10-2022

Disappearing Messages: Privacy or Piracy?

Áine MacDermott

Howard Heath

Alex Akinbi

10. Disappearing Messages: Privacy or Piracy?

Áine MacDermott
Liverpool John Moores University
a.m.macdermott@ljmu.ac.uk

Howard Heath
Merseyside Police, Digital Forensics Unit
howard.heath@merseyside.police.uk

Alex Akinbi
Liverpool John Moores University
o.a.akinbi@ljmu.ac.uk

Abstract

Disappearing messages is an optional feature available in popular applications for more privacy. The Telegram instant messenger application is a rival and alternative to the popular messaging application WhatsApp, with both applications citing end-to-end encryption for both messages and calls as a key offering. While Telegram doesn't officially have a 'disappearing message' feature like WhatsApp it still is possible to send disappearing messages using the secret chat functionality. In this paper, we analyse and evaluate 'disappearing messages' across Telegram and Snapchat to see whether they can be forensically preserved and/or recovered across Apple and Android operating systems. As these messages could be vital to investigations, with potential evidence and intelligence stored on them, not to mention the limited timeframe in which they are 'viewable' to the user, it is a great opportunity for digital forensic analysts to understand how they are stored, managed, and 'deleted' compared to traditional messages on the same platforms/applications.

Keywords: digital forensics, messages, privacy, security, telegram.

1. Introduction

Instant Messengers (IMs) are one of the most common ways of communicating in the modern world. With 2 billion active users, WhatsApp is the number one IM application, followed by the Chinese messaging app WeChat with 1.2 billion users and the Messenger app by Meta with close to 1 billion users (Statistica, 2022). While their underlying features are very similar, users are attracted to different applications for improved security and privacy. Applications that offer 'secure messaging' utilise end-to-end encryption which means that other parties (e.g., your Internet service providers (ISP), the app maker, the government) can't see your data and your messages. Telegram (Das, 2022) is cited as being one of the best messaging applications for secure encrypted messaging offering client-server encryption for standard chats. In addition, messages cannot be forwarded on the Telegram app to anyone by the recipient from secret chats.

Recently, Instagram and Facebook Messenger have introduced 'secure messaging' options on their platforms, such as 'Disappearing Photo/Video' on Instagram (Instagram, 2022) and 'disappearing messages' listed as 'Secret Mode' on Messenger (Facebook, 2022). Meta was not the first to offer such measures to improve users' privacy matters, as Snapchat had these features included by default since its launch in 2011 (Wikipedia, 2022), and WhatsApp's main rival Telegram was later released in 2013 (Telegram, 2022). However, despite these apparent privacy safeguards, just how private are these 'secret/disappearing messages' on these platforms, and are they truly secure? At present, the only known ways of being able to preserve these 'disappearing' messages as evidence are as follows:

- Screenshotting the messages using the device (which is not forensically sound/contains time constraints)

- Photographing the device in which the messages are displayed (which imposes time constraints and yields no metadata)
- Replying to a message (which is not forensically sound and imposes time constraints)
- Extracting a backup from the Cloud (which is subject to legal issues surrounding cloud forensics, and does not guarantee that the message will not expire upon extraction)

Currently, of all the above, photographing the device while it displays these messages is the most effective means of providing evidence. However, we argue that even this method is subject to several further issues such as:

- The state of the device (damage, powered off)
- Security measures (passwords, hidden/secure areas)
- Network access (in network isolation, the device may not be able to retrieve messages from servers i.e., Snapchat)
- Outdated applications (some apps require verification by synchronizing to a server after being disconnected i.e., WhatsApp).

Disappearing messages present an increase in risk to all cases involving modern technology and set a hard timeframe for the investigators to adhere to, with many cases to balance and high-risk cases taking priority. With other risks involved in the mobile forensic process, such as password/PIN protection, encryption, and data sizes, any hindrance to the investigation, such as the mobile device requiring a PIN/password (with the suspect being non-compliant), alongside other issues (e.g., compatibility problems and/or extraction length) result in no time remaining for analysis and potentially unrecoverable messages.

Our study aims to find the most forensically sound and effective manner for capturing the data, and being able to present it as credible evidence. We explore Telegram and Snapchat, as Telegram is a popular alternative to WhatsApp, and Snapchat has disappearing messages by default. These two applications will also be used to compare the separate ways in which messages can 'disappear', answering the following research questions: *Can these messages be forensically recovered and/or secured? Are these messages truly secret?* Our results and analysis will provide reliable and repeatable means to recover these messages for digital forensics investigators; specifically, whether they can be recovered and preserved, and whether they pose a challenge to criminal investigations for digital forensic investigators in the field.

2. Related Works

While there are related works exploring the forensic analysis of Snapchat and Telegram the works are dated and not within our scope of the investigation - analysing the features of the disappearing message. Alyaha and Kausar (2017) focus on the analysis of Snapchat and its artefacts via an Android smartphone. Their methodology is simplistic, by following the process of population > acquisition > examine > report. While they do state how many data artefacts they have created on the device, they do not provide any details for these artefacts beyond a categorisation such as "photo", "video", and "message". They locate the cache directory, main databases, and Snapchat folder which provides limited artefacts back; namely the messages and received images. From their findings, they recovered little in deleted artefacts, retrieving only one deleted story photo. However, they did recover the chat database which contained some messages (26 of the 36 sent – 11 of which were duplicates). The duplicate files were due to files having existed in multiple directories. They concluded that deleted snaps were not recoverable. As we are focusing on the disappearing side of these messages, it would

have been useful to have provided a better insight as to why these messages were not presented, and whether any changes in the methodology would have changed this outcome.

Anglano et al. (2017) focuses on the forensic analysis of the Telegram messenger application on an Android smartphone. Their contributions are twofold; the creation of a methodology for the forensic analysis of Android-based IM Applications, and a thorough analysis of the Telegram messenger's artefacts (their structure, formatting, message data, etc). Their methodology revolves around a series of experiments, where user actions are performed and how this changes the extractable artefacts and investigations results are analysed. The experiments are varied and cover all aspects of the application's features, but the main contribution of the work is the analysis of secret chats (Anglano et al., 2017). From their findings, Telegram stores 'secret chat' messages in a separate table on the database, under "enc_chats". From here, they were able to discern distinct characteristics regarding these chats, such as: 'Chat ID (uid)', 'TDS Encrypted Chat (data)', 'Username of the owner (user)' and 'Name of the secret chat (name)'. From here, they were then able to dissect the TDS Encrypted down into a structure containing the following: 'ID of the chat (id)', 'TID of the secret chat partner (admin_ID)', 'Creation date/time of the secret chat (date)' and 'TID of users who join the chat (participant_ID)'.

Azhar & Barton (2016) conducted a forensic analysis of Wickr and Telegram in an attempt to recover artefacts removed by the ephemeral (disappearing) functions. Results from their experiment showed that disappearing messages set using the self-destruct timer were not successfully recovered from the digital forensic remnant for both apps. However, they were able to recover expired image files associated with the Telegram application from the cache directory on the Android device's physical image. Son et al. (2020) conducted a forensic analysis of instant messengers that also have disappearing messaging features including Signal, Wickr and Threema. The focus of their study was on the successful decryption and relevant forensic artefacts that could be recovered from the encrypted SQLCipher databases used by these instant messaging applications. Similarly, studies by Kim et al. (2020) and Kim et al. (2021), also focused on forensic analysis of ephemeral instant messengers, Telegram X, BBM-Enterprise and Wickr respectively, although the focus of both investigations were limited to the decryption of encrypted databases and not the recovery of disappearing messages. To the best of our knowledge, there has been no recent study that has focused on the successful recovery of disappearing messages for Telegram and Snapchat messaging apps on both iOS and Android devices. Therefore, by focusing on the recovery of disappearing messages, we can make the most of the potential investigative impact of our work.

3. Methodology and Experiments

Given that the goal of any forensic analysis is to allow the analyst to obtain the digital evidence generated by the applications under consideration, the methodology we adopted allowed completeness, repeatability, and generality (Anglano et al., 2017, Akinbi & Ojie, 2021). As the 'disappearing messages' trend is particularly new there are (at the time of writing) no viable reports to review and compare against our own set of results. We will use a Samsung S6 (Android 7 OS) and an Apple device (iOS 12.1). The results of the devices will be compared to provide an insight into how both operating systems handle the data differently. We created an investigative scenario followed by subsequent phases, "Installation of application" and "Design of experiments" respectively for each application. We installed and ran Telegram v 8.5.1 and Snapchat v 11.64.0.36.

In the "Design of experiments" phase, we define a set of experiments that involve using the applications, creating photos and videos using the camera, sending and downloading messages.

To ensure we knew what data should be present on the device we created a table of sample data, as well as interactions made with the device during the population period. This is useful as we can audit and log what data was seeded, to ensure that the data extracted could be cross-examined and checked for accuracy. Table 1 shows the types of media messages supported by the apps. Four images and four videos have been created, two of each on both devices. Audio and files have been excluded from the media used on the premise that we believe they will act in the same way as images and videos. Locations and contacts have been excluded from the media available, due to limitations in GDPR regarding personal information. The extraction of data from the mobile applications was completed using the tools: UFED' 4PC, and MSAB's XRY.

Application	Texts/Chats	Images	Video	Audio/Voice	Files	Location	Contacts
Telegram	✓	✓	✓	✓	✓	✓	✓
Snapchat	✓	✓	✓	✓	x	✓	✓

Table 1: Types of media supported by Telegram and Snapchat

We split the experiments into two test groups: *Snapchat Messages* and *Telegram Secret Chat*. 'Snapchat Messages' will be a comparison and test to see whether Snapchat messages can be recovered via forensic means by performing a standard mobile extraction on the device with both 'unsaved' and 'saved' messages on Snapchat. It will also determine what data can be brought back from the application from extractions, and how Snapchat deals with disappearing messages. 'Telegram Secret Chat' will be a comparison and test to see whether Telegram's 'Secret mode' messages can be recovered via forensic means by performing a standard mobile extraction on the device. It will also determine what data can be brought back from the application from extractions, and how Telegram deals with disappearing messages.

3.**1 Snapchat Messages**

Using the Snapchat application, we compared "disappearing by default" and "decisive disappearing" where Snapchat automatically deletes messages unless they are specifically saved by the user via tapping on them. The iPhone extraction was not able to extract any Snapchat data other than the application files, as seen below under the "toyopagroup.picaboo" (Figure 1) application name.

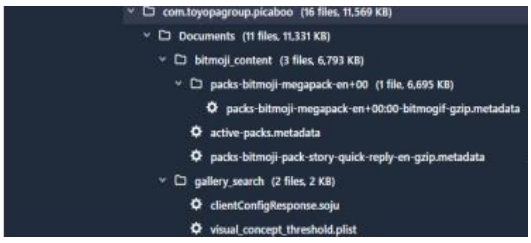

Figure 1: iPhone File System Snapchat

The Samsung phone managed to recover most of the chat data regardless of whether the messages were saved or unsaved (minus 1 timed photo, and 2 videos) as shown in Figure 2.

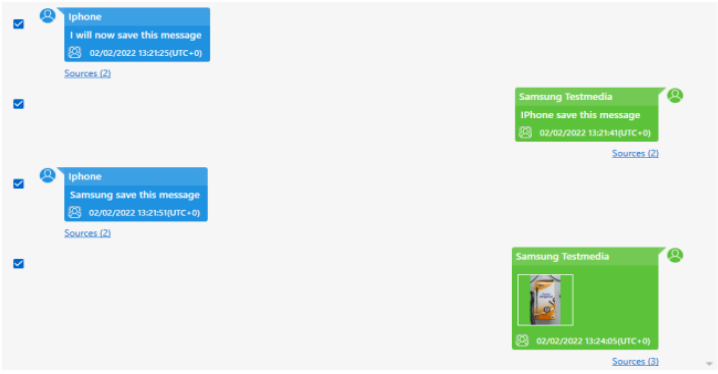

Figure 2: Samsung Snapchat Chats

By creating an Autopsy case and placing the extracted .com files out of the UFED extraction, a database known as "arroyo.db" (found in */com.snapchat.android/databases)* contained the data for the conversation shown above. Further work would have to be conducted to translate the BLOB data into messages using a hex viewer and decoder, images, or videos to see whether the missing data could still be recovered.

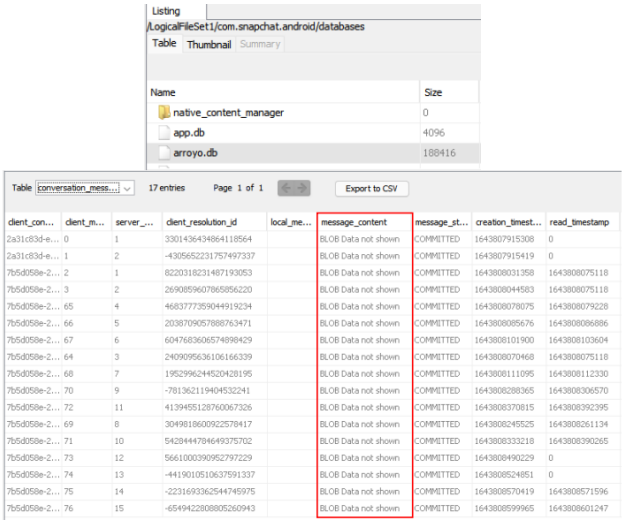

Figure 3: Autopsy "Arroyo.db"

3.2 Telegram Chats

We created two Telegram chats: a "regular chat" and a "secret messages" chat which enables

disappearing messages. Neither of these Telegram chats were extracted in either pre or post-expiry extraction on the iPhone. The only data retrieved was the application data as shown in Figure 4.

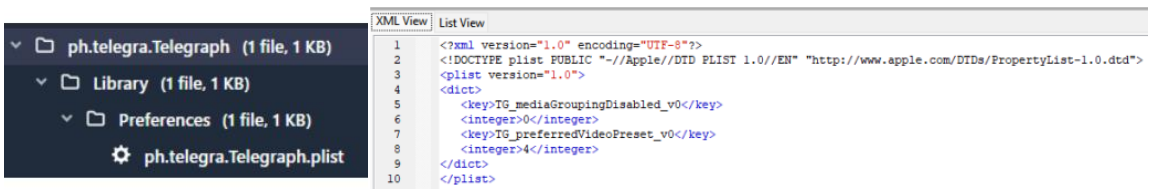

Figure 4: iPhone Telegram File System and plist details

When opened, the “preferences.plist” contained no data regarding disappearing messages. In both Samsung extractions, the regular chat was extracted without issue, showing both messages – Figures 5 and 6. Limited data were extracted from the secret chats in both extractions but the metadata was incorrect, showing “15/05/2015”.

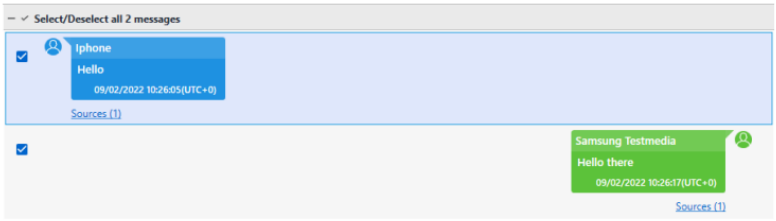

Figure 5: Telegram Samsung regular chats

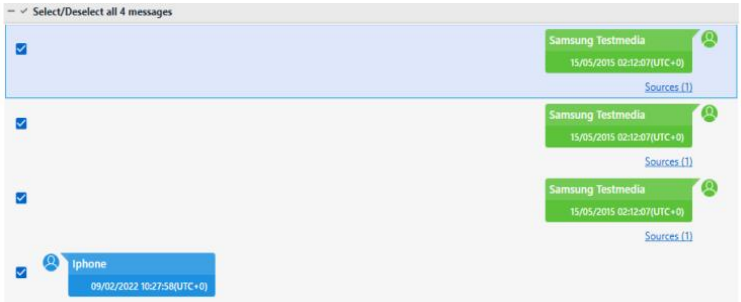

Figure 6: Telegram Samsung Secret Chats

The wrong metadata was surprising, so we investigated further to see where the data had been extracted from (as shown in Figure 7). As identified, we opened “Cache4.db” located within the Telegram “files” folder.

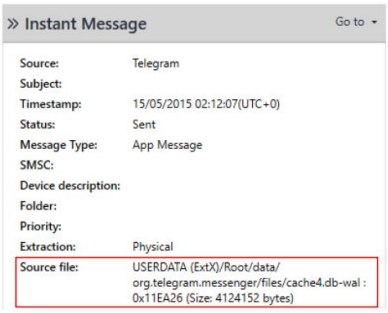

Figure 7: Storage Location Telegram Chats Samsung

As shown in Figure 8, the data has not been parsed correctly and there are fragments of data contained within the “data” column of the table “messages_v2”. By converting the time into “Seconds from UTC

1970” the correct metadata times are now shown – see Figures 9 and 10. Using the in-built hex editor, the hex data shows some of the message contents that were sent.

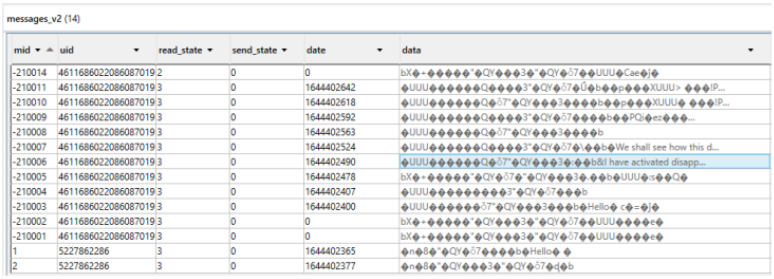

Figure 8: "Cache4.db" messages_v2 table

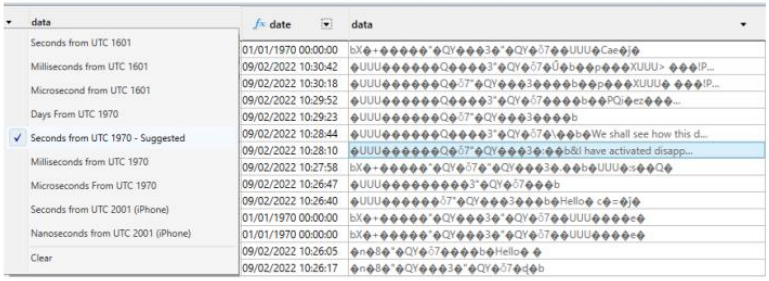

Figure 9: Date conversion

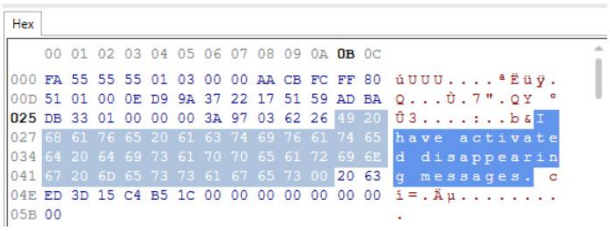

Figure 10: Cache4.db hex editor

Another piece of evidence found was the file path of the images that had been sent through the “secret chat” (Figure 11) within the hex.

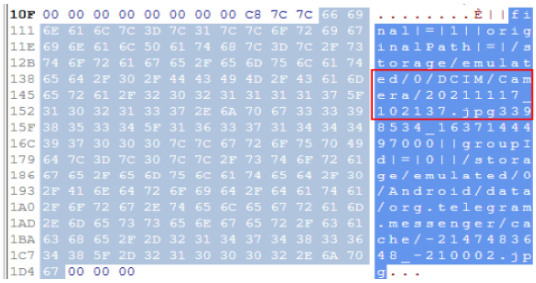

Figure 11: File paths from hex

Using this, and the Cellebrite search tool, “221117_102137.jpg” returned a result on both the pre and post-extractions, showing the original image as shown in Figure 12. It is clear that Cellebrite has not accurately parsed the data and further follow-up testing should be conducted to see whether this is a recurring issue. However, manual data can be extracted using the above techniques to retrieve incorrectly parsed artefacts. Not all artefacts may be available, as deleted messages and video messages were not recovered.

Figure 12: File path photo

4. Analysis and Significance of Findings

Within this section, we analyse and present the significance of our findings. We highlight the main findings from our Snapchat experiments, and Telegram experiments, and then compare Snapchat and Telegram.

Snapchat: A series of messages were sent/received between the two devices. When examining the iPhone, no data could be forensically recovered from the device, besides the installation of the application on the device. These results highlight sanitization of data within Snapchat, which in turn, poses an issue for forensic investigations. However, the same data when examined on the Samsung was almost completely retrievable (aside from 3 artefacts); showing that Snapchat for Android has a poor data sanitization procedure, alongside Telegram. Whether this is due to Samsung’s physical extraction or down to the specific hardware/software of the device in a forensic investigation is unclear, however, an Android device is likely to provide more data due to this. Overall, forensically analysing Snapchat for iOS should be conducted manually first (if possible) before attempting to conduct a logical extraction. For Android, a physical extraction (if possible) is the best available method for the extraction of Snapchat artefacts.

Telegram: Telegram was used on both devices to send/receive a series of messages and media. On the iPhone data was completely irretrievable, both pre and post-expiry; showing that Telegram for iOS has a commendable sanitization procedure. However, on Samsung, the examination of the device, while not as straightforward as the Snapchat examination did contain some artefacts from the experimental data. This required a manual review of the Telegram application files and even browsing hex-data

contained within the BLOB entries. Telegram's data sanitization for Android is inconsistent but is better than Snapchat. Overall, a manual review of Telegram for iOS may be required before conducting any extractions. This would ensure that data residing on the device is captured before attempting to retrieve (and potentially lose) more data via an extraction. Regarding Android, a physical extraction is the best available extraction and the examiner should ensure that they verify and review the associated database files and data.

Snapchat vs Telegram: both Telegram and Snapchat share similar results. These are presented in more detail within Tables 3-6 below. The iOS retains no artefacts on either application (besides the basic installation files), whereas Samsung has a greater potential for the recovery of artefacts across both extractions. From a forensic perspective, Snapchat provides the examiner with an 'easier' extraction, without the need for manually reviewing database files, as well as the near complete recovery of artefacts, making Snapchat an easier application to analyse. Each of the tables below contains the results of each group testing, supplying an easy-to-read graphic of what data persists pre and post "disappearing".

Key	Meaning
Y	Data was fully retained and parsed
N	Data was missing/not extracted
/	Data was partially available/parsed

Table 2: Key explanation

Snapchat Extraction, Device: iPhone 6s

Tool Used: UFED 4PC

Extraction(s): Logical & Advanced Logical

Date/Time added	Sent/Received?	Data description	Cellebrite Recoverable?
02/02/2022 13:21	Received	"Hello"	N
02/02/2022 13:21	Received	"This is a test of the disappearing messages"	N
02/02/2022 13:21	Sent	"I will save this message" – iPhone saved	N
02/02/2022 13:21	Sent	"Hello"	N
02/02/2022 13:21	Sent	"I will now save this message"	N
02/02/2022 13:21	Received	"iPhone save this message" – iPhone saved	N
02/02/2022 13:21	Sent	"Samsung save this message" – Samsung saved	N
02/02/2022 13:23	Received	Photo of BIC pen – Saved by iPhone	N
02/02/2022 13:23	Received	Timed (10s) photo of screwdriver	N
02/02/2022 13:25	Sent	Photo of evidence tape – Replayed & saved by Samsung	N
02/02/2022 13:26	Sent	Timed (10s) photo of duct tape	N
02/02/2022 13:28	Sent	Photo of screwdriver	N
02/02/2022 13:28	Received	Photo of screwdriver	N
02/02/2022 13:29	Received	"This message will not be saved"	N
02/02/2022 13:90	Sent	"Neither will this"	N

Table 3: Snapchat extraction of iPhone 6s

Snapchat Extraction, Device: Samsung S6

Tool Used: UFED 4PC

Extractions(s): Physical (decrypted bootloader) – Full file system

Date/Time added	Sent/Received?	Data description	Cellebrite Recoverable?
02/02/2022 13:21	Received	"Hello"	Y
02/02/2022 13:21	Received	"This is a test of the disappearing messages"	Y
02/02/2022 13:21	Sent	"I will save this message" – iPhone saved	Y
02/02/2022 13:21	Sent	"Hello"	Y
02/02/2022 13:21	Sent	"I will now save this message"	Y
02/02/2022 13:21	Received	"iPhone save this message" – iPhone saved	Y
02/02/2022 13:21	Sent	"Samsung save this message" – Samsung saved	Y
02/02/2022 13:23	Received	Photo of BIC pen – Saved by iPhone	Y
02/02/2022 13:23	Received	Timed (10s) photo of screwdriver	/ (Blank message)
02/02/2022 13:25	Sent	Photo of evidence tape – Replayed & saved by Samsung	/ (Video file missing)
02/02/2022 13:26	Sent	Timed (10s) photo of duct tape	/ (Video file missing)
02/02/2022 13:28	Sent	Photo of screwdriver	Y
02/02/2022 13:28	Received	Photo of screwdriver	Y
02/02/2022 13:29	Received	"This message will not be saved"	Y
02/02/2022 13:90	Sent	"Neither will this"	Y

Table 4: Snapchat extraction Samsung S6

Telegram Secret Chat Messages, Device: iPhone 6S

Tools used: UFED 4PC

Extraction(s): Logical & Advanced Logical

Date/Time added	Sent/Received	Data Description	Cellebrite Pre-Disappearing?	Cellebrite Post-Disappearing?
09/02/2022 10:26	Sent - (non-disappearing)	"Hello"	Y	Y
09/02/2022 10:26	Received - (non-disappearing)	"Hello there"	Y	Y
09/02/2022 10:28	Sent	"I have activated disappearing messages"	/ (Required manual hex viewing)	/ (Required manual hex viewing)
09/02/2022 10:28	Received	"We shall see how this does"	/ (Required manual hex viewing)	/ (Required manual hex viewing)
09/02/2022 10:29	Sent	"Have a photo" PHOTO 2 attached	/ (Required manual hex viewing)	/ (Required manual hex viewing)

09/02/2022 10:29	Received	PHOTO 1 sent	/ (Required manual hex viewing)	/ (Required manual hex viewing)
09/02/2022 10:30	Sent	VIDEO 2 attached	N	N
09/02/2022 10:30	Received	VIDEO 1 sent	/ (Blank message)	/ (Blank message)
09/02/2022 10:30	Sent	“Can you delete messages?”	N	N
09/02/2022 10:31	Received	“I will also delete this message”	N	N

Table 5: Telegram extraction iPhone 6S

Telegram Extraction, Device: Samsung S6

Tools used: UFED 4PC

Extraction(s): Extraction: Physical (decrypted bootloader) – Full File System

Date/Time added	Sent/Received	Data Description	Cellebrite Pre-Disappearing?	Cellebrite Post-Disappearing?
09/02/2022 10:26	Sent - (non-disappearing)	“Hello”	N	N
09/02/2022 10:26	Received - (non-disappearing)	“Hello there”	N	N
09/02/2022 10:28	Sent	“I have activated disappearing messages”	N	N
09/02/2022 10:28	Received	“We shall see how this does”	N	N
09/02/2022 10:29	Sent	“Have a photo” PHOTO 2 attached	N	N
09/02/2022 10:29	Received	PHOTO 1 sent	N	N
09/02/2022 10:30	Sent	VIDEO 2 attached	N	N
09/02/2022 10:30	Received	VIDEO 1 sent	N	N
09/02/2022 10:30	Sent	“Can you delete messages?”	N	N
09/02/2022 10:31	Received	“I will also delete this message”	N	N

Table 6: Telegram extraction Samsung S6

5. Conclusion

Disappearing messages have a severe impact on digital forensics due to the time-sensitivity involved, as well as investigative inexperience with this new and evolving technology. With criminals requiring new ways to hide their crimes, and leaving no trail of evidence, they may indeed turn to disappearing messages to achieve this. Although a users right to privacy is not openly investigated within these experiments, the findings will help investigators determine the most appropriate way in which data could be retrieved, reviewed and preserved. For example, informing and training both technical and non-technical staff about disappearing messages and ensuring both sides are aware of the risks and impact which they may have on the investigation is the first step to ensuring that disappearing messages are dealt with correctly. In cases where disappearing messages are present on the device, a manual

review should be performed at the earliest priority, ensuring a photograph of the screen (showing the expiring messages) is taken, which will allow for both evidence of the messages existing, as well as potentially verifying any post-expiry messages within the data verification stage of the examination. In cases where messages have not yet expired or have just expired, there is still potential for evidence to be recovered using extractions where deleted data can be recovered (such as file system and physical extractions).

However, both applications are somewhat competent for the thorough sanitation of data, which impacts potential forensic investigations being able to retrieve and accurately verify data's integrity, for admission to court as evidence. Of our investigated apps, Snapchat is the most destructive for potential evidence, whereas iOS devices would have to be subject to a manual review, and Android physicals could retrieve all the necessary artefacts required for admissible evidence. With Telegram incomplete data was the best extraction possible within our report, providing minimal artefact evidence.

Cloud extractions were not supported by Cellebrite Cloud Analyzer for either Snapchat or Telegram at the time of writing. This testing group and its limited data have shown that Cloud extractions are not a valid replacement for traditional mobile forensics as they currently stand and pose an unnecessary risk in the potential loss of data and evidence by breaking the traditional forensic practice of network isolation. Following this, the legal issues and complications in the retrieval of credentials provides further evidence that this methodology is best reserved as a "last resort" in gaining evidential data.

References

Akinbi, A. and Ojie, E., 2021. Forensic analysis of open-source XMPP multi-client social networking apps on iOS devices. Forensic Science International: Digital Investigation, 36, p.301122. https://doi.org/10.1016/j.fsidi.2021.301122

Alyahya, T. and Kausar, F., (2017) Snapchat Analysis to Discover Digital Forensic Artifacts on Android Smartphone. Procedia Computer Science, 109, pp.1035–10407

Anglano, C., Canonico, M. and Guazzone, M., (2017) Forensic analysis of Telegram Messenger on Android smartphones. Digital Investigation, 23, pp.31–49.

Azhar, M. and Barton, T., 2016. Forensic Analysis of Secure Ephemeral Messaging Applications on Android Platforms. Global Security, Safety and Sustainability - The Security Challenges of the Connected World, pp.27-41. https://doi.org/10.1007/978-3-319-51064-4_3

Das, A. 10 Most Secure and Encrypted Messaging Apps In 2022 (Android & iOS): Keeping Privacy Intact In the age of Internet Surveillance with These Secure Messaging Apps. Retrieved 03 March 2022. Available at: https://fossbytes.com/best-secure-encrypted-messaging-apps/

Facebook (2022) How do I start a secret conversation? | Messenger Help Centre. Retrieved 25th January 2022. Available at: https://www.facebook.com/help/messenger-app/811527538946901?cms_platform=androidapp&helpref=platform_switcher

Instagram (2022) How do I send a disappearing photo or video on Instagram? | Instagram Help Centre. Retrieved 23rd January 2022. Available at: https://help.instagram.com/1310346208996329

Kim, G., Kim, S., Park, M., Park, Y., Lee, I. and Kim, J., 2021. Forensic analysis of instant messaging apps: Decrypting Wickr and private text messaging data. Forensic Science International: Digital Investigation, 37, p.301138. https://doi.org/10.1016/j.fsidi.2021.301138

Kim, G., Park, M., Lee, S., Park, Y., Lee, I. and Kim, J., 2020. A study on the decryption methods of telegram X and BBM-Enterprise databases in mobile and PC. Forensic Science International: Digital Investigation, 35, p.300998. https://doi.org/10.1016/j.fsidi.2020.300998

Menahil, A., Iqbal, W., Iftikhar, M., Shahid, W.B., Mansoor, K. and Rubab, S., 2021. Forensic Analysis of Social Networking Applications on an Android Smartphone. Wireless Communications and Mobile Computing, 2021.

Snapchat Inc., (2022) Snap Inc. Retrieved 16th March 2022. Available at: https://investor.snap.com/news/news-details/2022/SnapInc.-Announces-Fourth-Quarter-and-Full-Year-2021-Financial-Results/default.aspx

Son, J., Kim, Y., Oh, D. and Kim, K., 2022. Forensic analysis of instant messengers: Decrypt Signal, Wickr, and Threema. Forensic Science International: Digital Investigation, 40, p.301347. https://doi.org/10.1016/j.fsidi.2022.301347

Statista (2022) Most popular messaging apps | Statista. Retrieved 23rd January 2022. Available at: https://www.statista.com/statistics/258749/most-popular-global-mobile-messenger-apps/

Telegram (2022) The Evolution of Telegram. Retrieved 23rd January 2022. Available at: https://telegram.org/evolution#2013

Wikipedia (2022) Snapchat - Wikipedia. Retrieved on 20th February 2022. Available at: https://en.wikipedia.org/wiki/Snapchat