Mobile Phone Forensics
Challenges and Tools Classification: A Review

Ms. Mohini N. Umale, Prof. A. B. Deshmukh, Prof. M. D. Tambhakhe

Abstract— now every day billions of individuals use mobile phones in their daily activities, and generally, those activities could be criminal in nature. The exceptional advancements within the technology and increase in computing power of those devices over the previous few years, has junction rectifier to a rise of their practicality whereas keeping the dimensions of such devices sufficiently small to suit in a very pocket. The employment of mobile phones in criminal activities has junction rectifier to the necessity of sick the info in them. The acquisition of knowledge derived from cellular devices is often used as rhetorical proof that has become a main element of crime scene investigations. There square measure many common obstacles that lie before any mobile rhetorical skilled.

Keywords— *Mobile phone forensics, Smart phone, Data protection, forensic soundness, smart phone extraction, tools.*

*****

I. Introduction

A great variety of the mobile phones used worldwide need special data and skills from rhetorical consultants. More often, it's not enough to be associate degree older knowledgeable in pc forensics to know all the peculiarities and difficulties of mobile forensics. Smartphone's, the foremost well-liked mobile communications devices these days, also are a number of the foremost tough to extract evidentiary knowledge from Mobile rhetorical includes the strategies that show however evidences area unit taken from mobile phones. It's the science of convalescent digital proof from a mobile underneath forensically sound conditions exploitation accepted strategies. It includes analysis of each SIM and Phone Memory. Mobile phones have the similar potential of holding proof as the other digital media will. Phenomena of convalescent deleted data from mobile area unit similar because it may be finished a tough drive. Like all alternative digital media, evidence items contained in mobile phones area unit fragile and might simply be deleted or may be overwritten. Main aim for carrying analysis within the field of mobile forensics is to extract helpful data from these devices and gift it as proof in court of law. One should be ready before making an attempt to look at knowledge on a mobile device. Mobile device forensics needs data of the technology and knowing the tools and their limitations of processes is should exploitation multiple tools and confirmatory the results manually will facilitate. Non-forensic tools area unit less effective whereas the rhetorical tools give wide varied results. A rhetorical examiner should be clear concerning what's nonheritable and the way it's to be nonheritable [1]. Whereas several industrial rhetorical tools have created nice strides in supporting knowledge extraction, decoding, and analysis from iOS, Android, and BlackBerry devices, some challenges stay.

II. Related Work

Mobile Phone Forensics

As standard of living and business moves at the speed of electrons through the air, most civil and criminal investigations involve some kind of digital part. As mobile phones become thus omnipresent and play such an oversized social group role, there's a high chance that these same devices are going to be a part of those investigations. There are four ways that within which a mobile are often tied to crime:

- It is often used as a communication tool within the Process of committing a criminal offense.
- It is often a device providing proof of a crime.
- It will contain victim data.
- It is often a way of committing a criminal offense.

Today's criminal investigators should be conversant in mobiles and perceive the intricacies of mobile phone forensics. In alternative words, deed and analyzing the information on the device, hooked up SIM cards, and inclusive memory cards. These procedures are well documented and will be adhered to within the forensics acquisition and Analysis of mobile knowledge. But documented, it's acknowledge that there's presently nobody examination facilitation tool (hardware or software) that's universally used or suggested to get rid of the information from every and each mobile. Mobile phones will yield associate degree abundance of data. The foremost obvious styles of knowledge that may be retrieved from a phone are decision logs, contact lists, and text messages. However, in associate degree investigation, alternative options of a contemporary mobile, like ring tones, T9 dictionaries, canned responses, video files, still image files, calendar events, miscellaneous documents and knowledge files, and placement data can even offer valuable clues. Given the range of kinds of data accessible, it's imperative to look at each single one with utmost preciseness, particularly since it's

entirely potential, with the employment of specialized tools, too typically recover deleted data [2, 3].

Current Challenges

1. A Smartphone is never just a smart phone

Vendors and operational systems will vary wide, notably with robot, however conjointly even at intervals iOS and BlackBerry user teams. quite forty iOS versions are commercially offered, and are unfold among six totally different iPhones, five iPads, and 5 iPod bit devices. Unlike iPhone users, it's uncommon for robot users to upgrade their operational systems. It's conjointly out of the question to upgrade from simply any version.

2. Data protection: passwords and encryption

Not solely will information storage vary from device to device and OS to OS, however devices may additionally be pass code-protected or encrypted. Obviously, it's straightforward to extract information from a sensible phone with no pass code. A mobile information extraction tool ought to be able to reveal a straightforward pass code mechanically for all devices. Following the pass code extraction method, it'll be doable to extract and rewrite all information together with protected files. Android devices can even be user-locked. Not like iPhones, they usually use a pattern lock that is often not advanced. Bypassing the pattern lock altogether is perfect. A classification system or physical extraction, once decoded, can offer the proper pattern or PIN code accustomed lock the device. as an alternative, if decryption is unsupported inside the extraction tool, it ought to be doable to carve the PIN lock. Following a physical extraction, a classification system extraction exploitation the pattern lock and ADB mode ought to be doable. However, not all physical extractions from each robot are supported for decryption. That's as a result of chipsets and hardware will vary from device to device, that affects whether or not a rhetorical tool will reconstruct the classification system.

3. Prepaid "burner" phones

Prepaid phones are a tangle for a few times, and still be a tangle for enforcement specially. That's as a result of the disabled information port on these devices cannot be enabled, and vendors don't build the devices APIs—the traditional mode by that logical and classification system extractions square measure completed—available to industrial rhetorical extraction tools developers. Classification system extractions have the twin advantage of creating additional data—including some deleted data—available quickly. However, as a result of it extracts solely information from allotted house on a device's memory, it still remains restricted in some ways that. It conjointly needs a better degree of experience on the examiner's half as a result of it needs decryption.

4. There's no app for that

Apps, not simply accessible for iPhone or automaton however conjointly through device vendors like Samsung, Nokia, and LG—as well as from mobile carriers like T-Mobile and retailers like Amazon—are another challenge. Rhetorical tools' support for mobile apps has hardly begun within the past year about, and covers solely the foremost standard apps. iOS apps are sandboxed, thus all of one app's information are going to be in its specific folder. With automaton, however, this can be not the case. A minimum of some app information are going to be accessible with a logical or classification system extraction. However, getting app information through physical extraction means that secret writing. To decipher app information, the mobile rhetorical tool should be ready to perform a classification system reconstruction. This can be a difficult method because of the manner Flash file systems is implemented: designed to avoid delete cycles, they keep deleted info within the device's memory. However, once the Flash classification system has been reconstructed, it's attainable to start out secret writing the content, together with locations, Bluetooth devices, device info, and cookies, put in apps, net history, and so on.

5. Accurate data, forensic soundness

Boot loaders square measure presently thought-about the foremost forensically sound physical extraction methodology. Whereas they are doing involve loading a chunk of code onto the device, this happens before the rhetorical tool accesses any evidentiary information. Boot loaders have the extra benefits of being generic and so applicable to entire device families—not specific devices. And that they change access to unallocated areas for a completely correct extraction. In some golem devices, however, boot loader use isn't supported, and it's going to become necessary to briefly root the device to perform physical extraction. a brief root doesn't for good modification body permissions or different information on the device. Rather, it provides access to the software system in order that the examiner will change ADB debugging and from there, image the device's non-volatile storage for a full physical extraction. Following this method, upon bring up, the device is not any longer frozen.

6. Some Smartphone extractions remain unsupported

What happens once a wise phone is latched and unsupported by rhetorical tools? Flasher box, JTAG, or chip-off extraction ways become necessary. All 3 change physical extraction—a logical examination can't be performed on associate degree unsupported latched device. However, even this capability may be restricted. for instance, though it's attainable to use the chip-off method on associate degree iPhone latched with a fancy pass code, the info are going to be encrypted and therefore not a lot of use. Indeed, good phone forensics is that

the results of years of analysis by several dozens of pros, each industrial and freelance. That analysis will vary from reverse engineering the device's hardware, firmware, and communication protocols; to exploiting vulnerabilities at intervals the device's code, software package, or secret writing algorithms.

Tools

In recent years variety of hardware/software tools have emerged to recover logical and physical proof from mobile devices. Most tools comprise each hardware and package parts. The hardware includes variety of cables to attach the phone to the acquisition machine; the package exists to extract the proof and, often even to analyze it. Most recently, mobile device rhetorical tools are developed for the sphere. This is often in response each to military units demand for quick and correct anti-terrorism intelligence, and to enforcement demand for rhetorical previewing capabilities at a criminal offense scene, warrant execution, or exigent circumstances. Generally, as a result of it's not possible for anyone tool to capture all proof from all mobile devices, mobile rhetorical professionals suggest that examiners establish entire toolkits consisting of a combination of business, open supply, broad support, and slender support rhetorical tools, along with accessories like battery chargers, physicist baggage or alternative signal disruption instrumentality, and then forth.

Commercial Forensic Tools

Some current tools embody lamp three SECURE read 3AccessData's MPE+, Cellebrite UFED, FINALDATA FINALMobile Forensics, Logicube CellXtract, small Systemation XRY, and MOBILedit! Rhetorical, O rhetorical Suite, Paraben Device Seizure, Radio Tactics Pallas Athena and Aceso merchandise. Some tools have to boot been developed to handle increasing criminal usage of phones factory-made with Chinese chipsets, that embody MediaTek (MTK), Spreadtrum and MStar. Such tools embody Cellebrite\'s CHINEX and EDEC's Tarantula, whereas different vendors have additional some Chinese phone support to their software system.

Open Source Tools

Most open supply mobile forensics tools are platform-specific and intermeshed toward sensible phone analysis. Examples embody iPhone instrument, Katana Forensics lamp light imager, the Mobile Internal Acquisition Tool, TULP2G, and via Forensics Open supply robot Forensics application. Although not originally designed to be a forensics tool, BitPim has been wide used on CDMA phones furthermore as LG VX4400/VX6000 and plenty of Sanyo Sprint cell phones.

Physical Tools

Forensic desoldering

Commonly stated as a Chip-Off technique inside the business, the last and most intrusive technique to induce a image is to desolder the non-volatile microchip and connect it to a microchip reader. This technique contains the potential danger of total information destruction: it's doable to destroy the chip and its content thanks to the warmth needed throughout desoldering. Before the invention of the BGA technology it had been doable to connect probes to the pins of the microchip and to recover the memory through these probes. The BGA technique bonds the chips directly onto the PCB through liquid solder balls, specified it\'s now not doable to connect probes.

Desoldering the chips is finished fastidiously and slowly, in order that the warmth doesn't destroy the chip or information. Before the chip is desoldered the PCB is baked in associate degree kitchen appliance to eliminate remaining water. This prevents the questionable popcorn impact, at that the remaining water would blow the chip package at desoldering. There are principally 3 strategies to soften the solder: hot air, infrared emission, and steam-phasing. The infrared emission technology works with a targeted infrared emission beam onto a selected computer circuit and is employed for tiny chips. The new air and steam strategies cannot focus the maximum amount because the infrared technique.

Chip re-balling

After desoldering the chip a re-balling method cleans the chip and adds new tin balls to the chip. Re-balling are often wiped out 2 other ways. The first is to use a stencil. The stencil is chip-dependent and should work specifically. Then the tin-solder is placed on the stencil. When cooling the tin the stencil is removed and if necessary a second cleansing step is finished. The second technique is optical device re-balling; here the stencil is programmed into the re-balling unit. A bondhead is mechanically loaded with one tin ball from a solder ball singulation tank. The ball is then heated by a optical device, such the tin-solder ball becomes fluid and flows onto the clean chip. Instantly when melting the ball the optical device turns off and a brand new ball falls into the bondhead. Whereas reloading the bondhead of the re-balling unit changes the position to consecutive pin. The advantage of rhetorical desoldering is that the device doesn't have to be compelled to be practical which a duplicate with none changes to the first information are often created. The disadvantage is that the re-balling devices area unit high-ticket, thus this method is incredibly expensive and there area unit some risks of total information loss. Hence, rhetorical desoldering ought to solely be done by tough laboratories.

JTAG

Existing standardized interfaces for reading information square measure engineered into many mobile devices, e.g., to induce position information from GPS instrumentality (NMEA) or to induce slowing data from airbag units. Not all

mobile devices give such a homogenous interface nor will there exist a customary interface for all mobile devices, however all makers have one drawback in common. The miniaturizing of device components opens the question a way to take a look at mechanically the practicality and quality of the soldered integrated elements. For this drawback associate trade cluster, the Joint take a look at Action cluster (JTAG), developed a take a look at technology referred to as boundary scan.

Command Line Tools

System commands

Mobile devices don't offer the chance to run or boot from a CD, connecting to a network share or another device with clean tools. Thus system commands may be the sole thanks to save the volatile memory of a mobile device. With the danger of changed system commands it should be calculable if the volatile memory is absolutely vital. an analogous downside arises once no network affiliation is on the market and no secondary memory are often connected to a mobile device as a result of the volatile image should be saved on the inner non-volatile memory, wherever the user information is keep and presumably deleted vital information are going to be lost. System commands square measure the most cost effective technique; however imply some risks of knowledge loss. Each command usage with choices and output should be documented.

AT commands

AT commands square measure recent electronic equipment commands, e.g., Hayes command set and Motorola phone AT commands, and might so solely be used on a tool that has electronic equipment support. Exploitation these commands one will solely acquire data through the software package, such no deleted information will be extracted.

dd

For external memory and also the USB flash drive, acceptable package, e.g., the UNIX operating system command DD, is required to create the bit-level copy. What are more USB flash drives with memory protection don't would like special hardware and may be connected to any pc. Several USB drives and memory cards have a write-lock switch that may be wont to stop information changes, whereas creating a duplicate. If the USB drive has no protection switch, a blocker will be wont to mount the drive in a very read-only mode or, in associate exceptional case, the microchip will be desoldered. The SIM and memory cards would like a card reader to create the copy. The SIM card is soundly analyzed; such it's potential to recover (deleted) information like contacts or text messages.

Non-Forensic Commercial Tools

Flasher tools

A flasher tool may be a programming hardware or package which will be accustomed program (flash) the device memory, e.g., EEPROM or non-volatile storage. These tools primarily originate from the manufacturer or service centers for debugging, repair, or upgrade services. They will write the non-volatile memory and a few, reckoning on the manufacturer or device, may browse the memory to form a replica, originally supposed as a backup. The memory is shielded from reading, e.g., by package command or destruction of fuses within the browse circuit. Note this may not stop writing or victimization the memory internally by the mainframe. The flasher tools are straightforward to attach and use, however some will modification the info and produce other dangerous choices or don't create a whole copy.

III. Conclusion

Mobile device rhetorical is an ever-evolving field stuffed with challenges and opportunities once analyzing a mobile device for forensic proof in support of a criminal investigation. the method are often harder than ancient laptop forensics owing to the volatile nature of electronic proof. Though forensics toolkits do exist for the investigator, the bulk of the tools area unit either not absolutely developed and don't nevertheless offer full practicality for multiple devices. Budget constraints of enforcement departments command the acquisition of quality software package packages to use with the varied mobile device makers. The secret's for the investigator to use the acceptable toolset that's meant for that individual purpose in activity forensics analysis in a good manner which will support a criminal case.

References

[1] Forensic analysis of mobile phone internal memory Svein Y. Willassen Norwegian University of Science and Technology

[2] Ayers, R., Jansen, W., Cilleros, N., Daniellou, R. (2006). An Overview of Cell Phone Forensic Tools. Retrieved on Sept. 10, 2007 from http://www.techsec.com/TF-2006- PDF/TF-2006-RickAyers-MobileForensics-TechnoForensics.pdf

[3] Ayers, R., Jansen, W., Cilleros, N., Daniellou, R. (2006). Cell Phone Forensic Tools: An Overview and Analysis. Retrieved on Sept. 12, 2007 from http://csrc.nist.gov/publications/nistir/nistir-7250.pdf

[4] DerationsWhenDealingwithCellularTelephones-040507.pdf Article by Ronen Engler Christa M. Miller

[5] Mobile device forensics: Wikipedia, the free encyclopedia.

Ms. Mohini N. Umale: Doing Master of Engineering from Sipna College of Engineering & Technology, Amravati from S.G.B.A. University in Computer Science and Engineering field. Completed B.E. in Computer Technology field from R.T.M.N. University. Publish the research paper in National Conferences.

Prof. Anand B. Deshmukh: Associate Professor at Sipna College of Engineering & Technology, Amravati. He did his B. E. in Electronics and Telecommunication Engineering from S.G.B.A. University and M. E in Digital Electronics from Amravati University. He has more than 12 years of Teaching Experience. He has published many research papers in National as well as International journal and conferences. And also he is a member of IETE. His area of interest is Digital Image Processing.

Prof. Manoj D. Tambhakhe: Assistant Professor at Sipna College of Engineering & Technology, Amravati. He did his M. E in Information Technology. He has more than 4 years of Teaching Experience. His area of interest is Theory of Computation, System Softwares