International Journal of Forensic Science and Legal Medicine

Vol. 2, Issue - 2, July-December 2022

IDENTIFICATION, EXTRACTION, ANALYSIS OF POTENTIAL EVIDENCES USING SOCIAL NETWORKING APPLICATIONS USING ANDROID DEVICES: A REVIEW

Wishard Barreto[1], N.P Waghmare[2], W.B Jeberson[3] and Vaibhav Saran[4]

[1]Department of forensic Science, SHUATS (211007)
[2]State Forensic Laboratory, GOA
[3]Department of Computer Sciences and IT, SHUATS (211007)
[4]Department of Forensic Science, SHUATS (211007)

ABSTRACT

The uses of smartphone devices have increased with an unexpected rate. Such types of devices are capable of doing some major works as compared to the current computer systems large storage space. Using such device the major concern of an individual is to become socialized with his friends, family and other relatives and all of that is possible because of such social networking applications and by using them a person can connect to other person anywhere throughout the world. These social networking applications may sometimes become a source of potential evidence in cases where the crime is committed using such devices or applications.it facilitate the forensic investigator to corroborate the scenarios in providing fair conclusions. The reason being the updated versions and the frame wire of such software's making it typical for the objective of its acquisition. These social networking applications can be accessed by malicious users to leverage important information from the user's account which he or she had shared unknowingly for eg: their likes, dislikes their contact details, pictures of their new belongings like cars new house etc. The malicious user gain access to one's private information for the aim of his economic gain. The main purpose of this study is to highlight the weakness of such updated applications and also the evaluation of the currently available tools for the purpose the acquisition of data.

Keywords: Cyber, Forensic, Social media, Smart-phone, Forensic Analysis etc.

INTRODUCTION

The last several years have experienced spontaneous growth of a new variety of online communication known as social networking. This type of social networking is enhancing us to communicate to people far in many various ways ,By using such services, the users can interact and become social, can share information and comments and updates on such platform, letting them participate in live activity and events, upload documents and pictures , and engaging them in real-time on spot messaging and conversations. These applications have fascinated people from all the corner of the world.

The hardware architecture of a typical Smartphone usually consists of a microprocessor, mother board, Read Only Memory (ROM), Random Access Memory (RAM), a radio, a signal processor, a display unit, a microphone and speaker, an input interface device (i.e., keypad, keyboard, or touch screen) and a battery. The OS is usually casted inside ROM while RAM is used to store other information regarding

***Corresponding Author Email:** vikahuja@aol.com

the user's data and user desired settings. The ROM may be upgraded by the user of the smartphone by downloading a patch file from a web site and enacting the device that is connected to his phone.

RELATED WORKS

Mobile Device Forensics

Physical collection is preferable to the more common logical collection (via the stock OS) for a number of reasons. Physical collection of digital information allows for a more thorough analysis of the data stored on the device's flash memory by ensuring that we collect all of the files on the partition. In comparison, a logical collection using a tool such as Android backup will only return the files that the OS provides as part of a backup (this tends to be somewhat vendor specific, but is generally a subset of the available data). The collection of a physical image also allows for the potential recovery of deleted files from unallocated space, file signature verification and header/keyword search using existing forensic tools that are able to read the ext. partition format used by latest version of Android.

Mobile phones apps are being enhanced in vast and frequent lap of time. Word processors, spreadsheets, and data-based apps have also been added into smart mobiles Westtek (2008).

The mobile phone's ability to keep a large amount of data storage, view and print electronic media documents transforming the units into smart mobile office. The ability to send and receive (SMS) messages also transformed mobiles into a massive message Centre. In India, almost 150 crore text messages (SMS) were sent per week between January and May, 2008, the Mobile Data Association (MDA) said Doran (2008).

Mobile phones and their applications may being involved in a large variety of criminal cases, including frauds, thefts, money laundering, illicit distribution of copyrighted material or child pornographic images, or even distribution of malware's in cybercrime cases Taylor (2012).

Smartphone's are now used as a mobile office or entertainment purposes, incorporating basic needs. Their storage capacity and processing capabilities are now being equated computers. Smartphone's became susceptible to the same and greater vulnerabilities as computers. The data in Smartphone's such as images, documents, emails, videos and short messages (SMS) can be remotely accessed if the device is connected to the Internet. This reality poses a major challenge for forensics investigators Sipior (2013). There are many social networking applications that can run on a Smartphone and more are developed every day. Considering the variety of Smartphone brands, mobile applications and networking protocols, the task of forensic analysist on mobile phones is much more challenging now days. When dealing with compact devices such as Smartphone's, there are three areas where data is stored: the SIM card, which primarily contains contact information and texts; the device memory, which stores user created data such as MMS, text messages, photographs, media etc, and also contains the phones operating system and settings and, the device memory which also stores application software and the appropriate logs Hutchings (2012).

The fame of smartphones, it is not surprising that the smart phones are becoming easy targets for cyber-attacks. Smartphone malware/viruses is a growing issue, and the large volume of mobile applications brings with it a fear of potential attack vectors. For example, Damopoulos et al. developed malware which performed DNS poisoning on the iPhone's tethering feature, and exposed important user data (such as location and account access details) when the user used the Siri service Damopoulos et al. (2013).

Beginner work in this field has focused on field of acquisition techniques and general forensic analyses of smart devices. He discussed forensic analysis of older versions of the BlackBerry and covered the hardware and software used for acquisition Burnette (2002). He also described several methods for examination, including the use of hex editors and emulators. Later research provided foundational concepts on forensic analysis of the new generations of Smartphone's. It mentioned the main aspect of the technologies used in the handling procedures, and all the common evidence storage locations in each smartphone. The data/evidence which could be recovered from the internal memory of these devices included call logs, SMS, MMS, e-mails, webpage bookmarks, photos, videos, and calendar Notes Punja SG (2008). recent scientific research has focused on individual types of Smartphone's, investigating the methods that could be used to acquire and analyze the internal memory of the device and the data that could be extracted from each device. IPhone data could be acquired by either a physical or a logical method. The physical method requires jail breaking the system, which causes a slight modification to the

system's data NIST (2007).

The latest technique developed by Zdarsky (2010) acquires a physical-logical image of an iPhone without jail breaking the phone. It is considered the best forensic method for acquiring iPhone and has been evaluated by the National Institute of Standard and Technology (NIST.) Similar to iPhones, Android-based Smartphone's can also be acquired using either a physical or a logical method. The physical technique consists of obtaining a dd image of the phone's memory and requires root access to the device (Vidas et al (2011).

Discussed an acquisition methodology based on overwriting the "Recovery" partition on the Android device's SD card with specialized forensic acquisition softwar Mutawa (2011).

Forensically acquired and analyzed all the device-stored data and network traffic of all 20 popular instant messaging applications available on the basis of playstore in Android. They reconstruct some or the entire message content from 16 of the 20 applications tested, which were very low on the security and privacy measures employed by these applications but may be searched positively for evidence collection purposes by digital forensic investigating officer Asma (2009). The work showed which features of these instantaneous messaging apps leave evidentiary traces allowing for suspect data to be regained or partially regained, and whether network forensics or device forensics permits the reconstruction of that activity.in most cases reconstruct or intercept data such as: passwords, screenshots taken by apps, pictures, videos, audio sent, messages sent, sketches, profile pictures and more was possible Walnycky (2015)

His research focused on available forensic tools with NIST forensic method for extracting latest WhatsApp's artifacts.WhatsApp's security features can lead to crime by people that have criminal intentions. Investigators need to use mobile forensic methodologies and tools for investigating smartphone and finding out the crime evidence. (Rusydi 2018).

In the Below mention table : the details of all the type of social networking applications their versions and their capabilities that is sending text massage, videos, audios, audio chats, video chats, locations, photographs etc. Their performed actions that they can perform and their data traces or the track of the information that can be retrieved from the storage of the smart device.

Table 1: Application Capabilities, Actions Performed By The Social Media Applications And Traces Which Could Be Analyzed By The Forensically Sound Software's.

Applications and versions	Capabilities	Performed activity	Data storage Traces
WhatsApp	Text chat Audio Video Image Location V-card sharing	Sent/Received message Sent/Received voice note Sent/Received image Sent/Received video Sent V-card Sent/Received GPS location	Text chat Audio Video Image Location V-card sharing
Viber	Text chat Voice call Audio Video Image Sketch Location sharing	Sent/Received message Sent/Received sketch Sent/Received image Sent/Received voice note Received voice call Sent/Received GPS location	Text chat Voice call Audio Video Image
Instagram	Text chat Video Image sharing	Sent/Received image	Text chat Video Image
Tango	Text chat Voice call Video call Image sharing	Sent/Received message Sent/Received image	Text chat Voice call Video call Image sharing

Kik	Text chat Video Image Sketch sharing	Sent/Received message Sent/Received image Sent/Received sketch	Chat Log Text chat Video Image
Nimbuzz	Text chat Voice call Audio Video Image Location sharing	Sent/Received message Sent/Received image Sent/Received GPS Location Sent/Received Video	Plain Text Password Chat Log Audio Video Image
MeetMe	Text chat Image sharing	Sent/Received message Sent/Received image	Chat Log Image
MessageMe	Text chat Audio Video Image Sketch Location sharing	Sent/Received message Sent/Received image Sent/Received sketch Sent/Received GPS Location Sent/Received Video Sent/Received Music	Text chat Audio Video Image Sketch Location sharing
TextMe	Text chat Voice call Video call Video Image sharing	Sent/Received message Sent/Received image Sent Drop box file Received video	Plain Text Password Chat Log
HeyWire	Text chat Voice call Audio Image Location sharing	Sent/Received message Sent/Received image Sent/Received GPS Location	Text chat Voice call Audio Video Image Location
Hike	Text chat Voice call Audio Video Image Location V-Card sharing	Sent/Received message Sent/Received image Sent/Received sketch Sent/Received GPS Location Sent/Received Video Sent/Received Music	Text chat Voice call Audio Video Image Location Stickers
Telegram	Text chat Voice call Audio Video Image Location Stickers	Sent/Received message Sent/Received image Sent/Received sketch Sent/Received GPS Location Sent/Received Video Sent/Received Music	Text chat Voice call Audio Video Image Location Stickers
Facebook Messenger	Text chat Voice call Audio Video Image Location Stickers	Sent/Received message Sent/Received image Sent/Received video Sent/Received audio Sent/Received GPS location Sent/Received stickers	Text chat Voice call Audio Video Image Location Stickers

Types of data acquisition techniques:

1. Manual Extraction
2. Logical Extraction
3. Hex dump /JTAG extraction
4. Chip-Off extraction
5. Micro Read extraction

1. Manual Extraction
   - Scroll through data, view, record
     I. Acquires data by direct access to Smart device internal and external storage
     II. Bit-by-bit copy of device media
     III. All data including deleted, but not overwritten
   - Tedious, error prone
   - Works on most of the devices
2. Logical Extraction
   - Fast and easy to perform, cookie cutter methodology (little training required to perform the method)
     I. Uses device APIs
     II. May only acquire some of data
     III. Will not get unallocated data
   - Usually writes data to device
   - Deleted data not accessible
3. Hex Dump – also called Physical Extraction
   - Pushes unsigned code or boot loader onto phone
   - Memory dump is in binary format
   - Retrieves deleted data
4. Chip Off
   - Reads data directly from memory chip
   - Joint Test Action Group (JTAG)
5. Micro Read
   - Electron microscope to read gates status
   - No commercial tools/softwares available at this time

Social Networking Forensic Artifacts

Scientific research has also included all the aspects of investigation of artifacts left by social networking sites on computer systems and also the tools/ software's that can assist in the extraction of these artifacts. Zellers in his research has examined the unique data tags created in different Myspace source-codes and used those tags to create focused artifact keyword searches Bader(2010). Other research has also discussed the analysis process of recovering and reconstructing Facebook chat artifacts from computer's hard disk Thakur (2013). Many social networking applications are integrated into new Smartphone's, in cases involving social networks, forensic examiners may be able to find relevant evidence on a suspect's Smartphone. A forensic examination of the iPhone (via a logical acquisition) showed that a database related to the Facebook application is mostly stored on the phone's memory. The database stores all information as in the list, including their names, ID numbers, and phone number Morrissey (2010). Two more directories associated to the Twitter application were also found. These directories store information about Twitter account data, attachments like documents and pictures sent with tweets, user names, and tweets with date and time values. the forensic analysis of an Android phone's image showed that basic Facebook detail is stored in the contacts of friend list database (contacts.db) as the device synchronizes all contacts of Facebook with the smart devices phone book ". It also explained that the device stores confidential information like Twitter passwords and Twitter updates performed through the Twitter application in plain text Zellers (2008).

WhatsApp is an example of a mobile messaging application. Anglano examined WhatsApp on Android devices in recent work aiding forensic examiners with information about what data is stored on the smart Android phone by WhatsApp application, facilitating the examiner in reconstruction of contact lists and text conversations. Probably all of the applications examined in this work fall into the same category as WhatsApp in that they are first and foremost smartphone applications Anglano (2014).

Another major advantage of physical collection is that it will circumvent passcode lock controls on the device by bypassing the stock OS, something that will generally thwart a collection process that requires the device to be rooted and uses the stock OS. When conducting forensic analysis on a traditional PC, a common technique for physical collection is to boot the PC using a triage live OS (which runs in RAM) or to remove the disk(s) from the PC and use a write blocker in a second PC to collect an unmodified physical image. These techniques have parallels in collection of evidence from Android mobile devices. The physical disk collection method is analogous to the 'chip-off' (i.e. physically removing the NAND

flash from a device) technique used in mobile forensics. While this method has proved useful, it is very time consuming and the technique may not be perfected for the flash storage used in each type of Android mobile device. The live OS collection method is used for physical collection of other mobile devices (e.g. the custom ram disk approach used in 'iPhone-data protection Karp(2008)

Anti-Forensics Techniques

Anti-forensics, generally, is the use of technology to defeat forensic investigation.

Smartphone forensic investigators must understand the working of Smartphone operating system layers because layers depend on each other. It supports 256-bit AES symmetric encryption and RSA 4096 encryption and works without relying on their PGP key and the end to end encryption. Attackers could deliberately mask or hide digital evidence in the Smartphone. IN recent years, anti-forensics for mobiles faces major challenges. For instance, mobile devices used in the field of forensic medicine-store a significant amount of personal information. A dedicated laboratory environment should be available to correctly acquire and handle forensic evidence from the acquisitioned data. There is a spread of applications used to erase evidences that can be used by forensics analysts. Procedures and standards should be observed during data acquisition, transportation and storage. This complexity of anti-forensics hardens the job of forensic analysts.

Such application elevates the challenge faced by mobile forensics scientists. Data acquisition from Smartphone is the process of imaging or otherwise obtaining information from a digital device and its peripheral equipment and media ".Acquisition of data imaging from the mobile is critical. Wicker is an application designed to hide digital traces from governments or companies. Moreover, when comparing Internet and fixed line subscriptions, the trend of Global Information and Communications Technology development in 2001 through 2011 shows mobile cellular telephone subscriptions as having the highest increases. While social networks vary in features and architecture, we identify the following generic data sources to be of interest in forensic examinations on social networks.

METHODOLOGY

NIST defines about digital forensics analysis that consists of four main stages, namely identification, collection, organization and presentation.

The identification step refers to the identification of incident or the evidence that took place or the electronic media which was used. Evidence data is acquired and then imaged which is followed by reducing the amount of data by discarding off any redundancies. The organization phase, carved data is analysis and its relation with the scene of crime in order to reach true justification. Last, the presentation part which deals with reporting the data/evidentiary in a format that can be understood by the jury.

The three steps of analysis are mentioned below:-

A. Identification In digital forensic examination, identification of digital evidence could mean a walkthrough of the scene of crime and identifying any hardware or software worthy of collection.

B. Collection we refer to process of acquiring the disk image as the collection phase. We used FTK Imager for acquisition purpose (as well as for examination as discussed later on in this paper). The choice was made owing to the fact that FTK Imager is considered the fastest and most reliable imaging tool. A raw (dd) bit by bit (physical) image was acquired and saved onto another partition drive on the same system. The identification of artifacts and their examination was easily carried out over the live system. However we chose to execute the entire examination process on storage media's image so as to reflect a real world scenario whereby integrity preservation is of considerable significance. To further preserve the integrity, we used digital hashes of the collected evidence. Initially process monitoring was done in order to get to the artifact locations. Collection of only specific folders identified by Process Monitor could be made, however we chose to image the entire disk space instead as our intention was to study the unallocated space for deleted artifacts as well.

Examination (Organization) The image was explored for artifacts. The artifacts were examined and correlated in order to analyse their usefulness in any real world case. After analysis of the digital data has been undertaken, then a report would typically be produced detailing the relevant evidence found and the process by which the evidence was obtained. This could then be used in a corporate disciplinary hearing or in a court case. Not only is social media evidence commonly available, but when presented may be highly influential with jurors. It is a familiar medium, and will often represent the very words typed or the images uploaded by defendants. The same would be

true of such evidence presented during the hearings.

CONCLUSION

The forensic analysis of the social media application in the Smartphone is playing a vital role in investigation of crime. Sometimes such new type of security updates and new framework affect the functioning of the acquisition in various. Latest trends of smart phone locking systems such as facial recognition and biometric locking also sometimes affect the investigation as the device is not accessible by the software and the software sometimes fails to bypass the lock for extensive extraction procedures.

FURTHER RESEARCH

As the technology is developing day by day the upgradation of software's as well as operating systems of the smartphone the investigator and the analysis software's have to be upgraded accordingly. The gap which is created due to upgradation of smart devices with respect to the forensically sound analysis tools can be studied as to what challenges the investigator has to face during the analysis.

REFERENCES

[1] Asma Majeed., Haleemah Zia., Rabeea Imran and Shahzad Saleem. Forensic Analysis of three Social Media Apps in Windows 10, 12th International Conference on High-capacity Optical Networks and Enabling/Emerging Technologies (HONET) Kubasiak R., Morrissey S and Varsalone J. Macintosh OS X, iPod, and iPhone forensic analysis DVD toolkit. Burlington, MA: Syngress; 2009.

[2] Al Mutawa N., Al Awadhi I., Baggili I and Marrington A. Forensic artifacts of Facebook□s instant messaging service. International Conference for Internet Technology and Secured Transactions (ICITST); 2011. p. 771–6. Abu Dhabi, UAE.

[3] Anglano C. Forensic analysis of WhatsApp messenger on Android smartphones. Digit Investigation 2014; 11(3):13.

[4] Burnette MW. Forensic examination of a RIM (BlackBerry) wireless device http://www.mandarino70.it/Documents/Blackberry%20Forensics.pdf.2002.

[5] Bader M., Baggili I+. IPhone 3GS forensics: logical analysis using apple itunes backup utility. Small Scale Digital Device Forensics Journal, September; 2010, 4(1).

[6] Cellebrite LTD. Cellebrite Android Forensics. Available at http://www.cellebrite.com/mobileforensics/capabilities/android forensics.2013

[7] Cosimo Anglano. Forensic Analysis of WhatsApp Messenger on Android Smartphones. Digital Investigation Journal, Vol. 11, No. 3, pp. 201{213, September.2014}

[8] D. Cortjens., A. Spruyt., and W.F.C. Wieringa. WhatsApp Database Encryption Project Report. Available at https://www.os3.nl/ media/2011-2012/students/ssn project report.pdf.

[9] Damopoulos D, Kambourakis G, Anagnostopoulos M, Gritzalis S, Park JH. User privacy and modern mobile services: are they on the same path Pers Ubiquitous Comput 2013;17:1437e48.

[10] Hutchings, G. (2012) Commercial use of Facebook and Twitter – risks and rewards, Computer Fraud and Security, 2012, 6, 19-20.

[11] IOCE. (2002). Best Practice Guidelines for Examination of Digital Evidence, URL http://www.ioce.org/2002/Guidelines%20for%20Best%20Practices%20in%20Examination%20of%20Digital%20Evid.pdf, (Accessed in August 18, 2008).

[12] Karp, S. (2007, October 31). Facebook's vulnerabilities. http://publishing2.com/2007/10/31/facebooksvulnerabilities/, accessed December 2008

[13] Lessard J., Kessler GC., Android forensics: simplifying cell phone examinations. Small Scale Digital Device Forensics Journal September 2010; 4(1).

[14] Morrissey S. iOS forensic analysis for iPhone, iPad, and iPod touch. New York: Apress.2010.

[15] Mohammad Iftekhar Husain., Ramalingam Sridhar. Forensic Analysis of Instant Messaging on Smart Phones. Springer Berlin Heidelberg, 2010.

[16] NIST, S. 800-86. "Guide to Integrating Forensic Techniques into Incident Response", 2006, 800-86.

[17] N.S. Thakur. Forensic Analysis of WhatsApp on Android Smartphones. Master's thesis, University of New Orleans,. Paper 1706, 2013.

[18] Punja SG., Mislan RP. Mobile device analysis. Small Scale Digital Device Forensics Journal June;2008 2(1).

[19] Paul Doran, MDA (2008). 2008- The year of mobile customers, URL, http://www.themda.org/documents/PressReleases/General/_MDA_future_of_mobile_press_releas e_Nov07.pdf (Accessed in August 18, 2008).

[20] Parsons, A."Windows 10 Forensics: Conclusion" - Computer & Digital Forensics Blog, April 30. http://computerforensicsblog.champlain.edu/2015/04/30/windows- 10-forensics-conclusion 2015.

[21] Rusydi, U. (2018). Mobile Forensic Tools Evaluation for Digital Crime Investigation. International Journal on Advance Science Engineering Information and Technology. https://www.researchgate.net/profile/Imam-Riadi 2/publication/326020731_Mobile_Forensic_Tools_Evaluation_for_Digital_Crime_Investigation/

links/5b340cbaa6fdcc8506d6ee55/Mobile-Forensic-Tools-Evaluation-for-Digital-Crime-Investigation.pdf

[22] S. Jeon., J. Bang., K. Byun., and S. Lee. A recovery method of deleted records for SQLite database. Personal and Ubiquotous Computing, 2012.

[23] Sipior, J., Ward, B., Volonino, L., MacGabhann, L. (2013) A framework for the e-discovery of social media content in the United States, Information Systems Management, 30, 14, 352-358.

[24] Taylor M, Hughes G, Haggerty J, Gresty D, Almond P. Digital evidence from mobile telephone applications. Comput Law Secur Rev 2012; 28(3):335-9.

[25] USSS. (2006). Best Practices for Seizing Electronic Evidence, URL http://www.ustreas.gov/usss/electronic_evidence.shtml, (Accessed in August 18, 2008).

[26] Vidas T., Zhang C., Maloof M. Toward a general collection methodology for Android devices. In: Proceedings of the Eleventh Annual DFRWS Conference, vol. 8S; 2011. p. S14–23. New Orleans, USA, published in Digital Investigation.

[27] Zdziarski J. iPhone forensics: recovering evidence, personal data, and corporate assets. Sebastopol, CA: O□Reilly; 2010.

[28] Zellers F. MySpace.com forensic artifacts keyword searches. http://www.inlanddirect.com/CEIC-2008.pdf; 2008.

*****