STM JOURNALS

E - Commerce for Future & Trends

Volume 1, Issue 1
www.stmjournals.com

Study on Digital Forensics in IoS Devices

P. Ravi Shankar[1], P. Parimala[1], P. Krishna Subba Rao[2]*, Ch. Avinash[2]
[1]MVGR College of Engineering, Vizianagaram, India
[2]Gayatri Vidya Parishad College of Engineering (A), Visakhapatnam, India

Abstract

Digital forensics has progressed rapidly but much more is required, including developing more sophisticated techniques for acquiring and analyzing digital evidence, increasing scientific rigor in our work, and also professionalizing the field. This paper surveys the area of digital forensics, with the aim of systematizing the existing techniques which is useful for promoting future research. The authors first present the unique aspects and also the tools used in digital forensics. Finally, they summarize the lessons learnt and discuss future research opportunities in the area of portable devices like smart phones, IoS devices, etc.

Keywords: *Forensics, triaging, IoS, chip-off, jail breaking*

[*]***Author for Correspondence*** E-mail: krishnasubbarao@gvpce.ac.in

INTRODUCTION

The proliferated usage of electronically connected devices has evoked a speedy growth in cyber-related crimes. Mobile device forensics has grown tremendously with the advent of smart phones. A lucid fact in the release of smart phones is that they are not used just for communication purposes but urging a large storage area for documents, messages, pictures, videos, emails and other types of files. Forensic examiners can find interesting information acquired from mobile devices which helps them to investigate the case to catch criminals and their accomplices.
According to Gartner Report (2013) on the usage of smart-phones worldwide, statistics state that sales of smart phones are based on the operating systems. Android OS occupies a share of 78.4%, IoS takes up a 15.6%, while the other OS like Microsoft, Blackberry and others take up 3.2, 1.9 and 0.9% respectively.

Mobile phone forensics is the science of recovering digital evidence under forensically sound conditions. A forensic investigator can find evidence of interest in mobile phone storage locations such as subscriber identity module (SIM), internal memory of mobile, memory cards and network service providers. External memories may include SIM, MM, SD, micro-SD and memory stick. These external cards can have a large storage area up to 32 GB.

The forensic analysis of acquired digital evidence on mobile-phones begins with preserving data acquisition followed by analysis using available forensic tools and preparing a detailed report. Data acquisition methods depend on the model, OS installed on the phone, time, nature of the case and sometimes the service provider by reports.

The detection of digital evidence in its original form is the first and foremost step in the investigation process. After seizure, the mobile phone must be switched off to preserve its battery power. The other approach is it should be isolated for blocking the signals by placing the device in a radio wave-blocking paint can or usage of a Paraben stronghold bag or eight layers of antistatic bags. The drawback with the above procedure is that the battery drains off very quickly. So a battery-powered charger should be plugged until the evidence is carried to the forensic lab for further investigation.

I-phone has an active hacking community which has yielded research and tools which supports forensic investigations. This paper is structured as follows. First section is mobile phone forensics challenges, analysis and tools; the next section is on practical investigation of

digital forensics tools for mobile devices and forensics tools for mobile devices and forensic data recovery from android OS devices; further paragraphs deal with mobile phone challenges analysis and tools and quantitative approach in triaging in mobile forensics; the later section consist of third party application forensics on Apple mobile devices and design and implementation of digital forensic software for iPhone; and the last sections explain the forensics related to IoS and summarize the paper contributions and outline further work.

MOBILE PHONE FORENSICS CHALLENGES, ANALYSIS AND TOOLS

Data acquisition is the process of extracting data from the digital device after careful retention, documentation and transportation to the forensic lab for future investigation [1]
Data acquisition types are manual, logical, physical, and chip-off.

1. Manual Acquisition

It is a simple and easy method for retrieval of data from mobile phones. Manual acquisition involves searching for text messages, call logs and taking pictures of data displayed on the screen. The advantage of this method is that no training is required, works with all phone models and does not require any drivers, cables or software. The disadvantage is that any hidden or deleted data cannot be found, no assurance of data integrity and does not work with password-protected phones. Fernico ZRT tool is being used to perform manual examination which takes photos of the screen and merge into a designed template.

2. Logical Acquisition

This method performs a bit-by-bit copy of logical storage objects residing in logical partitions. It is not possible to retrieve any hidden or deleted files from unallocated space. This method is performed by connecting the mobile phone to the investigator's PC using blue tooth connection or a cable. The advantage is that the system data structures are easier for a tool to extract. Oxygen phone manager, Paraben and TULP2, are the tools that are used with AT commands for logical acquisition.

3. Physical Acquisition

Bit-by-bit copying of entire physical memory, i.e., the flash memory is the method of acquiring data in this type of acquisition. The memory can be volatile and non-volatile in the flash memory.
Three different types of this method of acquisition are

1. Using flashes tools (copying of flash memory)
2. Joint test action group (JTAG)
3. Physical removal of flash memory from a board and reading memory with a card reader.

4. Chip-off

Finally, the Chip-off method is used to get an image of internal non-volatile memory by disordering it from printed circuit board (PCB) and acquiring data from the chip by using a chip reader. Microball grid array (BGA) or their small outline package (TSOP) chips can be disordered using hot air nozzle; the advantage is that it answers data integrity. The major disadvantages are that the original structure of the phone cannot be retained and due to heat for de-soldering the memory chip can get damaged.

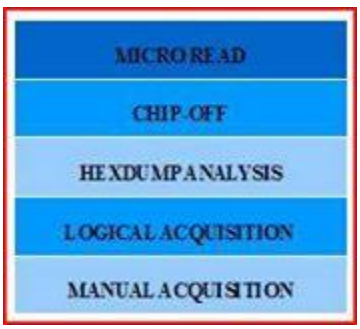

Fig. 1: *Levels of Analysis.*

PRACTICAL INVESTIGATION OF DIGITAL FORENSIC TOOLS FOR MOBILE DEVICES AND FORENSIC DATA RECOVERY FROM ANDROID OS DEVICES

With continued growth of mobile device market, the possibility of their use in criminal activity will only continue to increase. While the mobile device market provides a great variety of manufactures and models causing a strong diversity, it becomes difficult for a professional investigator to choose the proper forensic tools for seizing internal data from mobile devices. In view of commercial popular digital forensic tool and offer an inside view for investigators to choose their free sources or commercial tool [2].

Some of the digital forensic tools will be discussed briefly which include both open source and commercial tools.

A) FTK Mobile Phone Examiner

FTK mobile phone examiner is the most commonly used forensic tool for mobile devices in the United States, a distinction shared with Guidance's Encase Forensic suite.

B) Oxygen Forensic Suite

Oxygen prides itself on its reputation of being able to extract unique information from a smartphone.

C) Paraben's Device Seizure

Device seizure focuses on the physical level of acquisition because you can acquire more information with physical acquisition than logical.

D) Other Tools

The recovery of data from mobile phones is a very specialist and evolving field, which can make considerable assistance in the prosecution of criminal cases. Data can include not just call history or text messages but, as mobile phones become more smart, it can also include internet web pages, chat data, social media files and other application data [3]. In this paper, the authors present an open-source toolkit developed to improve work flow for forensic analysts and to aid Android OS mobile phone forensics.

The assumption is that the initial sentences of a paragraph are the most important. Therefore, the investigators rank a paragraph sentence according to their position and consider maximum positions of 5 [4].

Issues	Forensics of Computers	Forensics of Handheld Devices
On/off dilemma	Less problematic	More problematic
Evidence volatility	Lower	Higher
Imaging process	Less tricky	More tricky
Size of evidence	Larger	Smaller
Technological development	Slower	Faster
Operating systems	Less problematic	More problematic
Training	Clear	Unclear
Forensic tools	More proprietary tools	More open source tools

Table 1: *Forensic of Computers versus Forensics of Mobile Devices.*

MOBILE PHONE FORENSICS CHALLENGES, ANALYSIS AND TOOLS CLASSIFICATION AND QUANTITATIVE APPROACH TO TRIAGING IN MOBILE FORENSICS

Nowadays mobile phones and other hand-held devices are everywhere. Cell phones and cellular devices can be involved in a crime or other incidents. Digital forensic specialists will require specialized tools for forensic examination of mobile phones for proper recovery and speedy analysis of data [5] present on mobile phones.

A. Evidence Items Available in Mobile Phones

Mobile phones contain various evidence items which can be of interest for a forensic examiner. The main source of evidence on a mobile phone may include subscriber identity module (SIM), mobile phone internal memory, memory cards and network service providers.
External memories for mobile phones may include SIM, SD, MMC, CF cards, and the memory stick.

B. Levels of Analysis for Data Acquisition from Mobile Phones

Methods for data acquisition from mobile phones mainly depend upon the condition, model, time and nature of the case. Methods that are currently used in the field of mobile phone forensics focus on extracting information by using the AT-command set which has been specified for communication with serial modems as per GSM specifications. Based on various extraction methods, different levels of analysis can be logically made for evidence acquisition from mobile phones.

Manual acquisition involves reviewing phone documentation and browsing manually using the keypad and display of mobile phone to document data present in the mobile phone.
Logical acquisition involves access to user files while connecting data cable to the handset and extracting data using AT commands using various software tools. Hex Dump Analysis involves physical acquisition of a mobile phone's file system. Data is obtained in a "raw" form which requires interpretation. This method provides access to deleted data from the mobile's internal memory and helps extract data hidden from handset menus.

Chip-off method involves the removal of a memory chip from mobile phone and read in either second phone or Eeprom reader to conduct forensic analysis. Micro Read is a process that involves the use of a high-power microscope to provide a physical view of the electronic circuitry of mobile phone memory.

Forensic study of mobile devices is a relatively new field, dating from the early 2000s. The proliferation of phones (particularly smart phones) on the consumer market has caused a growing demand for forensic examination of the devices, which could not be met by existing computer forensic techniques. As a matter of fact, law enforcement agencies are much more likely to encounter a suspect with a mobile device in his possession than a PC or laptop and so the growth of demand for analysis of mobiles has increased exponentially in the last decade. Early investigations, moreover, consisted of live analysis of mobile devices by examining phone contents directly via the screen and photographing it with the risk of modifying the device content, as well as leaving many parts of the proprietary operating system inaccessible. The recent development of mobile forensics, a branch of digital forensics, is the answer to the demand of forensically sound examination procedures of gathering, retrieving, and identifying, storing and documenting evidence of any digital device that has both internal memory and communication ability.

Cell phone, PDA and new generation smart phone proliferation is on the increase all over the world. Worldwide sales of mobile devices to end users totaled 455.6 million units, according to Gartner, Inc. After a few interviews with Italian law enforcement cyber-crime specialists, the authors noticed a growing complexity in today's forensic investigations due to the quantity of new mobile phones released every year, each with its own operating system (i.e., Android, Symbian, Apple IoS, RIM, Windows, etc.) and a different file system and memory organization. In Figure 3, worldwide smartphone selling figures by operating systems in 2Q13 are presented.

Table 3

Worldwide Mobile Phone Sales to End Users by Vendor in 3Q13 (Thousands of Units)

Company	3Q13 Units	3Q13 Market Share (%)	3Q12 Units	3Q12 Market Share (%)
Samsung	117,053.8	25.7	97,956.8	22.7
Nokia	63,048.4	13.8	82,300.6	19.1
Apple	30,330.0	6.7	24,620.3	5.7
LG Electronics	18,030.7	4.0	13,968.8	3.2
ZTE	13,696.4	3.0	16,605.9	3.9
Huawei	13,574.4	3.0	11,918.9	2.8
Lenovo	12,999.8	2.9	7,203.7	1.7
TCL Communication	12,345.6	2.7	9,326.7	2.2
Sony Mobile Communications	9,757.5	2.1	8,202.4	1.9
Yulong	8,801.0	1.9	5,218.5	1.2
Others	156,004.7	34.2	153,701.20	35.7
Total	**455,642.3**	**100.0**	**431,023.8**	**100.0**

Source: Gartner (November 2013)

Fig. 2: *World Wide Mobile Device Sales-3Q13.*

Table 2

Worldwide Smartphone Sales to End Users by Operating System in 3Q13 (Thousands of Units)

Operating System	3Q13 Units	3Q13 Market Share (%)	3Q12 Units	3Q12 Market Share (%)
Android	205,022.7	81.9	124,552.3	72.6
iOS	30,330.0	12.1	24,620.3	14.3
Microsoft	8,912.3	3.6	3,993.6	2.3
BlackBerry	4,400.7	1.8	8,946.8	5.2
Bada	633.3	0.3	4,454.7	2.6
Symbian	457.5	0.2	4,401.3	2.6
Others	475.2	0.2	683.7	0.4
Total	**250,231.7**	**100.0**	**171,652.7**	**100.0**

Source: Gartner (November 2013)

Fig 3: *Worldwide Smart Phone Sales by OS in 2Q13.*

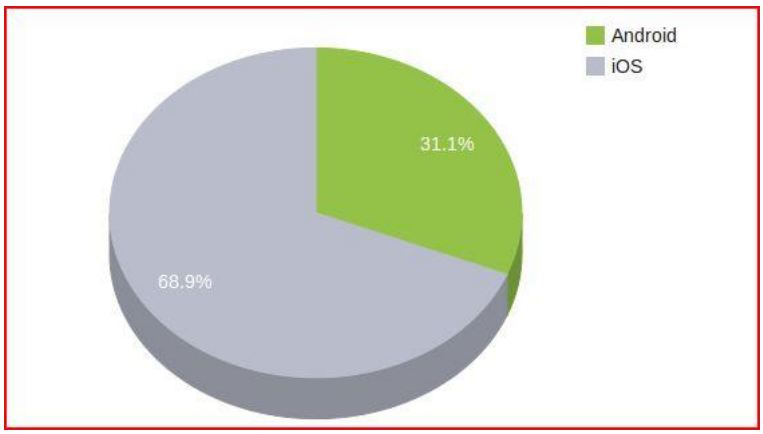

Fig. 4: *Android OS (VS) IoS.*

Nowadays most of the users are using android and IoS as their mobile operating systems. Figure 4 shows how many of people are using android and IoS operating systems.

The four-step mobile forensic work flow, based on device identification, acquisition, and analysis and reporting, was found to be inadequate to current investigation. To modify it introducing an intermediate step, called triage [6, located between acquisition and analysis, with the aim of limiting the area of interest and reduce the number of relevant devices to focus on.

FORENSICS RELATED TO IoS

The field of iPhone forensics is still currently under development. They are currently non forensic methods that can be used in order to get an image off an iPhone. Some of these tools and methods involve altering the iPhone in some manner, which may cause any evidence retrieved in this manner to be considered inadmissible in the court of law.
New tools being released in the market allow you to gather information when iPhone data is backed up to a Mac or PC. Using proven forensic methods, artifacts from the iPhone can be retrieved.

In an effort to unlock any suspicious devices, iPhone has become the subject of many hacker groups and developers. These methodologies were originally designed to assist in jail breaking the device, a third-party software for unlocking which has originated from Unix practice of unlocking jail directory structure. The very first jail break involved breaking Apple's AFC protocol

In an effort to unlock any suspicious devices, iPhone has become the subject of many hacker groups and developers. These methodologies were originally designed to assist in jail breaking the device, a third-party software for unlocking which has originated from Unix practice of unlocking jail directory structure.

Mobile forensics requires limited interaction with the device in its data extraction. In general, a forensic imaging agent is instituted as a process in the device memory – remote code consisting of the aspect of file transfers, encrypting keys and connection aspects of raw disks. The new advancements have enabled the device to make it fit into handling hardware-based decryption and in obtaining restricted information from the devices such as secret encryption keys.

Model Number	Device
A1203	iPhone (First Generation)
A1241	iPhone 3G
A1303	iPhone 3G[s]
A1332	iPhone 4 (GSM)
A1349	iPhone 4 (CDMA)
A1288	iPod Touch (Second Generation)
A1318	iPod Touch (Third Generation)
A1367	iPod Touch (Fourth Generation)
A1219	iPad WiFi (First Generation)
A1337	iPad WiFi+3G (First Generation)
A1378	Apple TV (Second Generation)

Fig. 5: *Table Representing Generations of Different iPhone Devices.*

THIRD PARTY APPLICATION FORENSICS ON APPLE MOBILE DEVICES AND DESIGN AND IMPLEMENTATION OF DIGITAL FORENSIC SOFTWARE FOR iPHONE

Forensics on mobile devices are not new. Law enforcement agencies and academia have been performing forensics on mobile devices [4] for the past several years.

Forensics on mobile third-party applications is new. There have been third-party applications on mobile devices before, but none that provided the number of applications available in the iTunes app store. Mobile forensic software tools predominantly addresses "typical" mobile telephony data – contact information, SMS, and voice mail messages. These tools overlook analysis of information saved in third-party applications. Many third-party applications installed in Apple mobile devices leave forensically relevant artifacts available for inspection. This includes information about user accounts, timestamps, geo-locational references, additional contact information, native files, and various media files. This information can be made readily available to law enforcement agencies through simple and easy-to-use techniques.

A. Apple Devices

With the introduction of iPhone, Apple allows users to install and configure a wide variety of applications via "app store." The applications are downloaded to the device from Apple's servers and installed. An application can be launched by the user. Apps are typically backed up to the personal computer of the user whenever the device is synced as well.
Applications can be written by anyone after they agree to the terms prescribed in the Apple Developers License. Apple closely regulates applications submitted for sale in the app store.

B. Application & Platform Growth

There are currently over 200,500 active applications in the app store. According to Steve Jobs presentation during the iPad announcement in April 2010, the number of iPhone-based OS devices exceeded 90 million; it includes both iPhone and iPad touch devices.
The Apple mobile device platform is popular and will continue to grow as a platform for third-party applications.

iPhone, which is equipped with the IoS operating system, has become one of the most popular smart phones since its release in June, 2007; with its popularity and extensive use, it has certainly become the microcomputer that is necessary in our daily lives. However, the increasing trend of safety and criminal issues have made the development of iPhone forensics a must. Because of the gradual development and the increasing attention it receives, it is required to develop forensic software.

iPhone has dominated the market of cell phones. According to the latest research of Gartner organization, the sales amount of the fourth quarter of 2011 has surpassed Samsung and LG and taken the third place in the cell phone market share. It has still remained in the first three places till the third quarter in 2012; the amount of download of applications of Apple Store has grown from 3 to 10 billion from January 2010 till now. This shows that iPhone plays a crucial role in smart phones. The study uses Objective-C as the developing device and uses the National Institute of Standards and Technology to design and implement smart phones forensic program system of iOS platform, to help forensic investigators to retrieve crucial information from cell phones via simple installation and operating procedures, and to offer digital evidence-related collection of investigation and analysis report.

CONCLUSIONS

This paper provides a comprehensive survey of recent research papers in the area of digital forensics and describes unique characteristics of different forensic tools, about different preservation and investigation procedures using forensic tools. It also addresses the comparison of operating systems based on the usage which might be useful for the process of digital forensics. After surveying several papers on digital forensics, the authors would like to identify some more forensic methods

and procedures in the area of IoS operating system.

REFERENCES

1. *Mobile Phone Forensics Challenges, Analysis and Tools Classification* (http://dl.acm.org/citation.cfm?id=1829569).
2. *Forensic Data Recovery from Android OS Devices: An Open Source Toolkit* (http://ieeexplore.ieee.org/xpl/login.jsp?tp=&arnumber=6657168&url=http%3A%2F%2Fieeexplore.ieee.org%2Fxpls%2Fabs_all.jsp%3Farnumber%3D6657168).
3. *Design and Implementation of Digital Forensic Software for iPhone* (http://ieeexplore.ieee.org/xpl/login.jsp?tp=&arnumber=6621657&url=http%3A%2F%2Fieeexplore.ieee.org%2Fiel7%2F6621628%2F6621634%2F06621657.pdf%3Farnumber%3D6621657).
4. *Third Party Application Forensics on Apple Mobile Devices* (http://ieeexplore.ieee.org/xpl/login.jsp?tp=&arnumber=5719010&url=http%3A%2F%2Fieeexplore.ieee.org%2Fxpls%2Fabs_all.jsp%3Farnumber%3D5719010).
5. *Practical Investigations of Digital Forensics Tools for Mobile Devices* (http://www.famu.edu/cis/p156-yates.pdf).
6. *A Quantitative Approach to Triaging in Mobile Forensics* (http://ieeexplore.ieee.org/xpl/login.jsp?tp=&arnumber=6120868&url=http%3A%2F%2Fieeexplore.ieee.org%2Fxpls%2Fabs_all.jsp%3Farnumber%3D61208680.