ISSN:0975-9646

The Forensic Process Analysis of Mobile Device

Dasari Manendra Sai[1], Nandagiri R G K Prasad[2], Satish Dekka, [3]

[1]*Assoc. Professor, Sai Ganapathi Engineering College, Visakhapatnam*
[2,3]*Asst. Professor, Sai Ganapathi Engineering College, Visakhapatnam*

Abstract:As mobile devices grow in popularity and ubiquity in everyday life, they are often involved in digital crimes and digital investigation as well. The world of mobile device forensics is a complicated one. Unlike the PC world's limited number of major operating system vendors, there are countless manufacturers of mobile devices. To complicate things further, each mobile device manufacturer may have his own proprietary technology and formats. Add to this the blistering pace at which new mobile devices such as cellular phones and personal digital assistants (PDAs) are released, and you have a challenging environment to work in. This research paper will document in detail the methodology used to examine mobile electronic devices for the data critical to security investigations. The methodology encompasses the tools, techniques and procedures needed to gather data from a variety of common devices.

Keywords: Mobile Phone Forensics, Handheld devices, Evidence, Analysis

I. INTRODUCTION:

As Mobile Device use becomes more widespread, Mobile Device forensics becomes more and more important as Mobile Devices are often found in crime scenes. Forensics is used in all types of situations from internally in a corporate auditing case to a criminal investigation case commonly seen in the law enforcement world. Many crimes and other misconducts make forensics very important as a means of making the world a better place.

Digital forensics is becoming important because our society is becoming more dependent of various computers and telecommunication tools and technologies. Mobile Device forensics, being part of digital forensics, aims at the retrieval or gathering of data and evidence from mobile phones and similar devices used in daily life. Mobile Device forensics allows investigators to answer questions of interest on a certain subject related to Mobile Device based communication. It is based on proven scientific methodology and norms to collect facts regarding an object, an event, or an artifact in certain time period to determine whether the object was in fact what it claims to be or is alleged as being. In these efforts of forensics, Mobile Device forensic specialists have encountered major challenges that hinder their work. As we know mobile devices are becoming the main mobile computing power with all its constant upgrades, changed, and new additions, this has caused the forensic specialists to undergo a lack in available Forensic tools for retrieval that is compatible with today's uprising of newer model devices.

The main difference between Mobile Device forensics and computer forensics is that in Mobile Device forensics, one has to deal with multiple different hardware and software standards, which makes creating a universal standard tool near to impossible. Since the software is embedded and more special purpose than computers, solutions for obtaining data are non-standardized thus causing a need for vast solutions. With the advent of new phones coming into the market at an exponential rate, as well as new companies coming into the market using a whole different blend of proprietary software, the problem has been even more compounded as time progresses. The purpose of a Mobile Device forensic tool is to obtain data from a Mobile Device without modifying the data. The tool should provide critical updates in time to keep pace of the rapid changes of Mobile Device hardware and software. The tools can be either forensic or non-forensic, which each of them providing different challenges as well as allowing for different solutions.

Forensic tools are tools that are designed primarily for uncovering data from Mobile Devices, while non-forensic tools are not designed for uncovering data but can be manipulated for that purpose. Two different methodologies have been used to address this situation, either reduce the latency period between the introduction of the phone and the time the Mobile Device forensic software is available for that phone or create a baseline to determine the effectiveness of a tool on a certain device. The first method is to reduce the latency period between the time a Mobile Device gets on the market and the availability of the tools and this is primarily done by adding a new layer called a phone manager protocol filtering, which sits at a higher abstraction level between the programming interface and the library, thus in a way achieving a kind of program data independence. The value of this method is increased by the fact that most phone managers use the Windows operating system. The main approach for this method is to obtain a phone manager and modify it so dangerous "write" commands cannot be issued, i.e. forensic scientists will not accidentally write data onto a suspect phone and thus compromise or jeopardize a case. This modification to the phone manager is done by a program called a filter. This filter will not only block dangerous write commands, but also will intercept data from the target phone in binary form and then send it to the phone manager for further decoding. The second method is to provide a baseline or test data to evaluate forensic tools. With this method, the user populates the phone with certain data and then attempts to retrieve it with a forensic tool. Thus the baseline is the original data that is populated on the telephone. The baseline is usually set up by Identity Module Programming (IMP).

The data that is obtained by the forensic tool from the Mobile Device is tested against the baseline and therefore one can determine what the effectiveness of the Mobile Device forensic tool is. The major identity module that is used today is called the Subscriber Identity Module or SIM card which is used to separate the personal information from the actual mobile device as well as hold onto phone numbers, names and network settings and allows for the portability between phones. The SIM card is broken up into a file system organization with root directory file subdivided into multiple directory files (DF) that contain the elementary files (EF) which holds the binary data. Thus creates another problem as the data that needs to be obtained could be contained anywhere in the elementary files. In order to insert the test data onto the SIM card an IMP (Identity Module Programmer) needs to be inserted and then it will be allowed to write test EF.

II. Literature survey on mobile forensics

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

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

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

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

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

Logical acquisitions of mobile devices are much more common than physical acquisitions. Logical acquisitions recover the files and directories of a drive; information such as call records, text messages and contact lists, this type of acquisition cannot recover deleted files. Many mobile phones come with security software such as passwords, biometrics, or pattern locks so the individual can protect the data within the phone. This can cause issues for investigators if these measures are allowed to activate. One such way these security measures can be activated is due to power depletion.

Due to the nature of investigations on a mobile phone, an exact forensically sound reproduction may not be possible. This issue requires investigators to take special care in documenting all the steps taken during the search of the device. It is important that this recovery is done under forensically sound conditions. There are a number of items that must be kept in mind when dealing with mobile forensics.

2.1 Data acquisition

Usually you will be forced to acquire data from a powered-on system, as there might be no way to take images, as interfaces (hardware/software) to access internal device memory may be missing on purpose. Take care to acquire data from memory extensions (such as SD Cards) as they may contain valuable information for investigation purposes.

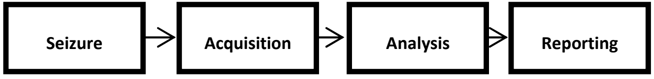
2.2 Chain of custody

Establishing and maintaining the chain of custody (CoC) and maintaining integrity on the mobile device can prove quite difficult when dealing with mobile devices. Most available forensic tools require the investigator to install an application to the system to be analyzed. Additionally, there is no way to physically make file systems read-only. Investigating the device in a test environment might be recognized by malware and lead to evidence loss. Acquiring evidence from mobile devices may therefore taint the integrity of the evidence rendering it non admittable for trials.

III. Methodology

Mobile forensics is the process to analyses the mobile phone to detect and collect the evidences related to the crime. A method is proposed to analyze the mobile phone to detect crime, main focus of the method is to analyze mobile phone internal and external memory and SIM card. Mobile forensic process of mobile devices

There are four phases in mobile forensic process:-



Seizure:

Prior to the actual examination digital media will be seized. In criminal cases this will often be performed by law enforcement personnel trained as technicians to ensure the preservation of evidence. In civil matters it will usually be a company officer, often untrained. Various laws cover the seizure of material. In criminal matters law related to search warrants is applicable. In civil proceedings the assumption is that a company is able to investigate their own equipment without a warrant, so long as the privacy and human rights of employees are observed.

This phase is very important in digital forensics; It Collects the digital evidence provided in the mobile device. In this phase the investigator preserve the device in its original stage. As in this phase the cell phones are seized that are involved in the activity, so that there should not be any change in the evidences. Seize the mobile device means to cut off all the wireless networks. Any failure in this stage will result in the failure of all the rest stages. The goal of seizure is to preserve the evidence as it avoidsshut down the device.

Acquisition:

Once exhibits have been seized an exactsectorlevelduplicate of the media is created, usually via a write blocking device, a process referred to as ImagingorAcquisition.The duplicate is created using a hard-drive duplicator or software imaging tools such asDCFLdd,IXimager,Guymager, TrueBack,EnCase. The original drive is then returned to secure storage to prevent tampering.

The acquired image is verified by using the SHA-1 or MD5 hash functions. At critical points throughout the analysis, the media is verified again, known as "hashing", to ensure that the evidence is still in its original state.

The second phase is acquisition phase after the preservation on the device is done.This phase chooses a right method and approach for analysis phase and the phase starts when the device is received at the forensic lab. In this phase the model and type of device is identified. After this the right tool for the acquisition is to be choose as this is very difficult because there are many no of devices in the market.

Analysis:

After acquisition the contents of (the HDD) image files are analysed to identify evidence that either supports or contradicts a hypothesis or for signs of tampering (to hide data).

During the analysis an investigator usually recovers evidence material using a number of different methodologies (and tools), often beginning with recovery of deleted material. Examiners use specialist tools (EnCase, ILOOKIX, FTK, etc.) to aid with viewing and recovering data. The type of data recovered varies depending on the investigation; but examples include email, chat logs, images, internet history or documents. The data can be recovered from accessible disk space, deleted (unallocated) space or from within operating system cache files.

Various types of techniques are used to recover evidence, usually involving some form of keyword searching within the acquired image file; either to identify matches to relevant phrases or to parse out known file types. Certain files (such as graphic images) have a specific set of bytes which identify the start and end of a file, if identified a deleted file can be reconstructed. Many forensic tools use hash signatures to identify notable files or to exclude known (benign) ones; acquired data is hashed and compared to pre-compiled lists such as the Reference Data Set (RDS) from the National Software Reference Library

On most media types including standard magnetic hard disks, once data has been securely deleted it can never be recovered. SSD Drives are specifically of interest from a forensics viewpoint, because even after a secure-erase operation some of the data that was intended to be secure-erased persists on the drive.

Once evidence is recovered the information is analysed to reconstruct events or actions and to reach conclusions, work that can often be performed by less specialist staff. Digital investigators, particularly in criminal investigations, have to ensure that conclusions are based upon data and their own expert knowledge.

Reporting:

Presentation phase shows the result of the analysis phase. The forensic examiner should know the expectations of the audience as different audience have different expectations. As when investigator come to know about the expectations of the audience it is easy for him to prepare the presentation. Whatever data is collected is presented in the presentation phase.

When an investigation is completed the information is often reported in a form suitable for non-technical individuals. Reports may also include audit information and other meta-documentation.

When completed reports are usually passed to those commissioning the investigation, such as law enforcement (for criminal cases) or the employing company (in civil cases), who will then decide whether to use the evidence in court. Generally, for a criminal court, the report package will consist of a written expert conclusion of the evidence as well as the evidence itself.

IV. MOBILE FORENSIC CHALLENGES:

One of the biggest forensic challenges when it comes to the mobile platform is the fact that data can be accessed, stored, and synchronized across multiple devices. As the data is volatile and can be quickly transformed or deleted remotely, more effort is required for the preservation of this data. Mobile forensics is different from computer forensics and presents unique challenges to forensic examiners.

Law enforcement and forensic examiners often struggle to obtain digital evidence from mobile devices. The following are some of the reasons:

- **Hardware differences**: The market is flooded with different models of mobile phones from different manufacturers. Forensic examiners may come across different types of mobile models, which differ in size, hardware, features, and operating system. Also, with a short product development cycle, new models emerge very frequently. As the mobile landscape is changing each passing day, it is critical for the examiner to adapt to all the challenges and remain updated on mobile device forensic techniques.

- **Mobile platform security features**: Modern mobile platforms contain built-in security features to protect user data and privacy. These features act as a hurdle during the forensic acquisition and examination. For example, modern mobile devices come with default encryption mechanisms from the hardware layer to the software layer. The examiner might need to break through these encryption mechanisms to extract data from the devices.
- **Lack of resources**: As mentioned earlier, with the growing number of mobile phones, the tools required by a forensic examiner would also increase. Forensic acquisition accessories, such as USB cables, batteries, and chargers for different mobile phones, have to be maintained in order to acquire those devices.
- **Anti-forensic techniques**: Anti-forensic techniques, such as data hiding, data obfuscation, data forgery, and secure wiping, make investigations on digital media more difficult.
- **Dynamic nature of evidence**: Digital evidence may be easily altered either intentionally or unintentionally. For example, browsing an application on the phone might alter the data stored by that application on the device.
- **Accidental reset**: Mobile phones provide features to reset everything. Resetting the device accidentally while examining may result in the loss of data.
- **Device alteration**: The possible ways to alter devices may range from moving application data, renaming files, and modifying the manufacturer's operating system. In this case, the expertise of the suspect should be taken into account.
- **Passcode recovery**: If the device is protected with a passcode, the forensic examiner needs to gain access to the device without damaging the data on the device.
- **Communication shielding**: Mobile devices communicate over cellular networks, Wi-Fi networks, Bluetooth, and Infrared. As device communication might alter the device data, the possibility of further communication should be eliminated after seizing the device.
- **Lack of availability of tools**: There is a wide range of mobile devices. A single tool may not support all the devices or perform all the necessary functions, so a combination of tools needs to be used. Choosing the right tool for a particular phone might be difficult.
- **Malicious programs**: The device might contain malicious software or malware, such as a virus or a Trojan. Such malicious programs may attempt to spread over other devices over either a wired interface or a wireless one.
- **Legal issues**: Mobile devices might be involved in crimes, which can cross geographical boundaries. In order to tackle these multijurisdictional issues, the forensic examiner should be aware of the nature of the crime and the regional laws.

CONCLUSION:

With the growing demand for examination of cellular phones and other mobile devices, a need has also developed for the development of process guidelines for the examination of these devices. While the specific details of the examination of each device may differ, the adoption of consistent examination processes will assist the examiner in ensuring that the evidence extracted from each phone is well documented and that the results are repeatable and defensible in court. The information in this document is intended to be used as a guide for forensic examiners and digital investigators in the development of processes that fit the needs of their workplace.

FUTURE SCOPE:

Future scope of mobile phone forensic technique to analyze various file systems used in mobile phones e.g. Android, Windows mobile, IOS etc. That may be very helpful to detect crimes and to collect evidences.

REFERENCES:

[1] R. Ayers, W. Jansen, L. Moenner, and A. Delaitre, CellPhone Forensic Tools: An Overview and Analysisupdate, NISTIR 7387, 2007.

[2] J. Bates, Fundamentals of computer forensics,Information Security Technical Report, Elsevier, 1998.

[3] B. Carrier, Performing an autopsy examination on FFSand EXT2FS partition images: An introduction toTCTUTILs and the Autopsy Forensic Browser, Proc.SANSFIRE 2001 Conference, 2001.

[4] E. Casey, (ed.) Handbook of Digital Forensics andInvestigation, Academic Press, 2010.

[5] S. Conder and L. Darcey. Android Wireless ApplicationDevelopment, Addison Wesley, 2009.

[6] L. Garber, Computer Forensics: High-Tech LawEnforcement, IEEE Computer, 34 (1) (2001), 202-205.

[7] S. Garfinkel, Digital Forensics Research: The Next 10Years, Digital Investigation, 7 (2010), S64-S73.

[8] Garner, "Sales of Mobile Devices in Second Quarter of2011 Grew 16.5 Percent Year-on-Year; SmartphoneSales Grew 74 Percent," Gartner, Inc., August 11, 2011.

[9] J. Halderman, S. Schoen, A. Heninger, and E. Felten,Lest We Remember - Cold Boot Attacks on EncryptionKeys, Proc. 17th USENIX Security Symposium, 2008.

[10] N. Al Mutawa, I. Baggili, A. Marrington,"Forensic analysis of socialnetworking applications on mobile devices", Digital Investigation,Volume 9, Pages S24-S33, August 2012.

[11] J. Park, H. Chung, S. Lee," Forensic analysis techniques forfragmented flash memory pages in Smartphone", Digital Investigation,Volume 9, Issue 2, Pages 109-118, November 2012.

[12] A. Zareen, & S. Baig,." Mobile Phone Forensics Challenges, Analysisand Tools Classification".Fifth International Workshop on SystematicApproaches to Digital Forensic Engineering (SADFE.2010), (pp. 47 – 55),2010.

[13] S. Raghav, & A. K. Saxena," Mobile Forensics: Guidelines andChallenges in Data Preservation and Acquisition". IEEE studentConference on Research and Development, (pp. 5-8), Malaysia, 2009.

[14] W. Jansen, R. Ayers,: "Guidelines on Cell Phone Forensics "Recommendations of the National Institute of Standards andTechnology, 2007