Available online at www.sciencedirect.com

ScienceDirect

Procedia Computer Science 109C (2017) 1035–1040

Procedia Computer Science

www.elsevier.com/locate/procedia

The 7th International Symposium on Frontiers in Ambient and Mobile Systems
(FAMS 2017)

Snapchat Analysis to Discover Digital Forensic Artifacts on Android Smartphone

Tadani Alyahya, Firdous Kausar*

Computer Science Department ,College of Computer and Information Science
Al Imam Mohammad Ibn Saud Islamic University (IMSIU), Riyadh, KSA
t.n.alyahya@gmail.com, firdous.imam@gmail.com

Abstract

Smartphones play an important role in our lives. With the advent of applications for smartphones, the more functionalities and services are offered to users. Online social networks (OSN) applications are the most popular applications worldwide. OSN applications, such as Facebook and Twitter, allow users to share personal information such as posts, age, gender, location, photos and videos. This valuable information saved on smartphones' internal memory and could be used as evidence during forensic investigation. Snapchat is a popular OSN application that is available for Android and iOS devices. It allows users to share photos and videos called *Snaps* with predetermined time to view. Once the time expired, snaps are automatically deleted. This paper analyses artifacts saved by Snapchat application on Android smartphones and identifies their significance to the forensic investigation process.

Keywords: Android; Smartphone; Forensic analysis; Autopsy; Magent Axiom; Snapchat

1. Introduction

OSN applications are the most popular applications worldwide such as Facebook and Twitter. They allow users to share personal information such as posts, age, gender, location, photos and videos. These valuable information saved on smartphones' internal memory and could be used as evidences during digital forensic investigation.

* Corresponding author. Tel.: +966112597556; fax: +966112597546.
E-mail address: t.n.alyahya@gmail.com

10.1016/j.procs.2017.05.421

Therefore, there is increasing interest in exploring artifacts (digital evidence) saved by OSN applications on smartphones internal memory. Al Mutawa et al.[2] studied the activities performed on Facebook, Twitter, and Myspace. They determined the recovered activities from the internal memory of different smartphone platforms. Said et al.[3] examined artifacts created by Facebook and Twitter on three different smartphones platforms. Andriotis et al.[4] presented a model that connects the OSN activity of suspects with their evidence emerged and extract them from their Android smartphones. Jang et al.[5] examined, analyzed and compared artifacts left by Facebook on Android-based smartphone by suing suggested digital forensic process. Chu et al.[6] examined Facebook on smartphones and discovered previous Facebook user accounts (e-mail address) that were logging in without shutting off the power.

Snapchat[7] is an OSN application that allows users to send instant messages, stories, and snaps (photos and videos). A story is list of items (images and videos) that are publicly seen by friends who added a user. The story is available only for 24 hours and then deleted automatically. The user can save his story and can delete any item from his story, as a consequence, friends cannot view the deleted item any more. The user can chat with friends privately by sending snaps and messages. He cannot view the snaps (photos and videos) once they are sent. The recipient friend can view the received snaps only once and then deleted. Sometimes, there is an option to replay the recent received snaps. The user can view his chat message by saving it once he sends it or before his friend views it. Otherwise, the chat message will be deleted. Although most of the suspect's Snapchat activates are deleted when he caught, the activates can be recovered from the internal memory of his smartphone. Thus, there is a need to study the artifacts left by Snapchat on the internal memory.

Mobile device forensics generally involve a basic procedure for successful investigation. The procedure consists of acquisition phase, examination and analysis phase, and reporting phase. Most of the popular mobile forensic tools are interactive programs that were designed to make visible information that is hidden or hard to find such as Oxygen and UFED. They allow the examiner to extract the internal memory of smartphone and automatically analyze and generate a summarized report to be presented in the courtroom. These tools are friendly but extremely expansive. However, most of the open-source tools are not friendly and do not include all the mobile device forensics phases.

In this paper we analyzed Snapchat artifact on the Android platform using two forensic analysis tools, Autopsy and AXIOM Examine. Autopsy[8] is an open source digital forensic tool that allows you to examine either hard drive or mobile device in order to recover evidence from it. AXIOM[9] is a digital forensic platform developed by Magnet Forensics. The AXIOM platforms consist of two applications, AXIOM Process and AXIOM Examine. The AXIOM Process acquires and processes evidences from computes or mobile devices. The AXIOM Examine analyzes and examine the evidences. It should be noted that AXIOM is not free. We used a trial version.

The rest of the paper is organized as follows. Section 2 presents some of the resent studies related to our work. Section 3 shows the our methodology. Section 4 provides a analytical study of Snapchat artifacts. Section 5 discusses the results of the experiment. Section 6 concludes with summery and some proposed future work.

2. Related work

A. Mahajan et al.[10] conduct a forensic analysis of two instant messages application, WhatsApp and Viber, on five Android smarphones. Cellebrite UFED Classic Ultimate is used to physically acquire the internal memory of the smartphones. They performed the forensic analysis using UFED physical Analyzer and a Manual Analysis. The UFED physical Analyzer presents chat sessions of the users using WhatsApp and timestamps for every chat. However, it did not show any artifacts related to Viber. Manual analysis discovered that WhatsApp application stores its activities in two databases; one stores the logs and records including chat, the other stores contact list. Similar to WhatsApp, Viber application stores a record and logs of all messaging history and calling sessions send and received by the user in a database.

K. Alzaabi et al.[11] propose a set of ontologies, named F-DOS, that models the content of smartphone for the purpose of forensic analysis. F-DOS enables a forensic analysis system to encode the semantics of the smartphone content using concepts and their relationships. The advantages of this encoding are a unified representation of evidence, facilitate evidences to be explored, and the ability to perform reasoning to infer new implicit knowledge from explicit ones.

I. Akarawita et al.[12] developed the first open-source mobile forensic tool, named ANDROPHSY, that support the entire cycle of mobile forensic procedure. Its performance and features compete other popular commercial tools in the market. The analysis phase of Android application files collected through logical acquisition. It provides SQLite decoder into the tool to facilitate analysis of custom applications. It also offers the activity time line, file browser, and hex view in the tool. Moreover, it creates a sample MD5 hash repository of Android application. The MD5 hash can be used on demand to compare application file Md5 against repository for best and accurate results. ANDROPHSY analyzer contains file carving, and keyword searching features. It generates a text files which contain the extracted strings from raw image with their byte offset.

In this research [13], the author evaluated three forensic analysis tools, Pladin Forensic Suits, Autopsy, and Andriller on Android and iOS smartphones. Pladin was able to image two tested Android smartphones, while Autopsy imaged one Android smartphone. They were unable to use Pladin, and they had problem in dealing with databases in Autopsy. In Andriller, they used only Android Backup method for extraction on five Android smartphones. They could recover from four smartphones Wi-Fi passwords, Android web backup history, Android download history, and contacts. The fifth smartphone was not recognized.

3. Methodology

This section will provide details about the methodology used in the experiment.

3.1. Tools used

- Windows 7.
- Samsung Galaxy Note GT-N7000 (running Android 4.1.2) with Snapchat application (version 9.21.0 1).
- Magnet AXIOM forensic tool trial version (version 1.0.8.3142) and Autopsy (version 4.2.0).
- USB data cables.

3.2. File naming and delivery

The created scenario of the expected forensic Snapchat artifacts is as follows:

- Create test account for Snapchat.
- Received and automated chat message form Snapchat.
- 5 Friends added to the test account.
- Sent story images and photos.
- Delete story images and photos.
- Sent and received snaps (chat messages, photos, and videos).

Table 1 shows Snapchat data setup in 24 hours.

Table 1. Snapchat data setup.

	User	Friends	Sent direct			Received direct			Story		
			Photo	Video	Message	Photo	Video	Message	Photo	Video	Deleted
#	1	6	20	20	20	26	16	16	13	13	4

3.3. Physical acquisition

The acquisition was done using Magnet AXIOM which was introduced by Magnet Forensic. AXIOM platform is comprised of two applications: AXIOM Process and AXIOM Examine. AXIOM Process performs a full or quick recovery image automatically to be ready for examination and analysis. In this section we will perform a manual analysis using both tools.

Using the AXIOM Process, we were able to create a physical image of Galaxy Note memory. Prior acquisition, the Debugging mode was enabled in the Galaxy Note in order AXIOM Process reboot it automatically. AXIOM

Process provides the option to calculate hash values. It also provides the option to select the artifacts from a particular application to be analyzed further using AXIOM Examine. Then the AXIOM Process performed the physical acquisition and transferred the copied image to the computer over a USB cable. It took about 3 hours to recover 14.6 GB memory.

3.4. Analysis

A detailed description of the analysis examination of the acquired images is presented in the Forensic Analysis Examination section.

4. Forensic analysis examination

In this section we focused on analyzing the Snapchat artifacts. The analysis of the recovered image was done using AXIOM Examine and Autopsy. The most relevant evidence for Snapchat application resided in the main snapchat archive and in the data of snapchat folder (see Table 2). Table 3 shows the content of each folder. Files and data that we did not identify as being of forensic value have been omitted in this list.

Table 2. Snapchat artifacts location in the physical memory.

Forensic analysis tools	Data folder	Snapchat archive
AXIOM Examine	Partition 10/data/com.snapchat.android/	Partition 11/snapchat/
Autopsy	vol15/data/com.snapchat.android/	vol16/ snapchat/

4.1. cache folder

AXIOM Examine and Autopsy provided only textual preview of files in the chat, profile, received image and video snaps folders, with detailed file metadata (e.g. name, type, size and created time). Both tools did not indicated the sender nor the receiver of the received image and video snaps.

Autopsy has the preferences in showing the story snaps photos over AXIOM Examine. It provided visual preview of the 13 photos and a textual preview of 1 deleted story photo. Unfortunately, only textual preview for 13 story videos. AXIOM Examine provided only textual preview of photos and videos stories.

Table 3. Snapchat artifacts.

Folder	Location	Content
cache	/data/com.snapchat.android/	Chat Profile Received image snaps Received video snaps Snaps Stories
databases	/data/com.snapchat.android/	tcspahn.db tcspahn.db-journal
snapchat	/snapchat/	Sent and deleted images and videos snaps

4.2. databases folder

AXIOM Examine has the preferences in showing the databases of evidences in tabular format over Autopsy. Databases were not installed on the program or computer which limited Autopsy as an analyzer tool. SnapChat artifact is held in tcspahn.db . Table 4 shows the key tables in this database. Tables that we did not identify as being a forensic value have been omitted.

Table 4. Structure of tcspahn.db.

Table	Content	#
AnalyticEvents	List of activities and artifacts on Snapchat.	-
Chat	List of text messages with detailed information such as sender, receiver, status, etc.	18
ChatRecivedInLastHour	List of text messages received in the last hour.	3
Conversation	List of conversations between user and friends.	6
FriendProfileImageFile	Locations to friends profiles.	0
Friends	List of friends with detailed information such as display name added time, best friends, etc.	5
FriendsWhoAddedMe	List of friends who added the user with detailed information such as display name, best friends, etc.	5
MyPostedStorySnapTable	List of story snaps by user showing caption text written on snaps.	26
MySnapImageFileTable	Locations to all story photo snaps.	13
MySnapVideoFileTable	Locations to all story videos snaps.	13
PreviewSnapVideoFileTable	Locations to previews snap videos.	4
ProfileImageFile	Locations to profile images.	3
ReceivedSnapImageFileTable	Locations to received snap photos.	1
ReceivedSnap	List of received snaps with detailed information such sender, time, status, etc.	1
SentSnaps	List of sent direct snaps with detailed information such receiver, time, status, etc.	21
SnapVideoFiles	Locations to sent snap videos.	1

4.3. Snapchat folder

AXIOM Examine as well as Autopsy presented visually some of the photo snaps. They indicate the deleted snap with no preview. The video snaps can only be viewed by Autopsy.

5. Results discussion

AXIOM Examine is more sophisticated program than Autopsy. It is more friendly with evidence view options. It enables the user to analyze the recovered image and presents specific applications artifacts instead of entire evidences. In our situation we selected Snapchat application to be presented. It generates separated text file reports about the case. 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. In Snapchat event logs, it shows a sequenced events of activities and artifacts. In Snapchat friends list, all the 5 friends were listed. User names and friends are indicated along with the date and time of adding friends. In sent snaps list, 42 snaps were listed, half of them are duplicated due to different location. The recipient, data and time, status (sent, opened, and delivered) are presented. The type of sent snap is not included. In the chat messages list, AXIOM Examine showed overall 26 sent chat messages, 11 chats were duplicated. It also showed overall 11 received chats, 5 chats were duplicated. AXIOM Examine indicates sender, receiver, date and time, the message, status (sent and delivered), and status of saving or releasing message by either sender or receiver. Some messages may be duplicated due to different location. In received videos, only one snaps was presented form 16 received videos snaps. AXIOM Examine specifies its name, type, size, creation and access time, and location. The main disadvantages of AXIOM Examine are:

- Not all artifact are presented in the home page such as stories, sent snaps, and received snaps photos.
- Evidences, such as chat messages and sent snaps, are duplicated at the home page.
- It does not have a visual preview for sent video snaps.
- Deleted snaps are not presented.

Autopsy on the other hand, presents all analyzed artifacts of the physical image and categorize it (e.g. videos, images, audio). It provides a keyword search and save it to be used for later use. It generates an Excel file report about the case, but it does not contain enough information to be used in the courtroom. The presented artifacts cannot be determined whether it is a story or sent snap. Chat messages are stored in tcspahn.db database which cannot be viewed. The main disadvantages of Autopsy are:

- Cannot preview databases.

- Not all snaps artifact are presented in the home page such as stories, sent snaps, received snaps photos, chat messages, user, and friends.
- Snaps are not specified whether are story or direct snap.
- Sender and receiver of snaps are not indicated.
- Deleted snaps are not presented.
- Chat messages, user, and friends must be searched manually in databases.

Table 5 compares between Autopsy and AXIOM Examine in the term of recovered Snapchat artifacts.

Table 5. Recovered Snapchat artifacts.

Forensic analysis tools	Profile		Sent snaps			Received snaps		Chat
	User	Friends	Photo	Video	Deleted	Photo	Video	messages
Autopsy	-	-	2	2	0	0	0	0
AXIOM Examine	1	5	21		0	0	1	21

6. Conclusion

In this paper we analyzed Snapchat artifacts on the Android platform using AXIOM Examine and Autopsy forensic analysis tools. The Snapchat artifacts were acquired from Samsung Galaxy Note GT-N7000 using AXIOM Process. Autopsy viewed 10% images and 10% videos. Basic information about type, size and time were stated, but it did not indicate the if they are a story snaps or chat snaps. It was not able to indicate deleted snaps, chat messages, user, and friends. AXIOM Examine present textual view of event logs, sent snaps, 100% friends, 100% user, 58% chat messages, and 6% delivered video with detailed information about artifact such as sender, receiver, time, and status. Sent snaps and chat messages evidence lists were suffering from duplicating artifacts. It was not able to indicate deleted, story, and delivered photo snaps. By using manual analysis with the help of both tools, more artifacts were found. Autopsy viewed chat snaps and story snaps, while a textual preview of received snaps. It indicated the deleted snaps with its type without preview. Same as Autopsy, AXIOM Examine viewed chat snaps, while a textual preview of received snaps. It indicated the deleted snaps with its type without preview. However the video snaps presented textually. It has the advantage over Autopsy in presenting Snapchat database artifact. Manual analysis found 100% friends, 100% user, 50% chat messages, 100% story photo snaps, 100% story video snaps, 50% deleted snaps, 52.5% sent snaps, 6% received video snaps.

References

1. Egham, "Gartner.," 2016. [Online]. Available: http://www.gartner.com/newsroom/id/3323017. [Accessed 12 1 2017].
2. N. Al Mutawa, I. Baggili, A. Marrington, "Forensic analysis of social networking applications on mobile devices", *Digital Investigation* 9, Supplement, 0 (2012), pp. S24 - S33.
3. H. Said, A. Yousif, and H. Humaid, "IPhone forensics techniques and crime investigation", in *Current Trends in Information Technology (CTIT), 2011 International Conference and Workshop on* (, 2011), pp. 120-125.
4. P. Andriotis, Z. Tzermias, A. Mparmpaki, S. Ioannidis, and G. Oikonomou, "Multilevel Visualization Using Enhanced Social Network Analysis with Smartphone Data", *Int. J. Digit. Crime For.* 5, 4 (2013), pp. 34-54.
5. Y. Jang and J. Kwak, "Digital forensics investigation methodology applicable for social network services", *Multimedia Tools and Applications* (2014), pp. 1-12.
6. H. Chu, S. Yang, C. Hsu, and J. Park, "Digital evidence discovery of networked multimedia smart devices based on social networking activities", *Multimedia Tools and Applications* 71, 1 (2014), pp. 219-234.
7. Snapchat, [Online]. Available: https://www.snapchat.com/l/en-gb/. [Accessed 15 1 2017].
8. Autopsy, [Online]. Available: https://www.sleuthkit.org/autopsy/. [Accessed 15 1 2017].
9. Magnet AXIOM, [Online]. Available: https://www.magnetforensics.com/magnet-axiom/. [Accessed 15 1 2017].
10. A. Mahajan, M. Dahiya and H. P. Sanghvi, "Forensic Analysis of Instant Messenger Applications on Android Devices," *International Journal of Computer Applications,* vol. 68, no. 8, p. 0975 – 8887, 2013.
11. M. Alzaabi, T. A. Martin, K. Taha and A. Jones, "THE USE OF ONTOLOGIES IN FORENSIC ANALYSIS OF SMARTPHONE CONTENT," *The Journal of Digital Forensics, Security and Law : JDFSL,* vol. 10, no. 4, pp. 105-113, 2015.
12. I. U. Akarawita, A. B. Perera and A. Atukorale, "ANDROPHSY-forensic framework for Android," 2015.
13. "An Analysis of Smartphones Using Open Source Tools versus the," Marsheall Univ. Forensic Science Center, Huntington. Available: http://www.marshall.edu/forensics/files/BACHLER_MARCIE_Research-Paper_Aug-5.pdf