INTERNATIONAL JOURNAL FOR ADVANCE RESEARCH IN ENGINEERING AND TECHNOLOGY

WINGS TO YOUR THOUGHTS…..

Information System Forensic Research Paper Mobile Device Forensics

Sarvesh Kapre

Master of Science in Information Assurance
College of Computer and Information Science, Northeastern University
kapre.s@husky.neu.edu

***Abstract**: The need for mobile device forensics has increased prodigiously since the last decade. Mobile devices have overtaken the count of humans and computers and so is its involvement in crime and other illegal activities. The need to study mobile device forensic is vital as it is the most challenging aspect in computer forensics. The reason being, each company having their own proprietary format and standards in developing mobile devices, thus causing difficulty for the forensic investigator to perform forensic investigation using a standard tool. Mobile technology is progressing at such a blistering pace that new mobile devices are being launched and updated every month. Due to this reason the forensic investigators must follow and unrelenting and tenacious approach in this field. This paper involves the study of pertinent mobile forensic tools for performing forensic analysis and data acquisition on mobile devices.*

***Keywords:** Chain of Custody, Acquisition, Chip-Off, JTAG, Bootloader, ADB, MD5, SHA 1, CRC, IMEI, File Slack, GREP.*

1. INTRODUCTION

It won't be inappropriate to say that our mobile phones know much more about us than we know about ourselves. Mobile devices have become an integral part of or life and most of our activities are performed through our cell-phones. Criminals and persons performing illegal activities communicate to each other via mobile devices, either by calling or by SMS or E-mails. Law enforcement needs proof to prove the guilt of the accused and what else can be a better medium to extract information than with the help of mobile devices? But how to perform these acquisitions? How to extract hidden files and deleted files from locked devices? How to access the network logs and volatile information form mobile devices? These tasks are performed by the forensic investigators with the help of mobile device forensics tools. Extracting the information is not the only task here, the investigator must also prove that the evidence is untampered and chain of custody has been followed, to legally accept the information against the victim. [7] Chain of custody must be followed to maintain the integrity of the data which is to be documented and submitted in the court. Mobile devices have different operating system developed by different companies and the market is ever-growing where each company trying to release and update new cell-phones every month. Every vendor has their own proprietary format and technology used in their devices. It is practically not possible to design different forensic tools for every different mobile device.

Part I. Data Extraction Methods involved in Mobile Forensics

Operating system like android, being open source, is an advantage for the software developers; but, it is the biggest disadvantage for forensic analysts, as they have to craft and implement new methods for breaking into the device and performing forensic analysis. The methods of performing forensics analysis and data acquisitions on mobile devices are not constant. Investigators must adapt to new methods and change their approach each time they perform forensic investigation on mobile devices.[5]Important aspects of cell phones which are to be analyzed:

- Internal memory
- Sim card
- Memory card
- Network provider

Important data types which can be extracted from the forensic analysis of mobile devices are -
Text messages, contacts, history, photos, audio, video, GPS location, emails, memos, calendar, documents, web-history such as use of social media applications like Facebook, twitter, Instagram, WhatsApp etc. There are four methods, commonly used for extracting the information contained in the mobile devices. Depending on the type of case, the forensic analyst can adopt to just one or sometimes multiple methods of analysis of data. According to my research, I would suggest you to adopt logical as well as physical analysis as it are more exhaustive. A single method cannot extract all the required information and each different method of analysis can contribute in extracting different and vital information from the mobile devices. These methods are discussed below:

A. Screen Captures

Sometimes, this is the only option you are left with, while analyzing the phone. Even though this is the easiest way to extract the data as it requires minimum technical skills, this method is not comprehensive. Eclipse is the most popular tool in performing screen capturing of data from the mobile devices and calculates hash value for each image to prove the integrity of evidence in court. Eclipse uses SHA 1 algorithm to calculate the hash value. Advantage of this method is, the data directly extracted in the user readable format which avoids the necessity to convert it from raw format. The disadvantage associated with this method is that, it is very time consuming. Every tool designed to perform screen capture requires manual swiping of the screen and pushing the buttons to navigate through the device. This method extracts the info which is visible to the operating system. Hidden and deleted files and documents and the data from the file slack cannot be extracted.[13 7]

B. Logical Analysis

Most common and standard practice today, is the use of logical analysis in extraction of emails, text messages, call logs, contacts. This analysis extracts the information which can be seen and accessed by forensics analyst. Data is copied bit-by-bit from the mobile device using forensic tools which resides on the computer. It is easier to perform this type of analysis using tool, but this method is not as comprehensive as physical extraction, where a skilled forensic analyst can extract more information. The tools used to perform logical analysis cannot extract deleted and hidden data and cannot analyze the locked devices.[13]

C. Physical Analysis:

Undoubtedly, the most comprehensive method of data acquisition. In this method, data is directly accessed from the flash memories and helps us to extract deleted and hidden files, documents, images, videos, passwords etc. It is just like logical analysis which includes bit-by-bit copy of entire data but also includes hidden files and passwords. The tools provided by the vendors to perform such analysis have their own bootloaders to start the mobile and perform physical analysis and also maintaining the integrity by leaving the data untampered even after analyzing.[13]

D. Chip-Off and JTAG Analysis:

The Chip-Off and JTAG methods are increasingly gaining popularity because of capability of this method to by-pass complicated phone locks and drive encryption. Ultimately, the tool on which forensic analysis is performed will be provided with physical image of the memory chip from that mobile device. In Chip-Off method, the chip is removed or unmounted from the circuit board of the mobile device and testing and programming is done using JTAG (Joint Test Action Group). This method requires the knowledge of location of the chip and JTAG connectors in the device. Along with this, the person must have the knowledge of dismantling and repairing the hardware of the device. The main difference between Chip-Off and JTAG method is that, in the chip extracted during Chip-off analysis cannot be re-mounted again in the device unlike the JTAG where the connections can again be soldered. Hence, Chip-Off is normally used on damaged devices. This physical image is created by bit-by-bit copy of data stored on memory chip. There are many cases, where calculating a physical dump is not possible with physically extracting the storage chip. Today with such a fast growing pace of mobile devices, it is impossible to design a customized tool for every device, but the physical dump obtained from a memory chip can be analyzed in a similar way. Even though Chip-off and JTAG are complicated processes, due to their output obtaining capabilities, there use is on the rise.[3] Sometimes, forensic experts need to analyze mobile devices which are completely damaged in an accident or even sometimes the suspects damage it on purpose, in-order to destroy the evidence, during such time, this method can be very effective and where the above processes fail.

Part II. Areas of concern for Mobile Forensics

A. Loss of power:

Mobile devices have very low battery life and once discharged it leads to the loss of volatile data from the RAM. Even though you can charge the device using cables, the lost RAM data cannot be retrieved. Hence, data acquisition must be performed before the mobile is switched off. Mobile is constantly connected to the network which changes its data continuously. Switching the mobile phone is not an option, as it is has the same consequences of discharged phone.[5] Hence, it must be kept in containers which blocks it from the all the signals from communication medium and helps in maintaining the consistency and integrity of data.

B. Synchronization with Cloud:

Most of the devices support cloud storage which motivates the user to store their information on cloud. The problem while performing cloud investigations are the need of a separate search warrant. The data might have also been encrypted on the cloud which will again require the permission from the Cloud Service Provider (CSA). Data-duplication, jurisdiction and multi-tenancy in which separating the victims data from irrelevant data, for performing digital forensics, are three major tasks for the forensic investigator to perform forensic investigation on cloud storage.

C. Remote Wiping:

This is just a security feature in which the network administrator can remotely wipe the data, after being requested from the owner to do so. As the mobile thefts are on the rise, network providers support remote wiping of data so as to maintain the confidentiality of the data. Remote wiping can wipe data from specific folders, or perform factory reset, or delete every information from the mobile.[14]This feature is used by the victims to their advantage, so as to remotely wipe the data making it useless for the forensic analysts to gather evidence against the person accused. The victim can easily wipe his entire system data from the mobile phones which is confiscated. To avoid this, it is better to keep the mobile in airplane mode so as to isolate it from the network. Thus, we must isolate the mobile from signals so that remote wiping is avoided as it an evidence killer.

Part III. Challenges faced while performing Mobile Device Forensics

A. Variation in Technology:

Mobile devices such as smartphones are available in wide variety of vendor options, where each vendor offers different features and modifications in operating systems. Most commonly used operating systems are Android, Windows and iOS. Different tools must be used to perform forensic analysis on these OS's. Apart from the software part, the hardware configurations must also be taken into consideration. If we consider the statistics, there are more than forty iOS versions which are available commercially. These iOS spread across different six iPhones, five iPads and five iPod touch devices.[4] Android is currently the most popular OS as it is open source and is widely used across the globe. It is reported to have dominated to 82.8% of market share, whereas iOS contributed to 13.9% and 2.6% of windows. Due to these variations in technology it is difficult for the forensic investigator to follow standard procedures for investigations and must innovate his methods as per technology.[8]

B. Passwords and Encryptions to lock devices and files:

This is the biggest hindrance even before beginning the investigation on mobile devices. Most devices are locked with different passcodes or patterns or even fingerprint lock. Latest mobile phones like nexus 5X are already encrypted. The investigator must unlock the device to perform forensic investigation. Most easy and popular method used by the investigators is to ask the victim to give his/her password. This method is successful most of the time. But what if the victim is not present or denies to handover the password? Another method is to contact the manufacturer and ask him to unlock the device or to investigate the victim's friends, family or relatives. There are no laws or rules regarding the disclosure of the passwords or disk encryption keys to the forensic investigator to perform analysis and hence it is important for the investigator to have the knowledge of cryptography for decrypting the passwords and keys. A complex iPhone password is difficult to reveal and hence the investigator must know and insert it manually in-order to gain access and decrypt all the files. No mobile forensic tool exists that can decrypt the password, it can extract certain data but not encrypted files. Keychains are an integral part of encryption of passwords of iOS. The vault which contains the stored passwords is itself encrypted and using tools this password can be decrypted and eventually provide us the details of other passwords and accounts. Just like the iPhones, even android phones are locked but they normally contains pattern which is easy to guess or decrypt. Another option is to root the phone, but this may result in altering or deleting the files and debug mode must also be on to carry out this rooting operation and it takes expertise on the examiner's part. Even with the help of extraction tool, it should be possible to carve out the PIN lock on android. Chipsets and hardware vary from device to device and physical extraction may always not be possible.[4]

C. Forensic soundness and accurate data extraction:

Bootloaders are currently the most forensically sound physical extraction method. They replace the normal bootloader inbuilt in the device or just replace the initial program code with the bootloader code. Even though this method succeeds in extracting the content, few mobiles prevent the use of bootloader and thus we need to temporary root the system. The main advantage of bootloader is that they are not restricted any particular OS or vendor, they are generic in nature and can be used on multiple platforms. Temporary rooting of device does not transfer the administrative rights to the person, but it enables the access of operating system and we can used ADB (Android Debug Bridge) debugger and image the devices flash memory so as to perform full physical extraction.[4] Temporary rooting is not a forensically sound method as compared to the bootloader and hence we must document each step for showing the integrity of data extracted from the device.

D. Unsupported Extraction Methods:

What action does a forensic investigator perform, when he needs to investigate a mobile device which is locked and which is unsupported by mobile forensic tools? At such time three common methods are used: JTAG, Flasher box or chip-off extraction method. All these methods are based on physical extraction. For example the chip-off extraction method can be used to retrieve files from the locked iPhone, but the files are obtained in the encrypted form, which are not of much use. The use of these extraction method require a proficient investigator as these tools can be destructive if the investigator is untrained on how to use them. The JTAG and flasher-box methods are device specific. Physical removal of the residual data from the memory chip is done using the chip-off method.[5]

E. Anti- Forensic Skills

Person involved in cyber-security crimes is usually very smart and takes various precautionary measures for hiding the secret data, so that in-case of investigation it will be difficult or impossible for the investigator to extract any evidence against the suspect. This includes data obfuscation; where the suspect hides the original data with some random characters, which is also known as data masking. Another way is using data forgery where the original data is disguised as some other object so as to deceive the investigator. Another technique is data hiding, which can be done using several techniques.[10]The forensic investigator and even the tool used for performing forensic analysis, must be capable of overcoming the anti-forensic barrier.

F. Communication Shielding

Mobile devices continuously communicate over the network using various mediums such as;

Bluetooth, Wi-Fi, Cellular networks and Infrared. This can change the data present in the device and sometimes over-write the evidence leading to loss of integrity.[10]Even remote-wiping is possible if the device is exposed to communication medium and hence the device must be isolated by keeping in forensic faraday bag.

G. Malicious Programs

A very common challenge experienced by the investigator is the analysis of device containing malicious program or malicious software such as virus, worms or Trojan horse.[10]This problem can be more severe if the device containing malware connected to forensic workstation gets infected with it. Furthermore, these malicious programs alter the content of evidence again causing the problem of integrity of content.

As discussed above, there are many different challenges faced during mobile device forensic investigations. When one problem is solved, the next one arises. But the investigators must be on their toes to tackle these problems. Different methods to perform investigations evolve over the years with the research of professionals in these fields. Few methods involve understanding the operating systems its software and discover new vulnerabilities which could be exploited to grant the user privileges for the investigator. Few methods involves reverse-engineering the hardware and software so as to find out the vulnerabilities in applications and encryption of the files which can be decrypted.

Part IV. Different types of forensic tools and their performance, implementation and behavior:

A. Tools:

If the device is device is obtained in the unlocked state, then you must enable the USB debugging options. This can be done by going to Settings>About Phone>Software details> Click 7 times on the Model Number to activate the Debugging mode. When the device is connected via USB, there is a developer option at the bottom of Settings menu. Activate the USB debugging to perform forensic analysis using Mobile Forensic tools. The Developer option contains many option such as, Stay Awake which will prevent the screen from timeout, it will take a bug report. You can also enable the HCI snoop log and obtain geeky stats about running processes.

1. MOBILedit! Enterprise –

One of the most popular tool for conducting mobile device forensics as its cross platform solutions supports almost all phones. No doubt, you must update it regularly as it installs the packages which covers latest updates on android, iOS and newly launched mobile phones.[9]

When you connect the device to your laptop suing USB cable, it will first ask for verification of the RSA key which must be the same appearing on both the tool and the mobile. Even after disconnecting the USB, it can still perform the analysis because the backup of information is created. The screenshot option performs screen capture analysis of the entire device with the help of manual swiping.

Characteristics:

Absolute Extraction of Data from Phones and Sim Cards:

- Retrieve deleted data and detour/circumvent PIN, passcode and phone backup encryption.
- Collects data which includes- raw application data, phonebook, text messages, call history, multimedia messages, calendars, memo and reminders.
- Phone information such as operating systems, SIM details, IMEI and local area information.[9]

Support for Almost All Phones:

- Operating systems like Windows Phone, Android, iPhone, Blackberry, Symbian, Chinese phones and CDMA phones.[9]

Additional Utilities:

- It can extract data from applications such as WhatsApp, Evernote, Skype, Dropbox etc and even deleted data from applications.
- It can bypass the iOS passcode and direct us to retrieve all the data files when the mobile is connected to computer even if the iOS is locked.
- Live logical acquisition can be performed on iPhone even without knowing the encryption code.[9]
- Extract the list of contacts through Skype, Gmail or Facebook accounts even without knowing the passwords.

Displays detailed Phone information about the hardware and software present:

- Picture of Phone, Name, Manufacture and Model
- IMEI, Network Operator, Connection Type, Hardware and Software revision.
- Also displays signal strength and battery status.

Report Generator for Forensic Investigator:

- Creates and translates reports into your regional language.
- Print reports ready for courtroom and back-up reports
- Measure the integrity of messages using MD5 and SHA-512 hash.

2. OXYGEN MOBILE FORENSIC TOOL

The Oxygen Forensic Suite consists of four versions, all of them are similar but with little different functionality, to assist the forensic analyst in providing the needed data focused on particular issues such as:

- Oxygen Forensic Analyst in analyzing the mobile device

- Oxygen Forensic Detective in extracting the data from multiple sources.
- Oxygen Forensic Extractor in providing time-proven forensic acquisition.
- Oxygen Forensic Cloud Extractor especially for the resolving the issues regarding the storage of data on the clouds such as Apple, Google, Microsoft etc.

The performance of each tool in the suite is explained below along with its characteristics.[12]

Oxygen Forensic Analyst:

- Supports wide range of devices for performing analysis, can import device backups and extract deleted data and find hidden files. The data which is collected can be documented in the form of reports containing hash values of data collected to prove its integrity and can export file in various formats such as pdf, xml, xls, rtf etc. Large amount of data can be analyzed effectively using graphs, timelines and pie charts etc. Rooting of data provides super-user privilege and better data acquisition which can be performed using oxygen forensic analyst.[12]

Oxygen Forensic Detective:

- It can be considered as a more advanced version of Oxygen Forensic Analyst with additional capabilities such as extracting the passwords or pin-codes of encrypted mobile phones and backups, it can disable the screen-locks and import data stored on the cloud. The locations of the user can be found out using GPS system.[12]

Oxygen Forensic Extractor:

- The tool was specially designed to perform time-proven analysis and collects only common device information such as emails, mms, messages, photos, audio, video etc. It also calculates missed call information and contacts of the user device, and Wi-Fi and account passwords of the user.[12]

Oxygen Forensic Cloud Extractor:

- Many users store their data on cloud due to limitations of physical memory and hence it is important to analyze the data from cloud. This tool analyzes the data from various cloud manufacturers and extracts the details of the user account such as ID and password used to access cloud. Documentation after extracting the relevant data from the cloud is also done by this tool.[12]

After connecting the device using USB cable, it will first display the hardware and software information about the device which is important and must be documented as proof during legal proceedings. The next window will ask for case information such as investigator name, case number and even the type of hash algorithm which can be used such as MD5 or SHA1. The next window consists of two options such as recommended or advanced to perform the forensic analysis. After choosing the recommended option, the next window as displayed above will ask for more details about the forensic analysis to be performed such as logical extraction>parse user data> OFB backup. In Forensic Extractor, you cannot use the physical dump method as the device is not rooted. To use the physical dump method you can analyze the device using Oxygen Forensic Detective tool, where temporary rooting can be performed. The next window consist of the type of data which is to be collected such as calendar, event logs, images, audio, video, documents, messages, phonebook etc. As per the time and requirement of case, the necessary information can be extracted.[12]

To extract the above data, it takes about an hour and more. Once the data is extracted, parsed and then hashed the next window will ask for the creation of reports and the different formats such as xml, xls, pdf, doc etc in which the report is to be produced.

Thus Oxygen Forensic Suite is one of the best and the most comprehensive tool in performing Forensic Analysis on devices.

3. ENCASE MOBILE FORENSIC TOOL

EnCase Mobile Forensic Tool has an edge over its competitors in terms of speed and the power in performing disk level forensic analysis. It is the fastest tool to extract data and provides an additional feature where the investigator can perform simultaneous analysis of collected data which increases the productivity.

Strengths: Reliable and embraced by law enforcement agency as a comprehensive mobile forensic tool.

Weakness: Precarious or Perilous when operated in network environment which already contains several different products such as CodeMeter Dongles running on its server.

It operates in read-only mode to avoid over writing of vital data and can wipe or restore the drives as per requirement. Relevant information depending on the case can be bookmarked and then printed in the report with md5 or CRC hash value methods. The location of the user can be calculated by exporting the geo-tags located in the google maps application in the cell-phone.[6]

The new evidence processor of the EnCase tool can perform automated tasks for the investigator such as indexing. For comprehensively analyzing the data within the files, EnCase provides us with variety searching options such as

- Boolean
- Word Searches
- Conditional
- GREP

It provides us with important information regarding the metadata such as; the data of originated data, the type of activity of the user which led to the creation of data and the last date when the data was accessed. The analysis of data is done is advanced methodology, which helps in the recovery of deleted data, recovery of partitions and files, hash analysis and even analyze the files within unallocated disk space or compounded files. Prioritized searching is the unique feature of EnCase forensics and helps in quicker analyzing of files and content. Various options are provided such as search entry slack, skip content of known files, undeleted entries before searching and using initialized size.

B. Evaluation of Mobile Device Forensic Tools

The characteristics of almost all the tools involved in performing mobile device forensics are similar in some aspects. Depending on the type of information to be retrieved we can use different tools. Evaluation of these tools is important in finding the best amongst the rest. It is also a process involved to find out whether the tool behaves appropriately in desired circumstances and meet the requirements for performing forensic analysis. Given below is a concise model which represents mobile device forensics.[11 15]

Mobile Device Forensic tools must accommodate the following requirements.[1]

1. Comprehensive: The tool must provide the forensic investigator, an access to all the data from the device including the deleted files and the files from the partition gaps.
2. Usability: The tool must be user friendly and should not overwhelm the investigator by data which is extracted.
3. Accuracy: The content must be displayed in court to prove the guilt of the accused and hence integrity must be maintained and accurate data must be extracted along with the hash values for each file.
4. Read only: The tool should use write block software and must operate in read only mode to preserve the integrity of content and maintain the chain of custody.
5. Deterministic: Every time an input is provided, the output obtained must be same, and in short consistency must be maintained.
6. Verifiable: To ensure the integrity of the content, verification of result must be performed manually or using any third party tools.

4. CONCLUSION

Mobile device forensic is an evolving field and its demand will continue to rise in future. Working in this field requires continuous study of new tools and concepts. It is important for the forensic analyst to understand traditional tools and new tools and data extraction methods, in-order to use them appropriately according to the situation. Each mobile forensic case requires different implementation of mobile device forensic knowledge, to extract the vital data, hidden or deleted from the mobile phones. Thus, it is important to know the features of different tools and there advantages and limitations. The following table consists of three different tools and the different properties they possess. Comparing helps in determining a better tool and in this case, its EnCase mobile forensic tool.

Table 1: Comparison of properties of different Mobile Device Forensic Tools [15]

Tools and Properties	MOBILedit	Oxygen Suite	EnCase
Data Carving	No	No	Yes
Bookmarking	No	Yes	Yes
Parsing Physical Acquisition	No	Yes	Yes
Windows Registry Viewer	No	No	Yes
SHA 1-256	No	Yes	Yes
CRC	No	No	Yes
Data Comparison	No	No	Yes
Boolean Search Function	No	No	Yes
PDF Report Format	No	Yes	Yes
GPS Point Mapping	No	No	Yes
File Sorting	No	Yes	Yes
Physical Data Dump	Yes	No	Yes
Deleted Data Recovery	Yes	Yes	Yes
TXT Report Format	Yes	No	Yes
Built-in hex Viewer	Yes	Yes	Yes

REFERENCES

[1] Carrier, Brian. Defining digital forensic examination and analysis tools using abstraction layers. International Journal of digital evidence, vol. 1, no. 4, pp. 1–12. 2003. http://digital4nzics.com/Student%20Library/Defining%20Digital%20Forensic%20Examination%20and%20Analysis%20Tools%20Using%20Abstraction%20Layers.pdf (accessed November 13, 2015).

[2] Eclipse CFI – Nothing Left Behind-Eclipse Video Screen Capture Tool. 2015. http://www.cfi.co.th /eclipse.html (accessed November 24, 2015)

[3] Elder, Bob. Chip-Off and JTAG Analysis-Evidence technology magazine. 2008. http://www.evidence magazine.com/index.php?option=com_content&task=view&id=922(accessed 13 November, 2015)

[4] Engler Ronen, Miller Christa, 2013. 6 Persistent Challenges with Smartphone Forensics. August 2. http://www.forensicmag.com/articles/2013/02/6-persistent-challenges-smartphone-forensics (accessed Nov 6, 15)

[5] Gonzalez, Jason. Bloomberg Law Reports Mobile Device Forensics - A brave new world?2 011.h tt p : //www.strozfriedberg.com/files/Publication/224ca0f8-5101-4e1b-938a-4d4b 12 8ad 5ed/Presentation/ Pu bli ca tion Attachment/ef4a28ad-ff7d-4014-aea8-80505 789b 86c /Mobile%20Device%20Forensics _%20A% 20Brave%20New%20World.pdf.(accessed November 15, 2015)

[6] Guidance Software EnCase Forensic v7- Guidance Software. 2015. https:// www2.guidance soft ware.co m/products/Pages/EnCase-Forensic/Triage.aspx (Accessed Nov. 5, 2015)

[7] Kessler, Michael. Cell Phone Forensics-Digital Forensics Investigation. 2015. http://investigation.com/services/digital-forensics/cell-phone-forensics/ (accessed Nov. 20, 2015)

[8] Llamas, Ramon. Smartphone OS market share-IDC Analyze the Future. 2015. http://www.idc.com/prodserv/ smartphone-os-market-share.jsp (accessed October 28, 2015)

[9] Mobiledit - Mobile Device Forensics. 2015. http://www.mobiledit.com/forensic (accessed October 26, 2015)

[10] Murphy, Cynthia. Cellular Phone Evidence Data Extraction and Documentation. Retrieved 4 August 2013.http://neelain.edu.sd/assets/magazines/pdf/3 /10/7.pdf (accessed November 15, 2015)

[11] Kubi, Appiah. Evaluation of UFED Physical Pro 1.1.3.8 and XRY 5.0: Tools for Extractinge-Evidence from Mobile Device. 2010.http ://link.springer .com/chapter/ 10.1007%2F978-3-642-39891-9_17#page-1. (accessed November 7, 2015)

[12] Oxygen Forensic-Smart Forensic for Smart Phones. 2015. http://www.oxygen-forensics.com/en/ (accessed November 25, 2015).

[13] Rosenthal, Bryan. Cell on Earth: The Forensics Challenges of Mobile Devices. 2015. http://www.srr.com/article/cell-earth-forensicchallenges-mobile-devices. (accessed November 24, 2015)

[14] Rouse, Margaret. Remote wipe definition - Tech Target Search Mobile Computing. 2013.http://search mobilecomputing.techtarget.com/definition/remote-wipe.(accessed November 7, 2015)

[15] Shahzad, Saleem. Academia - Evaluating and Comparing Tools for Mobile Device Forensic. 2015.http://www .ac ade mia.edu/ 4697424/ Evaluating _and_Comparing_Tools_for_Mobile_Device_Forensics_ using_Quantitative_Analysis.