Annual ADFSL Conference on Digital Forensics, Security and Law

2011
Proceedings

May 27th, 10:45 AM

Ios Mobile Device Forensics: Initial Analysis

Rita M. Barrios
Assistant Professor, University of Detroit Mercy, barriorm@udmercy.edu

Michael R. Lehrfeld
Assistant Professor, East Tennessee State University, lehrfeld@etsu.edu

Scholarly Commons Citation

Barrios, Rita M. and Lehrfeld, Michael R., "Ios Mobile Device Forensics: Initial Analysis" (2011). *Annual ADFSL Conference on Digital Forensics, Security and Law*. 4.
https://commons.erau.edu/adfsl/2011/friday/4

IOS MOBILE DEVICE FORENSICS: INITIAL ANALYSIS

Rita M. Barrios
Assistant Professor
University of Detroit Mercy
Detroit, Mi, 48221
barriorm@udmercy.edu

Michael R. Lehrfeld
Assistant Professor
East Tennessee State University
Johnson City, TN, 37614
lehrfeld@etsu.edu

ABSTRACT

The ability to recover forensic artifacts from mobile devices is proving to be an ever-increasing challenge for investigators. Coupling this with the ubiquity of mobile devices and the increasing complexity and processing power they contain results in a reliance on them by suspects. In investigating Apple's iOS devices -- namely the iPhone and iPad -- an investigator's challenges are increased due to the closed nature of the platforms. What is left is an extremely powerful and complex mobile tool that is inexpensive, small, and can be used in suspect activities. Little is known about the internal data structures of the device or the proper method of extracting forensically sound images of them.

This article will discuss the current state of iOS mobile device forensics. An examination of what data is contained on the devices as well as what can currently be extracted from suspect device is looked at. Jailbreaking an iOS device will be evaluated against its pros and cons along with current professional and open source tools. Finally, a discourse on our continuing research into deleted file recovery and future works is presented.

Keywords: Digital Forensics, iOS, iPhone, iPad, Mobile Devices, Security, Analysis, Tools

1. INTRODUCTION

Mobile platforms have been on the horizon for many years. Tablet PCs and PDAs have made portable computing very tangible for many organizations. Lightweight laptops and net-books have furthered this trend of mobilization and have increased their immersion into the business world. Pagers and terse text messages have been replaced by full document editing and rich text emails. In 2007 Apple introduced the iPhone, and in 2009, the iPad. The uniqueness of these iOS devices and their rapid adoption into multiple domains has been propelled by their portability, usability, and processing power.

The potential uses for the iOS devices vary greatly, but there is no denying their broad adoption. By the end of 2011, there are expected to be more than 100 million iPhones and 43 million iPads in the marketplace (Chaffin, 2010; Elmer-DeWitt, 2010). To contrast this to laptop sales, BestBuy CEO Brian Dun commented that iPad sales could cut into laptop sales by as much as 50% (Yarow, 2010).

As can be expected, the devices are being used for legitimate and illegitimate purposes. These portable devices can be found in every industry whether officially supported by the institution or not. It can be expected that sensitive data will find its way onto these devices and it is ultimately the institution's responsibility to provide the information safeguards. One must consider the effect of such an event should that device be compromised. The primary questions to consider is what sensitive data may be resident and to what level would accessibility to this information exist. Current research indicates that providing security mechanisms for mobile iOS platforms is drastically different from securing traditional mobile devices such as the standard laptop and PDA (Schuessler & Ibragimova, 2009).

As the digitization of information is accelerated by governmental mandates the ease of access of the data is greatly increased. The ability to secure confidential information behind a locked door no longer applies. Couple this with powerful iOS devices that are often misplaced or stolen (Helft & Bilton, 2010) or used for malicious activities and suddenly there is a need for 1) ensuring data security; and 2) in the event of a breach, investigators need to have the ability to determine exactly what has occurred and the impact to the organization, if any, related to the potential data compromise.

In the healthcare domain, for example, the *Health Insurance Portability and Accountability Act* (HIPAA) of 1996 provides some very specific challenges for data security (HIPAA 2010). This law established defined standards for data preservation and security across differing platforms. In a 2009 study of computing habits of healthcare professionals, it was determined, that over 85% used mobile devices and connected to secure systems using a myriad of network technologies (Justice, Wu, & Walton, 2009). For example, doctors can now use their iOS devices to write electronic prescriptions (Scoop, 2010). The Justice et al (2009) survey also found that only 4% of healthcare institutions have a dedicated computer crime unit that has the ability to include investigation of mobile devices. This environment as identified by Justice et al (2009) indicates that with the increase of mobile device usage in the healthcare industry, there are exponentially more ways to facilitate a data compromise however there are less people to investigate these new environments. With this wide adoption of mobile devices and an increase of the usage of heterogeneous connectivity mechanisms, a proportional increase in the amount of security breaches related to the organizational security protocols can be expected. This increase will ultimately lead to an increase in compromised data as well as an increase in the need for forensic investigations in this environment.

By no means is the healthcare domain the only industry affected by legal standards in terms of data protection. The Sarbanes-Oxley Act of 2002 ("The Sarbanes-Oxley Act of 2002," 2010), the Family Educational Rights and Privacy Act ("Family Educational Rights and Privacy Act (FERPA)," 2010), or the various state statutes regarding identity theft ("Identity Theft State Statutes," 2010) all have one common theme – policies, procedures and controls must be in place to ensure data security. What is not so overt in these legislative documents is the mandate for an organization to perform a forensic evaluation of a data breach to determine the events that occurred in the event of a compromise. What often happens is the organization simply utilizes a security policy checklist to decide the degree of the breach. While this can net some important information, there will be no physical digital evidence produced to support the investigation.

Currently accepted forensic process models, like Palmer's model (Palmer, 2001) or Pollitt (Pollitt, 2007), do little to illuminate digital forensics in terms of the smartphone platform (Dancer & Dampier, 2010). The NIST SP800-101 recommended standard is outdated when considering the current iOS devices (NIST, 2007). Additionally, there is little documented in the literature concerning one of the most popular mobile platforms in the 21st century, namely the iOS environment, when forensic acquisition is considered. Of the limited literature available, researchers, developers and investigators acknowledge the difficulty in obtaining the breadth of information available utilizing the current toolsets that is comparable to its desktop brethren. In fact, little is published concerning forensics for the iOS v4 devices and slightly more in known about previous iOS versions (Hoog & Strzempka, 2010). This gap in knowledge may be causing loss of forensics artifacts or critical information that may prove beneficial to an investigator. As such, a methodology and toolset needs to be developed that will enable investigators to pursue potential compromises in the iOS environment. As noted above, employees will find ways to utilize consumer devices and applications in order to accomplish their business goals and objectives, even if the alternative devices are not approved by IT (Information Technology) corporate directives (Brewin, 2010). With this compromised environment the digital forensics examiner is left to find these areas of inconsistency and to determine the degree of compromise.

The research presented in the following sections will begin to bridge the knowledge gap identified above by examining the current state of the iOS environment. This examination will include enumerating the data contained within the device and as well as what information can be extracted from the iOS environment as identified in section II. An introductory overview of Jailbreaking is then presented in section III. The Zdziarski Method as well as several digital forensic software suites will be examined at a high-level in section IV. Section V presents a conversation of our on-going efforts into the research of the deleted file recovery process within the iOS environment. Additionally, section V presents our continuing efforts in developing a toolset that will aid in the investigation processes for the iOS mobile environment.

2. DATA CONTAINED ON MOBILE DEVICES

The vast array of forensic artifacts found on iOS devices is expansive and valuable. The range of data varies slightly by device, but many categories overlap between iPhones and iPads with and without a cellular radio. Physically, iOS devices are similar in makeup as other solid-state handheld device. The forensically interesting parts to date are the flash chips, GPS chip, and RAM. Dancer and Dampier (2010) compiled a list of issues when confronting smartphone device forensics as it relates to the various areas of interest. They include but are not limited to 1) the various types of memory used in the device; 2) the varying power states of the device; 3) remote wipe capabilities and other mechanism for altering data remotely; 4) proprietary information; and 5) differing ways the device can share information.

Table 1 contains a listing of forensically interesting physical parts of the iPhone 4 and iPad with and without a cellular radio ("iFixit," 2010). Table 2 addresses some of the interesting forensic artifacts that an investigator will need to conduct a thorough investigation (Hoog & Strzempka, 2010). While neither of these two tables is exhaustive in composition as well as which forensic tools can identify the specific information identified, the tables do indeed give depth of understanding just how complex the iOS environment can be. It should be noted that due to the limitations of the paper format, a discussion of mobile tools and their extraction capabilities will not be presented. The reader is directed to the 2010 study as presented by Hoog & Strzempka where a comprehensive evaluation of each tool is presented along with the tools associated data extraction capabilities.

	iPhone 4	iPad	iPad with radio
RAM	√	√	√
Flash	√	√	√
GPS	√	√	√
Cellular Radio	√	N/A	√
Wi-Fi	√	√	√
Bluetooth	√	√	√
CPU Type	A4 Processor	A4 Processor	A4 Processor

Table 1: iPhone and iPad physical components (“ifixit”, 2010)

Artifact	Definition
Call logs – Native Dialer	Determine what calls were attempted and received from the device
Call logs – VoIP Dialer (3rd Party)	“”
Voice Mail	Access deleted and stored messages
SMS – Native Application	Retrieve attempted and received SMS, including deleted SMS
SMS – 3rd Party	Gather information from installed 3rd party application
MMS – Native	“”
MMS – 3rd Party	“”
Email	Retrieve sent/received/deleted emails
Notes - Native Application	
Notes – 3rd Party	
Pictures – Native	Retrieve all pictures from device, including deleted
Pictures – 3rd Party	Access pictures from 3rd party application
Web Tracking Information	Access browser history, cookies, bookmarks
Web Tracking Info – 3rd Party	“”
Process Listing of Device	Plist
GPS Data	Access GPS waypoints
WiFi Connections	List of all access points
Songs	Recovery of all songs on device
Videos	Listing of videos contained on device or deleted

Table 2: Potential digital artifacts on iOS devices (Hoog & Strzempka, 2010)

As noted in Table 2, there are many different categories where forensic artifacts may reside. Moreover, acquisition techniques can be further broken down into the physical and logical. As in traditional computer forensics, a physical acquisition is usually the best method of acquiring evidence. Logical is usually a secondary tactic as is leaves some evidence unrecoverable. However, the ability to recover deleted files relies heavily on a physical acquisition methodology. As previously discussed, physical acquisitions of current iOS devices is difficult to obtain because of the closed architecture of Apple’s devices; thus complicating the recovery of deleted artifacts.

3. JAILBREAKING

Jailbreaking an iPhone or iPad enables the user to gain root access to the device. From this position, a physical image of the device may be obtained using various tools. The current issue with this methodology is the forensic validity of the evidence: will the evidence be accepted in court as part of an ongoing investigation or will the findings be compromised because of the acquisition method? The iDevice communicates with the computer using Apple’s Apple File Communication (AFC) protocol. This protocol enables iTunes to communicate with a sandbox on the iDevice; excluding raw access to the iDevice and a majority of the file system.

By Jailbreaking a device, the current limitations of iTunes can be subverted and root access achieved. With root access, typical Linux utilities can be loaded to the device where SSH and dd commands can be run to produce a full drive image extraction (Harrington, 2008).

Jailbreaking presents a difficult problem for law enforcement entities. According to the NIST Guideline for Mobile Phone Forensics;

- *No actions performed by investigators should change data contained on digital devices or storage media that may subsequently be relied upon in court.*
- *Individuals accessing original data must be competent to do so and have the ability to explain their actions.*
- *An audit trail or other record of applied processes, suitable for replication of the results by an independent third-party, must be created and preserved, accurately documenting each investigative step.*
- *The person in charge of the investigation has overall responsibility for ensuring the above-mentioned procedures are followed and in compliance with governing laws.*

Table 3 NIST principles for mobile phone forensics (NIST 2007)

Jailbreaking violates the first of these principles since jailbreaking circumvents the locked state by injecting processing components into the device which forces a change in the data/program composition. This injection may provide for technical issues during the legal phase for the investigator with the remaining three components of the NIST principles. As reported by Sean Morrisey in the July 2010 newsletter for Digital Forensics Magazine, Jailbreaking is a legal and acceptable method of access in the iOS environment for law enforcement agencies however; it is not legal for the civilian examiner (Morrisey, 2010). What this results in is forcing the civilian examiner to be bound by the logical data collection process which may result in incomplete evidence being reported to the judicial body. Clearly there is a need for a more forensically sound approach to obtaining a raw disk image of an iDevice while adhering to commonly accepted computer forensics processes, procedures and controls.

4. ACQUISITION METHODOLOGIES AND TOOLSETS IN THE IOS ENVIRONMENT

When considering the availability of forensic tools for the iOS device, the choices are rather limited. The commonly used toolsets of Forensic Tool Kit (FTK) as offered by Access Data and EnCase as offered by Guidance Software perform very well with standard hard disk forensics. However, both of these tools fall short when it applied to the iOS environment and the recovery of deleted files.

As noted, the most significant issues the forensic examiner is presented with in terms of toolset utilization are the ability to recover deleted files within the iOS environment. As Zarren & Baig (2010) note in their 2010 study as well as has been previously identified in table 2 of this study, a significant amount of evidence can be obtained during the deleted file recovery process. This evidence can include text messages and the contact list of the suspect device.

To begin the discussion, the following paragraphs will overview the acquisitions methods used in mobile device investigations followed by challenges often encountered during the acquisition processes. This section will conclude with a brief discussion of a few of the commonly used forensic tools for the iOS environment as well as their evaluation within the Hoog & Strzempka study (2010).

4.1 Acquisition Methods

Acquisition can be considered the most important task during the investigative process. When considering the mobile device environment, advances in the technology allow the potential to retrieve a vast amount of information. The method of acquisition employed depends largely upon the vendor of the device but also the model, condition, amount of time available and the nature of the investigation.

With these advancements, Owen, Thomas & McPhee (2010) remind the investigator that strict guidelines must be followed so that the evidence as well as the procedures presented can be considered forensically sound within the judicial setting. While there is a close relationship to traditional hard disk forensics, the current guidelines are not appropriate for the mobile environment (Owen, Thomas

& McPhee, 2010). In addition, Zareen & Baig (2010) also remind the investigator that there is no standard in place for the analysis of internal device memory. This lack of standardization becomes a barrier since the iOS device relies on flash memory rather than a hard disk.

In the iOS environment, full acquisition becomes difficult to achieve, as there is a need for the investigator to interact with several processing layers: The hardware layer, the OEM (Original Equipment Manufacturer) layer and the application layer (Owen, Thomas, & McPhee, 2010). The hardware layer includes the processor, RAM, ROM, antenna, and other input/output devices. The OEM layer maintains the boot loading, configuration files and the application layers. Finally, the application layer supports the end user applications, internet applications, remote wiping and media players (Owen, Thomas, & McPhee, 2010). Additionally, an investigator has the luxury of removing the hard drive from a standard computer system, causing it to become more static in nature in terms of evidential integrity. This is not possible with a mobile device which results in a more complex investigative process (Owen, Thomas, & McPhee, 2010).

The limited research into forensics for the iOS environment identifies six methods of acquisition. These are manual, logical, hex-dump analysis, chip-off, back-up analysis, and bit-by-bit.

Manual Acquisition is the process by which the investigator reviews the device's documentation and employs a manual browsing procedure that utilizes the keypad and display features of the device to acquire the needed evidence. This process will not net all of the needed data, especially the deleted data objects. Issues associated with this method include errors in judgment and data modification as well as the incredible amount of time needed to move methodically through all features of the device (Zareen & Baig, 2010).

Logical Acquisition is the process by which the investigator gains access to the user data via cable connected to the device and to the evidence receptacle. The investigator extracts the evidence using the AT command set as employed by commercially available toolsets. This method does support foreign languages and there is a considerable amount of knowledge and research in this area. The challenges encountered when using the logical acquisition method include the potential to have data written to the device which can be expected to be, at a minimum, changes to the log file, the requirement of many types of cables that are device dependent. While the recovery of live data can be achieved using this method, there is no access to the deleted data since the memory cards need to be directly accessed. Even with these concerns, this method is preferred over an attempt to acquire the data using a computer to which the device has been synced with (Hoog & Strezempka, 2010; Zareen & Baig, 2010)

Hex-dump analysis allows for the physical acquisition of mobile device files (Zareen & Baig, 2010). This procedure involves connecting the mobile device to an evidence receptacle or removing the SIM card and utilizing a reader then 'dumping' the contents to the receptacle. The evidence retrieved is in a raw format, which requires a data conversion. Access to the deleted files that have not been over-written can be achieved however the nature of the evidence obtained results in inconsistent reporting, is difficult to use, requires custom cables and the source code is often protected by the manufacturer (Zareen & Baig, 2010). Additionally, this method is a derivation of the hacker community that may be considered inappropriate in an investigation as is the utilization of the Jailbreaking methodology.

Chip-off is a method of acquisition where the investigator physically removes the chip from the device then proceeds to read the device using a secondary device such as another mobile device or an EEProm reader to perform the forensic analysis. This method is very expensive but is able to extract all of the data. In addition, the resulting acquisition can be difficult to interpret and convert (Zareen & Baig, 2010). It should be noted that since the drive is always encrypted in the iOS environment, this method has a low degree of success (Wright & Adler, 2010).

Back-up utilization is simply using a backup of the mobile device to perform the forensic analysis. The primary constraint when utilizing this method is that the investigator only has access to those files that have been implicitly synchronized using the device's standard protocol (Hoog & Strezempka, 2010). When considering the iPhone device, this method can serve the investigator well since there is much information in the SQLite database that is supported by the protocol. This database can be queried directly to obtain the deleted information however, to do so requires the investigator to use a Jailbreaking method, which, as has been noted, is not considered a forensically sound procedure.

Bit-by-bit method of acquisition is considered the most thorough of all acquisition methods for mobile devices (Hoog & Strezempka, 2010). This method creates a physical bit-by-by copy of the mobile device's data including the deleted files that net in the greatest amount of information. It is considered the method that is most closely related to the traditional methods of evidence acquisition. Unfortunately, in the iOS environment, this method is not possible without the use of Jailbreaking.

4.2 Challenges in Acquisition

There are many challenges when considering forensics within the iOS environment that prevent a full acquisition of the iDevice. The speed of change within the technology landscape continues to prove to be a barrier to the investigation (Owen, Thomas, & McPhee, 2010; Zarren & Baig, 2010). This causes conflicts between version of the OS as well as within the vendor's offerings.

There is also a lack of write-blocking techniques for mobile devices. Without write blocking, there is nothing to prevent the device from receiving messages such as calls and texts while performing a forensic investigation (Zarren & Baig, 2010; Zdziarski, 2010). While blocking can be prevented using a shielded lab, as Zdziarski notes (2010), it is very expensive to implement. A more economical approach may be to remove the SIM to disable reception during the investigation. However, access to the SIM, which may contain information such as encryption keys that may be associated with user authentication, will be unavailable which may in turn hinder the investigative process. If we take a different point of view from the investigative approach, it may be beneficial to maintain the incoming call reception while maintaining a block of the write activities in order to capture on-going communications. This of course is driven by the goals and objectives of the investigative body.

From a forensic process point of view, there is a lack of standardization within the manufacturing community in terms of data storage. This creates an environment where commonly known tools are rendered substandard with each release of an update to the OS.

Often times, the investigator has to work on the actual device, which affects the forensic integrity of the investigation (Owen, Thomas, & McPhee, 2010). For example, when an acquisition is taken, the device must be powered on. When this is done, the state of the device is modified. This situation forces the investigator to become acutely aware of which state the device is in at any given time and how to handle the evidence for the given state (Owen, Thomas, & McPhee, 2010). Initially, it appears as if the chip-off method would negate the need to power on the device in order to take the image. However, as noted above, in the iOS environment, the drive is always encrypted therefore the chip-off method has little degree of success (Wright & Adler, 2010).

One of the most significant challenges is that the commonly available forensic tools most often only perform logical acquisitions, which does not capture the deleted data as is done with a physical acquisition (Zareen & Baig, 2010). This is where many investigators turn to Jailbreaking as a method to perform a physical acquisition. As noted above, Jailbreaking is not considered a forensically sound procedure since in effect the investigator is altering the information contained on the device that may have an impact on the evidence presented.

Finally, although this presentation of challenges is not exhaustive by any means, there is the challenge of backward compatibility between releases of the iOS environment that needs to be addressed. One facet of our research shows that each release of the iPhone environment has a software version, a baseband version and a bootloader version which will have an impact on how one must handle the device during an investigation. Currently, it is known that the baseband updates the software version when an update occurs via iTunes. While the software version can be rolled back to its original state, the baseband cannot unless jailbreaking methods are employed. Also, the bootloader version cannot be modified as it is dependent upon the timeframe in which the device was manufactured. To negate this version dependence that is currently a factor in the investigation, one area of our research is focusing on building an external device that is platform independent. This device is expected to be attached to the iOS device which will allow the investigator to gain access to the necessary areas of the system without the need to jailbreak the device. Our future work will further address the challenges presented as well as present the findings of building the external device via the presentation of a more detailed study.

4.3 iOS Forensic Toolsets

The primary goals of any forensic toolset are to extract the evidence from the mobile device, support the reporting objectives as well as to provide for the examination functions. The level of quality that is expected of any investigation when utilizing a forensic toolset is to preserve the integrity of the acquired and extracted data at all costs. As Hoog and Strezempka (2010) state in their study, the key aspect is to avoid modification of any data components within the storage areas of the device. However, if that is not possible, all modifications must be supported by the audit trail put forth (Hoog & Strzempka, 2010).

In order to provide a complete, forensically sound acquisition, both the logical and physical acquisition must be accomplished. As Owen, Thomas and McPhee (2010) identify, with the current landscape of tools that are available to the investigator it is not possible to make a complete image of the mobile device, as these tools do not support both the physical and logical acquisition. Unfortunately, most available tool-sets provide for only the logical acquisition meaning that in order to retrieve the deleted files of the iOS device, one must also perform a physical acquisition. The reasons a second, physical acquisition must occur, as stated previously, is that the iOS device relies on flash memory instead of a traditional hard drive which renders the majority of the toolsets available inadequate (Janson, Delaitre & Moenner, 2008). It is because of this gap, that data recovery is usually carried out via the logical acquisition by utilizing one or more of the iOS supported protocols (Janson, Delaitre & Moenner, 2008).

To give an understanding of the current toolset landscape, a discussion of the current state of software tools available to the forensic investigator follows. It should be noted that this list of software tools is not exhaustive. It should also be noted that the consideration of the information obtained from a Network Service Provider, while an important part of any investigation, is beyond the scope of this research.

When considering traditional digital forensics, there is an industry focus on two primary toolsets, Encase (Guidance Software) and FTK (Access Data) (Owen, Thomas, & McPhee, 2010). With the surge of iOS devices entering the market place between 2007 and present day, these two vendors have emerged with forensic toolsets to support the iOS device.

Encase Neutrino is Guidance Software's mobile solution in forensic acquisition. It has the ability to support devices from Nokia, Motorola, Samsung, Siemens, LG, Palm, Blackberry (RIM), HTC, UTStarCom, and Sony Ericsson. (Guidance Software, 2010) The tool can collect data from unallocated space (deleted files) on select devices including the iPhone (Hoog & Strezempka, 2010). However, according to the corporate brochure, there is no mention of iPhone support (Guidance Software, 2010). Testing as presented by Hoog & Strzempka (2010) identified that the toolset missed SMS messages and photos in unallocated space (deleted files), was unable to pick up screen shots, music files, passwords, phone information, HTML files and MS Office documents. The study also identified that the tool-set fell below expectations when retrieving email (Hoog & Strzempka, 2010)

Access Data's Mobile Phone Examiner (MPE) Plus software brochure indicates that it supports more than 1200 various devices with support for 2300 devices by January 2011 however there is no indication that it supports the iOS system. Logical acquisition is supported but the vendor's website indicates that physical acquisition will be forthcoming for iPhone, iPad and Android. Following acquisition, the file must be imported to Forensic Tool Kit 3 (FTK3) as there is no backward capability to prior releases of the FTK toolset.

As recently as 2010, there are a few software toolsets and procedures to support forensics in the iOS environment. A few of the more popular software tools and methods for iOS forensics are presented.

Perhaps the most popular and receiving the most focus as of the writing of this study is Zdziarski's Method of iOS acquisition. At a high-level, the Zdziarski Method is what is termed as a "semi-Jailbreak" solution. We state this because the method uses system RAM to inject code into the space that will allow full access to a raw disk image as well as bypass security components such as user passcodes (Zdziarski, 2010). The image can be captured via a SSH protocol using a WiFi connection once access has been gained (Zdziarski, 2010). To gain a full understanding of the Zdziarski Method, the reader is encouraged to further enhance their knowledge by examining the research as presented by Zdziarski in 2010. While Zdziarski (2010) indicates that there are no Jailbreaks employed when utilizing his methods to perform a physical acquisition since the user area of RAM is left untouched, the device's system RAM is loaded with the needed imaging components to allow the iOS device to boot from memory. The modified device reverts to its original state when rebooted. By definition, this is Jailbreaking the system since RAM is modified to bypass the manufacturer's preventative measures as well as device security components. Granted, there is a lower probability that since system RAM is being modified, that critical data will be over-written. This of course assumes that the system RAM was 'clean' prior to the forensic acquisition. Zdziarski uses a tool-set that was developed in-house to perform the forensic examination and this tool-set is only available to law enforcement personal (Zdziarski, 2010). It should be noted that the Zdziarski Method was validated in draft by NIST in October 2010 (NIST, 2010). Testing showed that the methodology did acquire all supported data objects when using the Smartphone Tool Test Assertions and Test Plan with the iPhone 3G device (NIST, 2010). However, when Hoog and Stzempka (2010) performed their testing against the iPhone 3G, there were occasions where various components, such as passwords, were missed.

Another popular tool-set used for iOS forensics is the Paraben Device Seizure 4.0 tool. The software specifications indicate that 2200 devices are supported however; there is no direct indication that there is support for the iOS environment. The software specification indicates that the tool has the ability to perform both logical and physical acquisition however; the testing as perform by Hoog & Strzempka (2010) indicates that the tool uses the devices backup function to recover the deleted files. The Hoog & Strzempka (2010) testing survey indicated that the tool missed SMS messages and photos in unallocated space (deleted files). The tool also missed music files, screen shots, passwords, HTML and MS Office files as the Encase Neutrino tool did. In addition, like Encase Neutrino, the tool fell below expectations for email recovery. The tool also fell below expectation in video and voice mail recovery (Hoog & Strzempka, 2010)

There are many more commercial and open source forensic tools coming into the digital forensic landscape but continue to face the common issues as noted above (Hoog & Strzempka, 2010; Owen, Thomas, & McPhee, 2010)

As can be seen, unallocated space (deleted files) continues to be a troublesome area without the use of device modification tools and methods as demonstrated by Zdiarski's Method. The research, as will be presented in future works, will attempt to eliminate these concerns.

5. FORENSICS IN THE IOS ENVIRONMENT

As can been expected, the amount of ubiquitous information stored on mobile devices will continue to grow (Owen, Thomas, & McPhee, 2010). Zareen & Baig (2010) stress the need for the development of new forensic tools and techniques to support this non-traditional computing environment.

With this gap in mind, we are proposing the development of a forensic toolset which includes building an external device as outlined above that will support both physical and logical acquisition in the iOS environment. The software side of the toolset is expected to function in much the same way that traditional forensic toolsets perform when applied to the standard computing environment however there will be no need to first jailbreak the device prior to imaging process. We believe that enabling a toolset that does not require jailbreaking will aid the civilian examiner as noted above in regards to the legal issues that surround the jailbreaking process. Also, being able to perform both, a logical and physical acquisition in such a manner will support the integrity of the investigation.

We also are focusing on the development of this toolset in such a way as to support platform independence as well as version change independence. We believe that with an external device, the version of the software, the baseband and the bootloader of the iOS environment will no longer be a consideration when moving forward with acquisition.

Additionally, as indicated in the literature, there is not a full understanding of the ramification when using the jailbreaking methodology during the iOS investigation. As our research moves forward, we expect to develop this understanding in a well-documented study that will be presented to the research community upon its completion.

The toolset under development that will be presented to the research community is being developed based on the NIST CFTT (Computer Forensics Tool Testing) specifications. The objectives of the CFTT program is to provide measureable assurance to practitioners, researchers, and other application users that the tools used in computer forensics investigations provide accurate results (NIST, 2010).

6. CONCLUSIONS

Smartphone usage has grown considerably over the past year with the 2nd quarter of 2009 showing that these types of devices have accounted for 16% of the total mobile market (Dalrymple, 2010). This staggering surge further jumped to 23% in Q1 of 2010 (Dalrymple, 2010). iPhone and iPad devices are responsible for a considerable amount of this growth. As noted above and is presented in a study from the Nielsen organization and was presented by Dalrymple (2010), since its introduction to the market in 2007, the iPhone (28%) has more than triple market share over Android (9%). Currently, Blackberry still holds the lead at 35% (Dalrymple, 2010). iPhone and iPad are expected to continue to dominate the market place in coming years due to its user focused platform.

With this growth in mobile device usage, the primary challenges in mobile forensics, in particular the iPhone/iPad environments, continue to be rapid changes in the technology stack, a lack of standardized methods for data storage and the closeness of the OS. It is because of these reasons that there is a need for the development of new forensic tools and techniques that specifically address these unique attributes of the mobile environment.

The toolset that will be presented to the research community in future publications will address and resolve the shortcomings of obtaining a complete image (physical and logical) of the iOS device, the current usages of Jailbreaking in a forensically sound environment as well as the issues of platform and version dependence.

REFERENCES

Access Data. (2010). Mobile Forensics Examiner (product brochure). Retrieved December 27, 2010, from http://accessdata.com/products/forensic-investigation/mobile-phone-examiner

Brewin, B. (2010). VA employees tap cloud apps on their own, posing security risk. Retrieved December 24, 2010, from http://www.nextgov.com/nextgov/ng_20101222_6852.php

Chaffin, B. (2010). iSuppli Bumps 2011 iPad Forecast to 43.7 Million. Retrieved December 16, 2010, from http://www.macobserver.com/tmo/article/isuppli_bumps_2011_ipad_forecast_to_43.7_million/

Dalrymple, J. (2010). iPhone triples Android in mobile market share. Retrieved December 27, 2010, from http://news.cnet.com/8301-13579_3-20006889-37.html

Dancer, F. C. T., & Dampier, D. A. (2010). *A Platform Independent Process Model for Smartphones Based on Invariants.* Paper presented at the IEEE International Workshop on Systematic Approaches to Digital Forensic Engineering.

Elmer-DeWitt, P. (2010). What's driving iPhone 4 sales? Retrieved December 16, 2010, from http://tech.fortune.cnn.com/2010/06/17/whats-driving-iphone-4-sales/

Family Educational Rights and Privacy Act (FERPA). (2010). Retrieved December 16, 2010, from http://www2.ed.gov/policy/gen/guid/fpco/ferpa/index.html

Guidance Sotftware. (2010). Encase Neutrino (software brochure). Retrieved December 27, 2010, from http://www.guidancesoftware.com/mobile-cellphone-forensics-software-neutrino.htm

Harrington, M. (2008). iPhone Forensic Examinations – A Series. Retrieved December 25, 2010, from http://mobileforensics.wordpress.com/2008/09/15/iphone-forensic-examinations-a-series/

HIPPA-1996 (2010). Retrieved December 16, 2010, from http://www.hhs.gov/ocr/privacy/index.html

Helft, M., & Bilton, N. (2010). For Apple, Lost iPhone Is a Big Deal. Retrieved December 16, 2010, from http://www.nytimes.com/2010/04/20/technology/companies/20apple.html

Hoog, A., & Strzempka, K. (2010). iPhone Forensics White Paper. Retrieved Dec 16, 2010, from http://viaforensics.com/education/white-papers/iphone-forensics/

Identity Theft State Statutes. (2010). Retrieved December 16, 2010, from http://www.ncsl.org/?tabid=12538

iFixit. (2010). Retrieved December 18, 2010, from http://www.ifixit.com/Device/iPhone_4

Janson, W., Delaitre, A., & Moenner, L. (2008). Overcoming Impediments to Cell Phone Forensics. In Proceedings of the 41st Hawaii International Conference on Systems Sciences.

Justice, C., Wu, H., & Walton, E. (2009). *Mobile Forensics in Healthcare*. Paper presented at the Proceedings of the 2009 Eighth International Conference on Mobile Business.

Morrisey, Sean. (2010, July). New DFM recruit Sean Morrisey writes about the iPhone forensic tool Lantern. DFM Newsletter July 2010. Retrieved March 19, 2011 from http://www.digitalforensicsmagazine.com/newsletter/DFM-Newsletter07.html

NIST. (2007). SP800-101 Guidelines on Cell Phone Forensics (pp. 104). Retrieved from http://csrc.nist.gov/publications/nistpubs/800-101/SP800-101.pdf.

NIST. (2010). Test Results for Mobile Device Acquisition Tool: Zdziarski's Method (draft). October 2010. Retrieved from http://www.ntis.gov/search/product.aspx?ABBR=PB2011104749

Owen, P., Thomas, P., & McPhee, D. (2010). *An Analysis of the Digital Forensic Examination of Mobile Phones* Paper presented at the 2010 Fourth International Conference on Next Generation Mobile Applications, Services and Technologies.

Palmer, G. (2001). *A Road Map for Digital Forensic Research.* Paper presented at the First Digital Forensics Research Workshop (DFWRS). Retrieved from http://www.dfrws.org/2001/dfrws-rm-final.pdf

Pollitt, M. M. (2007). *An Ad Hoc Review of Digital Forensic Models*. Paper presented at the Proceedings of the Second International Workshop on Systematic Approaches to Digital Forensic Engineering. http://ieeexplore.ieee.org/xpl/freeabs_all.jsp?arnumber=4155349

The Sarbanes-Oxley Act of 2002. (2010). Retrieved December 16, 2010, from http://www.gpo.gov/fdsys/pkg/PLAW-107publ204/content-detail.html

Schuessler, J. H., & Ibragimova, B. (2009). *Portable Privacy: Mobile Device Adoption*. Paper presented at the Annual Security Conference. Retrieved from *www.security-conference.org/SecurityConf_2009_Proc/Papers/4.doc*

Scoop, E. (2010). DrFirst™ Creates Stunning E-Prescribing Experience on iPhone Retrieved December 16, 2010, from http://www.emrconsultant.com/forum/topic/722-drfirst-creates-stunning-e-prescribing-experience-on-iphone/

Wright, J. & Adler, M. (2010). Session 209-Securing Application Data. Apple World Wide Developers Conference 2010. San Francisco, CA, USA. Retrieved December 29, 2010 from http://developer.apple.com/videos/wwdc/2010/

Yarow, J. (2010). Best Buy CEO: iPad Is Cannibalizing Laptop Sales By As Much As A Shocking 50%. Retrieved December 16, 2010, from http://www.businessinsider.com/best-buy-ceo-ipad-is-cannibalizing-laptop-sales-2010-9

Zdziarski, J. (2010). The Zdziarski Method. Retrieved December 26, 2010, from http://viaforensics.com/education/white-papers/iphone-forensics/zdziarski/

Zareen, A. & Baig, S. (2010). Mobile phone forensics: Challenges, analysis, and tool classification. In Proceedings of 5th International workshop on Systematic Approaches to Digital Forensic Engineering, 47-55. May 2010, Oakland, CA, USA.