GIAC
CERTIFICATIONS

Global Information Assurance Certification Paper

Copyright SANS Institute
Author Retains Full Rights

This paper is taken from the GIAC directory of certified professionals. Reposting is not permited without express written permission.

Interested in learning more?

Check out the list of upcoming events offering
"Advanced Incident Response, Threat Hunting, and Digital Forensics (Forensics
at http://www.giac.org/registration/gcfa

Mobile Device Forensics

GCFA Gold Certification

Author: Andrew Martin

andrew@martinsecurity.net

http://www.martinsecurity.net

Advisor: Joey Niem

Accepted – August 29, 2008

© SANS Institute 2009, Author retains full rights.

© SANS Institute 2009, Author retains full rights.

Table of Contents

Abstract 4
Devices 5
Tools – General 5
Motorola Razr V3C 7
  Scenario 7
  Tools 8
  Techniques 9
  Verification 9
  System Description 10
  Evidence Acquisition 10
    Dumping Memory 11
    Accessing the File System 13
    Accessing the Phone via AT Commands 14
  Analysis 17
    Security Lock 17
    Phone Book 19
    SMS Messages 23
    SIM Card - Phonebook & SMS messages 26
    Recent Calls 28
    Calendar 31
    Web Browsing 32
    Multimedia 33
    Other Artifacts 33
  Conclusion – Razr 34
Blackberry 8700r 36
  Scenario 36
  Tools 38
  Techniques 38
  Verification 38
  System Description 39
  Evidence Acquisition 39
    Blackberry Enterprise Server Considerations 40
    Acquisition Scenarios 40
    Content Protection 42
  Analysis 43
    IPD file on Windows 43
    Obtaining Data with Barry on Linux 49
  Conclusion – BlackBerry 53
Coby MP3 Player 55
  Scenario 55
  Tools 56
  Techniques 57

© SANS Institute 2009, Author retains full rights.

Verification 57
System Description 59
Evidence Acquisition 59
Analysis 61
Conclusion MP3 Player 65
Final Conclusion 66
Challenges 67
Tools and Techniques 67
Direct References 69
Direct References 69
Other References Accessed & Used 71

© SANS Institute 2009, Author retains full rights.

© SANS Institute 2009, Author retains full rights.

Abstract

The world of mobile device forensics is a complicated one. Unlike the PC world's limited number of major operating system vendors, there are countless manufacturers of mobile devices. To complicate things further, each mobile device manufacturer may have his own proprietary technology and formats. Add to this the blistering pace at which new mobile devices such as cellular phones and personal digital assistants (PDAs) are released, 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 daily 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.

© SANS Institute 2009, Author retains full rights.

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 that possesses many of the standard features we have come to expect.

The Blackberry is a smart phone that 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 challenge of how to analyze their data quickly and effectively. There are no free tools capable of analyzing every single phone on the market. Several vendors have surfaced in an attempt to fill the need for a common analysis platform for the many different phone manufacturers and models.

© SANS Institute 2009, Author retains full rights.

"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.

In the computer world, there is always more than one way to accomplish a task. Analyzing mobile devices is no exception. 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 discussed in this paper that output their data as text. To better illustrate the commands issued and the output displayed, the following format is used:

Command

Output

© SANS Institute 2009, Author retains full rights.

Motorola Razr V3C



Scenario

(This scenario has been fabricated for the purposes of illustration.)

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 darting to a bag poorly concealed under the passenger seat. The officer asks the suspect to exit the car, and checks the bag, which contains a large amount of drugs. After questioning, it is believed the suspect was simply acting as a courier; however he is not telling the investigators anything. The police suspect he is in contact with a distributor, whom the police would like to apprehend.

© SANS Institute 2009, Author retains full rights.

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 who 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 malcode analysis pack)
- HyperTerminal
- Motorola Drivers
- P2KToolsVS

© SANS Institute 2009, Author retains full rights.

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 some differences. P2K Commander and Flash & Backup are both usable on most models of Motorola phones.

Verification

Before commencing 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. In order 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.

© SANS Institute 2009, Author retains full rights.

© SANS Institute 2009, Author retains full rights.

System Description

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

Date/Time device was taken from suspect: June 1st, 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 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. Since the phone's memory must be dumped while it is running, however, 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

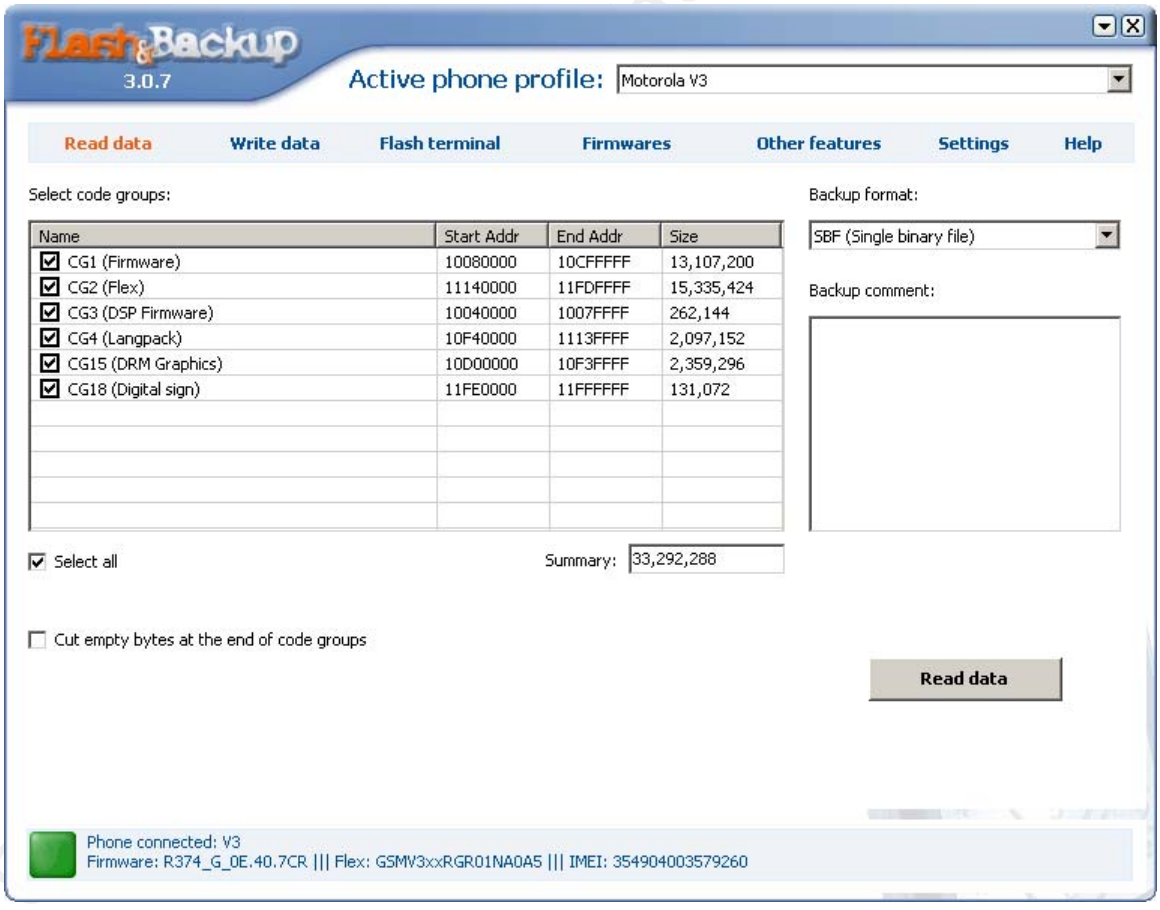
© SANS Institute 2009, Author retains full rights.

commands. 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

© SANS Institute 2009, Author retains full rights.

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 six 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 for the investigation in this section. But having a backup 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).

© SANS Institute 2009, Author retains full rights.

© SANS Institute 2009, Author retains full rights.

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

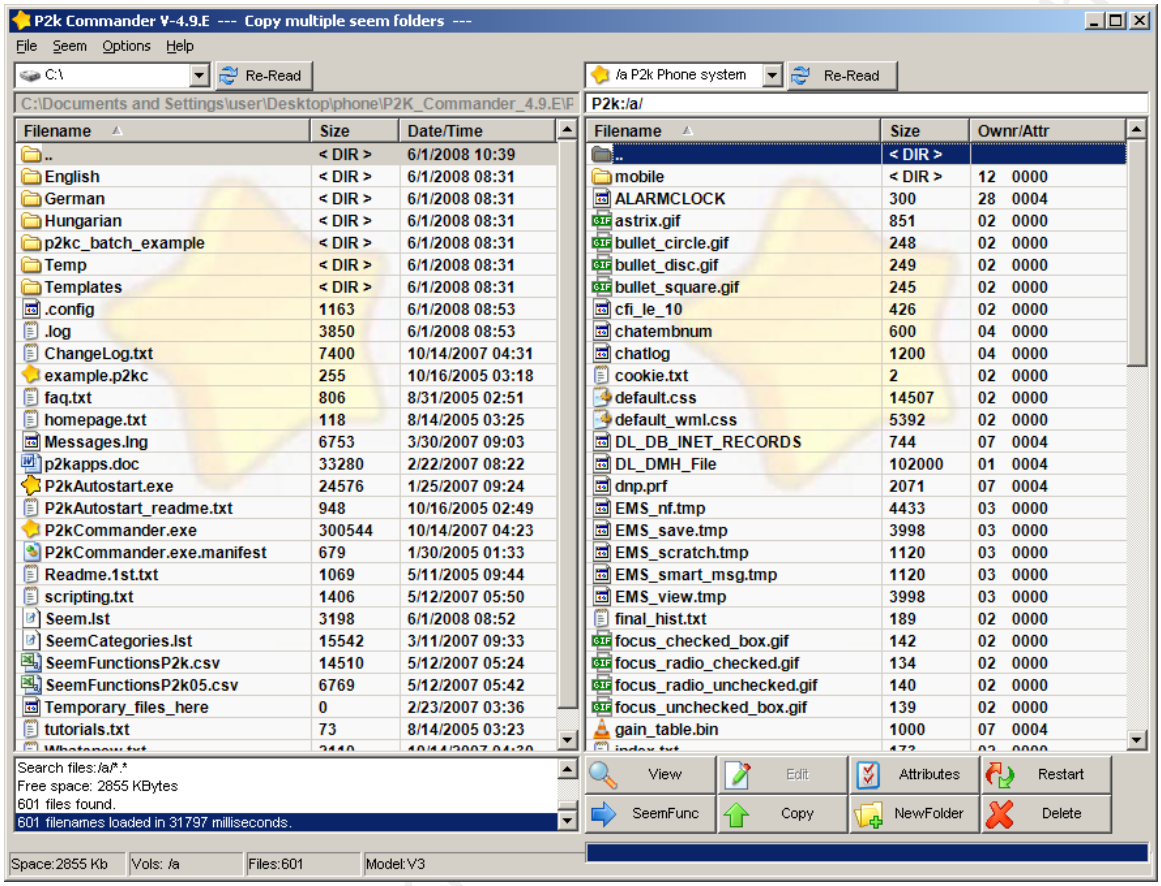
P2K Commander:
http://handheld.softpedia.com/get/Developer-Tools/File-Manager/P2kCommander-38120.shtml

Once the above files have been 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.

© SANS Institute 2009, Author retains full rights.

© SANS Institute 2009, Author retains full rights.

Figure 2 – P2k Commander – Phone file listing



Ensure the left pane is pointing to a local hard drive, and the right pane is pointing 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 composed 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

© SANS Institute 2009, Author retains full rights.

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/

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.

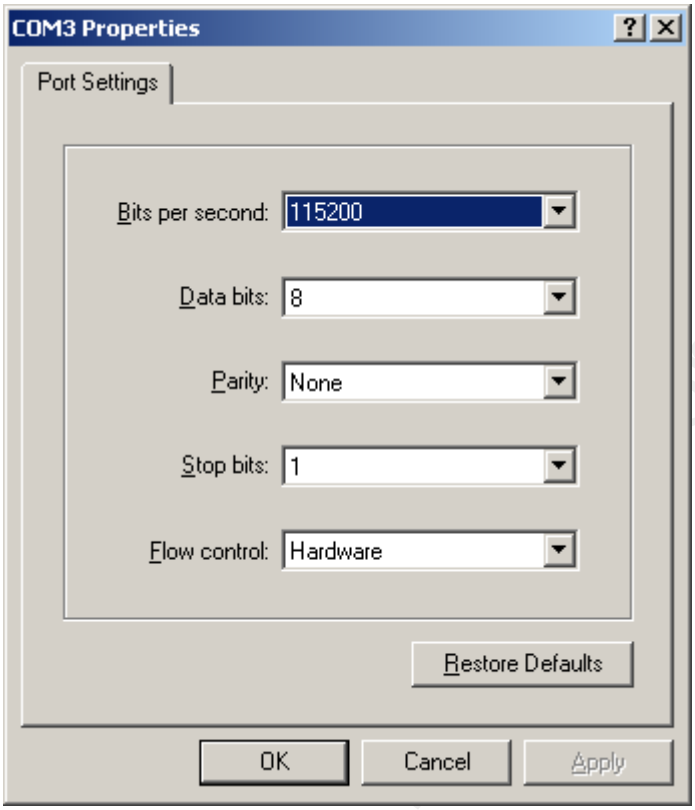
Bits per second: 115200
Data bits: 8
Parity: None

© SANS Institute 2009, Author retains full rights.

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.

© SANS Institute 2009, Author retains full rights.

Analysis

It is difficult to adhere to the standard forensic investigation methodology when analyzing a cellular phone since 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

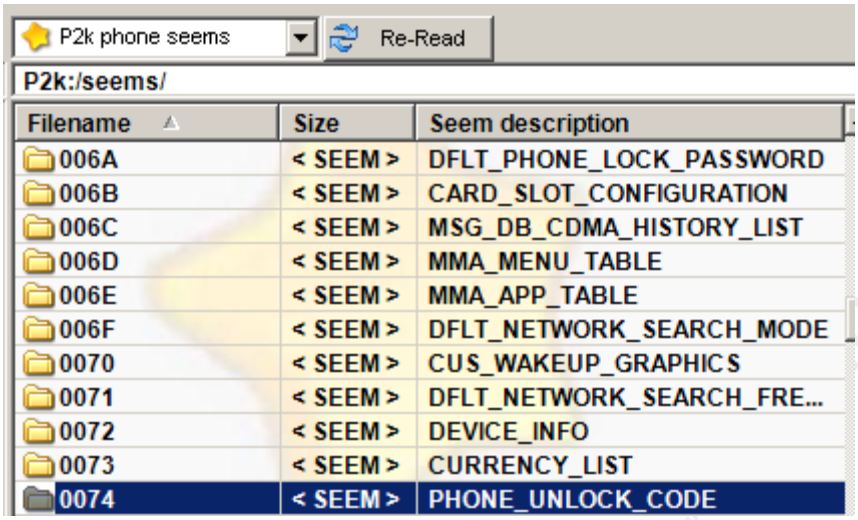
There is always the possibility that a phone is locked and the analyst needs to navigate around the phone's GUI (keeping in mind that the investigator is changing data on the device). In the Razr's case, the phone lock does not block access to the file system. We will use P2k Commander to extract the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

© SANS Institute 2009, Author retains full rights.

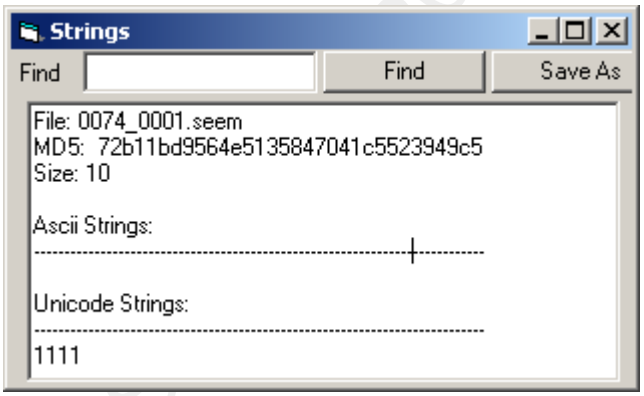
© SANS Institute 2009, Author retains full rights.

Figure 5 – Unlock code



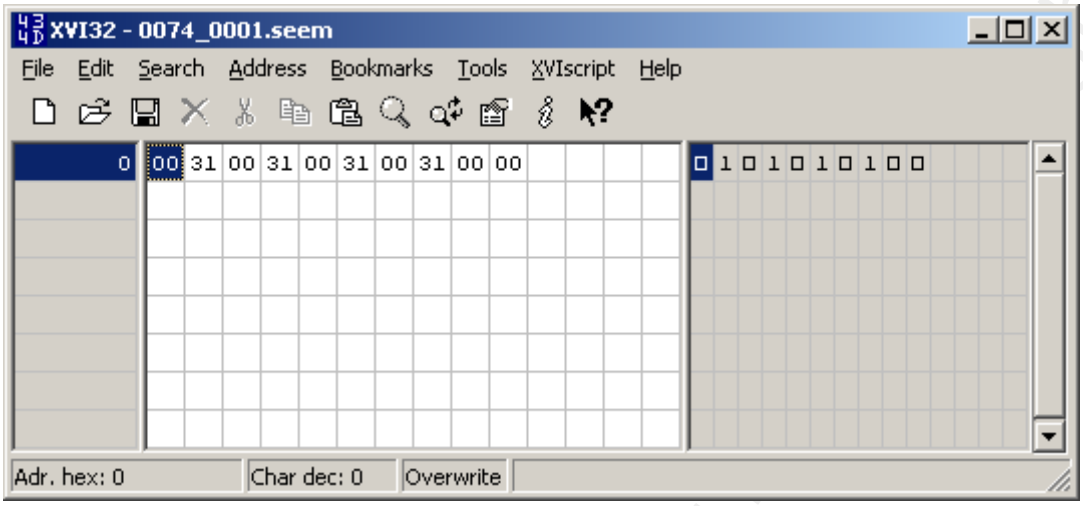
Using XVI32 or Strings, we can quickly discern that the unlock code is "1111". See Figure 6 below for the output using Strings. Figure 7 illustrates the same data using XVI32.

Figure 6 – Strings output of SEEM 0074



© SANS Institute 2009, Author retains full rights.

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 that allows for an extended character set for other languages. The above unlock code is stored as four 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.

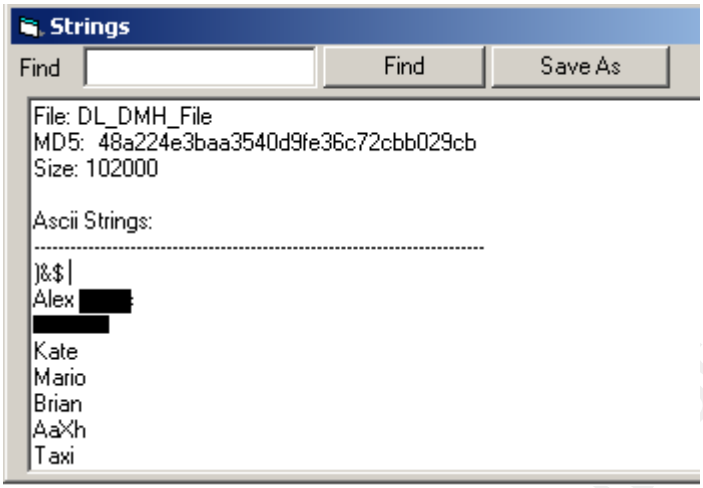
Phonebook via file system

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.

© SANS Institute 2009, Author retains full rights.

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



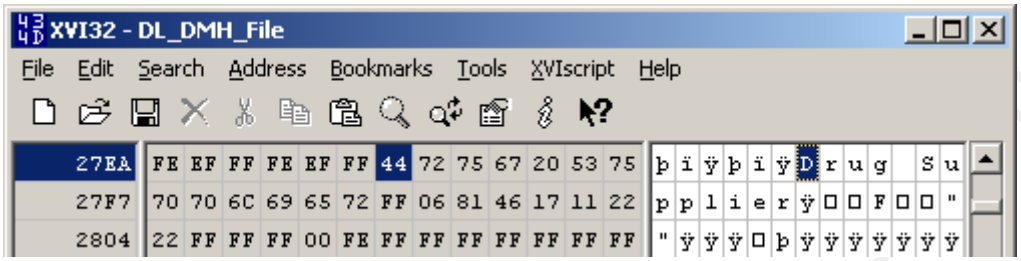
Closer inspection with XVI32 yields the data we need, names and phone numbers of all the contacts in the phonebook. There happens to be an entry for a contact called “Drug Supplier” (this was made overly obvious for the purpose of the paper).

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

© SANS Institute 2009, Author retains full rights.

Figure 9 – Hex view of DL_DMH_File



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

© SANS Institute 2009, Author retains full rights.

© SANS Institute 2009, Author retains full rights.

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"

© SANS Institute 2009, Author retains full rights.

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 XXXXXXX ",129,"Joey"
+CPBR: 65,"416 XXXXXXX ",129,"Parking"
+CPBR: 66,"416XXXXXXX",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

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

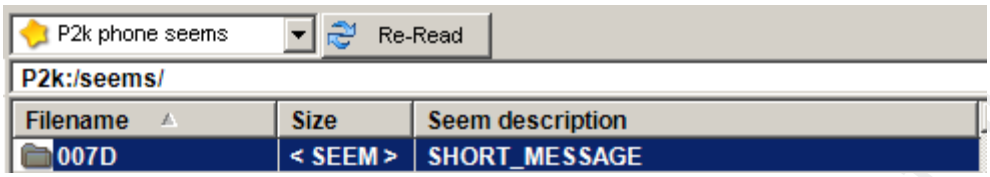
There are some subtle nuances with the way SMS messages are stored. Messages in the Inbox are stored on the SIM card of the phone (by default, but this can be changed). The Quick Notes, Outbox and Drafts are saved in the phone’s memory.

SMS Messages via File System

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

© SANS Institute 2009, Author retains full rights.

Figure 10 – SMS SEEM



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
```

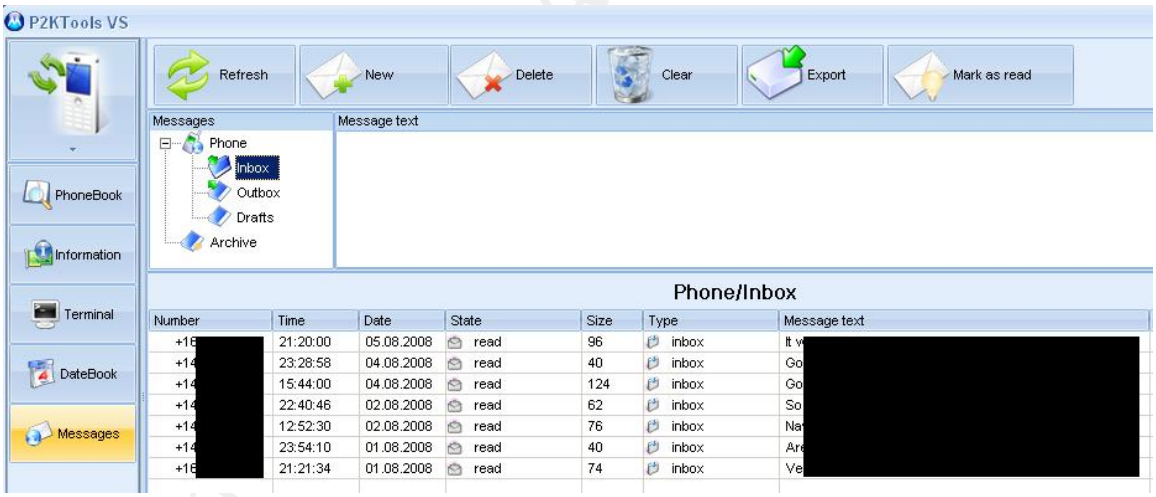

© SANS Institute 2009, Author retains full rights.

```
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
```


© SANS Institute 2009, Author retains full rights.

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 have been 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

© SANS Institute 2009, Author retains full rights.

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.

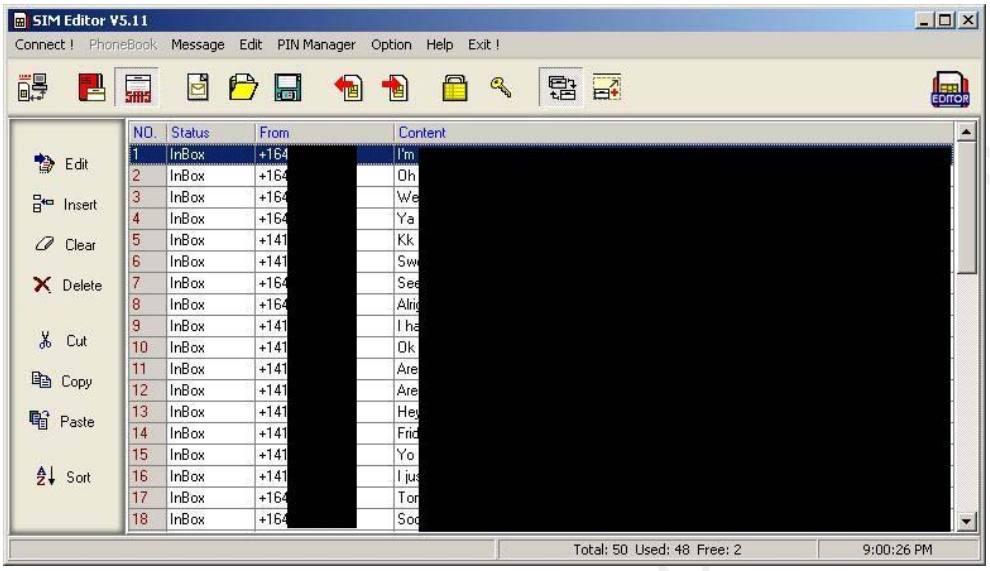


The software provided with the device was able to read the SIM card and display the phonebook entries and SMS messages. See Figure 12 below.

© SANS Institute 2009, Author retains full rights.

© SANS Institute 2009, Author retains full rights.

Figure 12 – Contents of SIM SMS messages



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.

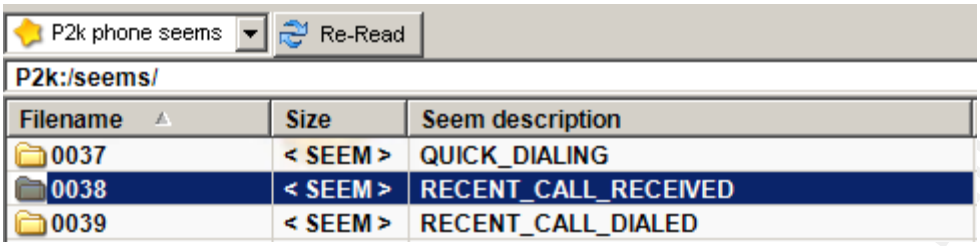
Recent Calls

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.

© SANS Institute 2009, Author retains full rights.

Figure 13 – Recent calls via P2k Commander

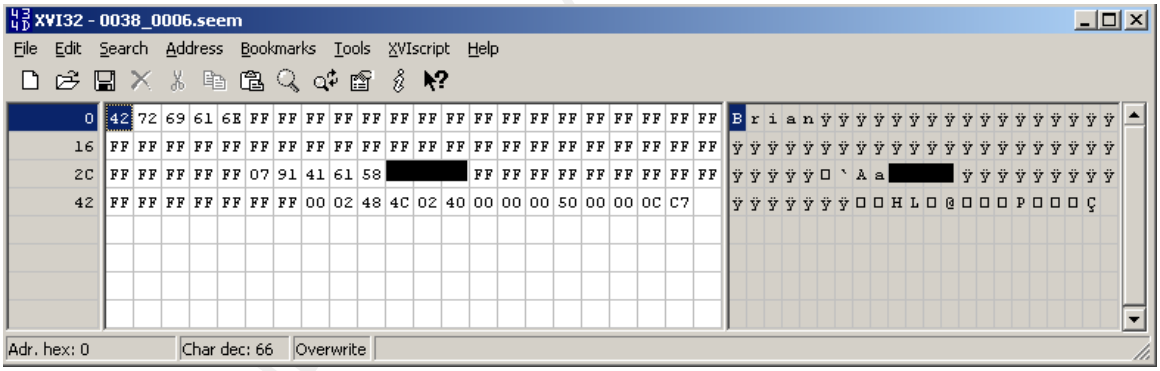


The first section of the file contains the caller name, “Brian”. The second section contains the phone number which has been reversed. See Figure 14 below.

41 61 58 XX XX XX

1 416 85X XXXX

Figure 14 – Example call received



While there is more data at the end of the file that may represent the time and date of the call, I was not 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.

© SANS Institute 2009, Author retains full rights.

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

AD Abbriviated 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,"+141685X8XXXX",145,"Brian"
+CPBR: 3,"+141659XXXXX",145,"Lobby"
```


© SANS Institute 2009, Author retains full rights.

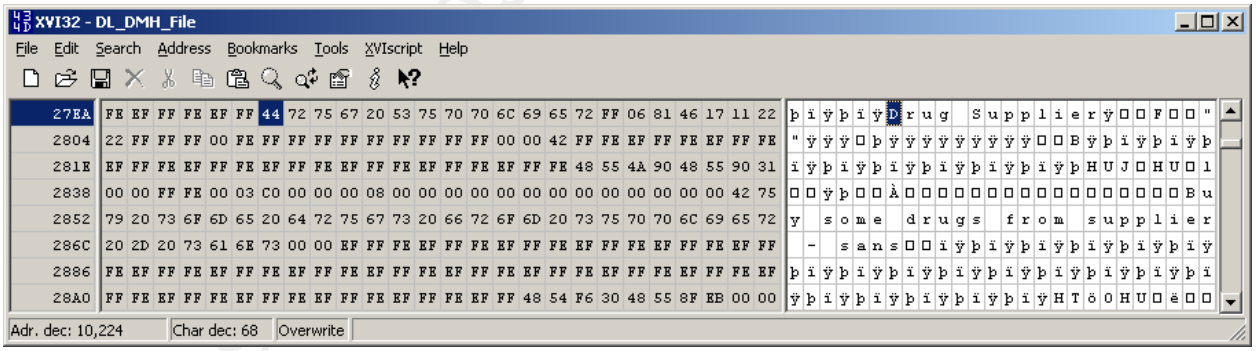
Calendar

The calendar can be accessed just like the rest of the data. Like SMS messages, the file system will contain data on past calendar entries as well as upcoming ones, and the AT commands will only display current or future entries.

Calendar entries via file system

Using a hex editor, we perform a simple search for “Drug”, which will yield the follow calendar entry. The entry contains the name, phone number (stored backwards again) and description of the event, which in this case is “Buy some drugs from supplier – sans”.

Figure 15 – Calendar entries in DL_DMH_FILE.



Calendar entries are stored in the same file as the phonebook data, DL_DMH_File.

Calendar entries via AT commands

The commands needed for accessing the calendar are not documented in Motorola’s Developer’s Guide. They can be found in /plugins/moto-sync/moto-sync.py from opensync, http://www.opensync.org/changeset/1235?format=diff&new=1235

© SANS Institute 2009, Author retains full rights.

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 that should be analyzed during an investigation. There are several files on the device that 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

© SANS Institute 2009, Author retains full rights.

/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 such as

© SANS Institute 2009, Author retains full rights.

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 that 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 the following information on the suspect's phone:

- 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 15th, 5PM

This information can be used to search thro1ugh the phone for additional evidence or as key reference material in an interview with the suspect. If the suspect had a PC that had been seized as well, this information could be

© SANS Institute 2009, Author retains full rights.

used to conduct a more targeted investigation of the computer.

© SANS Institute 2009, Author retains full rights.

© SANS Institute 2009, Author retains full rights.

Blackberry 8700r



Scenario

Consider the following scenario: an employee at a large company has approached HR regarding inappropriate messages and phone calls he has received from a co-worker. In order to confirm the unwanted behavior, management authorizes the analysis of the harasser's BlackBerry, which had been 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 his/her PIN so that the device may be backed up. Support staff explains that a

© SANS Institute 2009, Author retains full rights.

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.

© SANS Institute 2009, Author retains full rights.

© SANS Institute 2009, Author retains full rights.

Tools

There are many tools that can be used to perform an investigation on a BlackBerry. Basic tools such as a hex editor and the strings command are pretty standard for examining any device. A BlackBerry can be very easy or extremely challenging to analyze, 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 an .ipd backup file and the second will be to analyze the device interactively using Barry with OpenSync in Linux.

Verification

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

© SANS Institute 2009, Author retains full rights.

- The phone number of the device is viewable from the Call Log application, note “My Number”.
- The owner might have entered his 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 an understanding of the Blackberry Enterprise Server and the security technology built into the hand-held unit.

© SANS Institute 2009, Author retains full rights.

© SANS Institute 2009, Author retains full rights.

Blackberry Enterprise Server Considerations

The Blackberry Enterprise Server (BES) is a tool used to centrally manage an organization's devices. While it has a number of features, we will only discuss those 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

© SANS Institute 2009, Author retains full rights.

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 his/her 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 his 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 that would be contained inside a Faraday Cage. This would prevent any signals from reaching the device from the time of seizure to analysis.

© SANS Institute 2009, Author retains full rights.

If the unit is locked, there are several 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.

© SANS Institute 2009, Author retains full rights.

© SANS Institute 2009, Author retains full rights.

Analysis

Once the device has been 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 memory contents 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. 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.

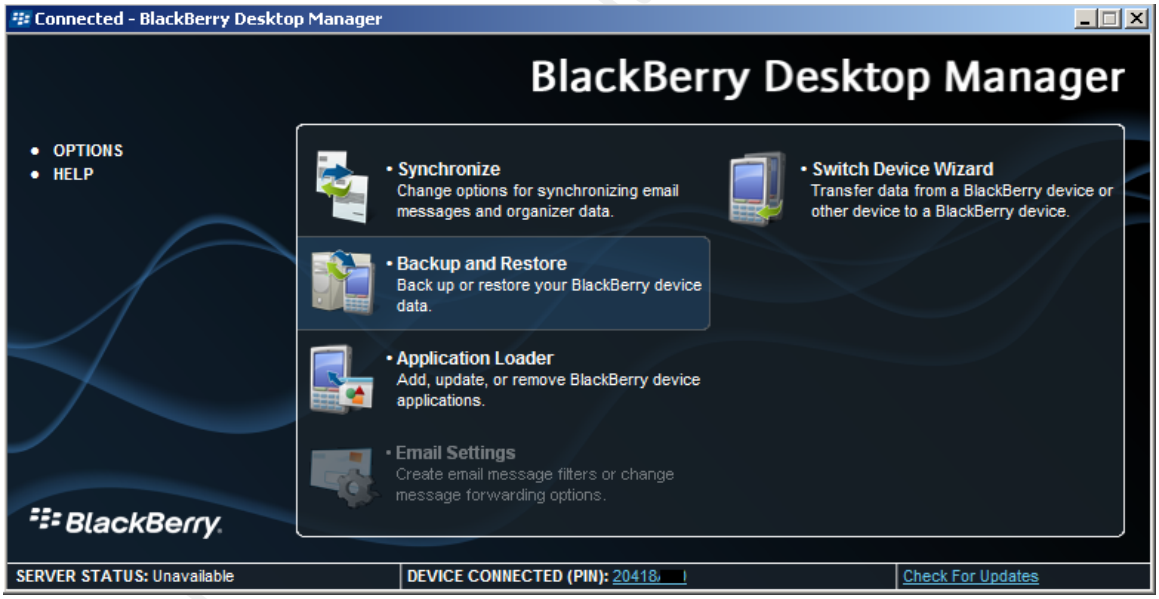
Consider the following scenario: The corporate user referred to earlier is being investigated, but he is away on vacation with his Blackberry in his possession. One of

© SANS Institute 2009, Author retains full rights.

the things an investigator can look for is .ipd files on the user's home or work PC, as well as 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.

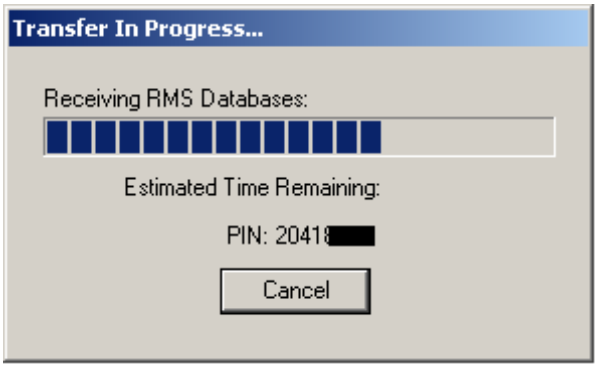
Figure 16 – Obtaining IPD backup



The status of the backup is shown below.

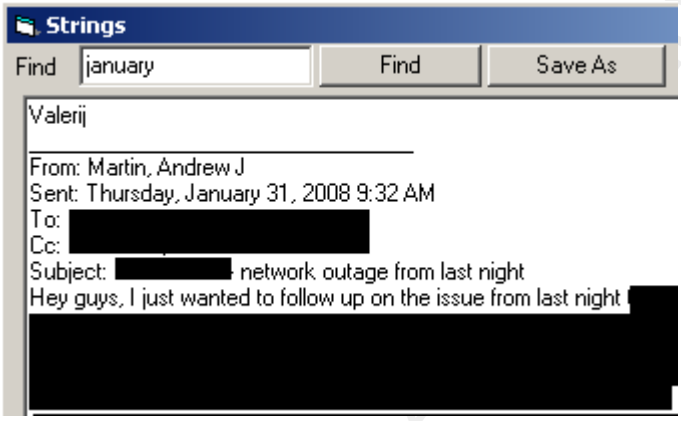
Figure 17 – Progress of IPD backup process

© SANS Institute 2009, Author retains full rights.



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

Figure 18 – Strings output of newly created IPD backup



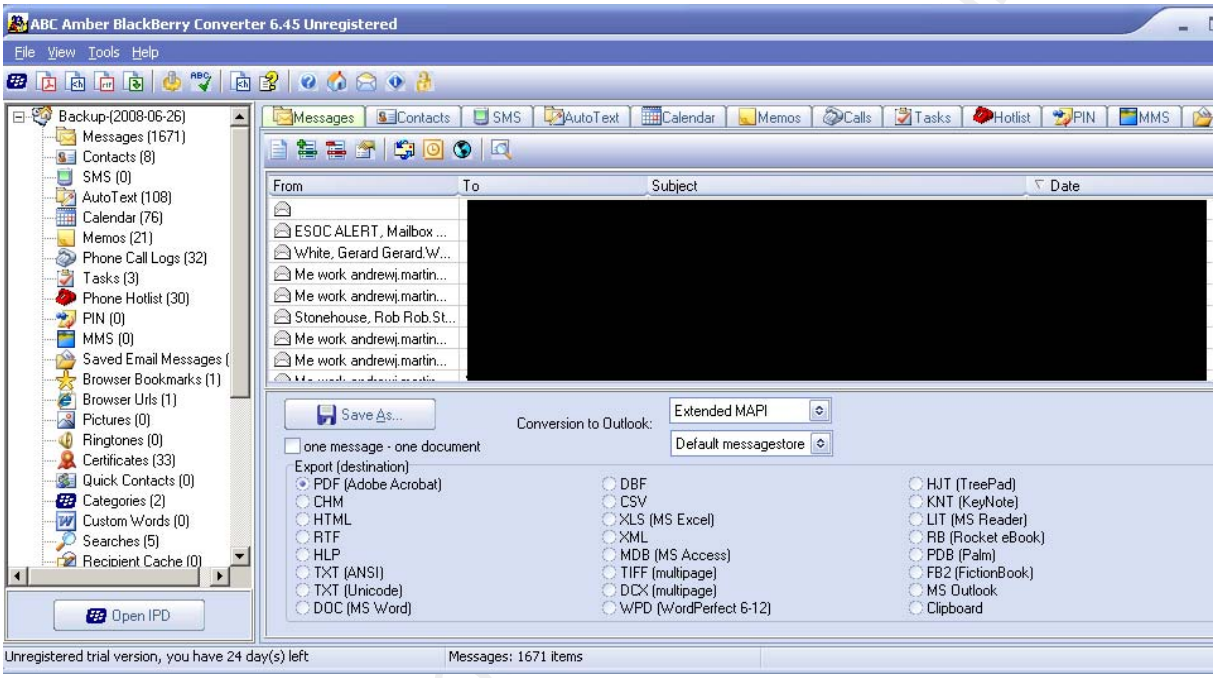
The data stored in the ipd file is mostly clear text, which makes analysis pretty straightforward. Key word searches can be performed to gather information on the suspect being investigated.

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

© SANS Institute 2009, Author retains full rights.

imported into ABC. This Blackberry has 1671 messages stored.

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 that would be useful to an investigator includes the following:

- Messages (Emails)
- Contacts
- SMS (Text messages)
- Calendar
- Memos
- Phone Call Logs
- Tasks
- Phone Hotlist
- PIN (PIN to PIN messages)

© SANS Institute 2009, Author retains full rights.

- 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 he were the user. As is the case with Desktop Manager, it is necessary to download the appropriate version of the simulator 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.

© SANS Institute 2009, Author retains full rights.

© SANS Institute 2009, Author retains full rights.

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].

© SANS Institute 2009, Author retains full rights.

© SANS Institute 2009, Author retains full rights.

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)

© SANS Institute 2009, Author retains full rights.

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:
```


© SANS Institute 2009, Author retains full rights.

```
   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)
```


© SANS Institute 2009, Author retains full rights.

```
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)
```


© SANS Institute 2009, Author retains full rights.

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 -- 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 that the device is not erased remotely by the person being investigated or their support staff. If the device is

© SANS Institute 2009, Author retains full rights.

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

© SANS Institute 2009, Author retains full rights.

© SANS Institute 2009, Author retains full rights.

Coby MP3 Player



With MP3 players becoming more and more popular, investigators must be prepared for analyzing them for interesting data. These devices are much different from the Razr and BlackBerry discussed previously as MP3 players typically use a standard file system. This section will quickly detail the analysis of a 1GB MP3 player that uses the FAT32 file system.

Scenario

(This is a fictitious example scenario. I am not a lawyer and cannot comment on legal issues.)

This scenario involves two companies that make many different types of widgets. On July 21st, 2008 Company A is approached by a man named Jim who claims to have Company B's strategy for the coming year for their version of the widgets. Jim tries to sell the strategy to Company A for a large sum of money. Each company's widgets are in great demand, and the competition between the two is healthy. In

© SANS Institute 2009, Author retains full rights.

fact, the executives at each company have a good relationship and share some information freely.

Company A rejects Jim's offer and secretly informs Company B of his plan to sell their strategy. Company B only knows the suspect's first name, Jim. After looking through the employee manifest, they find an IT administrator whose first name is Jim.

Searching through his email does not yield any leads and CD/DVD writers are disallowed in the company. Investigators check his work PC while he is out of the office and find in the registry that Jim plugs in a USB MP3 player:

HKLM\System\CurrentControlSet\Enum\USBSTORE\Disk&Ven_&Prod_COBY_MP3_Player&Rev_

Company B is able to obtain an Anton Piller order to search Jim's personal MP3 player for evidence of the theft given the evidence present. An Anter Piller order "is a court order which provides for the right to search premises and seize evidence without prior warning. This is used in order to prevent the destruction of incriminating evidence, particularly in cases of alleged trademark, copyright or patent infringements" (Wikipedia, 2009) The investigators are looking for the presence of the data on his machine. The document is in Microsoft Word format and has the extension .doc.

Tools

© SANS Institute 2009, Author retains full rights.

To analyze the device, we use standard forensic tools. These have all been covered in the GCFA course material and include the following:

- DD for Windows
- Autopsy

Techniques

Since the scope of the investigation has been clearly defined to find evidence of the stolen information, the techniques needed are clear. The device in question must be imaged and analyzed for the presence of data that would indicate the theft of sensitive information.

Verification

To first validate that this device is used on Jim's PC, the following registry is checked.

HKLM\System\CurrentControlSet\Enum\USBSTORE\

Under this key is a subkey named:

Disk&Ven_&Prod_COBY_MP3_Player&Rev_

This indicates the type of USB device used. To further validate that this is the device in question, the USB device has a unique ID which in this case is:

0010100010141000771290

© SANS Institute 2009, Author retains full rights.

With the USB device plugged in, navigating to the properties of the MP3 player's entry in the Windows device manager shows the same serial number in Figure 22 below.

© SANS Institute 2009, Author retains full rights.

© SANS Institute 2009, Author retains full rights.

Figure 22 – MP3 player serial number



System Description

In this case, the system description phase is quite brief. The following information is recorded about the device:

Make: Coby MP3 Player
Model: MP550-1G
Memory: 1GB
Memory Format: Flash

Evidence Acquisition

With the verification and system description phases of the investigation complete, we now move on to the acquisition stage. To acquire a copy of the MP3 player, a USB write blocker should be employed to prevent any changes to the device. Once acquired, the resulting image may be hashed to prove integrity. For this example, no USB write blocker was available.

Instead, the image was acquired directly as a logical partition using dd (from http://gmgsystemsinc.com/fau/) and using the following command.

© SANS Institute 2009, Author retains full rights.

```
dd if=\\.\f: of=e:\output.img bs=512 --localwrt
conv=noerror

Statistics for logical volume \\?\Volume{402dc764-4e99-
11dd-9e04-005056c00008}\
               0x014742000 bytes available
               0x014742000 bytes free
               0x03d700000 bytes total
Volume Name:    \\?\Volume{402dc764-4e99-11dd-9e04-
005056c00008}
Volume Label:
Mount Points:
                       F:\
Drive Type:            Removable
Volume Serial Number:          30a3-239e
Maximum Component Length:      255

Volume Characteristics:
                       File system preserves case
                       File system supports Unicode file
names
File System:           FAT32
Mounted:               Yes
Clustered:             No
Volume Extents:
        Disk Number:     3
        Starting Offset: 0x0000000000004000
        Extent Length:   0x000000003d7fc000



Copying \\.\f: to e:\output.img
```


© SANS Institute 2009, Author retains full rights.

```
Output: e:\output.img
1031782400 bytes
2015200+0 records in
2015200+0 records out
1031782400 bytes written

Succeeded!
```

This command copies volume f to output.img on drive e using a blocksize of 512 bytes. Once complete, we may continue to the analysis phase.

Analysis

Using Autopsy, it is now possible to analyze the newly created file output.img. From http://localhost:9999 we create a new case, give it a name, and assign the name of the investigator. We can then add a host and give it a description, time zone and specify a known good hash database to compare our files to. Given the small number of files that should be present on this device, this option is not necessary for this investigation. We then add an image to our host using the partition option, since the image we have acquired is only of one partition (the removable drive F). Autopsy then allows us to create an MD5 hash of the image. This image can be used to prove image integrity later. Generating an MD5 hash of a large image will require a significant amount of time and resources, so patience is required.

With the hash calculated, we move on to the actual analysis of the image. With the appropriate image selected,

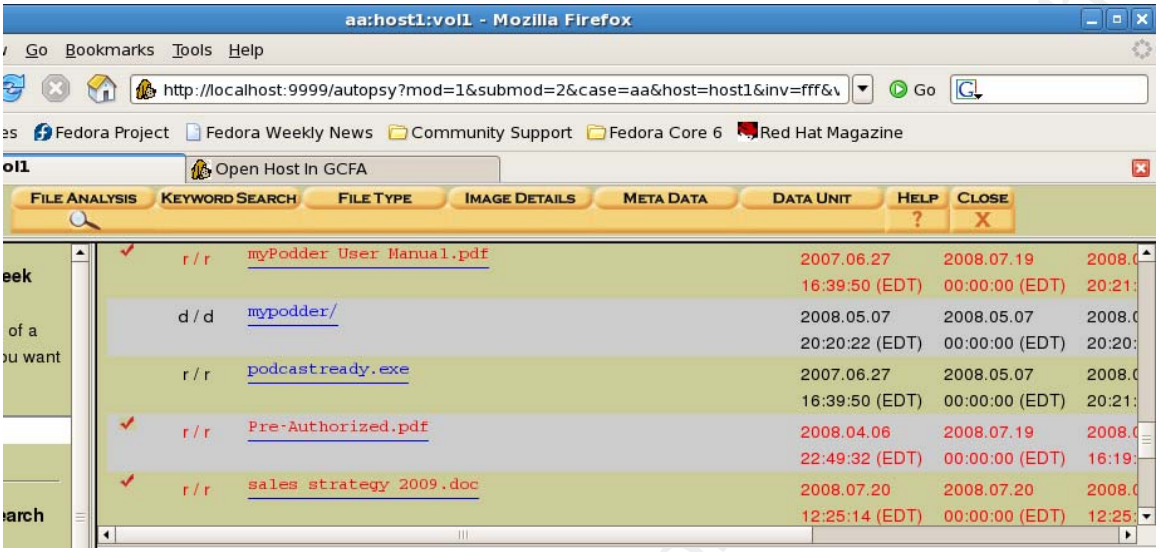
© SANS Institute 2009, Author retains full rights.

we select “analysis” and navigate to “file analysis”. Figure 23 below depicts several files stored on the device. Files with a checkmark are deleted files. It seems that after Jim’s offer was rejected, he probably deleted the “sales strategy 2009.doc” file.

© SANS Institute 2009, Author retains full rights.

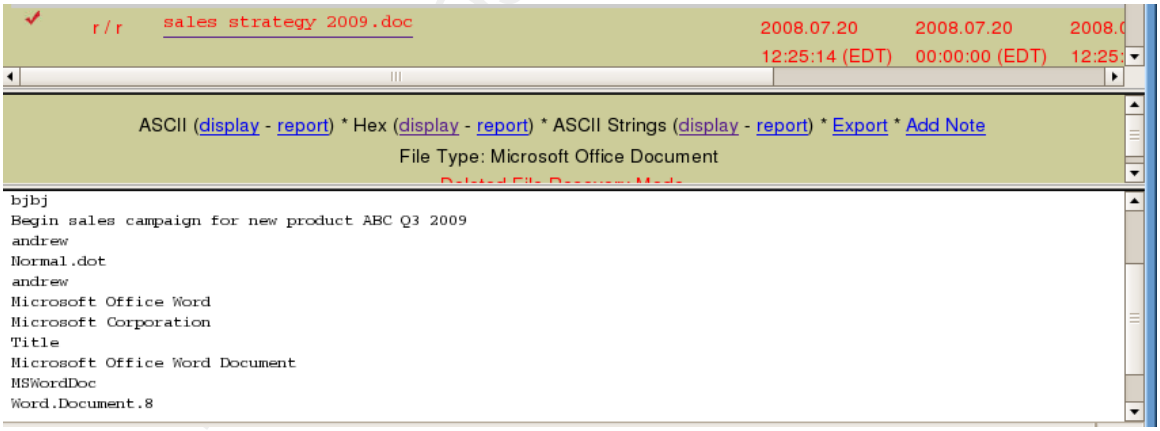
© SANS Institute 2009, Author retains full rights.

Figure 23 – File analysis of output.img



Selecting the ASCII Strings – Display option runs the strings command on the file and displays its output.

Figure 24 – ASCII Strings in "sales strategy 2009.doc"



One of the strings contained in the document says "Begin sales campaign for new product ABC – Q3 2009. It seems we have found the file that Jim tried to sell to the competition.

The timestamp on the file places it on the device on July 20th, a day before Company A was approached by Jim.

© SANS Institute 2009, Author retains full rights.

July 20th was a weekend, and Jim would typically not be in the office on a Sunday. Reviewing the swipe card access logs to the building on July 20th reveals that Jim accessed the building premises.

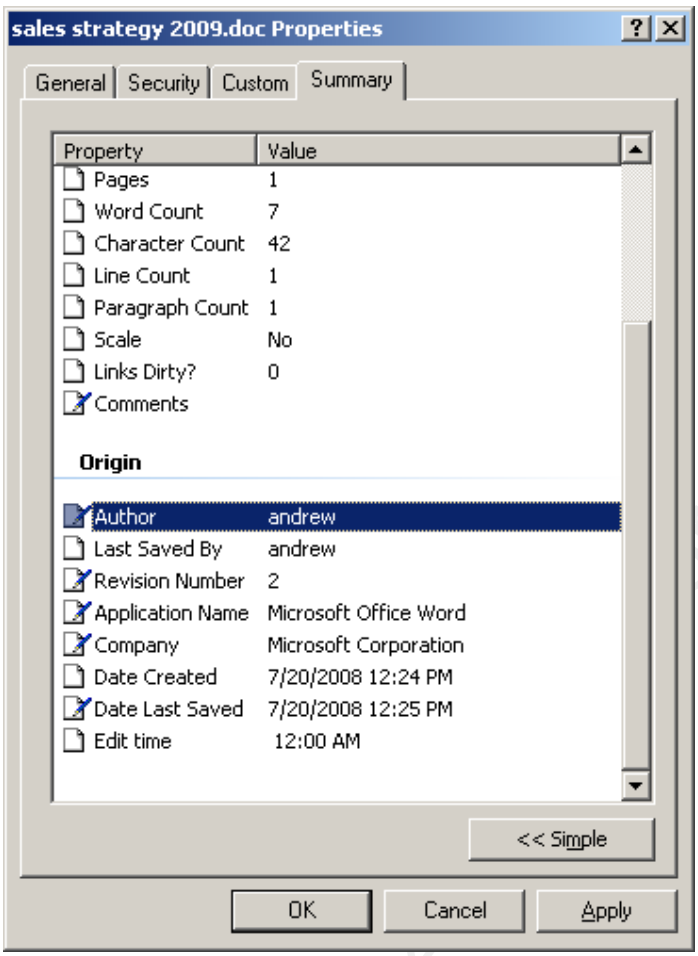
Reviewing the document's metadata points us to the person, who last modified the file. This gives us a direct point of contact to follow up on the document's purpose and target audience. Figure 25 below shows that the author of this document is "andrew". The file may be exported for further analysis.

With the file located and read in detail, timeline confirmed, swipe card logs and testimony from the group responsible for creating the "sales strategy 2009.doc" file, we now can bring a compelling case against Jim.

© SANS Institute 2009, Author retains full rights.

© SANS Institute 2009, Author retains full rights.

Figure 25 – sales strategy 2009.doc meta data.



Conclusion MP3 Player

Analyzing a portal MP3 device is quite similar to performing a standard investigation on a hard drive. Most MP3 players use the standard FAT32 file system whose structure is well known and documented. There are a number of both commercial and open source tools for both *nix and Windows that are mature and capable of analyzing a FAT32 image.

Given the size of such portable devices, they are typically quicker to analyze than a full hard drive. The

© SANS Institute 2009, Author retains full rights.

device analyzed above was only 1GB, but with large hard drive-based MP3 players on the market, the average size of such devices will steadily increase over time.

In a corporate environment, the biggest hurdle faced by investigators will probably be obtaining authorization to acquire the device. MP3 players are typically personal devices that are not provided by the company. This puts an investigator on much different legal ground than if the device in question was a company issued BlackBerry.

With these considerations in mind, it is probably more prudent for corporations to look at preventing this type of event from occurring. The affected company could disable USB functionality on their desktops, remove them entirely or even fill them in with a glue gun. **No one method is totally effective for blocking the removal of sensitive data.** Layering many different measures from the host to the network level is a best practice.

Final Conclusion

Throughout this paper we have covered several tools and techniques for retrieving and analyzing data from mobile devices. Three different types of devices have been discussed including a cellular phone, smart phone and MP3 player. Each device presented its own unique challenges as outlined below.

© SANS Institute 2009, Author retains full rights.

© SANS Institute 2009, Author retains full rights.

Challenges

Cellular phone – Razr V3

- Lack of mature open source tools to analyze data
- Number of mobile devices is so large that even commercial forensic suites do not support them all
- Not possible (using tools available) to reliably hash data to prove integrity

Smart Phone – BlackBerry 8700r

- Not possible (using tools available) to acquire data from device if it is locked and the PIN is not known.
- Must be mindful of remote delete function
- Deleted data difficult to obtain. It is possible with certain configurations and using older firmware, but these techniques are outdated and not usable on newer firmware
- Not possible (using tools available) to reliably hash data to prove integrity

MP3 Player – Coby MP550-1G

- MP3 players not issued by most companies, can present legal dilemma for acquiring data.

Tools and Techniques

After analyzing three different types of devices using a variety of tools, it is clear that some tools are useful for any investigation. Strings, grep, a hex editor and

© SANS Institute 2009, Author retains full rights.

developer tools (for some devices) may be used in practically every investigation of a mobile device to great success.

The techniques used are also very similar for each device. To be successful, it is best to begin an investigation with the most information possible. Names, dates, file names, file types, type of investigation, phone numbers, email addresses -- all these seemingly small pieces of information can be combined to provide a solid starting point for an investigator.

As documented in the SANS Forensic Investigation Methodology, we are constantly moving through media analysis, string searches, data recovery and timeline analysis phases. Due to the nature of mobile devices, the timeline analysis phase is not always useful as many mobile device file systems do not record timestamps.

In order to be a successful investigator, the analyst must be able to don his “detective hat” when analyzing a device. An open mind and curiosity for delving into the unknown are key to getting to the end of an investigation. **Mobile device forensics is a new and evolving field that is only now starting to mature.** It is only through the experience of working with many types of devices that an investigator becomes proficient in this art.

[END]

© SANS Institute 2009, Author retains full rights.

© SANS Institute 2009, Author retains full rights.

Direct References

Motorola, MOTORAZR V3xx Specifications Sheet (2008)
Retrieved June 27, 2008
https://developer.motorola.com/docstools/specsheets/

Motorola, MOTOROLA G24-L AND G24-LC DEVELOPER'S GUIDE (2008)
AT COMMANDS REFERENCE MANUAL.
Retrieved June 1st, 2008, from
https://developer.motorola.com/docstools/developerguides/G24-L_AT_Commands_Final2_250909.pdf/

Research In Motion, Administration Guide (no date)
BlackBerry Enterprise Server for Microsoft Exchange
Retrieved June 26, 2008, from
http://www.blackberry.com/knowledgecenterpublic/livelink.exe/fetch/2000/8067/645045/7963/7965/1180408/Administration_Guide.pdf?nodeid=1418582&vernum=0

Research In Motion, Features and Technical Overview (no date)
BlackBerry Enterprise Server for Microsoft Exchange
Retrieved June 26, 2008 from
http://www.blackberry.com/knowledgecenterpublic/livelink.exe/Feature_and_Technical_Overview.pdf?func=doc.Fetch&nodeId=1418677&docTitle=Feature+and+Technical+Overview

Burnette, Michael, Forensic Examination of a RIM (BlackBerry) Wireless Device (2002)
Retrieved June 20th, 2008 from
http://www.rh-law.com/ediscovery/Blackberry.pdf

© SANS Institute 2009, Author retains full rights.

Faraday Cage. (n.d). Retrieved June 28, 2008 from, Wikipedia http://en.wikipedia.org/wiki/Faraday_cage

National Institute of Standards and Technology, Cell Phone Forensic Tools (2005)
Retrieved July 5th, 2008 from
http://csrc.nist.gov/publications/nistir/nistir-7250.pdf

Anton Piller Order. (n.d). Retrieved January 19, 2009 from, http://en.wikipedia.org/wiki/Anton_Piller_order

© SANS Institute 2009, Author retains full rights.

© SANS Institute 2009, Author retains full rights.

Other References Accessed & Used

http://www.blackberryforums.com/
http://www.csparks.com/MotoBackup/MotorolaAT.xhtml
http://www.forensicswiki.org/
http://ab.id.au/MotorolaATCommands
http://mobileforensics.wordpress.com/
http://modmymoto.com
http://www.linux.com/feature/123251
http://www.e398mod.com
http://www.processtext.com

© SANS Institute 2009, Author retains full rights.

© SANS Institute 2009, Author retains full rights.