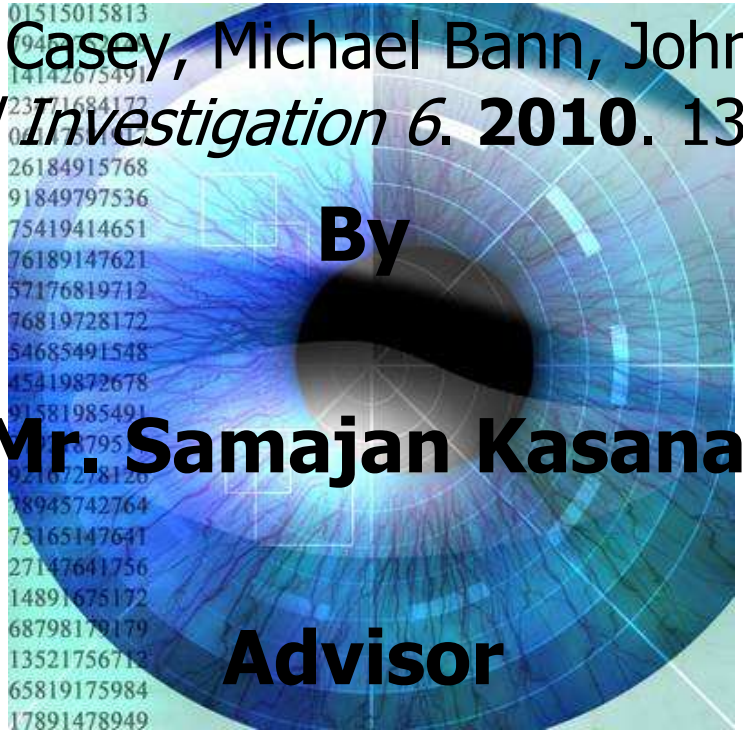
Introduction to Windows Mobile Forensics

Eoghan Casey, Michael Bann, John Doyle.
Digital Investigation 6. **2010**. 136-146



By

Mr. Samajan Kasana

Advisor

Pol.Col. Siripong Timula

Introduction

- The personal nature of the information on these devices can provide digital investigators with valuable insights into the *modus operandi* of suspects and activities of victims.



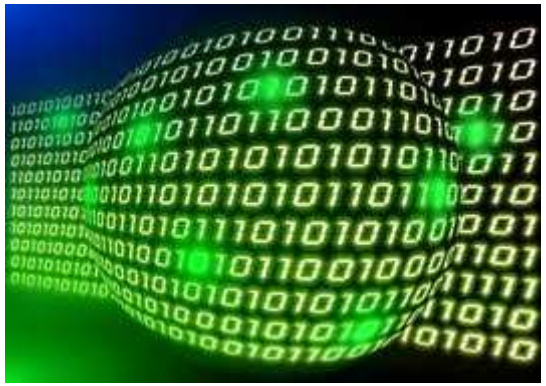
Introduction *(to…)*

Table 1-Summary of test device characteristics.

Manufacturer/model	OS version	OS build	Radio version
HTC S620 (Dash)	Window Mobile 6 Standard,5.2.1236	17741.0.2.1	4.1.13.61_03.21.90
Motorola Q	Window Mobile 5.0,5.1.195	14960.2.4.0	Q2-BP_C_06.OB.11P, Q2 Portable
Samsung i607(Blackjack)	Window Mobile 5.0 with Messaging and Security Feature Pack,5.1.342	15100.3.0.2	

Introduction *(to…)*

- The remainder of this paper describes where useful information is stored and how to examine these important data sources.



Windows Mobile overview

- Windows Mobile uses a variation of the FAT file system called the Transaction-safe FAT (TFAT) file system, which has some recovery features in the event of a sudden device shutdown.

Windows Mobile overview *(to…)*

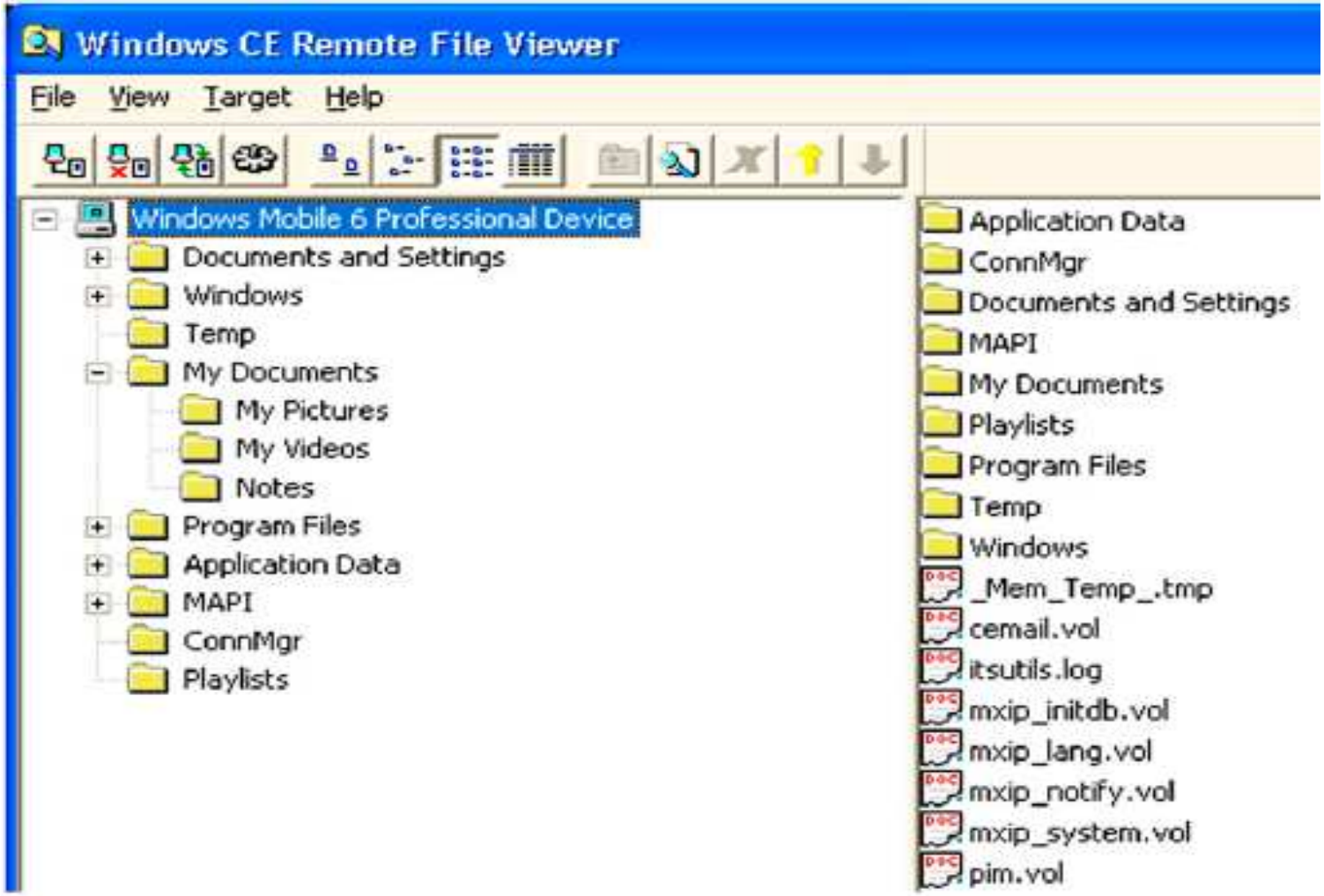


Fig. 1 – File system hierarchy on a Samsung i607 (Blackjack).

Locations of Usage Artifacts on Windows Mobile Devices

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.

Forensic Processing of Windows Mobile Devices

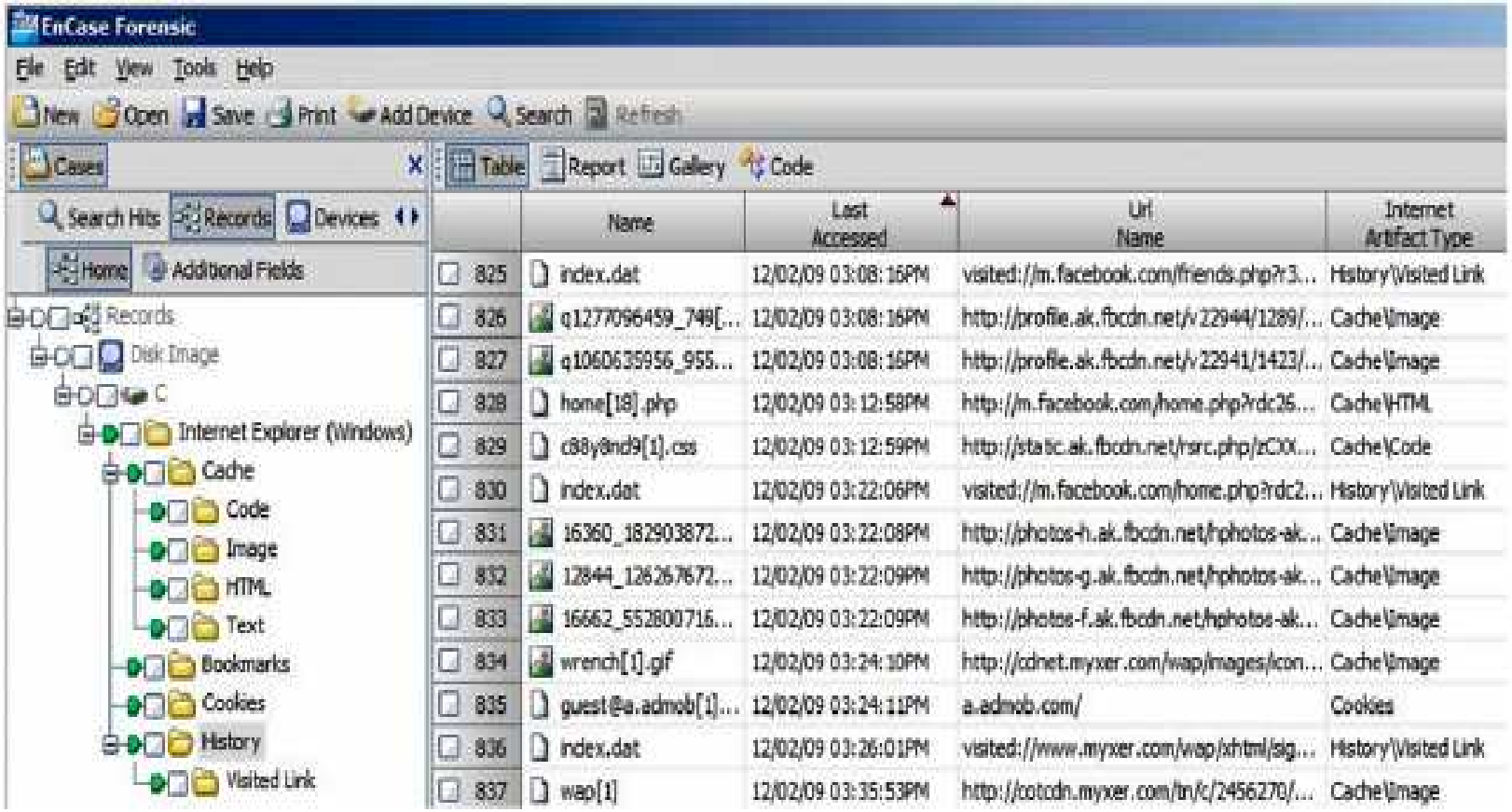


Fig. 2 – Remnants of Internet Explorer browsing activities on a Samsung i607 (Blackjack) device viewed using EnCase.

Forensic Acquisition

- The forensic acquisition tools that are available to most forensic analysts do not have direct access to flash memory on Windows Mobile devices and are limited to acquiring data through a hardware abstraction layer.

Forensic Acquisition *(to…)*

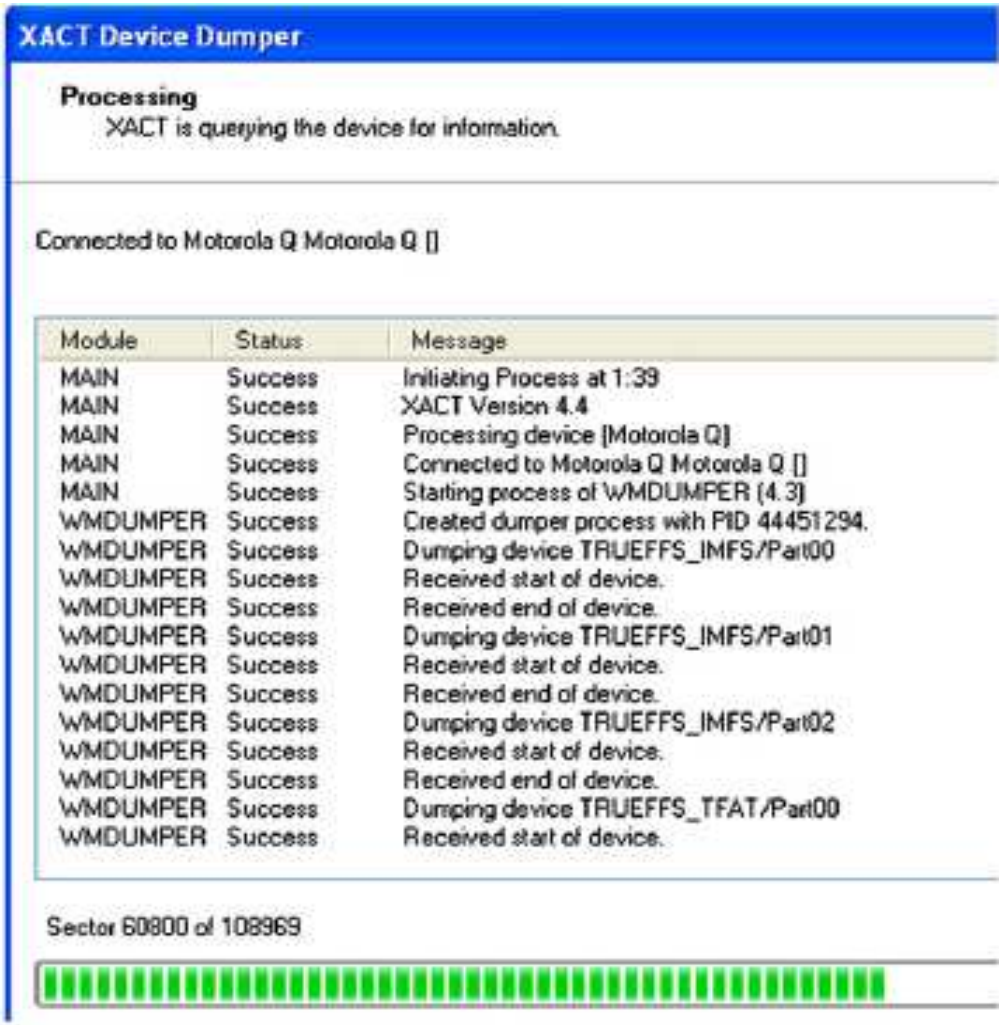


Fig. 3 – XACT acquisition screenshot of Motorola Q.

Deleted File Recovery

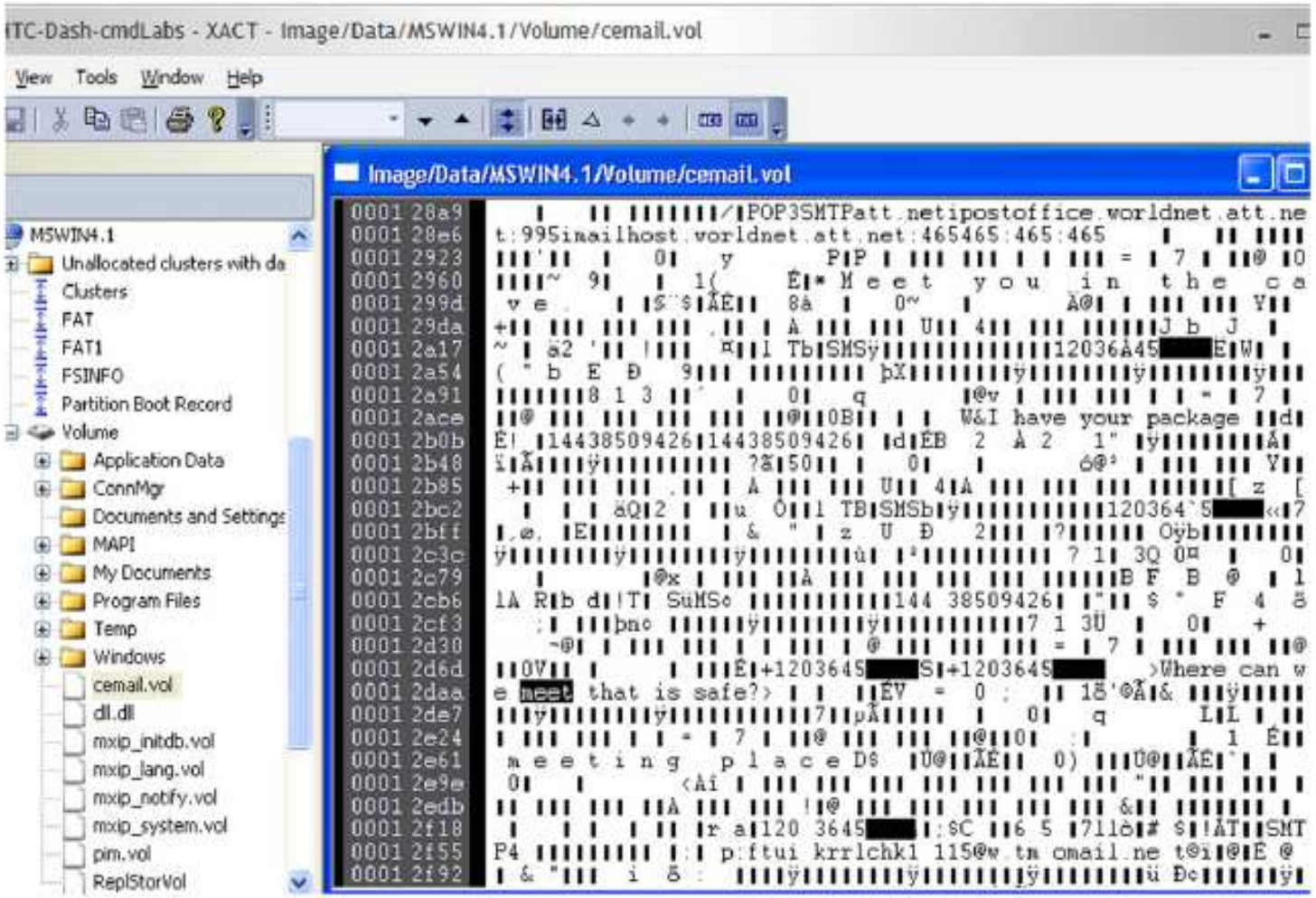


Fig. 4 – Windows Mobile file system viewed using XACT with missing folders.

Examining Embedded Databases

- Windows Mobile devices store some significant information in volume files that encapsulate multiple embedded databases that include details about communications, contacts, and calls.

Examining Embedded Databases *(to…)*

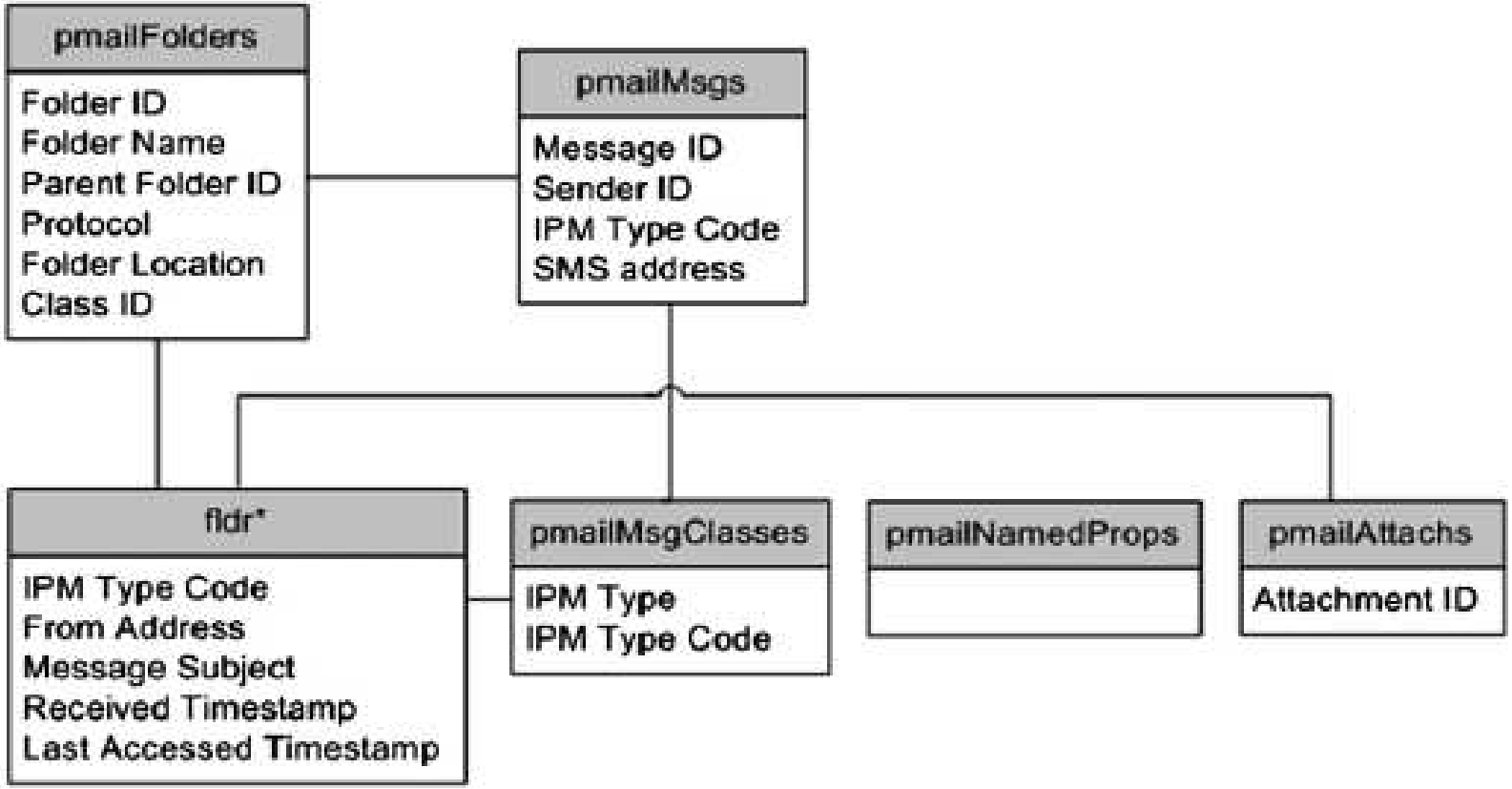


Fig. 5 – Overview of `cemail.vol` file.

Examining Embedded Databases *(to…)*

Table 3 – Property identifiers for useful items within the "pmailMsgs" database.

Property ID	Description
0x800C	Contains sender identification information, such as a phone number in the case of an SMS message.
0x8001	Contains the Interpersonal Message (IPM) type code, which indicates the type of message sent (e.g. SMS, MMS, e-mail). The lookup table for IPM type code resides within the "pmailMsgClasses" database.
0x0E09	Contains the Folder ID in decimal form. This must be converted into its hexadecimal equivalent to determine the containing "fldr#" database.

Examining Embedded Databases *(to…)*

Table 4 – Property identifiers for useful items within "fldr*" databases.

Property ID	Description
0x8005	OID used as a lookup value.
0x0C1F	From address (contact name unresolved)
0x0C1A	From address (contact name resolved)
0x003D	Denotes the message prefix, either "Re: ", "Fw: ", or "" denoting reply, forward, and null, respectively.
0x0037	Message subject or, when applicable, the message body if it is small enough.
0x0E06	Message received timestamp.
0x3008	Message last modified timestamp.
0x001A	Lookup field, which links this database to the "pmailMsgClasses" database.

Tools and Interpretation

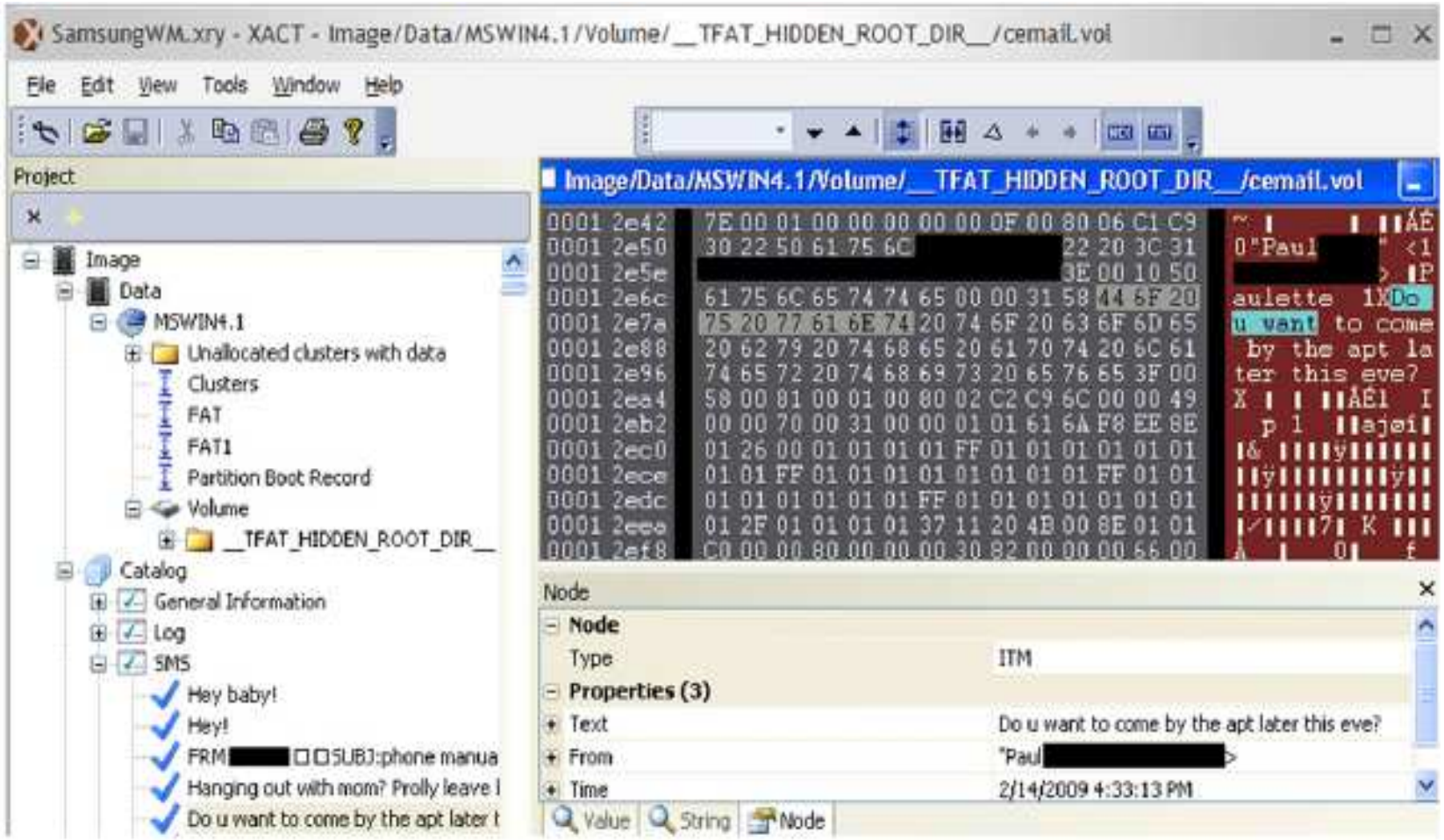


Fig. 6 – XACT showing data in `cemail.vol` file.

Examining Registry Hives

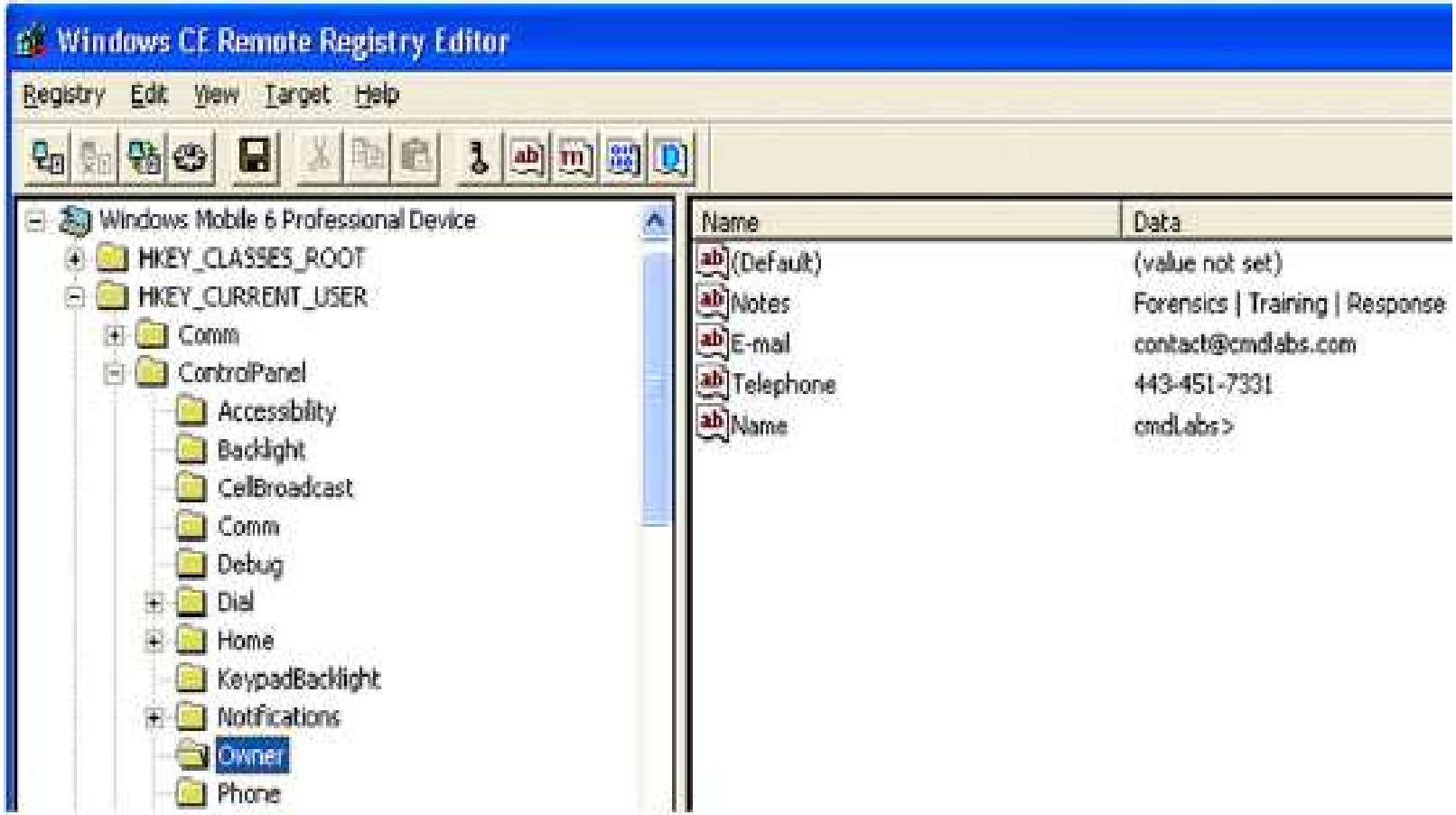


Fig. 7 – Registry values on a Samsung i607 (Blackjack) device.

Examining Registry Hives *(to…)*

Table 5-Items in the user Registry hive on Windows Mobile devices of potential interest.

Registry key	Description
HKCU\ControlPanel\Owner	Contact details entered by user
HKCU\System\State\Shell	Most recently used (MRU) items
HKCU\Software\Microsoft\pMSN\SavedUsers	Windows Live ID
HKCU\ControlPanel\Home\CurBgImageName	Home screen background image
HKCU\Comm\EAPOL\Config	WiFi access point information

Examining E-mail and MMS Remnants

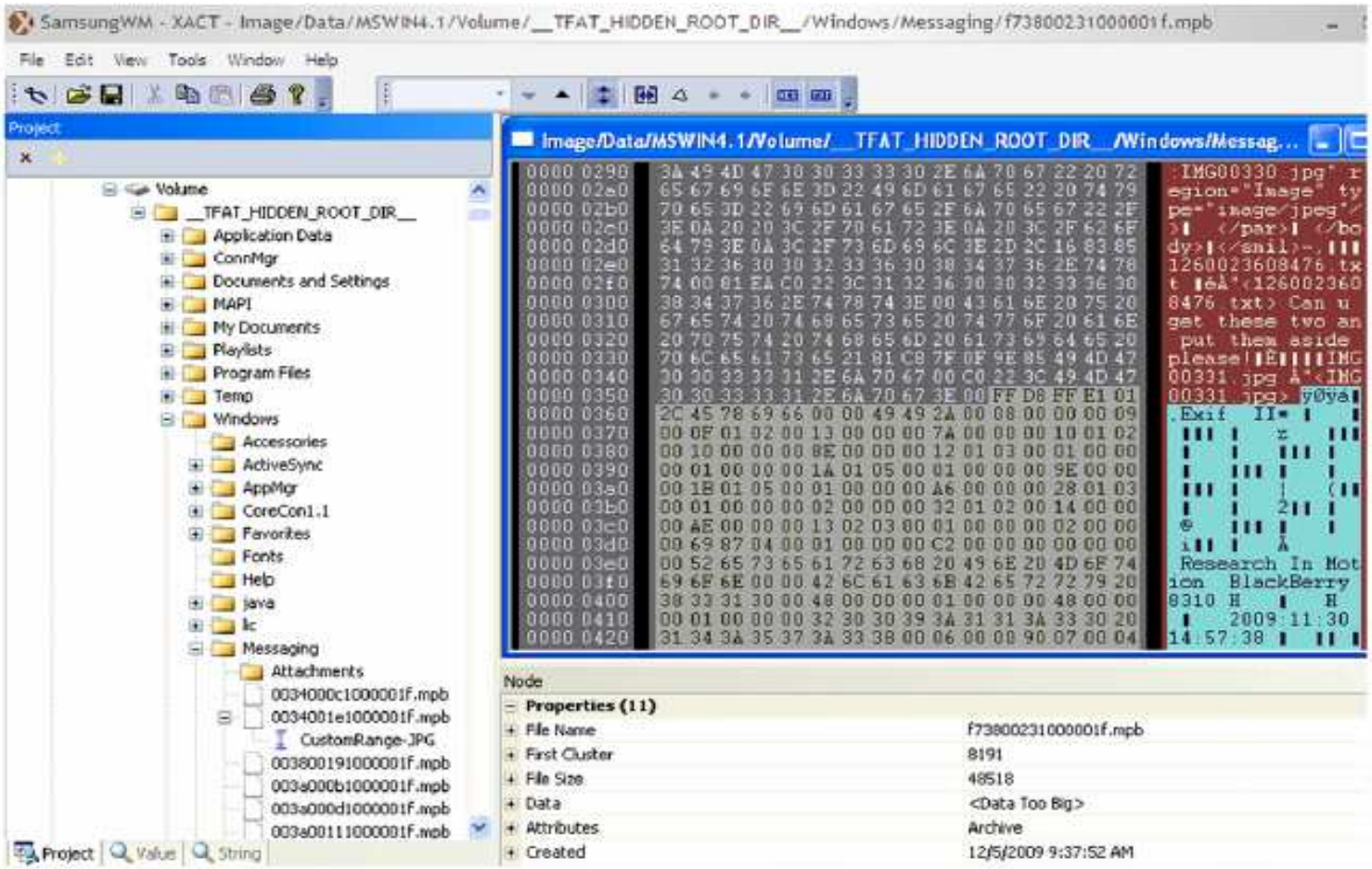


Fig. 8 – Message contents on a Windows Mobile device that contains a digital photograph with embedded EXIF header details from a Blackberry.

Examining E-mail and MMS Remnants

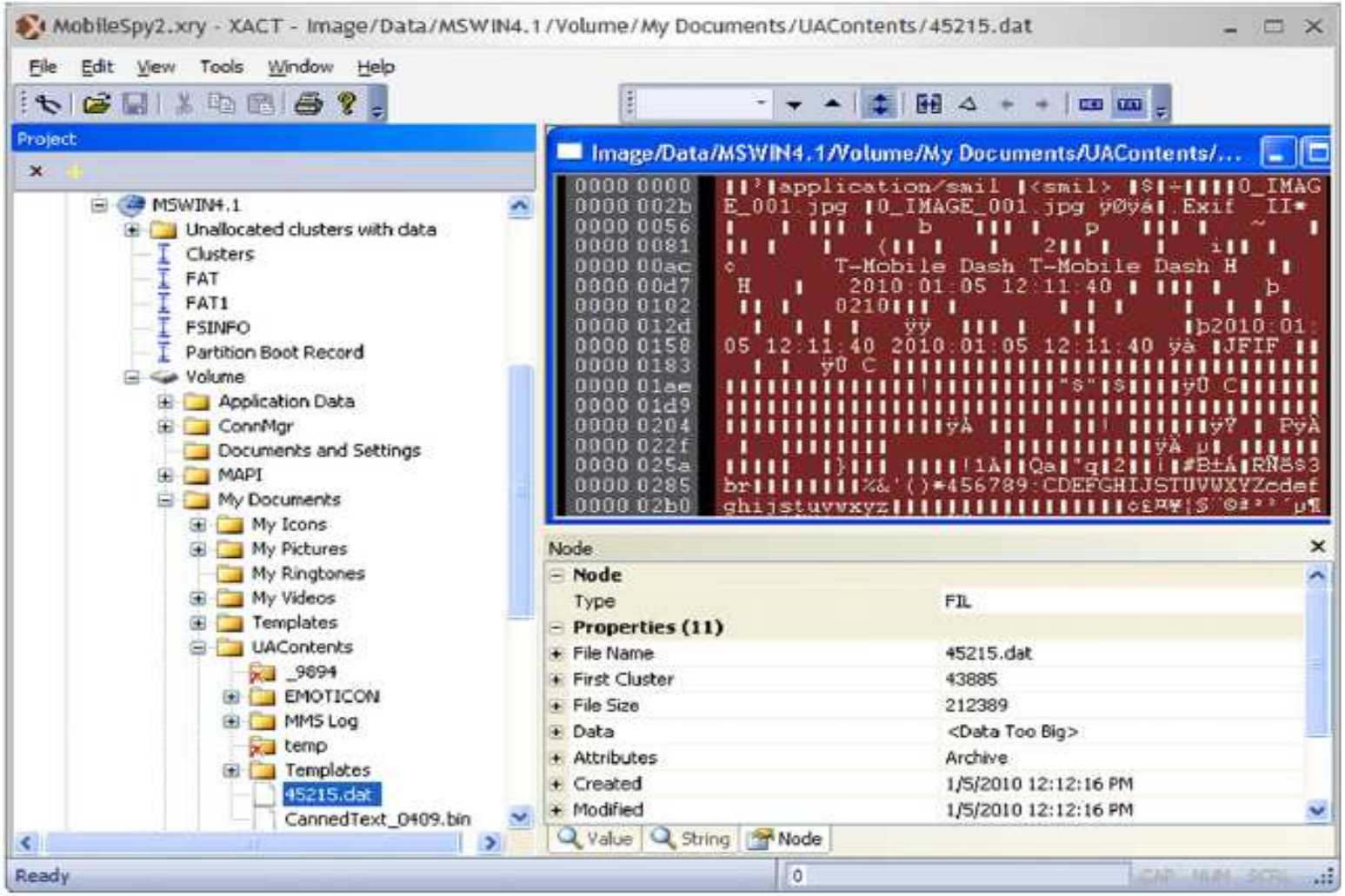


Fig. 9 – Example ".dat" file containing data associated with a sent MMS message.

Malicious Eavesdropping Case Study

Fig. 10 – MobileSpy Web site showing SMS traffic on a monitored device.

Malicious Eavesdropping Case Study

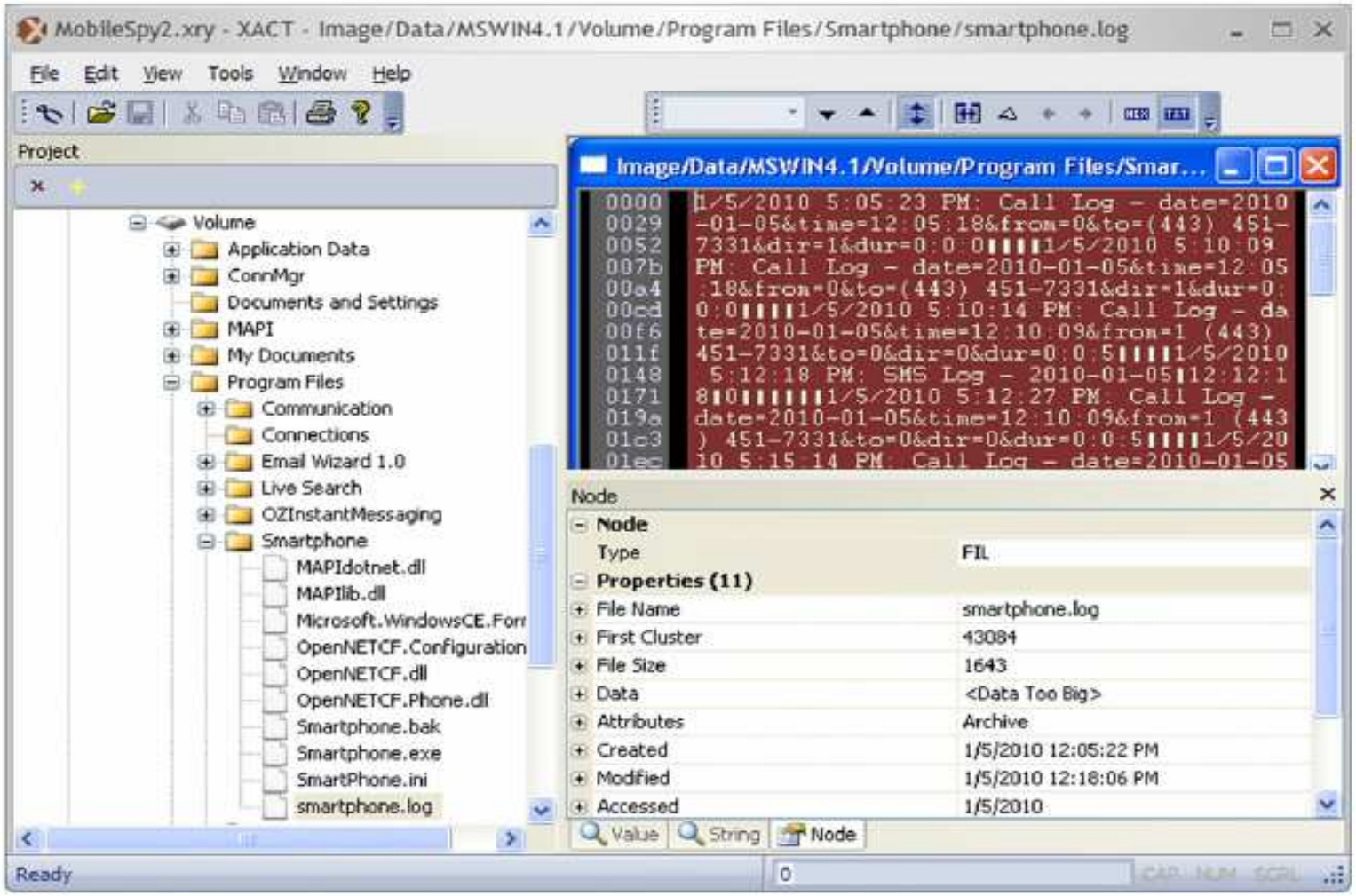
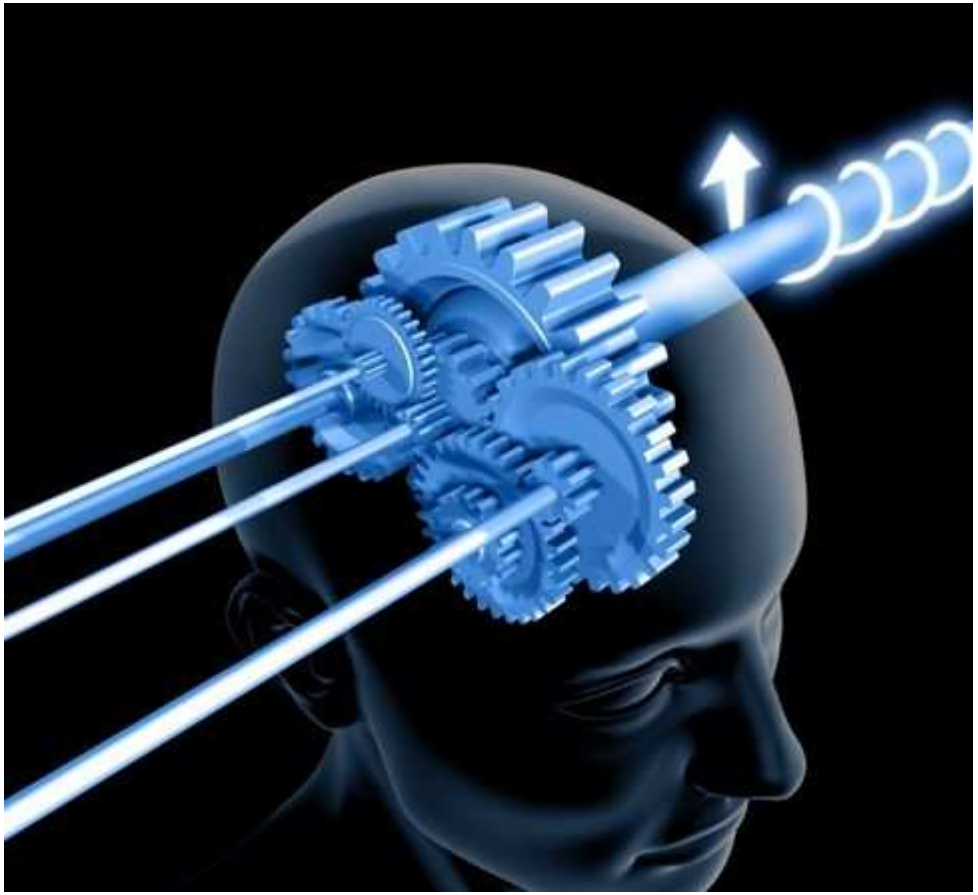


Fig. 11 – MobileSpy program installed in "Program Files\Applications\Smartphone" with "smartphone.log" file recording activities on the device.

Conclusions

- As Windows Mobile devices become more prevalent, there is a growing need for forensic analysts who can acquire evidence from these devices.

Discussion



QUESTION ?