

Mobile Device Forensics

GCFA Gold Certification

Author: Andrew Martin, [andrewjasm@gmail.com](mailto:andrewjasm@gmail.com)

Advisor: Joey Niem

Accepted - August 29, 2008

**Table of Contents**

Abstract.....	4
Devices.....	5
Tools - General.....	5
Motorola Razr V3C.....	8
Scenario.....	8
Tools.....	9
Techniques.....	10
Verification.....	10
System Description.....	11
Evidence Acquisition.....	11
Dumping Memory.....	12
Accessing the File System.....	14
Accessing the Phone via AT Commands.....	15
Analysis.....	18
Security Lock.....	18
Phone Book.....	20
SMS Messages.....	24
SIM Card - phonebook & SMS messages.....	27
Recent Calls.....	29
Calendar.....	32
Web Browsing.....	33
Multimedia.....	34
Other Artifacts.....	34
Conclusion - Razr.....	35
Blackberry 8700r.....	37
Scenario.....	37
Tools.....	39
Techniques.....	39
Verification.....	39
System Description.....	40
Evidence Acquisition.....	40
Blackberry Enterprise Server Considerations.....	41
Acquisition Scenarios.....	41
Content Protection.....	43
Analysis.....	44
IPD file on Windows.....	44
Obtaining Data with Barry on Linux.....	51
Conclusion - BlackBerry.....	55
Coby MP3 Player.....	57
Scenario.....	57
Tools.....	58
Techniques.....	59

Verification..... 59  
System Description..... 60  
Evidence Acquisition..... 60  
Analysis..... 62  
Conclusion MP3 Player..... 66  
Final Conclusion..... 67  
Challenges..... 67  
Tools and Techniques..... 68  
Direct References..... 70  
Other References Accessed & Used..... 72

## Abstract

The world of mobile device forensics is a complicated one. There are countless manufacturers of mobile devices, unlike the PC world's limited number of major operating system vendors. To complicate things further, each mobile device manufacturer may have their own proprietary technology and formats. Add to this the fact that new mobile devices such as cellular phones and personal digital assistants (PDAs) are released at a blistering pace and you have a challenging environment to work in.

This research paper will document in detail the methodology used to examine mobile electronic devices for the data critical to security investigations. The methodology encompasses the tools, techniques and procedures needed to gather data from a variety of common devices.

Consider that more and more people are using mobile devices in their day to day lives. An average consumer may use several of the following items:

- Cellular Phone
- Smart Phone
- MP3 Player
- Digital Camera
- External USB Drive

All of these devices could potentially carry data and thus would be targeted by an investigator for analysis. The following section describes each mobile device that will be discussed in this document.

Andrew Martin

## Devices

In order to cover the range of mobile devices available today, this paper will analyze three different types.

- Cellular Phone - Motorola Razr V3
- Smart Phone - Blackberry 8700r
- MP3 Player - Coby 1GB - MP550

The Razr is a traditional cellular phone which possesses many of the standard features we have come to expect.

The Blackberry is a smart phone which has become a standard device for many business people. Recently, Research In Motion has expanded into the high end consumer market with models that include additional multimedia features.

MP3 players are capable of storing vast amounts of data for their size. This makes the Coby MP550-1G a good candidate to round out our list of mobile devices.

## Tools - General

The boom in mobile devices has led to the challenges of how to analyze their data quickly and effectively. There are no free tools that are capable of analyzing every single phone on the market. Several vendors have surfaced in an attempt to fill the need of a common analysis

platform for the many different phone manufacturers and models.

"The variety of forensic toolkits for cell phones and other handheld devices is diverse. A considerable number of software tools and toolkits exist, but the range of devices over which they operate is typically narrowed to distinct platforms for a manufacturer's product line, a family of operating systems, or a type of hardware architecture." (National Institute of Standards and Technology, 2005, p. 8)

These tools are highly capable, and also highly expensive. To remain vendor neutral, all tools covered in this document are either freeware or trialware.

As is common in the computer world, there is always more than one way to accomplish a task. Analyzing mobile devices is no different. For example, there are numerous ways to extract the contents of the phonebook from a cellular phone. In order to truly understand the underlying technologies of these devices, this paper will focus on non-automated techniques for data recovery and analysis. Understanding how to perform these tasks using several different methods gives the reader the fundamental knowledge needed to investigate and solve problems.

There are many tools used in this paper which output their data as text. To better illustrate the commands issued and the output displayed, the following format is used:

**Command**

*Output*

## Motorola Razr V3C



### ***Scenario***

(This scenario is fabricated for the purposes of this paper)

A suspicious vehicle is pulled over for speeding on a local highway. The officer who pulled the speeder over notices that the driver is acting strangely as he approaches the vehicle. While talking to the driver, the officer notices the man's eyes quickly darting to a bag that is poorly concealed under the passenger seat. The officer asks the suspect to exit the car, and checks the bag. There is a large amount of drugs in the bag. After questioning, it is believed the suspect was simply acting as a courier; however he is not telling the investigators anything. It is believed he is in contact with a distributor, who the police would like to apprehend.

After placing the suspect under arrest for drug possession, they confiscate his cellular phone (a Motorola Razr) and turn it over for analysis to determine who the contact is and when the driver was supposed to meet him.

### **Tools**

The Motorola Razr uses Motorola's own file system and operating system (OS), which make it a challenge to analyze. Thankfully, there is a large community of hackers (in the classic sense) or modders that have written their own tools to interact with Motorola's file system. While most of the publicly accessible information on the Razr is geared towards making the most use of the functions of the phone, many of the same tools and information can be used to analyze the Razr's stored data.

The following tools are used to conduct our analysis of the Razr:

- P2K Commander 4.9.E
- Flash Backup 3.0.7 (Trialware) or Flash Backup 2.62 (Free)
- XVI32 (Hex editor)
- Strings (via cmd line or from iDefence malware analysis pack)
- HyperTerminal
- Motorola Drivers
- P2KToolsVS

## **Techniques**

This paper will document how to obtain all the necessary data using both GUI tools and AT commands from HyperTerminal.

It should be noted, that while this analysis is being conducted on a specific phone, the tools and techniques are portable across many different devices. Interacting with a phone using AT commands is universal for CDMA/GSM phones although with there are differences. P2k Commander and Flash & Backup are both usable on most models of Motorola phones.

## **Verification**

Before commencing with any investigation the first step is to initiate documentation.

Basic verification can be performed on this device to ensure the correct phone is being analyzed. The suspect's phone was on at the time it was confiscated so to confirm his phone number, we can simply navigate to Menu -> Settings -> Phone Status -> My Mobile Numbers -> TELEPHONE (View). This displays the number assigned to the phone, 647-123-4567. The main screen also displays "Rogers" which is the suspect's carrier. A query to Rogers for the name of the account owner for 647-123-4567 yields the suspect's name. Even if the phone was off, it can be powered on to retrieve this information.

## ***System Description***

Now that the device in question is known to be the suspect's, the gathering of key information continues. It only takes a few minutes to note the following:

Date / Time device was taken from suspect: June 1<sup>st</sup>, 2008 at 4pm

Make: Motorola

Model: V3 (g8.5/9/18/19)

S/W Version: 0E:40.7CR

IMEI: 354904001234567

SIM: 89302720123456781234

Carrier: Rogers

Phone Number: 647-123-4567

## ***Evidence Acquisition***

Acquiring a physical copy of the phone's memory is a challenging task. From the tools we have at our disposal, none will make a reproducible hash of the phone's memory contents. Hashing a file is used to validate its integrity. Hashing algorithms are used to create a reproducible string of characters that can be used to validate if a file has changed or not.

Flash Backup can make a copy of memory, however since the phone's memory must be dumped while it is running; its contents are in a constant state of flux. A reproducible hash may not be generated in this case. There are three ways to acquire evidence from the Razr. These are: a memory dump, direct access to the file system and via AT commands.

Andrew Martin

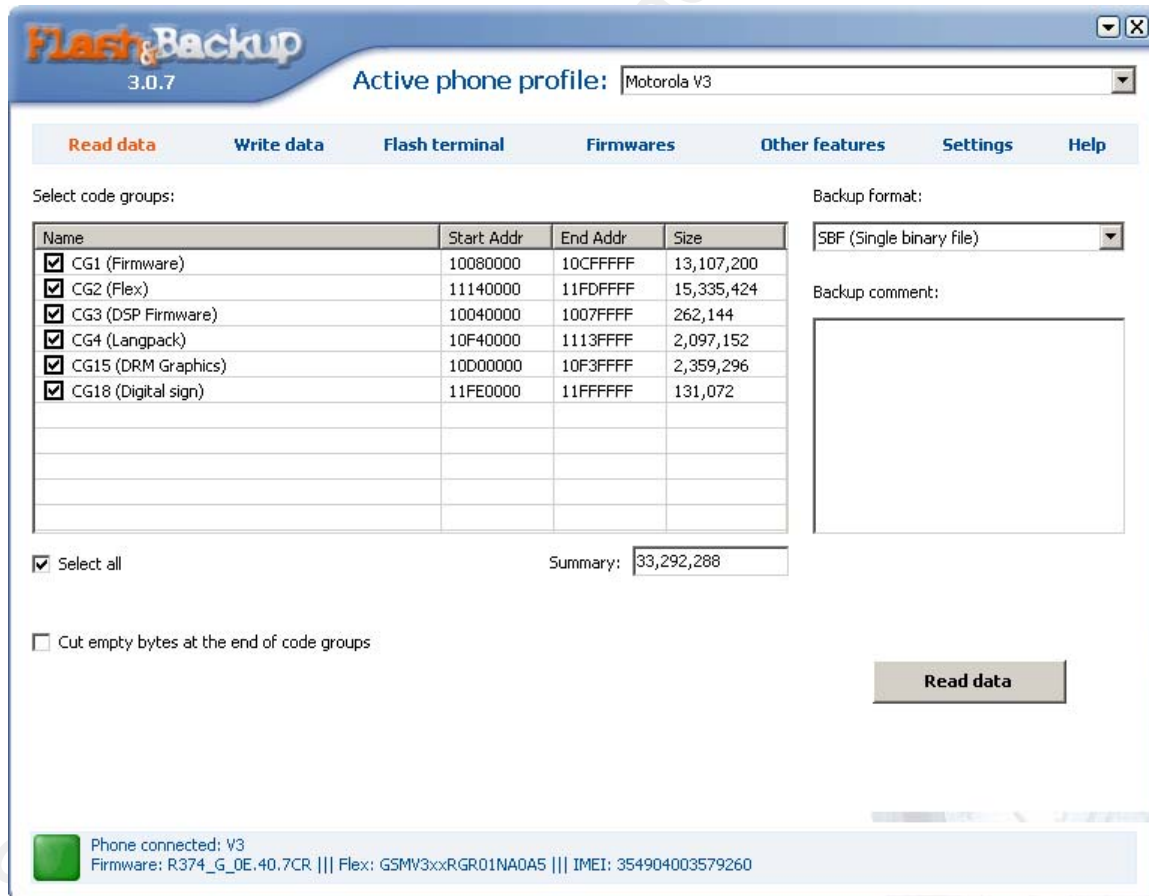
11

We will cover dumping memory in detail in this section, with brief introductions to the file system and AT commands. Individual files and AT commands will be covered in depth in the media analysis phase.

### Dumping Memory

Flash and Backup presents an easy to use GUI for performing memory dumps on Motorola devices.

Figure 1 - Phone connected in Flash & Backup 3.0.7



To create a backup memory dump select "Read Data", check "select all", uncheck "Cut empty bytes at the end of

code groups" and select either "SBF" (Single Binary File) or "SMG" (Binary Files).

SBF will create a single large file and SMG will create a separate file for each of the 6 memory regions. For analysis of the device, only the CG2 region (Flex) is needed, however all the sections can be backed up for completeness.

The regions are as follows:

CG1 (Firmware) - Contains the hardware level operating system of the phone. There is minimal relevant data to investigation in this section. But having a backup of it would be useful in case there is a need to fully restore the phone.

CG2 (Flex) - The Flex area contains the applications and data on the phone. This is the area we will be analyzing.

CG3 (DSP Firmware) - Contains the Digital Signal Processor firmware. The DSP processes audio so that conversations can occur in real time.

CG4 (Langpack) - This area contains the fonts used by the phone. In this case, the language pack will contain English fonts.

CG15 (DRM Graphics) - This section contains all the icon files used on the Razr phone (Battery indicator icon, signal bar icon, etc).

CG18 - (Digital Sign) - Contains the phone's digital signature

### **Accessing the File System**

A huge Motorola modding community has grown over the years as a result of the Razr's popularity. This has led to the creation of many file manager applications for the Paragon 2000 (P2K) file system. This document discusses the use of P2k Commander to recover data from the phone.

In order to use P2k Commander, the analyst machine must have the Motorola USB drivers installed.

USB Driver:

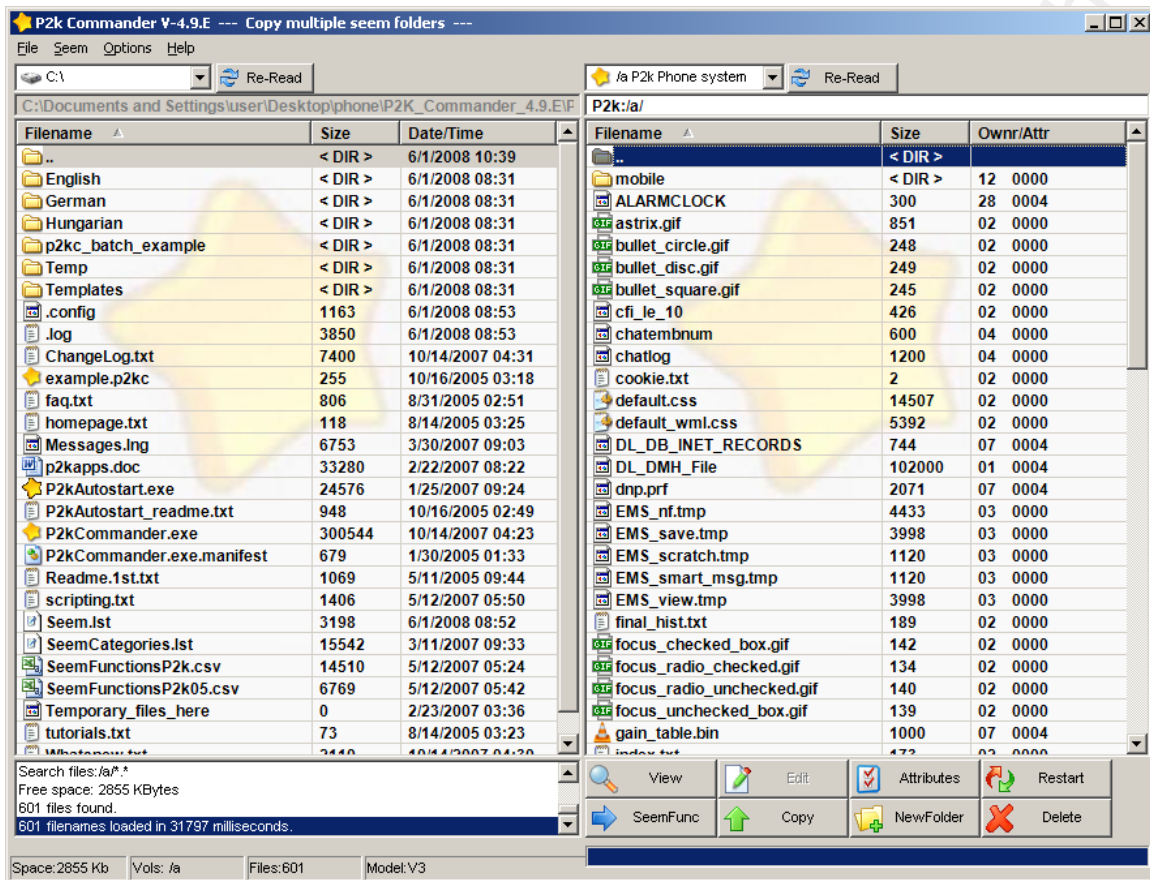
<http://direct.motorola.com/hellomoto/nss/driversNplugins.asp>

P2k Commander:

<http://handheld.softpedia.com/get/Developer-Tools/File-Manager/P2kCommander-38120.shtml>

Once the above files are installed, run P2k Commander with the phone connected. The program will take a minute to read all the files on the device in the /a directory. This is the root directory of the device where all files are stored. This is shown in figure 2 below.

Figure 2 - P2k Commander - Phone file listing



Ensure the left pane is pointing to a local hard drive, and the right pane is pointed to the /a folder of the phone.

### Accessing the Phone via AT Commands

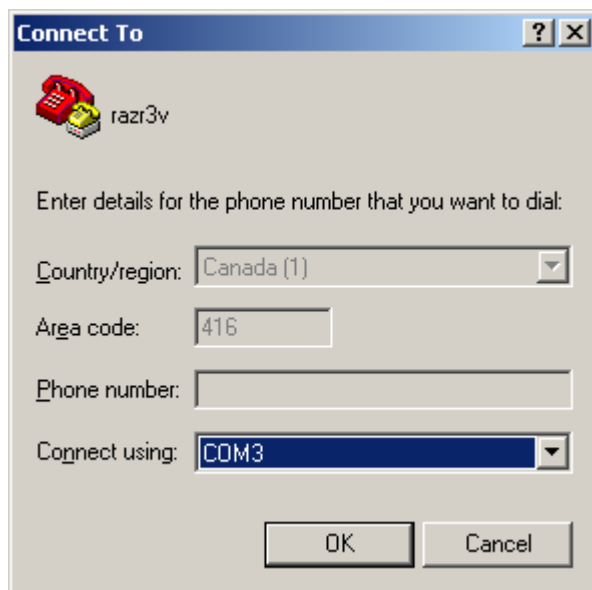
The most time consuming (yet strangely satisfying) method for accessing data from a phone is via AT commands. "AT commands are comprised of assemblies of ASCII characters which start with the "AT" prefix (except the commands A/ and +++). The AT prefix is derived from the word Attention, which asks the modem to pay attention to the current request (command)." (Motorola, 2008, p. 57) For

a comprehensive list of AT commands, refer to the following link (registration required).

[https://developer.motorola.com/docstools/developerguides/G24-L\\_AT\\_Commands\\_Final2\\_250909.pdf/](https://developer.motorola.com/docstools/developerguides/G24-L_AT_Commands_Final2_250909.pdf/)

To connect to the phone, use HyperTerminal, which comes with Windows. HyperTerminal can be found in the Communications folder under Accessories. Create a new connection and set it to COM3. This could vary depending on the phone system.

Figure 3 - Create phone connection



Once created, configure the connection with the following settings. See figure 4 below.

Bits per second: 115200

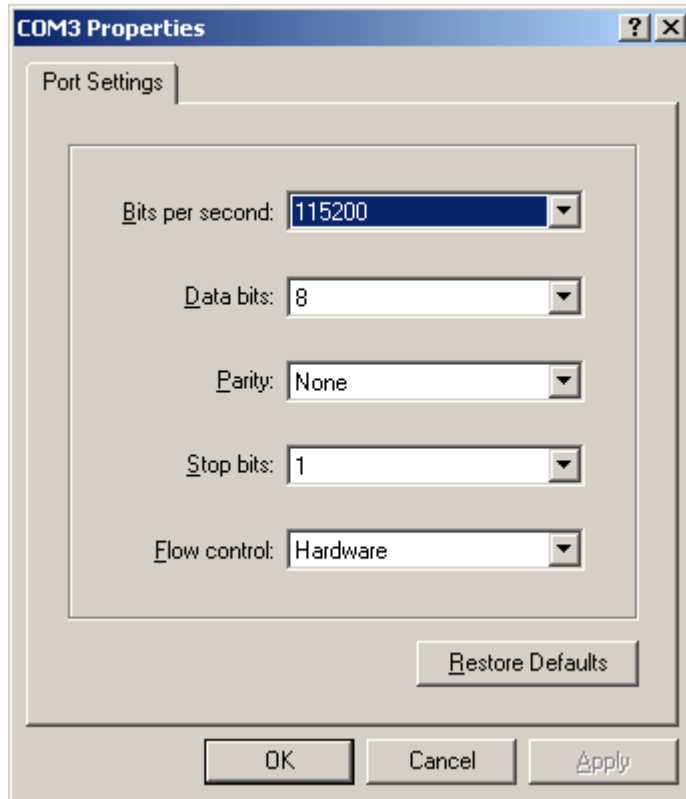
Data bits: 8

Parity: None

Stop Bits: 1

Flow control: Hardware

Figure 4 - Configure phone connection



With the connection set up properly, commands may now be issued to the phone. Connectivity can be tested by simply issuing the "at" command. AT commands are not themselves case sensitive, but their parameters are.

```
at[enter]
OK
```

Data may now be retrieved from the phone using various commands. These will be covered in subsequent sections.

## ***Analysis***

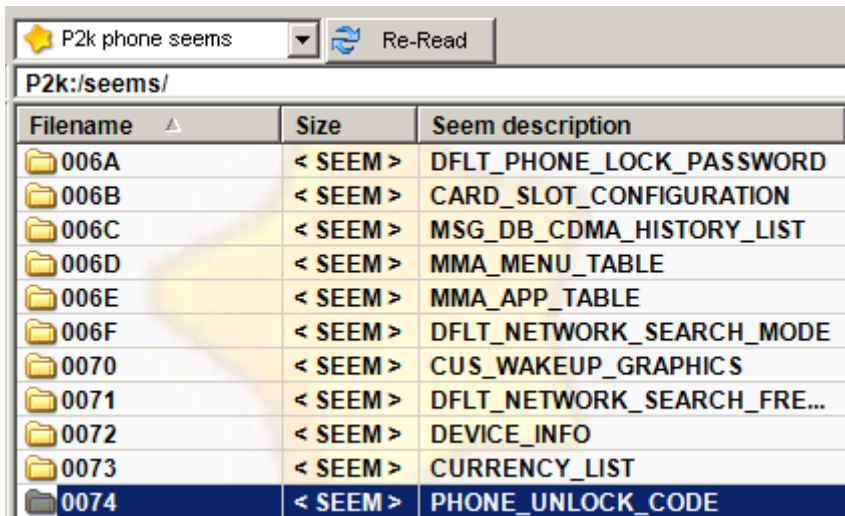
It is difficult to adhere to the standard forensic investigation methodology when analyzing a cellular phone as there is no timeline to create. The media analysis, string search, and data recovery phases are continuous in each section that follows in the analysis section.

### **Security Lock**

There is always the possibility that a phone is locked and the analyst needs to navigate around the phone's GUI (keeping in mind that the investigator is changing data on the device). In the Razr's case, the phone lock does not block access to the file system. We will use P2k Commander to extract the portion of memory that contains the lock code.

The Razr uses "SEEMS" to store basic configuration settings for the phone in memory. The SEEM that contains the phone lock code is 0074, shown in figure 5 below. Using p2kcommander, change to the /seems directory and copy seem 0074 to our machine.

Figure 5 - Unlock code



Filename	Size	Seem description
006A	< SEEM >	DFLT_PHONE_LOCK_PASSWORD
006B	< SEEM >	CARD_SLOT_CONFIGURATION
006C	< SEEM >	MSG_DB_CDMA_HISTORY_LIST
006D	< SEEM >	MMA_MENU_TABLE
006E	< SEEM >	MMA_APP_TABLE
006F	< SEEM >	DFLT_NETWORK_SEARCH_MODE
0070	< SEEM >	CUS_WAKEUP_GRAPHICS
0071	< SEEM >	DFLT_NETWORK_SEARCH_FRE...
0072	< SEEM >	DEVICE_INFO
0073	< SEEM >	CURRENCY_LIST
0074	< SEEM >	PHONE_UNLOCK_CODE

Using XVI32 or Strings we can quickly discern that the unlock code is "1111". See figure 6 below for the output using Strings. Figure 7 illustrates the same data using XVI32.

Figure 6 - Strings output of SEEM 0074

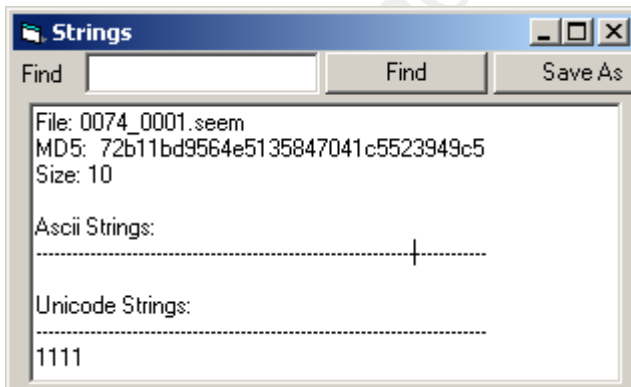
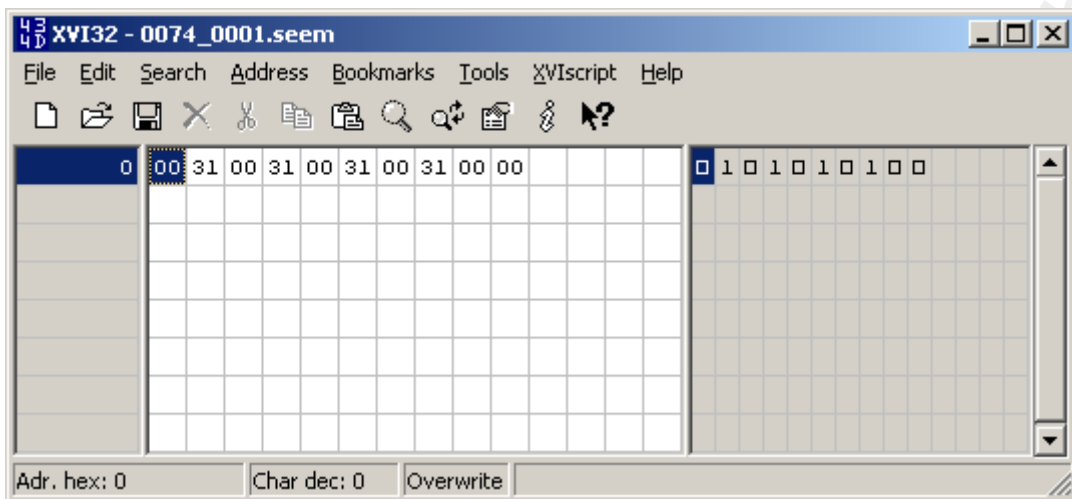


Figure 7 - hex view of SEEM 0074 using XVI32



Looking ahead in this paper we will cull additional data from SEEMS as we continue our analysis. The phone may now be unlocked using "1111" as the unlock code. Note that data is stored in the phone as both ascii and Unicode. Unicode uses two bytes to represent a character which allows for an extended character set for other languages. The above unlock code is stored as 4 2 byte Unicode characters.

### Phone Book

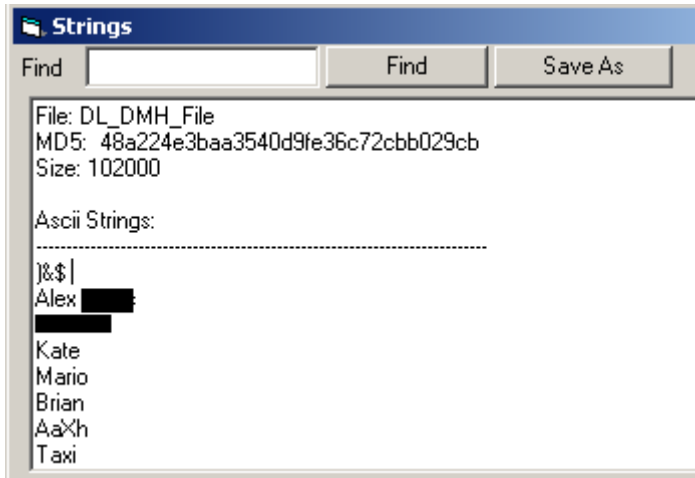
The phonebook may be accessed by both the file system and AT commands. Both techniques are covered below. The Razr is also capable of storing phone book entries in the phone's SIM card.

#### Phonebook via file system

By copying all the files from the phone's /a/mobile directory to our analysis workstation, it does not take long before a file with a series of names becomes apparent.

Simply by running strings on each file, it is apparent that the DL\_DMH\_File is the phone book.

Figure 8 - Contents of DL\_DMH\_File

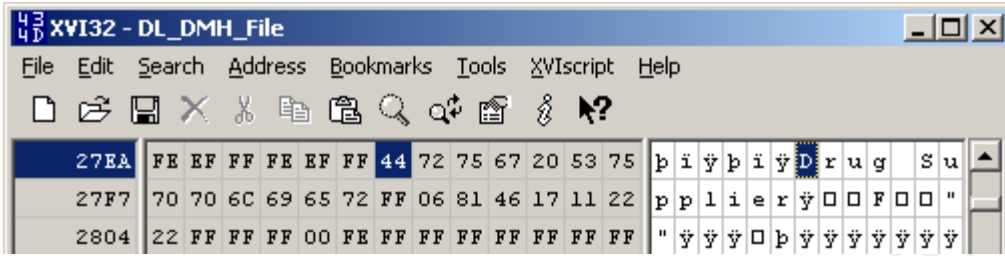


Closer inspection with XVI32 yields the data we need, names and phone numbers of all the contacts in the phonebook. There happens to be an entry for a contact called "Drug Supplier" (this was made overly obvious for the purpose of the paper).

The phone number is stored in reverse on the Razr. From the output in figure 9, the number begins at address 27FF.

```
81 46 17 11 22 22
18 64 71 11 22 22 or 647-111-2222
```

Figure 9 - Hex view of DL\_DMH\_File



It should be noted that this phone book entry was made recently as it is the latest entry in the file. For this device as new entries are added, they are appended to the end of the file.

## Phonebook via AT commands

```

at
OK

at+cpbs=? //Query the phone for its available phonebooks
+CPBS:
("ME","SM","MT","ON","DC","MC","RC","EN","AD","QD","SD","FD"
)
OK

at+cpbs=mt //Select the MT (merged) phonebook for the
Combined G24-L and SIM phone book
OK

at+cpbr=? //Get the index of the contents of the MT
phonebook
+CPBR: (1-1250),40,18
OK

at+cpbr=1 //From the above output we know there are up to
1250 entries available. The output of selecting entry one
is below

+CPBR: 1,"647XXXXXXX",129,"Dan"
OK

```

This series of commands has returned the first phonebook entry. Below is a detailed breakdown of the returned entry.

Command	Index number	Phone Number	Address Type (129 is a local call)	Name
+CPBR:	1,	,"647XXXXXXX",	129,	"Dan"

To list more than one phonebook entry, we give the cpbr command a range of values.

```
at+cpbr=1,100 // Returns the first one hundred entries
[removed]
+CPBR: 64,"416 XXXXXXXX ",129,"Joey"
+CPBR: 65,"416 XXXXXXXX ",129,"Parking"
+CPBR: 66,"416XXXXXXXX",129,"Other Taxi"
+CPBR: 67,"6471112222",129,"Drug Supplier"

OK
```

It would appear there are 67 entries in the phonebook, and as we saw earlier, the last entry is for a contact by the name of "Drug Supplier".

### **SMS Messages**

Another gold mine of information, SMS messages can yield vital data to an investigator. While conducting analysis on the Razr, we will see that old messages are still recoverable.

There are some subtle nuances with the way SMS messages are stored. Messages in the Inbox are stored on the SIM card of the phone (by default, but this can be changed). The Quick Notes, Outbox and Drafts are saved in the phone's memory.

### **SMS Messages via File System**

To copy the messages from the phone to the analysis PC, simply copy SEEM 007D in P2k Commander.

Andrew Martin

Figure 10 - SMS SEEM

Filename	Size	Seem description
007D	< SEEM >	SHORT_MESSAGE

This will output a series of files from 007D\_0001 to 007D\_009F. SEEMs 007D\_0001 to 007D\_000A contain the quick notes. Once copied, the files can be searched for data with the strings command. Since we know the suspect had contact with someone at 647-111-2222, it is easy to search for messages sent to this number.

```
C:\messages3>strings * | findstr "6471112222"
C:\messages3\007D_000B.seem: _6471112222

C:\messages3>strings 007D_000B.seem

_6471112222
"When can i pick up the stuff"
```

The output contains the phone number the message was sent to and the message that was sent. Note that messages may span across multiple SEEMs. They will be stored in an adjacent SEEM as seen below.

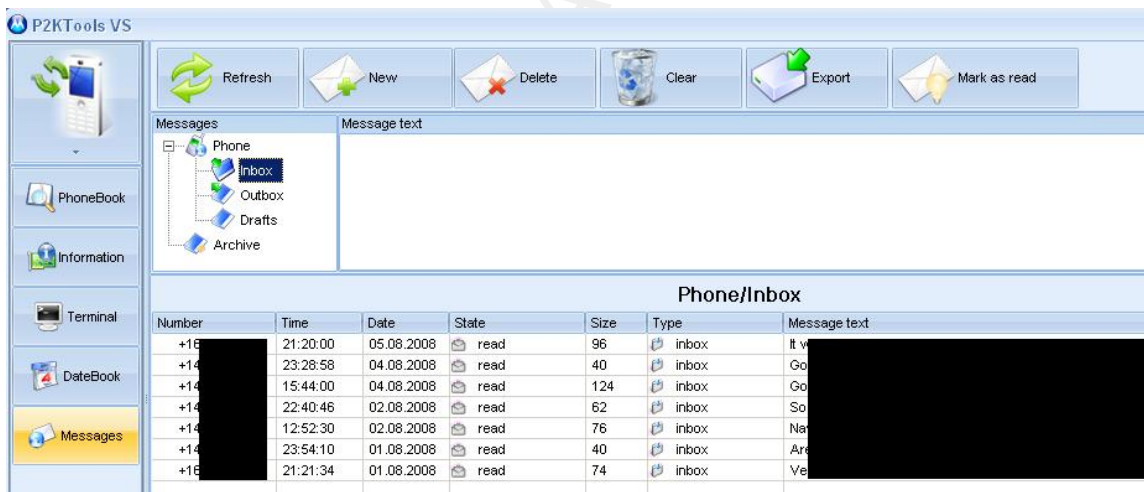
```
C:\messages3>strings 007D_0022.seem
+16474XXXXXX
Im getti
```

```
C:\messages3>strings 007D_0023.seem
+17057969301**
n in a cab shortly
```

\*\*I am not certain what this 705 number is. It appears to be added to the end of any message that spans multiple SEEMs.

Another tool, P2KToolsVS is able to extract the date and time a SMS message was received. P2KToolsVS is similar to P2k Commander in that it is able to access the phone's file system.

Figure 11 - Viewing received messages using P2KToolsVS



### SMS Messages via AT Commands

To read the output of the following commands, we must first put the phone into text mode, otherwise the message output will be in PDU format.

```
at+cmgf=1 //Put phone in text mode
OK
```

```

at+cmgl=? //Display available parameters to list messages
+CMGL: ("REC UNREAD", "REC READ", "STO UNSENT", "STO SENT",
"ALL")
OK

0 "REC UNREAD", received unread message (for example, new
message).
1 "REC READ", received read message.
2 "STO UNSENT", stored unsent message.
3 "STO SENT", stored sent message.
4 "ALL", all messages (default).
(Motorola, 2008, p. 154)

at+cmgl="STO SENT" //List all stored sent messages
+CMGL: 2052, "STO SENT", "+1416XXXXXXX"
Grats :)
+CMGL: 2041, "STO SENT", "+1647XXXXXXX"
Im gettin in a cab shortly

```

To compare the two methods, we are able to recover deleted data using the file system method by accessing SEEM 007D. This method did not capture received messages as these are stored on the SIM card by default. By issuing AT commands we are only able to see the messages that are currently available in the handset's GUI. However, the messages are neatly organized into groups and messages are readable from the SIM card.

### **SIM Card - phonebook & SMS messages**

A Subscriber Identity Module (SIM) card is used in all modern cellular phones. These modules uniquely identify the

user on a provider's network and are used to store small amounts of information. For investigative purposes, we are interested in the phonebook entries and SMS messages that are stored on the card. This data is stored on the card for portability between devices.

To access the data on a SIM card, a special SIM card reader is required. For the purposes of this paper, I purchased an \$8 SIM card reader from a merchant on the Internet.



The software provided with the device was able to read the SIM card and display the phonebook entries and SMS messages. See figure 12 below.

Figure 12 - Contents of SIM SMS messages

NO.	Status	From	Content
1	InBox	+164	I'm
2	InBox	+164	Oh
3	InBox	+164	We
4	InBox	+164	Ya
5	InBox	+141	Kk
6	InBox	+141	Sw
7	InBox	+164	See
8	InBox	+164	Alin
9	InBox	+141	I ha
10	InBox	+141	Ok
11	InBox	+141	Are
12	InBox	+141	Are
13	InBox	+141	He
14	InBox	+141	Frid
15	InBox	+141	Yo
16	InBox	+141	I jus
17	InBox	+164	Ton
18	InBox	+164	Soc

It is also possible to recover deleted SIM card data for investigative purposes. Unfortunately the reader I purchased was not supported by tulp2g which is one of the only open source tools capable of this task. Any PC/SC card reader is supposed to work, but a GemPC reader is preferred.

## Recent Calls

### Recent calls via file system

Both received and dialed calls are available from the phone's file system in SEEM 0038 and 0039. XVI32 can then be used to explore their contents.

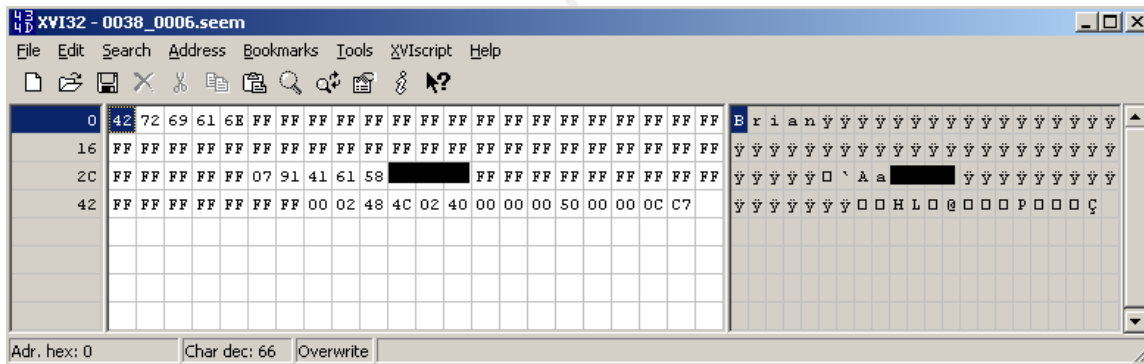
Figure 13 - Recent calls via P2k Commander

Filename	Size	Seem description
0037	< SEEM >	QUICK_DIALING
0038	< SEEM >	RECENT_CALL_RECEIVED
0039	< SEEM >	RECENT_CALL_DIALED

The first section of the file contains the caller name, "Brian". The second section contains the phone number which has been reversed. See figure 14 below.

```
41 61 58 XX XX XX
1 416 85X XXXX
```

Figure 14 - Example call received



There is more data at the end of the file which may represent the time and date of the call, however I have not been able to determine the format used. This information is not documented by Motorola.

**Recent calls via AT commands**

Recent calls are stored in the phonebook and are easily accessed using some of the commands covered above.

```

at+cpbs=? //Query the phone for its available phonebooks
+CPBS:
("ME","SM","MT","ON","DC","MC","RC","EN","AD","QD","SD","FD"
)
OK

```

```

AD Abbreviated dialing numbers.
DC ME dialed calls list
EN SIM emergency numbers
FD SIM Fixed dialing phone book.
MC G24-L missed
ME G24-L phone book.
MT Combined G24-L and SIM phone book.
ON SIM own numbers (MSISDNs) list
QD Quick dial phone book.
RC G24-L received calls list
SD Service dialing numbers.
SM SIM phone book.
(Motorola, 2008, p. 123)

```

```

at+cpbs=RC //Enter received calls list
OK
at+cpbr=? //Read received calls
+CPBR: (1-10),40,24
OK
at+cpbr=1,3 //Read the last three received calls
+CPBR: 1,"+164799XXXXX",145,"Ed"
+CPBR: 2,"+141685X8XXXXX",145,"Brian"
+CPBR: 3,"+141659XXXXX",145,"Lobby"

```



First, we must lock access to the calendar using the following command.

```
at+mdbl=1 //block access to calendar from GUI
OK

at+mdbr=? //display calendar information, the second entry
(1) indicates the number of calendar entries
+MDBR: 500,1,64,8,2
OK

at+mdbr=0 //display the first calendar entry
+MDBR: 0,"Buy some drugs from supplier -
sans",1,0,"17:00","06-15-2008",60,"00:0
0","00-00-2000",0

OK
```

See <http://ab.id.au/MotorolaATCommands> for field descriptions. It looks like we've found another useful piece of information for the investigation.

## Web Browsing

The Razr also has basic web browsing capability which should be analyzed during an investigation. There are several files on the device which may contain information on the subject which are set out below. These files are accessed via P2k Commander.

/a/cookie.txt - browser cookies

/a/final\_hist.txt - browsing history

Andrew Martin

/a/mib\_vlh - also contains browsing history  
/a/uaprof\_url.txt - xml file that describes the web browser. Also contains a sample user agent string for the phone: MOT-V3/xx.xx.xxR MIB/2.2.1 Profile/MIDP-2.0 configuration/CLDC-1.0

## **Multimedia**

Multimedia content is only accessible via the file system and is located in several folders under /a/mobile/. P2k Commander can be used to copy the content off the phone for analysis. Below are some examples:

P2k:/a/mobile/picture/ - pictures taken with phone's camera (640x480)

P2k:/a/mobile/audio/

P2k:/a/mobile/mms/ - multimedia messages

P2k:/a/mobile/video/

## **Other Artifacts**

The Razr's file system contains other interesting data that does not fall into the above categories. These will be discussed briefly.

/a/iTAP\_User\_Dictionary/

This file contains all the words that have been entered by the user that are not in the phone's dictionary. This file can provide valuable information to an investigator if the subject uses text messaging extensively. This dictionary will store things like slang,

email addresses and names of places. The contents of this file would be useful to include in a dirty word list.

/a/EMS\_save.tmp

/a/EMS\_view.tmp

Both of these files may contain partial text messages which are stored in Unicode.

/a/chatlog

The Razr also has basic chat capability and this file is used to keep a log of the received messages.

### ***Conclusion - Razr***

Gathering data from the phone via AT commands and the phone's file system has proven very effective. We have been able to uncover a great deal of information without the use of vendor specific tools. For our sample scenario, the author has uncovered that the suspect's phone contained the following:

- A contact in the phonebook for "Drug Supplier"
- The phone number for this individual is 647-111-2222
- The date and time of their next meeting - June 15<sup>th</sup>, 5PM

This information can be used to search through the phone for additional evidence or as key reference material in an interview with the suspect. If the suspect had a PC

which was seized as well, this information can be used to conduct a more targeted investigation of the computer.

## BlackBerry 8700r



### *Scenario*

Consider the following scenario; an employee at a large company has approached HR regarding inappropriate messages and phone calls they have received from a co-worker. In order to confirm the unwanted behavior, management authorizes the analysis of the harasser's BlackBerry, which is issued by the company for business purposes.

Management does not want to alert the subject in question or other staff to the investigation. A note is sent to that group's manager explaining that their group is being targeted for BlackBerry firmware updates. A member of the desktop support staff is dispatched to each PC. The staff member asks each user to enter their PIN so that the

Andrew Martin

device may be backed up. It is explained that a backup is needed just in case the firmware update does not go smoothly.

All backups are copied to a network share and the .IPD file associated with the subject in question is taken for analysis.

## ***Tools***

There are many tools that can be used to perform an investigation on a BlackBerry. The basic tools like a hex editor and the strings command are pretty much standard for examining any device. A BlackBerry can be very easy to analyze, or extremely challenging depending on what state it is in. The states are discussed in the acquisition section.

The following tools are used:

- BlackBerry Desktop Manager 4.2.1
- ABC Amber BlackBerry Converter 6.45
- Strings
- XVI32
- OpenSync
- Barry

## ***Techniques***

To analyze the BlackBerry, we use two methods. The first will be to analyze a .ipd backup file and the second will be to analyze the device interactively via Barry with OpenSync in Linux.

## ***Verification***

Verification is fairly simple; there are several pieces of information to collect.

- The phone number of the device is viewable from the Call Log application, note "My Number".
- The owner might have entered their name and other personal information under Options -> Owner.
- The PIN and IMEI are obtainable from Options -> Status
- The SIM ID is located under Options -> Advanced -> SIM Card.

### ***System Description***

In addition to the information obtained in the verification phase, there are several other items to note before diving into the investigation.

- All installed applications are listed under Options -> Advanced Options -> Applications
- The model number and MAC address are located under the battery on the back of the unit
- The device firmware version is available in Options -> About

### ***Evidence Acquisition***

In order to discuss how data can be acquired from a Blackberry, we first have to obtain a understanding of the Blackberry Enterprise Server and the security technology built into the hand held unit.

## **Blackberry Enterprise Server Considerations**

The Blackberry Enterprise Server (BES) is a tool used to centrally manage an organization's devices. It has a number of features, but we will only discuss a few of these that are of particular interest to a security investigation. First, the BES has the ability to remotely lock, change the password or even erase a unit.

"Set a Password and Lock Handheld

This command creates a new password and locks a lost BlackBerry device remotely. You can communicate the new password to the user when the user locates the BlackBerry device. When the user unlocks the BlackBerry device, the BlackBerry device prompts the user to accept or reject the password change.

Erase Data and Disable Handheld

This command remotely erases all user information and application data that the BlackBerry device stores. You can use this command to prepare a BlackBerry device for transfer between users in your organization or to protect a stolen BlackBerry device."

(Research In Motion, 2008, p. 91)

## **Acquisition Scenarios**

When trying to obtain a Blackberry unit for investigation, it is important not to alert the suspect to

the investigative intentions. Without proper handling, an investigator could obtain a device for analysis, only to have it erased remotely because the suspect got suspicious, phoned the organization's helpdesk and told them their unit was lost.

Knowing this, there are the four possible scenarios to consider when obtaining a Blackberry.

- If the RIM is off, leave it off
- If the RIM is on, turn the radio off
- If the RIM is password protected, get the password

(Burnette, 2002, p. 4)

- \*If the device is password protected and you cannot get the password, put it in a Faraday Bag.

\*This is an additional scenario I have added.

Turning off the radio will prevent remote commands from reaching the device to lock or erase it. If the device is locked, it is not possible to disable the radio without the password. This leaves a window of opportunity for the suspect to have their device erased remotely. To mitigate this risk, the device can be placed in a Faraday Bag. According to Wikipedia (n.d), a Faraday Bag is similar to a Faraday Cage in that it prevents signals from reaching the device. Once safely inside a Faraday bag, the device can be transported to the analysis lab which would be contained inside a Faraday Cage. This would prevent any signals from reaching the device from the time of seizure to analysis.

If the unit is locked, there are a few options:

- Guess the password successfully in 10 tries (if unsuccessful the device will erase itself). This is not recommended!
- Obtain the correct password through other means: social engineering, interview, shoulder surf, etc.
- Reset the device's password via the BES (if the BES is controlled by the investigator)

### **Content Protection**

The Blackberry has an additional feature called content protection. With this security measure enabled, user data is protected with 256-bit AES encryption.

"When the content protection feature on the BlackBerry device is turned on, the BlackBerry device is designed to protect user data in the following ways:

- use 256-bit AES encryption to encrypt stored data
- use an ECC public key to encrypt data that the BlackBerry device receives." (Research in Motion, p. 34)

If the device uses firmware earlier than version 4.3, the password cannot be reset remotely on the device.

## ***Analysis***

Once the device is unlocked, we can proceed to the analysis phase. This section discusses two methods for obtaining data from the blackberry.

The first is via the .ipd file. An ipd file is a backup file created by the Desktop Manager application. Users have the ability to keep a backup of their data handy just in case they lose their device. The ipd files are also useful for upgrading from one Blackberry to another. This is because a backup can be taken from the old device and restored onto a new device. As with the Razr discussed earlier, an IPD file is collected with the device turned on. This means the contents of memory are constantly changing which will not result in a reproducible hash of the backup file.

The second method we will discuss is the use of the Barry and OpenSync tools to interactively view data on a live Blackberry.

### **IPD file on Windows**

An ipd file can be obtained in two different ways. Either it can be created directly from a device in the possession of an investigator or a copy could be obtained from the user's PC.

Consider the following scenario: The corporate user referred to earlier is being investigated, but they are away on vacation with their Blackberry in their possession.

One of the things an investigator can look for are .ipd files on the user's home or work PC and on the corporate network if the user has a home directory on it.

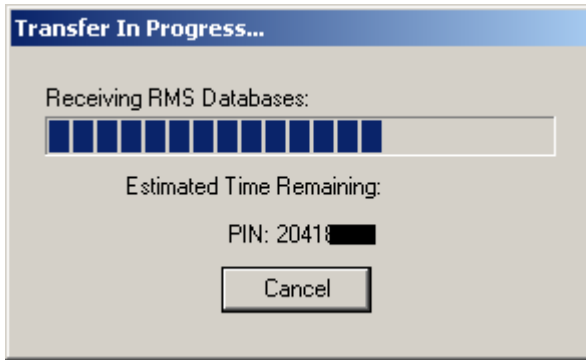
To obtain an ipd backup from a device, first install the BlackBerry Desktop Manager. See figure 16 below. The version of Desktop Manager used will depend on the version of the firmware loaded on the device. Simply select "Backup and Restore" -> Backup and choose a file name. The backup process will begin.

Figure 16 - Obtaining IPD backup



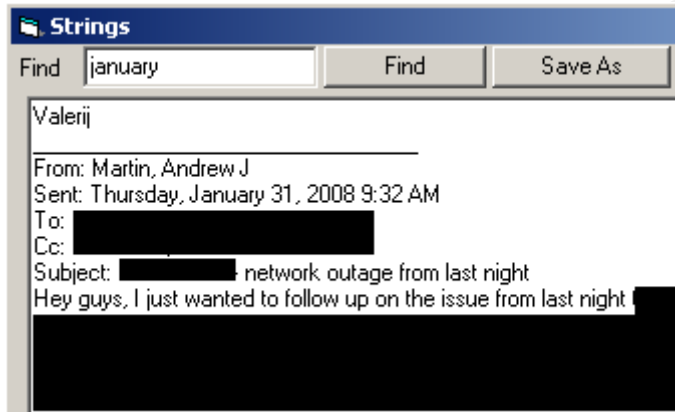
The status of the backup is shown below.

Figure 17 - Progress of IPD backup process



Once the backup is completed, we can take a quick look at it with strings.

Figure 18 - Strings output of newly created IPD backup



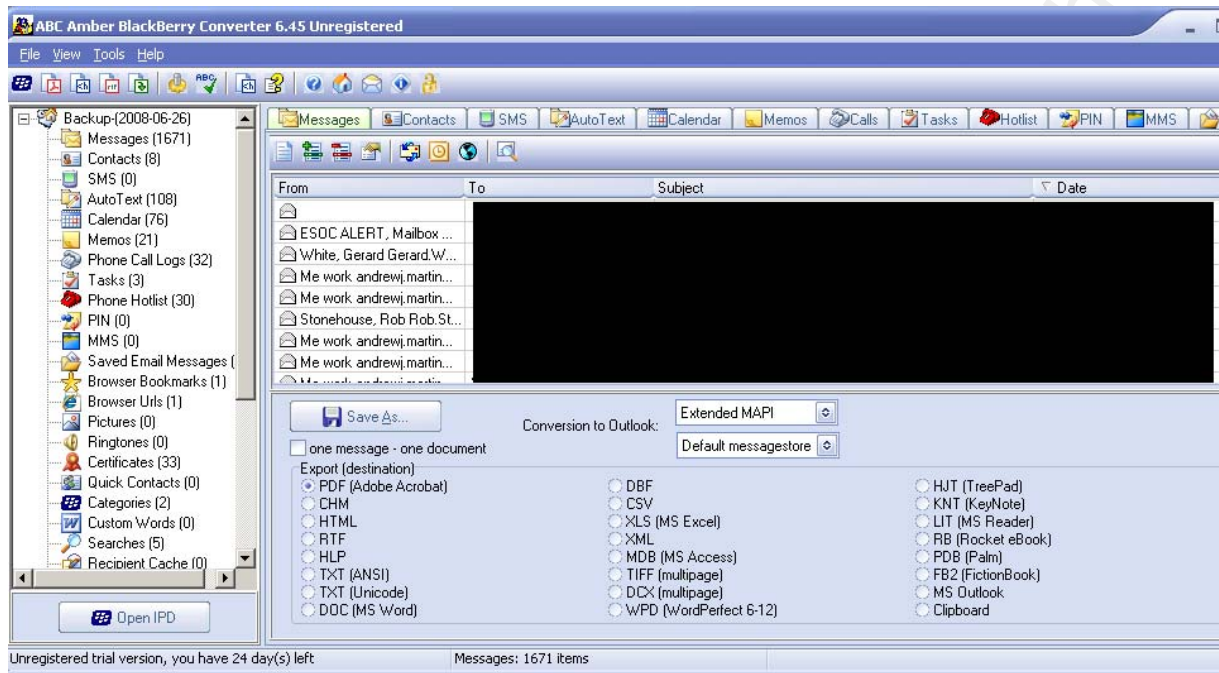
The data stored in the ipd file is mostly clear text which makes analysis pretty straight forward. Key word searches can be performed to gather information on the suspect being investigated.

Given the amount of data that can be stored on a Blackberry, performing an automated analysis of the ipd file is preferable. ABC Amber BlackBerry Converter is written for this specific task. This program is trialware, and must be registered after 30 days. Select File -> Open IPD, select the file to analyze and ABC will parse it and display its contents. The data can now be sorted, exported, saved and more. The screenshot below depicts an IPD backup Andrew Martin

imported into ABC. This Blackberry has 1671 messages stored.

© SANS Institute 2008, Author retains full rights.

Figure 19 – ABC with IPD backup loaded



With this amount of information, a comprehensive dirty word list is essential. Information stored in the following databases would be useful to an investigator:

- Messages (Emails)
- Contacts
- SMS (Text messages)
- Calendar
- Memos
- Phone Call Logs
- Tasks
- Phone Hotlist
- PIN (PIN to PIN messages)
- MMS (Multimedia messages)
- Saved Email Messages
- Browser Bookmarks
- Browser URLs

- Pictures
- Quick Contacts
- Map Locations
- Handheld Agent (installed packages)
- BlackBerry Messenger
- Folders (Email messages are sorted into their respective folder)
- Email Settings

Another option available to the analyst is to take a backup of the device in question, and restore it onto a simulated Blackberry device. This allows the investigator to browse through the user's data as if they are the user themselves. As with Desktop Manager, the appropriate version of the simulator must be downloaded that corresponds to the firmware version and model of the device. In this case, we must use a simulator for the 8700r as seen in figure 20 below.

Figure 20 - 8700r simulator



To connect the simulated device, select Simulate -> USB Cable Connected. This will cause the device to register with the host PC. As before, select Backup & Restore -> Restore -> select IPD file. This will restore the contents of the selected IPD file onto the simulated device. See figure 21.

Figure 21 - 8700r simulator with restored backup IPD



It is now possible to interact with the device as the user would. We can browse emails, recent calls, SMS messages, calendar, contacts, simply by navigating through the device's menus.

### Obtaining Data with Barry on Linux

As with the Razr, there are multiple ways to analyze the data on a Blackberry. The second approach covered is how to interact with the device via the Barry command line tool in Linux. Before this can be done, the appropriate tools must be installed. The following packages are needed for Ubuntu 8.04:

- Opensync-0.22
- Barry (lib, opensync plugin, utils, barrybackup)

With all the packages installed, it is now possible to interact with the Blackberry using the `btool` command. Simply connect the device via USB and issue the following command to view the available options for Barry.

```
user@comp:~$ btool -h
```

*Below are the options we are most interested in:*

```
-P pass    Simplistic method to specify device password  
-S         Show list of supported database parsers  
-t         Show database database table  
-T db      Show record state table for given database
```

The database parsers are used to read data from the device and present it in a human readable format. The `-S` option shows the available parsers.

```
user@comp:~$ btool -S
```

*Supported Database parsers:*

```
Address Book  
Messages  
Calendar  
Service Book  
Memos  
Tasks  
PIN Messages  
Saved Email Messages  
Folders  
Time Zones (read only)
```

*Supported Database builders:*

*Address Book*

We now use Barry to dump the contents of any of these databases in a readable format. Other databases may be dumped as well, but their contents will be displayed in hex.

The command `btool -t -p 'password'` will connect to the Blackberry and show all the databases on the device where 'password' is the PIN for the device. This unit has 69 databases, the output has been trimmed to show some of the more relevant databases.

```
user@comp:~$ btool -t -P 'password'
```

```
Blackberry devices found:
```

```
Device ID: 0x809d9f0. PIN: 20418XXX, Description: RIM 8700
```

```
Series Colour GPRS Handheld
```

```
Using device (PIN): 20418XXX
```

```
Database database:
```

```
Database: 0x0 'Content Store' (records: 18)
```

```
Database: 0x1 'Trusted Key Store' (records: 33)
```

```
Database: 0x2 'Handheld Key Store' (records: 33)
```

```
Database: 0x3 'KeyStoreManager' (records: 1)
```

```
Database: 0x4 'Policy' (records: 1)
```

```
[...]
```

```
Database: 0xc 'Messages' (records: 1571)
```

```
Database: 0xd 'Calendar' (records: 78)
```

```
Database: 0xe 'Folder Id' (records: 1)
```

```
Database: 0xf 'Folders' (records: 14)
```

```
Database: 0x10 'Purged Messages' (records: 305)
```

```
Database: 0x11 'Phone Call Logs' (records: 33)
```

```
Database: 0x12 'Attachment Data' (records: 0)
Database: 0x13 'BlackBerry Messenger' (records: 1)
Database: 0x14 'Memos' (records: 21)
[...]
Database: 0x1d 'Browser Bookmarks' (records: 1)
Database: 0x1e 'Message List Options' (records: 1)
Database: 0x1f 'Smart Card Options' (records: 1)
Database: 0x20 'Categories' (records: 2)
Database: 0x21 'Handheld Configuration' (records: 0)
Database: 0x22 'Profiles Options' (records: 1)
Database: 0x23 'Alarm Options' (records: 1)
Database: 0x24 'Saved Email Messages' (records: 1)
Database: 0x25 'TLS Options' (records: 1)
[...]
Database: 0x31 'Phone Hotlist' (records: 30)
Database: 0x32 'SMS Messages' (records: 0)
Database: 0x33 'Searches' (records: 5)
Database: 0x34 'Calendar Options' (records: 1)
Database: 0x35 'Browser Folders' (records: 2)
[...]
Database: 0x41 'PIN Messages' (records: 0)
Database: 0x42 'Address Book' (records: 8)
Database: 0x43 'WTLS Options' (records: 1)
Database: 0x44 'Email Settings - 4975' (records: 1)
```

The device has a large number of messages stored on it:

```
Database: 0xc 'Messages' (records: 1571)
```

To get the contents of this database, issue the following command:

```
user@comp:~$ btool -P 'password' -d 'Messages' >
messages.txt
```

This will put the contents of the messages database into messages.txt. This file can now be searched using strings and grep for information pertaining to an investigation. Similarly, other databases such as the address book, calendar and PIN messages can be dumped and searched in the same manner.

### **Conclusion - BlackBerry**

Using the techniques discussed above, acquiring the data from a BlackBerry is not without its challenges. Analyzing the data once acquired is fairly straightforward.

There are multiple commercial and open source tools available that can analyze an .IPD file with ease. With an .IPD backup file, all data is stored in one location and is easily searched for interesting data.

However, there is one difficulty, this being the ability to gain access to the data on the device in the first place. Careful steps must be taken when acquiring the device to ensure the device is not erased remotely. If the

device is locked, the investigator must acquire the password for the device using more traditional investigative methods or the investigation cannot continue.































