



Contents lists available at [ScienceDirect](#)

Forensic Science International: Digital Investigation

journal homepage: www.elsevier.com/locate/fsidi



Forensic analysis of ephemeral messaging applications: Disappearing messages or evidential data?

Howard Heath ^a, Áine MacDermott ^{b,*}, Alex Akinbi ^c

^a Merseyside Police Digital Forensics Unit, UK

^b School of Computer Science and Mathematics, Liverpool John Moores University, UK

^c Department of Computing and Mathematics, Manchester Metropolitan University, UK



ARTICLE INFO

Article history:

Received 2 September 2022

Received in revised form

27 May 2023

Accepted 30 May 2023

Available online 19 June 2023

Keywords:

Anti-Forensics

Digital forensics

Disappearing messages

Ephemeral messaging

Mobile forensics

Messaging application

ABSTRACT

Ephemeral messaging or 'disappearing messages' is the mobile-to-mobile transmission of multimedia messages that automatically disappear from the recipient's screen after the message has been viewed. This new feature can be enabled by users for more privacy when using instant messaging apps. A user can set messages to disappear within a certain timeframe: 24 hours, 7 days, or 90 days, after the time they are sent. While disappearing messages provide additional privacy to users, its anti-forensics capability creates challenges for investigators in the recovery of evidential artefacts that could be crucial to an investigation. In this paper, we conduct a comprehensive forensic analysis of 'disappearing messages' across different digital platforms (mobile, desktop, and cloud) and instant messaging apps (WhatsApp, Snapchat, and Telegram) to determine whether they can be recovered within a limited timeframe. The results from this study provide valuable information to investigators dealing with instant messaging apps that have this feature enabled and provides detailed understanding of how disappearing messages are stored, managed, and deleted compared to messages sent without this feature enabled.

© 2023 The Authors. Published by Elsevier Ltd. This is an open access article under the CC BY-NC-ND license (<http://creativecommons.org/licenses/by-nc-nd/4.0/>).

1. Introduction

Instant Messengers (IMs) are one of the most common ways of communicating in the modern world. Statista quotes the most popular Messaging Apps of October 2021 are WhatsApp, Facebook Messenger, and WeChat ([Statistica, 2022](#)). The first two are child companies of the parent group Meta. The rise of instant messages can be contributed to the inexpensiveness of internet communication over traditional SMS messages. Whilst texting over SMS requires a SIM card, credit, and a phone; IMs only require access to the internet, with an applicable device, and an account – which is usually free. With the surge of free Wi-Fi hotspots and no ties to a contract or a SIM, IMs allow almost any user to access these applications and begin communicating with little effort.

Following this, WhatsApp has over two billion active users since March 2020, just over 25% of the world's population ([United Nations, 2022](#)). In digital forensics capturing communication between two suspects, or a suspect and a victim, can be crucial in providing evidence for criminal investigations. With over one

hundred billion messages being sent through one application alone per day, it makes the collection of said messages ever more crucial. Therefore, this communication needs to be readily available to a digital forensic investigator, by making it easy to locate, preserve, analyse, and report upon. Regulations surrounding GDPR (General Data Protection Regulations), and the DPA (Data Protection Act) of 2018, mean privacy around user data has become an ever-increasing issue. Users are now more conscious than ever about their personal data and looking for more secure ways to protect their data.

In November 2020, WhatsApp released 'Disappearing Messages' for their platform. These messages allowed users to set an expiry timer on their message for 7 days. In 2023 this has now been set to allow for 24 hours, 7 days, or 90 days, based on the user's preference. WhatsApp states that this feature is for the privacy of its users ([WhatsApp, 2022](#)), having already boasted about being end-to-end encrypted. Other popular applications such as Instagram and Facebook Messenger (Messenger) (part of the bigger Meta family) also recently adopted 'disappearing messages', listed as Disappearing Photo/Video' on [Instagram \(2022\)](#) and 'Secret Mode' on Messenger ([Facebook, 2022](#)).

However, Meta was not the first to introduce such measures

* Corresponding author.

E-mail address: a.m.macdermott@ljmu.ac.uk (MacDermott).

regarding users' privacy matters, as Snapchat ([Snapchat Inc, 2022](#)) had these features included by default since its launch in 2011 ([Awrara, 2020](#)), and WhatsApp's main rival Telegram later released in 2013 ([Telegram, 2022](#)). Just how secret are these 'secret/disappearing messages' on these platforms, and are they secure? One of these questions can be answered with WhatsApp's and Telegram's declarations that there are ways of preserving these messages beyond the chat ([Das, 2022](#)). However, these known methods – replying to, forwarding, or otherwise altering the original data in an attempt to preserve the data – are not forensically sound, and would in turn violate the ACPO guidelines. WhatsApp states that if you reply to a disappearing message, the quoted text might remain in the chat after the duration you select. Also, if a disappearing message is forwarded to a chat with disappearing messages off, the message won't disappear in the forwarded chat. For example, it's possible for someone to forward or take a screenshot of a disappearing message and save it before it disappears. To copy and save content from the disappearing message before it disappears, or to take a photo of a disappearing message with a camera or other device before it disappears ([WhatsApp, 2022](#)). These aforementioned methods are in place to ensure messages remain private, and however only being viewable between the creator and the intended recipients cannot be 100% guaranteed, with the idea that messages may be screenshotted on Telegram or WhatsApp (with Telegram alerting you), or quoted via reply or forwarding, saved to the device, or photographed for WhatsApp. This declaration from both companies then begs the further question: *Can these messages be forensically recovered and/or secured?*

These questions are why we have chosen to research these ephemeral messaging applications and their disappearing message methods, to see whether they truly are secret, whether they can be recovered and preserved, and whether they pose a threat to criminal investigations for digital forensic investigators in the field. The key contribution of this paper is that we aim to see how the disappearing messages methods differ between the three applications and provide reliable and repeatable means to recover these messages for digital forensics practitioners. At the time of original publication, neither Cellebrite nor XRY had official support for the preservation or recovery of disappearing messages. Since the experiments, official support is now available for the recovery of disappearing messages. We will be reviewing the current research into the following mobile applications: WhatsApp, Snapchat, and Telegram. Our reasoning for these three applications is that WhatsApp holds the largest audience as seen from the statistics in this section, Telegram is a popular alternative to WhatsApp, and Snapchat was the first to introduce this level of privacy within instant messaging applications.

The research questions to be addressed are as follows:

1. Are 'disappearing messages' forensically recoverable and/or preservable?
2. How do 'disappearing messages' work?
3. What impact could this have on a criminal investigation for a forensic investigator?

This paper seeks to answer the question of how digital forensic investigators can better understand the state of ephemeral messaging, by performing a series of tests on a variety of operating systems such as Android, Apple, and Windows. We also set ourselves on to evaluate the effectiveness of some of the most popular forensic software available to forensic practitioners like Cellebrite's UFED 4 PC, MSAB's XRY, and Magnet's AXIOM, to see if different tools and their available extractions produce differing results. This paper ultimately aims to establish a base knowledge for forensic practitioners to perform forensic examinations of ephemeral

messages from our findings, so that they can achieve the best possible evidence in their reports. The remainder of this paper is outlined as follows: In Section 2 we identify related literature and how this research identifies the gaps in knowledge. Our analysis methodology and tools are presented in Section 3, and experiments and analysis are detailed in Section 4. In Section 5 a discussion of results is presented, with concluding remarks in Section 6. Test data is included in the Appendix.

2. Related literature

This paper attempts to address the gap in the literature on forensic analysis and extraction of disappearing messages and message timer features. We will be looking primarily at WhatsApp, as it is the most popular messaging application. We will also explore Snapchat and Telegram; Telegram is a popular alternative to WhatsApp, and Snapchat has disappearing messages by default. These applications will be used to compare the separate ways in which messages can 'disappear'.

Notable works exploring WhatsApp include [Anglano \(2014\)](#). The authors explore the WhatsApp artefacts recoverable by the investigator in a digital forensic investigation, and the correlation of these artefacts to infer user-actions made on the device. The report provides solid framework for further research to be conducted in disappearing messages, with traditional message artefacts having been examined thoroughly and having provided a good oversight into the structure of WhatsApp on Android devices. [Alyahya and Kausar \(2017\)](#) focuses on the analysis of Snapchat and its artefacts via an Android smartphone. From their findings they recovered little in deleted artefacts, with only one deleted story photo. However, they did recover the chat database, which contained some messages, being twenty-six overall messages of the thirty-six sent – eleven of which were duplicates. They also concluded that deleted snaps were not recoverable. As we are focusing upon 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 their methodology would have changed this outcome.

[Azhar and Barton \(2016\)](#) conducted a forensic analysis of Wickr and Telegram 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. [Anglano et al. \(2017\)](#) focuses upon the forensic analysis of the Telegram Messenger application on an Android smartphone. They present a thorough analysis of Telegram messenger's artefacts, their structure and formatting, and how to recover vital information such as contact lists, messages and their data, and call logs. From their findings, Telegram stores 'secret chat' messages in a separate table on the database, under "enc_chats".

[Son et al. \(2022\)](#), conducted a forensic analysis of instant messengers that also have disappearing messaging features including Signal, Wickr and Threema. However, 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, the focus of both investigations were limited to the decryption of encrypted databases and not the recovery of disappearing messages.

Therefore, by focusing on the recovery of disappearing

messages, we make the most of the potential investigative impact of our work. To the best of our knowledge, there has been no recent study that has focused on the successful recovery of disappearing messages on WhatsApp, Telegram and Snapchat messaging apps on both iOS and Android devices. This research will help influence digital forensic investigations in their decision-making process to counter disappearing messages that they will meet within their investigations.

3. Analysis methodology and tools

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 and Ojie, 2021). We created an investigative scenario followed by subsequent phases, "Installation of application" and "Design of experiments" respectively for each application. In the "Installation of application" stage, we installed and ran WhatsApp v 2.21.221 (and other variations required per group: 2.21.23.23, 2.21.243, 2.21.24.22, 22.2.75, 2.22.2.73, 2.21.23.23), Snapchat v 11.64.0.36 and v 11.64.0.38, and Telegram v 8.5.1. **Table 1** summarizes the profiles and test devices that were used.

Cellebrite UFED & Physical Analyzer (including UFED Cloud Analyzer) 7.50.0.137 - 7.52.0.152 will be our main tool for mobile extractions on both the iOS and Android device, as well as utilised for our Cloud extractions. MSAB XRY & XAMN 9.6.1 will be used on both the Apple iPhone and Samsung S6 for extractions, to compare and verify the findings that were found on UFED. XRY, like UFED can extract, analyse, and report data using its built-in analyser and parsers, while also allowing the user to browse the databases manually. DB Browser SQLite 3.12.2 will be used to open, edit, and view SQLite databases. The tool is useful for forensic investigators who require access to the.db files that are common in smartphones and tablets. FTK Imager will be used for the imaging process of group 5 (WhatsApp Desktop). Using FTK Imager we can drag-and-drop the virtual disk image (VDI) file into to create a forensically sound image of the drive. This in turn will then allow us to analyse the data within Autopsy. AXIOM Process & Examine 5.6.0.26839 will be used to sift through and analyse RAM data from memory dumps (Group 5).

The results of the devices will be compared, to provide an insight into how both operating systems handle the data differently. Our analysis methodology provides the possibility for the experiments to be generalized, replicable and reproduced by a third party under the same operational conditions, and to obtain the same results regardless of the iOS version and iPhone model.

3.1. Design of experiments

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, and switching between different network modes. This is to generate as many forensic artefacts as possible and to demonstrate a typical user's realistic interaction with these applications and their message features. Specifically, we required the devices to be populated

Table 1
Test devices.

Device	OS Version
Samsung S6	Android 7
iPhone 6s	iOS 12.1

with sample data, so that we could extract this during our testing to see whether the messages were still present on the device, or whether they had indeed 'disappeared'. **Table 2** shows the types of media messages supported by the apps.

A selection of media has been created to fully comprehend the limits and workings of disappearing messages. To ensure that 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, to be able to audit and log what data was seeded, and when, to ensure that the data extracted could be cross-examined, and checked for accuracy. To ensure that the data on the device could not be tampered with or accidentally modified, deleted, or otherwise interacted with between extractions and testing, we utilised network isolation as is standard within digital forensic investigations. In the case of UFED Cloud extractions, network isolation was exempt, as a required Wi-Fi connection was required for the extraction to be successful and was always monitored whilst connected.

3.2. Testing groups

Four images and four videos have been created, two of each on both devices, to use in the below group tests. 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 tables for data seeding and device population for each group can be seen in the Appendix.

Group 1 – WhatsApp Disappearing Messages Pre and Post Disappearing Date: Messages and media sent between two phones via WhatsApp, with disappearing messages mode turned on. This test is used to determine how WhatsApp deals with the messages both pre- and post-disappearing date. Samsung S6 and Apple iPhone 6s will be used to evaluate the capabilities and limitations of both Android and iOS. 5.3.2.

Group 2 – WhatsApp Rollforward Disappearing Date: This test will determine whether the disappearing timer works based upon a server or localised timestamp check. This is an attempted forced deletion via date adjustment, which will evaluate the reaction of both Android and iOS to the local time/date being rolled forward past the disappearing date before it reaches that point on internet-based time.

Group 3 – WhatsApp Rollback Disappearing Date: This test in conjunction with Group 2 will determine whether the disappearing timer works based upon a server or localised timestamp (date and time in the user's time zone) check. As above, it is an attempted forced deletion via date adjustment, rolling the local time/date backwards before the disappearing date, to see whether the messages are retained for a prolonged period after the initial disappearing date. This test was conducted on both using both the Samsung S6, and Apple iPhone 6s to assess the reaction of both Android and iOS.

Group 4 – WhatsApp Cloud Backups: This test will determine whether cloud forensics is a viable means to extract the disappearing messages, as according to WhatsApp – these messages are still held within backups post disappearing date. It assesses the capabilities of Cloud extractions of private cloud-based applications, using the WhatsApp Cloud extraction on UFED Cloud Analyzer. This test was conducted using both the Samsung S6, and Apple iPhone 6s to evaluate the capabilities and limitations of both Android and iOS Cloud backups via Google Drive, and iCloud.

Group 5 – WhatsApp Desktop Application: This test determines whether there is any benefit to performing a 'live' acquisition of a computer running WhatsApp Desktop with

Table 2

Media messages supported by the messaging applications.

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

disappearing messages, by performing a RAM dump on the machine while the application is active. It will also determine whether any residual data is stored on the HDD of the computer when it is powered off, and acquired using traditional computer forensics, via an E01 image. This test will determine whether computer forensics is a viable alternative to retrieving disappearing messages.

Group 6 – Snapchat Messages: This test is 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.

Group 7 – Telegram Secret Chat: This test compares and tests 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.

The extraction of data from the mobile applications was completed using the tools: UFED 4 PC, and MSAB’s XRY. The reason for using these tools is that they are two of the most popular commercially available services for mobile forensics, with a wide range of profiles and types of extractions for multiple devices. Once the data was verified, we produced UFED reports, which made our dataset readily viewable on any workstation without the need for a UFED/XRY license attached.

4. Experiments and analysis

4.1. Group 1

In Group 1, the main objective is analysing WhatsApp’s treatment of disappearing messages. Specifically, we are to determine how WhatsApp deals with the messages both pre and post the disappearing date across Android and iOS. Additionally, both XRY and Cellebrite were used to perform pre- and post-disappearing extractions to see whether the forensic tool used had any impact on the data that could be extracted. From the results gathered, Cellebrite was better equipped at extracting data both pre- and post-disappearing, down to its use of advanced logical and physical extractions on both the iPhone and Samsung respectively. Using XRY XAMN’s built-in chat functions we were able to view the chat that had taken place on the iPhone and Samsung devices before the messages had disappeared.

The Samsung had better retention of data than the iPhone as shown in Fig. 1. This may be down to how the app data is stored on the phone and the differences in data sanitisation across OS. Traditionally Apple devices are harder to get data from due to their full-disk encryption model, where the phone is notoriously hard to ‘break into’, but once in, there is little in the way in terms of extracting data. Whereas Android OS seems to have more relaxed security in comparison, due to its open-source nature; at the cost of making each application secure in its own way. Due to this, Android tended to be easier to get deeper extractions.

When sending a regular image, XRY was able to locate the image

from the phone’s memory and display it for the examiner. However, when one time view (OTV) was active on the message, XRY was not able to recover the image completely or its location. Instead, it showed a blurred thumbnail despite the image existing on the device in the same directory as the original. Using Cellebrite Reader to export and view the WhatsApp directory, the “mgstore” database for Samsung allowed us to find the file paths and “message urls” via the “message_media” table. Media sent via WhatsApp is sent as a weblink and is stored on the WhatsApp server. The same result is available for iPhones by exporting the “ChatStorage.sqlite” file and using the table “ZWAMEDIAITEM”.

Following the Samsung file paths for “/data/user/0/com-whatsapp/files/ViewOnce” led us to a singular file labelled “.nmedia” which was 0 bytes. The iPhone led us to a series of folders containing all the original images sent and received over WhatsApp, except for the OTV in which only a thumbnail was available for the image. When examining the post results via XAMN, most messages had “disappeared”. Out of the 14 original artefacts available only 5 remained. The Samsung device managed to retain slightly more, where it had captured the attachments of VID1 and VID2 but could only provide file locations and not the files themselves. Using Cellebrite Reader we were able to view the messages from the Samsung and iPhone as well as locate the database they were being stored in. We did this by selecting a message and using the “Source file” shown in Fig. 2. These paths show us where the data is being stored within the extraction, down to the specific database and table it is found under.

Unlike XAMN, Cellebrite Reader was able to locate the OTV image as shown in Fig. 3. This would happen if the image was sent from the device but not when it was received. We believe this is due to the phone creating a thumbnail of every image it receives but due to the OTV feature, the phone is unable to download the full image to view.

Using the ‘sources’ link within the conversation we located the directory of the messages and exported them via Cellebrite Reader’s built-in file system browser for manual review (see Fig. 4).

From the manual review of the iPhone “ChatStorage.sqlite” database, the chat messages were in the table “ZWAMESSAGE”. While here, converting the time from Apple’s NSDate, alongside the column “ZMESSAGEDATE” allowed us to see that the disappearing timer was being stored within the message database. The times for messages (sent on the 17th November 2021) were set to expire on the 24th November 2021 (7 days after the message had been created). Fig. 5 illustrates the disappearing timer status, settings, and associated text.

From the manual review of Samsung’s “mgstore.db”, the message timer was stored under the table “lagacy_available_messages_view”, with the column “expire_timestamp”. Converting the time from EPOCH allowed us to view the same expiration times. Fig. 6 illustrates the disappearing message timestamp, expiry timestamp, media type, media caption, etc.

Following this we examined the post disappearing reports in which Cellebrite. Unfortunately, we could not extract all the messages within the Samsung physical extraction. In the Samsung report the only artefacts were system messages and messages containing attachments (such as images and videos) remained, but

Artifacts 14	Conversations	Artifacts 13	Conversations
17/11/2021 10:24:34 Incoming Hello	Test Media iPhone	17/11/2021 10:24:34 447719546912@s.whatsapp.net	Phone; 447719546805@s.whatsapp.net
17/11/2021 10:24:55 Samsung	Hey there Outgoing Test Media iPhone	17/11/2021 10:24:55 Incoming Phone; 447719546912@s.whatsapp.net	447719546805@s.whatsapp.net
17/11/2021 10:25:34 Incoming This is a test of the disappearing messages?	Test Media iPhone	17/11/2021 10:25:34 447719546912@s.whatsapp.net	This is a test of the disappearing messages? Outgoing Phone; 447719546805@s.whatsapp.net
17/11/2021 10:26:02 Samsung	Yes. It is. Outgoing Test Media iPhone	17/11/2021 10:26:03 Incoming Phone; 447719546912@s.whatsapp.net	447719546805@s.whatsapp.net
17/11/2021 10:26:31 Incoming Here is a photo	Test Media iPhone	17/11/2021 10:26:31 447719546912@s.whatsapp.net	Here is a photo Outgoing Phone; 447719546805@s.whatsapp.net
17/11/2021 10:27:17 Samsung	Here is another photo Outgoing Test Media iPhone	17/11/2021 10:27:18 Incoming Phone; 447719546912@s.whatsapp.net	447719546805@s.whatsapp.net
17/11/2021 10:28:44 Incoming Samsung	Test Media iPhone	17/11/2021 10:28:42 447719546912@s.whatsapp.net	You can only view this one once Outgoing Phone; 447719546805@s.whatsapp.net
17/11/2021 10:29:45 Samsung	Outgoing Test Media iPhone	17/11/2021 10:29:43 Incoming Phone; 447719546912@s.whatsapp.net	447719546805@s.whatsapp.net
17/11/2021 10:31:12 Incoming Samsung	Test Media iPhone	17/11/2021 10:31:02 447719546912@s.whatsapp.net	Outgoing Phone; 447719546805@s.whatsapp.net
17/11/2021 10:31:22 Incoming Samsung	Outgoing Test Media iPhone	17/11/2021 10:31:23 Incoming Phone; 447719546912@s.whatsapp.net	447719546805@s.whatsapp.net
17/11/2021 10:32:40 Samsung	Outgoing Test Media iPhone	17/11/2021 10:32:42 Incoming Phone; 447719546912@s.whatsapp.net	447719546805@s.whatsapp.net

Fig. 1. XAMN's iPhone Pre Chatlog (left) and Samsung Pre Chatlog (right).

the attachments themselves did not remain – see Fig. 7 and the error thumbnail. The iPhone however managed to fully retain all the data sent and received.

Group 1 shows the message remnants available when forensically analysing WhatsApp's disappearing messages feature – detailed in Table 3 and Table 4, but it also shows that data can differ depending on the available forensic tools. The experiments clearly show that Cellebrite is better equipped at retrieving WhatsApp message data than XRY. Cellebrite provided marginally more data pre-expiry and significantly more data post expiry which would be the situation in a real-world forensics' environment. Cellebrite was also able to recover more image/video data compared to XRY. Using Cellebrite's built-in file system browser and database viewer, it is also able to provide the manual review of the data to locate the expiry timestamp, although this could be achieved through exporting the data to a third-party forensic tool with XRY. Group 1 also has proven that the expiry timestamp is localised to the application's databases and does not require an internet connection to establish when a message is due to expire (both phones were isolated from the network for this experiment).

Key Meaning:

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

4.1.1. Group 2

Group 2 allowed us to evaluate the ability to force the messages to disappear, by rolling the date/time forward on the device to post-disappearing, before beginning an extraction – see Tables 5 and 6. Cellebrite UFED was used to extract data in Group 2. Two reports were created after the “Rollforward” of the date to analyse the results of forcing a data wipe, and whether this impacted the retention of data. The iPhone did not retain any data past the point where disappearing messages were enabled; only retaining normal messages and system messages Fig. 8.

Samsung (due to its physical extraction) was able to extract more data, including all the message data, but not the attachment data. Viewing the “msgstore” data in DB Browser also shows less data on the Samsung device, than what Cellebrite can parse. Deleted data was retrieved from the “db-wal” temporary files, which are no longer available on the device. It is possible that due to the logical extraction on the iPhone we are not able to obtain the

» Chat

Go to ▾

Conversation	Details	Attachments (8)
ID:	447719546805@s.whatsapp.net	
Source:	WhatsApp	
Account:		
Start Time:	17/11/2021 10:16:04(UTC+0)	
Last Activity:	17/11/2021 10:32:40(UTC+0)	
Number of attachments:	8	
Extraction:	Advanced Logical	
Source file:	iPhone/mobile/Containers/Shared/AppGroup/group.net.whatsapp.WhatsApp.shared/ChatStorage.sqlite : 0xAFA6 (Table: ZWAMESSAGE, ZWACHATSESSION, Size: 352256 bytes) iPhone/mobile/Containers/Shared/AppGroup/group.net.whatsapp.WhatsApp.shared/Library/Preferences/group.net.whatsapp.WhatsApp.shared.plist : 0x47E (Size: 11583 bytes)	

Fig. 2. Source File Cellebrite Reader.

Samsung

You can only view this one once

image/jpeg
a9a0deeb-bc0e-45a2-a5ec-143b62c83ce9.thumb
<https://mmg.whatsapp.net/d/f/AtS7nowddOYSJ2OIOG9wR4Rw5Nojo2aHriuYrM030xz4.enc>

17/11/2021 10:28:44(UTC+0)

Sources (2)

Test Media Iphone

image/jpeg
446d87b0-1d30-4b67-85fd-8c3782158db7.jpg
<https://mmg.whatsapp.net/d/f/AvNeAiZJSIP5frDXEpmGcRBfzndGR2BjEROzDPmpTqB.enc>

17/11/2021 10:29:45(UTC+0)

Sources (3)

Fig. 3. Cellebrite Reader iPhone OTV.

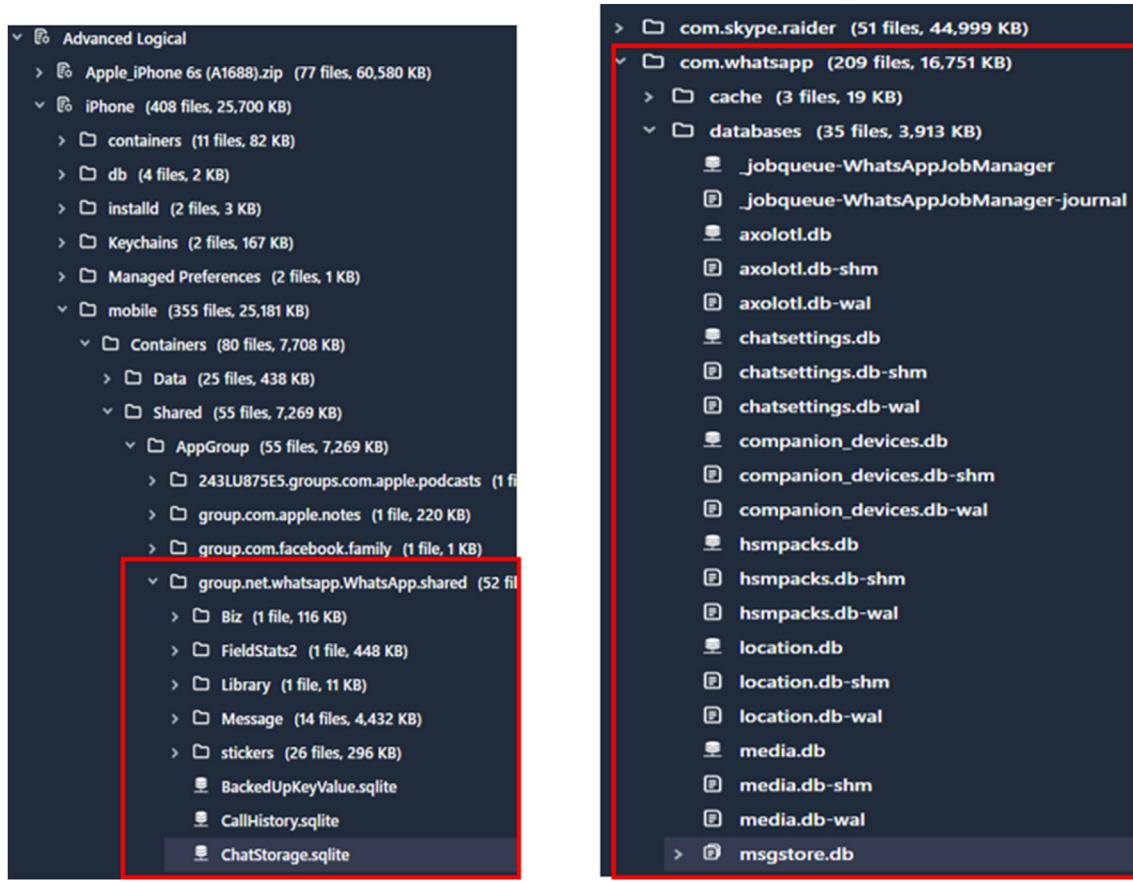


Fig. 4. Cellebrite File System viewer iPhone (left), Samsung (right).

ZMESSAGEERRORSTATUS	ZMESSAGEDATE	ZSENTDATE	ZTEXT
Filter	Filter	Filter	Filter
2001-01-01 00:00:00	2021-11-17 10:16:04	NULL	NULL
2001-01-01 00:00:00	2021-11-17 10:16:04	2021-11-17 10:16:04	NULL
2021-11-17 10:29:30	2021-11-17 10:28:44	2021-11-17 10:28:44	NULL
2021-11-17 10:29:45	2021-11-17 10:29:45	2021-11-17 10:29:45	NULL
2021-11-17 10:32:42	2021-11-17 10:32:40	2021-11-17 10:32:40	NULL
2021-11-24 10:24:34	2021-11-17 10:24:34	2021-11-17 10:24:36	Hello
2021-11-24 10:24:56	2021-11-17 10:24:55	2021-11-17 10:24:55	Hey there
2021-11-24 10:25:34	2021-11-17 10:25:34	2021-11-17 10:25:34	This is a test of the disappearing messages?
2021-11-24 10:26:03	2021-11-17 10:26:02	2021-11-17 10:26:02	Yes. It is.

Fig. 5. iPhone disappearing timers.

cached “-wal” or “-shm” files that are available with the Samsung - see Figs. 9 and 10.

From the data retrieved on the iPhone, forcing the date forward is an effective means to ensure that the data is sanitised. This is not the case with the Samsung device. We are unsure as to why the OSs behave differently, and further work needs to be conducted to see whether iOS and Android have separate ways of validating the date/time of time-sensitive applications and data.

4.1.2. Group 3

In Group 3, the device messages were left to run past their expiration before rolling the system clock back to before they had been sent. This was done to see whether there were any procedures were in place to counter this. Once imaged, both devices were successful in retaining all the data that had been created - see Tables 7 and 8. From the data retrieved on the iPhone, forcing the date forward is an effective means to ensure that the data is sanitised, whereas this was not the case with the Samsung device. This was the only series of testing in which 100% of the data had been

data	timestamp	media_wa_type	media_caption	expire_timestamp
Filter	Filter	Filter	Filter	Filter
NULL	2021-11-17 10:18:47.543	0	NULL	NULL
NULL	2021-11-17 10:16:05.0	36	NULL	NULL
Hello	2021-11-17 10:24:34.317	0	NULL	2021-11-24 10:24:34.0
Hey there	2021-11-17 10:24:55.0	0	NULL	2021-11-24 10:24:55.0
This is a test of the disappearing messages?	2021-11-17 10:25:34.78	0	NULL	2021-11-24 10:25:34.0
Yes. It is.	2021-11-17 10:26:03.0	0	NULL	2021-11-24 10:26:03.0
NULL	2021-11-17 10:26:31.315	1	Here is a photo	2021-11-24 10:26:32.0
NULL	2021-11-17 10:27:18.0	1	Here is another photo	2021-11-24 10:27:18.0
NULL	2021-11-17 10:28:42.375	42	You can only view this one once	2021-11-24 10:28:44.0

Fig. 6. Samsung disappearing timers.

The screenshot shows a Cellebrite Samsung POST interface displaying a list of messages. The messages are categorized by source, such as 'Test Media iPhone' and 'System Message'. Each message entry includes a timestamp, media type (e.g., video/mp4), file ID, and a preview of the media content. The interface also shows 'Sources' counts for each category.

Fig. 7. Cellebrite Samsung POST disappearing chatlog (left) and iPhone (right).

successfully recovered due to WhatsApp not having a procedure in place to sanitise the database if the dates are incorrect.

WhatsApp was also able to be opened and browsed through by the examiner post-acquisition without the data being wiped. We believe this is vital information for law enforcement, as if the suspect's device does contain disappearing messages, the examiner may decide to "roll the clock back", or "pausing the clock at the point of seizure" to preserve the evidence on hand if the date of expiry is known. However, this contradicts ACPO guidelines, and should be used as a last effort to retain data (and a standardised decision would have to be agreed upon between forensic investigators).

4.1.3. Group 4

Group 4 utilised UFED Cloud Analyser to retrieve data both publicly and privately through the WhatsApp Cloud and Google Drive/iCloud backups that were created after the messages were populated. This is an extremely uncommon method of data acquisition as it requires breaking network isolation and using user credentials/tokens. It constitutes a plethora of legal issues so is often a last resort. The WhatsApp/iCloud backup before the expiration date managed to extract the metadata of the messages but the content was unavailable to view - Table 9. Some of the data were discernible, such as the system message which states the messages are "End to end encrypted" being the 2nd message from

Fig. 8. Cellebrite Reader iPhone messages.

Table 3
Group 1 – WhatsApp Disappearing Messages iPhone 6s.

Date/Time added	Sent/Received?	Data Description	XRY Pre Disappearing?	XRY Post Disappearing?	Cellebrite Pre Disappearing?	Cellebrite Post Disappearing?
17/11/21 10:24	Received	"Hello"	Y	N	Y	Y
17/11/21 10:24	Sent	"Hey there"	Y	N	Y	Y
17/11/21 10:25	Received	"This is a test ..."	Y	N	Y	Y
17/11/21 10:26	Sent	"Yes. It is"	Y	N	Y	Y
17/11/21 10:26	Received	"Here is a photo" Photo 1	Y	N	Y	Y
17/11/21 10:27	Sent	"Here is another photo" Photo 2	Y	N	Y	Y
17/11/21 10:29	Received	Photo 3 -OTV	(Blank message)	(Blank message)	(Blurred thumbnail)	(Blurred thumbnail)
17/11/21 10:29	Sent	Photo 4 -OTV	(Blank message)	(Blank message)	Y	Y
17/11/21 10:31	Received	Video 1	(Attachment missing – blurred thumbnail)	N	Y	Y
17/11/21 10:31	Sent	Video 2	(Attachment missing – blurred thumbnail)	N	Y	Y
17/11/21 10:32	Received	Video 3 – OTV	(Blank message)	N	(Blurred thumbnail)	(Blurred thumbnail)
17/11/21 10:32	Sent	Video 4 – OTV	(Blank message)	(Blank message)	Y	Y

"System Message". The only other system messages contained "Revoke:" followed by a key; we believe this to be the system messages to show that disappearing messages had been activated (see Fig. 11).

The WhatsApp web from the Samsung device managed to partially recover messages - see Table 10. Two messages between the user and the other device were not recovered, and some of the media messages (containing OTV) were blank. The Google Drive backup was unable to authenticate and therefore potential data could have been missed. Post-disappearing, the iCloud & WhatsApp backup managed to extract almost no data at all from the same iCloud backup a week prior (besides the beginning of the chat thread), and the system message for end-to-end encryption. This may be due to the iCloud backup not having been completed correctly.

Overall, only the pre-disappearing data proved useful for examination, as it provided at least the metadata of the messages sent. However, we believe the UFED Cloud "WhatsApp Web" extraction uses the same principle as "WhatsApp Web" and "WhatsApp

Desktop", in which a mobile device scans a QR Code to synchronise its data to the target device. Due to the issues seen in getting UFED Cloud to authenticate the tokens via Google/iCloud, as well as obtaining credentials from the user, relying on cloud backups being present, and the legal issues involved in real-world scenarios, we would not deem UFED Cloud to be an effective means to extract disappearing messages data. This would be a method used as a last resort and with the legal jurisdiction/approval to perform this.

4.1.4. Group 5

In Group 5, a VM to simulate a WhatsApp mobile device being paired to the partner-app WhatsApp Desktop for Windows and Mac was imaged both pre- and post-disappearing. A memory dump was also taken at both intervals for review. From the analysis, we have identified the following file paths of interest: *Root/Users/%USER%/AppData/Local/WhatsApp/*

This path holds the installation and update files, including a setup log "*SquirrelSetup.log*". No data or messages were found in this location - Fig. 12.

Table 4

Group 1 – WhatsApp Disappearing Messages Samsung S6.

Date/Time added	Sent/Received?	Data Description	XRY Pre Disappearing?	XRY Post Disappearing?	Cellebrite Pre Disappearing?	Cellebrite Post Disappearing?
17/11/21 10:24	Sent	"Hello"	Y	N	Y	N
17/11/21 10:24	Received	"Hey there"	Y	N	Y	N
17/11/21 10:25	Sent	"This is a test ..."	Y	N	Y	N
17/11/21 10:26	Received	"Yes. It is"	Y	N	Y	N
17/11/21 10:26	Sent	"Here is a photo" Photo 1	Y	N	Y	N
17/11/21 10:27	Received	"Here is another photo" Photo 2	Y	N	Y	N
17/11/21 10:28	Sent	"You can only view this photo once" Photo 3 – OTV	/(Blurred thumbnail, message exists)	N	/(Blurred thumbnail, message exists)	N
17/11/21 10:29	Received	Photo 4 - OTV	/(Blurred thumbnail, message exists)	N	/(Blurred thumbnail, message exists)	N
17/11/21 10:31	Sent	Video 1	/(Blank message, no video)	/(Blank message, no video)	Y	/(Blank message, video no longer exists)
17/11/21 10:31	Received	Video 2	/(Blank message, no video)	/(Blank message, no video)	Y	/(Blank message, video no longer exists)
17/11/21 10:32	Sent	Video 3 – OTV	/(Blank message, no video)	/(Blank message, no video)	/(Blurred thumbnail, message exists)	/(Blank message, video no longer exists)
17/11/21 10:32	Received	Video 4 – OTV	/(Blurred thumbnail, message exists)	/(Blank message, no video)	/(Blurred thumbnail, message exists)	/(Blank message, video no longer exists)

Table 5

Group 2 – WhatsApp Disappearing Messages with Rollforward iPhone 6s.

Date/Time added	Sent/Received?	Data Description	Cellebrite Recoverable?
14/01/2022 11:06	Received (non-disappearing)	"Hello"	Y
14/01/2022 11:07	Sent - (non-disappearing)	"Hello there"	Y
14/01/2022 11:08	Received	"This is a test of the changing the date and time"	(Blank message)
14/01/2022 11:08	Sent	"Okay. we wonder how this will work?"	N
14/01/2022 11:09	Received	"Here is a photo" Photo 1	N
14/01/2022 11:09	Sent	"Here is one back" Photo 2	N
14/01/2022 11:10	Received	"Here is a video" Video 1	N
14/01/2022 11:10	Sent	"Here is another" Video 2	N
14/01/2022 11:11	Received	"This is a deleted message"	N
14/01/2022 11:11	Sent	"This is also deleted"	N

Table 6

Group 2 – WhatsApp Disappearing Messages with Rollforward Samsung S6.

Date/Time added	Sent/Received?	Data Description	Cellebrite Recoverable?
14/01/2022 11:06	Sent	"Hello"	Y
14/01/2022 11:07	Received	"Hello there"	Y
14/01/2022 11:08	Sent	"This is a test of the changing the date and time"	Y
14/01/2022 11:08	Received	"Okay. we wonder how this will work?"	Y
14/01/2022 11:09	Sent	"Here is a photo" Photo 1	/(Blurred thumbnail, message exists)
14/01/2022 11:09	Received	"Here is one back" Photo 2	/(Video no longer exists, message exists)
14/01/2022 11:10	Sent	"Here is a video" Video 1	/(Video no longer exists, message exists)
14/01/2022 11:10	Received	"Here is another" Video 2	/(Video no longer exists, message exists)
14/01/2022 11:11	Sent	"This is a deleted message"	/(You deleted this message)
14/01/2022 11:11	Received	"This is also deleted"	/(Deleted by the sender)

Also: *Root/Users/%USER%/AppData/Roaming/WhatsApp*. This path holds folders including "databases", "cache", and files such as "cookies" and "main-process log". Initial results led us to investigate the "database" folder contained within AppData/Roaming, however the singular "databases.db" held no message data. "Databases.db" only held one populated table with mmap_status, version, and last compatible version.

The next folder of interest was "local storage", following this led us to a file: *Root/Users/%USER%/AppData/Roaming/WhatsApp/Local*

Storage/leveldb/000003.log. This log did not contain any message data but appears to contain the keys in which messages are encrypted/decrypted, as well as the device which was paired with the application. This information could allow investigators to identify suspect devices, and prioritise them: see Fig. 13.

As a final measure, we placed the WhatsApp application folders from "Roaming" and "Local" into Autopsy and began a "keyword search" of the messages. However, only false positives such as "Windows Hello" were returned. Using AXIOM Examine to explore

Table 7

Group 3 – WhatsApp Disappearing Messages with Rollback iPhone 6s.

Date/Time added	Sent/Received?	Data Description	Cellebrite Pre Disappearing?	Cellebrite Post Disappearing?
25/01/22 12:13	Sent	"Hello"	Y	Y
25/01/22 12:14	Received	"Hi"	Y	Y
25/01/22 12:15	Sent	"This is a test of the rollback feature"	Y	Y
25/01/22 12:15	Received	"Let's see how it does"	Y	Y
25/01/22 12:15	Sent	PHOTO 2	Y	Y
25/01/22 12:16	Received	PHOTO 1	Y	Y
25/01/22 12:16	Sent	VID 2	Y	Y
25/01/22 12:17	Received	VID 1	Y	Y

Table 8

Group 3 – WhatsApp Disappearing Messages with Rollback Samsung S6.

Date/Time added	Sent/Received?	Data Description	Cellebrite Pre Disappearing?	Cellebrite Post Disappearing?
25/01/22 12:13	Received	"Hello"	Y	Y
25/01/22 12:14	Sent	"Hi"	Y	Y
25/01/22 12:15	Received	"This is a test of the rollback feature"	Y	Y
25/01/22 12:15	Sent	"Let's see how it does"	Y	Y
25/01/22 12:15	Received	PHOTO 2	Y	Y
25/01/22 12:16	Sent	PHOTO 1	Y	Y
25/01/22 12:16	Received	VID 2	Y	Y
25/01/22 12:17	Sent	VID 1	Y	Y

Table 9

Group 4 – WhatsApp Cloud Backups iPhone 6s.

Date/Time added	Sent/Received?	Data Description	Cellebrite Pre Disappearing?	Cellebrite Post Disappearing?
06/12/2021 16:08	Received	"Hello"	(Blank message)	N
06/12/2021 16:08	Sent	"Hello there"	(Blank message)	N
06/12/2021 16:08	Received	"This is a test"	(Blank message)	N
06/12/2021 16:08	Sent	"Yes. It is"	(Blank message)	N
06/12/2021 16:08	Received	"Here is a photo" Photo 1	(Blank message)	N
06/12/2021 16:09	Sent	"Here is another" Photo 2	(Blank message)	N
06/12/2021 16:12	Received	"You can only view this photo once" Photo 3 – OTV	(Blank message)	N
06/12/2021 16:12	Sent	Photo 4 – OTV	(Blank message)	N
06/12/2021 16:13	Received	Video 1	(Blank message)	N
06/12/2021 16:13	Sent	Video 2	(Blank message)	N
06/12/2021 16:15	Received	Video 3 – OTV	(Blank message)	N
06/12/2021 16:16	Sent	Video 4 – OTV	(Blank message)	N

Table 10

Group 4 – WhatsApp Cloud Backups Samsung S6.

Date/Time added	Sent/Received?	Data Description	Cellebrite Pre Disappearing?	Cellebrite Post Disappearing?
06/12/2021 16:08	Sent	"Hello"	Y	N
06/12/2021 16:08	Received	"Hello there"	N	N
06/12/2021 16:08	Sent	"This is a test"	N	N
06/12/2021 16:08	Received	"Yes. It is"	Y	N
06/12/2021 16:08	Sent	"Here is a photo" Photo 1	Y	N
06/12/2021 16:09	Received	"Here is another" Photo 2	Y	N
06/12/2021 16:12	Sent	"You can only view this photo once" Photo 3 – OTV	(Blank message)	N
06/12/2021 16:12	Received	Photo 4 – OTV	(Blank message)	N
06/12/2021 16:13	Sent	Video 1	Y	N
06/12/2021 16:14	Received	Video 2	Y	N
06/12/2021 16:15	Sent	Video 3 – OTV	(Blank message)	N
06/12/2021 16:16	Received	Video 4 – OTV	(Blank message)	N

the memory dump from the "pre-disappearing" stage which had been processed allowed us to find the images which had been sent both via phone and desktop within the RAM of the VM, whilst the application was still open and in the foreground.

Overall, there is little to no residual data contained within WhatsApp Desktop, but RAM dumps are a practical choice if images are used within the application - see [Table 11](#). This can be used by law enforcement in situations where a suspect has been caught live

viewing/sending material, and where the device is still running and can be forensically triaged at the scene to capture early evidence. However, this is subject to the volatility of RAM, as the data may only reside within the RAM for a brief period, which may be flushed by the user, or lost when the device is powered down.

4.1.5. Group 6

Group 6 involved using the Snapchat application to compare

Table 11

Group 5 – WhatsApp Desktop Disappearing Messages iPhone 6s.

Date/Time added	Sent/Received?	Data Description	Pre Disappearing Recovery?	Post Disappearing Recovery?
15/12/21 12:22	Received	"Hello"	N	N
15/12/21 12:23	Sent - iPhone	"Hello back" message sent	N	N
15/12/21 12:24	Received	"This is a test of WhatsApp Desktop"	N	N
15/12/21 12:24	Sent - iPhone	"This message was sent through the phone"	N	N
15/12/21 12:25	Sent - Desktop	"And this one sent through the Desktop"	N	N
15/12/21 12:25	Received	"Here is a photo" – PHOTO 1 attached	Y (Saved in memory)	N
15/12/21 12:25	Sent - iPhone	"Here is one back from the phone" – Photo 2 attached	Y (Saved in memory)	N
15/12/21 12:26	Received	Photo 3 - OTV	Y (Saved in memory)	N
15/12/21 12:27	Received	"Don't open this one"	N	N
15/12/21 12:27	Sent - iPhone	"Here is a video from the phone" – VID 2	N	N
15/12/21 12:29	Sent - Desktop	"Delete this message"	N	N
15/12/21 12:29	Received	"Also delete this one"	N	N

Table 12

Group 6 – Snapchat Messages (Unsaved & Saved) iPhone 6s.

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 13:30	Sent	"Neither will this"	N

Table 13

Group 6 – Snapchat Messages (Unsaved & Saved) Samsung S6.

Date/Time added	Sent/Received?	Data Description	Cellebrite Recoverable?
02/02/2022 13:21	Sent	"Hello"	Y
02/02/2022 13:21	Sent	"This is a test of the disappearing messages"	Y
02/02/2022 13:21	Received	"I will save this message" – iPhone saved	Y
02/02/2022 13:21	Received	"Hello"	Y
02/02/2022 13:21	Sent	"iPhone save this message" – iPhone saved	Y
02/02/2022 13:21	Received	"Samsung save this message" – Samsung saved	Y
02/02/2022 13:23	Sent	Photo of BIC pen – Saved by iPhone	Y
02/02/2022 13:23	Sent	Timed (10s) photo of screwdriver	(Blank message)
02/02/2022 13:25	Received	Photo of evidence tape – Replayed & saved by Samsung	(Video file missing)
02/02/2022 13:26	Received	Timed (10s) photo of duct tape	(Video file missing)
02/02/2022 13:28	Received	Photo of screwdriver	Y
02/02/2022 13:28	Sent	Photo of screwdriver	Y
02/02/2022 13:29	Sent	"This message will not be saved"	Y
02/02/2022 13:30	Received	"Neither will this"	Y

"disappearing by default" to "decisive disappearing" where Snapchat automatically deletes messages unless they are specifically saved by the user via tapping on them. The iPhone extraction was unfortunately not able to extract any Snapchat data other than application's files as shown in **Table 12**. The Samsung device managed to recover most of the chat data regardless of whether the messages were "saved" or "unsaved" (minus 1 timed photo, and 2 videos). 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 conversation data (MacDermott et al., 2022), see **Table 13**.

4.1.6. Group 7

In group 7, we created two Telegram chats: a regular chat and a "secret messages" chat (which enables disappearing messages). In the iPhone, neither Telegram chats were extracted in either pre- or post-expiry extraction, only the application data. The only file consisted of a "preferences.plist" file, which when opened contained no data regarding disappearing messages. In both Samsung extractions, the regular chat was extracted without issue, showing both messages – Figs. 14 and 15. However, limited data were extracted from the secret chats in both extractions and the metadata was incorrect, showing "15/05/2015".

Table 14

Group 7 – Telegram Secret Mode iPhone 6S.

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 15

Group 7 – Telegram Secret Mode Samsung S6.

Date/Time added	Sent/Received?	Data Description	Cellebrite Pre Disappearing?	Cellebrite Post Disappearing?
09/02/2022 10:26	Received – Non-Timed	"Hello"	Y	Y
09/02/2022 10:26	Sent – Non-Timed	"Hello there"	Y	Y
09/02/2022 10:28	Received	"I have activated disappearing messages"	(Required manual hex viewing)	(Required manual hex viewing)
09/02/2022 10:28	Sent	"We shall see how this does"	(Required manual hex viewing)	(Required manual hex viewing)
09/02/2022 10:29	Received	"Have a photo" PHOTO 2 attached	(Required manual hex viewing)	(Required manual hex viewing)
09/02/2022 10:29	Sent	PHOTO 1 sent	(Required manual hex viewing)	(Required manual hex viewing)
09/02/2022 10:30	Received	VIDEO 2 attached	N	N

Seeing the wrong metadata, we investigated further, looking to see where the data had been extracted from (Fig. 16). From there, we opened "Cache4.db" located within the Telegram "files" folder.

As shown in Fig. 17, the data has not been parsed correctly. 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. Using the in-built hex editor, the hex data shows some of the message contents that were sent (see Fig. 18).

Another piece of evidence found was the file path of the images that had been sent through the "secret chat" within the 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. Manual data can be extracted using the above techniques to retrieve incorrectly parsed artefacts – although not all artefacts may be available, as deleted messages and video messages were not recovered – see Table 14 and Table 15.

5. Discussion of results

In this section, we will now analyse the group tests results and supply a cross-comparison as to the amount of data which has been recovered by the different extraction/testing groups. We will also

discuss and analyse which method is best suited to obtain the maximum data available. Finally, we will critically analyse how these results would affect real-world investigations within law enforcement.

5.1. WhatsApp disappearing messages

Below we will discuss and compare the extraction methods of both XRY and Cellebrite using Group Test 1's results as evidence to support the claims and comparisons made.

5.1.1. XRY logical extraction

XRY's logical extraction of both the Samsung & Apple devices was effective at retrieving data during the pre-disappearing test extractions. Although, not all data was retrieved and parsed via XRY, media that used the "View Once" feature as well as the attached videos, were not extracted and parsed correctly – with the latter only keeping a blurred thumbnail. XRY struggled with the post-disappearing stage of the group test with XRY unable to recover the regular text-based messages. Only three of eleven artefacts in each extraction were retrieved; none of which supplied any evidential value besides the date/times of the messages.

Table: legacy_available_messages_view						
_id	data	timestamp	media_url	media_name	media_caption	expire_timestamp
1	2 NULL	2022-01-14 11:06:23.42	NULL	NULL	NULL	NULL
2	3 Hello	2022-01-14 11:06:23.21	NULL	NULL	NULL	NULL
3	4 Hello there	2022-01-14 11:07:45.0	NULL	NULL	NULL	NULL
4	5 NULL	2022-01-14 11:07:59.695	NULL	NULL	NULL	NULL
5	10 NULL	2022-01-14 11:10:19.341	https://mmg.whatsapp.net/d/f/...	298f9b26-6126-4d63-a34a-c00c9fec91a3.mp4	Here is a video	2022-01-15 11:10:28.0
6	11 NULL	2022-01-14 11:10:43.0	https://mmg.whatsapp.net/d/f/...	NULL	Here is another	2022-01-15 11:10:43.0
7	12 NULL	2022-01-14 11:11:17.481	NULL	44F7C6E1825A3974F19FA87ADD24B0DB	NULL	2022-01-15 11:12:11.0
8	13 NULL	2022-01-14 11:11:40.0	NULL	3A29429D1746213DC544	NULL	2022-01-15 11:11:40.0

Fig. 9. DB Browser Samsung messages.

ZMESSAGEDATE	ZSENTDATE	ZFROMJID	ZMEDIASECTIONID	ZPHASH	ZPUSHNAME	ZSTANZAID	ZTEXT	ZTOJID
Filter	Filter	Filter	Filter	Filter	Filter	Filter	Filter	Filter
663851228	NULL	447719546805@s.whatsapp.net	NULL	NULL	CNyhhY8G	3A8C3E80EE359971EF2D	NULL	447719546912@s.whatsapp.net
663851228	663851228.204216	447719546805@s.whatsapp.net	NULL	NULL	CNyhhY8G	484B925607C3B710C3465381415CF2CS	Hello	NULL
663851264.884302	663851264.938986	NULL	NULL	NULL	CIGzhy8G	3A60079458FE1002A6F8	Hello there	447719546805@s.whatsapp.net

ZTEXT	ZTOJID
Filter	Filter
NULL	447719546912@s.whatsapp.net
Hello	NULL
Hello there	447719546805@s.whatsapp.net

Fig. 10. DB Browser iPhone messages.

Cloud Info

App Name	User	Date range	Credential type	Authentication type	Status
iCloud	Test Media	01/09/2021 - 31/12/2021	User credentials	Standard	✓
iCloudWhatsApp	Test Media	01/09/2021 - 31/12/2021	User credentials	Standard	
WhatsApp Web	Test Media	01/09/2021 - 31/12/2021	QR	Standard	

Select/Select all 14 messages

- Samsung 06/12/2021 16:07:27(UTC+0)
- System Message E2eEncrypted: 06/12/2021 16:07:27(UTC+0)
- Samsung 06/12/2021 16:08:16(UTC+0)
- System Message Revoke: 3AD5BBB568B4E2ED25B0 06/12/2021 16:08:20(UTC+0)
- System Message Revoke: 2E0AF89819C48D6D60F19137358A9864 06/12/2021 16:08:31(UTC+0)

Test Media 06/12/2021 16:08:35(UTC+0)

Fig. 11. UFED Cloud iPhone Pre extraction.

Cellebrite logical and advanced logical extraction performed well in the pre-disappearing stages of the Group 1 testing, with all but two of the artefacts retrieved from the Apple device, with a slightly less impressive three artefacts not fully retrieved from the Samsung. Cellebrite's advanced logical and logical extraction performed well against the XRY equivalent. Furthermore, it is during the post-disappearing stage that Cellebrite excelled against XRY. Whereas XRY had managed to retrieve three of eleven artefacts, Cellebrite had retrieved the same data from the pre-disappearing Apple extraction. However, Cellebrite also performed the same as XRY with the Samsung post-disappearing testing.

5.1.2. Cellebrite physical extraction

Cellebrite's physical extraction should have managed to retrieve more deleted data than its logical equivalent, with physical extractions being more capable of retrieving deleted data. However, the Group 1 testing proved otherwise. With Cellebrite's physical extraction, only two more artefacts were retrieved pre-disappearing and the equivalent amount to XRY post-disappearing.

5.1.3. XRY vs cellebrite summary

Overall, Cellebrite has managed to excel over XRY in its retrieval of artefacts both pre- and post-disappearing on the iPhone 6s, supporting a near-complete extraction even after data is supposedly deleted from WhatsApp. However, the same cannot be said for the Samsung device, which kept the same level of data retrieval as XRY's logical extraction. From the results gathered within test Group 1, Cellebrite is the clear tool for use on Apple devices, while XRY and Cellebrite maintain equal opportunity for Android devices, given the data provided.

5.2. WhatsApp 'rollforward' and 'rollback'

The attempted forced deletion via date adjustment 'rollforward' and 'rollback' the times were successful. The rollforward procedure was successful in showing what occurs when the localised date is forced beyond the disappearing date of the messages. The database will be sanitised accordingly if the application is forced to refresh, as the data pertained whilst the application was still running in the

Name	Size	Flags(Dir)	Flags(Meta)	MD5 Hash
[current folder]	56	Allocated	Allocated	
[parent folder]	56	Allocated	Allocated	
app-2.2146.9	56	Allocated	Allocated	
packages	56	Allocated	Allocated	
app.ico	415922	Allocated	Allocated	ea3a9a304ce7e7ac102f64aba5fee52d
SquirrelSetup.log	2994	Allocated	Allocated	84e2e0b77e016769e6dc1eeaa4cb64fb
Update.exe	2252496	Allocated	Allocated	9a3cae1e403a05553eb9e20e7bd88cab
WhatsApp.exe	678608	Allocated	Allocated	273db5b1c03ac0d4131c3c4e1d7a3d47

Fig. 12. AppData/Local folder.

```

000003.log - Notepad
File Edit View

L•~°ø  VERSION@10
META:file://
Ø“ÍxÈ, Íøøwøø_file:// ØWABrowserId@LNg0Vz/Vk30VLZBkjJyMuw==@ø_file:// ØWALangP
META:file://
Øöð»ñÈ, ÍøøÄøø_
file:// Ø1zBAAdmKCgQmrXH6hw8Hw==@øfalse@
file:// Ø8RrdUTS9nD9Zmtkk08vVUA== @"Test Media"@
file:// Ø9qdyAYN1WQ8js2EW8W1QVA==@øfalse@
file:// ØN9Y6q/FDzfqp8DyLfEZFB@=@[]
file:// ØWADailyStatsStartTime@1639570545875@
file:// ØWALangPref@en-GB@
file:// ØWASecretBundle$@{"key": "15Xc+BZhjNX0eX+SdpCatiCwnuwI4zp0auZYmjQzOiw=", "file:// ØWAToken1[@T8B4YARKGEr0UiBEDQi9jFLmweHyXeLvZTlwHCYAEIE0m2ngrdF1YLT49+Cbf
file:// ØWAToken2U@1@M5HgwJP5yK1epb91WLx2YuyKyc2JiFcB4ED8x0bomiantkGXe89FBTqC+eT
file:// ØdebugCursor@177@
file:// Øf4pasOZ2KYkmWUSkmIQ7Sw==9@>{"id": "global_mute", "expiration": 0, "callExpir
file:// ØkkDBDM0vebCHTJURK16XmQ==@øfalse@
file:// Ølast-wid@447719546912@c.us@
file:// Ølogout-token@1@OkmGM5WtnMDq+3RQ7wBtuIpCeJTU0P86yfY1mVxpgNHfR00jWGmjZP
file:// Ømobile-platform @"iphone"@
file:// ØnrDI25JeFxRuPvxf41log=="ØBB0D7DC-F8D5-4556-85B3-B0AF7011F2A2"@
file:// Øu7t0Dt0YghNd36mYIrEP5A==@øfalse-ØøkC @
META:file://
ØØÉ`ŽÉ, ÍøøÄøø_file:// ØdebugCursor@179

```

Fig. 13. 000003.log.

background. On the Apple device, only the two non-disappearing messages, as well as one 'blank' disappearing message were retained, whilst the Samsung only managed to recover text-based messages from the extraction. This dataset, compared to the earlier group 1 dataset shows that the forced deletion and interaction with the device has negatively impacted the ability to recover these messages. Furthermore, this could be useful in the

manual extraction of disappearing data close to expiry, as keeping the application running in the foreground may prolong the visibility of data until an examiner has managed to capture it (via photographic evidence), however, further research needs to be conducted on this.

The 'Rollback' procedure whilst effective at retaining otherwise lost data, breaks the first rule of the 'ACPO Guidelines' in which "No

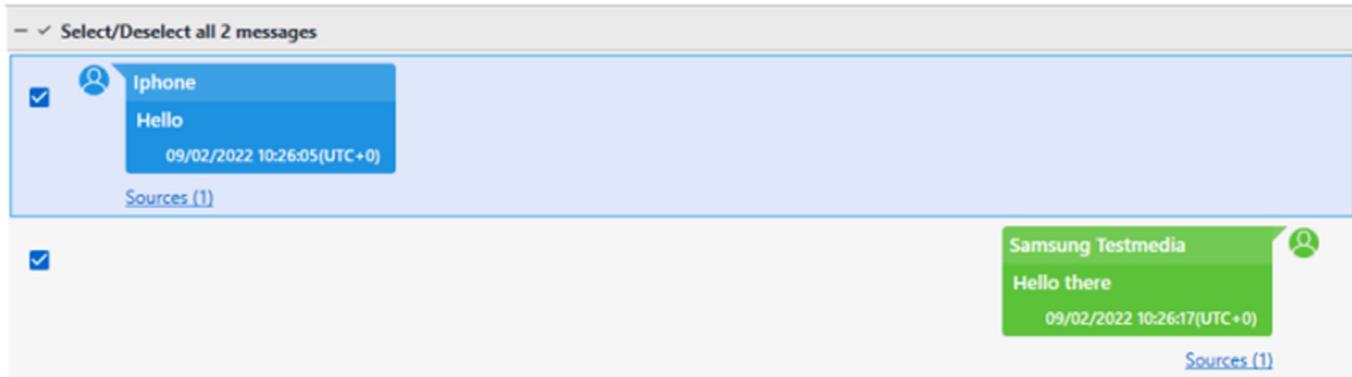


Fig. 14. Telegram Samsung regular chats.

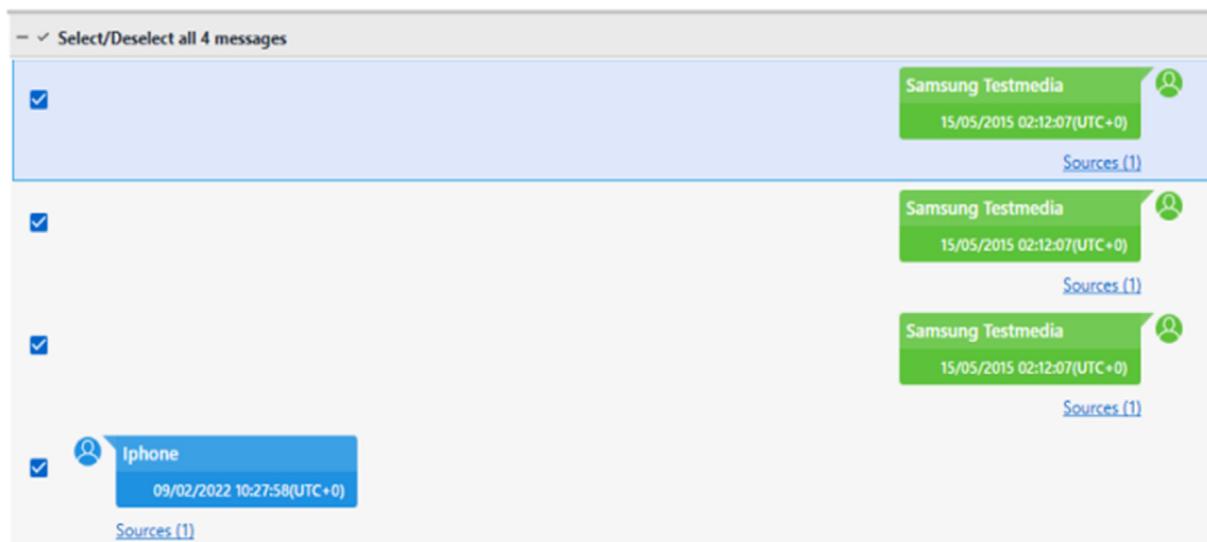


Fig. 15. Telegram Samsung secret chats.

» Instant Message		Go to ▾
Source:	Telegram	
Subject:		
Timestamp:	15/05/2015 02:12:07(UTC+0)	
Status:	Sent	
Message Type:	App Message	
SMSC:		
Device description:		
Folder:		
Priority:		
Extraction:	Physical	
Source file:	USERDATA (ExtX)/Root/data/org.telegram.messenger/files/cache4.db-wal : 0x11EA26 (Size: 4124152 bytes)	

Fig. 16. Storage location telegram chats Samsung.

action taken by law enforcement agencies, persons employed within those agencies, or their agents should change data which may

subsequently be relied upon in court" (ACPO, 2012). By changing the date and/or time on the device, the examiner may be changing potential evidence, and therefore data cannot be verified as being accurate once this change is made. However, one may argue that changing the date/time may be a necessary risk following Principle 2 and 3, in which where access to original data is needed, one must be competent to do this, and any steps undertaken to retrieve data must be audited. The dilemma is not an easy one to solve, as the risks may outweigh the rewards on a case-by-case basis, and a mutual agreement between digital forensic units and forensic labs across the country would be needed.

Regardless, as seen in the test results of Group 3, the rollback procedure that had been used proved to be remarkably successful. In both the Samsung and Apple devices, all data was retrievable both pre and post disappearing. When the date had been rolled back to the day the messages had been sent, no data had been wiped from the devices – as we believe this is due to the WhatsApp application having to rely upon localised dates due to the network isolation. Unfortunately, due to time constraints, further testing could not be established with regards to how prolonged this procedure could work. There is no guarantee that this procedure could be reliably used for all potential disappearing messages.

The execution of the rollback and roll forward testing has managed to prove our original hypothesis that the application did

data	fx date	data
Seconds from UTC 1601	01/01/1970 00:00:00	bX+000000"QY003"QY057UUU0CaeJ
Milliseconds from UTC 1601	09/02/2022 10:30:42	UUU00000Q0003"QY057Ub0p0XUUU>00!P.
Microsecond from UTC 1601	09/02/2022 10:30:18	UUU00000Q057"QY00300b0p0XUUU0000F
Days From UTC 1970	09/02/2022 10:29:52	UUU00000Q003"QY05700b0PQi0ez000...
Seconds from UTC 1970	09/02/2022 10:29:23	UUU00000Q057"QY00300b
<input checked="" type="checkbox"/> Seconds from UTC 1970 - Suggested	09/02/2022 10:28:44	UUU00000Q003"QY057\0bWe shall see how this d...
Milliseconds from UTC 1970	09/02/2022 10:28:10	UUU00000Q057"QY0030:b&l have activated disapp...
Microseconds From UTC 1970	09/02/2022 10:27:58	bX+00000"QY057"QY00300b0UUU0:s0Q0
Seconds from UTC 2001 (iPhone)	09/02/2022 10:26:47	UUU00000Q003"QY05700b
Nanoseconds from UTC 2001 (iPhone)	09/02/2022 10:26:40	UUU0000057"QY0030:bHello c=0j0
Clear	01/01/1970 00:00:00	bX+00000"QY003"QY057UUU0000c0
	09/02/2022 10:26:05	bX+00000"QY003"QY057UUU0000e0
	09/02/2022 10:26:17	bX+00000"QY003"QY057d0b

Fig. 17. Date conversion.

Hex
00 01 02 03 04 05 06 07 08 09 0A 0B 0C
000 FA 55 55 55 01 03 00 00 AA CB FC FF 80 úUUU....äÜüý.
00D 51 01 00 0E D9 9A 37 22 17 51 59 AD BA Q...Ü.7".QY °
025 DB 33 01 00 00 00 3A 97 03 62 26 49 20 Ü3....:..b&I
027 68 61 76 65 20 61 63 74 69 76 61 74 65 have activate
034 64 20 64 69 73 61 70 70 65 61 72 69 6E d disappearin
041 67 20 6D 65 73 73 61 67 65 73 00 20 63 g messages. c
04E ED 3D 15 C4 B5 1C 00 00 00 00 00 00 00 00 i=.Äp.....
05B 00 .

Fig. 18. Cache4.db hex editor.

not rely upon server connections to authorise a deletion of disappearing messages and that the application had a localised command to sanitise the database. This also supplied a means of prolonging the data, to allow for the capture of time-sensitive material that could be used as evidence. However, this is not dependable nor a forensically sound approach to the preservation of data.

5.3. Extractions – traditional, cloud and desktop

Below is an analysis of the extraction methods performed, covering their effectiveness in the retrieval of data, as well as how suited they may be for real-world investigations.

5.3.1. Traditional

The traditional methodology of seizing and extracting data from the device itself is the most used and standardised way of retrieving data in real-world forensic investigations. Therefore, it was our primary methodology in the retrieval of disappearing data across WhatsApp, Cloud, and Desktop devices. The methodology was somewhat of a success, with varied results between groups 1, 6, and 7. In group 1, Cellebrite excelled at the retrieval of disappearing data

on the Apple device, but not the Samsung. In group 6, the results were the opposite, with Snapchat data only being extracted successfully on the Samsung device. Finally, group 7 followed suit 6, with only a partial extraction being successful on the Samsung device.

The data retrieved from the applications used between the two devices shows that there is no clear-cut decision for the traditional extraction of data of devices, besides the already tried and true method of best possible extraction for real-world investigations. Of the three applications tested, two were more successful using Cellebrite's physical extraction method, over Cellebrite's advanced logical and logical extractions.

5.3.2. Cloud

The cloud extractions were tested using WhatsApp as there was no support for neither Snapchat nor Telegram at the time of writing. Due to this, the cloud data available to analyse is limited in its capacity and focused solely on WhatsApp's disappearing messages. Comparing the pre and post extractions, the contrast is stark; with no disappearing messages recovered post the disappearing date, and little data recovered pre-disappearing (message sent times/dates and contact information). Mixed with the difficulties

previously mentioned in attempting to obtain authentication, and the risk involved in breaking network isolation, 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 for a last resort approach to gain evidential data.

5.3.3. Desktop

The testing in group 5 surrounding the use of a paired computer device was used to evaluate whether an alternative method of forensically examining a paired device would contain cached or stored data for analysis. However, after a thorough examination and using data-carving with AXIOM, little data could be recovered from the VM acting in place as the secondary device. From the data recovered, only the pre-disappearing RAM capture managed to save the images sent in residual memory, as the application was still live and running at the time of capture. This methodology is once more not the best-suited practice to the retrieval of disappearing data, with the data having only been stored in a volatile memory – which could have easily been lost in a real-world environment. Therefore, this test has concluded that secondary-linked devices are not a viable alternative for the retrieval of disappearing data.

From the testing that we have conducted, it is fair to conclude that traditional forensics still prevails as the best possible method for extracting disappearing data from mobile applications.

5.4. WhatsApp, snapchat, and telegram data comparisons

In this section we compare the data retrieved from each application, as well as how effective each application was in the sanitisation of disappearing data.

5.4.1. WhatsApp

From the results obtained within groups 1-3, WhatsApp's sanitisation of data is not consistent. WhatsApp does a mediocre job at the sanitisation of data and fails to prevent the most basic way of overriding disappearing messages, leaving a major weakness to be exploited. Both devices may provide some artefact data back to the investigator, but it cannot be guaranteed that all the data can be extracted as WhatsApp is inconsistent in its data retention.

The Apple device data in group 1 was mainly recoverable. Whilst in group 2, where the data was forced to disappear (through local date manipulation), the data was unable to be retained. When data was forced to remain on the device (through local date manipulation) data was fully retrievable. The Samsung device data in group 1 yielded no recoverable data, but in groups 2 and 3, data was consistently recoverable. The Samsung device is more consistent regarding data sanitisation (with the group 1 results capturing almost no data) whereas the Apple device failed to sanitise any data post-expiration. Data can easily be preserved past the expiry date on both devices by a simple method of “pausing or rewinding” the local clock of the device until data can be captured.

5.4.2. Snapchat

In group 6, a series of messages were sent/received between the two devices. When examining the iPhone, no data could be

forensically recovered from the device (other than the installation of the application on the device). These results show a clear regard for the sanitisation of data within Snapchat, which in turn, poses an issue for forensic investigations. However, the same data, when examined on the Samsung, was near completely retrievable (except for three artefacts); showing that Snapchat for Android has a poor data sanitisation procedure, alongside Telegram. Whether this is due to the Samsung's physical extraction, or down to the specific hardware/software of the device is unclear. Overall, Snapchat for iOS for forensic investigations should be conducted manually first, if possible; before attempting to conduct a logical (or greater) extraction. For Android, a physical extraction, if possible, is the best available method for the extraction of Snapchat artefacts.

5.4.3. Telegram

In group 7, Telegram was used on both devices to send/receive a series of messages and media. Data was completely irretrievable on the iPhone both pre and post expiry. This shows that Telegram for iOS has a commendable sanitisation procedure. However, the Samsung device did contain some artefacts from the experimental data. This required manual review of the Telegram application files and browsing hex-data contained within the BLOB entries. Telegram's data sanitisation for Android is inconsistent but overall better than Snapchat or WhatsApp. A manual review of Telegram for iOS may be required before conducting any extractions to ensure that data which is available on the device is captured; before attempting to retrieve more data via an extraction. Regarding Android devices, a physical extraction is the best available extraction, and the examiner should take due care to ensure that they verify the database files are reviewed to retrieve the maximum data possible.

5.4.4. WhatsApp vs snapchat

Both WhatsApp's and Snapchat's disappearing messages behave differently. Snapchat disappears by default and WhatsApp's approach is something the user must enable (with greater assurance as to whether the messages will disappear). In Snapchat either side may wish to save a message, whilst letting the other user delete it. Comparing the data in groups 1 and 6, the iPhone managed to retain all data in group 1, whilst retaining no data in group 6. The opposite is shown in the Samsung results where all the data is retrieved in group 6, yet little data is retrieved in group 1. From the above, WhatsApp holds the greatest potential for the recovery of data on iOS, whilst Snapchat holds the greatest potential for the recovery of data from Android.

5.4.5. WhatsApp vs telegram

Both WhatsApp and Telegram are very similar regarding disappearing messages. Both applications require user interaction to enable the disappearing messages feature. This allows the user to set a timer for the visibility period/duration of these messages. Telegram goes beyond WhatsApp and allows the user a separate secret chat thread, as compared to WhatsApp's default message thread. Telegram users set a timer between 1 s–1 week, whereas WhatsApp locks the user in to a set: 24 h, 7 days, or 90-day period.

WhatsApp's and Telegram's results for group 1 and group 7 differ. Whilst the iPhone retains all data on WhatsApp, it does not retain any data beyond Telegram's installation files for the application. The Samsung device had a greater chance at recovering the data from Telegram, than WhatsApp (although this required

manual hex viewing to retrieve artefacts). From a user's perspective: Telegram is the greater choice for privacy, allowing for secret and non-secret chats, as well as allowing for the greater variety of disappearing timers. However, from a forensic perspective, Telegram also remains the choice for best potential evidence via Android extractions, whilst WhatsApp remains the choice for best potential evidence via iOS extractions.

5.4.6. Telegram vs snapchat

As previously mentioned, both Telegram and Snapchat share related results in group 6 and 7, where the iOS retains no artefacts on either application and the 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.

6. Conclusions

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. Given the vastly expanding world of digital forensics, as well as the ever-changing scenarios we are faced with, alongside the lack of knowledge and research conducted around this new and evolving aspect of digital forensics; we feel that we have provided significant new research into this field.

This paper has been successful in providing a series of results of what may be obtainable through forensic tools and processes regarding disappearing messages, and we hope this may set a base for future projects and further research to be conducted, using our evidence and methodology to achieve this. All three applications

Group	Summary of Results
Group 1 – WhatsApp disappearing messages and comparison of XRY to Cellebrite	<ul style="list-style-type: none"> ● Can determine from analysis that an "expiry timestamp" exists within the WhatsApp messages database. ● Cellebrite manages to recover more disappearing messages than XRY in terms of iOS extractions. ● However, neither XRY nor Cellebrite succeed with Samsung's post-disappearing messages, despite having a better level of extraction than the iPhone. ● XRY manages to retrieve 50% of data pre-disappearing, and 0% post. ● Cellebrite manages to retrieve 75% pre-disappearing, and only 42% of data post disappearing. ● By rolling forward the date on the device manually, it forces the data to be wiped after a "reset" of the application WhatsApp, either via closing and re-opening the application, or restarting the device itself. ● Therefore, it is imperative to keep the device in an AFU state and to not tamper with the volatile evidence by interacting with the application beyond what is deemed necessary. ● WhatsApp's disappearing messages, when isolated from automatic network time, is forced to rely upon the localised clock. ● This means that Law Enforcement can manually adjust the time/date to when the device was seized in an attempt to "prolong" the retention of disappearing messages by "freezing time". ● Provides a problem for Law Enforcement as the changing of original data affects the 1st ACPO guideline of not changing data - however this could be mitigated under the 2nd guideline. ● Only pre-disappearing metadata, contact information and media can be retrieved from UFED Cloud extractions. However, if the examiner already has access to the device for verification purposes this becomes a moot point. ● Post-disappearing, only metadata can be retrieved from the extractions. This is useful for proving that messages did exist at one time, as the examiner can see when they were sent/received, however does not provide a more in-depth as to what the contents of the messages were, or whom they were sent too - not enough substantial evidence for a conviction. ● The only useful data that could be retrieved from a deadbox forensic examination of the VM: <ul style="list-style-type: none"> - Which device has connected - Install dates/times. ● Utilising RAM captures allows media contained within residual memory to be captured forensically, however this is not substantive as it does not provide other data alongside it such as messages ● Snapchat differs from WhatsApp as the message timer is on by default - immediate or 24 h. ● The extractions from the iPhone were unable to recover the Snapchat data - requires a Full File System extraction in order to achieve this. ● Samsung having a physical extraction allowed for a near-complete recovery of the data ● Allows for much more varied options - ranging from 1 s to 1 week before disappearing. ● Creates a secondary, 'secret chat' when selecting disappearing messages, rather than continuing the conversation within the main chat. ● The iPhone was once again unable to recover data from the chats - not even the databases were extracted for a manual examination. ● A partial-recovery of the databases was available on the Samsung, allowing examiners to view the databases via SQLite readers - requiring advanced knowledge from the examiner to perform this. ● WhatsApp is the best supported. ● Snapchat allows for a partial support through standard means of extraction but requires advanced data recovery via Full File System using Premium Services for full support. ● Telegram, despite having the best available means of extraction was still not parsed - meaning the examiner must use advanced knowledge to recover the data and produce evidence
Group 2 - Rollforward	
Group 3 - Rollback	
Group 4 - Cloud	
Group 5 - WhatsApp Desktop	
Group 6 - Snapchat Messages	
Group 7 - Telegram Messages	
Which is the best supported application for the forensic recovery of Disappearing Messages?	

have evidenced themselves as being competent for the thorough sanitation of data, which impacts potential forensic investigations within Law Enforcement from being able to retrieve and accurately verify data's integrity, for admission to court as evidence. WhatsApp is the least destructive for potential evidence, as shown by group 1 – in which both devices were able to retain some data, as well as providing an alternative, but arduous means to retrieve data via the Cloud. Snapchat is the second most destructive for potential evidence, where iOS devices would have to subject to a manual review, whilst physical Android analysis could retrieve all the necessary artefacts required for admissible evidence. Telegram, finally, is the most destructive method for potential evidence. Incomplete data was the best extraction possible within our report, providing minimal artefact evidence. Encryption-based applications such as Signal could be researched as part of further work upon this study.

Declaration of competing interest

The authors declare that they have no known competing financial interests or personal relationships that could have appeared to influence the work reported in this paper.

Data availability

We created an investigative scenario and populated the devices with sample data

Appendix

Group 1

Device: iPhone 6s – A1688				
Date/Time added	Data Description	Metadata (where applicable)	Deleted? Y/N	Date/Time Deletion
17/11/21 10:06	Installed WhatsApp v 2.21.221		N/A	
17/11/21 10:07	WhatsApp setup		N/A	
17/11/21 10:16	Disappearing messages turned on – Samsung chat		N/A	
17/11/21 10:23	Photos 2 and 4, videos 2 and 4 created via Camera		N	
17/11/21 10:24	"Hey there" message sent		N	
17/11/21 10:26	"Yes, It is" message sent		N	
17/11/21 10:27	"Here is another photo" Photo 2 sent	b2b97559501579af333e8e2be08e0766	N	
17/11/21 10:29	Viewed Photo 3 via OTV		N	
17/11/21 10:29	Photo 4 sent - OTV on	d922aa46456206cfdec390202799adca	N	
17/11/21 10:31	Video 2 sent	2e6bb5604cf4eb032081277b1e214266	N	
17/11/21 10:32	Video 4 sent – OTV on	222327ec820290c13ec9135d07f3f85d	N	
17/11/21 10:33	Airplane Mode turned on – network isolated		N/A	
17/11/21 10:39	Phone powered off		N/A	

Device: Samsung S6 – G920F				
Date/Time added	Data Description	Metadata (where applicable)	Deleted? Y/N	Date/Time Deletion
17/11/21 10:08	WhatsApp installed – v.2.21.23.23		N/A	
17/11/21 10:11	WhatsApp set up		N/A	
17/11/21 10:22	Photos 1 and 3, videos 1 and 3 created via Camera		N	
17/11/21 10:24	"Hello" message sent		N	
17/11/21 10:25	"This is a test ..." message sent		N	
17/11/21 10:26	"Here is a photo" Photo 1 sent	2322d57a9f877bc6d68d2cbc3d66f477	N	
17/11/21 10:27	Photo 2 downloaded		N	
17/11/21 10:28	"You can only view this photo once" Photo 3 sent – OTV on	72c4e5bf05afddc7c6b40b4d7a3de296	N	
17/11/21 10:30	Viewed Photo 4 via OTV		N	
17/11/21 10:31	Sent Video 1	2e2ca86c4c285e65ca24314d17bb2457	N	
17/11/21 10:31	Video 2 downloaded	2e6bb5604cf4eb032081277b1e214266	N	
17/11/21 10:32	Video 3 sent – OTV on	e1768de38f32f41952c09f728bf9452c	N	
17/11/21 10:33	Airplane Mode on – network isolated		N/A	
17/11/21 10:34	Handset powered off		N/A	

Group 2

Device: iPhone 6s – A1688				
Date/Time added	Data Description	Metadata (where applicable)	Deleted? Y/N	Date/Time Deletion
14/01/2022 10:57	Installed WhatsApp v 2.21.243		N/A	
14/01/2022 11:01	WhatsApp setup		N/A	
14/01/2022 11:07	"Hello there"		N	
14/01/2022 11:07	Disappearing messages activated – 24 h		N/A	
14/01/2022 11:08	"Okay, we wonder how this will work?"		N	
14/01/2022 11:09	"Here is one back" Photo 2 sent	b2b97559501579af333e8e2be08e0766	N	
14/01/2022 11:10	"Here is another" Video 2 sent	2e6bb5604cf4eb032081277b1e214266	N	
14/01/2022 11:11	"This is also deleted"		Y	14/01/2022 11:12
14/01/2022 11:12	Phone isolated from network		N/A	
14/01/2022 11:15	Phone taken off automatic time/date and set to +2 days in advance		N/A	
14/01/2022 11:15	WhatsApp closed and restarted; messages are gone		N/A	
14/01/2022 11:15	Phone powered down for extraction		N/A	

Device: Samsung S6 – G920F				
Date/Time added	Data Description	Metadata (where applicable)	Deleted? Y/N	Date/Time Deletion
14/01/2022 10:58	WhatsApp installed – v.2.21.24.22		N/A	
14/01/2022 11:05	WhatsApp setup		N/A	
14/01/2022 11:06	"Hello"		N	
14/01/2022 11:07	Disappearing messages enabled – 24 h		N/A	
14/01/2022 11:08	"This is a test of the changing the date and time"		N	
14/01/2022 11:09	"Here is a photo" Photo 1 sent	2322d57a9f877bc6d68d2cbc3d66f477	N	
14/01/2022 11:10	"Here is a video" Video 1 sent	2e2ca86c4c285e65ca24314d17bb2457	N	
14/01/2022 11:11	"This is a deleted message"		Y	14/01/2022 11:12
14/01/2022 11:12	Phone network isolated		N/A	
14/01/2022 11:13	Phone taken off automatic time zone, and put forward +2 days		N/A	
14/01/2022 11:14	WhatsApp closed and restarted; messages gone		N/A	
14/01/2022 11:15	Phone powered down for extractions		N/A	

Group 3

Device: iPhone 6s – A1688				
Date/Time added	Data Description	Metadata (where applicable)	Deleted? Y/N	Date/Time Deletion
25/01/22 12:08	Installed WhatsApp v 22.2.75		N/A	
25/01/22 12:10	WhatsApp Setup		N/A	
25/01/22 12:13	Disappearing messages turned on – 24 h		N/A	
25/01/22 12:13	"Hello"		N	
25/01/22 12:15	"This is a test of the rollback feature"		N	
25/01/22 12:15	PHOTO 2 sent	b2b97559501579af333e8e2be08e0766	N	
25/01/22 12:16	VID 2 sent	2e6bb5604cf4eb032081277b1e214266	N	
25/01/22 12:17	Wi-Fi switched off, airplane mode on		N/A	
25/01/22 14:23	Time rolled back 48 h		N/A	

Device: Samsung S6 – G920F				
Date/Time added	Data Description	Metadata (where applicable)	Deleted? Y/N	Date/Time Deletion
25/01/22 12:00	WhatsApp installed – v.2.22.2.7		N/A	
25/01/22 12:09	WhatsApp Setup		N/A	
25/01/22 12:14	"Hi"		N	
25/01/22 12:15	"Let's see how it does"		N	
25/01/22 12:16	PHOTO 1	2322d57a9f877bc6d68d2cbc3d66f477	N	
25/01/22 12:17	VID 1	2e2ca86c4c285e65ca24314d17bb2457	N	
25/01/22 12:17	Wi-Fi off, airplane mode on		N/A	
25/01/22 14:23	Rollback date/time – 48 h		N/A	

Group 4

Device: iPhone 6s – A1688				
Date/Time added	Data Description	Metadata (where applicable)	Deleted? Y/N	Date/Time Deletion
06/12/2021 15:57	Installed WhatsApp v 2.21.221		N/A	
06/12/2021 15:58	WhatsApp setup		N/A	
06/12/2021 16:07	Disappearing messages turned on – Samsung chat		N/A	
06/12/2021 16:08	"Hello there" message sent		N	06/12/2021 16:16
06/12/2021 16:08	"Yes. It is" message sent		N	
06/12/2021 16:09	"Here is another" Photo 2 sent	b2b97559501579af333e8e2be08e0766	N	
06/12/2021 16:12	Viewed Photo 3 via OTV		N	
06/12/2021 16:12	Photo 4 sent - OTV on	d922aa46456206cfdec390202799adca	N	
06/12/2021 16:13	Video 2 sent	7903acdb71152655fc9bf7aa0bbdf1f8	N	
06/12/2021 16:16	Video 4 sent – OTV on	222327ec820290c13ec9135d07f3f85d	N	
06/12/2021 16:17	Airplane Mode turned on – network isolated		N/A	
06/12/2021 16:17	Phone powered off		N/A	

Device: Samsung S6 – G920F				
Date/Time added	Data Description	Metadata (where applicable)	Deleted? Y/N	Date/Time Deletion
06/12/2021 16:03	WhatsApp installed – v.2.21.23.23		N/A	
06/12/2021 16:06	WhatsApp setup		N/A	
06/12/2021 16:07	Disappearing Messages turned on		N/A	
06/12/2021 16:08	"Hello" message sent		N	
06/12/2021 16:08	"This is a test" message sent		N	06/12/2021 16:16
06/12/2021 16:08	"Here is a photo" Photo 1 sent	2322d57a9f877bc6d68d2cbc3d66f477	N	
06/12/2021 16:09	Photo 2 downloaded		N	
06/12/2021 16:12	"You can only view this photo once" Photo 3 sent – OTV on		N	
06/12/2021 16:12	Viewed Photo 4 via OTV		N	
06/12/2021 16:13	Sent Video 1	2e2ca86c4c285e65ca24314d17bb2457	N	
06/12/2021 16:14	Video 2 downloaded	7903acdb71152655fc9bf7aa0bbdf1f8	N	
06/12/2021 16:15	Video 3 sent – OTV on	e1768de38f32f41952c09f728bf9452c	N	
06/12/2021 16:17	Airplane Mode on – network isolated		N/A	
06/12/2021 16:17	Handset powered off		N/A	

Group 5

Devices: iPhone 6s – A1688 Windows 10 - VM				
Date/Time added	Data Description	Metadata (where applicable)	Deleted? Y/N	Date/Time Deletion
15/12/21 10:48	Installed WhatsApp v 2.21.241		N/A	
15/12/21 10:54	WhatsApp setup completed		N/A	
15/12/21 10:55	Disappearing messages turned on		N/A	
15/12/21 11:03	SIM removed/Airplane Mode on – Wi-Fi left on		N/A	
15/12/21 12:16	WhatsApp Desktop linked to VM		N/A	
15/12/21 12:23	"Hello back" message sent		N	
15/12/21 12:24	"This message was sent through the phone"		N	
15/12/21 12:25	"And this one sent through the Desktop"		N	
15/12/21 12:25	"Here is one back from the phone" – Photo 2 attached	b2b97559501579af333e8e2be08e0766	N	
15/12/21 12:26	Photo 3 OTV viewed	7226d0aef3d336086d1d725b9f6ff2b	N	
15/12/21 12:27	"Here is a video from the phone" – VID 2 attached	7903acdb71152655fc9bf7aa0bbdf1f8	N	
15/12/21 12:29	"Delete this message"		Y	15/12/21 12:29
15/12/21 12:30	Wi-Fi OFF on iPhone, iPhone powered down		N/A	
15/12/21 12:31	VM powered down		N/A	

Device: Samsung S6 – G920F				
Date/Time added	Data Description	Metadata (where applicable)	Deleted? Y/N	Date/Time Deletion
15/12/21 10:48	WhatsApp installed – v.2.21.24.17		N/A	
15/12/21 11:02	WhatsApp setup completed		N/A	
15/12/21 11:04	SIM Card removed – restarted into Airplane Mode		N/A	
15/12/21 12:22	"Hello"		N	
15/12/21 12:24	"This is a test of WhatsApp Desktop"		N	
15/12/21 12:25	"Here is a photo" – PHOTO 1 attached	2322d57a9f877bc6d68d2cbc3d66f477	N	
15/12/21 12:26	Photo 3 OTV sent	7226d0aef3d336086d1d725b9f6ff2b	N	
15/12/21 12:27	"Don't open this one" Photo 3 sent	72c4e5bf05afddc7c6b40b4d7a3de296	N	
15/12/21 12:29	"Also delete this one"		Y	15/12/21 12:29
15/12/21 12:30	Wi-Fi OFF, Samsung powered down		N/A	

Group 6

Device: iPhone 6s – A1688				
Date/Time added	Data Description	Metadata (where applicable)	Deleted? Y/N	Date/Time Deletion
02/02/2022 13:00	Snapchat installed – v.11.64.0.38		N/A	
02/02/2022 13:15	Snapchat setup		N/A	
02/02/2022 13:21	"Hello"		N	
02/02/2022 13:21	"I will save this message" – iPhone saved		N	
02/02/2022 13:21	"Samsung save this message" – Samsung saved		N	
02/02/2022 13:25	Photo of evidence tape sent – Replayed & saved by Samsung		N	
02/02/2022 13:26	Timed (10s) photo of duct tape sent		N	
02/02/2022 13:28	Photo of screwdriver sent		N	
02/02/2022 13:30	"Neither will this"		N	
02/02/2022 13:31	Network isolated		N	
02/02/2022 13:31	iPhone powered off		N	

Device: Samsung S6 – G920F				
Date/Time added	Data Description	Metadata (where applicable)	Deleted? Y/N	Date/Time Deletion
02/02/2022 13:00	Snapchat installed – v.11.64.0.36		N/A	
02/02/2022 13:19	Snapchat setup		N/A	
02/02/2022 13:21	"Hello"		N	
02/02/2022 13:21	"This is a test of the disappearing messages"		N	
02/02/2022 13:21	"I will save this message" – Samsung saved message		N	
02/02/2022 13:21	"iPhone save this message" – iPhone saved		N	
02/02/2022 13:23	Photo of BIC pen sent – Saved by iPhone		N	
02/02/2022 13:23	Timed (10s) photo sent of screwdriver		N	
02/02/2022 13:28	Photo sent – Screwdriver		N	
02/02/2022 13:29	"This message will not be saved"		N	
02/02/2022 13:31	Network isolated		N	
02/02/2022 13:31	Samsung powered off		N	

Group 7

Device: iPhone 6s – A1688				
Date/Time added	Data Description	Metadata (where applicable)	Deleted? Y/N	Date/Time Deletion
09/02/2022 10:23	Telegram installed – v.8.5.1		N/A	
09/02/2022 10:24	Telegram account setup		N/A	
09/02/2022 10:26	"Hello"		N	
09/02/2022 10:28	Disappearing messages set to 24 h hours		N/A	
09/02/2022 10:28	"I have activated disappearing messages"		N	
09/02/2022 10:29	"Have a photo" PHOTO 2 attached	b2b97559501579af333e8e2be08e0766	N	
09/02/2022 10:30	VIDEO 2 attached	7903acdb71152655fc9bf7aa0bbdf1f8	N	
09/02/2022 10:30	"Can you delete messages?"		Y	09/02/2022 10:30
09/02/2022 10:32	Network Isolation > Powered down		N/A	

Device: Samsung S6 – G920F				
Date/Time added	Data Description	Metadata (where applicable)	Deleted? Y/N	Date/Time Deletion
09/02/2022 10:23	Telegram installed – v.8.5.1		N/A	
09/02/2022 10:25	Telegram account setup		N/A	
09/02/2022 10:26	"Hello there"		N	
09/02/2022 10:28	"We shall see how this does"		N	
09/02/2022 10:29	PHOTO 1 sent	2322d57a9f877bc6d68d2cbc3d66f477	N	
09/02/2022 10:30	VIDEO 1 sent	2e2ca86c4c285e65ca24314d17bb2457	N	
09/02/2022 10:31	"I will also delete this message"		Y	09/02/2022 10:31
09/02/2022 10:32	Network isolation > power down		N/A	

References

- Akinbi, A., Ojie, E., 2021. Forensic analysis of open-source XMPP multi-client social networking apps on iOS devices. *Forensic Sci. Int.: Digit. Invest.* 36, 301122. <https://doi.org/10.1016/j.fsidi.2021.301122>.
- Alyahya, T., Kausar, F., 2017. Snapchat analysis to discover digital forensic artifacts on android smartphone. *Procedia Comput. Sci.* 109, 1035–10407.
- Anglano, C., 2014. Forensic analysis of whatsapp messenger on android smartphones. *Digit. Invest.* 11 (3), 201–213.
- Anglano, C., Canonico, M., Guazzone, M., 2017. Forensic analysis of telegram messenger on android smartphones. *Digit. Invest.* 23, 31–49.
- Awrara, R., 2020. The Curious History of Snapchat and its Increasing Importance for Businesses. Retrieved 17 April 2023. Available at: <https://businesschief.com/digital-strategy/curious-history-snapchat-and-its-increasing-importance-businesses>.
- Azhar, M., 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.
- 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., Kim, J., 2021. Forensic analysis of instant messaging apps: decrypting Wickr and private text messaging data. *Forensic Sci. Int.: Digit. Invest.* 37, 301138. <https://doi.org/10.1016/j.fsidi.2021.301138>.
- Kim, G., Park, M., Lee, S., Park, Y., Lee, I., Kim, J., 2020. A study on the decryption methods of telegram X and BBM-Enterprise databases in mobile and PC. *Forensic Sci. Int.: Digit. Invest.* 35, 300998. <https://doi.org/10.1016/j.fsidi.2020.300998>.
- MacDermott, Á., Heath, H., Akinbi, A., 2022. Disappearing messages: privacy or piracy?. In: International Conference on Information Resources Management (CONF-IRM) 2022 Proceedings, vol. 10. <https://aisel.aisnet.org/confirm2022/10>.
- 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., Kim, K., 2022. Forensic analysis of instant messengers: decrypt signal, Wickr, and Threema. *Forensic Sci. Int.: Digit. Invest.* 40, 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>.
- United Nations, 2022. World Population by Year. Retrieved 27th March. Available at: <https://www.worldometers.info/world-population/world-population-by-year/>.
- WhatsApp, 2022. WhatsApp Help Center - about Disappearing Messages. Retrieved 23rd January 2022. Available at: <https://faq.whatsapp.com/general/chats/about-disappearing-messages/?lang=en>.
- Das, A., 2022. 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/>.