Recovering the content and meta-data of ephemeral message on mobile devices

Shona Start
Northumbria University, KF7001
shona.start@northumbria.ac.uk

Abstract *- Ephemeral messages are multimedia messages that are not permanent and automatically delete after a set amount of time. Previous research into ephemeral messages focused on secure instant messaging applications and showed that recovering ephemeral messages from these applications is extremely challenging. However, in recent years, many mainstream applications have added ephemeral messaging. This paper will analyse the applications Facebook and Instagram in order to determine whether it is possible to recover ephemeral messages. In the research and whether mainstream applications offer the same obstacles as security instant messaging applications.*

Index Terms— *mobile forensics; instant messaging; android; ephemeral messaging; cellebrite.*

I. Introduction

In recent years, many popular applications have added features which give users the ability to send ephemeral messages. Ephemeral messaging is the transmission of multimedia messages that are not permanent.

There are also many applications that exist to only provide ephemeral messaging, usually alongside other security measures and anti-forensics techniques. The removal of ephemeral messages is usually triggered in one of 2 ways; after the message has been viewed by the recipient or after a set amount of time has passed since the message was sent. Many applications allow users to choose the trigger they want to be used for each of their messages; allowing for ephemeral messages to exist within normal messages.

Digital analysis and recovery of ephemeral messages can be very challenging, especially as ephemeral features are often used in tandem with other security measures. Research into recovery is scarce and mainly focuses on applications that are designed for the security of their instant messaging (IM). It is clear from the research conducted most of these applications are well built and offer little opportunity for recovery of ephemeral messages.

However, in recent years, many mainstream IM applications have added security features, including ephemeral messaging. In fact, the 2 most popular social media applications in the UK both have ephemeral messaging capabilities [1]. These applications are Facebook and Instagram, and both provide a feature called “vanish mode” which allows users to send encrypted ephemeral messages. For users to access the feature, both sender and receiver must enable it on their account [2]. As this vanish mode is a separate entity from the normal IM that these applications provide, it queries how an investigator can establish if the feature has even been used as well as if any data can be recovered.

This paper will discuss and evaluate the tools and techniques used by other researchers to investigate ephemeral messages, so that effective methods can be established. The author will then conduct their own analysis of the popular applications Facebook and Instagram on an Android 10 operating system (OS), in order to determine:

- If these applications provide the same level of secure messaging as IM apps designed for the main purpose of security.
- If it can be determined when ephemeral/secure messaging features have been used.
- If any of the content or metadata of ephemeral messages (including images) can be recovered.

II. Techniques

While investigating ephemeral messaging, researchers have tried several techniques. In order to compare and establish methods of recovery, this section of the paper will review the techniques used by others and suggest other techniques that may not have been tried.

In the paper “Forensic Analysis of the Recovery of Wickr’s Ephemeral Data on Android Platforms”, the authors conducted an analysis of the application Wickr, using several methods to determine what can be recovered when both ephemeral messaging and end-to-end encryption are used. The authors gather data from multiple sources, including the Wickr installation

package (Wickr.APK), the Wickr data directory, and finally from a RAM dump. [3]

In order to acquire this data, they had to root the phone. In digital forensics investigations, rooting is conducted in order to obtain privileged access to a device as this allows investigators to bypass security mechanisms and acquire a physical image. However, doing this threatens the data integrity as rooting can alter the data on the phone [4]. Alternative methods that can be used instead of a physical image are Joint Test Action Group (JTAG) and chip-off. JTAG is a standard used to test circuit boards, with investigators using this process to force the processor to acquire a physical image. This method is not destructive if done properly, and does not affect data integrity. On the other hand, chip-off imaging can destroy a device and is usually only ever used as a last resort. This method involves removing the flash memory chip from a device and using a chip reader to acquire its raw data [5].

The investigators first analysed the Android Application Package (APK). APK's are a file format used by Android devices to distribute and install applications. Analysis of an applications APK can provide investigators with an insight into how the app uses directories, databases and other resources [6]. In order to perform an analysis, they converted the APK into a Java archive and then deconstructed this Java. By doing this the authors were able to uncover how the application encrypts its SQLite files, using the SQLCipher extension [3].

As the researchers were only investigating an Android device, they do not discuss using this technique on an iOS device. The nearest corresponding file type is the iOS app store package (IPA) file. Like APK files, IPA files are the file format used to distribute and install applications on iOS devices so they could potentially be used in the same way as an APK file [7].

The authors also analysed Wickr's data directory. A data directory is the storage location for all the applications permanent data. They first discovered that many files lacked normal headers which further proved Wickr uses extensive encryption. In order to understand how the application removes data, the authors acquired data during different stages of a messages life cycle so that they could compare changes. By doing this they were able to find where Wickr stores its messages. They found out that before messages are deleted, their filesystem and headers are removed, so they cannot be accessed via the application. However, their contents exist in unallocated space, as they have not been overwritten. This means that they can possibly be recovered from the same unallocated space [3].

Analysis of an applications data directory is a common way of searching for evidence and was conducted in other studies researching ephemeral messaging. For example, the paper "Forensic Analysis of Secure Ephemeral Messaging Applications on Android Platforms", also researched the application Wickr. In this the researchers conducted analyses of the applications Wickr and Telegram to find out if and how much message data could be recovered from these messaging applications [8].

In both papers, another method that was used was the analysis of volatile memory. Volatile memory is data that is only maintained while the device is powered; once a device is powered down this data is lost. This means that when acquiring volatile memory there is a risk of accidentally removing or changing data. There are two methods of acquiring volatile memory: hardware-based acquisition, and software-based acquisition. Software-based acquisition is the most popular method; and the method used by the authors. This method can provide data on current processes, including hidden processes and terminated processes. It can also provide information on network connections, open files, passwords, encrypted content and malicious code [9].

In order to analyse the memory data that they had acquired, in both papers, the authors used a string search to search for keywords [3] [8]. String searching is usually done at the beginning of an analysis in order to quickly determine if anything recognizable exists on the image. Security applications, such as Wickr and Telegram, will often use anti forensics techniques such as encryption and advanced functions so that string searches won't detect useful information. Thus, in both papers, the researchers were not able to recover much data. There are other techniques that could be appropriate.

For example, another technique that is often done at the beginning of an analysis is to establish the current state of every running process. This allows investigators to determine if an application was being used when the image was taken [9]. A further technique is file carving. File carving is the extraction of files from raw data, which is done by using file formats to identify file types and can allow for hidden or partial files to be recovered. This method is designed for analysis of drives but can sometimes be used on voluntary memory dumps; although results vary [10]. The paper "Techniques and Tools for Recovering and

Analyzing Data from Volatile Memory" discusses a method for recovering deleted and hidden data from volatile memory. This involves an investigator using a script that goes through an entire image searching for constant patterns, such as the headers that will always be the same. By doing this an investigator can use these patterns to detect files and processes [9].

A further method that was used in the paper "Forensic Analysis of Secure Ephemeral Messaging Applications on Android Platforms" is hex analysis. Hex analysis is the examination of the binary and hexadecimal data of files. The authors used a hex editor to analyse the file "cache4.db" which is an SQLite database. By doing this, they were able to recover messages that were stored in the database, including those that were not accessible through the application itself [8]. There are many other uses for hex analysis that could be explored, for example, analysis of file signatures. A file signature is the first bytes of a file, these indicate to the OS what type of file it is. However, as discussed earlier, the paper "Forensic Analysis of the Recovery of Wickr's Ephemeral Data on Android Platforms", discovered that Wicker removes the file signatures of deleted data [3]. It is possible that other applications may do this or change the extension of a file to disguise them. By performing file signature analysis these discrepancies may be discovered [11]. Another method used in hex analysis is the examination of unallocated space. Deleted files are usually stored in unallocated space until they are overwritten. By performing file signature analysis, files or parts of files can be recovered; potentially giving access to not just deleted data but also unencrypted data and timestamps [12].

Another research paper that researched the recovery of ephemeral messages was "Comparisons of Forensic Tools to Recover Ephemeral Data from iOS Apps Used for Cyberbullying". In this paper the authors compared how efficient two different forensics tools were at recovering ephemeral data from three different applications; Snapchat, Cyberdust and Confide. Due to the nature of the research, the techniques used by the authors are determined by the forensics tools capabilities. This meant that the main method of analysis is of a logical acquisition of the file system. The authors focused their investigation on the data directories for each of the applications. They also performed keyword searches [13]. A further paper that primarily analysed the file system of a device was "Snapchat Analysis to Discover Digital Forensic Artifacts on Android Smartphone". In this paper the authors analysed snapchat artifacts to determine what data can be recovered, including ephemeral data. Similarly, the researchers analysed each applications data directory and performed keyword searching. However, they also investigated the cache folders and database folders of the devices [14]. In both papers, no ephemeral data was recovered through analysis of the file system. However, in digital forensics the file system is often one of the most vital locations for evidence, so it is important to analyse this source thoroughly [15].

By analyzing previous investigations conducted by other researchers; several techniques for recovery of ephemeral messages have been highlighted. These include file system analysis, file carving, hex analysis, volatility memory analysis and APK/IPA analysis. It is apparent that even with these established techniques, recovering the content and meta data of ephemeral messages is normally not possible.

III. Tools

In their research, the authors of the previous papers used several tools. In this section the author will examine the tools to determine usefulness in recovering ephemeral messages from mobile devices.

The authors of the "Forensic Analysis of the Recovery of Wickr's Ephemeral Data on Android Platforms" used the tools Kingo Root, Android Debug Bridge (ADB), Java Decompiler (JD) and Autopsy/The Sleuth Kit (TSK) [3].

The application Kingo Root is a rooting software used with android OS [16]. There are many rooting software packages available that all perform similar functions.

ADB is a tool used to access the command-line of an Android device. This allows an investigator to issue commands to a phone from their workstation. The researchers used ADB to run the "ADB pull command" [3]. This command allows for the copying of directories to any location on the device, such as the SD card. Therefore, it can be used to acquire specific files and folders from a device for further analysis with minimal integrity loss [17].

JD is a tool that reverse engineers machine code into source code [18]. This can allow investigators to analyse how an application processes data. JD is one of many tools that can decompile code, however, because Java is the default development language to write Android apps, [19] JD is fundamental when analyzing Android applications and archives.

TSK is an open-source forensic toolkit used to analyse volume and file system data collected from

both hard drives and mobile devices. Autopsy is the graphical interface that makes using TSK easier. This forensics toolkit is one of the most popular available, however many alternatives are available. For example, the toolkits Oxygen Forensic Detective Enterprise and MOBILedit Forensic Express were used in the paper "Comparisons of Forensic Tools to Recover Ephemeral Data from iOS Apps Used for Cyberbullying" [13].

Oxygen Forensic was built to allow for extraction and analysis of a wide variety of devices and systems, including mobiles and Internet-of-Things(IoT) devices. MOBILedit focuses only on mobile phone forensics [20]. As this paper is a comparison of these toolkits, it can give some insight into how effective these toolkits are at recovering ephemeral messages. The authors were not able to recover any ephemeral messages on the applications they tested using either of the toolkits and Oxygen Forensic had issues recognizing the applications [13].

Autopsy was also used by the authors of "Forensic Analysis of Secure Ephemeral Messaging Applications on Android Platforms" [8]. The authors used a second tool called WinHex. This tool is a hex reader and editor and was used by the authors to analyse the clusters of data where the ephemeral messages had been stored.

It is clear a range of tools are available to asset investigators in investigating mobile devices. But unsurprisingly there are no tool explicitly for the recovery of empirical data. Forensics toolkits such as Autopsy, Oxygen and MOBILedit seem to be the most promising. However, one of the major roadblocks that was apparent from previous study's is that encryption is often used alongside ephemeral messaging and these tools do not have decryption capabilities.

IV. Methodology

For this investigation, a Samsung Galaxy S9 running Android version 10 will be wiped and loaded with the applications Facebook and Instagram, so that the messages and images shown in Table 1 can be transmitted. A selection of types of ephemeral messages, including images, have been selected in order to determine if this will make any difference to the recoverably.

Cellebrite UFED is a forensics software designed for data extraction of a wide range of mobile devices. It will be used to take three acquisitions of the Samsung Galaxy S9; Advanced Logical and Physical. logical extraction is the quickest, and least intrusive way of collecting data. However, it can fail to gather much data from applications. Although it is unlikely much data will be recovered, this type of acquisition will still be taken so that this can be established as fact. Physical acquisition is more likely to recover data as it extracts all the raw data at the binary level, including the physical storage, filesystem and device memory. However, it is also one of the more intrusive methods of extraction and generally takes a long time. It requires the device to be restarted a number of times which will affect the credibility of volatile memory [21].

Once these acquisitions have been taken, the forensics analysis software Cellebrite Physical Analyzer will be used to run the analysis tools location carving and archive data recovery. The software will then be used to perform file system analysis and hex analysis on the device in order to determine if any data can be recovered.

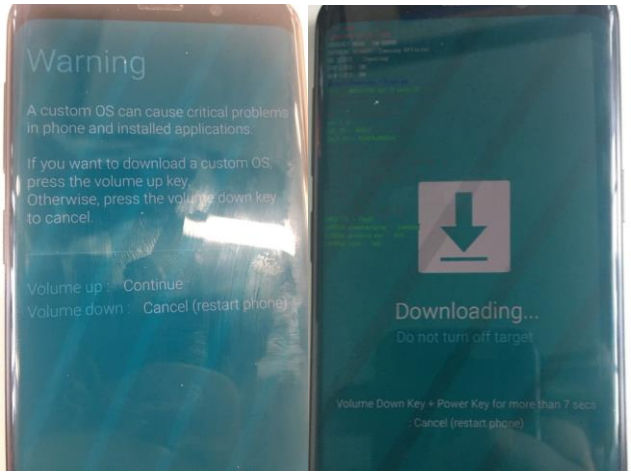

Figure 1 - Galaxy S9 Physical acquisition

Facebook			
Type	**Sender**	**Content**	**Time (BST)**
Nonephemeral	Samsung	Ad astra per aspera	30/04/21 12:58
Nonephemeral	iPhone	Sapere aude	12:59
Nonephemeral	iPhone	[pink-cat.jpg]	12:59
1 min Ephemeral	Samsung	Carpe vinum	13:00
1 min Ephemeral	iPhone	Alea iacta est	13:01
1 min Ephemeral	iPhone	[yellow-cat.jpg]	13:01
1 hour Ephemeral	Samsung	Acta non verba	13:02
1 hour	iPhone	Audentes	13:03

Ephemeral		fortuna iuvat	
1 hour Ephemeral	iPhone	[green-cat.jpg]	13:03
1 hour Ephemeral unopened	iPhone	Quid infantes sumus	13:05

Table 1 – Facbook messages

Instagram			
Type	**Sender**	**Content**	**Time (BST)**
Nonephemeral	Samsung	Natura non constristatur	30/04/21 13:14
Nonephemeral	iPhone	Ad meliora	13:14
Nonephemeral	iPhone	[blue-cat.jpg]	13:15
Allow reply	Samsung	Creo quia absurdum est	13:17
Allow reply	iPhone	In absentia lucis	13:18
Allow reply	iPhone	[purple-cat.jpg]	13:19
View once	Samsung	Tenebrae vincunt	13:19
View once	iPhone	Ars longa vita brevis	13:20
View once	iPhone	[skull-cat.jpg]	13:21
View once unopened	iPhone	De omnibus dubitandum	13:22

Table 2 – Insagram messages

V. Results

As expected, the Advanced Logical acquisition preserved very limited data. All data collected was of no relation to the investigation and no data connected to Facebook or Instagram was found. Therefore, the data analyzed in this section was all recovered through the physical acquisition.

a. Facebook

A keyword search performed across the acquisition provided no matches, suggesting the content of the messages has been completely removed from the file system or is encrypted.

Cellebrite collected many images from the phone. One of the images recovered from the Facebook cache is a copy of the 1-hour ephemeral image sent by the iPhone (Figure 2). It's not clear from the meta data of this image that it was received as an ephemeral message however the timestamp is accurate. This image was recovered from a Facebook cache located in the folder "com.facebook.orca". Further analysis of this folder revealed that it is a storage location automatically created by Facebook for the storage of a range of data files that relate to messages, including images, videos, audios, cookies and cache data. It is not clear why only the 1-hour Ephemeral image was recovered from here and not the Nonephemeral or 1 min ephemeral.

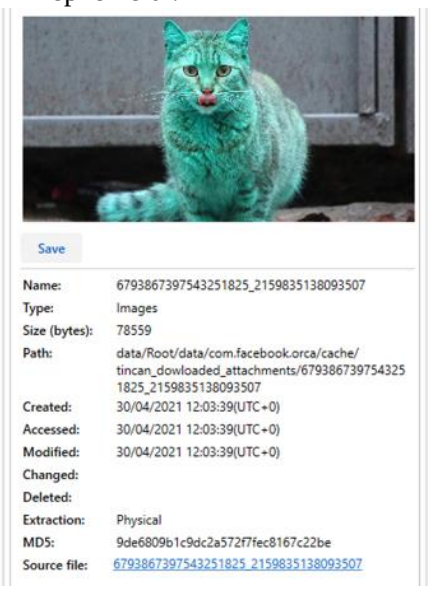

Figure 2 - green-cat.jpg

Another source of data found in the folder was the file "notification_log_event0.txt" (Figure 3). Analysis of this file revealed it to be a log of messaging events which includes timestamps for when the application received and notified the user of new messages. Unfortunately, this file does not specify any details beyond this so determining what type of messages were sent is not possible.

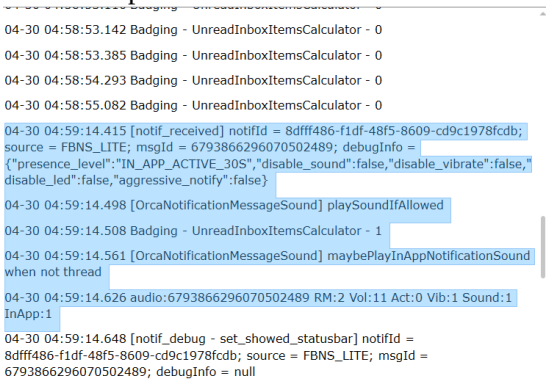

Figure 3 - notification_log_event0.txt

Another source of data from "com.facebook.orca" that other researches have noted as a possible message

recovery location is the file “threads_db”. In other studies, researchers have found that this database stores chat messages [22] [23]. However, analysis of this database on the Samsung revealed it to be completely empty, suggesting that messages sent using the secure channel are stored elsewhere as even the nonephemeral messages were not recovered (Figure 4).

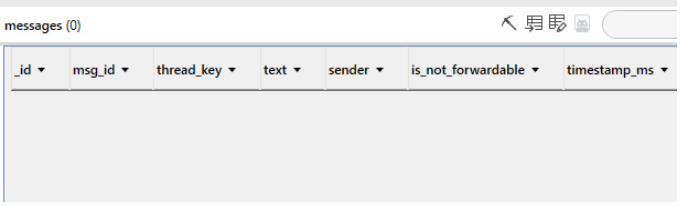

Figure 4 - threads_db

b. Instagram

As with Facebook, a keyword search was performed across the acquisition and provided no matches.

However, analysis of the data that Cellebrite recovered from databases found that in the database “direct.db” there is clear evidence of communication using ephemeral messages (Figure 5). The database provides a record of most messages sent between the devices, besides the first three nonephemeral messages and the unopened message. Further analysis of this database confirmed that the content of the messages is not recoverable from this database. But unlike Facebook, Instagram appears to store all messages in the same location and clearly includes the type of message, tagging ephemeral messages as “raven_media” (Figure 6).

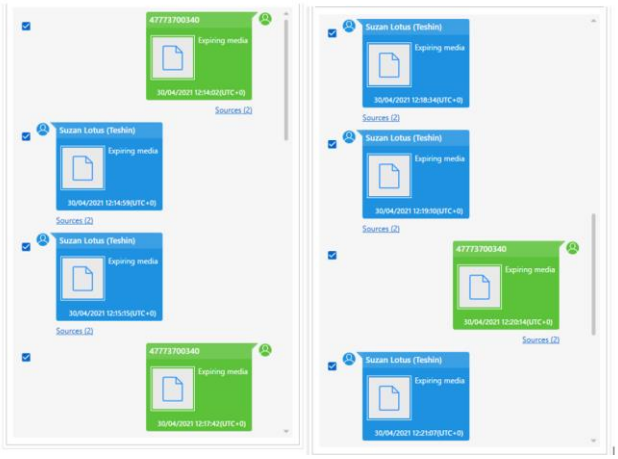

Figure 5 - direct.db messages

recipient_ids	timestamp	message_type	text	message
47628713761	1619785340209022	raven_media		{"content_type":"EXPIRING_MEDIA","st
47628713761	1619785285690482	raven_media		{"content_type":"EXPIRING_MEDIA","st
47628713761	1619785267596769	raven_media		{"content_type":"EXPIRING_MEDIA","st
47628713761	1619785214204366	raven_media		{"content_type":"EXPIRING_MEDIA","st
47628713761	1619785150232915	raven_media		{"content_type":"EXPIRING_MEDIA","st
47628713761	1619785114841617	raven_media		{"content_type":"EXPIRING_MEDIA","st
47628713761	1619785062895361	raven_media		{"content_type":"EXPIRING_MEDIA","st
47628713761	1619784915796511	raven_media		{"content_type":"EXPIRING_MEDIA","st
47628713761	1619784899785269	raven_media		{"content_type":"EXPIRING_MEDIA","st
47628713761	1619784842422239	raven_media		{"content_type":"EXPIRING_MEDIA","st
25588890808	1619706758472794	raven_media		{"content_type":"EXPIRING_MEDIA","st
25588890808	1619706608536564	raven_media		{"content_type":"EXPIRING_MEDIA","st
25588890808	1619706241698353	text	hi	{"content_type":"TEXT","status":"UPLO

Figure 6 - direct.db message logs

As stated, earlier Cellebrite collected many images from the phone, among these images exists all the messages sent from the Samsung (Figures 7, 8 and 9). All the types of message sent from the device were stored in the folder “pending_media_images” and transparent versions of the messages were stored in the file “decors”. There is nothing in the images meta-data to suggest that these images were messages, however the timestamps can be matched with data from “direct.db” in order to hypothesize the origin. The paper “Forensic Analysis of Instagram on Android” lists “pending_media_images” as the storage location for “Instagram Stories” [24]. Stories are photos and videos that vanish after 24 hours, they are usually shown at the top of a users account and can be viewed multiple times before they expire [25]. This finding suggests that Instagram uses the same method of deletion for sent ephemeral messages that it uses for stories; if this is true then it is possible that all sent ephemeral messages may persist on a device for 30 days, as this is how long stories are stored on a device before automatic deletion [26].

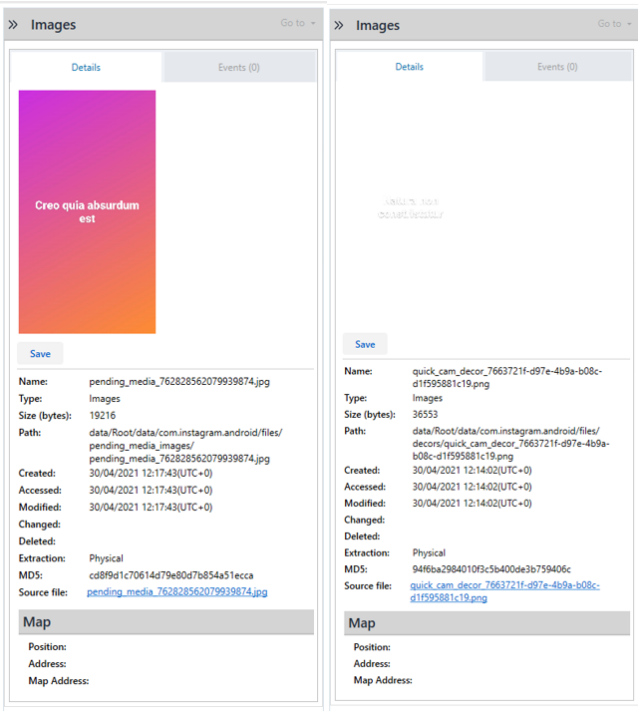

Figure 7 - Nonephemeral message

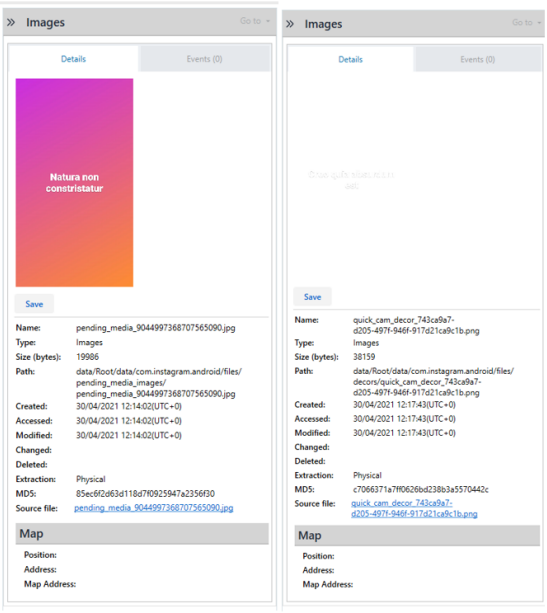

Figure 8 - Allow reply message

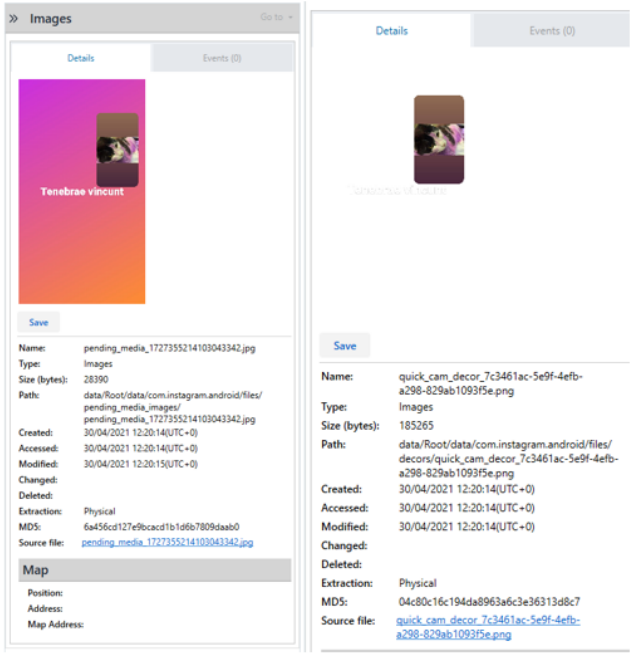

Figure 9 - View once message

VI. Conclusion

The findings of this report suggest that although mainstream social media is incorporating more anti forensics techniques, the methods they use do not always match the security of the secure messaging applications explored by other researchers. There is a clear increased chance of recovery of ephemeral messages from Facebook and Instagram compared to previous research.

Instagram appears to provide a high rate of recovery, especially with the discovery of it potentially storing sent ephemeral messages for 30 days. If this finding is correct recovery of both devices would allow investigators to recover an entire conversation. However, to confirm this finding further research would need to be conducted.

On the other hand, Facebook was significantly harder to recover data from. These finding reinforce that one of the most challenging aspects of recovering ephemeral messages is that it is often used in tandem with encryption. If Instagram implemented encryption it is likely the findings would be very different.

One of the shortcomings of this research was the speed in which the acquisitions were taken from the device. In this study the images were taken on the same day as the data was propagated; whereas in reality it is unlikely an acquisition would be taken that fast. In future research it would be beneficial to take acquisitions from a set period of time.

It would also be advantageous to analyze other sources of data such as volatile memory and unallocated space as both can provide the possibility of recovering deleted data and decrypted data providing it hasn't been overridden.

VII. References

[1] YouGov, "The Most Popular Social Networks (Q4 2020)," 2020. [Online]. Available: https://yougov.co.uk/ratings/technology/popularity/social-networks/all .

[2] S. Nick, "Facebook's Vanish Mode on Messenger and Instagram lets you send disappearing messages," The Verge, 2020. [Online]. Available: https://www.theverge.com/2020/11/12/21561286/facebook-vanish-mode-launch-instagram-messenger-disappearing-snapchat.

[3] T. E. A. Barton and H. B. Azhar, "Forensic Analysis of the Recovery of Wickr's Ephemeral Data on Android Platforms," *The First International Conference on Cyber-Technologies and Cyber-Systems,* pp. 35-40, 2016.

[4] T. Almehmadi and O. Batarfi, "Impact of Android Phone Rooting on User DataIntegrity in Mobile Forensics," *2nd International Conference on Computer Applications & Information Security (ICCAIS),* pp. 1-6, 2019.

[5] S. Krishnan, B. Zhou and M. K. An, "Smartphone Forensic Challenges," *International Journal of Computer Science and Security(IJCSS),* vol. 13, no. 5, pp. 183-197, 2019.

[6] T. Surin, "Inspecting APK Files," PSPDFKit, 2019. [Online]. Available: https://pspdfkit.com/blog/2019/inspecting-apk-files/.

[7] Raz, "Pulling apart an iOS App," 2017. [Online]. Available: https://razb.me/pulling-apart-an-ios-app/index.html.

[8] H. B. Azhar and E. A. T. Barton, "Forensic Analysis of Secure Ephemeral Messaging Applications on Android Platforms," *Communications in Computer and Information Science (CCIS),* vol. 630, pp. 27-41, 2017.

[9] K. Amari, "Techniques and Tools for Recovering and Analyzing Data from Volatile Memory," SANS Institute, 2009.

[10] Warlock, "File Carving," InfoSec Institute, 2018. [Online]. Available: https://resources.infosecinstitute.com/topic/file-carving/.

[11] Science Direct, "Signature Analysis," 2017. [Online]. Available: https://www.sciencedirect.com/topics/computer-science/signature-analysis .

[12] R. Graham, "An Introduction to Hex Editing for Cybercrime Investigators," 2020. [Online]. Available: https://roderickshawngraham.medium.com/an-introduction-to-hex-editing-for-cybercrime-investigators-15041a1f3911.

[13] A. Chamberlain and H. B. Azhar, "Comparisons of Forensic Tools to Recover Ephemeral Data from iOS Apps Used for Cyberbullying," *The Fourth International Conference on Cyber-Technologies and Cyber-Systems,* pp. 88-93, 2019.

[14] T. Alyahya and F. Kausar, "Snapchat Analysis to Discover Digital Forensic Artifacts on Android Smartphone," *Procedia Computer Science,* vol. 109, pp. 1035-1040, 2017.

[15] Science Direct, "File System Analysis," 2018. [Online]. Available: https://www.sciencedirect.com/topics/computer-science/file-system-analysis.

[16] Kingo Root, "FAQ," 2017. [Online]. Available: https://www.kingoapp.com/faq.htm.

[17] N. Son, Y. Lee, D. Kim, J. James, S. Lee and K. Lee, "A study of user data integrity during acquisition of Android devices," *Digital Investigation,* vol. 10, pp. 3-11, 2013.

[18] Java Decompiler, "JD Project," 2013. [Online].

] Available: http://java-decompiler.github.io/.

[19] I. Blair, "14 Programming Languages for Mobile App Development," Build Fire, 2016. [Online]. Available: https://buildfire.com/programming-languages-for-mobile-app-development/.

[20] Forensics Digest, "Most Used Digital Forensics Tools," 2020. [Online]. Available: https://forensicsdigest.com/most-used-digital-forensic-tools/ .

[21] Privacy International, "A technical look at Phone Extraction," 2019. [Online]. Available: https://privacyinternational.org/long-read/3256/technical-look-phone-extraction .

[22] K. Paul, "Generic process model for smartphones live memory forensics," KCA University, 2014.

[23] M. Ntonja and M. Ashawa, "Examining artifacts generated by setting Facebook Messenger as a default SMS application on Android: Implication for personal data privacy," Cranfield University, 2019.

[24] C. Alisabeth and Y. R. Pramadi, "Forensic Analysis of Instagram on Android," IOP Conference Series: Materials Science and Engineering, 2020.

[25] A. Read, "Instagram Stories: The Complete Guide to Using Stories," Buffer, 2020. [Online]. Available: https://buffer.com/library/instagram-stories/.

[26] Instagram, "Introducing 'Recently Deleted'," 2021. [Online]. Available: https://about.instagram.com/blog/announcements/launch-of-ig-recently-deleted-media-folder.

[27] L. Zhang and Q. J. Fei Yu, "The Security Analysis of Popular Instant Messaging Applications," *International Conference on Computer Systems, Electronics and Control (ICCSEC),* pp. 1324-1328, 2017.

[28] S. Salter, "Storage and Privacy in the Cloud: Enduring Access to Ephemeral Messages," *Hastings Communications and Entertainment Law Journal,* vol. 32, no. 3, pp. 365-407, 2010.