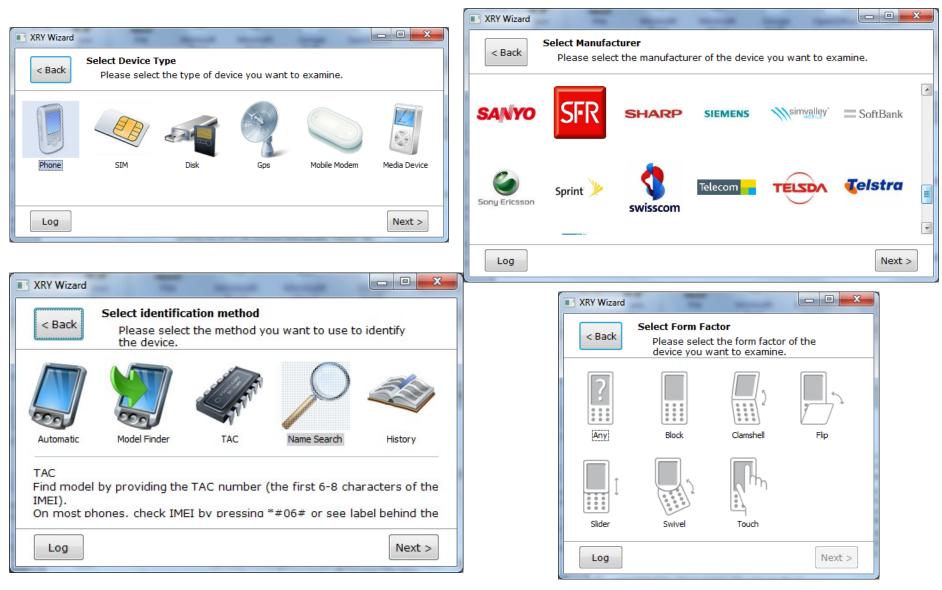
MSAB XRY

· · · · · · · · · · · · · · · · · · ·				XRY - [SonyEricsson_K800i.xry]	_	_	_	_ 0	X
File Edit	View Wind	ows Tools						Options 🕆 🕕 About	-8>
Extract Data Extract Data	· ·	ave Save As *	File	Microsoft Microsoft Google OpenO Excel Word Earth Export	Office XML	Print •	Ma	evice Help anual Help	
Media Window 4 ×	Summary	SMS SMS message	ges sent or rec	ceived from the device (13 items)					
		Number	Name	Message	Time	Status	Storage 1	Index Service Center	
	Case Data	0632082356		Goedenmorgen schoonheid		Sent	Device	1 +31653131313	
	i	□ 1300		KPN helpt u graag met het instellen van internet op uw mobiel. U ontvangt hiervoorzometeen instellingen. Accepteer deze als uw toestel er om vraagt. Afz KPN	2010-03-29 13:45:16 (+02:0	Read	Device	2 +31653131316	
	General Information	0620125081		Is everything OK, it looked like you were going somewhere, because of your tickets. Ihope you are coming out of it? Let me know how you are. Maybe i can also help abit with everything. Best regards. Stephan.		Sent	Device	3,4 +31653131313	E
	Contacts	□ 1300		Uw toestel werkt nu optimaal. Wiltu 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	
	Calls	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	ł	Sent	Device	7,8 +31653131313	
	SMS	0632082356		Vergeet je niet vandaag naar de tandarts te gaan?		Sent	Device	9 +31653131313	
	Pictures	+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 +31654088100	8
💽 🔹 🍋 🛶	×	0615646978		Everything arranged!		Sent	Device	11 +31653131313	Ŧ
Ready								CAP NUM	SCRL .

Geocoded Data



MSAB XRY Wizard 1



MSAB XRY 2



XRY Wizard and the local distances of the local distance 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 Not Supported Not Supported Calls SMS Not Supported Files Not Supported × MMS Not Supported E-mail Not Supported Calendar × Not Supported

Not Supported

Not Supported

×

X

Info

Tasks

Notes

Decoding not supported.

Log

MSAB XRY (3 Select File Please select file to save the extraction to.
XRY Wizard < Back	Save in: C:\hjo\MSAB\dump\ Contents: Sony Ericsson C702_nodecode.xry Sony Ericsson K800i_nodecode.xry
 Ensure that the phone battery is fully charged. Remove the battery, SIM and memory cards from the phone. Insert the battery back to the phone. Insert "Ericsson Cable 3" to the XRY device USB port. Click "Next" to continue the phone dumping. 	Sony Ericsson K850i_nodecode.xry
Log Next	
< Back Process Options Create and select the options you want to apply during this process.	File name: Sony Ericsson C702.xry Password: Use Encryption Verify:
	Log Next > Image: XRY Wizard Image: XRY Wizard
Full read (including Everything except multimedia, documents and other files	Processing XRY is querying the device for information.
Dump Your profiles are locked. Press the lock icon to create, edit or delete a profile.	 Press "C" button on the phone and keeping it pressed attach "Ericsson Cable 3" to the phone. Wait for the driver to be installed, if needed, and for the dumping to continue keeping the button pressed. Release the button after the dumping process continues.
Log Next >	Log Next >

l

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 with-

Micro Systemation AB Visiting address: Hornsbruksgatan 28

out 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 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

.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 rewriteable, which means that you don't need one for every examination

All Contract of the Contract o

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,
- Individual account identification
- Max 12 digits plus
- Parity check digit

(Total all 6 digits including the MII)

<u>F</u> ile		2FE2	5	Serial	Numbe	r			•	🛞 🖗	•	6			
File Infi	ō	Re	Struct File ty Sta	ure: ype: itus: size: size:		FE2				Acce		tights Read Update Increment Invalidate tehabilitate	: F : 0 : F	1: 2: 3-E:	Always PIN1 PIN2 Locked Never
98 6	4	10	10	80	70	90	10	58	67						

MSAB XRY SIM Id Cloner

XRY SIM Id Cloner			Identification data: ICCID: 89460101080709012108
XRY Sim ID-	Welcome to the	SIM Id Cloner	INSI: 24001000709012108
CLONER	This wizard will help you setup the data you input.	identity of a SIM card based on the	O2 IMEI:
	Please select if you have an existing enter the data manually.	ng SIM card to clone or if you wish to	
		XRY SIM Id Cloner	Show Log
and the second s	Clone an existing SIM card Image: Manually enter data	Input Source Data Input the data you wish to be written to the S	M card.
			< Back Next > Cancel
	Your license is valid until 2011-1	Input the data you want to be written to the SIM o satisfied with one of the ICC or IMSI numbers, whi	ard. Different phones react differently. Some will be e others will require both.
		ICCI	(up to 20 digits)
MICRO SYSTEMATION		IMSI:	(up to 15 digits)
	<	LP: (None)	(optional)
		Enter advanced settings	
			< Back Next > Cancel

XRY SIM Id Cloner

Insert Destination Card

Insert the SIM card that will be configured.

Please insert the SIM card that will be configured to assume the cloned identity.

This should be a SIM card supplied by Micro Systemation.





celebrite 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

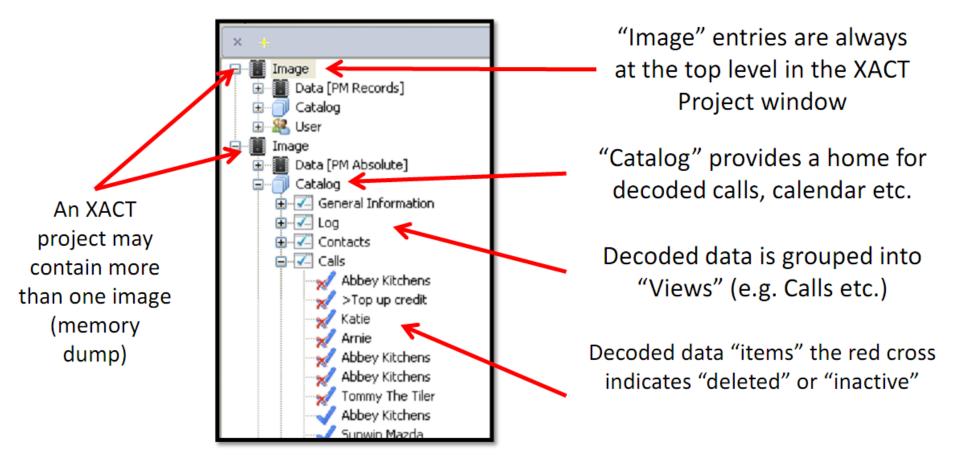


Apple_iPhone 2G_3G_3GS (iPhone 2G/3G/3GS)	Detected manufacturer: N/A Detected model: N/A	365							
	Selected manufacturer: Apple Selected model: iPhone 2G/3G/3GS Detected manufacturer: N/A								
	Content:								
i⊞ <mark>)</mark> Audio (1967) ⊞) ∏ Text (15)		Items	Deleted items	Total					
Beport	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 R	eport						
A Cert	.7 .7 .No. 110	:06:42 PM							

MSAB XACT 1

Samsung SGH-E360.xry - XACT - Data [OneNAND]	
<u>File Edit View Node Tools Window Help</u>	
♥ ☞ ₽ % ₽ 8 ₽ ?	
Project # ×	Data [OneNAND]
x 🕱	0000 0000 64 00 00 00 0F 00 00 01 00 00 058 53 52 31 d 🔅
Image Data [NOR:1000000-11FFFFFF] Catalog Image	0000 0000 00 00 00 00 00 00 00 00 00 00 00 00 00
Data [OneNAND] Translation Layer Partition Partition Partition Boot Record	000 Identify Device 29993 000 XACT is identifying the device. 29993 000 29993 29993 000 29993 29993
FAT FAT1 KFAT0	0000 000 000 Filter:
	Nokia 6230 Nokia 6230i Nokia 6230i VYYYY Occ Nokia 6230i Nokia 6585 VYYYY
JAVA JAVA JAVA DEFAULT JAVA MINIMEDIA	OOC Nokia 6610i OOC Nokia 7270 OOC Nokia 7360
e-Construction of the second s	000 Samsung SGH-D500 729999
Photo-0001.jpg Photo-0002.jpg Photo-0003.jpg	OOC OOC
 ⊕-☐ my photos ⊕-☐ favorite images ⊕-☐ VIDEOS 	0000 0220 FF
MUSIC SOUNDS	0000 0250 FF





XACT Project Structure



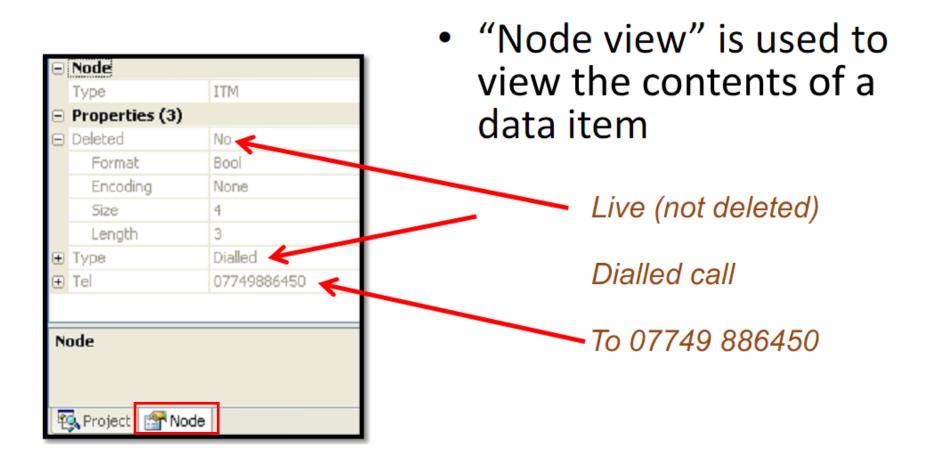
××
Image Data [NOR:10000000-11FFFFFF] Create Create Delete Decode View Export Image Data [OneNAND] Translation Layer Partition

- 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:	
File Edit View Tools Window Help	_ & ×
i≓ = X = a ? , i ¥	
Project	0000 53 A5 C4 F8 EB 20 DC E4 B9 5C E3 D2 39 03 41 CA C3 9F S¥Äøë Üä¹∖ãÒ90 AÊÃ 0012 18 6A 00 00 00 05 51 E 00 01 00 1E 00 00 55 55 1E 00 0 j U 0 UU
x *	0024 01 00 1E 00 00 55 55 1E 00 01 00 1E 00 00 55 55 1E 00 0 UU 0 UU 0036 01 00 1E 00 00 55 55 1E 00 01 00 1E 00 00 55 55 1E 00 0 UU 0 UU
Image NOR:44000000-45FFFFF GDFS Data GDFS O-49 O-49	0048 01 00 1E 00 00 55 00 FF 00 00 00 00 00 00 00 00 00 00 00
17 View	Node Data
I9 Export	Subject
20	Data
Review Re	Deleted
Ready	Index 0 CAP NUM SCRL .::

Viewing Item Properties **XRY**



XACT Hex Viewer



00 000 000	10 00 38 9C 00 00 00 B1 00 0C 02 01 FF 00 08 20 8 5 ± 11 ¥
00 000 016	01 DC 02 FF FF 00 08 20 10 00 00 95 10 00 00 00 🛛 🚺 💥 🚺 🚺
00 000 032	10 00 EF D7 10 08 00 00 10 00 E8 00 10 00 F0 00 11 F8 08 00 28 63 29 20 43 F 70 79 72 69 67 68 74 20 4D 6F 74 6F 72 6F 6C 61 20 32 30 30 34 2C t Motoroia 2004,
	11 F8 08 00 28 63 29 2 43 F 70 79 72 69 67 68 6 6 (c) 🕻 🔂 pyrigh
00 000 064	74 20 4D 6F 74 6F 72 6F 6C 61 20 32 30 30 34 2C t Motoroia 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 . yyyyyyy
00 000 112	FF

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

Sony Ericsson K800i_nodecode.xry - XACT - [Image/Son	yEricsson_K800i_NAND_NAND51	D512 Find	×
File Edit View Tools Window Help Image: Second		T GAL	Find Next
Project Image SonyEricsson_K800i_NAND_NAND512R3A.bin Catalog Image Image SonyEricsson_K800i_Norflash_PF38F5060M0Y0BE	$\begin{array}{cccc} 0000 & 0000 & FF \ FF \ FF \ FF \\ 0000 & 000f & FF \ FF \ FF \ FF \\ 0000 & 001e & FF \ F$	FFF Data Dictionary Search FFF File Signature Search FFF Findstrings FFF Number Search FFF PDU Finder FFF Regex search FFF Regex search FFF Timestamp Search FFF FFF FFF GSM (7 bit packed)	Close
Searching	0000 0003 FF 0000 0000 0000 FF FF FF FF 0000 0000 0000 0000 FF FF FF FF 0000 0000 0000 0000 0100 FF FF FF FF 0000 0100 0100 FF FF FF FF FF 0000 0100 0100 0100 0100 FF FF <td< th=""><th>F FF FF FF FF Unicode Big Endian (Motorola) FFF FF FF FF Unicode Little Endian (PC/Intel) FFF FF FF FF ANSI and Unicode FFF FF FF FF ANSI and Unicode No Case FFF FF FF FF UTF8 UTF7 FFF FF FF FF FF UTF7 FFF FF FF FF GSM (7 bit packed) FFF FF FF FF FF GSM No Case (7 bit packed) FFF FF FF FF FF GSM (8 bit unpacked) FFF FF FF FF FF FF GSM (8 bit unpacked) FFF FF FF FF FF FF MAC</th><th></th></td<>	F FF FF FF FF Unicode Big Endian (Motorola) FFF FF FF FF Unicode Little Endian (PC/Intel) FFF FF FF FF ANSI and Unicode FFF FF FF FF ANSI and Unicode No Case FFF FF FF FF UTF8 UTF7 FFF FF FF FF FF UTF7 FFF FF FF FF GSM (7 bit packed) FFF FF FF FF FF GSM No Case (7 bit packed) FFF FF FF FF FF GSM (8 bit unpacked) FFF FF FF FF FF FF GSM (8 bit unpacked) FFF FF FF FF FF FF MAC	
 III ► III ► III ► Project III Node Q Value Q String Ready 	0000 0159 FF FF FF F 0000 0168 FF FF FF F 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 01c2 FF FF FF FF 0000 01c0 FF FF FF FF	F FF FF FF FF IBA/IA5 (7 bit) F FF FF FF FF IBA/IA5 (7 bit) F FF FF FF FF 8859-1 (West European/Latin 1) F FF FF FF FF 8859-2 (Central/East Europe/Latin 2) F FF FF FF FF 8859-3 (South European/Latin 3) F FF FF FF FF 8859-4 North European/Baltic) F FF FF FF FF 8859-5 Cyrillic) F FF FF FF FF FF 8859-6 Arabic) F FF FF FF FF FF 8859-7 Greek) F FF FF FF FF FF 8859-8 Hebrew)	

MSAB XACT 4

SMS 7-bit Encoding

String 00e7 626a 00 00 00 00 00 00 00 00 00 00 00 00 00	Sony Ericsson K800i_nodecode.xry - XACT - [Image/SonyEric	sson_K800i_NAND_NAND512R3A.bin]
Ode 7 6279 Ode 7 6279 Ode 00 00 00 00 00 00 00 00 00 00 00 00 00		SMS - text end start
	Encoding: 7Bit Codepage: Ansi Goedenmorgen schoonheid Find Find <th>$\begin{array}{cccccccccccccccccccccccccccccccccccc$</th>	$\begin{array}{cccccccccccccccccccccccccccccccccccc$

🔊 S	ony Ericsson K800i_nodecode.xry - XACT		- 1 -			
File	View Tools Help	_				
1	New	+ +	⊉ ⊞ △ →	•	→ [0000 1001 -	
	Open 🕨					_
	Add By File Import					
	Script >	F	Run	+	[Demo] Decode Samsung SMS	
	Close Project	E	Edit	×	Carving SMS from image	
	Save Project	1	Vew		Carving SMS from image test	
	Save Project As	E	Browse Scripts		Decode Sony Ericsson J110	
	1 Sony Ericsson K800i_nodecode.xry	0	Get More Scripts		Iterate all SMS and print the SHA1 hash of the text contents of the SMS	
	2 Sony Ericsson C702_nodecode.xry				Search images for IMEI	
	3 C:\hjo\MSAB\Testproject3.xry				Search images for IMSI	
	4 Sony Ericsson W800i_nodecode.xry			03	XRY Wizard	
	5 Sony Ericsson K850i_nodecode.xry				Select Scripts	
	6 C:\tmp\smssms.txt			L	< Back Please select optional scripts to run.	
	7 Sony Ericsson C702xry					
	8 Sony Ericsson C702_noencode.xry			L	Available scripts: Queued scripts (executed in order list	ted):
	9 Sony Ericsson W800i_noencode.xry			Ŀ	[Demo] Decode Samsung SMS Carving SMS from image	Up
	10 Sony Ericsson K850i_noencode.xry			L	Carving SMS from image test Decode Sony Ericsson J110	
	Exit	J		L	Iterate all SMS and print the SHA1 Search images for IMEI	Davia
		_			Search images for IMSI <<< Dequeue	Down
	III Project Mode Q Value Q String			L		
Read						
	,	-			Decede images Wizerd (VDV starts)	
	MCAR X	Λ	$\frown T$		Decode images Wizard (XRY starts)	
	INISAD A	A				
		-				
	Dhutan a		into		Remember queued scripts for this	model
	Phyton se		IDIS			
		-			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

KRY Wizard		XACT Image Decoder	×
Welcome Welcome	e to the XRY Wizard	XACT Welcome to the XACT Image Decode	er Wizard
XRY	This wizard will help you extract data from a mobile device.	DECODER WIZARD This wizard will help you decode the contents of an im	iage.
	License key serial number:		
	XRY Logical: There is no valid license for this module	License key serial number:	
	XRY Physical: There is no valid license for this module	There is no valid license for this module	
l have MSAE	e compiled my questions 3 regarding XACT, XRY a	and an <mark>swers from</mark> and dumping	
See the	e questions_msab*.pdf files at	[server]\embedded_forensics\MSAB	.com
Log		< Back	Next > Cancel

Extracting dump data

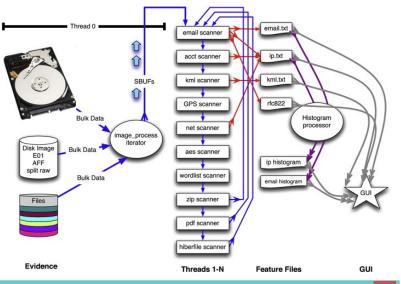
• Non file based

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

- 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



Phone Image Carver v1.0.2(33)		<u>\$</u>	Bulk E	ktractor Viewer – 🗆 🗙
Those mage currer readings		File Edit View Tools Help		
Eile Recover Help		× 🔒 🎭 📲 🖤	÷	
		💥 Highlight:	✓ Match case	
🖌 🖳 Start Recovery 📃 Save Fi	iles 👻 🎹 Options 🌑 Update 🕜 Help	Reports	Feature Filter Match case	Navigation
		Acquisition testing		RAM-Dump.Ex01, 1232648516, e4 36 15 d8 76 af 12 c9 79 1d b1 bf 35 ca f5 89
		ccn.txt	Feature File aes_keys.txt	Feature File aes keys.txt
Files Found: 16	Scanning block 421,745 of 4,849,664 for lost	ccn_histogram.txt	feature_recorder::get_name(# UTF-8 Byte Order Mat ^ 666289600 fd fl 08 d4 3b fD 1a 10 69 13 94 b4 f8 78	Feature Path 1232648516 Feature e4 36 15 d8 76 af 12 c9 79 1d b1 bf 35 ca f5 89
		 domain.txt domain histogram.txt 	955126316 94 ef 93 4a 3b 01 c7 ab 82 de 40 ab a9 d9	Image
		elf.txt	955126892 1c 9a ab 75 02 55 dc d3 7b c8 25 47 ae 6c	12326465281p.,.M
	Preview Event Log	email.txt email histogram.txt	1232648516 e4 36 15 d8 76 af 12 c9 79 1d b1 bf 35 ca 1232649172 e3 da ad 09 0e bd aa 4e 17 07 64 91 9a c6	1232646592
📤 File Type 🗿 Date 🔺 🔺	EVENLLOG	• ether.txt	1218044864 40 3c 3a f5 99 f5 71 d2 5e ca a4 44 cb af c	1232646656 (C6
	Name 9	<pre>ether_histogram.txt exif.txt</pre>	1378644524 94 ef 93 4a 3b 01 c7 ab 82 de 40 ab a9 d9	1232646784E1/.S0.1,4.sL!.Va)'"3wq.
🖃 🔛 🔲 Filetype List (5)		exir.txt	1378645100 1c 9a ab 75 02 55 dc d3 7b c8 25 47 ae 6c 1650164908 30 99 e3 a3 81 9d ef d7 49 64 3d 18 e7 5e	1232646848 ^]}v?qCD.GB r <vcp*f6.q.w< td=""></vcp*f6.q.w<>
	LostFile_JPG_4.jpg 39	• ip.txt	1650167212 3b 3d 03 fD 32 97 ad 06 56 41 30 62 bc 0t	1232646912 .v.h <v<wbwzvwyx?.u.! 1232646976 .;)</v<wbwzvwyx?.u.!
- 🗌 🔬 Icon (2)	🔄 👩 LostFile_JPG_136.jpg 361	···· ip_histogram.txt ison.txt	1800716844 da f5 ee 9f 4e 6f 27 5a aa 26 e6 9e c6 aa 1	1232647040,
	LostFile_JPG_384.jpg 361	 Logical.Lx01 	1974703212 28 b9 07 42 31 c5 06 3c 01 25 f9 5c 84 78 1974704364 8c 4c 67 db 29 8f 45 8f b8 3c 1e 5d e2 0e	1232647104
🗌 🁥 JPG (8)		packets.pcap	2062420268 da f5 ee 9f 4e 6f 27 5a aa 26 e6 9e c6 aa 1	1232647168 q.=k. 603)vois>6I.U.b. V.Rudga 1232647232 WPd9.@4.dp.h.vb.e7).d9<(%.G.Z.@#("V0:pK
🖸 Mov (1)	LostFile_JPG_515.jpg 39	Ram-Dump.e01.ad1	2346410540 da f5 ee 9f 4e 6f 27 5a aa 26 e6 9e c6 aa 1	123264/232
	LostFile_JPG_586.jpg 6	Ram-Dump.e01.ad2	2363380672 40 3c 3a f5 99 f5 71 d2 5e ca a4 44 cb af a 2393368900 44 36 15 48 76 af 12 c0 70 14 b1 bf 35 ca	1232647360 { M\$"yg./H.r.wzd5tjb6"\$
🛄 📬 Zip (1)		RAM-Dump.Ex01 RAM-Dump.Ex02	< > >	1232647424I"G.\$rvOhaS7u.J.X+.:TMWD
	. · · · · · · · · · · · · · · · · · · ·	rfc822.txt	Referenced Feature File None	
		•••• tcp.txt	Referenced Feature None	1232647616 %EEI8.hu*.SR\$/
	Property Value ^	tcp_histogram.txt telephone.txt		1232647680r.+!CoFP?`La.'0.Q/paoLR:>(
	Type JPG	telephone_histogram.txt		1232647744
	ATARA AND	••• url.txt ••• url_facebook-address.txt		1232647860
	Filename LostFile	url_facebook-address.txt		1232647936
	Directory	• url_histogram.txt		1232648000um?*.u40V.4.2V[f.tsst.S.Ki5.A]u0S 1232648064 [pIXt[3ZA.\.CSZZNp.J.,VV.H
	Record 0	• url_searches.txt		1232640004 [pixt[52A.\
		vcard.txt		1232648192 .hwZz.{E6.7V.)}P9a.@qd.X e.,PZ.SI
	Directo 0	• windirs.txt		1232648256 4W^.uW[.#A+jM.Sk.hRb)o6ttmu.Cm}X
	Type JPEG Sta	 winpe.txt wordlist.txt 		1232648320 \.^.3H.0\$.jH.I9.&&`M.B.I].&y!.*n!iH2.@{U` 1232648384 .m.BP.(.jNJA.@.\$@l.&.w. .Fv"]U*.+
	Version JFIF:1.1			1232648448 kP"oR.gs.;K5.5J.OL5.fyj)+.)'.rhga.Nx1.^`
		Acquisition testing		1232648512 n=G.n.}.00.(.0\.*>R@G 4.W.[8.@a.'+.
Show All Show Deleted	🥜 Height 480 🗸 🖌			1232648576 .M
				<pre></pre>
File Recovery Normal Lo	ogging Showing Deleted Items Selected it			🖲 Text 🔿 Hex 🛛 🙀 🎒

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
                                              build fat fs.py
 contact = "hjo@du.se"
 version = "0.1.0"
                                              from the XACT manual
 _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

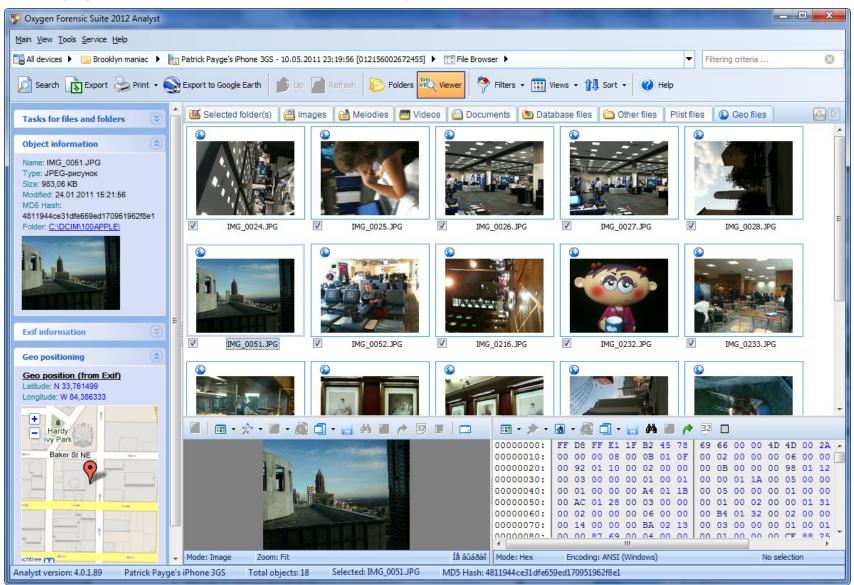
nodebrowser											
	K800i-Recover										
nodebrowser											
View											
- 🔶 31	Icon size:	Small 🔹 🔻	Show attributes								
Name			Name	Siz	ze	Accessed time	Changed time	Modified time	Module		
🔺 🥼 Sony	Ericsson_K800i_NAND_NAND512R3A.bin		def_acc.dat	691		4/4/2010 12:00:00	12:00:00 AM	4/4/2010 8:58:54	Fat File System		
	800-base		-			AM 3/16/2010		AM 3/16/2010	,		
4	fullfs		J _ELCOM~5	0		12:00:00 AM	12:00:00 AM	12:18:56 PM	Fat File System		
	J partition	=	📕 SA gmail	0		3/16/2010	12:00:00 AM	3/16/2010	Fat File System		
	800-dfrws-eval1] part_tpa/settings/ui/bgim/cache	=				12:00:00 AM 3/29/2010		12:20:02 PM 3/29/2010			
	part_tpa/settings/u/bgim/cache		i Mv	0		12:00:00 AM	12:00:00 AM	10:49:48 AM	Fat File System		
	⊿	nodebro	wser K800i-Recover								
	Fat File System										
Þ	part_ifs	nodebrows	er								
4.8	part_system	View									
4	🛛 🥼 partition		3 33 3	Terra cierca (Mardia		Channattributaa					
	🔺 🧻 part1	-	3 44 3- 🛲 🚜	Icon size: [Mediu	um 🔹	5 Show attributes					
	4 🤳 Fat File System										In the second
	a 🚚 wap	Name									
	profile										A LO DE L
		4 🌒	SonyEricsson_K800i_NAND_NAND5	12R3A.bin							Q & OT
	4 🤳 settings		🥼 k800-base	12R3A.bin							OCTOR S
	 settings messaging 		k800-base k800-restore-1	12R3A.bin							DSC0007 IPG
	 settings messaging cb 		 k800-base k800-restore-1 a part_system 	12R3A.bin							DSC00007.JPG
	 settings messaging cb 		 k800-base k800-restore-1 part_system partition 	12R3A.bin		_SC00010.JPG	_sC00009.JPG	_SC00008.JPC	GSC00007.JPG	MOV00002.3GP	DSC00007.JPG
	 settings messaging cb email 		 k800-base k800-restore-1 part_system partition partition 	12R3A.bin		_SC00010.JPG	_SC00009.JPG	_SC00008.JPC	G _SC00007.JPG	MOV0002.3GP	DSC00007.JPG
	 settings messaging cb email Mv 		 k800-base k800-restore-1 part_system partition part1 part_usb 	12R3A.bin		_SC00010.JPG	_SC00009.JPG	_SCO0008.JPC	G _SC00007.JPG	MOV00002.3GP	DSC00007.JPG
	 settings messaging cb email Mv mms 		 k800-base k800-restore-1 part_system partition partition 	12R3A.bin		_SC00010.JPG	_SC00009.JPG	_SCO0008.JPC	G _SC00007.JPG	MOV00002.3GP	DSC00007.JPG
	 settings messaging cb email Mv mms 		 k800-base k800-restore-1 part_system partition part1 part_usb partition 	12R3A.bin			A			MOV00002.3GP	DSC00007.JPG
	 settings messaging cb email Mv mms 		 k800-base k800-restore-1 part_system partition part1 part_usb partition part1 	12R3A.bin		_SC00010.JPG	_SC00009.JPG DSC00005.JPG			MOV00002.3GP	DSC00007.JPG
	 settings messaging cb email Mv mms 		 k800-base k800-restore-1 part_system partition part_usb partition partition partition partition Fat File System 	12R3A.bin			A			MOV00002.3GP	DSC00007.JPG
	 settings messaging cb email Mv mms 		 k800-base k800-restore-1 part_system partition part1 part_usb part1 Fat File System music picture other 	12R3A.bin			A			MOV00002.3GP	DSC00007.JPG
	 settings messaging cb email Mv mms 		 k800-base k800-restore-1 part_system partition part1 part_usb part1 Fat File System music picture other webpage 	12R3A.bin			A			MOV00002.3GP	DSC00007.JPG
	 settings messaging cb email Mv mms 		 k800-base k800-restore-1 part_system partition part1 part_usb part1 Fat File System music picture other webpage DCIM 			DSC00006.JPG	DSC00005.JPG	DSC00004.JPC	B DSC00003.JPG		
	 settings messaging cb email Mv mms 		 k800-base k800-restore-1 part_system partition part1 part_usb part1 Fat File System music picture other webpage DCIM 100MSDC 			DSC00006.JPG	DSC00005.JPG	DSC00004.JPC	bscoood JPG		
	 settings messaging cb email Mv mms 		 k800-base k800-restore-1 part_system partition part_usb part_usb partition part1 Fat File System music picture other webpage DCIM 100MSDC system 	TF		DSC00006.JPG	DSC00005.JPG	DSC00004.JPC	bscoood JPG		
	 settings messaging cb email Mv mms 		 k800-base k800-restore-1 part_system partition part1 part_usb part1 Fat File System music picture other webpage DCIM 100MSDC 	CF	gr	DSC00006.JPG	DSC00005.JPG	DSC00004.JPC	bscoood JPG		

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

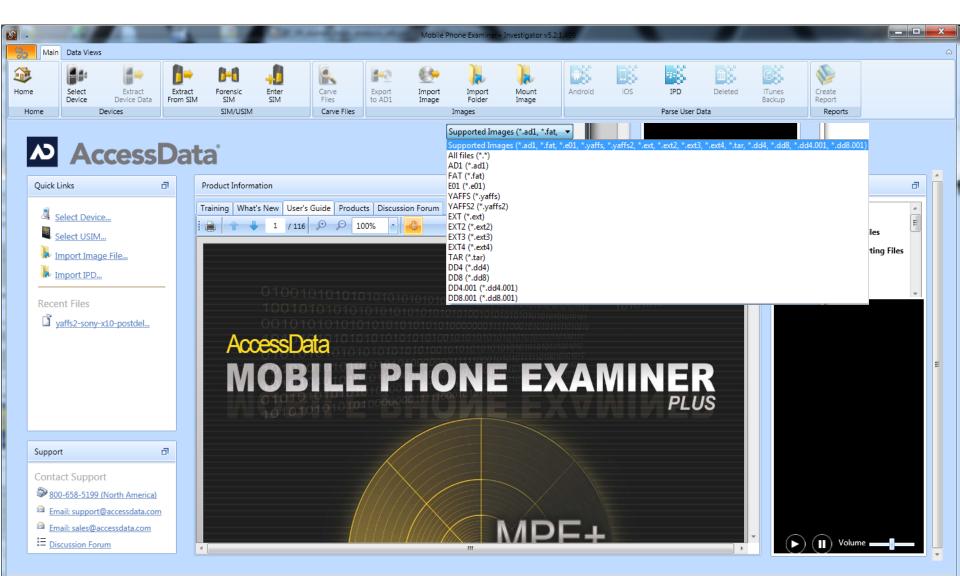
AccessData Forensic Toolkit Version: 3.2.0.32216 Database: localhost Case: iphone	
Eile Edit View Evidence Filter Tools Manage Help Image Filter: - unfiltered - Image Filter Manager Image Image	More iPhone dumps are available from [server]
Explore Overview Email Graphics Bookmarks Live Search Index Search Volatile	
Evidence Items 4 b File Content	▼ ×
Partition 1 00000410 C6 47 BF F7 C8 47 Image: Control of the state sta	0 0 02-00 00 <t< th=""></t<>
Cursor pos = 0; log sec = 0; phy sec =	- 64
[Apple] File Content Properties	Hex Interpreter
File List	
🖉 🗗 🗗 📕 🔳 🔹 🔻 🖽 👘 🗊 🛄 Normal 🔹 Disp	olay Time Zone: W. Europe Standard Time (From local machine) 👛 🔀 🗙 🔅
	ategory P-Size L-Size MD5 SHA1 SHA256 Created Accessed Modified
Partition 1 1004 iphone3g.dmg/Partition 1 P	artition 260,0 MB 260,0 MB n/a n/a
Unpartitioned Sp 1001 iphone3g.dmg/Unpartitioned Space [Apple] U	npartitioned 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]



AccessData MPE+



Time stamps and search terms

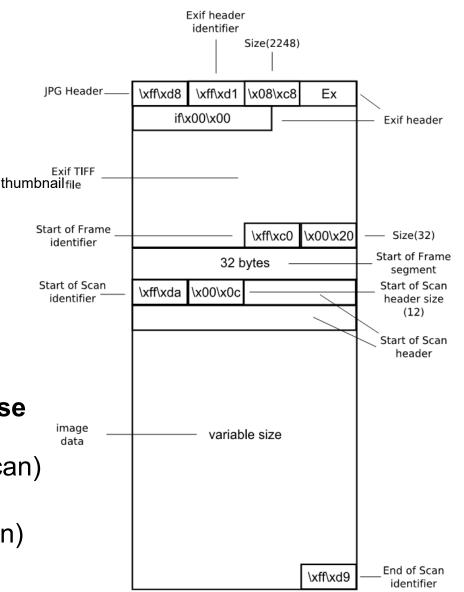
- A wide variety of storage formats are used for storing timestamp data in embedded system memories
- To illustrate the timestamp "30 April 2008 14:30:59 UTC" is encoded as follows in some formats found in different mobile phone memories:
 - 0x80400341039500 (ETSI SMS)
 - 0xB19E0CA3 (Nokia)
 - 0x07D8041E0E1E3B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



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)



🔁 damaged.jpg - Windows Photo Viewer	
File ▼ Print ▼ E-mail Burn ▼ Open ▼	0
Exif JPEG Thumbnail	
EXIF Reader	
Open image C:\Users\hjo\Desktop\damaged.jpg	
EXIF Sub IFD EXIF Interoperability IFD Maker Note IFD 1	humbnail
C:\utils\exiftool\exiftool(-k).exe	
Compression : JPEC <sld-< th=""> Thumbnail Offset : 4096 Thumbnail Length : 5130</sld-<>	
Image Width 2288 Image Height 1712	
Encoding Process : Baseline DCT. Huffman coding	
Color Components : 3	
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	
act) Airela Africa fusion - A AAFrica	
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 Digital Still Camera Forensics - SSDDFJ_V1_1_Cohen.pdf Tags Relating to GPS GPSVersionID GPSLatitudeRef GPSLatitude GPSLongitudeRef Degrees/Minutes/Seconds GPSLongitude GPSAltitude May need conversion GPSTimeStamp GPSSatellites GPSStatus GPSMeasureMode GPSDOP GPSSpeedRef GPSTrackRef GPSTrackRef N35 deg 36 ' GPSImgDirectionRef GPSImgDirectionRef E139 deg 41' GPSMapDatum GPSDestLatitudeRef GPSDestLatitude GPSDestLongitudeRef GPSDestLongitude GPSDestBearingRef GPSDestBearing GPSDestDistanceRef GPSDestDistanceRef GPSProcessingMethod GPSAreaInformation GPSDateStamp 35 84507 430 8073 GPSDifferential

PmExplorer

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

🥱 PmEx	plorer v1.0).20(c) Sar	nderson Forensi	cs Ltd. 2010 -	Licenced to : DE	MONSTRATION SOFTWARE
File Ph	none Profil	es Abou	ıt			
Drag a c	olumn head	ler here to	group by that col	umn		
Кеу	SKey	Current	Description		Туре	In Report Data
				o data to displa		>
		sar	Iderso	<u>n fo</u> re	nsics	
┛						
PM						•
						Data Interpreters
						Name Dec Little Endian Hex Little Endiar
						<no data="" display="" to=""></no>
						Name Date Little Endian Date Big Endian
						<no data="" display="" to=""></no>
					T	Data
Offset:	0		0x00000000	0	Selected: 0	<no data="" display="" to=""></no>
			0 %			
			Key:	SubKey:		li.

Nokia PM tables/records Phone flashers 1

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

•	DCTxBB5 TO	DLS v 2.0.8.0 HWK by SarasSoft			▲ _ 문 ×
Disconnect Check Info Verify Flash	Self Tests UI Settings Local 💌	Restart TORNADO	series		
■ Disconnect Check Info Verify Flash Action / Mode Scenario Flash + UI Options Interface F-Bus Speed I Auto Clear Result Window Image: Auto Autodetect Product Import Auto Scroll Result Window Image: Auto Autodetect Product Import Record: 8, 20 byte(5), 0k Record: Flash Id: [10] 32 Record(5) Record: Record: 9, 20 byte(5), 0k Record: 1, 20 byte(5), 0k Record: 2, 20 byte(5), 0k Record: 3, 20 byte(5), 0k Record: 3, 20 byte(5), 0k Record: 5, 20 byte(5), 0k Record: 5, 20 byte(5), 0k Record: 5, 20 byte(5), 0k Record: 6, 20 byte(5), 0k Record: 10, 20 byte(5), 0k Record: 10, 20 byte(5), 0k Record: 10, 20 byte(5), 0k Record: 11, 20 byte(5), 0k Record: 11, 20 byte(5), 0k Record: 13, 20 byte(5), 0k Record: 13, 20 byte(5), 0k Record: 13, 20 byte(5), 0k Record: 14, 20 byte(5), 0k Record: 14, 20 byte(5), 0k Rec	Self Tests UI Settings Local Fast SimLocks PPM Only START Serial Port COML ISSUE FLASH D KebJDK600 NOR Flash Operation NAND Flash	Restart TORNADO	DCT3 DCT Files and Setti Froduct RH MCU PPM CNT PM CNT PM UI Options Save Users S Full UI Defax UI Factory 0 Full Factory 0	eltings dia generalization of the second eltings dia generalization eltings dia generalization eltings dia generalization dia generalization eltings dia generalization dia gen	se 9 € Index Flashing CNT Auto Enable Flashing CNT Auto CAUTO CAUTO
	** Now you can 1. Download the 2. Dump NDR-FI 3. Grass NDR-FI 4. Format Nand 5. Dump TF5 fits 6. Check the sta	EXIT	H=English, Gree I=English, Portu 0=English, Germ P=English, Chin R=English, Chin S=English, Chin T=English, Chin T=English, Chin V=English, Chin V=English, Chin	ch.useman.spanish.vadic ki,French,Geeman guese,Spanish,French nan,Italian.Spanish,Turkish ese S.Chinese T (Hong Kong) ese S,Chinese T (Hong Kong) ese S,Chinese T (China) ese S,Chinese T (China) ese S,Chinese T (Shinese T chinese S,Chinese T eamese,Chinese T ese S,Chinese T (Shinese T ese S,Chinese T, Bahasa Ind	Create Ini File

Samsung OneNAND

Downloader

Phone flashers 2

HJF- XS++ - Connected phone: W800 (DB2010 CID36)

- O X

05.20.201 ACUVAUIU GDLD GDFS Operations Sony Ericsson XS++ 09:26:29 Phone name detected! Locks: 09:26:29 09:26:29 Sending db2010_cid36red_flash_r2ab.bin... Reads the phone locks code Phone Lock 09:26:29 Applet ID: 050425 0904 MATCXC 1326738 COMPACTFLASH or, if DB2020, resets it to '0000' 09:26:29 This is a FLASH loader GDFS Profile: 09:26:29 09:26:29 Profiling SEMC phone... Retrieve phone properties and Profile Phone 09:26:30 Platform: DB2010 useful debugging ID data (Global Data File System) 09:26:30 OTP CID: 36 09:26:30 EROM CID: 36 Read GDFS: 09:26:30 EROM Color: Red Read out a backup from the device Backup GDFS 09:26:30 | IMEI: 35682800xxxxxx GDFS area 09:26:30 Phone ID: W800 http://en.wikipedia.org/wiki/GDFS 09:26:30 Region: EUROPE 4 GDES Script: 09:26:30 CDA: CDA102430/12 R2A Run Script 09:26:30 Firmware Version: R1BC002 09:26:30 EROM: n/a 09:26:30 Ready for operation! Restore GDFS: 09:27:31 After making any changes with FSX 09:27:31 you must press the 'Shutdown' button Write GDFS SE W800 from lab with (FAT?) FS! 09:27:48 After making any changes with FSX 09:27:48 you must press the 'Shutdown' button Stop 111 - - X Configuration HJ- XS++ - Connected phone: W800 (DB2010 CID36) ○ Settings ○ Flash ○ FSX ™ ◎ GDFS ○ Patch Close 05,25,17 | Arter making any changes with 1 5A FSX ™ 09:29:17 you must press the 'Shutdown' button 09:29:18 Bypassing RSA... Filesystem Explorer: /tpa/ 09:29:18 ⊞∵ifs Enumerated Files -09:29:18 Sending db2010_cid00_prodid_r2f.bin... OUEUE 09:29:19 Applet ID: 050404 1011 LLECXC125872 COMPACTPRODUC . ⊡∽smsdata XS++ Settings 09:29:19 This is a PRODUCTION_ID loader Communication Settings: 09:29:19 - messaging **IPACTPRODU** Download = flash image 09:29:19 Sending db2010_cid00_cert_r2e.bin... Connect Select Port: USB + sms -09:29:19 Applet ID: 040319 0923 LLECXC1326739 COMPACTCERTL - system 09:29:19 This is a CERTIFICATE loader Upload = save image Baud (Speed): 921600 Disconnect messaging 09:29:19 RSA security disabled! ---- sms 09:29:19 SMARTPHONE CONNECT DMPACTFLASH 09:29:19 Sending db2010_cid00_hack_cs_v23.bin... ⊕ system Server Settings: 09:29:20 Applet ID: 060118 0312 EMPCXC1327364_COMPACT_SEM 🖃 ·· tpa 09:29:20 This is a CHIPSELECT loader Username: Password: IP Address: drm 09:29:20 Activating loader... XS++ 127.0.0.1 ... 09:29:20 Activating GDFS... 09:29:21 This loader is UNLOCKED . <u>
</u>
<u>
</u>
<u>
</u>
pdh Check Server 09:29:21 Success! CS-loader has been unlocked! . ⊕ preset 09:29:21 Please wait while XS builds a list of directories... Wayin: . i settings 09:29:21 Activating filesystem BreakXS FastXS O BruteXS SmartXS 09:30:20 Device FS mapped...OK! Controls: Start FSX Upload Download Delete Make Dir Shutdown Configuration Progress: Close Configuration Settings ○ Flash ○ FSX ™ ○ GDFS ○ Patch
 Close Enumerating files from selected path! Connected phone: W800 (DB2010 CID36)

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://computerforensics.sans.org/blog/2010/09/22/digital-forensics-quickcellebrite-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