2011

A Comparison of Forensic Evidence Recovery: Techniques for a Windows Mobile Smart Phone

George Grispos
University of Nebraska at Omaha, ggrispos@unomaha.edu

Tim Storer
University of Glasgow

William Bradley Glisson
University of Glasgow

Recommended Citation

Grispos, George; Storer, Tim; and Glisson, William Bradley, "A Comparison of Forensic Evidence Recovery: Techniques for a Windows Mobile Smart Phone" (2011). *Interdisciplinary Informatics Faculty Publications*. 45.
https://digitalcommons.unomaha.edu/interdiscipinformaticsfacpub/45

A Comparison of Forensic Evidence Recovery Techniques for a Windows Mobile Smart Phone

George Grispos[a], Tim Storer[a,*], William Bradley Glisson[b]

[a]*School of Computing Science, University of Glasgow, Lilybank Gardens, Glasgow, G12 8QQ, Scotland.*
[b]*School of Humanities, University of Glasgow, University Gardens, Glasgow, G12 8QQ, Scotland.*

Abstract

Acquisition, decoding and presentation of information from mobile devices is complex and challenging. Device memory is usually integrated into the device, making isolation prior to recovery difficult. In addition, manufacturers have adopted a variety of file systems and formats complicating de-coding and presentation.

A variety of tools and methods have been developed (both commercially and in the open source community) to assist mobile forensics investigators. However, it is unclear to what extent these tools can present a complete view of the information held on a mobile device, or the extent the results produced by different tools are consistent.

This paper investigates what information held on a Windows Mobile smart phone can be recovered using several different approaches to acquisition and decoding. The paper demonstrates that no one technique recovers all information of potential forensic interest from a Windows Mobile device; and that in some cases the information recovered is conflicting.

Keywords: Windows Mobile, Digital Forensics

[*]Corresponding author. Tel: 0044 141 330 4970, Fax 0044 141 330 4913

Email addresses: `0906129G@student.gla.ac.uk` (George Grispos), `timothy.storer@glasgow.ac.uk` (Tim Storer), `Brad.Glisson@glasgow.ac.uk` (William Bradley Glisson)

1. Introduction

Mobile phones and related devices are now a critical component of the global ICT infrastructure. Smart phone (mobile phones with superior processing speed and memory) sales increased during 2010 with over 60 million units sold in the second quarter of 2010 (Gartner, 2010). Smart phones can run a variety of 'desktop' applications and are typically capable of connecting to the World Wide Web and other Internet based services. As the smart phone has effectively become 'the Internet in your pocket', it could also play an important role in future investigations involving Internet related crime.

Evidence from mobile phones has played an increasing role in recent years in the United Kingdom. For example, mobile phone evidence was used in the prosecution of Ian Huntley (Summers, 2003), and also used to locate and apprehend suspects in the failed London car bomb attacks in 2007 (Fresco, 2010). Investigators in the later case, who examined recovered mobile phones and SIM cards, found phone numbers belonging to further members of the terror cell, subsequently leading to their arrest. Mobile phones have also been recovered from inmates in prison and forensic evidence recovered from these devices has shown that criminals are committing further crimes even when they have been sentenced to long jail terms (Whitehead, 2009).

The established approach to digital forensics (developed for personal computers) is generally inappropriate for mobile devices. Typically, the computer is isolated and then the hard disk is removed (ACPO, 2007). However, the internal memory of a mobile phone device is usually integrated with other components. Memory chips must be de-soldered from the device's printed circuit board (PCB) to achieve isolation, risking permanent damage to private property (Willassen, 2005). In some cases, an examiner can instead access the memory via firmware or or by interacting with the device's operating system to gain access to the logical objects stored in the device's file system (Jansen and Ayers, 2007). However, this makes the examiner dependent on the fidelity of the firmware and software on the device. Once an acquisition has been completed successfully, the data acquired must be decoded. However, there is no standard format of accumulating information in a mobile phone or standard file system (Moore, 2006), and different manufacturers and models of mobile device will amass the same types of information (call records, SMS messages) using different file formats.

Consequently, recovering evidence from mobile devices in accordance with established principles of forensic evidence is complex and challenging (ACPO, 2007; Jansen et al., 2008). Different approaches and toolkits may recover only subsets of data on mobile devices, or recover artifacts inaccurately. Imperfections in the evidence presented to a forensic investigator may not be apparent from a single tool (or even several different tools).

The capabilities of different mobile forensic tools and approaches can be better understood by comparing the results obtained from a carefully prepared test device. A comparison demonstrates the limitations of different approaches; assists a forensic examiner in justifying why different data sets are recovered using different methods; and helps to detect defects in the forensic software.

This paper describes an experiment which compared several methods for recovering evidence from a Windows Mobile smart phone (WMS). The contribution of the paper is two-fold; the paper presents a comparison of information recovery techniques for a single device; and a number of aspects of the Windows mobile platform of relevance to forensics practitioners are identified and documented.

The hypothesis that guides the research proposed in this paper is as follows:

> **$\mathbf{H}_1$:** different information recovery techniques yield diverse and inconsistent results sets for Windows mobile smart phone devices.

Three supplementary research questions are also to be examined:

1. Is it possible to recover deleted data from a binary image of a Windows Mobile device memory?
2. What embedded databases or artifacts can be retrieved from a physical acquisition that cannot be retrieved using a logical acquisition?
3. How efficient are current digital forensics products in locating all the evidence on a Windows Mobile device?

The paper is structured as follows. Section 2 describes the available technology for mobile phone forensics and for Windows smart phone devices in particular, and reviews previous empirical investigations of mobile forensic applications. Aspects of the Windows Mobile operating system architecture relevant to the experiment are also described. Section 3 introduces the design of the experiment used to investigate the hypothesis given above, and Section 4 reports the results and also some of the qualitative observations made during the experiment. Finally, Section 5 draws broader conclusions from the experiment and proposes future work.

2. Literature Review

This section will discuss the state of the art regarding Windows mobile smart phones (WMSs).

2.1. Acquisition Methods

Various acquisition methods are available for extracting evidence from mobile devices and specifically WMSs. Different methods are generally categorized as being either a physical or logical acquisition.

Physical acquisition tools recover binary representations of the internal memory of mobile devices and dump them to files. It is possible to acquire a memory image from a mobile device by performing a 'forensic de-soldering' of the internal memory chip(s) from the device's printed circuit board (PCB) (Willassen, 2005). However, this approach is rather invasive and risks damaging the mobile device. A less invasive approach is to interact with the device memory via JTAG ports attached to the PCB, however, these are not available on all models (Breeuwsma et al., 2007). These two methods can be used to circumvent security codes on mobile phones, allowing an investigator to retrieve evidence from devices which are deemed to be 'locked' (Klaver, 2010).

Klaver coined the term 'pseudo physical acquisition' (Klaver, 2010), which describes the type of acquisition performed by a variety of tools. These tools interact with a Hardware Abstraction Layer (HAL), a generic term for software which abstracts hardware specific features from other operating system components. Typically, this requires running additional software on the mobile device, either by diverting the device's boot sequence or using remote control applications such as Microsoft's ActiveSync. Two commercial toolkits are available for performing a pseudo physical acquisition from mobile devices. XRY Physical, developed by MicroSystemation, which loads the acquisition software onto the device directly from a personal computer, and Cellebrite's Universal Forensic Extraction Device (CUFED) Physical Pro, which is a Windows CE based flasher box, that loads an application from the flasher box to the device using ActiveSync. Both toolkits have been assessed under the National Institute of Standards and Technology's Forensics Tool Testing Project. The XRY toolkit was assessed against the test plan for GSM (Global System for Communication) standard devices (Allen, 2008; National Institute for Justice, 2008) and the CUFED toolkit was assessed against the non-GSM test plan (Kuhn, 2009; National Institute for Justice, 2009). Neither tool has been assessed against the smart phone test plan (Kuhn, 2010). The RAPI tools developed by Hengeveld can also be used to perform a pseudo physical acquisition (Hengeveld).

Finally, Rehault has demonstrated that it is possible to create a memory image by using a bootloader. This approach has been demonstrated on a Windows-based 'Kaiser 130' mobile device. Rehault was able to transfer a binary image of the device's memory to a personal computer (Rehault, 2010).

Logical acquisition tools interact with a mobile device's operating system to recover the logical objects stored in a mobile device's file system, rather than the raw image of a memory chip. XRY Logical by MicroSystemation and the Standard version of the Universal Forensic Extraction Device by Cellebrite can be used to perform a logical acquisition. The Mobile Internal Acquisition Tool (MIAT) can also be used to perform a logical acquisition and was developed specifically for WMSs (Dellutri et al., 2008). The MIAT software is stored on an external flash memory card (e.g. SD card), which is inserted into the target device. After executing the application the resulting acquisition is then stored on the memory card, which is removed from the device for further analysis of the files acquired.

Several tests have demonstrated that 'on-the-phone' tools such as MIAT can miss forensically significant artifacts on mobile phones, including on WMSs (Dellutri et al., 2008; Mokhonoana and Olivier, 2007). This is due to the operating system 'withholding' these files from such acquisition tools.

Jahankhani (Jahankhani, 2009) describes several logical acquisition tools, which can be used to examine a smart phone, but does not perform any testing; these tools include BitPim, Oxygen Phone Manager, Paraban Cell Seizure and MOBILedit. (Williamson et al., 2006) conducted several tests on Nokia mobile phones using TULP 2G, MOBILedit, Paraban Cell Seizure and Oxygen Phone Manager. The main results from these tests show that these tools cannot be used to recover deleted data and that different tools recover different information from the test devices. The information not recovered by some of the tools included call logs and SMS messages.

This paper will focus on the use of Cellebrite's Universal Forensic Extraction Device (CUFED) as an acquisition tool. This is because alternative tools such as XRY Physical and the RAPI toolkit have been well documented by Casey et al. (Casey et al., 2010) and Klaver (Klaver, 2010) respectively.

2.2. Windows Mobile Analysis

So far, there are only exploratory investigations of forensic approaches for WMSs. The Windows Mobile operating system has a number of similarities with the Windows desktop OS, including file system structure, directory layout and the common presence of many files and applications (Casey et al., 2010). WMSs use the Transaction Safe- FAT (TFAT) file system to manage persistent memory, which has a similar layout to the FAT file system on which it is based (Casey et al., 2010). In addition, the directory structure on Windows Mobile devices is similar to that of the Windows desktop operating system, including directories such as '`Document and Settings`', '`My Documents`' and '`Program Files`'.

Short-message service (SMS) messages, personal contact records and phone call records are stored in the embedded databases in the files `cemail.vol` and `pim.vol` in the root directory of the WMS file system. Casey et al. has reviewed files of interest to a forensic investigator on a Windows Mobile; and proposed a method for examining the contents of the `cemail.vol` file using a Windows Mobile emulator, having extracted the file from the device (Casey et al., 2010).

Klaver has also investigated the `cemail.vol` and `pim.vol` files, and has developed several tools to extract information from them. The `xpdumpcedb.exe` tool (developed for use with Windows XP) can be used to recover information from the `cemail.vol` file, after it has been extracted from the binary image. A second tool,`wmdumpedb.exe`, was developed to examine `pim.vol`, but this tool can only be run on a Windows CE device or emulator. Both of these tools export their results to an XML file. Furthermore, Klaver has also developed a Python script called, `cedbexplorer.py`, which can be used to recover both active and deleted data from the `cemail.vol` file on a Windows XP system. This tool has been made available by Klaver for inclusion in this paper as a comparison to alternative tools (Klaver, 2010).

Rehault has developed Python scripts to reconstruct the TFAT file system, and like Klaver, has also developed a script called `MsgCarving.py` to recover message directory structure and content, including deleted data, from a `cemail.vol` file (Rehault, 2010).

WMSs, like their desktop counterparts, which run Windows, use a registry to house information about the mobile device. Such information can include configuration of the device and user settings, which is stored in files called hives. Rehault used a custom-built tool to extract registry keys and information from hives, which revealed a wealth of information (Rehault,

(a) HTC Touch Pro 2

(b) Cellbrite UFED

Figure 1: Equipment Used for the Experiment

2010). Casey et al. have also examined the Windows Mobile registry using Microsoft Remote Registry Editor to examine various registry hives (Casey et al., 2010). This paper will not deal with the issue of the Windows Mobile registry and its hives as this has been well documented elsewhere.

Whether it is a physical or a logical acquisition method used to examine a mobile phone, the problem identified from the literature is that different acquisition tools and methods recover different subsets of data from memory. This has left forensic investigators needing to use more than one tool to be confident that they are extracting all the evidence from the device they are examining. In addition, it is not clear that the superset of data recovered using all the different toolkits is consistent.

3. Experiment Design

The Windows Mobile smart phone used for this work was a HTC Touch Pro2 (Figure 1(a)), which runs version 6.1 Professional of the operating system (referred to hereafter as ‘the device’). The model was chosen because of compatibility with the acquisition toolkit used in the experiment. The device features include 288Mb of RAM and a further 512Mb of internal flash memory; is equipped with GSM, Bluetooth and wireless connectivity; and a camera.

Figure 2 illustrates the overall process of the experiment. In summary, the device was pre-loaded with a test data set designed to explore the research questions listed above. A logical and physical acquisition of the device memory was undertaken using Cellebrite’s Universal Forensics Extraction Device

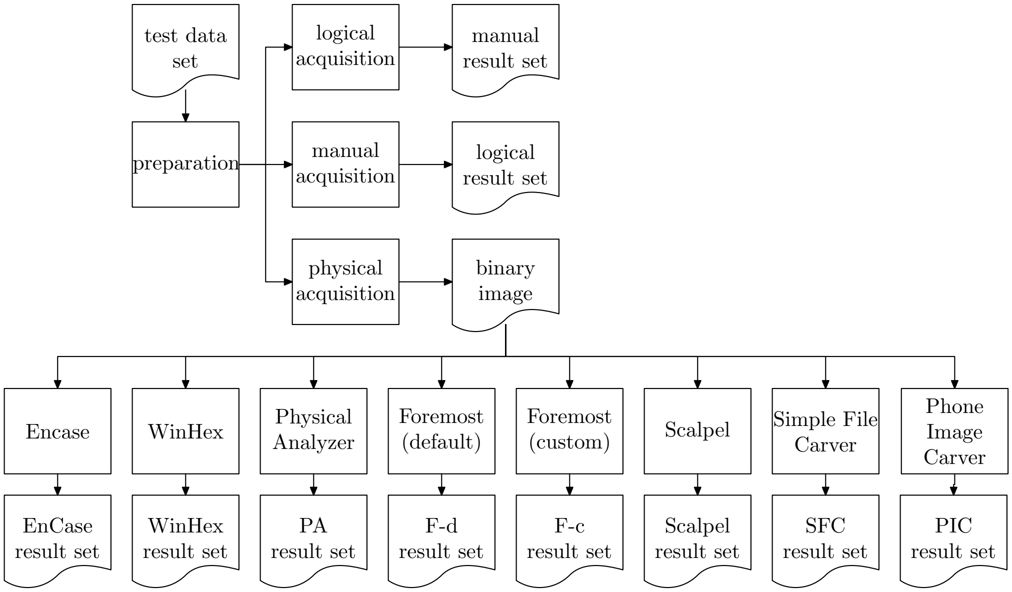


Figure 2: Progression of the Experiment

(Figure 1(b)) Physical Pro edition, version 1.1.3.8. The results of the physical acquisition were decoded using a selection of different tools and the results were compared to those of the logical acquisition and a manual inspection of the device's contents using the device user interface.

3.1. Preparation

A pre-examination of the device was undertaken to determine the data types supported, so that a suitable data set of these files and artifacts could be constructed. For example, textual documents are handled by the Windows Mobile version of Microsoft Word 2007, which supports Word 2007 XML Document (.docx extension), Rich Text Format (.rtf) and Text (.txt) file formats. Consequently, textual documents in the experimental data set were only created in these formats.

The device was also examined to determine which pre-installed applications on the device could generate artifacts of potential forensic value through their use. Two web browsers were selected for the experiment: Internet Explorer and Opera.

The Touch Pro2 was not supplied with an external memory card. Examination of external media has been investigated previously (Jansen and Ayers, 2007), so no external memory was added to the device.

An experimental data set was constructed, consisting of 82 files and artifacts, to include most of the types of data usually found on a WMS.

A number of methods were used to load the data set onto the device, in a manner that would mimic the normal usage of the device:

- creating data via the user interface, e.g. using Microsoft Word to create a document, using the on-device camera to take a picture and browsing the Internet to create web history;
- receiving data using the Bluetooth and wireless connection, e.g. from another mobile device;
- communication via GSM e.g. sent and received SMS messages and making a phone call; and
- deletion of data just prior to the beginning of the forensic acquisition stage.

The device was connected to an unsecured wireless network to access the Web and a Blackberry 8520 was used as the 'other' device for the Bluetooth connection. A T-Mobile (UK) pay-as-you go SIM card was used for performing GSM communication.

The data set is split into three subsets:

- smart phone data, i.e. data generally found on a smart phone and not a conventional mobile phone. Examples of this include Office files, Website favourites and multimedia files (Table 1);
- telephony artifacts found on conventional mobile phones, for example SMS messages, call logs and personal contact information (Table 2); and
- a combination of artifacts and files which were added to the device using the same methods described in Tables 1 and 2 were deleted prior to performing the first acquisition (Table 3).

Message-Digest 5 (MD5), context triggered piecewise hash (fuzzy hashes) and file header information of each file was also recorded (where appropriate), for use during the analysis section of the experiment.

Table 1: Smart Phone Test Set Data

Item	Type	Size	Created by	Item	Type	Size	Created by
1	docx	9677b	on phone	10	jpg	165Kb	bluetooth
2	docx	155Kb	emailed	11	jpg	640Kb	camera
3	rtf	9Kb	emailed	12	jpg	695Kb	camera
4	txt	78b	on phone	13	jpg	640Kb	camera
5	xlsx	91Kb	emailed	14	mp3	1623Kb	bluetooth
6	pptx	962Kb	emailed	15	wav	9073Kb	bluetooth
7	pdf	227Kb	emailed	16	avi	2297Kb	bluetooth
8	pdf		web/wireless	17	wmv	4800Kb	bluetooth
9	jpg		web/wireless	18	mp4	8742Kb	bluetooth

3.2. Forensic Acquisition

A physical acquisition of the device was performed immediately after the test data set was loaded. The device was connected to the source port of the CUFED using the appropriate cable and a 2GB USB flash drive (forensically wiped using Department of Defense Computer Forensics Lab dd tool (dcfldd) version 1.3.4) was connected to the target port. Following instructions from the CUFED, ActiveSync was enabled on the device (this is necessary for a software client, `WMDmp111.exe`, to be transferred to the device). The device make and model were selected and confirmed. The USB flash drive was selected as the target media. The acquisition then proceeded, taking approximately 1 hour to complete. Four image files were created on the USB flash drive, as well as a text file containing a log of the acquisition and a .ufd file, which is used by the software accompanying CUFED (Physical Analyzer) to recover the device file system and artifacts from the image (hereafter the 'Physical Analyzer result set').

The logical acquisition was performed immediately after the physical acquisition and followed a similar process to the one described above, except that the transferred software client interacted with the device file system, rather than lower level software. The logical extraction took 6 minutes and 17 seconds to complete. The CUFED confirmed that the acquisition was successful, and displayed the device's International Mobile Equipment Identity (IMEI) number. After completing the acquisition, the contents of the USB Flash drive were examined (hereafter the 'logical result set'). CUFED created a summary report in HTML format, as well as a report of the Phonebook entries and three directories called ('Audio', 'Video' and 'Images').

Finally, a manual examination of the device was conducted via the device user interface. A log of all actions taken during the examination was

Table 2: Mobile Phone Test Set Data

Item	Type
19	Appointment
20	Appointment
21	Appointment
22	Appointment
23	Appointment
24	Contacts
25	Contacts
26	Contacts
27	Contacts
28	Contacts
29	Email Sent
30	Email Sent
31	Email Received
32	Email Received
33	SMS Sent
34	SMS Sent
35	SMS Sent
36	SMS Received
37	SMS Received
38	SMS Messages Received
39	Visited Website(Explorer)
40	Visited Website(Explorer)
41	Visited Website(Explorer)
42	Visited Website(Explorer)
43	Visited Website(Explorer)
44	Visited Website(Opera)
45	Visited Website(Opera)
46	Visited Website(Opera)
47	Visited Website(Opera)
48	Visited Website(Opera)
49	Visited Website(Opera)
50	Visited Website(Opera)
51	Favourite Websites
52	Call From
53	Call From
54	Call From
55	Call To
56	Call To

maintained and a digital camera was used to provide supplementary documentation of the state of the user interface after each step. The log and camera were also used to record the information observed on the device during the examination.

3.3. Decoding Methods

Table 4 lists the software tools used to examine the binary image produced using the CUFED, categorised as either file system based forensic toolkits or file carvers. The forensic toolkits use file system information to locate and recover logical files. File carving tools can be used to recover files and data from hard disk drives; and in particular drives which have been formatted, or files that have been deleted. File carvers bypass the file system and instead use file signatures or file headers and trailers to locate and carve files from a binary image (Roussev, 2005).

Further manipulation of the logical result set (also produced using the CUFED) is not necessary, since the logical artifacts are provided by the device operating system. Similarly, the manual acquisition result set cannot be processed further, since it is based on observations of the device user interface.

Table 3: Deleted Test Set Data

Item	Type	Size(Kb)	Created by	Item	Type
57	docx	18	emailed	69	Appointment
58	xlsx	11	emailed	70	Appointment
59	pptx	67	emailed	71	Contacts
60	pdf		web/wireless	72	Contacts
61	jpg	36	bluetooth	73	Email Sent
62	jpg	93	bluetooth	74	Email Sent
63	jpg	1953	bluetooth	75	SMS Sent
64	jpg	58	bluetooth	76	SMS Sent
65	mp4	1863	bluetooth	77	SMS Sent
66	wmv	10105	bluetooth	78	Visited(Explorer)
67	mp4	5788	bluetooth	79	Visited(Explorer)
68	avi	4004	bluetooth	80	Call From
				81	Call From
				82	Call To

Each method produced a result set of recovered files. Each file or artifact in these results sets was then compared with the original file or artifact in the test set and categorized as follows:

Full recovery (F) : Full recovery of the file with an MD5 hash matching that of the original file.

Partial (P) : Contents of the file were recovered, and file appears to be the same as the original (via a visual inspection), but the MD5 hashes do not match. In the case of audio and video files, the recovered file plays a similar length to the original file.

Detected (D) : Contents were recovered for the file, but were noticeably different from the original file. Audio and video files, did not play in VLC media player. Images were classified as 'detected' if a recognisable but smaller version of the image was recovered. A file was also classified as detected if its fuzzy hash score was 0.

Not Applicable (N) : The file was not supported by the method used, or was not detected during the process of using that specific method.

Table 4: Tools used to examine the Binary Image

tool	**url**
Physical Analyzer 1.1.3.8	`http://www.cellebrite.com/forensic-products/ufed-physical-pro.html`
WinHex Forensic Edition 15.4 SR-5	`http://www.x-ways.net/winhex/index-m.html`
Forensic Toolkit 3.0.1.2052	`http://accessdata.com/products/forensic-investigation/ftk`
Encase 6.13.0.43	`http://guidancesoftware.com/`
Foremost 1.5.7	`http://foremost.sourceforge.net/`
Scalpel 1.60	`http://www.digitalforensicssolutions.com/Scalpel/`
Simple File Carver 1.6	`http://www.simplecarver.com/`
Phone Image Carver 1.2.8.52	`http://www.phoneimagecarver.com/`

Contents of files categorised as ‘partial’ or ‘detected’ were compared using a context triggered piecewise hash (fuzzy hash), implemented in the open source program SSdeep. Fuzzy hashes can be used to measure the similarity of two files, by breaking the file in question into smaller blocks and then calculating the hash of each block (Kornblum, 2006). SSdeep reports a similarity value between 0-100 for two files, with 100 meaning that they are the same.

3.4. File Carving Smart Phone Memory Dumps

Each of the file carving applications were configured to recover file types with signatures in the formats shown in Table 5 (prevailing file extensions are given for brevity of identification of the format). Header and trailer signatures can be specified for Scalpel and Foremost, as well as a maximum size of file to carve when a trailer is not found, or is not part of the file format. An online database of file signatures was used to extend the default file formats supported by each of the carvers where possible (Kessler, 2010).

Simple File Carver cannot be configured with a file signature specific maximum file size. Instead, a single global maximum file size value is defined for all file signatures, and this results in every file type being recovered as the same size. Files smaller than the limit will potentially contain ‘junk’ from other files, whilst files larger than the maximum size may not be completely recovered. For this work, the maximum file size was set to 15Mb.

Phone Image Carver is specifically designed for mobile phone image carving. The tool supports over 300 file types, but does not allow further file types to be added to its database, which meant a number of file types from the data set would not be detected.

Table 5: File Carver Configurations

File Carver	gif	jpg	avi	wav	mp3	mp4	wmv	mov	html	pdf	rtf	docx	xls,ppt	xslx, pptx	zip
Scapel	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓					✓
Foremost (default)	✓	✓	✓	✓			✓	✓	✓	✓		✓		✓	✓
Foremost (configured)	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓		✓		✓	✓
Simple File Carver		✓	✓	✓	✓	✓	✓			✓		✓		✓	✓
Phone Image Carver		✓	✓	✓	✓	✓	✓		✓	✓	✓	✓	✓	✓	✓

3.5. Recovering Artifacts from Files

None of the file carving tools used can directly extract artifacts from within files. Such information includes the contents of the two volumes `cemail.vol` and `pim.vol`, or data such as websites visited using the web browsers on a WMS. Instead, the file carving tools were configured to search for files containing these types of content and two string extractor tools (BinText and Strings) were used to recover the information artifacts.

3.5.1. Embedded Databases

We are unaware of a published source of information relating to the file headers for these files, so they were obtained during the analysis of the file system using Physical Analyzer. However, when the extraction was repeated to verify the information recovered, it was discovered that these header sequences had changed, so cannot be used to repeatedly recover embedded databases from Windows Mobile devices. The information was used to configure the two Linux based file carving tools and Simple File Carver, and both files were recovered. The two recovered files were then processed using the two string extractor tools.

Using the method discussed by Klaver (Klaver, 2010), an alternative method of recovering data from `cemail.vol` was also examined. A Windows XP system running Python version 3.1.3 was used to execute the script `cedbexplorer.py` from the command line. This script took as input the `cemail.vol` file, extracted from the binary image using Physical Analyzer, and produced output as a log file.

3.5.2. Internet Explorer History

The contents of the file:

```
\Windows\Profiles\guest\History\History.IE5\index.dat
```

were examined using the hex viewer in Physical Analyzer, which revealed a common pattern for identifying websites visited using the Internet Explorer web browser. The word '`Visited`' appears before the website address of the website history record, as can be seen in Figure 3. The history file for Opera, the second web browser on the device, has no file header nor do any of the addresses have a common starting reference, which makes file carving the Opera history file more difficult.

```
00 00 00 00 00 00 00 00 56 69 73 69 74 65 64 31 | ........Visited1
20 64 65 66 61 75 6C 74 40 68 74 74 70 3A 2F 2F |  default@http://
65 64 69 74 69 6F 6E 2E 63 6E 6E 2E 63 6F 6D 2F | edition.cnn.com/
41 46 52 49 43 41 2F 3F 66 62 69 64 3D 48 4A 65 | AFRICA/?fbid=HJe
5A 58 6F 54 4C 35 79 4D 00 00 00 00 10 00 02 00 | ZXoTL5yM........
00 00 00 10 00 00 00 00 00 00 00 00 94 00 10 1F | ................
41 00 66 00 72 00 69 00 63 00 61 00 20 00 4E 00 | A.f.r.i.c.a. .N.
65 00 77 00 73 00 20 00 2D 00 20 00 48 00 65 00 | e.w.s. .-. .H.e.
61 00 64 00 6C 00 69 00 6E 00 65 00 73 00 2C 00 | a.d.l.i.n.e.s.,.
20 00 53 00 74 00 6F 00 72 00 69 00 65 00 73 00 |  .S.t.o.r.i.e.s.
20 00 61 00 6E 00 64 00 20 00 56 00 69 00 64 00 |  .a.n.d. .V.i.d.
65 00 6F 00 20 00 66 00 72 00 6F 00 6D 00 20 00 | e.o. .f.r.o.m. .
43 00 4E 00 4E 00 2E 00 63 00 6F 00 6D 00 20 00 | C.N.N...c.o.m. .
49 00 6E 00 74 00 65 00 72 00 6E 00 61 00 74 00 | I.n.t.e.r.n.a.t.
69 00 6F 00 6E 00 61 00 6C 00 00 00 00 00 00 00 | i o n a l.......
```

Figure 3: Record of a Visited Website in the index.dat File

3.5.3. Internet Favourites

The two web browsers share a common ‘Favourites’ favourite websites repository. This information is stored in the directory `\Windows\Favourites`. The file contents of the directory were also inspected with the hex viewer in Physical Analyzer. Every file in this folder has a header beginning with the string `"[InternetShortcut]"`, which was used in a similar way as for locating and recovering the web history files from the binary image.

3.5.4. Email Messages

Email messages were also searched for using the file carvers. Emails are stored in a plain text encoding, and were found to use one of these headers:

```
MIME Delivered-To

Return-Path
```

The content was carved from the binary image and was viewable in either a text editor or could be decoded using Forensic Toolkit (FTK), Encase, or an email application.

4. Results

An initial survey of the four binary image files created by the physical acquisition revealed that user data was only stored on the fourth file - `04_FLASHDR_Part03.bin`, using a TFAT file system. Inspection of files `01_FLASHDR_Part00.bin` and `02_FLASHDR_Part01.bin` using the strings tool revealed that they contained operating system binaries. File `03_FLASHDR_Part02.bin` contained a factory default image for the user partition. All further analysis discussed below took place using the `04_FLASHDR_Part03.bin` file only.

A summary of the performance of each of the file recovery methods is given in Table 6. The table shows that there is considerable diversity in the information artifacts recovered by the different toolkits. In general, the toolkits which utilised file system information were better able to recover information artifacts more accurately. However, the file carvers, which did not depend on the fidelity of the file system were able to recover deleted information not detected by the other toolkits.

Looking across the table, a number of entries in the test set presented challenges to all the recovery approaches. For example, one .pdf file (item 8) was less well recovered by all the approaches compared with the other .pdf file (item 7). Many of the tools are unable to completely recover the Office documents, whereas all of the .jpg image files were at least detected by all the toolkits except Phone Image Carver. The following subsections discuss the different approaches in more detail.

4.1. Logical Acquisition

All .jpg, .wav, .mp4, and .mp3 files were fully recovered from the device. Office documents (.docx, .pptx, .xlsx), .pdf, .avi and .wmv files were not recovered at all. Call logs, and personal contacts were fully recovered from the device. Appointments, emails, web history and web favourites were not recovered. Deleted files and artifacts were not detected by the logical acquisition.

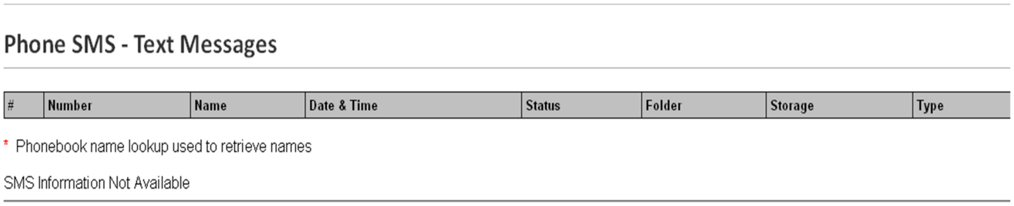
The Cellebrite documentation states that the version of CUFED used should recover SMS messages from the device model (Cellebrite, 2010a). However, an examination of the report revealed that no SMS messages were recovered (Figure 4).

4.2. Manual Examination

The manual examination partially recovered all of the files from the test set still present in the file system. Full recovery (according to the defini-

Table 6: Comparison of File and Artefact Recovery Performance by Method (F=full,P=partial,D=detected,N=not applicable)

Item	**Type**	**Logical Acquisition**	**Manual Examination**	**Physical Analyzer**	**Scalpel (configured)**	**Foremost (default)**	**Foremost (configured)**	**Simple File Carver**	**Phone Image Carver**	**WinHex (modified image)**
1	docx	N	P	F	N	P	N	N	D	F
2	docx	N	P	F	N	P	N	N	D	F
3	rft	N	P	F	N	N	N	N	N	F
4	txt	N	P	F	N	N	N	N	N	F
5	xslx	N	P	F	N	P	N	N	N	F
6	pptx	N	P	F	N	P	N	N	N	F
7	pdf	N	P	F	F	F	P	D	P	F
8	pdf	N	P	F	D	D	D	D	D	F
9	jpg	F	P	F	D	F	D	D	D	F
10	jpg	F	P	F	D	F	D	D	D	F
11	jpg	F	P	F	D	F	D	D	N	F
12	jpg	F	P	F	D	F	D	D	N	F
13	jpg	F	P	F	D	F	D	D	D	F
14	mp3	F	P	F	P	N	P	N	D	F
15	wav	F	P	F	P	P	P	P	P	F
16	avi	N	P	F	D	D	D	N	D	F
17	wmv	N	P	F	P	P	P	P	P	F
18	mp4	F	P	F	D	N	D	N	N	F
19-23	Appointments	N	P	N	N	N	N	N	N	N
24-28	Contacts	F	P	N	N	N	N	N	N	N
29-30	Email Sent	N	P	P	F	N	F	F	N	N
31-32	Email Received	N	P	P	F	N	F	F	N	N
33-35	SMS Sent	N	P	P	N	N	N	N	N	N
36-38	SMS Received	N	P	F	N	N	N	N	N	N
39-43	Visited (IE)	N	P	P	F	N	F	F	F	P
44-50	Visited (Opera)	N	P	P	N	N	N	N	N	P
51	Favourite Websites	N	P	P	F	N	F	F	F	P
52-54	Call From	F	P	N	N	N	N	N	N	N
55-56	Call To	F	P	N	N	N	N	N	N	N
57-68	Deleted Files	N	N	D	N	N	N	N	N	D
69-70	Deleted Appointments	N	N	N	N	N	N	N	N	N
71-72	Deleted Contacts	N	N	N	N	N	N	N	N	N
73-74	Deleted Emails	N	N	N	N	N	N	N	N	N
75-77	Deleted SMS	N	N	N	N	N	N	N	N	N
78-79	Deleted Visited	N	N	N	N	N	N	N	N	N
80-82	Deleted Call Logs	N	N	N	N	N	N	N	N	N
Full		18	0	21	11	6	10	10	6	18
Partial		0	56	20	3	6	4	3	3	0
Detected		0	0	12	8	2	8	6	8	12
Not applicable		64	26	29	60	68	60	63	65	52



Phone SMS - Text Messages

#	Number	Name	Date & Time	Status	Folder	Storage	Type

* Phonebook name lookup used to retrieve names

SMS Information Not Available

Figure 4: Report of SMS messages Recovered by Logical Acquisition

tion given above) is not possible via manual examination, because the MD5 hash of the recovered file cannot be established from the user interface on the device. Artifacts such as Internet Explorer history, favourite websites and emails can be accessed using the appropriate application on the device. Unsurprisingly, manual examination did not recover deleted files and data types.

4.3. Physical Analyzer

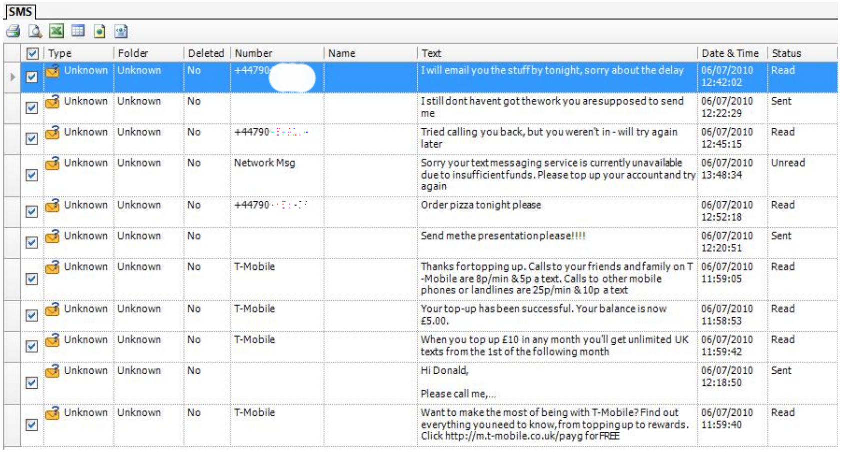
The application successfully reconstructed the TFAT file system from the binary image file, using information found in the accompanying UFD file. Several file and artifact types were decoded automatically by the application, as documented by Cellebrite including SMS and Email messages (Cellebrite, 2010b). Further processing of file contents is necessary when files are not decoded and presented automatically by the Physical Analyzer software.

All the audio and video file formats (.mp3, .mp4, .avi, .wmv and .wav), and .jpg images were fully recovered (the MD5 hashes matched the original files in the test set).

Files that are recovered but not decoded (for presentation) by Physical Analyzer include, .docx, .xlsx, .pptx, .pdf, .txt and .rtf. However, these files can be exported from Physical Analyzer and viewed in a native application (e.g. Microsoft Word 2007 for .docx documents).

Website page history for both the Opera and Internet Explorer web browsers as well as the favourite websites can be viewed using the hex viewer available in Physical Analyzer, or exported and run through a strings extractor. Contact information, calendar appointments and call log information were not recovered automatically from the `cemail.vol` and `pim.vol` volumes.

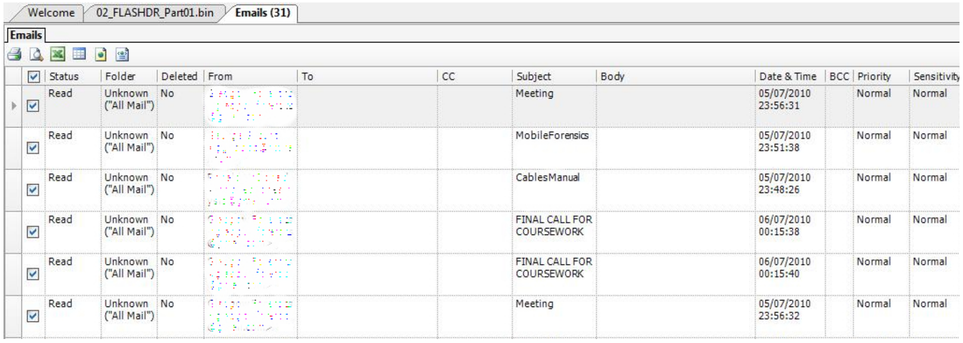
Some discrepancies between the documentation and performance of Physical Analyzer were also noted. The 'Number' field in SMS messages sent from the device was not recovered using Physical Analyzer, although all other



SMS

☑	Type	Folder	Deleted	Number	Name	Text	Date & Time	Status
☑	Unknown	Unknown	No	+44790[redacted]		I will email you the stuff by tonight, sorry about the delay	06/07/2010 12:42:02	Read
☑	Unknown	Unknown	No			I still dont havent got the work you are supposed to send me	06/07/2010 12:22:29	Sent
☑	Unknown	Unknown	No	+44790[redacted]		Tried calling you back, but you weren't in - will try again later	06/07/2010 12:45:15	Read
☑	Unknown	Unknown	No	Network Msg		Sorry your text messaging service is currently unavailable due to insufficient funds. Please top up your account and try again	06/07/2010 13:48:34	Unread
☑	Unknown	Unknown	No	+44790[redacted]		Order pizza tonight please	06/07/2010 12:52:18	Read
☑	Unknown	Unknown	No			Send me the presentation please!!!!	06/07/2010 12:20:51	Sent
☑	Unknown	Unknown	No	T-Mobile		Thanks for topping up. Calls to your friends and family on T -Mobile are 8p/min &5p a text. Calls to other mobile phones or landlines are 25p/min & 10p a text	06/07/2010 11:59:05	Read
☑	Unknown	Unknown	No	T-Mobile		Your top-up has been successful. Your balance is now £5.00.	06/07/2010 11:58:53	Read
☑	Unknown	Unknown	No	T-Mobile		When you top up £10 in any month you'll get unlimited UK texts from the 1st of the following month	06/07/2010 11:59:42	Read
☑	Unknown	Unknown	No			Hi Donald, Please call me,...	06/07/2010 12:18:50	Sent
☑	Unknown	Unknown	No	T-Mobile		Want to make the most of being with T-Mobile? Find out everything you need to know, from topping up to rewards. Click http://m.t-mobile.co.uk/payg for FREE	06/07/2010 11:59:40	Read

Figure 5: Missing SMS Sent To Numbers in the Physical Analyzer Report



☑	Status	Folder	Deleted	From	To	CC	Subject	Body	Date & Time	BCC	Priority	Sensitivity
☑	Read	Unknown ("All Mail")	No	[redacted]			Meeting		05/07/2010 23:56:31		Normal	Normal
☑	Read	Unknown ("All Mail")	No	[redacted]			MobileForensics		05/07/2010 23:51:38		Normal	Normal
☑	Read	Unknown ("All Mail")	No	[redacted]			CablesManual		05/07/2010 23:48:26		Normal	Normal
☑	Read	Unknown ("All Mail")	No	[redacted]			FINAL CALL FOR COURSEWORK		06/07/2010 00:15:38		Normal	Normal
☑	Read	Unknown ("All Mail")	No	[redacted]			FINAL CALL FOR COURSEWORK		06/07/2010 00:15:40		Normal	Normal
☑	Read	Unknown ("All Mail")	No	[redacted]			Meeting		05/07/2010 23:56:32		Normal	Normal

Figure 6: Missing Email Content in the Physical Analyzer Report

fields were recovered, including the date, time and status (see Figure 5). The 'Number' field for SMS messages received by the device was recovered.

The Cellebrite documentation also states that emails are decoded and recovered by Physical Analyzer for the device model (Cellebrite, 2010b). However, although the date, time, status, sender, status and priority fields are recovered, the actual contents of the email body are omitted (Figure 6).

No deleted file contents were recovered, although the file names of deleted files were listed in the report, or presented in the file system view. Flash memory space must be erased before it can be re-used (Casey et al., 2010), and the results suggest that this occurs immediately after deletion in the TFAT file system.

The ability of the Physical Analyzer software to recover data from a

```
00000000 | EB FE 90 4D 53 57 49 4E 34 2E 31 00 08 01 20 00 | ...MSWIN4.1.....
00000010 | 02 00 00 00 00 F8 00 00 01 00 01 00 00 00 00 00 | ................
00000020 | 40 BB 01 00 DE 00 00 00 00 00 00 00 02 00 00 00 | @...............
00000030 | 01 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 | ................
00000040 | 80 00 29 06 00 EA 07 20 20 20 20 20 20 20 20 20 | ...)...
00000050 | 20 20 54 46 41 54 33 32 20 20 00 00 00 00 00 00 | TFAT32 ......
```

(a) Original

```
00000000 | 00 00 00 00 00 00 00 00 00 00 01 00 08 01 20 00 | ................
00000010 | 02 00 00 00 00 F8 00 00 01 00 01 00 00 00 00 00 | ................
00000020 | 40 BB 01 00 DE 00 00 00 00 00 00 00 02 00 00 00 | @...............
00000030 | 01 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 | ................
00000040 | 80 00 29 06 00 EA 07 20 20 20 20 20 20 20 20 20 | ...)...
00000050 | 00 00 00 00 00 00 00 00 20 00 00 00 00 00 00 00 | ........ .......
```

(b) Modified

Figure 7: 'Corrupted' File System Label for the Binary Image File

corrupted file system was tested by replacing the file system type in the boot sector of the binary image with the value `x00` using a hex editor (Figure 7). When the altered binary image was loaded into Physical Analyzer, the software was unable to reconstruct the file system or decode and recover any of the contained files.

4.4. Forensic Toolkits

The FTK and Encase toolkits were unable to recover the file system from the binary image file. The FTK toolkit reported a boot sector error and did not proceed further. No error messages were reported by Encase. The file system was successfully recovered by the WinHex toolkit after altering the file system label from TFAT32 to FAT32 (see Figure 8) and files were recovered as reported in Table 6.

4.5. File Carvers

Recovering files from the binary image file presented several problems from a forensic perspective. Principally, the files recovered were not labelled with the original file names as in the test set (because information in the actual file system is not be used). In addition, very few of the files recovered using this method had matching hashes with their respective originals.

```
00000040 | 80 00 29 06 00 EA 07 20 20 20 20 20 20 20 20 20 |           .)..      .
00000050 | 20 20 54 46 41 54 33 32 20 20 00 00 00 00 00 00 | TFAT32 ......
00000060 | 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 | ................
00000070 | 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 | ................
```

(a) original

```
00000040 | 80 00 29 06 00 EA 07 20 20 20 20 20 20 20 20 20 |           .)..      .
00000050 | 20 20 46 41 54 33 32 20 20 00 00 00 00 00 00 00 | FAT32 .......
00000060 | 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 | ................
00000070 | 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 | ................
```

(b) modified

Figure 8: File System Label for the Binary Image File

Table 7 presents the results of fuzzy hash computations for selected files loaded onto the mobile device. The table also includes the fuzzy hash results for files recovered using WinHex and Physical Analyzer for comparison. These two toolkits utilised the file system information available in the image, so were able to completely and accurately recover the selected files. Results for individual file carvers are discussed below.

4.5.1. Scalpel (configured)

One of the .pdf documents was successfully recovered, whilst the second document was only 'detected' as its file contents were corrupted. Much smaller versions of the five .jpg images from the test set were recovered. The SSdeep score for all five recovered images was a 0 when compared with the original files.

The .mp4 and .avi files were all 'detected' by the carver but could not be reviewed in VLC media player. The .wav and .mp3 files were partially recovered and were playable, and the fuzzy hash scores for these files was 83 and 55 respectively. The .wmv file was also partially recovered with 21 seconds of playable content and had a SSdeep score of 82.

4.5.2. Foremost

Foremost was run in two configurations, default and custom. The default configuration fully recovered all the .jpg images and one of the .pdf files. The Office 2007 (.docx, .pptx, .xlsx) files, .wav and .wmv files were partially recovered, with SSdeep scores ranging from 61 to 99. The .avi file was 'detected' but unplayable and had a fuzzy hash score of 0.

Table 7: Fuzzy Hashes of Selected Test Set Files

Item	**Type**	**Physical Analyzer**	**Scalpel (configured)**	**Foremost (default)**	**Foremost (configured)**	**Simple File Carver**	**Phone Image Carver**	**WinHex (modifed image)**
1	DOCX	100	-	99	-	-	0	100
2	DOCX	100	-	93	-	-	0	100
5	XLSX	100	-	99	-	-	-	100
6	PPTX	100	-	61	-	-	-	100
7	PDF	100	100	100	99	0	54	100
8	PDF	100	0	0	0	0	0	100
9	JPG	100	0	100	0	0	0	100
10	JPG	100	0	100	0	0	0	100
11	JPG	100	0	100	0	0	-	100
12	JPG	100	0	100	0	0	-	100
13	JPG	100	0	100	0	0	0	100
14	MP3	100	55	-	55	-	0	100
15	WAV	100	83	97	97	83	97	100
16	AVI	100	0	0	0	-	0	100
17	WMV	100	82	99	65	65	99	100
18	MP4	100	80	-	80	-	-	100

A custom configuration was enabled by adding extra file type signatures for .mp3, and .mp4 files. This resulted in the .mp4 file being 'detected' but unplayable with a SSdeep score of 80, whilst the .mp3 file was partially recovered with a SSdeep score of 55. The .wmv file was also partially recovered, but with a reduced SSdeep score (65 instead of 99). The .avi file was 'detected' (SSdeep score of 0), and this too was unplayable. In addition, the Office documents recovered using the default configuration were not recovered using the custom configuration. It appears these Office documents are recovered using 'built in functions' which seem to be disabled when a custom configuration is used.

4.5.3. Simple File Carver

The Office 2007 (.docx, .pptx, .xlsx) files, .mp3, .mp4 and .avi files were not recovered. The .pdf, and .jpg files were 'detected', but all of these files had SSdeep scores of 0. The .wav and .wmv were partially recovered with mismatching MD5 hashes and SSdeep scores of over 65. The poor performance of this tool can be attributed to the fact that only a 'global' file size can be specified, and as a result incorrect MD5 hashes and poor SSdeep scores occurred.

4.5.4. Phone Image Carver

.docx files were the only Office documents 'detected' by Phone Image Carver, and both these files had SSdeep scores of 0. The .wmv, .wav and one of the .pdf files were partially recovered, with SSdeep scores of 99, 97 and 54 respectively. Two .jpg image files and the .mp4 file were not recovered by this tool. All other files were 'detected' but did not have sufficient content to be recovered accurately, and had SSdeep scores of 0.

Emails and website history were recovered as .html pages, whilst the favourite websites were recovered as "Internet shortcuts".

4.6. Recovering Artifacts from File Carver Output

Table 8 summarises the results of applying different recovery techniques to information stored in `cemail.vol` and `pim.vol` (volumes). Scalpel, Foremost and Simple File Carver were used to recover text-based artifacts. The contents of the recovered files were then processed using the string extractor tools (Strings and Bintext). The results were compared to the contents of the equivalent files in the Physical Analyzer result set.

Table 8: Comparison of Text Recovery Techniques from `cemail.vol` and `pim.vol`

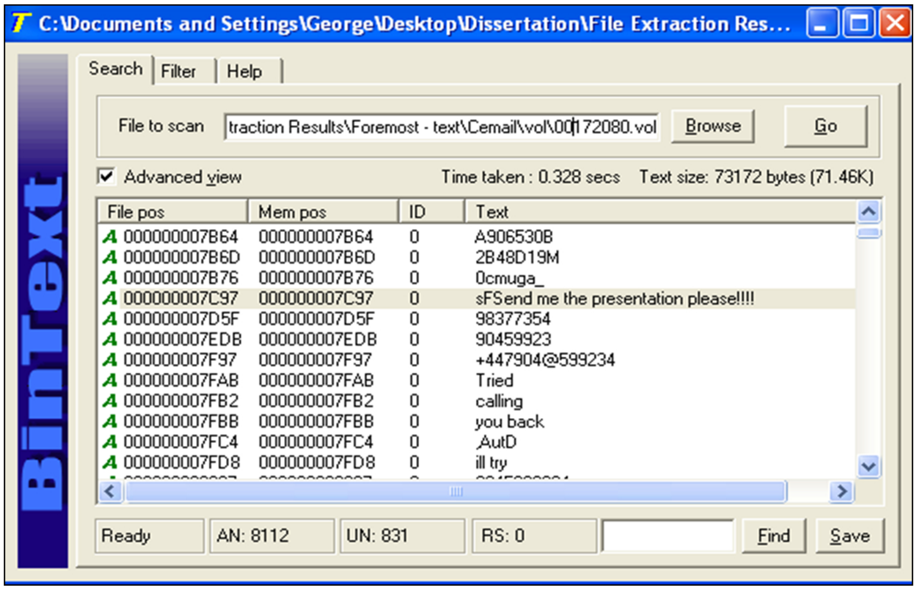
Item	**Type**	**Scalpel (configured)**	**Foremost (default)**	**Foremost (configured)**	**Simple File Carver**	**Phone Image Carver**	**WinHex (modifed image)**	**Physical Analyzer and cedbexplorer.py**
19-23	Appointments	P	N	P	P	N	P	N
24-28	Contacts	P	N	P	P	N	P	N
33-35	SMS Sent	P	N	P	P	N	P	F
36-38	SMS Received	P	N	P	P	N	P	F
69-70	Deleted Appointments	P	N	P	P	N	P	N
71-72	Deleted Contacts	P	N	P	P	N	P	N
75-77	Deleted SMS	N	N	N	N	N	N	F

The analysis revealed that the contents of the file carver recovered volumes differed from those recovered by Physical Analyzer assisted by file system information, as discussed earlier. The three file carvers (Scalpel, Foremost and Simple File Carver) appear to 'skip' several sectors of the two volumes and then resume carving. The reason for this phenomenon is unknown but as a result, these two carved volume files contain less information than the two volume files recovered using Physical Analyzer. Repeating the process using WinHex instead of Scalpel and Foremost recovered the same information as for Physical Analyzer (since WinHex also uses information about the file system to assist in recovery).

SMS messages (Figure 9), contacts, (Figure 10) calendar artifacts, Internet Explorer web history, favourite websites and emails were also successfully recovered using the file carving and string extracting method. This analysis confirms recent work by Casey et al., who also investigated the potential to recover deleted information from the `cemail.vol` and `pim.vol` files (Casey et al., 2010).

4.7. Recovering Artifacts from cedbexplorer.py

The python script, `cedbexplorer.py` was used to recover SMS messages from the files extracted by Physical Analyzer. After using the script, an



C:\Documents and Settings\George\Desktop\Dissertation\File Extraction Res...
BinText
Search
Filter
Help
Browse
Go
Find
Save

File to scan: traction Results\Foremost - text\Cemail\vol\00172080.vol

☑ Advanced view   Time taken : 0.328 secs   Text size: 73172 bytes (71.46K)

File pos	Mem pos	ID	Text
A 000000007B64	000000007B64	0	A906530B
A 000000007B6D	000000007B6D	0	2B48D19M
A 000000007B76	000000007B76	0	0cmuga_
A 000000007C97	000000007C97	0	sFSend me the presentation please!!!!
A 000000007D5F	000000007D5F	0	98377354
A 000000007EDB	000000007EDB	0	90459923
A 000000007F97	000000007F97	0	+447904@599234
A 000000007FAB	000000007FAB	0	Tried
A 000000007FB2	000000007FB2	0	calling
A 000000007FBB	000000007FBB	0	you back
A 000000007FC4	000000007FC4	0	,AutD
A 000000007FD8	000000007FD8	0	ill try

Ready | AN: 8112 | UN: 831 | RS: 0

Figure 9: SMS Message Recovered using BinText

examination of the files recovered showed that items 33–38 (SMS messages sent and received using the device) and 75–77 (messages deleted prior to the acquisition) were fully recovered in a log file output of the script. Due to the nature and purpose of this tool, it was not possible to recover any further files from the data sets in Tables 1, 2 or 3.

```
00000005CE25 00000005CE25 0 | MariX
00000005CE2D 00000005CE2D 0 | , Tina
00000005CE9C 00000005CE9C 0 | therwell
00000005CEA5 00000005CEA5 0 | 65 Tyson Roadh
00000005CEB4 00000005CEB4 0 | 0-253-000
00000005CEC3 00000005CEC3 0 | MariX
00000005CF31 00000005CF31 0 | Tina@
00000005CF3A 00000005CF3A 0 | Motherwell
```

Figure 10: Contact Information Recovered using Strings

5. Conclusions

This work has demonstrated that a diverse range of files and information artifacts are recovered from a Windows Mobile smart phone device, depending on the methods and tools employed. For example, the logical acquisition of contacts using the CUFED does not retrieve deleted contacts. However, these can be recovered using string extractor tools on the `pim.vol` file recovered from the binary image using Physical Analyzer. In addition, different recovery tools produce result sets of varying fidelity to the original test set.

The work has demonstrated that it is possible to recover files and artifacts from memory images of Windows Mobile devices using a combination of file carvers and string extraction software. The method can be used to both extend and complement the information recovered using industry standard forensic toolkits. Additional information is recovered, including Internet Explorer history, favourite websites and Email messages, as well as the contents of artifacts such as calendar appointments and contacts. It was also shown that it is possible to recover deleted versions of some of these artifact types.

The limitations of using file carvers for information recovery were also empirically demonstrated. The lack of file system information means that file carvers are dependent on the presence of file content signatures (at both the header and footer) and the contiguity of the file contents in the image. These requirements were not satisfied by the binary image recovered from the test device, causing files and artifacts to only be partially recovered.

The use of diverse methods of information recovery also presents challenges, since the multiple and quite diverse results set produced give rise to questions as to the fidelity of each of the tools used. The work demonstrates that while a diverse approach to information recovery leads to a more complete results set, cross comparisons of artifacts in multiple results (e.g. for merging an evidence base) presents challenges. Apparently similar artifacts in different results set have been demonstrated to be quite different when analysed using a fuzzy hashing technique. A practising forensics examiner, or a court might quite reasonably ask “which result set is correct?”.

The work identified several differences between the documented capabilities of the CUFED and its actual performance. The logical acquisition process was unable to recover the number fields of SMS messages, while for the physical acquisition, the contents of emails were not recovered. The challenge of maintaining accurate documentation and defect free, reliable software is well established in the software engineering community for multiple application domains (Robinson, 1996; Lock et al., 2008; Hunt and Thomas, 2002; Emam and Koru, 2008), however, it is often difficult to independently establish the reliability of proprietary forensic software.

Finally, the work has demonstrated the fragility of existing mobile forensic toolkits when recovering data from partially corrupted file system images. Physical Analyzer was unable to process and decode a corrupted file system, which meant that the file contents and artifacts were not recovered from the binary image. Two of the forensic toolkits (FTK and Encase) were unable to process the binary image at all, even when alterations were made to the file system boot sector. WinHex was able to process the binary image only when the file system type label was altered.

A practical consequence of the conclusions drawn above is the importance of digital forensic investigators utilising a diverse range of tools for the analysis of information held on mobile devices. Results from different tools must be compared for differences, and the causes of those differences investigated so that they can be explained as part of the evidence presentation process. Further work is also needed on tools for assisting forensics investigators with performing comparisons of results from different toolsets and methods.

The work presented in this paper is based on an analysis of a single Windows Mobile device running the Windows Mobile 6 operating system. Further investigation is required to establish the validity of the results across a range of Windows Mobile devices. Since this work was conducted and submitted for review, version 7 of the Windows Mobile operating system has been released. New research is now required to investigate the effectiveness of mobile forensics tools on this new platform. The design of the test set presented here provides a basis for future comparisons and evaluation.

Further work is also required in the area of file carvers designed for forensic work on mobile phones, and for the Windows Mobile platform specifically. The development of a dedicated carver to support recovery of artifacts from mobile devices without relying on information contained in the device file system. This would also provide a means of verifying the results recovered from mobile devices using standard forensics toolkits assisted by file system information. In addition, methods of establishing the integrity (e.g. computing hashes direct from the source image in a forensically sound manner) of on device information artifacts is necessary to support testing of mobile forensic acquisition toolkits.

Acknowledgments

The authors would like to thank Coert Klaver (Netherlands Forensic Institute) for supplying his Python scripts for inclusion in the comparison and for providing feedback on an earlier draft of this paper. The authors would also like to thank Mike Dickson (Scottish Crime and Drug Enforcement Agency) for advice provided during the conduct of the work. Any remaining errors are, of course, the responsibility of the authors.

ACPO, . Good practice guide for computer-based electronic evidence. Association of Chief Police Officers, 7Safe; 2007.

Allen, T.. GSM Mobile Device and Associated Media Tool Test Assertions and Test Plan. National Institute for Science and Technology; 1st ed.; 2008. .

Breeuwsma, M., de Jongh, M., Coert Klaver, R.v.d.K., Roeloffs, M.. Forensic data recovery from flash memory. Small Scale Digital Device Forensics Journal 2007;1(1). Available from: `http://www.ssddfj.org/papers/ssddfj_v1_1_breeuwsma_et_al.pdf`.

Casey, E., Bann, M., Doyle, J.. Introduction to windows mobile forensics. Digital Investigation 2010;6(–):136–146.

Cellebrite, 2010a. UFED Logical Support list. Cellebrite; v1138 ed.; 2010. Available from: `http://www.mydocbox.com/cellebrite2/newsletter/05-13-2010/Standard/UFED_Logical_v1138_Phone_support_list.xls`.

Cellebrite, 2010b. UFED Physical Pro Supported Phones list. Cellebrite; v1138 ed.; 2010. Available from: `http://www.mydocbox.com/cellebrite2/newsletter/05-13-2010/Pro/UFED_Physical_Pro_v1138_Phones_supported.xls`.

Dellutri, F., Ottaviani, V., Me, G.. MIAT-WM5: Forensic acquisition for windows mobile pocketpc. In: Smari, W.W., editor. Proceedings of the Workshop on Security and High Performance Computing Systems, part of the 2008 International Conference on High Performance Computing and Simulation: HPCS. Nicosia, Cyprus; 2008. .

Emam, K.E., Koru, A.G.. A replicated survey of it software project failures. IEEE Software 2008;25(5):84–90.

Fresco, A.. Abandoned mobile phones may have led police to arrests on m6. The Times, London, UK; 2010. Available From: `http://www.timesonline.co.uk/tol/news/uk/crime/article2017532.ece`. Last Accessed: 23/6/2010.

Gartner, 2010. Gartner says worldwide mobile device sales grew 13.8 percent in second quarter of 2010, but competition drove prices down. Online Press Release; 2010. Available from: `http://www.gartner.com/it/page.jsp?id=1421013`.

Hengeveld, J.W.. Xda project - rapi tools. Online. Available From: `http://www.xs4all.nl/~itsme/projects/xda/tools.html`. Last Accessed: 17/6/2010.

Hunt, A., Thomas, D.. Software archaeology. IEEE Software 2002;19(2):22–24.

Jahankhani, H.. Criminal investigation and forensic tools for smartphones. International Journal of Electronic Security and Digital Forensics 2009;2(4):387–406.

Jansen, W., Ayers, R.. Guidelines on Cell Phone Forensics. Special Publication 800-101; National Institute of Standards and Technology; Gaithersburg, MD 20899-8930; 2007.

Jansen, W., Delaitre, A., Moenner, L.. Overcoming impediments to cell phone forensics. In: Proceedings of the 41st Hawaii International Conference on System Sciences. Waikoloa, Big Island, HI, USA: IEEE Computer Society; 2008. p. 483–.

Kessler, G.. File signatures table. Available from: `http://www.garykessler.net/library/file_sigs.html`; 2010.

Klaver, C.. Windows mobile advanced forensics. Digital Investigation 2010;6(3-4):147–167.

Kornblum, J.. Identifying almost identical files using context triggered piecewise hashing. Digital Investigation 2006;3(Supplment 1):91–97.

Kuhn, R.. Non-GSM Mobile Device Tool Test Assertions and Test Plan. National Institute for Science and Technology; 1st ed.; 2009.

Kuhn, R.. Smart Phone Tool Test Assertions and Test Plan. National Institute for Science and Technology; 1st ed.; 2010. .

Lock, R., Storer, T., Harvey, N., Hughes, C., Sommerville, I.. Observations of the Scottish elections 2007. Transforming Government: People, Process and Policy 2008;2(2):104–118.

Mokhonoana, P., Olivier, M.. Acquisition of a Symbian smart phone's content with an on-phone forensic tool. In: Southern African Telecommunication Networks and Applications Conference 2007. Sugar Beach Resort, Mauritius; 2007. .

Moore, T.. The economics of digital forensics; 2006. To appear, Workshop on the Economics of Information Security.

National Institute for Justice, . Test results for mobile device acquisition tool: Micro Systemation .XRY 3.6. National Institute for Justice; U.S. Department of Justice, 810 Seventh Street N.W. Washington, DC 20531, USA; 2008.

National Institute for Justice, . Test results for mobile device acquisition tool: Cellebrite UFED 1.1.05. National Institute for Justice; U.S. Department of Justice, 810 Seventh Street N.W. Washington, DC 20531, USA; 2009.

Rehault, F.. Windows mobile advanced forensics: An alternative to existing tools. Digital Investigation 2010;7(1-2):38–47.

Robinson, B.. Limited horizons, limited influence: Information technology the london ambulance service. In: Proceedings of the International Symposium on Technology and Society Technical Expertise and Public Decisions. IEEE Computer Society Press; 1996. p. 506–514.

Roussev, G.G.R.V.. Scalpel: A frugal, high performance file carver. In: Digital Forensic Research Workshop. New Orleans, Louisiana, USA; 2005. .

Summers, C.. Mobile phones - the new fingerprints. BBC News Online; 2003. Available from: http://news.bbc.co.uk/1/hi/uk/3303637.stm.

Whitehead, T.. Terror concerns over mobile phones in prison. The Telegraph, London, UK; 2009. Available From: `http://www.telegraph.co.uk/news/uknews/law-and-order/6906211/Terror-concerns-over-mobile-phones-in-prison.html`. Last Accessed: 12/6/2010.

Willassen, S.. Forensic analysis of mobile phone internal memory. In: Pollitt, M., Shenoi, S., editors. Advances in Digital Forensics. IFIP International Conference on Digital Forensics. Orlando, Florida, USA: Springer; 2005. p. 191–204.

Williamson, B., Apeldoorn, P., Cheam, B., Macdonald, M.. Forensic analysis of the contents of nokia mobile phones. In: Australian Digital Forensics Conference. 2006. Paper 36.