1-1-2012

DEVELOPING A FORENSIC METHOD OF ACQUISITION AND ANALYSIS OF THE MOTOROLA XOOM TABLET

Justin A. Tolman
jtolman@purdue.edu

DEVELOPING A FORENSIC METHOD OF ACQUISITION AND ANALYSIS OF THE MOTOROLA XOOM TABLET

A Thesis

Submitted to the Faculty

of

Purdue University

by

Justin Tolman

In Partial Fulfillment of the

Requirements for the Degree

of

Master of Science

August 2012

Purdue University

West Lafayette, Indiana

TABLE OF CONTENTS

LIST OF TABLES

LIST OF FIGURES

LIST OF TERMS

Biometrics – measurement and analysis of unique physical or behavioral characteristics as a means of verifying personal identity (Merriam-Webster, 2012).

Checksum - a value used to verify the integrity of a file or a data transfer. An example would be an MD5 hash value (TechTerms Checksum, 2012).

Digital Forensics – A process that uses science and technology to analyze digital objects and that develops and tests theories, which can be entered into a court of law, to answer questions about events that have occurred (Carrier, 2010).

Encryption – coding or scrambling of information so that it can only be decoded and read by someone who has the correct decoding key (TechTerms Encryption, 2012).

File System – A mechanism for users to store data in a hierarchy of files and directories. Consists of structural and user data that are organized such that the computer knows where to find them. (Carrier, 2010)

Forensically Sound - The use of scientifically derived and proven methods toward the preservation, collection, validation, identification, analysis, interpretation, documentation and presentation of digital evidence derived from digital sources for the purpose of facilitating or furthering the reconstruction of events found to be criminal, or helping to anticipate unauthorized actions shown to be disruptive to planned operations (DFRWS, 2001).

Image – A file with clear boundaries that contains the data extracted from another drive or piece of digital evidence. (Carrier, 2010)

Operating System – software that communicates with the hardware and allows other programs to run (TechTerms Operating System, 2012).

Logical Acquisition – An exact bit for bit copy of the logical objects on the media, such as directories and files.

Physical Acquisition – A bit for bit copy of the physical disk media.

Torrent – a file sent via the BitTorrent protocol. It can be just about any type of file, such as a movie, song, game, or application (TechTerms Torrent, 2012).

Write-Blocker – A device that sits in the connection between a computer and a storage device. It monitors the commands that are being issued and prevents the computer from writing data to the storage device. (Carrier, 2010)

LIST OF ACRONYMS

ADB – Android Debug Bridge

AVD – Android Virtual Device

BSSID – Basic Service Set Identification

DHCP – Dynamic Host Configuration Protocol

FTK – Forensic Toolkit

JDK – Java Development Kit

PRIO – Priority

SDK – Software Development Kit

SSID – Service Set Identifier

ABSTRACT

Tolman, Justin A. M.S., Purdue University, August 2012. Developing a Forensic Method of Acquisition and Analysis of the Motorola Xoom Tablet. Major Professor: Marcus Rogers.

There is currently no forensically sound method for analyzing the Motorola Xoom tablet. The purpose of this research is to determine whether a forensically sound method can be developed for the Motorola Xoom tablet running the Ice Cream Sandwich Android operating system. This research is important for investigators as the more forensically sound method offers greater protection relating to an individual’s privacy rights.   Furthermore, tablets are a relatively new form of digital devices that are rising quickly in the public. This research sets the groundwork for investigating tablets in a forensically sound manner. The tablet is used in such a way as to emulate the real use of such a device. Sources of evidence such as images, web browsing, WiFi information and email accounts are used as test objects. The research minimizes manual user interaction, delivers an outline of what can be acquired and the forensic integrity of such items upon recovery, and the reason for any changes to the device. Furthermore, this research presents questions for further research relating to the topic.

CHAPTER 1 INTRODUCTION

As digital devices become more prevalent in society old crimes are being committed in new ways using computers, laptops, cell phones, tablets, and any other type of device capable of digital information storage or processing (Clifford, 2006). In recent years there have been significant increases in digital crimes being committed (HITCIA, 2011). It is important that law enforcement’s digital investigators have available the information they need to combat these new methods of committing crime.

One device playing a part in these new methods is Tablets. Tablets are rising in popularity and forecasted to represent twenty-three percent of all computing devices (excluding phones) by the year 2015 (Epps, 2010). With increased tablet market share, investigators may see a rise in the crimes being committed with tablet devices.

Tablets and other mobile devices pose a new problem for digital investigators as there are many different models and mobile devices update both software and hardware very quickly. Mobile devices are designed to be connected to a live network while on, this increases the risk of remote wiping of evidence as well as creating issues with evidence retrieval.

One of the most common crimes investigated by digital investigators is viewing, distribution and production of child pornography (BJS, 2007). One common way for people to obtain child pornography is via the internet, and specifically with torrent programs. Torrent programs allow users to download files from other users across the internet peer to peer. With the increase in high speed data cellular networks these programs are present in mobile device market places. This allows users to download illegal material, such as child pornography, directly to a mobile device.

With the possibility of mobile devices being the primary device for obtaining and storing illegal content, investigators must take steps to examine these devices in a forensically sound manner. Investigators may not be able to rely on traditional computers for evidence.

Unfortunately, the investigator may not have the tools or the information necessary to recover evidence in a forensically sound method from a mobile device. The technical and legal methods and procedures on traditional computer forensics have changed little in the last few years. The differences in methods for creating physical images of evidence across different operating systems and manufactures are minimal. In contrast, methods for obtaining evidence from mobile devices may differ significantly from device to device. The technical issues and legal problems that come with mobile devices are always changing and it can prove difficult for investigators to maintain the proper tools and training to keep pace with the change.

This chapter gives the basic outline of the research that will attempt to address that problem. It states the problem being researched, the research question, the scope and the significance of the research. Also included are the definitions, assumptions, limitations and delimitations with this research.

1.1 Problem Statement

There is currently no forensically sound method for analyzing the Motorola Xoom tablet. This can cause issues relating to individual's Fourth, Fifth, and Fourteenth Amendment rights.

1.2 Research Question

Can a forensically sound method be developed for acquisition and analysis of the data contained within the Motorola Xoom Tablet running the Ice Cream Sandwich Android operating system?

For the purposes of this research, a forensically sound method will be a method that obtains the evidence with minimal changes by the investigator to the device. It will also be a method that when repeated on separate devices achieve the same result.

1.3 Scope

The research develops a forensically sound method of acquiring and analyzing the data contained within the Motorola Xoom Tablet. The tablet is running the Android operating system Ice Cream Sandwich version 4.0.4. Version 4.0.4 is the latest version of Ice Cream Sandwich. The method is using tools and software commonly or freely available to law enforcement officers. The method adds as little cost (both in time and in money) to the officer as significant increases in either area may result in the method being ignored.

1.4 Significance

The significance of this research is that it provides investigators with a method of acquiring and analyzing data from Android tablets in a forensically sound manner. On the spectrum of forensics, you have “traditional” computers on one end, where the methods and the reliability are very strong. On the other end of the spectrum, you have cell phones where there are rapid changes in hardware and software. These changes, combined with the constant connection to a network, cause forensically sound methods to lag behind current technology.

The operating system landscape in the PC world is primarily Windows. Ninety-two percent of the market runs Windows (Netmarketshare Desktop, 2012). This distribution means an investigator can know only Windows and successfully investigate the vast majority of their caseload.

The mobile device operating system landscape among smart phones is much more diverse. IOS controls sixty percent, Android nineteen percent, and Java ME fifteen percent of all mobile devices accessing the internet (Netmarketshare, 2012). This diversity of smart phones, combined with the amount of non-smart phones, means the investigator needs a wide range of training when dealing with mobile devices.

Tablets fall in the middle of this spectrum. They store data much like a laptop or personal computer yet function like a cell phone. Currently, many investigators approach tablets the same way as they approach cell phones not supported by forensic examination devices. The officers simply thumb through the tablet looking for evidence. This method means that the investigator may alter the evidence, and may miss potential evidence such as deleted or hidden files. They may also miss evidence simply due to lack of familiarity with the device file structure.

As more and more people begin to use tablets in their everyday lives tablets will also be used more in the commission of crimes. My research aids in the investigation process by developing a set of steps and procedures that an investigator could follow to search an Android tablet for evidence in a forensically sound manner.

1.5 Assumptions

The following assumptions are being made:

- The Motorola Xoom is a fair representation of an Android Tablet.
- The Ice Cream Sandwich Operating System is a fair representation of the Android Operating System.
- The results and methods obtained may be applied to other Ice Cream Sandwich devices.
- A physical acquisition of the Xoom is possible.

1.6 Limitations

The following limitations are being made:

- This research is limited to finding a forensically sound method of acquisition and analysis of the data.
- Specific app research is limited to apps listed in the methodology section.
- For data recovery the research is limited to recovering deleted files

- The primary focus of this research is developing a method for the uses of law enforcement.

1.7 Delimitations

The following delimitations are being made:

- Other Android operating systems are not be evaluated in this research.
- User modified Android operating systems are not being evaluated in this research.
- Advanced forms (e.g. more than deletion or renaming) of data obfuscation are not addressed.
- The specific needs of military or business forensics are not addressed.

1.8 Chapter Summary

This chapter introduced research boundaries and definitions that will govern this study. The scope of the study and the significance of this study to the law enforcement community were also covered in this chapter. It also outlined important topics such as the assumptions, limitations and delimitations of the research.

CHAPTER 2 LITERATURE REVIEW

This chapter looks at the history of digital forensics as well as the legal and technical environment in which the research was conducted. The literature review will give the significance of this thesis research background and stability.

2.1 Computer Forensics – Technical Background

Forensic investigations historically have a basic four-step process when dealing with evidence. The evidence must first be collected or seized to maintain its integrity as evidence. Investigators examine the evidence using the required tools or methods. The results of the examination are then analyzed and the conclusions are then reported (NIST, 2006). This process combined with chain of custody procedures will help persuade the court that the integrity of the evidence has been maintained (Kruse, 2005). This process occurs for all items of evidence in any investigation whether the evidence is fingerprints or digital data on a hard drive.

Computers store data on non-volatile storage media called hard disk drives. Data on a hard disk drive is stored by placing positive or negative charges that represent ones and zeros to a set of spinning plates or platters. The computer's software interprets these ones and zeros into information the individual can use. Data typically remains on the drive, even if the user deletes the data. When new data overwrites the old, the old data is gone (Carrier, 2005).

The collection process for digital evidence found on a computer's hard drive may include two basic parts. First the physical drive may be collected to preserve the original evidence, and second the data (the actual evidence) contained on the drive must be collected for analysis.

To collect the physical drive traditionally The United States Secret Service recommends investigators pull the power plug from the computer (United States Secret Service, 2010). This action immediately cuts power to the computer, and thus the hard drive, preventing it from writing or erasing data from the drive. The data is now preserved on the hard drive at the exact moment power was removed. This method, however, can cause issues if the drive is password protected, has encrypted volumes, or had evidence that is now lost when the volatile memory disappears.

To examine the data the suspect drive is removed from the computer and connected to a write blocker. A write blocker is a device that prevents the examination computer, or the user, from writing or changing data on the suspect drive (Carrier, 2010). Using specialized software, the investigator then creates an image file that is an exact copy of the drive. The investigator can verify that the drive image is an exact copy by comparing the MD5 hash values (NIST, 2006). If the hash value of the suspect drive and the new image match, then the process was successful. This duplicate image allows the investigator to analyze the data without risking damage or modification to the original data.

Hard drives are non-volatile media, which means they maintain the data contained on them even after power is lost to the drive. Computers also use memory to store live or volatile data. This data is what is currently in use by the system and requires that power be present. The data does not remain when the device loses power (Harris, 2010).

Due to the unchanging nature of the hard drive architecture, collection and examination methods of a computer system have changed very little. This reliability is in direct contrast to the mobile area of forensics. A legal background of digital forensics must be established before the issues facing mobile forensics can properly be discussed.

2.2 Computer Forensics – Legal Background

Computer technology entered very quickly into the population and with that technology the ability to commit crimes in new ways emerged. Furthermore, as people begin to use digital devices to manage more of their lives, vast amounts of information about that individual may be stored on their computer. Thus the data contained within the computer can be a valuable source of evidence. However, the digital nature of the evidence and the amount of information contained has raised legal concerns on how the Fourth and Fourteenth Amendments to the United States Constitution govern digital investigations (Kerr, 2005).

The Fourth Amendment to the Constitution sets up the basic rules for how an investigation can happen and states,

> The right of the people to be secure in their persons, houses, papers, and effects, against unreasonable searches and seizures, shall not be violated and no

> Warrants shall issue, but upon probable cause, supported by oath or affirmation, and particularly describing the place to be searched and the persons or things to be seized. (U.S. Const. amend. IV)

The Fourteenth Amendment to the Constitution contains what is called the due process clause, which states,

> No State shall make or enforce any law which shall abridge the privileges or immunities of citizens of the United States; nor shall any State deprive any person of life, liberty, or property, without due process of law. (U.S. Const. amend. XIV)

While investigating a “traditional” crime one can easily specify where to look and what to seize. It is also fairly simple to define limitations on where the investigators can search. This specific language of what to search for and where exactly to search for it prevents law enforcement from using broad language warrants that may violate a person’s privacy (*Marron v. United States*). When dealing with digital evidence however, writing a specific warrant to limit the scope of a search can prove difficult (Kerr, 2006).

When searching for digital evidence the warrant should narrow the scope by defining the type of evidence, relating to a specific criminal activity sought. The file type to be searched may also be specified depending on the nature of the suspected criminal activity (*United States v Carey,* 1999). However, the location cannot be any more specific than the hardware investigators are allowed to search, such as a hard drive, a USB drive or CD. The actual physical location of evidence on digital media is not known till after examination and analysis. This lack of knowledge requires the investigator to search the entire drive (*United States v. Mann*, 2010).

There are exceptions to the Fourth Amendment search and seizure rules and one such exception is the plain view exception. The plain view exception has three criteria that must be satisfied to be held as valid. First, the item must be in plain view. Second, the incriminating nature of the item must be immediately apparent. Thirdly, the officer also must be in the location legally. This would include public locations, warrants or consent (*Horton v. California*, 1990).

The plain view exception is a debated legal principle in the digital world and requires the investigator to tread carefully when finding incriminating evidence that may be outside the scope of the warrant. *United States v. Carey* is an example of the plain view exception improperly applied.

Carey was being investigated for possession and transportation of cocaine. The officers seized Carey's computer to search for evidence of drug trafficking. During the course of the examination the investigator discovered an image of child pornography. The court found that the investigator then abandoned the original search and began searching for child pornography. The child pornography evidence was suppressed (*United States v. Carey,* 1999).

United States v. Wong illustrates the proper execution of the plain view exception in a digital case. Wong was being investigated on charges of murder. His computer was seized to be searched for evidence of murder. During the course of the digital investigation, the investigator came across an image of child pornography. He made note of the image and continued on with his search for evidence relating to the murder case. The investigator then used the images found in plain view as probable cause to obtain new warrants to search for child pornography. The motion to suppress was denied (*United States v. Wong,* 2002).

This exception is important to consider when investigating digital crimes as the investigator will need to open and view many (if not all, through the use of forensic software) files thought to contain data of evidentiary value. The potential for accidental discovery or the violation of a suspects privacy rights is high (Chang, 2007). Until the courts come to a decision that can be applied to every case, the investigator must exercise caution.

This discussion has described the technical and legal methods used to seize and search evidence found in a digital environment, as well as protect the suspect's privacy and due process rights as outlined in the United States Constitution. The issues specifically facing digital mobile device forensics and how they differ from traditional computer forensics must also be addressed.

2.3 Mobile Phone Forensics – Technical Background

The National Institute of Standards and Technology defines mobile phone forensics as, "the science of recovering digital evidence from a mobile phone under forensically sound conditions using accepted methods" (NIST, 2007, p ES-1). This is not an easy criterion to accomplish as release cycles for cell phone models are short, and the amount of variations and varieties of operating systems and hardware are many (NIST, 2007).

The variation in hardware and software combined with connection to a live network pose new problems. One problem is power failure, which can cause security protocols to reactivate. Another problem is remote wiping of key data (Marwan, 2006). These problems mean investigators face issues in both training and time limitations when attempting to examine a mobile phone or device on a live network.

Mobile phone devices use solid-state flash memory because it takes less power to operate, is smaller than a hard disk drive of equal storage capacity, and is not susceptible to shake damage (Regan, 2009). Solid-state drives do not use platters and have no moving parts. While the same basic process and methods for analyzing a hard disk drive apply to a solid state drive, there are some differences that can both aide and hinder and investigator.

Solid-state drives do not write magnetic charges to a disk. Instead, they store a charge, one electron, in a series of gates that represent ones and zeros. Because of this gate system there is a limited amount of writing available to the drive and so the drive employs the Flash Transition Layer, which manages where data is written to and balances the use of gates (Regan, 2009). This functionality is good for the investigator in that data can stick around much longer as the drive may resist writing back to the location of deleted content in an effort to preserve the life of the gate. Furthermore, when someone powers down the device it is possible that the live contents of the volatile memory are written to the non-volatile memory for storage (Harris, 2010). However, Solid-state can prove troubling for the investigator because if the data is properly deleted it is unrecoverable.

Currently, there is very little support of physical acquisition of mobile devices. When dealing with traditional PCs, investigators have easy access to the drives themselves and, when attached to a write blocker, the data can be retrieved easily and safely stored as a physical image. Mobile devices are typically sealed devices and require the device to be turned on for the tools to extract the data. Turning the mobile device on may make changes to the device, and it also connects the device to the live network introducing the problems previously stated. Physical acquisitions are much more difficult on mobile devices as they require specialized hardware or software and more training (Curran, 2010).

Logical acquisitions of mobile devices are much more common than physical acquisitions. Logical acquisitions recover the files and directories of a drive; information such as call records, text messages and contact lists, this type of acquisition cannot recover deleted files (Curran, 2010).

Many mobile phones come with security software such as passwords, biometrics, or pattern locks so the individual can protect the data within the phone. This can cause issues for investigators if these measures are allowed to activate. One such way these security measures can be activated is due to power depletion (NIST, 2007).

There are no standards in the United States for what type of adapter a mobile device must use to charge or transfer data. As an example, the Cellebrite UFED kit currently comes equipped with over 75 different cords to connect to various types of phones and mobile devices (Cellebrite, 2012). Depending on agency’s funding, access to a device such as the Cellebrite UFED may or may not be possible. Without such a device, simply finding a cord compatible to extract the data in a forensically sound method may prove difficult.

Due to the nature of investigations on a mobile phone, an exact forensically sound reproduction may not be possible. This issue requires investigators to take special care in documenting all the steps taken during the search of the device (Curran, 2010).

2.4 Mobile Phone Forensics – Legal Background

Issues facing investigators with mobile phones are not just technical, but also legal. The courts are still struggling to wrap "physical world" court precedents to the virtual environments and devices (Mayakis, 2010). This comparison does not always successfully hold up. The Fourth Amendment applied to physical world situations, but definitions of "search", "seizure", "container" and "plain view" when applied to virtual or digital systems is not easily transferred (Kerr, 2005).

As mobile technology becomes more powerful and more versatile, people are able to store more aspects of their lives on one device. The mobile phone is not just a phone it is also an office, a source of entertainment, a camera, a journal, a GPS and much more. Without a forensically sound method of analyzing mobile devices, privacy violations can easily occur (Orso, 2009).

Law enforcement has started to seize phones not just for digital crimes but for just about every crime committed due to the wealth of information contained in them (New York Times, 2006). The search incident to arrest exception is where many concerns with privacy and mobile technology come together.

The search incident to arrest allows an officer to search a person incident to arrest for illegal items and containers on his person or immediate control to prevent concealment or destruction allowing evidence to be preserved for trial (US v. Finley, 2007), and to search for weapons that may cause the officer harm or enable escape (Chimel v. California). In *US v. Finley*, the court defined a mobile phone as a container. Mobile phones connect to a live network and as such can be remotely accessed and even remotely wiped. Due to the threat of evidence destruction, the search incident to arrest seems to apply.

Opponents of this exception's application to mobile phones define two different types of information contained within a mobile device. Coding information is information used for identifying individuals engaged in the communication, such as phone numbers. Content-based information is the actual content of the call, message or email (Orso, 2009).

This distinction between data types is important as each type of information has a different level of protection under the Fourth Amendment (Mayakis, 2010). Coding information has very little protections under the Fourth Amendment due to the non-private nature of the information. However, mobile device content-based information may contain emails, text messages and other content about an individual that could raise privacy concerns.

The field of mobile phone forensics is still evolving. Law and procedure is lagging behind technology, which requires investigators to take special care when examining mobile devices (Chang, 2007). Investigators must resist the urge to search a mobile phone simply because a mobile phone is there and only search when there is probable cause to believe that evidence of the current crime has occurred with that device (*Thornton v. United States*, 2004).

2.5 Tablets

The tablet PC holds a place in the middle between traditional PC devices and new mobile devices. Current tablets have powerful processors and large storage drives to store various forms of media and documents much like a PC. Tablets also have the ability to operate with or without a live network via Wi-Fi or 3G cellular access.

The concept of tablet computing is not a new one. However, until recently, the technology and engineering were not to a level to create mass-market success. This situation changed drastically in 2010 with the release of the iPad (Schedeen, 2010). From launch, it only took the iPad three fiscal quarters to hit 10 million units (AAPLinvestors, 2011). Since the iPad, there have been numerous other tablets from other companies running other operating systems entering the market.

While the iPad dominates the tablet market share, tablets running the Android operating system developed by Google are starting to take hold (Netmarketshare, 2012). One aspect that separates Android tablets from the iPad is that any number of hardware manufacturers can make the tablet device. Android is also open source (Source.Android.Com, 2012), which allows companies to modify the operating system to their devices or target audience's needs. For investigators these differences mean two devices running the Android operating system may require slightly different methods of examination.

The Xoom, released in February 2011 by Motorola, launched running the Android Honeycomb 3.0 operating system. In January 2012, the device received updates for the Android Ice Cream Sandwich 4.0 operating system. The Xoom supports web access and various formats of pictures, videos and audio files (Motorola, 2012). The Google Play Store, the official app store for Android products, includes apps that allow access to popular torrent networks (Play.Google.Com, 2012). Because of these capabilities, the device has the capacity to contain high value evidence.

2.6 Chapter Summary

This chapter covered the technical and legal background of both traditional PC forensics as well as mobile phone forensics. This chapter also introduced tablets as an emerging technology in need of forensic research.

CHAPTER 3 METHODOLOGY

This research was searching for a forensically sound method of acquiring and analyzing the Motorola Xoom Android Tablet for evidence collection by law enforcement. The method for this research is divided into three main parts: setup, acquisition and analysis. Each part will be further divided into ordered steps or objectives.

3.1 Setup

The setup portion of the research required that the Motorola Xoom tablet must contain information. The following data is what was put on the device for acquisition and analysis. The “evidence” files placed on the tablet were hashed previous to placing on the tablet.

1. A factory default Motorola Xoom running Android operating system Ice Cream Sandwich version 4.0.4 will be used.
2. A primary Google account will be set up. Two emails were sent from the primary Google account via the device and two emails were received on the device. Only two emails per account were sent in the interests of time. One email contained a picture attachment. A secondary Google email account was setup and two emails were sent from the secondary account via this device,

and two emails were received on this account. Only two emails per account were sent in the interests of time. The emails were sent and received to determine what, if any, information about the emails are saved to the device.

3. Connected to, and saved, two WiFi networks in order to view how and what information the Xoom stores about WiFi networks. Three web pages were visited using the default browser on each network. Six pages were used to populate the history in such a way as to simulate regular use. A connection was made to the two WiFi networks to see how the Xoom saved multiple access points.
4. Using the camera on the device, two pictures were taken. Two images were downloaded from the internet and saved to the Xoom. The images emailed to the account were saved to the Xoom. The files and save locations were analyzed to see what if any information could be discovered. Two pictures and images is assumed to be enough to see a pattern in the placement of pictures taken with the camera compared to downloaded from the internet.
5. FrostWire 0.9.9, tTorrent Lite 0.9.6, and aDownloader 1.0.8.3 apps were installed from the Google Play Store. These programs were chosen because they were the three most downloaded torrent programs in the Google Play Store at the time of this research.

3.2 Acquisition

For the acquisition portion of the research, a physical Motorola Xoom Tablet was used. The tools used were AccessData's Forensic Tool Kit 3.4 and AccessData's Mobile Forensics Examiner Plus 4.6 software. The following steps were taken:

1. Using AccessData's Mobile Forensics Examiner Plus 4.6 software the researcher created a logical image of the built-in 32-gigabyte internal solid-state drive.
2. Mobile Forensic Examiner Plus 4.6 stores data collected to AD1 files. Without changing the data, the Xoom was imaged again, creating another AD1 file and the hashes compared of each file.
3. Mobile Forensics Examiner Plus 4.6 does not support creating a physical image of the device, attempts to find a method failed. The analysis of the Xoom was a logical acquisition.

3.3 Analysis

The analysis portion of the research mapped the data locations within the file system. The focus of this section was to obtain, forensically, the relevant information relating to the evidence placed on the device. A forensically sound method of analyzing the device is a method that can be repeated and requires little interaction from the investigator, thus minimizing the changes to the device. The analysis required AccessData's Forensic Toolkit 3.4 and Android Debug Bridge. The following steps were taken:

1. Using the AD1 image created by Mobile Forensic Examiner Plus, a diagram of the folder and file structure of the Ice Cream Sandwich operating system was made.
2. Using Android Debug Bridge the researcher dentified a key source where information about the device could be found. This included email and user profiles and network information held on the device.
3. Focus was placed on directories that typically contain images, videos, audio files, and downloads. These directories are: *\mnt\sdcard\DCIM\Camera,* *\mnt\sdcard\Download,* and *\mnt\sdcard\Pictures\Screenshot.*
4. The researcher analyzed the three installed Android Torrent applications and identified the default download and share directories, torrent directories, torrent files, and application settings that may aid an investigator. These torrent apps were chosen because at the time of research they were the three most downloaded torrents in the Google Play store.
5. The hash values of the files recovered were compared to the hash values calculated before the files were placed on the tablet.
6. The researcher describes how copies of deleted images may be obtained.

3.3 Chapter Summary

This chapter covered the basic outline of how the research was conducted and the three primary portions of the research.

CHAPTER 4: DATA AND FINDINGS

This chapter contains the findings from the research carried out and will answer the question as stated in chapter one: can a forensically sound method be developed for acquisition and analysis of the data contained within the Motorola Xoom tablet running the Ice Cream Sandwich Android operating system.

This research developed a forensically sound method of acquisition and analysis of the Xoom, but with limitations. This section also validates the soundness of the method based on three categories: validity, integrity, and reliability. This section will also describe the limitations of the method as well as the importance of the research.

4.1 Findings

The research is divided into two sections, acquisition and analysis. Acquisition on the physical level of the device was not possible. This section will describe the findings based on a logical acquisition, and describe the limiting factors in why a physical acquisition was not possible.

The items of evidence placed on the device were acquired successfully. These items included: account names for both email accounts, information about two different WiFi access points that were connected to the Xoom, three downloaded images from email (one of which was deleted), and the two downloaded images from internet via the default browser. In addition, items such as the files relevant to the three torrent apps installed, the three web pages visited, and the folder structure of the Xoom were acquired successfully.

4.1.1 Logical Acquisition Only

A forensically sound physical acquisition of the device was not possible. The Xoom does not grant the user root privileges by default. Root permissions are necessary to gain access to the physical layer of the device. The Xoom's boot loader is locked and in order to give the user root privileges (known as rooting) the boot loader needs to be unlocked. Unlocking the boot loader formats the Xoom, thus destroying the evidence.

A logical acquisition was accomplished using AccessData's Mobile Phone Examiner Plus. As it is a logical acquisition of a live system it is not possible to acquire two exact logical images from the Xoom. The hash values will constantly be changing as the clock and other services are still operating. The implications of a logical acquisition mean that the research cannot study the state of deleted files or files protected by root.

4.1.2 Device Email Accounts

The Xoom requires a primary email account, which synchronizes through the Gmail app. The user also has the option to enter more email accounts through the Email app. Using the Android Debug Bridge (adb) bugreport both email accounts were recovered.

```
------------- DUMP OF SERVICE account: Accounts: 2
Account {name=tolmanresearch.2@gmail.com, type=com.android.email}
Account {name=tolmanresearch.1@gmail.com, type=com.google}
```

The account type com.android.email is the account tied to the email app, while type com.google is the primary account for the device. These are the only two email accounts connected with this Xoom.

4.1.3 WiFi Information

The Xoom was connected with two WiFi access points, OptykUnreal and Optyk2 which were saved to the Xoom for automatic connection. Using adb bugreport some information relating to both access points were recovered.

```
ID: 0 SSID: "OptykUnreal" BSSID: null PRIO: 3  KeyMgmt: WPA_PSK
Protocols: WPA RSN  AuthAlgorithms:  PairwiseCiphers: TKIP CCMP
GroupCiphers: WEP40 WEP104 TKIP CCMP  PSK: *  eap:   phase2:
identity:   anonymous_identity:   password:   client_cert:
private_key:   ca_cert:  IP assignment: DHCP Proxy settings: NONE
LinkAddresses: [] Routes: [] DnsAddresses: []
ID: 1 SSID: "Optyk2" BSSID: null PRIO: 2  KeyMgmt: WPA_PSK
Protocols: WPA RSN  AuthAlgorithms:  PairwiseCiphers: TKIP CCMP
GroupCiphers: WEP40 WEP104 TKIP CCMP  PSK: *  eap:   phase2:
identity:   anonymous_identity:   password:   client_cert:
private_key:   ca_cert:  IP assignment: DHCP Proxy settings: NONE
LinkAddresses: [] Routes: [] DnsAddresses: []
```

The adb bugreport command does not return all fields, however the same fields were complete for both access point records. SSID, PRIO, KeyMgmt, Protocols, PairwiseCiphers, GroupCiphers, and IP assignment are returned for both records.

4.1.4 Images

The two images that were emailed to the device were recovered using Accessdata's Mobile Phone Examiner. The image's hash values were maintained through the emailing process, storage on the Xoom and then extraction.

Table 4.1 Image Hash Values

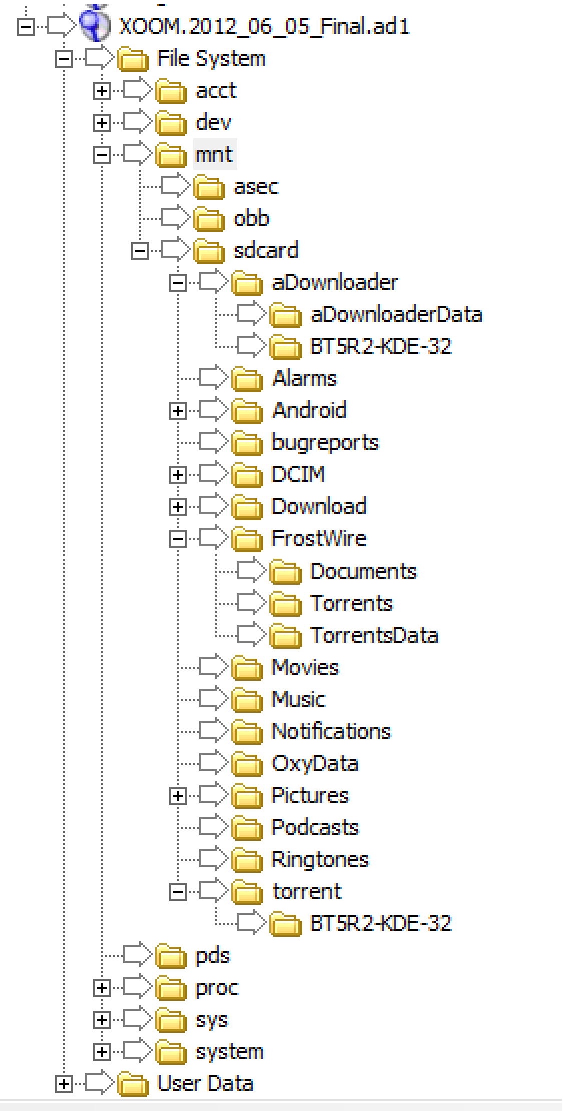
MD5 Prior To Email To Device	FileNames	MD5 On Device
23e207357fe31145b56ce625c48817ff	DeletedImage.jpg	83a744fb7d61dcc75600815c99affb0b
104c1775c8ca16e08cb0c0cdd65bea69	SecondaryTestImage2.jpg	104c1775c8ca16e08cb0c0cdd65bea69
163c970ab9d53c1acca12f41150563d9	TestImage1.jpg	163c970ab9d53c1acca12f41150563d9

Table 4.1 shows that the actual deleted image was not recovered, however the Xoom made a copy of the image which was recovered from *mnt\sdcard\Android\data\com.google.android.gallery3d*. This cache holds two thumbnails for each image on the Xoom that is viewed, one small and one medium sized. The hash values did not match, as it was not the original image. This is significant as the visual representation still exists on the device, only not as the actual hash match image. Known File Format filters will not detect contraband images in the *com.google.android.gallery3d* cache.

The images that were downloaded from web pages were saved by default to the *mnt/sdcard/Download* directory and recovered using AccessData's Mobile Phone Examiner Plus. The *mnt/sdcard/Download* directory is the same directory that files downloaded from email attachments are saved to by default.

4.1.5 Torrent Apps

The three torrent apps that were installed on the device all created their own download and share directories when installed on the device. The most significant finding when analyzing the torrents was that AccessData's Mobile Phone Examiner Plus would not export files with the .iso extension. Multiple attempts were made and failure to export was the result each time. The directory in which the file was contained was exported, but not the file itself. The cause of this failure was never found. This lack of knowledge of what file extensions Mobile Phone Examiner Plus supports is a limiting factor in how forensically sound this method is.



```
XOOM.2012_06_05_Final.ad1
    File System
        acct
        dev
        mnt
            asec
            obb
            sdcard
                aDownloader
                    aDownloaderData
                    BT5R2-KDE-32
                Alarms
                Android
                bugreports
                DCIM
                Download
                FrostWire
                    Documents
                    Torrents
                    TorrentsData
                Movies
                Music
                Notifications
                OxyData
                Pictures
                Podcasts
                Ringtones
                torrent
                    BT5R2-KDE-32
        pds
        proc
        sys
        system
    User Data
```

Figure 4.1 Torrent Directory Structure

4.1.6 Web History

Web history on the Xoom is not accessible without interacting with the device. The web history file is protected by root. The history is divided into very generic groupings: Today, Last 7 Days, Last Month, Older, Most Visited. Without root access to the actual web history file the exact time and date of each page visit is unknown.

4.1.7 Folder Structure

Figure 4.1 shows the directory structure of the Xoom as it would be before any user interaction.

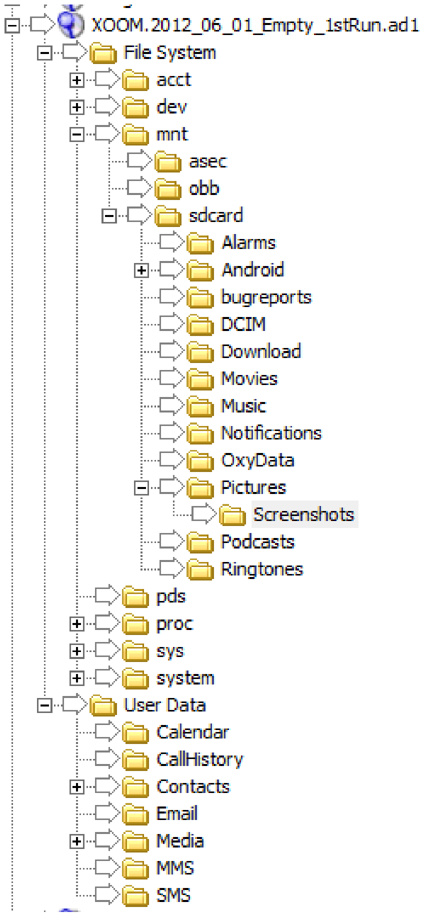


Figure 4.2 Directory Structure - No User Interaction

It is significant that the *OxyData* folder was created by Mobile Phone Examiner Plus when the information was being acquired. The directory was empty and the exact reason for its creation is unknown. This represents a change to the device by the examination software. Many of the directories contained in the *User Data* directory are only used on phones running Ice Cream Sandwich. The directory labeled *sdcard* is not an SD card but simply the label given the mountable section of the internal drive. If there is an SD card in the device it will appear labeled as *external1* as shown in Figure 4.2.

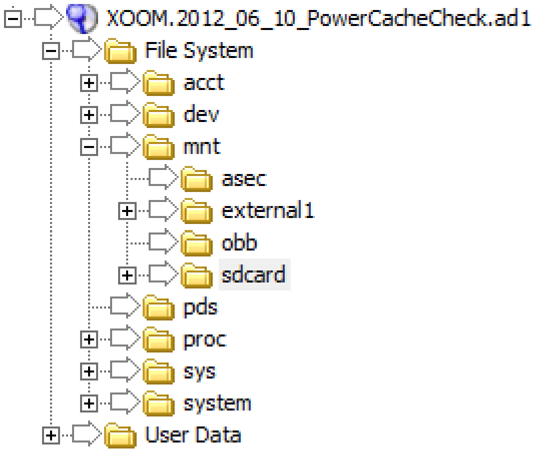


Figure 4.3 Physical SD card present

4.2 Validity

This study is externally valid as it used tools already accepted by the digital forensic community. These tools included AccessData's Mobile Phone Examiner Plus to extract much of the data, AccessData's Forensic Toolkit to analyze the AD1 image created by Mobile Phone Examiner Plus and AccessData's FTK Imager to create and compare hash values of files.

To acquire and analyze information such as the email accounts and WiFi information the Android Debug Bridge (adb) was used. By using the read only command *adb bugreport > <file>* information about the email accounts and saved WiFi connections were acquired without manual interaction with the Xoom. This study has construct validity as the information that was placed on the Xoom was successfully recovered, and when appropriate hash values were compared and found matching.

4.3 Integrity

For the method to be forensically sound the evidence must have maintained integrity. This means the evidence has not been altered to a significant degree in the execution of the method. This research showed that this method has a high degree of integrity through minimizing manual interaction with the device, matching hash values on the images and using read only commands to access key information. However, certain interactions were unavoidable due to the nature of the Xoom being a live acquisition.

This method limits the manual interaction to activating USB Debugging mode on the Xoom and the analysis of web history. The activation of USB Debugging mode is common practice with Android mobile devices. It is necessary to allow the Mobile Phone Examiner Plus and adb to communicate with the Xoom. Manual analysis of the web history is necessary as the files that contain the history are protected by root.

To maintain long term integrity of the evidence as it was when the examination begins adb can be used to create a backup file of the Xoom. This backup file will preserve the state of the device at the point the backup was made in a file that can be saved. This backup file saves such information as user settings, apps, user files (images, downloads, etc) web history, etc.

4.4 Reliability

For the method to be forensically reliable the method needs to have the attribute of repeatability that concludes with finding the same information. This method satisfies that requirement. The tests carried out in this method were done three times, each time with the same results. Three examinations were assumed to be enough to reliable. Furthermore, the use of forensic tools and the same adb commands means that the same information is being pulled from the device each acquisition.

4.5 Chapter Summary

This chapter covered the findings of the research and then addresses the validity, integrity and reliability of those findings. The chapter concluded with an explanation of why this research is important.

CHAPTER 5: CONCLUSIONS

This chapter covers the conclusions drawn from the research findings and data collected. This chapter will also address some of the questions that came from this research as well as possible opportunities for further research.

5.1 Conclusions

The research question was: can a forensically sound method be developed for acquisition and analysis of the data contained within the Motorola Xoom Tablet running the Ice Cream Sandwich Android operating system? This research has showed that a forensically sound method of acquisition and analysis is possible, but with limitations.

The research shows that a physical acquisition of an un-rooted Motorola Xoom may not possible with current forensic tools and methods. The Motorola Xoom has a locked boot loader. The action of unlocking the boot loader (which would allow giving the user root permissions) formats the device. This would destroy the information found on the device. The devices locked nature means that only a logical acquisition of the internal hard drive is possible.

The Xoom must be turned on to acquire the data contained on the device, and settings such as USB Debugger must be enabled manually. Further manual interaction is also required to obtain information such as browser history since the file containing browser history is protected by root. The research developed a method for law enforcement to acquire and analyze evidence from the Xoom with minimal manual interaction with the device. This allows for easier and more accurate documentation of how and where they found evidence. This research also shows that thumbnails of deleted images are saved on the device, which could not be found via a thumb through examination.

The method developed here minimizes risk of privacy violations. Email accounts tied to the device can be recovered directly without risk of accessing the content of emails. Investigators may then acquire the content of emails via warrant or subpoena, maintaining evidence integrity and forensic soundness.

The torrent apps create their own download and share directories. These directories combined with the various file types that a user could download from the torrent network mean that certain files may not be visible on a thumb through of the device. This research shows the directory structure of the three most downloaded torrent apps in the Google Play store, which may give investigators an idea of where to search for files of evidentiary value. Furthermore, this research showed that Mobile Phone Examiner Plus would not extract all file types from the device. Further research into this issue is encouraged, as law enforcement should be aware of possible weaknesses in Mobile Phone Examiner Plus.

5.2 Importance

This research is important as it sets the groundwork for forensic examinations of tablet devices running the Android operating system. No method had been developed for a forensic method of acquisition and analysis of tablet devices running Ice Cream

Sandwich. This research developed a forensic method for acquisition and analysis while generating questions and material for future research.

This method acquires the information necessary with minimal user interaction thus minimizing the alterations to the device. This allows for an easily documented analysis procedure that can be repeated with forensically sound results.

5.3 Further Research

The focus of this research was for the purposes of law enforcement and their specific needs. However, through the course of the research and development of the method several questions were generated that may be of worth to future researchers. The answers to these questions would also prove useful to law enforcement in the future.

In the course of this research, a *backup.ab* file was created and loaded into the Android Virtual Device (AVD) emulator. The purpose of this was to see if investigators could create a backup file of the Xoom, which would be an exact copy of the data contained on the Xoom, and then restore the device backup file to a virtual device in the emulator. The investigator could then interact manually with the virtual copy of the Xoom and not risk damage to the original and best evidence. The backup.ab file created successfully, however the file was not compatible with AVD.

Currently the AVD emulator only supports up to Android 4.0.3 and this may have caused the unsuccessful restorations. The *backup.ab* file is a type of compressed archive, however no tool could be found to extract the data from the file. Further research into either the hosting via virtual machine or extraction directly from the *backup.ab* file may yield a more forensically sound method of analysis for tablets running the Android Ice Cream Sandwich operating system.

AccessData's Mobile Phone Examiner Plus was used to export the data into an AD1 image that was then examined in FTK 3.4. It was discovered in this research that Mobile Phone Examiner Plus would not export .iso files from the device. Further research into the limitations of Mobile Phone Examiner Plus may help to improve the validity of this research as well as other forensic research and examinations using this tool.

A physical acquisition and access to lower level files of the Xoom requires root access to the device. To gain root access requires that the boot loader be unlocked, thus formatting the device. What type of format occurs during this process? Is there a way to bypass this process and still root the device, or access the files protected by root? Does this feature pose a risk to investigators by giving a user the ability to quickly format the device before seizure? These questions are some that were generated in the course of the research relating to the locked boot loader.

5.4 Chapter Summary

This chapter discussed the conclusions from the research and its implications to law enforcement and research. The section also contained suggestions for future research based on questions and issues that arose during the research.

REFERENCES

REFERENCES

Aaplinvestors. (2012). iPad versus iPhone versus iPod. http://aaplinvestors.net/stats/iphonevsipod/. Visited July 7th, 2012.

Al-Zarouni, Marwan. 2006. Mobile handset forensic evidence: a challenge for law enforcement. *Edith Cowan University.*

Bureau of Justice Statisics (BJS). 2007. Federal prosecution of child sex exploitation offenders, 2006. *Bureau of Justice Statistics Bulletin*. http://bjs.ojp.usdoj.gov/content/pub/pdf/fpcseo06.pdf

Merriam-Webster. (2012). Biometrics. http://www.merriam-webster.com/dictionary/hacker. Visited July 7th, 2012.

Cellebrite. (2012). UFED Ultimate. The premium, all in one mobile forensic solution. http://www.cellebrite.com/mobile-forensics-products/forensics-products/ufed-ultimate.html. Visited July 7th, 2012.

Chang, Rayming. (2007). Why the plain view doctrine should not apply to digital evidence. *Suffolk journal of trial and appellate Advocacy*. Vol 12. p 31-67

Carrier, Brian. (2010). File system forensic analysis. *Addison Wesley*. Upper Saddle River, New Jersey.

Clifford, Ralph. (2006). Cyber crime: the investigation, prosecution and defense of a computer related crime. *Carolina Academic Press*. Durham, North Carolina.

Curran, K., Robinson, A., Peacocke, S., Cassidy, S. (2010). Mobile phone forensic analysis*.* *International Journal of digital crime and forensics*. Vol 2. No 2.

Digital Forensic Research Workshop (DFRWS). (2001). A road map for digital forensic research. *DFRWS Technical Report*. DTR – T001-01 final.

Epps, Sarah R. Steve Ballmer is right: the PC market is getting bigger. *Forrester.com*. http://blogs.forrester.com/sarah_rotman_epps/10-06-17-steve_ballmer_right_pc_market_getting_bigger. Visited July 7th, 2012.

Harris. (2010). Discovery of Portable Electronic Devices. *Alabama law review*. Vol. 61:1:193.

High Technology Crime Investigation Association (HITCIA). (2011). 2011 report on cyber crime investigation.

Kerr, Orin S. (2005). Digital evidence and the new crminal procedure. *Columbia Law review.*

Kerr, Orin S. (2006). Searchs and seizures in a digital world. *Harvard Law Review*. Vol 119. Issue 2. p 532-585

Mayakis, Mark L.(2010). Cell Phone -- A "weapon" of mass discretion. *Campbell Law Review*. vol 33. no 1.p 151-72

Motorola. (2012). Motorola Xoom Specs. http://www.motorola.com/Consumers/US-EN/Consumer-Product-and-Services/Tablets/ci.MOTOROLA-XOOM-with-WiFi-US-EN.alt#anchor. Visited July 7th, 2012.

Netmarketshare. (2012). Mobile market share. http://marketshare.hitslink.com/. Visited July 7th, 2012.

Netmarketshare Desktop. (2012). Desktop Operating System Market Share. http://marketshare.hitslink.com/operating-system-market-share.aspx?qprid=8&qpcustomd=0. Visited July 7th, 2012.

NIST. (2007). Guidelines on cell phone forensics. *National institute of standards and technology*. NIST special publications 800-101

Orso, Matthew E. (2009). Cellular phones, warrantless searches and the new frontier of fourth amendment jurisprudence*. Santa Clara law review*. Vol 50 p 183.

Play.google.com. (2012). Torrent search result. https://play.google.com/store/search?q=torrent&c=apps. Visited July 7th, 2012.

Schedeen, Jesse. (2010). The history of the tablet pc. http://www.ign.com/articles/2010/04/01/the-history-of-the-tablet-pc. Visited July 7th, 2012.

Source.android.com. (2012). About the Android open source project. http://source.android.com/about/index.html. Visited July 7th, 2012.

Regan, James E. (2009) The forensic potential of flash memory. *Naval postgraduate school*

TechTerms Checksum. (2012). TechTerms.com. http://www.techterms.com/definition/checksum. Visited July 7th, 2012.

TechTerms Encryption. (2012). TechTerms.com. http://www.techterms.com/definition/encryption. Visited July 7th, 2012.

TechTerms Operating System. (2012). TechTerms.com. http://www.techterms.com/definition/operating_system. Visited July 7th, 2012.

TechTerms Torrent. (2012). TechTerms.com. http://www.techterms.com/definition/torrent. Visited July 7th, 2012.

United States Court of Appeals, Eighth Circuit. (1999). *United States v. Beatty*. No 98-1792

United States Court of Appeals, Tenth Circuit. (1999). United States v. Carey. No. 98-3077

United States Court of Appeals, First Circuit. (1977). United States v. Chadwick. No. 75-1721

United States Court of Appeals, Fifth Circuit. (2007). United States v. Finley. No. 06-50160

United States Court of Appeals, Seventh Circuit. (2010). United States v. Matthew Eric Mann. No. 08-3041

United States Court of Appeals, Ninth Circuit. 2002. United States v. Wong. No. 02-10070

United States Secret Service. (2011). Best practices for seizing electronic evidence. A pocket guide for first responders. v3.

United States Supreme Court. (1969). Chimel v. California. 395 U.S. 752 (1969).*Certiorari to the Supreme Court of California*. No. 770.

United States Supreme Court. (1990). Horton v California, 496 U.S 128 1990. *Certiorari to the court of appeal of California, sixth appellate district*. No. 88-7164

United States Supreme Court. (1927). Marron v. United States. 275 U.S. 192 (1927) No. 185

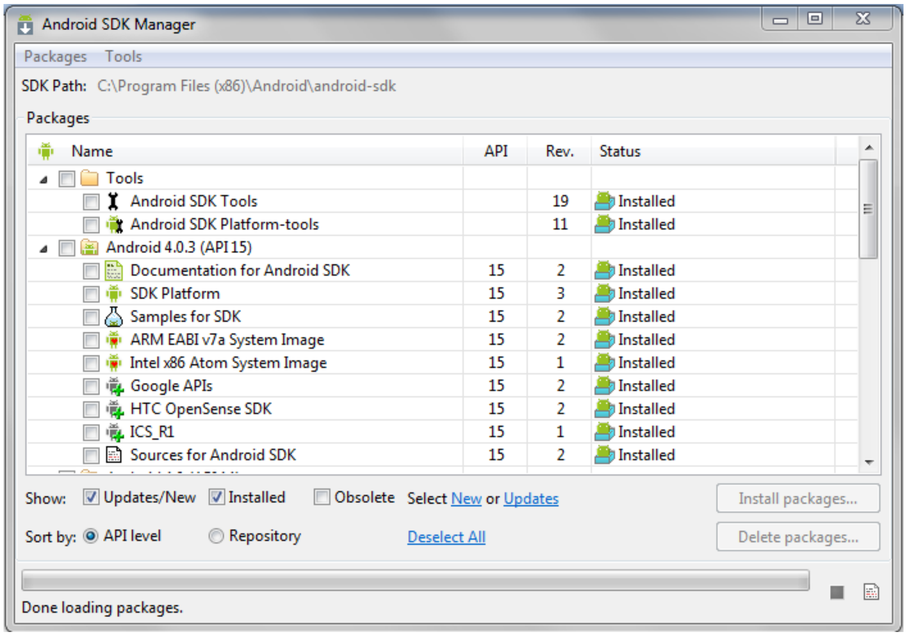
United States Supreme Court. (2004). Thornton v. United States 541 U.S. 615 (2004). *Certiorari to the United States court of appeals for the fourth circuit*. No. 03-5165

APPENDIX

APPENDIX

Investigators may be required to install the Android SDK suite on their examination machine in order to use the Android Debugger (adb). Download the installer from the following website: *http://developer.android.com/sdk/index.html*. The Java Development Kit (JDK) is also required to run Android SDK, JDK can be obtained from the following website: *http://www.oracle.com/technetwork/java/javase/downloads/index.html*.

When the installation is complete open SDK Manager (*Start>All Programs> Android> SDK Manager*). Update or Install the following items using the SDK Manager:



SDK Path: C:\Program Files (x86)\Android\android-sdk

Name	API	Rev.	Status
□ Tools			
□ Android SDK Tools		19	Installed
□ Android SDK Platform-tools		11	Installed
□ Android 4.0.3 (API 15)			
□ Documentation for Android SDK	15	2	Installed
□ SDK Platform	15	3	Installed
□ Samples for SDK	15	2	Installed
□ ARM EABI v7a System Image	15	2	Installed
□ Intel x86 Atom System Image	15	1	Installed
□ Google APIs	15	2	Installed
□ HTC OpenSense SDK	15	2	Installed
□ ICS_R1	15	1	Installed
□ Sources for Android SDK	15	2	Installed

Show: ☑ Updates/New ☑ Installed □ Obsolete Select New or Updates

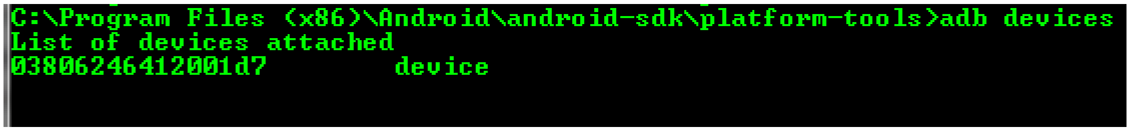
Sort by: ● API level ○ Repository Deselect All

Done loading packages.

Figure A.1 Android SDK Manager

Adb is a command line tool. Open a command prompt as Administrator and within the command prompt navigate to *C:\Program Files (x86)\Android\android-sdk\platform-tools\*. When working with adb you always work from this directory. Typing *adb* and pushing enter will display a list of commands available to you in adb.

To test the connection to the Motorola Xoom type *adb devices***.** The Xoom will be listed with a unique number identifier and labeled as a device. The investigator may see an emulator listed. If the emulator is listed the investigator may need to add the *-d* operator to commands give to point commands at the device.



```
C:\Program Files (x86)\Android\android-sdk\platform-tools>adb devices
List of devices attached
03806246412001d7        device
```

Figure A.1 ADB Devices

When the device is listed it is ready to receive commands from adb.