Section A-Research paper

Social Media Application Security Extraction and Analysis on Mobile Devices

Wishard Barreto[1], N.P Waghmare[2], Vaibhav Saran[3]

[1] Department of forensic Science, SHUATS (211007)

[2] State forensic laboratory, GOA

[3] Department of forensic Science, SHUATS (211007)

Abstract:

In today's world, everyone uses messaging apps. Many users prefer using messengers with built-in strong encryption for obvious reasons, from confidentiality to hiding data from researchers. Such an app is used by messengers because of the confidentiality and privacy they offer. Many social media application messengers and are considered to be the most used messengers in today's world, along with many other messenger applications, used by people living in regions known for corruption. Many social media messenger applications are free, open-source apps for iOS and Android mobile devices, PC, and Mac. It was Edward Snowden who called Signal the world's most trusted messenger on his Twitter account in 2015. app offers end-to-end encryption, allowing users to send encrypted group and single text messages, photos and video files, and make encrypted phone and video calls without being overheard during transmission. The messenger uses the ZRTP cryptographic protocol and an AES algorithm (Advanced Encryption Standard) with a key length of 128 bits. Second, a secure encryption protocol. The main difference between such applications and its current competitors lies in the reliable encryption algorithms. The security community highly appreciates the cryptographic scheme used by Messenger. Third, store encryption keys in Android KeyStore. Like the iOS keychain, the Android KeyStore is a storage location that contains software and hardware encryption keys on running devices. Java programs use the KeyStore to encrypt data, authenticate and establish an HTTPS connection.

Introduction:

Mobile Forensics is a department of Digital Forensics and its means to approximate the purchase and the evaluation of mobile gadgets to get better digital evidences collection. When we investigate approximately Mobile Forensics generally, we use the term "Forensically Sound Manner", normally used the forensic network to outline the utility of strategies, which appreciate the worldwide acquisition of digital evidence, and exam of cellular gadgets.

The concepts for the Forensically Sound strategies expect the number one purpose, that's the protection and the non-infection of the digital devices. This method isn't always clean at all,

especially in cellular gadgets. The non-stop evolution of cellular gadgets technology, lets in the commercialization of recent cellular phones, which creates new virtual investigations problems. Hardware and software program for those sorts of cellular tool evaluation are numerous, however none is capable of supply an included answer for the purchase and the forensic evaluation of all smartphones. Furthermore, cellular gadgets are capable of incorporate lots of virtual statistics, nearly like a computer, so now no longer simplest a name log or SMS messages as vintage cellular phones.

Many of the digital statistics in a phone is reliant on packages hooked up on it, which evolve in the sort of range that evaluation software program isn't capable of aid them completely. Often the facts acquisition from a cellular tool isn't always well matched with a few parameters, which outline a Forensically Sound method. In different phrases to have get entry to the cellular tool it's miles vital to apply communique vectors, bootloader and different retailers that are hooked up withinside the reminiscence to permit the communique among the cellular telecall smartphone and the tool that we use for the purchase and so it isn't always viable to apply a write blocking off option. Often, we inn on regulate the tool configuration for acquisition, however this operation dangers to invalidate the proof withinside the Court, despite the fact that all of the strategies are continually well-documented.

As a lot as viable it's miles continually essential to appreciate the worldwide recommendations on cellular forensic to make sure the proof integrity and the repeatability of the forensic method. 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. 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. 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).

Methodology

Basic Procedure for Extraction Using MD-Next:

MD-NEXT is mobile device data extraction forensic software. It offers physical and logical extraction methods for Android, iOS, Windows, Tizen, and other smartphone operating systems.MD-NEXT extraction process in its simplest form. MD-NEXT categories extraction methods into two types: physical and logical.

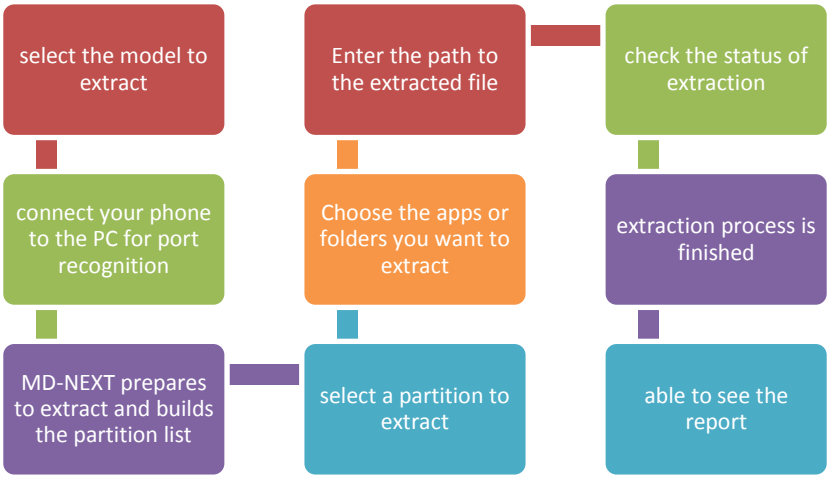

Fig-1 Extract procedure "Android Logical" through the "Bootloader"

Android Live Extraction:

- Android Live is a mechanism for quickly retrieving the currently most important files on an Android phone.
- Select the "Android Live" icon from the method selection window of your device model or press the button on the main page and select "Android Live Extraction" from the menu that appears on the right side of the screen.
- Select the make and model, then click the Confirm button. If MD-NEXT does not currently support your model, you can specify the manufacturer and model name directly.
- Set the phone to flight mode by following the on-screen instructions. After confirming that the device is connected, select the "Next" button to continue.
- Enter additional information and specify a location for the extracted file. To start the extraction process, press the "Confirm" button.
- If you entered a case number in the previous step, it will be displayed in the upper right corner and the extraction process will begin immediately. If the ripping process stops for a while and you see a backup notification on the mobile screen, tap the "Backup" button on the bottom right of the screen to continue to the next step.
- When the extraction is complete, you will receive a report with the results.

Result and Conclusion

Table 1: Extraction Information

Category	Content
Model	Xiaomi Redmi 4A
Extraction Method	Android Live
Extraction Time	2023-02-12 22:34:14 ~ 2023-02-12 22:44:42(10m 28s) (UTC+05:30) Chennai, Kolkata, Mumbai, New Delhi
Device Timezone	(UTC+05:30) Chennai, Kolkata, Mumbai, New Delhi
Program Version	1.91.18.1758

Table 2: Logical Extraction List
LOGICAL

File Name	Redmi 4A_AndroidLive_20230212.mdf
File Size	3,534,118,400 Bytes
Extracted Data Size	3,534,118,400 Bytes
SHA256	75FF671E551A5095F0FBC8561EA6B8727D3246E2547179E172662607A04A4B2F

Table 3: Logical Mobile Analysis Report

Model	Redmi 4A
Manufacturer	Xiaomi
Extraction Method	Logical
File Size	3.29 GB
File Name	Redmi 4A_AndroidLive_20230212.mdf
Extraction Date/Time	02/12/2023 22:34:14 ~ 02/12/2023 22:44:42
SHA256	Extraction: 75FF671E551A5095F0FBC8561EA6B8727D3246E2547179E172662607A04A4B2F
Extraction Tool	MD-NEXT v1.91.18.1758
Forensic Tool	MD-RED v3.10.8.2183

Table 3: Physical Mobile Analysis Report

Item	**Contents**
Case Name	Redmi 4A_AndroidLive_20230212
Created Date/Time	02/12/2023 22:47:13

Analysis Image	**Item**	**Contents**
Redmi 4A_AndroidLive_20230212	Message	All 6,979 / Active 6,979 / Deleted 0 / Etc0

Redmi 4A_AndroidLive_20230212		Picture		All 19,293 / Active 19,293 / Deleted 0 / Etc 0	
Redmi 4A_AndroidLive_20230212		Movie		All 245 / Active 245 / Deleted 0 / Etc 0	
Redmi 4A_AndroidLive_20230212		Sound		All 174 / Active 174 / Deleted 0 / Etc 0	
Redmi 4A_AndroidLive_20230212		Document		All 1,325 / Active 1,325 / Deleted 0 / Etc0	
Redmi 4A_AndroidLive_20230212		DB		All 177 / Active 177 / Deleted 0 / Etc 0	
Redmi 4A_AndroidLive_20230212		Compressed File		All 35 / Active 35 / Deleted 0 / Etc 0	
Redmi 4A_AndroidLive_20230212		Executable File		All 3 / Active 3 / Deleted 0 / Etc 0	
Analysis Image	**Item**	**All**	**Active**	**Deleted**	**Etc**
Redmi 4A_AndroidLive_20230212	Message	6979	6979	0	0
Redmi 4A_AndroidLive_20230212	Picture	19293	19293	0	0
Redmi 4A_AndroidLive_20230212	Movie	245	245	0	0
Redmi 4A_AndroidLive_20230212	Sound	174	174	0	0
Redmi 4A_AndroidLive_20230212	Document	1325	1325	0	0
Redmi 4A_AndroidLive_20230212	DB	177	177	0	0
Redmi 4A_AndroidLive_20230212	Compressed File	35	35	0	0
Redmi 4A_AndroidLive_20230212	Executable File	3	3	0	0

Conclusion

Manufacturers are rapidly adopting encryption and other difficult security techniques in response to the growing security and privacy concerns of mobile device consumers. This trend has significant implications for traditional forensic data collection capabilities. Traditionally, retrieving raw data from a mobile device's non-volatile memory yielded vital data, including deleted information, which could then be used in criminal investigations. Because of this, chip-off and micro reading have long been recognized as the most effective technology in forensic data collection. However, as we have said in this white paper, traditional physical data collection practices cannot provide human-readable data due to encryption. In addition, good OS-level data erasing capabilities make it impossible to identify data traces in physical data. At the same time, additional security features make it difficult for forensic investigators to obtain even live data from the target device. As a result, bypassing or disabling device lock and encryption while preserving the integrity of user data is fast becoming the number one forensic approach for mobile

devices today. Therefore, extensive reverse engineering and vulnerability exploitation is required for forensic investigators to perform mobile forensics. Reverse engineered vulnerabilities were previously exploited into obtain evidence from locked and encrypted mobile devices.

References:

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

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

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

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

[5]. 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.

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

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

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

[9]. 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.

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

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

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

[13]. 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.

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

[15]. 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.

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

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

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

[19]. Paul Doran, MDA (2008). 2008- The year of mobile customers, URL, http://www.themda.org/documents/PressReleases/General/_MDA_future_of_mobile_press_release_Nov07.pdf (Accessed in August 18, 2008).
[20]. 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).
[21]. USSS. (2006). Best Practices for Seizing Electronic Evidence, URL http://www.ustreas.gov/usss/electronic_evidence.shtml, (Accessed in August 18, 2008).
[22]. Karp, S. (2007, October 31). Facebook's vulnerabilities. http://publishing2.com/2007/10/31/facebooksvulnerabilities/, accessed December 2008
[23]. 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.

[24]. Anglano C. Forensic analysis of WhatsApp messenger on Android smartphones. Digit Investigation 2014; 11(3):13.
[25]. 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.
[26]. Hutchings, G. (2012) Commercial use of Facebook and Twitter – risks and rewards, Computer Fraud and Security, 2012, 6, 19-20.
[27]. 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.