Snapchat Forensics for iOS

Sienna Bates
Computer and Information Technology
Purdue University
West Lafayette, Indiana
bates46@purdue.edu

Umit Karabiyik
Computer and Information Technology
Purdue University
West Lafayette, Indiana
umit@purdue.edu

***Abstract*—Snapchat is a widely known and commonly used app amongst social media users. This application was one of the first to introduce the concept of disappearing messages, photos, or videos after viewing. Forensic analysis has been performed on different aspects of the application, typically on Android devices, such as messaging, and photo and video sharing based on whether the message or photo really is "deleted" after the allotted 10 seconds. However, since such few analyses have been done on the forensics of this application on iOS devices, the aim of this study is to focus primarily on the application of forensics on Snapchat for iOS using Cellebrite and Magnet AXIOM and comparing the results of the analyzed data to see what can be recovered. Forensic analysis will be performed by the creation and population of user data on an iPhone using the latest version of Snapchat. The gap that will be addressed is assessing how messages and photos on the iOS Snapchat application are deleted as intended and if they are not, where they would be stored. The digital artifacts such as messages, photos, videos, stories, and location data were able to be recovered and where they were found during our analysis is also discussed. A comparison was made between the software used and which was able to recover the most amount of useful data that could be used during an investigation.**

***Index Terms*—Forensics, Snapchat, Magnet AXIOM, iOS, iPhone, Cellebrite**

I. Introduction

Currently, Snapchat is one of the largest social media platforms on the market allowing users to send photos and videos to other users [1]. Snapchat was first released in July of 2011 [2]. Fifty-nine percent to be exact, of all U.S. internet users aged 13 to 24 years use the photo-sharing app [3]. Snapchat has been used by both Android and iOS users for the past 10 years and has reported usually having more iOS users than Android users. Many of the forensic examinations that have been done on this application have typically been done on Android phones [4]. The aim of this study is to focus primarily on application forensic for Snapchat on an iOS device. The application that was chosen for this study was Snapchat because of its popularity amongst the younger generation. Snapchat has also been a top form of social media and messaging communication platform for the past ten years and its user base continues to grow. It remains highly ranked on the App Store and Google Play for "social apps" and "recommended for you" sections.

Forensic analyses have been done on earlier versions of the Snapchat application; however, since then, Snapchat has introduced some other features. This means that there are more opportunities for recovering evidence and seeing what can be found with commonly used forensic tools such as Cellebrite (v. 7.42.0.50) and Magnet AXIOM (v. 4.9.1.23338). Forensic Analysis has been performed on different aspects of the application such as messaging, photo, and video sharing based on whether or not the media really is "deleted" after the allotted 10 seconds. The platform originally only allowed photos and videos to be captured within that time frame [5]. However, now users have the option to set an unlimited time period for photos as well as send videos up to 60 seconds and 24 hours for stories [6] [7].

The gap that will be addressed is to assess how messages and photos on the iOS Snapchat application are deleted as intended and if they are not, where they would be stored and how to recover them. It is imperative more research is done for this application on these types of devices as the majority of users are teenagers and young adults – meaning that they potentially view the app as a more secure way of messaging. Also, Snapchat reports the majority of its users in the past use iOS devices [8]. In the event of an investigation, it needs to be understood what kind of data can be recovered from this application on this kind of device. In this paper, forensic analysis will be performed on the latest version of Snapchat to ensure all new and current features can also be analyzed properly. The analysis will be performed on the creation and population of user data using Magnet AXIOM and Cellebrite UFED Physical Analyzer.

In this paper, we have demonstrated our forensic analysis for analyzing the Snapchat application on the iPhone 7 iOS device. The acquisition process is explained and includes the challenges and assumptions made. We presented the results found from analysis using Magnet AXIOM and Cellebrite over what communications could be recovered after the allowed time period for viewing said communications has passed. The files acquired from the device are examined for the totality then compared to the originally populated data.

The rest of this paper is organized as follows: Section II provides both background information and related work about the Snapchat application for iOS. In Section III, a detailed methodology is provided that can assist law e4enforcement agencies that utilize this application that may be found or seized during an investigation. Section IV will analyze the results from both Cellebrite and Magnet AXIOM and Section V will discuss the relevance of the findings and conclude our

work.

II. Background and Related Work

In 2021, Snapchat reports having 293 million daily users [9]. The application is for short-term viewing of those same photos and videos and claims they are "deleted" after a certain time period. Snapchat is made for both Android and iPhone users Also, in 2021, Snapchat reported having more Android users than iOS for the first time ever [10]. Over the years Snapchat has introduced other features such as map, Bitmoji, stories, memories, and My Eyes Only. In previous analyses of this application, certain features were analyzed due to the scope of the study or not being available to be analyzed using certain forensic software.

Third-party applications for Snapchat were very common in Snapchat's early days, however, now only certain third-party apps are authorized to work with Snapchat. It is currently against their terms of service to use unauthorized third-party apps or plugins with Snapchat as it can cause a user's account to be inaccessible. This application was chosen for its popularity amongst younger generational users as well as its success on the app stores for both Android and iOS devices. There are currently over 911,400 ratings on the Apple App Store and ranked number three in the photo and video applications. Analyzing this application is representative of one of the currently most popular social media applications available on mobile app stores.

A. Android

Forensic analysis has also been completed by Alyahya and Kausar where they performed analysis on a Galaxy Note GT-N7000 running Android 4.1.2 [4]. These authors also used Magnet AXIOM to perform the forensic analysis examination as well as an open-source tool named Autopsy. During these analyses, both tools only provided textual preview of the files in the chat but were not able to indicate the sender or receiver. The Snapchat artifacts recovered were found in the cache, databases, and Snapchat folders in AXIOM. By looking through these folders, chats, profiles, sent and received messages, photos, and stories were able to be recovered. While these folders were able to be examined from an analysis of an Android phone, it is unclear whether or not similar folders exist in the file system for iOS devices too.

Snapchat artifacts are held in tcspahn.db on android devices. Examining that a user could find the list of activities and artifacts, list of texts with detailed information, conversations between users, locations of friend's profiles, list of stories with captions, and all story photos and videos. Video snaps can only be viewed via Autopsy. However, AXIOM Examine has also been able to present some of the photo snaps but without a preview.

AXIOM has proven to be more sophisticated than some of the open-source forensic tools. Instead of going through the physical image folders and database tables, AXIOM Examine presents list of Snapchat event logs, Snapchat friends, sent snaps, chat messages, and received videos at the home page of the platform [4]. Autopsy on the other hand, presents all analyzed artifacts of the physical image and categorize it (e.g. videos, images, audio) and it provides a keyword search and save it to be used for later use [4]. For Autopsy it generates an excel report for the user to view but is not consistent with providing enough information to be used as evidence in a court case. A representative from Magnet Axiom mentioned other functions of Snapchat can be recovered on some android devices such as Android updated support to recover attachments from messages and memories on some versions (10.68, 10.69) [11].

B. iOS

While few analyses have been published in academic journals about the forensics on this specific application, Snapchat investigations for iOS have had data collections entail recovering contact lists, timestamps, and message ID [12]. Digital image evidence can potentially result in metadata which can include information on the file size, name, and time stamps. Metadata can also include information about where the data comes from, when, and who sent it. Forensic analysis has been performed with the approach of using XML in order to save the data in XML format and using XQuery to access the database and other data from the disk's images [13].

Some other possible data sources for finding evidence of photos, videos, and messages on iOS devices are in the arroyo.db, primary.docobjects, scdb-27.sqlite3 databases. Snapchat uses end to end encryption and uses SHA256 to hash identifiers and metadata [14] [15] and AES156 CBC hashes depending on the location of the evidence. Being able to recover this evidence from a file system could help any forensic investigations that include recovering data from the Snapchat application on iOS devices.

A representative from Magnet AXIOM, Jamie McQuaid, mentioned that the ability to decrypt the memories function for iOS can only be acquired using GrayKey [11]. The My Eyes Only function can also be recovered and decrypted if the snaps have been viewed locally and are available in the applications media cache. But for iOS, a full file system from GrayKey will be necessary in order to get the necessary files to decrypt properly [11].

C. Acquisition Methods

Various types of extractions can be used to produce forensic images of smartphones. A forensic image can be identified and defined as a copy of the data contained on a given device. Any forensic investigator's objective is to obtain and record as much data possible from a device while ensuring that the same data is not altered in any way in the event it is used as evidence in a formal investigation. Cellebrite is a forensic tool that is commonly used for mobile forensics. Cellebrite has different types of extraction, logical, advanced logical, and physical [16]. Physical acquisitions take a bit for bit copy of the data during the acquisition phase. This type of acquisition captures all of the device's storage in addition to unallocated space which then provides the opportunity to

recover potentially deleted or hidden files. Cellebrite UFED Analyzer is an industry-standard tool that can be used on older iOS versions like the device that is being utilized for this study. File system acquisitions can also be used to obtain a filesystem with the internal system folders for either jailbroken iOS devices or rooted Android devices. However, either of these types of rooted or jailbroken devices can potentially have altered the evidence due to the change in file system during the process of rooting or jailbreaking [17].

The most encompassing method for performing an acquisition on a mobile device whether it be Android or iOS is a physical acquisition if it is possible. A physical acquisition will be performed on the device. The iOS device used in this study will need to be jailbroken in order to achieve this kind of acquisition on this iOS version. Having a jailbroken device will allow access to lower-level system functions which will lead to more complete acquisitions. For this study, iOS 12.0.1 will be used. Performing another analysis on this type of device with the same iOS could potentially lead to more evidence being able to be recovered from the application.

III. Methodology

This study followed a standard forensic model to acquire and analyze images from the iOS Apple device [18]. The device that was used and analyzed for this study was a 2016 iPhone 7 using the iOS version 12.0.1. This iPhone was used to ensure the most recent versions of the application software were analyzed for the study and were compatible with the analysis tools chosen.

The tools used in this study for the acquisition and analysis include Cellebrite UFED analyzer for the acquisition and Magnet AXIOM Examine for the analysis. Both of these are commonly used forensic tools that have been used by law enforcement agencies across the United States and other countries. Both of these aforementioned tools are capable of performing the acquisition and examination of this type of mobile device.

The forensic workstation utilized for this study was a Dell Optiplex 7060 running Windows 10 Pro. The workstation had 16 GB of RAM and an Intel Core i7-4770 processor.

Both a new iCloud and Gmail account were created for this study. The iCloud account was to set up the iPhone 7 as a new device. The Gmail account was used to confirm that Snapchat account. The device was configured to factory default settings. The phone was also connected to only one Wi-Fi network for the duration of this study. The outline for the methodology followed this process:

- Restored the device to factory settings.
- Configured the device using the newly created iCloud and Gmail accounts (Used for the configuration of Snapchat account).
- Installed the latest version of Snapchat.
- Performed a baseline physical acquisition of the device (iPhone 7)
- Populated the device with data.
- Allowed the device to send messages, photos, videos, post stories using the created account.
- Allowed the device to also delete messages and stories (Snapchat does not allow for the deletion of already sent photos and videos to another account).
- Performed a full system acquisition of the iPhone 7
- Analyzed the results in UFED Physical Analyzer and AXIOM Examine.

A. Data Population

To follow along with the National Institute of Standards and Technology (NIST) standards [18], each phone was populated with sample data. The application Snapchat (v 11.51.0.33) was downloaded and installed on a device provided for this study, the iPhone 7. A profile account was created with a username and password. A friend was added from the initial profile account to the authors personal account in order to populate conversation data in the form of messages, pictures, and videos.

The device was used to create and populate the data for a period of 72 hours. During this time photos, videos, and stories were posted, sent, and deleted using the created account. This is to simulate how a typical user may use the application and ensure an ample amount of data exists and is able to be analyzed. During this time, location services and Wi-Fi were enabled.

B. Acquisition

A physical acquisition of the iPhone was performed using Cellebrite and both Cellebrite and Magnet AXIOM will be used to do the analysis. This type of acquisition was chosen because of its capability of being supported across different types of forensic tools and devices and does not modify significant amounts of data.

C. Analysis

An advanced logical image was taken with Checkm8 on Cellebrite UFED. The same software was used to create a report using Cellebrite Physical Analyzer in order to make the case portable. The image created was then uploaded to Magnet AXIOM Examine and Cellebrite UFED reader in order to analyze and interpret results. Using both software to examine the image would allow for a comparison to be made on what could be recovered from each forensics tool.

IV. Results

Upon analysis of the image of the iPhone 7, many artifacts of forensic interest were able to be recovered from the device. A summary of the artifacts recovered from the image taken of the iOS device is listed in Table I. iOS provided access to a large amount of data from both forensic tools used for this study. After jailbreaking the device using Cellebrite, additional information was able to be found in the image which was then uploaded into Magnet AXIOM to compare the results.

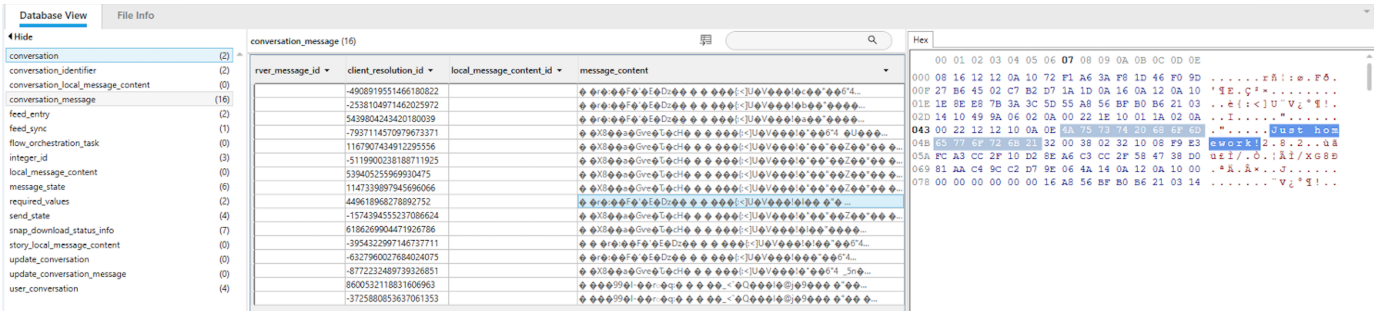

Fig. 1. Plain text of Snapchat Messages

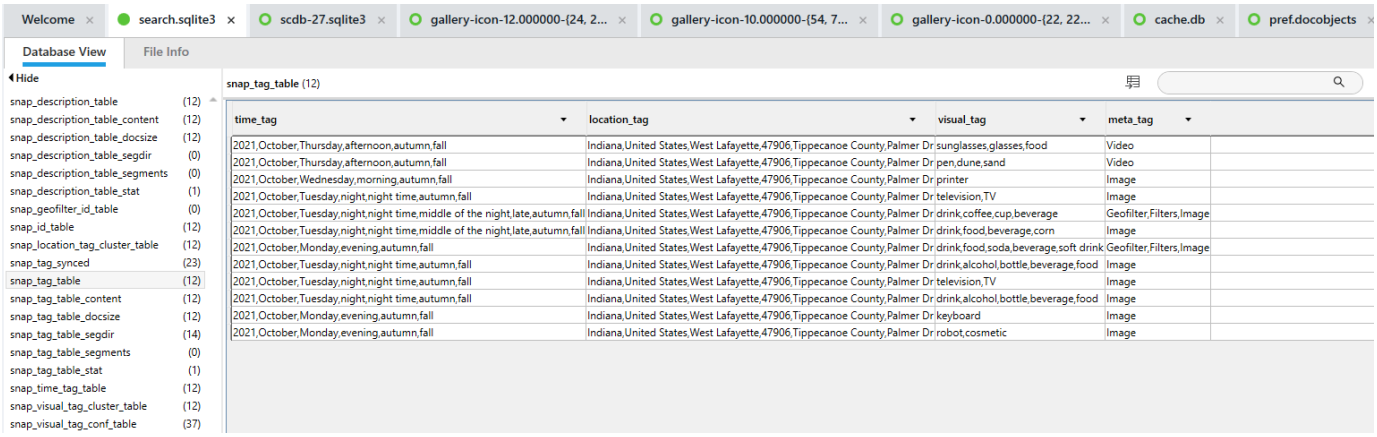

Fig. 2. Location, Time, Meta, and Visual tags of content sent and received from Cellebrite in `search.sqlite3` database

TABLE I
SUMMARY OF ARTIFACT AVAILABILITY

	Cellebrite	Magnet AXIOM
User Information	No	No
User Password	No	No
Photos	Yes	Yes
Videos	Yes	Yes
Stories	Yes	Yes
Memories	Yes	Yes
My Eyes Only	No	No
Location	Yes	No

A. Magnet AXIOM

The analysis of the image on Magnet AXIOM showed photos, videos, messages, memories, and stories were able to be recovered. All of this information was able to be found using the within the `\FullFileSystem.1.dar\private\var\mobile\Containers\Data\Application\15286BF5-6E2D-4F30-A63A-4621ABFA5855` folder in their respective locations in Table II. In Fig. 1, Snapchat messages can also be found in plain text hidden in the hex.

There was another feature of Snapchat that was unable to be recovered titled "My Eyes Only". While it is possible with GrayKey to recover Snapchat evidence from the My Eyes Only feature, that software is unavailable for public use [19].

Screenshots of the user information and user password were taken on the device when setting up the Snapchat application and saved to the camera roll. User information and password were not able to be recovered from Magnet AXIOM from the Snapchat application databases. Unlike the Cellebrite findings, no location data was able to be found either.

B. Cellebrite

The analysis of the image on Cellebrite showed similar findings to Axiom. Photos, videos, messages, and stories were able to be recovered. These all were able to be found in the `\DarArchive\root\private\var\mobile\Containers\Data\Application\15286BF5-6E2D-4F30-A63A-4621ABFA5855\Documents\user_scoped\0acd1389f326e811c2d57db5f8410a2b1e6a614ec86a505b7371fef5205e5598\arroyo\arroyo.db` folder shown in Table III. The user information and password was still unable to be recovered using Cellebrite.

The most informative finding from Cellebrite is shown in Fig. 2. Fig. 2 displays the location, meta, and visual tags from the content sent and received. This information was found in the `snap_tag_table` in the `search.sqlite3` database. The location tag shows the state, country, city, zip code, county, and even the street name of where each communication was sent and received. The visual tag states what items can be identified in the content. Meta tag shows what type of communication was sent and received such as photo or video.

TABLE II
IOS 12.0.1 (JAILBROKEN) ARTIFACT LOCATIONS - MAGNET AXIOM

Artifact Type	Application	Location
Messages	**Snapchat**	FullFileSystem.1.dar\private\var\mobile\Containers\Data\Application\15286BF5-6E2D-4F30-A63A-4621ABFA5855\ Documents\user_scoped\0acd1389f326e811c2d57db5f8410a2b1e6a614ec86a505b7371fef5205e5598\arroyo\arroyo.db
Photos	**Snapchat**	FullFileSystem.1.dar\private\var\mobile\Containers\Data\Application\15286BF5-6E2D-4F30-A63A-4621ABFA5855\ Documents\gallery_data_object\1\0acd1389f326e811c2d57db5f8410a2b1e6a614ec86a505b7371fef5205e5598\scdb-27.sqlite3
Videos	**Snapchat**	FullFileSystem.1.dar\private\var\mobile\Containers\Data\Application\15286BF5-6E2D-4F30-A63A-4621ABFA5855\ Documents\gallery_data_object\1\0acd1389f326e811c2d57db5f8410a2b1e6a614ec86a505b7371fef5205e5598\scdb-27.sqlite3 FullFileSystem.1.dar\private\var\mobile\Containers\Data\Application\15286BF5-6E2D-4F30-A63A-4621ABFA5855\ Library\Caches\SCPersistentMedia\cm-chat-media-video-1:1e8ee87b-3a3c-5d55-a856-bfb0b6210314:31:0:0.mov
Stories	**Snapchat**	FullFileSystem.1.dar\private\var\mobile\Containers\Data\Application\15286BF5-6E2D-4F30-A63A-4621ABFA5855\ Documents\stories.plist
Memories	**Snapchat**	FullFileSystem.1.dar\private\var\mobile\Containers\Data\Application\15286BF5-6E2D-4F30-A63A-4621ABFA5855\ Documents\gallery_data_object\1\0acd1389f326e811c2d57db5f8410a2b1e6a614ec86a505b7371fef5205e5598\scdb-27.sqlite3

TABLE III
IOS 12.0.1 (JAILBROKEN) ARTIFACT LOCATIONS - CELLEBRITE

Artifact Type	Application	Location
Messages	**Snapchat**	DarArchive\root\private\var\mobile\Containers\Data\Application\15286BF5-6E2D-4F30-A63A-4621ABFA5855\ Documents\user_scoped\0acd1389f326e811c2d57db5f8410a2b1e6a614ec86a505b7371fef5205e5598\arroyo\arroyo.db
Photos	**Snapchat**	DarArchive\root\private\var\mobile\Containers\Data\Application\15286BF5-6E2D-4F30-A63A-4621ABFA5855\ Documents\gallery_data_object\1\0acd1389f326e811c2d57db5f8410a2b1e6a614ec86a505b7371fef5205e5598\scdb-27.sqlite3
Videos	**Snapchat**	DarArchive\root\private\var\mobile\Containers\Data\Application\15286BF5-6E2D-4F30-A63A-4621ABFA5855\ Documents\gallery_data_object\1\0acd1389f326e811c2d57db5f8410a2b1e6a614ec86a505b7371fef5205e5598\scdb-27.sqlite3 DarArchive\root\private\var\mobile\Containers\Data\Application\15286BF5-6E2D-4F30-A63A-4621ABFA5855\ Library\Caches\SCPersistentMedia\cm-chat-media-video-1:1e8ee87b-3a3c-5d55-a856-bfb0b6210314:31:0:0.mov
Stories	**Snapchat**	DarArchive\root\private\var\mobile\Containers\Data\Application\15286BF5-6E2D-4F30-A63A-4621ABFA5855\ Documents\stories.plist
Memories	**Snapchat**	DarArchive\root\private\var\mobile\Containers\Data\Application\15286BF5-6E2D-4F30-A63A-4621ABFA5855\ Documents\gallery_data_object\1\0acd1389f326e811c2d57db5f8410a2b1e6a614ec86a505b7371fef5205e5598\scdb-27.sqlite3

Also within the meta tag it can identify whether a filter or Geo-filter was used on the photo. Geo-tags are specific to the location of where the photo was taken. The time tag also specifies the year, month, day, time of the day, and season of when the content was taken.

V. DISCUSSION AND CONCLUSIONS

Based on the results presented it was found that artifacts of importance can be recovered from the Snapchat application on the iOS device. Digital forensic investigators may be able to recover conversations and photos previously thought to have been "deleted" or disappeared from both the sender and receiver. The amount of information available will be dependent on whether a full file system is available, and the operating system of the device being examined.

The first steps that should be taken when approaching an application with supposed "disappearing" messages function such as Snapchat, is determination of the operating system the device uses. This would help a forensic investigator determine what the most appropriate acquisition method would be in order to get the most data recovered from the device. Some tools are more functional and can allow for more results to be found depending on whether one is using open source or licensed forensic tools. The results that were able to be recovered were found within the devices normal file system which any forensics tools should be able to analyze. Tools that can decode and visually display each database and its contents is heavily recommended due to the number of relevant artifacts that can be found within a database file. For iOS devices, the investigator needs to check whether the device is jailbroken. If the device is jailbroken, then the results in Table II and Table III depending on which forensics software is being used.These file paths are the most appropriate place to look for evidence.

A digital investigator should be careful when jailbreaking or rooting a mobile device. Jailbreaking or rooting can result in additional artifacts being available, it also changes the data permanently on an iOS device [17]. Artifacts from the logical acquisition should be considered first before attempting to reverse a jailbreak.

The amount of information found overall supports the research aim of how media is deleted and stored within the Snapchat application. The data available could assist in solving investigations where this app is used commonly for communication purposes and is "disappearing" messages appeal. It is possible to see what types of content users are sending back and forth as well as the content within those photos, videos, and messages. It can also show where the content has been sent and received from down to the street address depending on the forensics tool used. This work also shows the importance of understanding "disappearing" messages do not always disappear after a given time frame and are still able to be recovered using certain software and tools.

Future work would include extending this work to other disappearing messaging applications, or even applications that have disappearing messaging functions even if that is not the main purpose of that application. Additional analysis could be done by law enforcement agencies who have access to GreyKey for Magnet AXIOM in order to recover things that are password protected within the Snapchat application such as My Eyes Only. This study was limited to just a singular iOS device but would have been beneficial to see additional

analysis using more devices including Androids. By using more than one device, Cellebrite and AXIOM might have been able to recover additional artifacts or further validate the results. Another possible research area is to look more into the location data from this application to see where and how the application tracks media coming from multiple sources and if it can separate out the interactions.

REFERENCES

[1] S. Inc., "Snapchat application."

[2] B. Gallagher, "Snapchat's spiegel admits brown "came up with the idea for disappearing picture messages" in new court documents," July 2013. [Online]. Available: https://techcrunch.com/2013/07/01/new-snapchat-docs/

[3] S. Kemp, "Digital 2021: Global overview report - datareportal – global digital insights," Oct 2021. [Online]. Available: https://datareportal.com/reports/digital-2021-global-overview-report

[4] T. Alyahya and F. Kausar, "Snapchat analysis to discover digital forensic artifacts on android smartphone," *Procedia Computer Science*, vol. 109, pp. 1035–1040, 12 2017.

[5] "Snapchat," Dec 2021. [Online]. Available: https://en.wikipedia.org/wiki/Snapchat#Core_functionality

[6] "When does snapchat delete snaps and chats?" [Online]. Available: https://support.snapchat.com/en-US/article/when-are-snaps-chats-deleted

[7] J. Still, "'how long are snapchat videos?': How to take longer snapchat videos and share them with your contacts," May 2020. [Online]. Available: https://www.businessinsider.com/how-long-are-snapchat-videos

[8] A. Carman, "Snapchat now has more users on android than ios," Apr 2021. [Online]. Available: https://www.theverge.com/2021/4/22/22398237/snapchat-android-app-ios-earnings

[9] A. Heath, "Snapchat is growing faster than it has in years," July 2021. [Online]. Available: https://www.theverge.com/2021/7/22/22589236/snapchat-users-293-million-q2-2021

[10] A. Carman, "Snapchat now has more users on android than ios," April 2021. [Online]. Available: https://www.theverge.com/2021/4/22/22398237/snapchat-android-app-ios-earnings

[11] J. McQuaid, "Snapchat for my eyes only encryption," May 2019. [Online]. Available: https://www.forensicfocus.com/forums/mobile-forensics/snapchat-for-my-eyes-only-encryption/

[12] M. Aji, I. Riadi, and A. LUTFHI, "The digital forensic analysis of snapchat application using xml records," *Journal of Theoretical and Applied Information Technology*, vol. 95, 10 2017.

[13] B. d. V. Alink, Bhoedjang, "Xiraf – xml-based indexing and querying for digital forensics," pp. S50–S58, June 2006. [Online]. Available: doi:10.1016/j.diin.2006.06.016

[14] S. Inc., "Snap pixel faqs." [Online]. Available: https://businesshelp.snapchat.com/s/article/snap-pixel-faq?language=en_US

[15] S. Encrypt, "Is snapchat privacy-friendly? [analysis]," Jan 2021. [Online]. Available: https://choosetoencrypt.com/privacy/is-snapchat-privacy-friendly/

[16] "What happens when you press that button?" [Online]. Available: https://smarterforensics.com/wp-content/uploads/2014/06/Explaining-Cellebrite-UFED-Data-Extraction-Processes-final.pdf

[17] Y.-T. Chang, K.-C. Teng, Y.-C. Tso, and S.-J. Wang, "Jailbroken iphone forensics for the investigations and controversy to digital evidence," vol. 26, pp. 19–33, 07 2015.

[18] R. Ayers, B. Livelsberger, and B. Guttman, "Quick start guide for populating mobile test devices," *NIST 800-202*, 2018. [Online]. Available: https://10.6028/NIST.SP.800-202

[19] M. Forensics, "Decrypt app data using the ios keychain and graykey," https://support.magnetforensics.com/s/article/Decrypt-app-data-using-the-iOS-Keychain-and-GrayKey, June 2021.