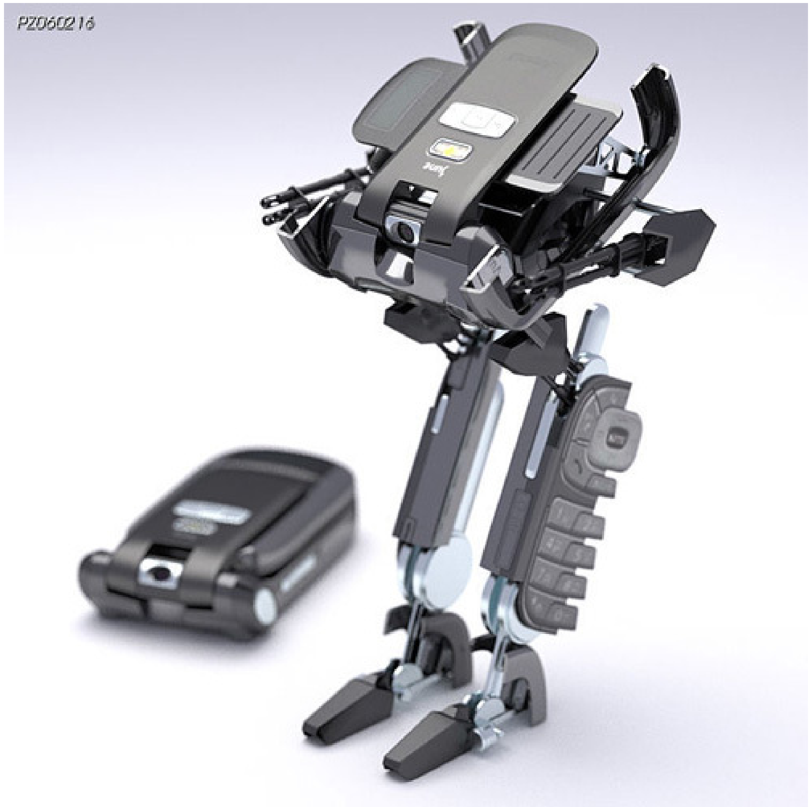


SSDD and SSDF

Handset seizure

Paraben * Seizure test

SE K850, SE Xperia

Small Scale Digital Device (SSDD)

- SSDD definition
  - A Small Scale Digital Device is any of a variety of small form factor devices utilizing volatile or non-volatile memory and various embedded chips for operating systems and/or storage for various computing and/or communication purposes
- Categories
  - Embedded Chip Devices, PDAs, Cellular Telephones, Audio/Video Devices, Gaming Devices, ...
- Characteristics
  - Mobile, Compact Size, Battery Operated, may have specialized Interfaces for Media and Hardware, ...
- Variety of Embedded Operating Systems
  - File System resides in Volatile Memory
- Short Product Cycles

Audio/Video Devices I

- Variety of formats!

A/V Devices II

- Evidence
  - Contacts
  - Calendar Events
  - To Do List
  - Memos
  - Photos
  - Music
  - Files!

Digital Cameras

- Evidence
  - Image
  - EXIF Information
  - Geo-Tag GPS Camera
  - Date Time Stamps
  - Other User Information
- What cell phone does not have a camera?
  - Camera with navigator

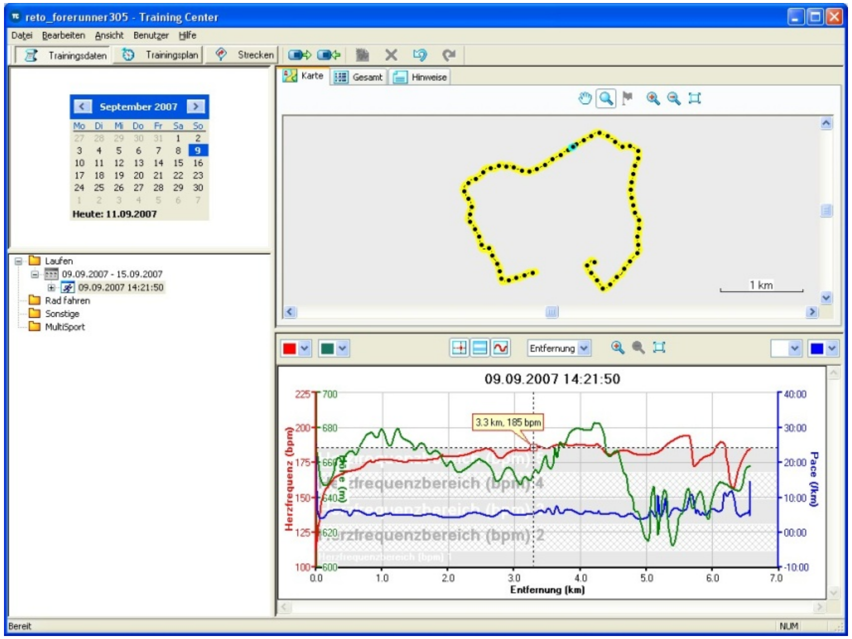
Gaming Devices

- Evidence
  - Games
  - Movies
  - Files
  - Internet
  - Email
  - IM
  - Contacts
  - Calendar Events
  - To Do List
  - Memos
  - Photos
  - Music

Forensic Investigation of the Nintendo Wii: A First Glance
http://www.ssddfj.org/papers/SSDDFJ_V2_1_Turnbull.pdf

GPS devices

- Evidence
  - Tracks
  - Waypoints
  - Routes
  - Date Time Stamps
- Mobilte phones with GPS navigation
  - http://www.prisjakt.nu/kategori.php?l=v615



Unusual Devices?

- Evidence
  - USB Missile Launcher with Webcam
  - http://www.everythingusb.com/
- Garmin Astro
  - Stand alone scanning equipment
- Aiptek pocket cinema
- Digital photo frames
- ...?

Seizing Mobile Evidence

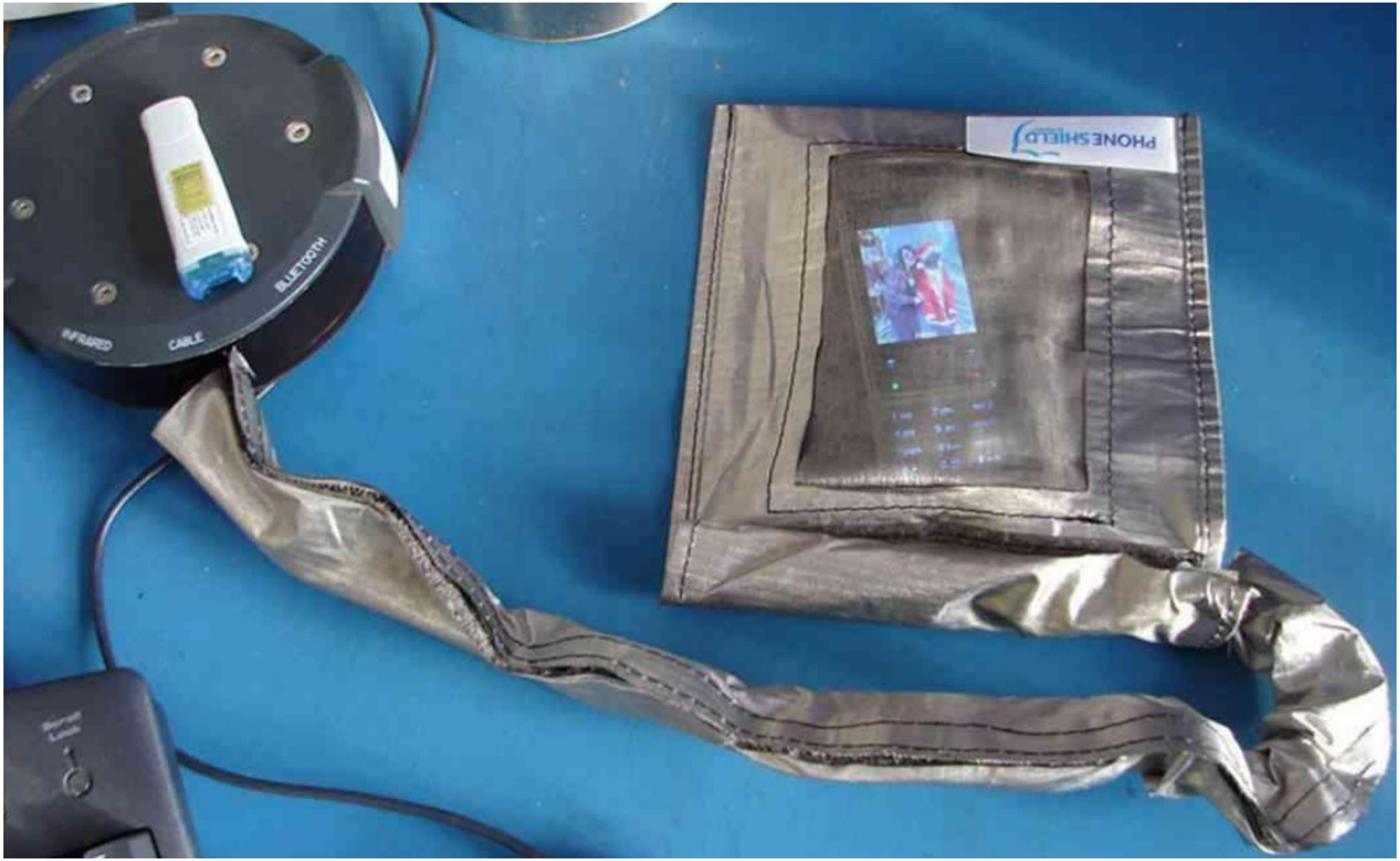
- General guidelines concerning the seizing of evidence are provided as follows
  - Determine the necessary equipment to take to the scene
  - Review the legal authority to seize the evidence
  - All suspects and witnesses should be removed from the proximity of the mobile phone to prevent modifications to the data
  - Ask for information as soon as possible from the mobile phone users to determine the phone number, pass codes or PINs etc.
  - Turn off phone immediately, remove battery if practical, and do not turn it back on
- Considerations
  - Chain of Custody limitations, connectivity options, workflow (reports, information sharing etc.)
  - Additional devices (GPS etc.), phone profiles (OS, phone system etc.), importance of physical dumping and decoding

Turn off or keep the mobile phone on?

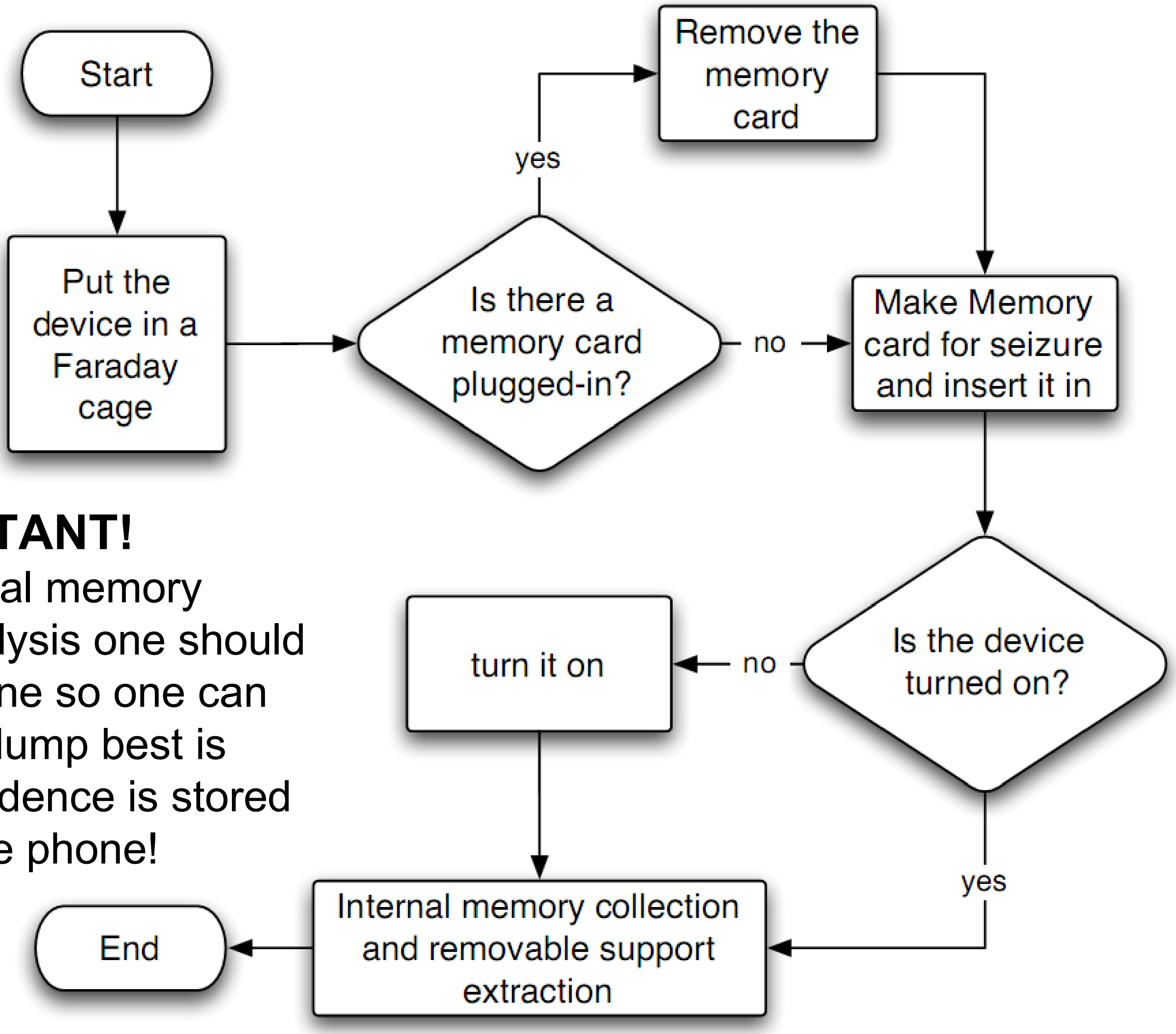
- The **benefits** of turning off the mobile phone include
  - Preserving call logs and last cell tower location information (LOCI)
  - Preventing overwriting deleted data
  - Preventing data destruction signals from reaching the mobile phone
  - Preventing improper mobile phone handling (i.e., placing calls, sending messages, taking photos or deleting files)
- The **risks** with turning the mobile phone off include
  - Possibly locking the phone by Password, Handset Lock or SIM PIN code
- If the mobile phone must be left on, isolate it from its different networks while maintaining power
  - Many mobile phones can be placed in “Airplane” mode preventing access to cell towers. This requires user input on the handset. Disable Wi-Fi, Bluetooth and IrDA communications if practical
- The scene should be searched systematically and thoroughly for evidence. Collect associated chargers, cables, peripherals, boxes, instruction manuals

Radio Frequency (RF) shielding

- Allowing cell tower communication will change data on the phone



General data collection workflow


Start
Put the device in a Faraday cage
Is there a memory card plugged-in?
yes
Remove the memory card
no
Make Memory card for seizure and insert it in
Is the device turned on?
no
turn it on
yes
Internal memory collection and removable support extraction
End

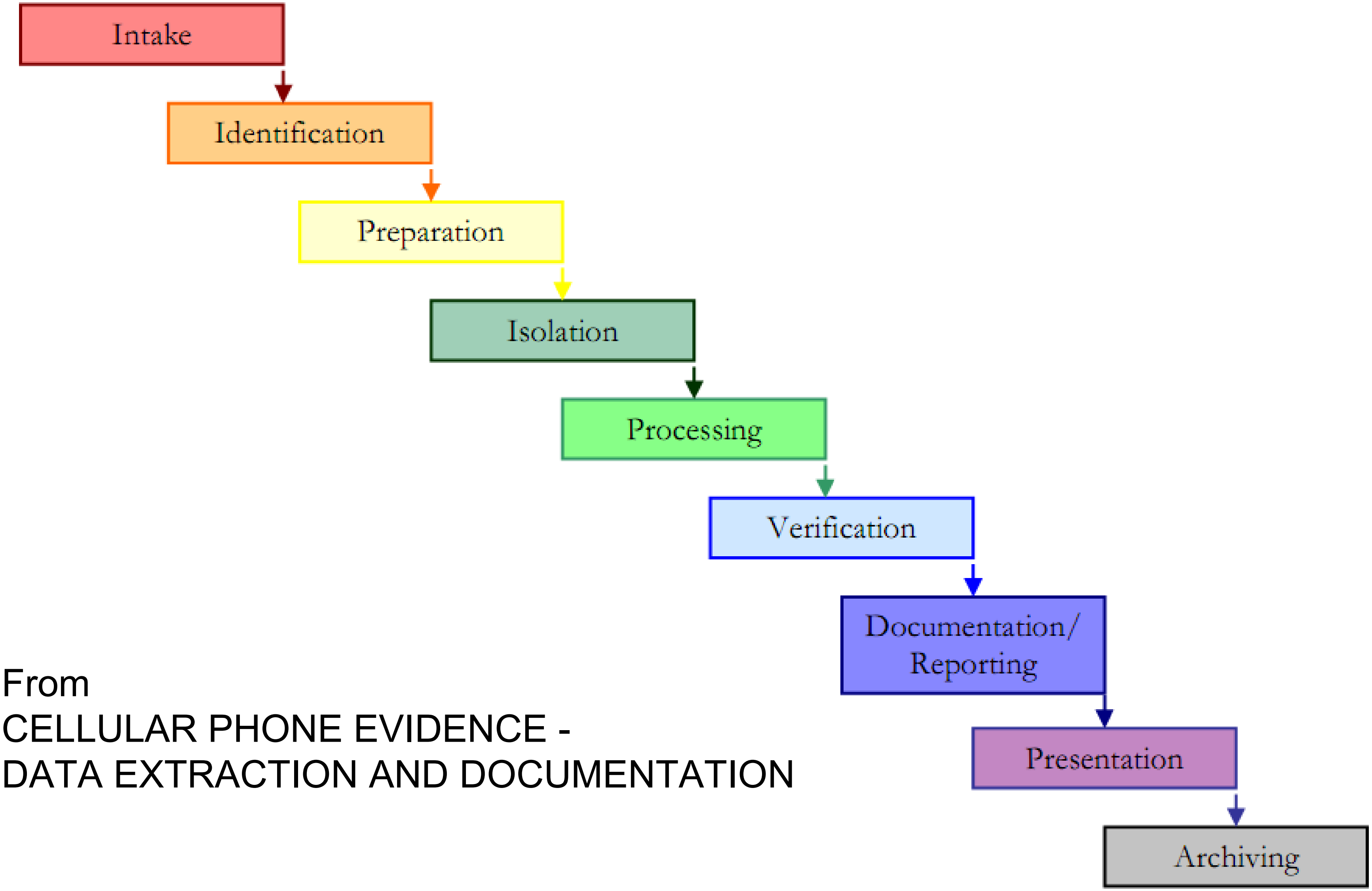
IMPORTANT!

When doing internal memory collection and analysis one should have a ”copy” phone so one can determine how a dump best is taken and how evidence is stored in the image by the phone!

SSDF workflow

- Seizure
  - Documentation
    - Sketches
    - Pictures
    - Video
  - Bag and Tag
- Preservation
  - RF Isolation
    - Shielded environment etc.
  - Power cables etc.
- Identification/Research
  - Web Sites
    - See end
- Connection
  - Cabling
  - Acquisition of data
- Analysis
  - Removable Media
    - Traditional Computer Forensic Tools
  - Cell Phones
  - SIM Cards
  - Smart Phones
    - See PDA and Cell Phone Lists!
    - Emulators
  - Other SSDDs
- Presentation

CELLULAR PHONE EVIDENCE EXTRACTION PROCESS



From
CELLULAR PHONE EVIDENCE -
DATA EXTRACTION AND DOCUMENTATION

Memory Cards

- Increasingly common in handsets
  - Sometimes built-in and non removable
- Different physical “form factors” exist
  - eMMC, *** SD card, MemoryStick Duo etc.
- 1 TB cards soon available (2016)
- PC-compatible FAT file system widely adopted
- May contain pictures, movies, MP3……..or any file at all!
- Deleted data retrievable with established computer forensic techniques

Handset Logical Extraction

- Connection Interfaces
  - Cable
    - Fast, secure, quite reliable
  - Infra-red
    - Slower, quite secure, less reliable
    - Not all data may be retrieved
  - Bluetooth
    - Quite fast, less secure, less reliable, more intrusive
- Extraction software asks handset what data is available
  - Handset may or may not provide data
  - Will not provide deleted data
- Different protocols may be used for
  - Different handsets
  - Different data types

Handset Logical Extraction

- Protocols Used in Logical Extractions
  - Handset API
    - Smartphones usually needs a forensic agent installed
  - AT (Attention commands)
    - Identification, basic information for most GSM models
  - OBEX (“OBject EXchange”)
    - Pictures, audio, video
    - Different flavors for different makes and models
    - http://en.wikipedia.org/wiki/OBEX
  - IrMC, SyncML
    - OBEX based protocols. Phone book, calendar, notes
    - http://en.wikipedia.org/wiki/SyncML
  - FBUS
    - Nokia’s binary protocol. Differences for almost each model
    - http://en.wikipedia.org/wiki/FBus

Cell phone forensic software

- Types
  - SIM
  - Cell phone
  - Forensic vs. Explorer (PC companion type)
- Interface
  - Cables (standard and properitary), Infra-red, Bluetooth, etc.
- Integration (sort of)
  - FTK Mobile Phone Examiner+, Encase 6 Neutrino
- Check out handheld forensic **updated** web pages
- [server]\embedded_forensics

Cell Phone forensic tools

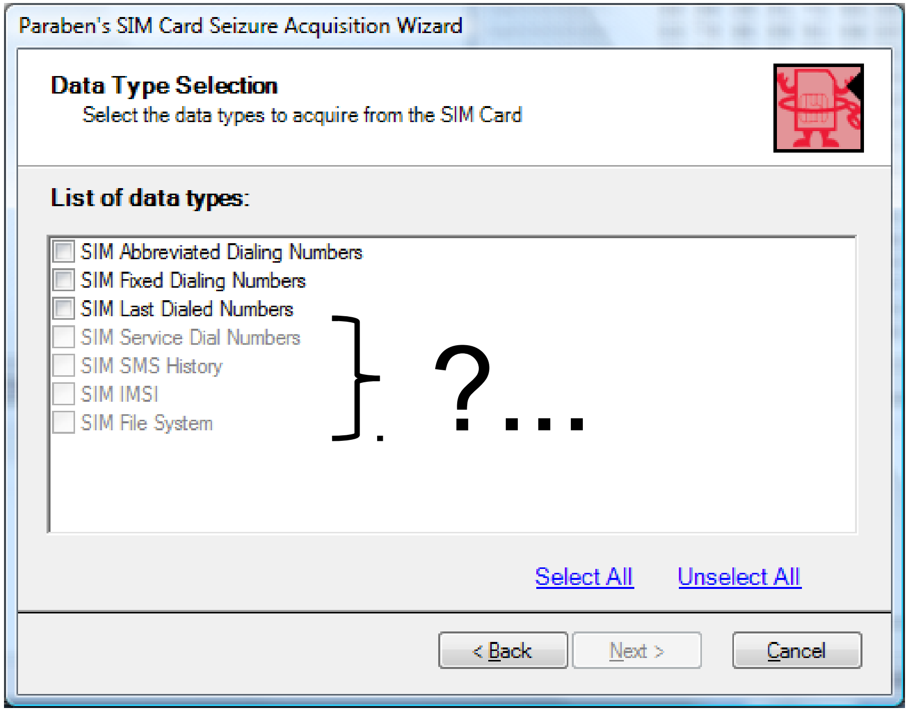
- BitPIM – MyPhoneExplorer etc.
- Oxygen Forensic Suite
  - http://www.oxygen-forensic.com
- Paraben Device Seizure
- SecureView
  - https://secure.susteen.com/secureview/reg_svf_trial.cgi
- MSAB .XRY/XACT
- PhoneBase
- MobilEdit! Forensic
- Cellebrite UFED (Universal Forensic Extraction Dev.)
  - Physical Pro
- Many more exist…
  - http://www.e-evidence.info/cellular.html

SIM card tools

- CHIPDRIVE Smartcard Commander
- Serial and USB SIM Card Readers
- Paraben SIM Card Seizure
- ForensicSIM
- SIMIS
- SIMScan
- SIM Detective
- Forensic Card Reader 2
- Many more exist…
  - http://www.e-evidence.info/cellular.html

Paraben SIM Card Seizure

- SCM Smart Card SCR335 and SCR3311
  - http://www.scmmicro.de/security/index.html
  - PC/SC driver needed (Windows Smartcard API)
    - http://en.wikipedia.org/wiki/PC/SC



Paraben's SIM Card Seizure Acquisition Wizard

Data Type Selection

Select the data types to acquire from the SIM Card

List of data types:

- □ SIM Abbreviated Dialing Numbers
- □ SIM Fixed Dialing Numbers
- □ SIM Last Dialed Numbers
- □ SIM Service Dial Numbers
- □ SIM SMS History
- □ SIM IMSI
- □ SIM File System

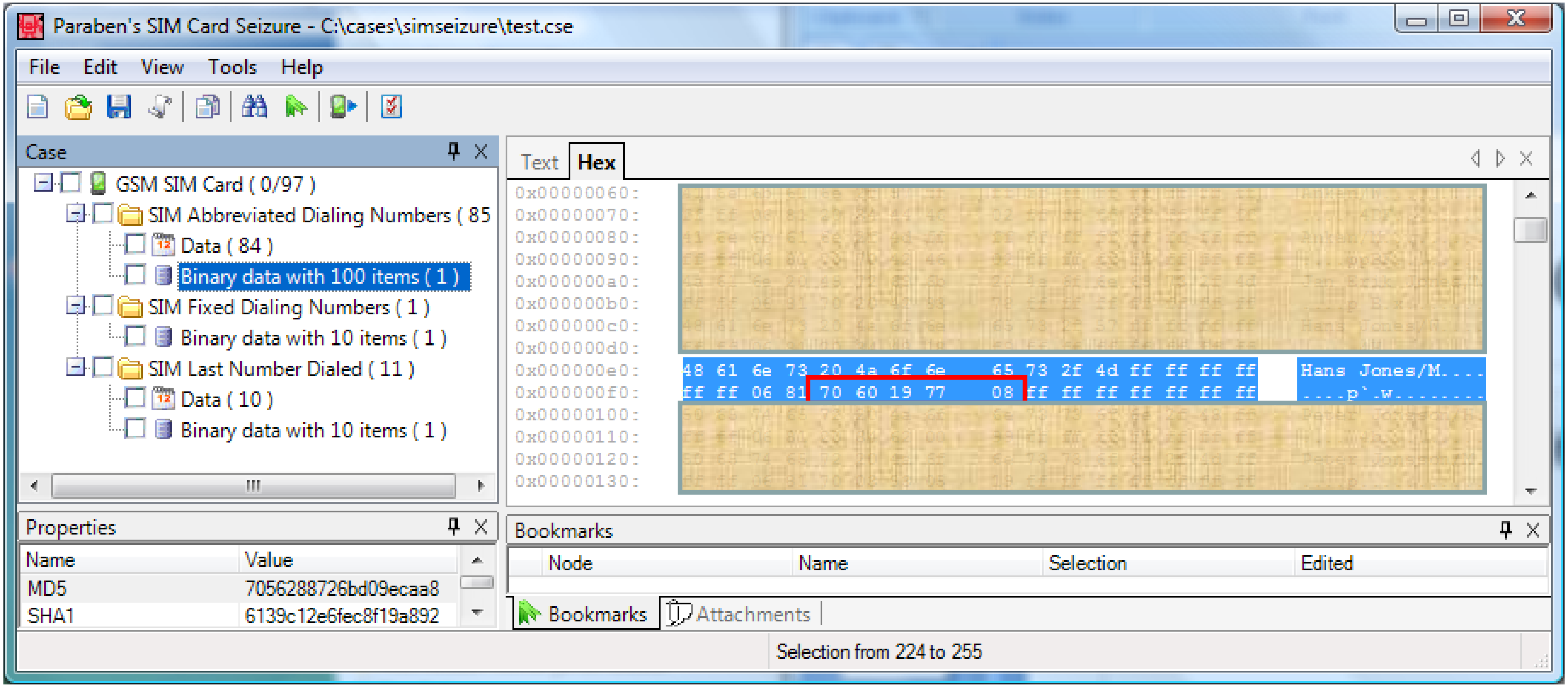
}. ?...

PC/SC
(Personal Computer/Smart Card)

- Architecture designed to ensure the following work together even if made by different manufacturers
  - Smart cards
  - Smart card readers
  - Computers
- Designed for Windows environment with development in Visual C+
  - http://www.codeproject.com/KB/smart/smartcardapi.aspx (.NET)
- Implementations are available for other OS
  - PC/SC Lite for Unix like OS (Mac OS X)
  - Java: http://www.openscdp.org/ocf/

SIM Card Seizure Hex view

- SIM Card Seizure (earlier had the name SIMCon)
- SIM card (older than year 2000)
- One record, Tel. 0706917780



Paraben's SIM Card Seizure - C:\cases\simseizure\test.cse
File Edit View Tools Help
Case
GSM SIM Card (0/97)
SIM Abbreviated Dialing Numbers (85
Data (84)
Binary data with 100 items (1)
SIM Fixed Dialing Numbers (1)
Binary data with 10 items (1)
SIM Last Number Dialed (11)
Data (10)
Binary data with 10 items (1)
Text
Hex
Bookmarks
Attachments

```
0x00000060:
0x00000070:
0x00000080:
0x00000090:
0x000000a0:
0x000000b0:
0x000000c0:
0x000000d0:
0x000000e0:  48 61 6e 73 20 4a 6f 6e  65 73 2f 4d ff ff ff ff   Hans Jones/M....
0x000000f0:  ff ff 06 81 70 60 19 77  08 ff ff ff ff ff ff ff   ....p`.w........
0x00000100:
0x00000110:
0x00000120:
0x00000130:
```

[redacted]

[redacted]

Properties

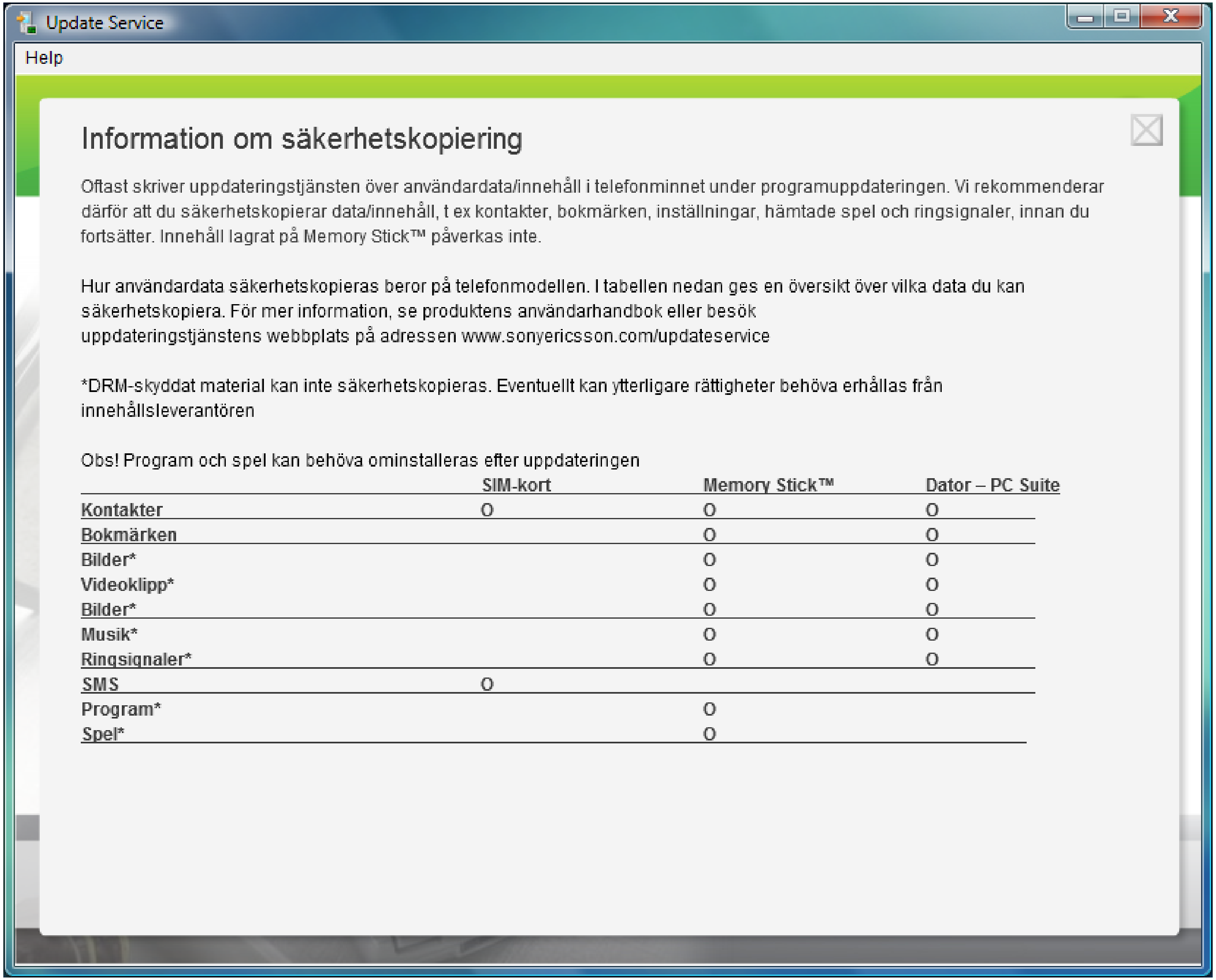
Name	Value
MD5	7056288726bd09ecaa8
SHA1	6139c12e6fec8f19a892

Bookmarks

Node	Name	Selection	Edited

Selection from 224 to 255

Mobile security copy - SE update



Information om säkerhetskopiering

Oftast skriver uppdateringstjänsten över användardata/innehåll i telefonminnet under programuppdateringen. Vi rekommenderar därför att du säkerhetskopierar data/innehåll, t ex kontakter, bokmärken, inställningar, hämtade spel och ringsignaler, innan du fortsätter. Innehåll lagrat på Memory Stick™ påverkas inte.

Hur användardata säkerhetskopieras beror på telefonmodellen. I tabellen nedan ges en översikt över vilka data du kan säkerhetskopiera. För mer information, se produktens användarhandbok eller besök uppdateringstjänstens webbplats på adressen www.sonyericsson.com/updateservice

*DRM-skyddat material kan inte säkerhetskopieras. Eventuellt kan ytterligare rättigheter behöva erhållas från innehållsleverantören

Obs! Program och spel kan behöva ominstalleras efter uppdateringen

	SIM-kort	Memory Stick™	Dator – PC Suite
Kontakter	O	O	O
Bokmärken		O	O
Bilder*		O	O
Videoklipp*		O	O
Bilder*		O	O
Musik*		O	O
Ringsignaler*		O	O
SMS	O		
Program*		O	
Spel*		O	

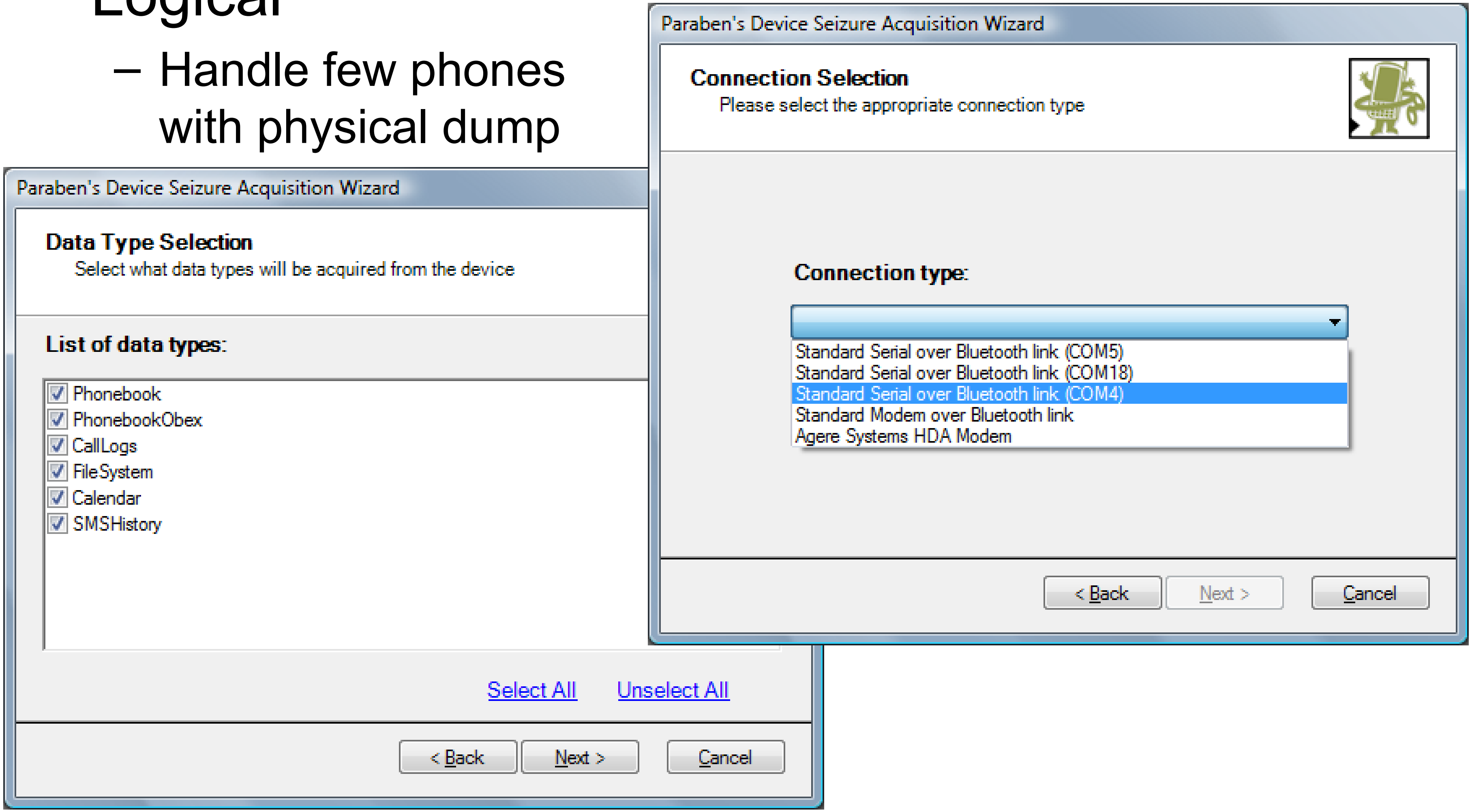
Paraben Device Seizure can acquire the following data:

- Acquire and analyze data from over 1,950 mobile phones, PDAs, and GPS devices including iPhones
- Most commercial cell phone forensic software only gets logical data files
- Deleted data and user data such as text messages and images can often be found in a physical data dump of a phone

- SMS History (Text Messages)
- Deleted SMS (Text Messages)
- Phonebook (both stored in the memory of the phone and on the SIM card)
- Call History
  - Received Calls
  - Dialed Numbers
  - Missed calls
  - Call Dates & Durations
- Datebook
- Scheduler
- Calendar
- To-Do List
- Filesystem (physical memory dumps)
  - System Files
  - Multimedia Files (Images, Videos, etc.)
  - Java Files
  - Deleted Data
  - Quicknotes
  - More...
- GPS Waypoints, Tracks, Routes, etc.
- RAM/ROM
- PDA Databases
- E-mail
- Registry (Windows Mobile Devices)

Paraben Device Seizure - SE K850

- Logical
  - Handle few phones with physical dump



Paraben's Device Seizure Acquisition Wizard

Data Type Selection

Select what data types will be acquired from the device

List of data types:

- ☑ Phonebook
- ☑ PhonebookObex
- ☑ CallLogs
- ☑ FileSystem
- ☑ Calendar
- ☑ SMSHistory

Paraben's Device Seizure Acquisition Wizard

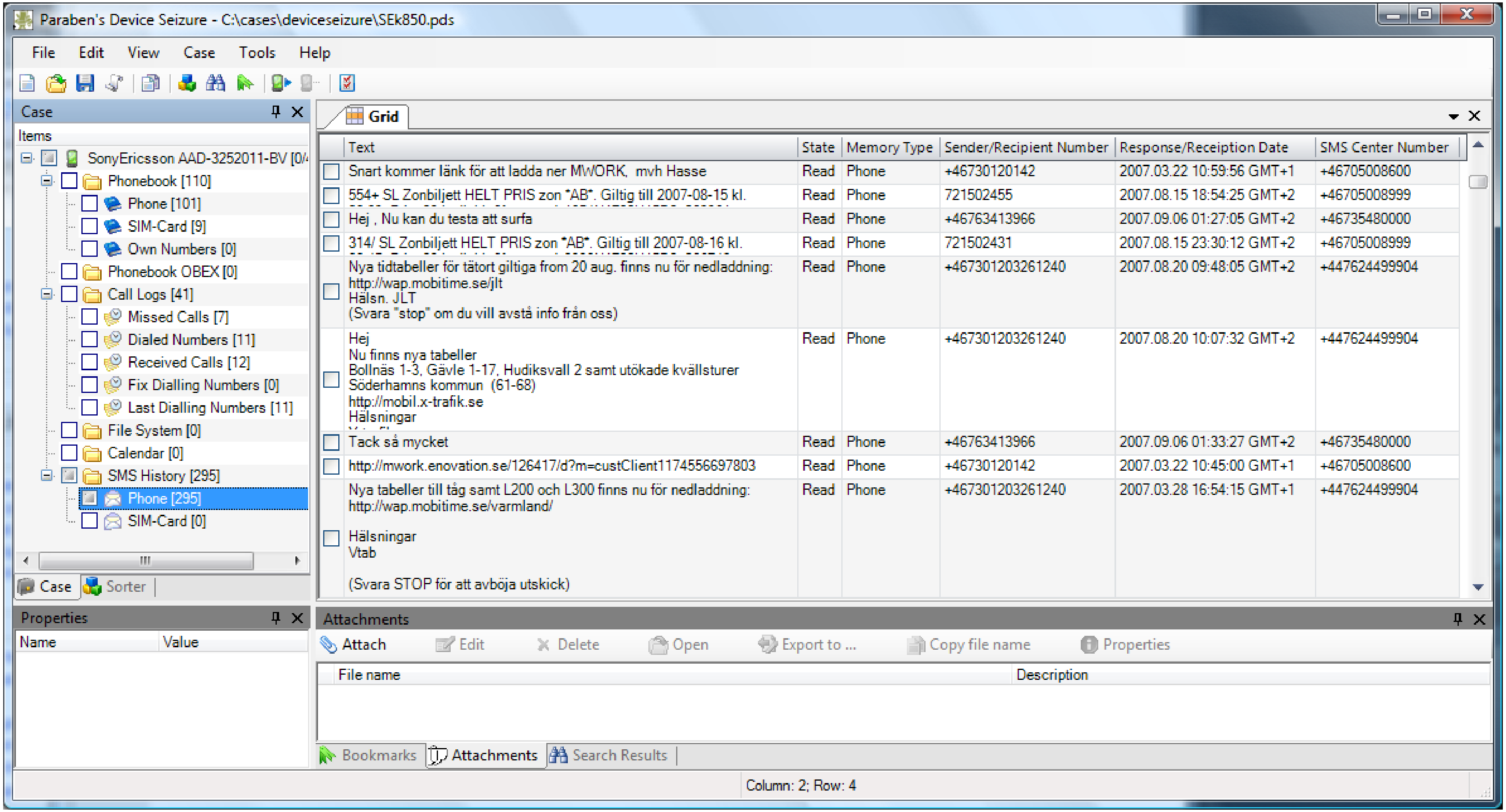
Connection Selection

Please select the appropriate connection type

Connection type:

- Standard Serial over Bluetooth link (COM5)
- Standard Serial over Bluetooth link (COM18)
- Standard Serial over Bluetooth link (COM4)
- Standard Modem over Bluetooth link
- Agere Systems HDA Modem

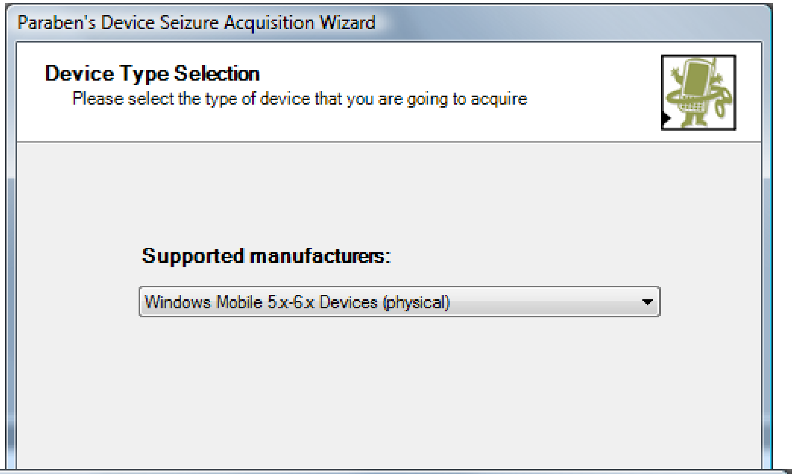
Paraben Device Seizure - SE K850



	Text	State	Memory Type	Sender/Recipient Number	Response/Reception Date	SMS Center Number
□	Snart kommer länk för att ladda ner MWORK, mvh Hasse	Read	Phone	+46730120142	2007.03.22 10:59:56 GMT+1	+46705008600
□	554+ SL Zonbiljett HELT PRIS zon *AB*. Giltig till 2007-08-15 kl.	Read	Phone	721502455	2007.08.15 18:54:25 GMT+2	+46705008999
□	Hej , Nu kan du testa att surfa	Read	Phone	+46763413966	2007.09.06 01:27:05 GMT+2	+46735480000
□	314/ SL Zonbiljett HELT PRIS zon *AB*. Giltig till 2007-08-16 kl.	Read	Phone	721502431	2007.08.15 23:30:12 GMT+2	+46705008999
□	Nya tidtabeller för tätort giltiga from 20 aug. finns nu för nedladdning: http://wap.mobitime.se/jlt Hälsn. JLT (Svara "stop" om du vill avstå info från oss)	Read	Phone	+467301203261240	2007.08.20 09:48:05 GMT+2	+447624499904
□	Hej Nu finns nya tabeller Bollnäs 1-3, Gävle 1-17, Hudiksvall 2 samt utökade kvällsturer Söderhamns kommun (61-68) http://mobil.x-trafik.se Hälsningar	Read	Phone	+467301203261240	2007.08.20 10:07:32 GMT+2	+447624499904
□	Tack så mycket	Read	Phone	+46763413966	2007.09.06 01:33:27 GMT+2	+46735480000
□	http://mwork.enovation.se/126417/d?m=custClient1174556697803	Read	Phone	+46730120142	2007.03.22 10:45:00 GMT+1	+46705008600
□	Nya tabeller till tåg samt L200 och L300 finns nu för nedladdning: http://wap.mobitime.se/varmland/ Hälsningar Vtab (Svara STOP för att avböja utskick)	Read	Phone	+467301203261240	2007.03.28 16:54:15 GMT+1	+447624499904

Paraben Device Seizure SE Xperia

- Windows Mobile 6.x
- Dump via cable
  - Physical (crash)
    - Rapisec.cab has not been installed
  - Logical
    - Dll.dll must be installed



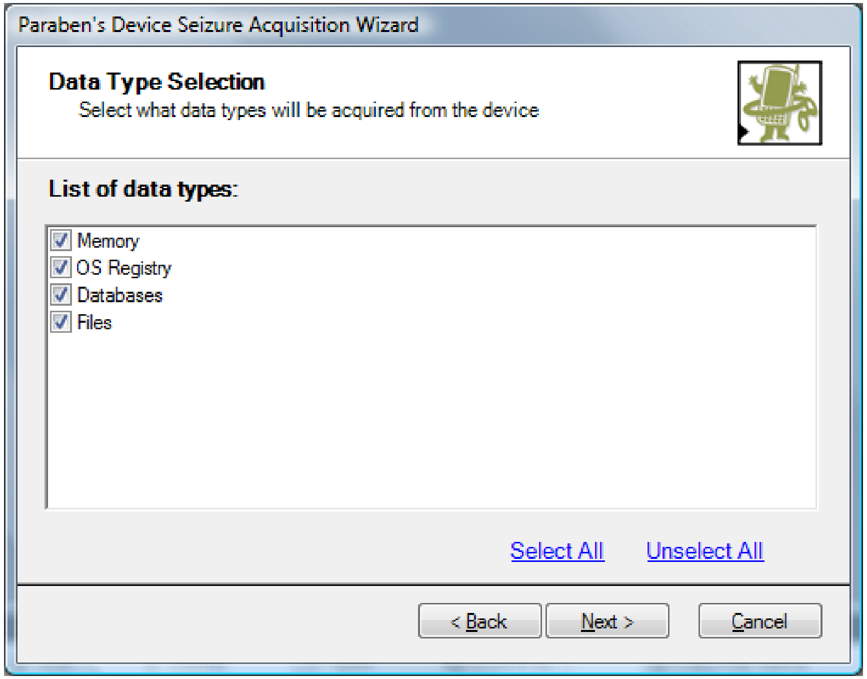
Paraben's Device Seizure Acquisition Wizard

Device Type Selection

Please select the type of device that you are going to acquire

Supported manufacturers:

Windows Mobile 5x-6x Devices (physical)



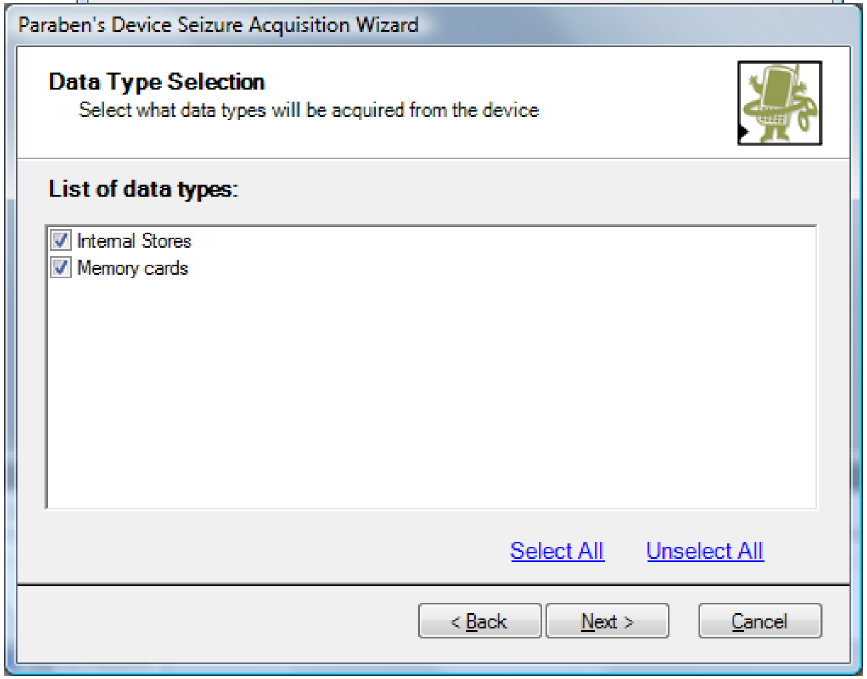
Paraben's Device Seizure Acquisition Wizard

Data Type Selection

Select what data types will be acquired from the device

List of data types:

☑ Memory
☑ OS Registry
☑ Databases
☑ Files



Paraben's Device Seizure Acquisition Wizard

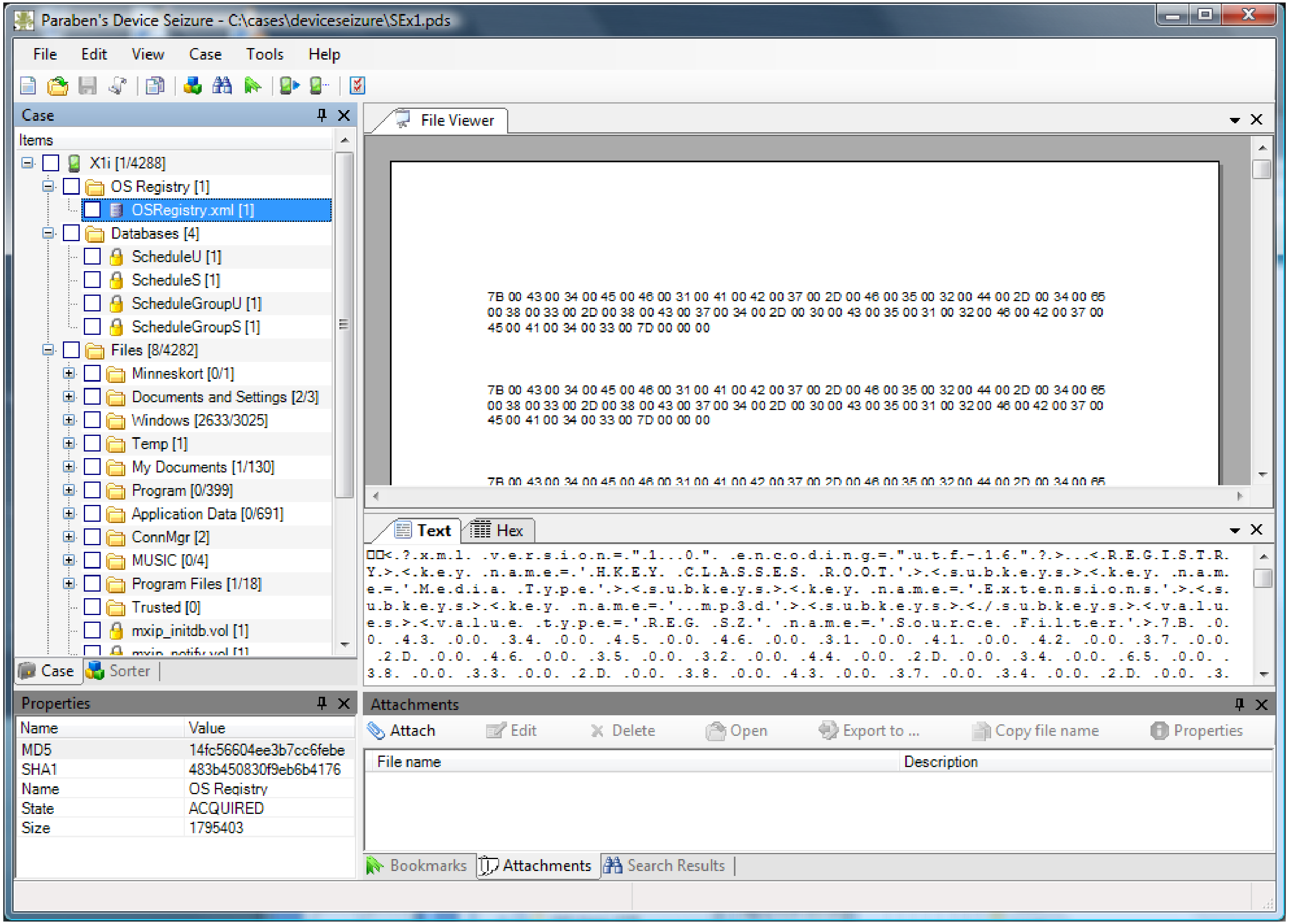
Data Type Selection

Select what data types will be acquired from the device

List of data types:

☑ Internal Stores
☑ Memory cards

Paraben Device Seizure SE Xperia



- X1i [1/4288]
  - OS Registry [1]
    - OSRegistry.xml [1]
  - Databases [4]
    - ScheduleU [1]
    - ScheduleS [1]
    - ScheduleGroupU [1]
    - ScheduleGroupS [1]
  - Files [8/4282]
    - Minneskort [0/1]
    - Documents and Settings [2/3]
    - Windows [2633/3025]
    - Temp [1]
    - My Documents [1/130]
    - Program [0/399]
    - Application Data [0/691]
    - ConnMgr [2]
    - MUSIC [0/4]
    - Program Files [1/18]
    - Trusted [0]
    - mxip_initdb.vol [1]
    - mxip_notify.vol [1]

Name	Value
MD5	14fc56604ee3b7cc6febe
SHA1	483b450830f9eb6b4176
Name	OS Registry
State	ACQUIRED
Size	1795403

```
7B 00 43 00 34 00 45 00 46 00 31 00 41 00 42 00 37 00 2D 00 46 00 35 00 32 00 44 00 2D 00 34 00 65
00 38 00 33 00 2D 00 38 00 43 00 37 00 34 00 2D 00 30 00 43 00 35 00 31 00 32 00 46 00 42 00 37 00
45 00 41 00 34 00 33 00 7D 00 00 00


7B 00 43 00 34 00 45 00 46 00 31 00 41 00 42 00 37 00 2D 00 46 00 35 00 32 00 44 00 2D 00 34 00 65
00 38 00 33 00 2D 00 38 00 43 00 37 00 34 00 2D 00 30 00 43 00 35 00 31 00 32 00 46 00 42 00 37 00
45 00 41 00 34 00 33 00 7D 00 00 00


7B 00 43 00 34 00 45 00 46 00 31 00 41 00 42 00 37 00 2D 00 46 00 35 00 32 00 44 00 2D 00 34 00 65
```

```
□□<.?.x.m.l. .v.e.r.s.i.o.n.=.".1...0.". .e.n.c.o.d.i.n.g.=.".u.t.f.-.1.6.".?.>...<.R.E.G.I.S.T.R.
Y.>.<.k.e.y. .n.a.m.e.=.'.H.K.E.Y. .C.L.A.S.S.E.S. .R.O.O.T.'.>.<.s.u.b.k.e.y.s.>.<.k.e.y. .n.a.m.
e.=.'.M.e.d.i.a. .T.y.p.e.'.>.<.s.u.b.k.e.y.s.>.<.k.e.y. .n.a.m.e.=.'.E.x.t.e.n.s.i.o.n.s.'.>.<.s.
u.b.k.e.y.s.>.<.k.e.y. .n.a.m.e.=.'...m.p.3.d.'.>.<.s.u.b.k.e.y.s.>.<./.s.u.b.k.e.y.s.>.<.v.a.l.u.
e.s.>.<.v.a.l.u.e. .t.y.p.e.=.'.R.E.G. .S.Z.'. .n.a.m.e.=.'.S.o.u.r.c.e. .F.i.l.t.e.r.'.>.7.B. .0.
0. .4.3. .0.0. .3.4. .0.0. .4.5. .0.0. .4.6. .0.0. .3.1. .0.0. .4.1. .0.0. .4.2. .0.0. .3.7. .0.0.
 .2.D. .0.0. .4.6. .0.0. .3.5. .0.0. .3.2. .0.0. .4.4. .0.0. .2.D. .0.0. .3.4. .0.0. .6.5. .0.0. .
3.8. .0.0. .3.3. .0.0. .2.D. .0.0. .3.8. .0.0. .4.3. .0.0. .3.7. .0.0. .3.4. .0.0. .2.D. .0.0. .3.
```

File name	Description

Windows Mobile 6.x and below

- From ”Introduction to Windows Mobile Forensics” on [server]

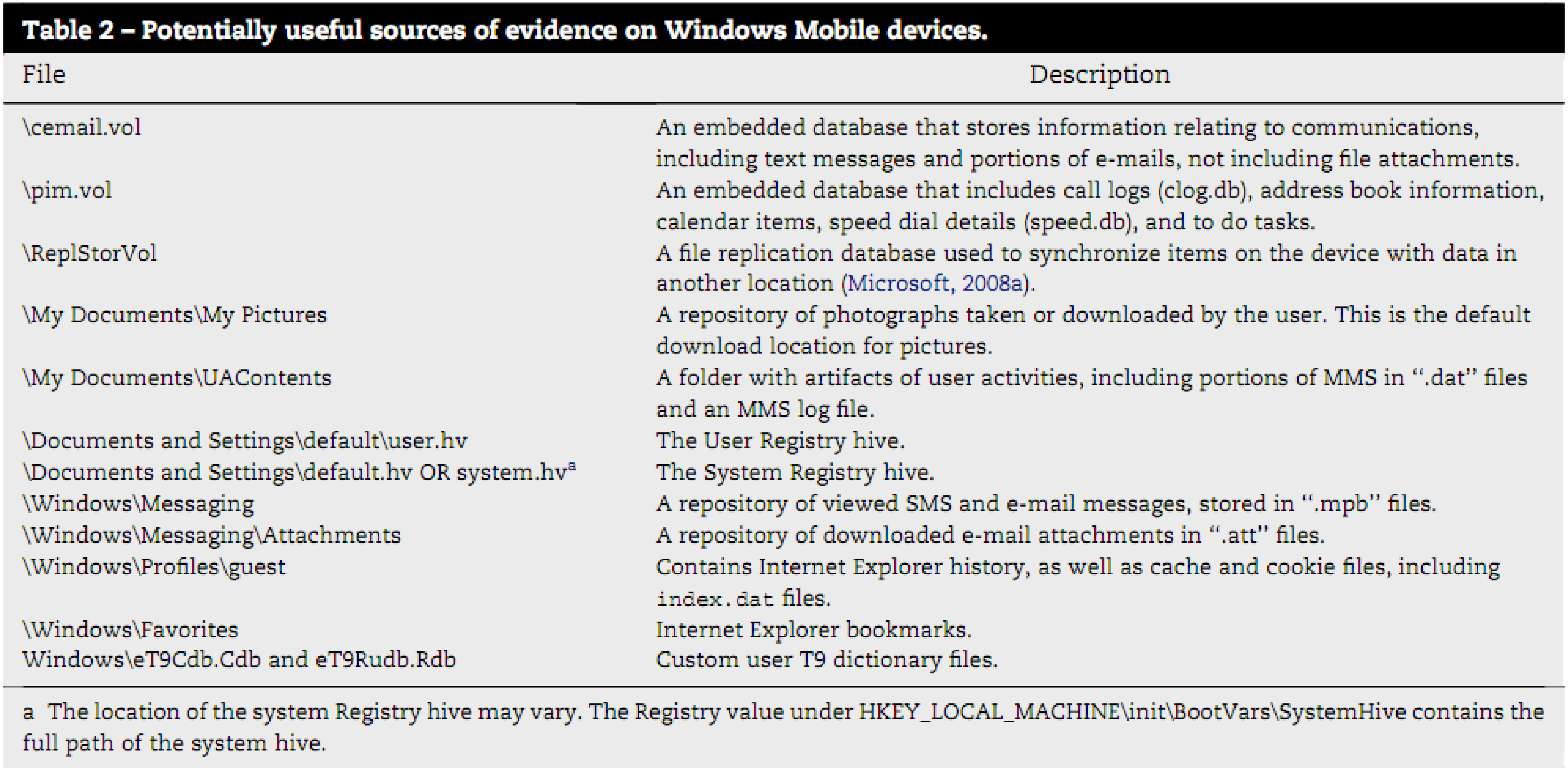


Table 2 – Potentially useful sources of evidence on Windows Mobile devices.

File	Description
\cemail.vol	An embedded database that stores information relating to communications, including text messages and portions of e-mails, not including file attachments.
\pim.vol	An embedded database that includes call logs (clog.db), address book information, calendar items, speed dial details (speed.db), and to do tasks.
\ReplStorVol	A file replication database used to synchronize items on the device with data in another location (Microsoft, 2008a).
\My Documents\My Pictures	A repository of photographs taken or downloaded by the user. This is the default download location for pictures.
\My Documents\UAContents	A folder with artifacts of user activities, including portions of MMS in ‘‘.dat’’ files and an MMS log file.
\Documents and Settings\default\user.hv	The User Registry hive.
\Documents and Settings\default.hv OR system.hv[a]	The System Registry hive.
\Windows\Messaging	A repository of viewed SMS and e-mail messages, stored in ‘‘.mpb’’ files.
\Windows\Messaging\Attachments	A repository of downloaded e-mail attachments in ‘‘.att’’ files.
\Windows\Profiles\guest	Contains Internet Explorer history, as well as cache and cookie files, including `index.dat` files.
\Windows\Favorites	Internet Explorer bookmarks.
Windows\eT9Cdb.Cdb and eT9Rudb.Rdb	Custom user T9 dictionary files.

[a] The location of the system Registry hive may vary. The Registry value under HKEY_LOCAL_MACHINE\init\BootVars\SystemHive contains the full path of the system hive.

Readings

- Check out the readings for the course!
  - [server]\embedded_forensics\docs
  - Forensic guidelines for Android, iOS, Symbian, Blackberry, MeeGo, Windows Mobile 6.x
  - SIM
- Evidence in Mobile Phone Systems
  - By Svein Y. Willassen, M.Sc.
- Sample Forensics Reports - SIM Card and Cell Phone
  - [server]\embedded_forensics\docs\sample_forensic_report
- Books, papers, tutorials, ...
  - https://github.com/secmobi/wiki.secmobi.com/tree/master/pages/publications