FORENSIC ANALYSIC OF ANDROID SOCIAL MESSAGING APPLICATION

[1]Maitry Yadav, [2]Chandresh D Parekh,
[1] Post Graduation, Cyber Security, M.Tech, Raksha Shakti University, Ahmedabad, Gujarat, India,
[2]Assistant Professor, Raksha Shakti University, Ahmedabad, Gujarat, India

Abstract: Mobile applications process a significant amount of user information. A large amount of sensitive information is stored locally on smartphones. Therefore, acquiring and analyzing artifacts generated by mobile applications is a crucial and necessary step in the forensic analysis of mobile devices. Digital evidence from smartphone instant messaging applications is potentially useful in many types of criminal investigation and court proceedings. Text messages have been an important component of the evidence presented in numerous high profile cases in recent years, the instant messaging application like WhatsApp , hike, line, Telegram, Snapchat, etc offer users a free or very low cost alternative to SMS for text messaging purposes, and frequently offer other additional features. It is therefore unsurprising that such instant messaging applications have become extremely popular, as a result of which, it is reasonable to expect that more and more cases will involve messages originally sent via such applications.

IndexTerms **- Android Forensic, Social-messaging Application Forensic**

I. INTRODUCTION

Android phones offer great opportunities but also cause a lot of problems. While the forensic analysis of ordinary cell phones typically results in a well-known set of data (e.g. call history, text messages, contacts, media) an analysis of a smart phone reveals a plethora of information, because each app stores application-related data [2]. Mobile phone and mobile networks is being used for crime increasingly. Mobile phone and mobile phone related crime do great harm to social, led the law-enforcing department attaching great importance to it. In treatment process of many cases, the related evidence from mobile is became more, generally the mobile phone often retained the important information

Mobile device forensics is a branch of digital forensics which deals with extracting, recovering and analyzing digital evidence or data from a mobile device under forensically sound conditions. Simply put, it deals with accessing the data stored on devices which includes SMS, contacts, call records, photos, videos, documents, application files, and browsing history and so on, and also recovering data deleted from devices using various forensic techniques. It is important that the process of recovering or accessing details from a device is forensically sound, if it has to be admitted in a court of law and to maintain the integrity of the evidence. If the evidence has to be admitted in a court of law, it is important that the original device is not tampered with.

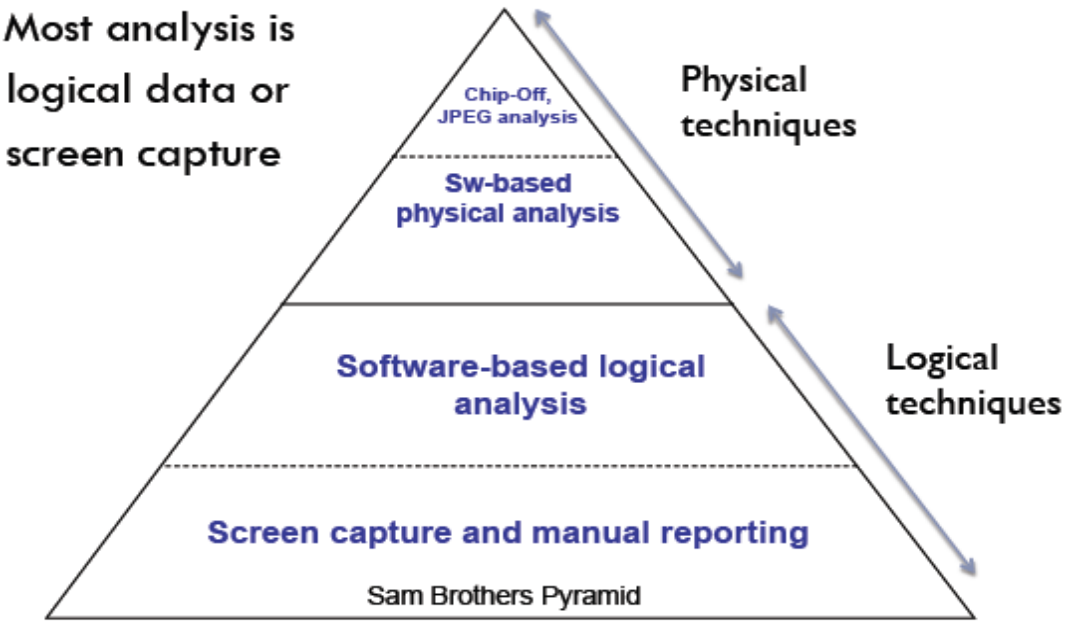


Fig 1.1 :- Approaches for cell phone forensics

- **Manual Analysis** – physical analysis of the phone involving manual manipulation of the keyboard and photographic documentation of data displayed on the screen.
- **Logical Analysis** - Connect data cable to the handset and extract data using AT, BREW, etc. commands in client/server architecture.
- **Physical Analysis (Hex Dump)** - Push a boot loader into phone, dump the memory from phone and analyse the resulting memory dump.
- **Physical Analysis (Chip-Off)** - Remove memory from the device and read in either second phone or Epsom reader.
- **Physical Analysis** (**Micro Read)** - Use an electron microscope to view state of memory

II. CHALLENGE AND ISSUES FOR ANDROID MOBILE FORENSICS

A. Manufacturers:- That is not as easy as it sounds, as there are hundreds of device manufacturers, each one introducing on average 15 new versions of mobile devices per year.

B. Operating systems Smartphone OS receive frequent major updates nearly every month. New security policies, new features, or changes in data storage of the OS constitute immense challenges for mobile forensics experts

C. Apps An increasing amount of data containing information very valuable to forensic investigations, is never saved on mobile devices in the first place but in cloud storage instead – be it by the devices OS or third- party apps data.

D. Security mechanisms Security mechanisms are used on mobile devices to protect data. These mechanisms range from handset user locks, to SIM card PINs and PUKs and device encryption.

E. Common security mechanisms, among others, are: Password,PIN,PUK,Pattern,Biometrical lock (fingerprint),Encryption of data,Data preservations.

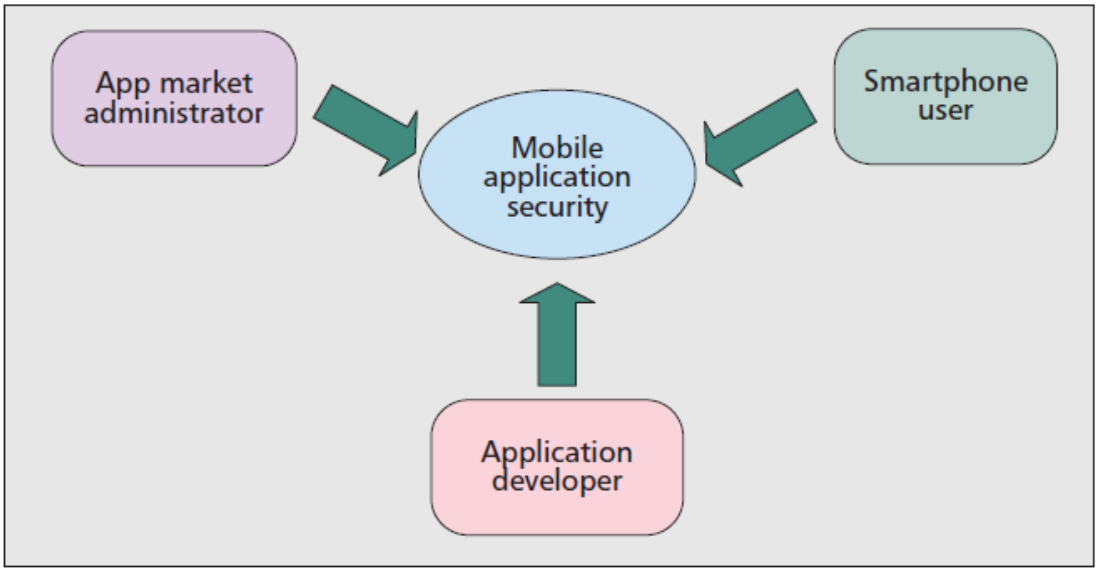
F. Extraction of all relevant data Especially on Android phones, extracting data from all relevant Apps can be difficult.Acquiring a physical extraction has become more and more challenging and is currently not possible for many devices on the market.

III. THE APPLICATIONS LAYERS

The topmost layer in the Android stack consists of applications (called apps) which are programs that users directly interact with. There are two kinds of apps discussed as follows:

System apps: These are applications that are pre-installed on the phone and are shipped along with the phone. Applications such as default browser, e-mail client, contacts, and so on, are examples for system apps. These cannot be uninstalled or changed by the user as they are read only on production devices. These are usually present mounted in the /system directory.

User-installed apps: These are the applications that are downloaded and installed by the user from various distribution platforms such as Google Play. Google Play is the official app store for the Android operating system, where users can browse and download the applications. These apps are presently found in the /data directory. More information about how security is enforced between them is discussed in the following sections



IV. APPLICATION FREAMWORK

Android applications are run and managed with the help of an Android application framework. It is responsible for performing many crucial functions such as resource management, handling calls, and so on. The Android framework includes the following key services,

- **Activity manager**: This service controls all aspects of the application lifecycle and activity stack.

- **Content providers**: This service allows applications to publish and share data with other applications.
- **Resource manager**: This service provides access to non-code embedded resources such as strings, color settings, and user interface layouts.
- **Notifications manager**: This service allows applications to display alerts and notifications to the user.
- **View system**: This service provides an extensible set of views used to create application user interfaces.
- **Package manager**: The system by which applications are able to find out information about other applications currently installed on the device.
- **Telephony manager**: This service provides information to the application about the telephony services available on the device such as status and subscriber information.
- **Location manager**: This service provides access to the location services allowing an application to receive updates about location changes.

V.TOOLS FOR LOGICAL ACQUISTION

OSAF-TK (Open Source Android Forensics – Tool Kit)
OSAF-TK is an open source Android forensics tool kit build from Ubuntu 11.10 specifically for Android Malware Analysis. This tool kit is having all the required pre-compiled tools for code review and application analysis. With this tool kit malicious application can detected and activities of the application can be analysed.

AFLogical
AFLogical is a logical memory acquisition tool for Android devices. The agent installed in the device will acquire the contact list, call logs, SMS, MMS and MMSParts and info.xml file details are send to the forensics workstation. In this acquisition USB debugging mode should be enabled and connect the device to the forensics workstation where AFLogical is installed. This tool acquires logical memory details of the device.

WhatsappXtract
WhatsappXtract is a WhatsApp Backup Messages Extractor for Android and iPhone devices. These tools are able to read whatsapp chats using a backup file. In this it will read older messages, chats and other information in whatsapp backup file and can display on the computer. This tool is specifically used for Whatsapp application.

Andriller
It is a utility which consists of various tools for serving various purposes which includes cracking of screen lock pattern, PIN and passwords, decoding of encrypted databases and files, data extraction automatically and unpacking of android backups. This tool kit solves many of mobile forensics needs for the Android OS. In this data recovery facility is not available and data carving feature is also not available. Correlation of malicious events occurred in the conversations. The excellent feature of this tool is extraction of data from android backups without any root privileges.

VI. PHYSICAL ACQUISITION AND TOOLS

A physical data acquisition from a mobile device means that a bit-for-bit copy of physical storage is extracted. This would give a forensic examiner a bit-for-bit copy of the mobile device's flash memory. This is similar to the way data is acquired in traditional computer forensics [11]. A physical data extraction extracts the data directly from the mobile device's flash memory. After the data is extracted, the memory dump is then decoded. This type of extraction enables the maximum amount of deleted data to be recovered. Physical data acquisition is usually the most difficult extraction type to achieve, as the manufacturers of mobile devices secure against arbitrary reading of the device's memory. Mobile device forensic tool manufacturers often develop custom boot loaders, allowing the forensic tool to access the mobile device's memory and, in many cases bypass pattern locks or pass codes.

VII TOOLS FOR PHYSICAL ACQUISITION

A. Cellebrite UFED Physical analyser
Unified Forensic Examination Device is hardware forensic examination device for extraction of evidences from mobile devices. CelleBrite (UFED) Communicates with a cell phone via a data cable, infrared (IR), or Bluetooth (BT). UFED can acquire data (logically and physically). UFED physical analyzer which analyses every segment of a device's memory using advanced logical, file system and physical extractions. Using simple stand-alone method with UFED, an examiner can recover MMS/SMS messages, call logs, photos, video, and contact information. UFED mainly focuses on logical extraction only. It does not recover emails, browser or search history.

B. Oxygen Forensics Suite
Oxygen mobile forensic Suite is used for logical acquisition and analysis of cell phones, PDAs and Smartphone's. This software kit is a proprietary and having registration key for forensics workstation. This mobile forensics suite can be used to extract device information, SMS messages, contacts, event logs, calendar events and files along with metadata. This tool kit supports major leading mobile platforms.

	Function	Features
GSM .XRY	Acquisition, Examination, Reporting	• Targets certain models of GSM phones • Supports recovery of internal and external SIM • Supports cable, Bluetooth, and IR interfaces
Oxygen PM (forensic version)	Acquisition, Examination, Reporting	• Targets certain models of GSM phones • Supports only internal SIM acquisition
MOBILedit! Forensic	Acquisition, Examination, Reporting	• Targets certain models of GSM phones • Internal and external SIM support • Supports cable and IR interfaces
BitPIM	Acquisition, Examination	• Targets certain models of CDMA phones • Open source software with write-blocking capabilities • No support for recovering SIM information
TULP 2G	Acquisition, Reporting	• Targets GSM and CDMA phones that use the supported protocols to establish connectivity • Internal and external SIM support • Requires PC/SC-compatible smart card reader for external SIM cards • Cable, Bluetooth, and IR interfaces supported

VIII. CONCLUSION

In this paper, I have provided and overview of Android Mobile Application Forensic and Few studies have addressed the forensic analysis and recovery of activities performed through social applications on smartphones. These studies have also been limited to the recovery of very basic information related to the use of social applications. This study focused on the recovery of artefacts and traces related to the use of social applications on a variety of smartphones using different operating systems. It aimed to determine whether activities performed through these applications are stored and can be recovered from the internal memory of these smartphones. The social networking applications on each device, conducting common user activities through each application, acquiring a forensically sound logical image of each device, and performing manual forensic analysis on each acquired logical image. The forensic analysis determined the amount, significance, and location of social networking data that could be found and retrieved from the logical image of each device.

X. FUTURE WORK

Work still needs to be conducted in this area. For one, these applications change constantly, they receive added features, updated security etc. Applications chosen are not the only messaging applications on the Android market, and there is clearly plenty of scope for similar testing to be conducted on other messaging applications. As mentioned before, many of the social media applications, such as Facebook, Whatsapp, Hike, Telegram, Line etc have their own messenger systems, which also require network traffic analysis. Furthermore, applications that could store and send data securely on one operating system may not do so on another, so testing needs to be performed across different operating systems.

Different smartphones employ a variety of techniques to “lock” the device’s interface and encrypt the data stored on the phone while the device is locked, and these privacy measures also serve as anti-forensics techniques to be overcome. Research into this issue would likely require different techniques for each smartphone platform

XI. REFERENCES

1. “Certify Releases Q1 2015 Report on Business Expense Trends”, Certify, 4th April 2015, URL: https://www.certify.com/PR-2015-04-07-Certify-Releases-Q1-2015-Report-on-Business-Expense-Trends, date accessed: 30/05/17.
2. K. Kashyap, “Its Uber vs. Ola for the battle of supremacy in the Indian market”, Forbes, 21st September 2016, URL: https://www.forbes.com/sites/krnkashyap/2016/09/21/its-uber-vs-ola-for-the-battle-of-supremacy-in-the-indian-market/#214a9df8d99f, date accessed: 30/05/17.
3. C. Anglano, “Forensic Analysis of WhatsApp Messenger on Android Smartphones”, Digital Investigation Journal, Vol. 11, No. 3, pp. 201–213, September 2014, date accessed: 30/05/17.
4. D. Walnycky, I. Baggili, A. Marrington, F. Breitinger, J. Moore, “Network And Device Forensic Analysis Of Android Social-Messaging Applications”, DFRWS 2015 USA, August 2015, URL: https://www.dfrws.org/sites/default/files/session-files/paper-network_and_device_forensic_analysis_of_android_social-messaging_applications.pdf, date accessed: 31/05/17.

5. A. Mahajan, M.S. Dahiya, H.P. Sanghvi, "Forensic Analysis of Instant Messenger Applications on Android Devices", International Journal of Computer Applications, Vol. 68-No.8, pg. 38-44, April 2013, URL: https://arxiv.org/ftp/arxiv/papers/1304/1304.4915.pdf, date accessed: 31/05/17.
6. J. Lessard, G. Kessler, "Android Forensics: Simplifying Cell Phone Examinations", Small Scale Digital Device Forensics Journal, 4(1), 1-12, September 2010, URL: http://ro.ecu.edu.au/ecuworks/6479/, date accessed: 05/06/17.
7. P. Albano, A. Castiglione, G. Cattaneo, A. D. Santis, "A Novel Anti-forensics Technique for the Android OS", BWCCA, 2011 International Conference on Broadband and Wireless Computing, Communication and Applications, October 2011, URL: http://ieeexplore.ieee.org/document/6103062/, date accessed: 06/06/17.
8. M. Lohrum, "Live imaging an Android device", Free Android Forensics, August 2014, URL: http://freeandroidforensics.blogspot.ie/2014/08/live-imaging-android-device.html, date accessed: 05/06/2017.