Practical Investigations of Digital Forensics Tools for Mobile Devices
Maynard Yates II, M.S.
Florida Agricultural and Mechanical University
Department of Computer and Information Sciences
Technical Building A, Room 211
Tallahassee, FL 32307-5100
Maynard1.yates@famu.edu

ABSTRACT
With the continued growth of the mobile device market, the possibility of their use in criminal activity will only continue to increase. While the mobile device market provides a great variety of manufactures and models causing a strong diversity. It becomes difficult for a professional investigator to choose the proper forensics tools for seizing internal data from mobile devices. Through this paper, we will give a comprehensive perspective of each popular digital forensic tool and offer an inside view for investigators to choose their free sources or commercial tools. In addition, a summary for the future direction for forensics tools in mobile devices.

Categories and Subject Descriptors

General Terms
Management and Security, Legal Aspects, Verification.

Keywords
Digital forensics, handheld devices, mobile devices, forensics tools, Paraben CSI stick, cell Seizure, XRY

1. INTRODUCTION
Advancements in technology over the last 20 years have drastically altered the way we live and do business. The continued evolution and development of mobile device technology will increase the need for security protocols and forensics of these devices. Technology has permeated almost every aspect of society from the way we communicate to the way information is discovered about a particular subject.

A few examples of these changes are:
- Correspondence: Postal mail → Electronic mail (E-mail) → SMS messages (text messages)
- Telecommunications: Telephones → car powered cell phones → battery powered cell phones
- Calendar: Secretary → Day Planner → Personal Data Assistant (PDA) → “Smartphone”

As technology continues to permeate society and mobile computing becomes more prevalent, people will more heavily depend on applications such as e-mail, SMS (Short Message Service), MMS (Multimedia Messaging Service) and online transactions (i.e. bank, ins, etc); such devices provide a good source of evidence for forensic investigators to prove or disprove the commitment of crimes or location of suspects/victims [6].

Digital forensics for handheld devices is starting now. Unlike traditional computers, two important factors that must be accounted for in a forensic investigation are the state of the device at the time of acquisition and radio isolation. Traditional digital forensics with personal computers allows an investigator to perform a dead forensic data acquisition simply by disconnecting the power source to preserve the current state of the computer. That option is not available with mobile forensics for fear of loss of evidence or security mechanisms, such as device locks or passwords, being activated [15]. The fact that various operating systems are used for different mobile devices in current markets makes development of digital forensics tools for mobile devices more complicated.

This paper is being proposed to survey available digital forensics tools for capturing e-evidence from mobile devices and meet the demand of e-evidence for current and future’s crimes. This paper focuses on practical investigations for digital forensics tools that will help investigators or students obtain first-hand experiences in digital forensics for mobile devices. Investigators should be able to perform their job more informed as a result of this case study.

This paper is organized as follows: section 2 will discuss the popular operating systems for mobile devices, while section 3 will discuss tools available for forensics of mobile devices. Section 4 will discuss related work; section 5 will discuss how this case study will be carried out, followed by conclusion in section 6.
2. OPERATING SYSTEMS

Compatibility with a tool is based upon the mobile device’s operating system, but how to determine compatibility with rapidly developing technology is a challenge. There are open-source operating systems as well as proprietary, each with own unique features. This paper will examine four of the most popular mobile device operating systems.

2.1 Android

Android OS [3] relies on the Linux 2.6 kernel, which acts as an abstraction layer between the hardware and the rest of the hardware stack. The Linux kernel provides access to core services such as security, memory management, process management, network stack, and driver model. It also provides support for the Dalvik virtual machine’s functionality, such as threading and low-level memory management.

Libraries are the next layer up, and are divided into the Android Runtime library and application libraries. Written in JAVA, the Android Runtime Libraries consists of the Dalvik Virtual Machine (VM) and the core libraries that provide the available functionality for the applications. Each time an Android application is launched, it runs as a separate process and instance of the VM. Android can run multiple instances of the VM efficiently. Other components of the Android OS use C/C++ libraries such as:

- **System C library** - a BSD-derived implementation of the standard C system library (libc), tuned for embedded Linux-based devices
- **Media Libraries** - based on PacketVideo's OpenCORE; the libraries support playback and recording of many popular audio and video formats, as well as static image files, including MPEG4, H.264, MP3, AAC, AMR, JPG, and PNG
- **Surface Manager** - manages access to the display subsystem and seamlessly composites 2D and 3D graphic layers from multiple applications
- **LibWebCore** - a modern web browser engine which powers both the Android browser and an embeddable web view
- **SGL** - the underlying 2D graphics engine
- **3D libraries** - an implementation based on OpenGL ES 1.0 APIs; the libraries use either hardware 3D acceleration (where available) or the included, highly optimized 3D software rasterizer
- **FreeType** - bitmap and vector font rendering
- **SQLite** - a powerful and lightweight relational database engine available to all applications

The Applications Framework layer builds on the advantages that the Android operating system is open source and open platform. This framework was designed to simplify the reuse of components as developers are given full access to the same framework APIs used by core applications. Any application can publish its capabilities and any other application may then make use of those capabilities (subject to security constraints enforced by the framework). Listed below are the core set of services and systems that support open development:

- A rich and extensible set of Views that can be used to build an application, including lists, grids, text boxes, buttons, and even an embeddable web browser
- Content Providers that enable applications to access data from other applications (such as Contacts), or to share their own data
- A Resource Manager, providing access to non-code resources such as localized strings, graphics, and layout files
- A Notification Manager that enables all applications to display custom alerts in the status bar
- An Activity Manager that manages the lifecycle of applications and provides a common navigation backstack

The top layer, Applications, consists of email client, SMS program, calendar, maps, browser, contacts, and other JAVA applications as depicted by Figure 1.

2.2 iPhone

The iPhone operating system derives from Mac OS X desktop operating system with the 3 base layers being ported over from the OS X architecture to the iPhone OS. iPhone OS [4] is a UNIX based operating system by virtue of sharing the Darwin Foundation from OS X. The iPhone OS has four layers: the core OS, core services, media, and Cocoa Touch, a variation of OS X Cocoa layer with added multi-touch functionality for the iPhone, depicted by Figure 2. The bottom two layers, Core OS and Core Services, contain the fundamental interfaces for iPhone OS, including those used for accessing files, low-level data types, network sockets, as well as access to POSIX and UNIX sockets among others.
The next layer, Media, contains the fundamental technologies used to support 2D and 3D drawing, audio, and video such as OpenGL, Quick Time, an audio & image viewer, Core Audio and Video. The top layer, Cocoa Touch, provides the fundamental infrastructure used by iPhone OS. Figure 3 shows that the Cocoa Touch layer has been divided into an application and application framework layers.

Two major components of Cocoa Touch are the Foundation framework in the Core services layer and the UIKit in the Application Frameworks division of the Cocoa Touch layer. The Foundation framework provides support for file management, network operations, collections, and more. The UIKit framework provides the visual infrastructure for your application, including classes for windows, views, controls, and the controllers that manage those objects. However, there are other frameworks available at this level that gives you access to user’s contact and photo information and other features of hardware for an iPhone.

2.3 Blackberry

Canadian company, Research in Motion (RIM), created the Blackberry phone that was originally geared towards business professionals as a way to stay connected while traveling. The Blackberry OS [9] that powers Blackberry phones is a proprietary system, with little information about it publicly. What is known, as depicted by Figure 4, is that like the Android, the Blackberry runs through a JAVA virtual machine.

2.4 Windows Mobile

Conceptually similar to the iPhone OS, Windows Mobile [11] is a Windows OS for mobile devices. They are structured similarly, with some of the same protocols in regards to user info and activities such as registry entries, files, and web activities (web browsing, recently connected computers, Wi-Fi access points), but there are substantial differences that distinguish Windows Mobile from Windows OS. While Windows has 2 diff types of file systems, NTFS & FAT, Windows Mobile uses a variation of the FAT file system called Transaction-Safe FAT, which has some recovery features in the event of sudden shutdown.

There are currently four different family types of processor cores in Windows Mobile, ARM (most common), MIPS, and SH4 and x86. There are 2 different types of flash memory, NOR and NAND. NOR has a RAM-like interface; it has a data bus, an address bus and control lines. NOR flash is mapped in the processor’s memory map and processor code can be executed directly from it (this is called ‘execute in place’; XIP). NOR flash can also be used as storage location for user data. NAND flash can be regarded as the solid state equivalent of a hard disk. It has an interface with an I/O bus and control lines connecting the
memory chip to the processor. Over this I/O bus, commands, addresses and data are sent. As NAND flash memory is not mapped in the memory space of the processor, code stored in a NAND flash chip cannot be executed directly, but has to be loaded into RAM first, again much like a hard disk. [12]

2.5 Symbian

The Symbian system [10] architecture has three layers, but each layer contains packages, which consist of collections of components as depicted by Figure 6.

- Layers contain packages with no static upward dependencies between layers. A package may depend on other packages in the same layer or in any lower layer.
- Packages are modular collections of components, owned and maintained by a single organization (although contributed to more widely).
- Component collections are used to organize the components within a package. All components are aggregated into component collections. A collection should be formed even if there is a single collection in the package.
- Components contain the files needed to build and test at least one target file. Components implement programming interfaces.

The Middleware layer provides APIs that are typically useful for multiple programs in the application layer. A middleware layer component is independent of the hardware platform and its APIs are not used by the operating system (OS) layer. It provides access to services, such as messaging, multimedia, and web & IP services.

The OS layer abstracts the hardware platform and contains lower-level APIs that are used within the OS layer. This layer defines plug-in interfaces (HAIs) for components that implement hardware adaptations. The OS layer device driver framework includes the API that is available to kernel-mode software (which mostly consists of device drivers).

3. DIGITAL FORENSICS TOOLS

The convenience of mobile computing has become frustrating for the forensic community because it is harder to build tools that can be considered industry standard. Unlike computers, technologies for mobile devices are constantly advancing faster than any other technology. Device are advancing so quickly, that development for tools are not able to keep up because there are some drastic differences between forensics of computers and mobile devices as describe in the table below

3.1 Digital Forensics tools for Computers

Forensics for computers is easier and less complex in comparison to mobile devices. Computers have two types of memory: Random Access Memory (RAM), or secondary or volatile memory, and Read Only Memory (ROM), or primary memory. A mobile device only has one, RAM, unless a SIM card is present then the SIM card functions as ROM. The most popular operating systems for personal computers are: Windows, Mac, and UNIX, but there is a variety of manufacturers that produce mobile devices: RIM, Apple, Symbian, Palm, etc. just to name a few. Table 1 shows some of the differences [6]:

Table 1 Forensics of Computers versus Forensics of Mobile Devices

<table>
<thead>
<tr>
<th>Issues</th>
<th>Forensics of Computers</th>
<th>Forensics of Handheld Devices</th>
</tr>
</thead>
<tbody>
<tr>
<td>On/off dilemma</td>
<td>Less problematic</td>
<td>More problematic</td>
</tr>
<tr>
<td>Evidence volatility</td>
<td>Lower</td>
<td>Higher</td>
</tr>
<tr>
<td>Imaging process</td>
<td>Less tricky</td>
<td>More tricky</td>
</tr>
<tr>
<td>Size of evidence</td>
<td>Larger</td>
<td>Smaller</td>
</tr>
<tr>
<td>Technological development</td>
<td>Slower</td>
<td>Faster</td>
</tr>
<tr>
<td>Operating systems</td>
<td>Less problematic</td>
<td>More problematic</td>
</tr>
<tr>
<td>Training</td>
<td>Clear</td>
<td>Unclear</td>
</tr>
<tr>
<td>Forensic tools</td>
<td>More proprietary tools</td>
<td>More open source tools</td>
</tr>
</tbody>
</table>
3.2 FTK Mobile Phone Examiner

FTK Mobile Phone Examiner (MPE) [2] is the most commonly used forensic tool for mobile devices in the US, a distinction shared with Guidance’s EnCase Forensic suite. Mobile Phone Examiner can be used as a standalone application or as a fully integrated part of Forensic Toolkit (FTK) interface. Using MPE affords the investigator the option of a quick and easy field acquisition via cable, Infrared, or Bluetooth connection without altering data on the device, which is essential in establishing court admissible evidence. When integrated with FTK, MPE can take advantage of leading technology validated by courts and organizations such as Securities & Exchange Commission (SEC), Federal Bureau of Investigations (FBI), and the Internal Revenue Service (IRS) just to name a few. This integration would allow MPE to perform forensic analysis on multiple phones simultaneously within the same FTK interface as well as manipulate that data for easy interpretation. Reports produced by the integrated suite, which are instantly ready to be used as evidence in court, include both phone and computer analysis which allows an investigator to easily correlate data from a mobile phone to evidentiary data from a computer or another phone.

3.3 Oxygen Forensic Suite

Oxygen Forensic Suite [7] is the tool of choice for many agencies in Europe, serving law enforcement, tax and customs, government authorities in Great Britain, Germany, Australia, Sweden, and Finland among others. Oxygen prides itself on its reputation of being able to extract unique information from a smartphone such as phone basic information and SIM-card data, contacts list, caller groups, speed dials, missed/outgoing/incoming calls, standard SMS/MMS/E-mail folders, custom SMS/MMS/E-mail folders, calendar events schedule, tasks, and text notes. However the features are not truly unique as all three tools can extract this information. However Oxygen’s ability to tap into the LifeBlog and geotagging in Symbian OS in Nokia phones gives it an advantage over its competition. Unlike MPE or Device Seizure, a special agent application is used to perform forensic analysis combining the advantages of both logical and physical data acquisitions.

3.4 EnCase Neutrino

Guidance Software has become an industry leader on the strength of its product EnCase Forensic software, aside from AccessData’s Forensic ToolKit (FTK), and has over 30,000 licensed users of EnCase®. Its customer base includes more than 100 of the Fortune 500 and over half of the top 50, including: Allstate, Chevron, Ford, General Electric, Honeywell, Mattel, Northrop Grumman, Pfizer, UnitedHealth Group, Viacom and Wachovia. As a complement to their award winning, industry leading forensic solution, EnCase Neutrino [5] is designed to provide the same technology and foundation for forensic investigations for mobile devices. Amidst all the wireless signal blocking technologies, EnCase boasts a claim that the WaveShield technology used in EnCase Neutrino is the only extensively tested technology, including within close proximity of cell towers, to ensure integrity of evidence and reliability for field acquisitions. When performing data acquisition, a phone wizard is launched that identifies the device and determines the correct USB cable for a forensically sound acquisition. Unlike other tools, data acquisition and analysis starts with the device’s SIM, if present, and then continues to the device. Neutrino’s ability to obtain the device’s serial number, cell tower location, manufacturer information among other information, shows why it is considered the de facto standard for forensic solutions.

3.5 Paraben’s Device Seizure

Device Seizure has low minimum system requirements so it can run on any computer, new, old, or ancient. It can also add support and perform forensic analysis on unsupported phones if they come from supported manufacturers. Similar to MPE, but unlike Oxygen, Paraben’s device seizure [8] can search through a phone’s memory dump for crucial evidence. Device Seizure focuses on the physical level of acquisition because you can acquire more information with physical acquisition than logical.

3.6 Other Tools

There is many other free source or commercial tools that are available for use in forensic investigations such as:

- **Palm dd (pdd)** [16], which is a spin off the UNIX dd, is a windows based command-line tool that allows an investigator to complete a physical data acquisition from Palm OS handelds. PDD creates two files; one file has device specific information and the other file contains the bit by bit image. These files can then be exported to different forensic tools, such as EnCase or Autopsy. However since this is a command-line tool, graphic libraries, report generation, and search facilities are not included in these files.

- **Pilot-Link** [16] can be used to retrieve an image of the RAM of a PDA device. Pilot Link is open source software developed within the Linux community to provide a communication bridge between a Linux host and Palm OS digital devices. It uses the HotSync protocol which allows Pilot-Link to logically acquire the devices contents that can then be analyzed by EnCase, HEX editor, or Palm OS Emulator. Unfortunately, it doesn’t support hashing algorithms, making it harder to compare acquisitions for data integrity.

- **TULP2G** is short for Telefoon Uitlees Programma, 2e Generatie and used to recover evidence from handheld devices. Currently, available plug-ins are mainly targeted towards GSM phone examinations.
4. RELATED WORK

Forensic tools for handheld devices are relatively fewer than those available for personal computers, and of those available, their application is generally limited to the popular operating systems – Palm and Pocket PC [6]. Most previous publications [11, 12] are concentrated on forensics concerns either a particular operating system (i.e. Symbian, iPod, PDA) or a comprehensive analysis of most smartphone features and performance. This paper [12] introduces the forensic application of freely available tools and describes how known methods of Physical Acquisition can be applied to Windows CE devices. Casey et al [12] provided an overview of Windows Mobile Forensics, describing various methods of acquiring and examining data on Windows Mobile devices. Mislan wrote a similar paper [15] concerning Blackberry and iPhone forensics. NIST has an excellent paper on PDA Forensics Tools that discusses the different procedures and techniques when performing Mobile forensics [14].

However, there lacks an overview research paper that does a comprehensive study of forensic tools for mobile devices within more operating systems or from the perspective of a digital forensics investigator. This overview will lay out the foundation of digital forensic tools for mobile devices as we endeavor to provide an avenue for discussion regarding mobile forensics.

5. PROPOSED WORK

There are many free sources and commercial digital forensics tools for mobile devices. However, there are few comparisons and benchmarks are available to guide investigator or students to choose those tools for their practical needs. The section will address those issues.

During the experimentation of this case study, we will use SIMfill [14], a tool created by the National Institute of Standards and Technology (NIST), to automatically generate the test data for this case study which will then be placed on each mobile device via USB cable connection. After the data has been transferred to each device, each forensic tool will perform a forensic data acquisition and the data acquired documented. This process will be repeated two more times to ensure consistency and accuracy of the data being acquired and to satisfy the Federal Rules of Evidence [1]. Once the process is complete, we will compare the results based upon the following:

- Time it takes to acquire data
- The type of data acquired against the test set
- Categorically
  - By device model
  - By forensic tool
- How admissible is it as evidence

Inconsistencies with the forensic tool and with the particular carrier (Verizon, AT&T, Sprint, etc.) of the phone will be recorded and how the results were affected by the inconsistencies.

Through this exploratory experimentation, we will be able to give substantial detail to back up a claim of which investigation tool is optimal for various mobile devices. In addition, we will build a set of benchmarks for robust comparisons of all digital tools for mobile/handheld devices in different operating system environments.

6. CONCLUSIONS

With the increase in research and practical use towards mobile devices, we hope to not just follow the trend but to supply investigators/practitioners a more interactive, convenient, efficient way of capturing e-evidences via choosing reliable and suitable digital forensics tools. We make the set of benchmarks available for any researcher who wants to compare the new tools with other tools for different operating systems.

In the future we hope to include more tools and create more benchmarks that exploit the features of many different handheld devices and concur with the design variations we want. In addition, we will improve on existing benchmarks and continuously retrieve various feedback to make benchmarks more effective and easy to use. Future research will be conducted to formalize the abstract design discussed in this paper that will eventually lead to implementation and testing.

ACKNOWLEDGMENTS

This work has been supported in part by U.S. Department of Education grant P120A080094.

REFERENCES


