THE DIGITAL FORENSIC ANALYSIS OF SNAPCHAT APPLICATION USING XML RECORDS

[1]MUKHLIS PRASETYO AJI, [2]IMAM RIADI, [3]AHMAD LUTFHI

[1]Department of Informatics Engineering, University Islam of Indonesia, Yogyakarta, Indonesia

[2]Department of Information System, Ahmad Dahlan University, Yogyakarta, Indonesia

[3]Department of Informatics Engineering, University Islam of Indonesia, Yogyakarta, Indonesia

E-mail: [1]prasetyo-aji@ump.ac.id,[2]imam.riadi@is.uad.ac.id, ahmad.lutfhi@uii.ac.id

ABSTRACT

The use of social media such Snapchat is quite popular in the United States. It is a free chatting application that allows the users to send images and videos, but it will remove the postings temporally. Uploading improper images and videos on social media becomes recent trends done by teens, even children. They do not realize the negative impact of posting their personal images and videos in virtual public area; it can trigger cyber-bullying and sexting. Some previous researches on the issue observed whether or not the files of image and video uploaded in Snapchat are really removed permanently. The researchers also observed whether or not metadata trace relating to images and videos location that have been sent by the users, and where Snapchat saves the files sent by them. The previous researchers found digital evidences of XML Records relating to Snapchat in saving images on a folder named com.snapchat.android_preferences.xml. The folder contains important information. The other things is existence of a folder named received_image_snaps. It contains program/s for removing files; it is ".nomedia" extention. If a directory has a file named ".nomedia" extention, so the hardware saving media would not scan and record metadata file in the directory.Therefore, this research is expected to reveal where Snapchat saves the data, how to recover images or videos, and how the correlation between XML Records and image name on Snapchat. Therefore, it is important to know the related files in XML records and image name to ease and accelerate investigation process.

Keywords: *Digital Forensics, Snapchat, XML records.*

1. INTRODUCTION

Internet is a media providing innovative results or products of technology. According to an analysis of 'We Are Social's", a social marketing agency, that issues its annual report on data of users using website mobile connections and social media all over the world, development of digital world in Indonesia achives 88.1 active internet users; 79.0 of them are social media users [1].

One of popular social media is Snapchat. It is a free chatting application. It allows the users to send images and videos, but it will remove the postings temporally [2]. A journal titled "Snapchat and Sexting" discusses roles of Snapchat in revolutionizing its users' behavior. It informs content exchange among the users, especially the improper contents such as pornographic images/videos, becomes a new trend in the virtual world [3]. In Google searching engine, the search results of keywords such "Snapchat Revenge Porn" and "Snapchat Adult" will show pornographic images from Snapchat. Knowthnet reveals more than 43% of 12 years old children have tried sexting for the first time. It is a threat on cyber-bullying and sexting that massively grows [4]. In addition, many users of Snapchat use it for cyber-crime and pornographic purposes.

This research is quite interesting to conduct because of the sexting phenomenon. The users assume their posting will remove themselves automatically, but in fact, the contents can be recovered. Hikman on his research said, the contents in forms of image and video can be recovered [5]. Therefore, this research is expected to find digital evidences used to reveal the criminals doing cyber-crimes or to be the evidences in courts.

This research result will reveal whether or not the content uploaded on Snapchat is permanently removed, and whether or not the existence of metadata related to Snapchat. Most of data is available in data/data/com.snapchat.android. In the folder, the are some folders inside; one of them is a folder named shared_prefs folder are several XML files. It contains some folder CameraPreviewActivity.xml,com.google.android.gcm.xml,com.snapchat.android_preferences.xml, and SnapPreviewActivity.xml. In the other hand, folder com.snapchat.android_preferences.xml is a quite important information storage [5].

Other interesting fact dealing with digital evidence is an existence of folder named received_images_snaps, and there is also a program for removing file; it is extension ".nomedia"[6]. Snapchat has file directory named .nomedia. If the directory has a file named .nomedia, so saving media will not scan and record metadata file on the directory"[6].

The folder named received_image_snaps has existence of .nomedia added in the last file name, it becomes something that is interesting to study, especially on the correlation between XML records and name of images. It because of a correlation between note on the file named com.snapchat.android_preferences.xml and file name of images saved on the folder named received_image_snaps. The fact says it is easier to obtain the artifact on Android; it is on a folder named com.snapchat.android/cache/my_media and rec_received_image_snaps with each image and video added with .nomedia extension [7]. In the other hand, users of iOS can faind it on cache/SCMediaCache, but the images and videos cannot be found manually, it should be with digital forensic way [8].

Therefore, the researcher will conduct the research both on iOS and Android, in the aspect of how Snapchat save the files of images and videos. It is also for contributing to analysis of digital forensics to overcome cyberbulliying and sexting which are massively growing.

2. BASIC THEORY

2.1 Related Researches

In a journal entitled "Network and device forensic analysis of Android social-messaging applications", those who want to conduct a research on social media can re-construct and take the data such password, screenshots of application, image, video, audio, messages sent by scetch, image and profile. [9].

The research of Snapchat Unvieled: An Examination Of Snapchat On Android Devices discussed whether or not "Snaps" really remove the image and video files. It also discussed whether or not the existence of metadata related "Snaps", and whether the "Snaps" can be recovered, as well as how metadata relating to images and ideos [5]. Posting personal images and videos then they will disappear automatically. In the other case, Snapchat is also used to upload sensitive contents [10]. Then we can find out the artifacts, structure, and storage locations of messenger application [11].

This research would develop previous research conducted by Hickman in 2014 on Snapchat issue; it would observe further how Snapchat saves the data and recovers removed images or videos, as well as how the correlation between XML records and image name on the latest Snapchat version on iOS and Android, so it would be an advice for forensic analysis and/or investigators in handling cyberbullying and sexting cases which become recent issues.

Whereas in iOS, Snapchat investigation on the data that can be recovered are contact list, timestamp, and messeage ID [12]. In fact, digital images protentially can result metadata such as information on file name, file size, and timestamps. Metadata file and system will be suitable to several aspects according to the information relating to who, when, and where it comes from [13]. For conducting analysis of digital forensic, it also requires special tool relating to how to utilize XML as an approach of the investigation; it is XIRAF using Automatic extraction, saving the data in form of XML, using Xquery (XML query language) to access database and other data from disk-image [14]. It could be also implemented the log mobile analysis to make sure that there is no illegal file access toward important file [27].

The following references were previous researches relating to the topic on Snapchat. Firstlly, a paper entitled Snapchat Unveiled: An Examination Of Snapchat On Android Devices." It disscussed investigation on Snapchat application. The research revealed a correlation between file com.snapchat.android_preferences.xml and folder received_image_snaps relating to image name; there was an extension nomedia, it was image name, score of mTimestamp, and mId score, but it was not all of image file (Hickman, 2014). Thesis: What are the security issues concerning the Mobile device app Snapchat, and how can forensic artefacts be determined and recovered by forensic examination? To obtain artefact from Snapchat installed in both Android and iOS was easier. It was in folder com.snapchat.android/cache/my_media and rec_received_image_snaps with each image and video was added with extension nomedia. Whereas in iOS, if the same way implemented, it would result differently, it might because of some reasons such as difference of their OS platforms, so it was different in their artefacts, or it might because iOS was compatible to the new version. The interesting fact of Snapchat was existence of folder of ‘SCMediaCache’, it contained encrypted information (Gemma Peet and Bob Bird, 2015). A jounal entitled “Forensic Analysis of Instant Messenger Applications on Android Devices” discussed Instant Messenger installed in Android devices to know artifacts, structure and storage locations of the messenger applications especially Whatsappand viber using Cellebrite UFED. The research result showed time of chat message artifact and file name sent and received .(Aditya Mahajan, M.S. Dahiya and H.P.Sanghvi, 2013). A research entitled ”Social Forensics in Mobile Phones – Analysis of the temporal dimension of Evidence Storage” gives a description of saved evidence on the device phone, especially the Android one. It was located in folder com.snapchat.android. Then, it was also discovered folder received_image_snaps which was the image location and the device added .nomedia extension to name the file (Abhishek Mitra,2015).

A reserch entitled “Forensic Analysis of Data Transience Applications in iOS and Android”, in Snapchat investigation of iOS installed devices that the contact, timestamp and message ID can be recovered.The file and folder of iOS installed devices is located in com.topoya.picaboo.plist and user.plist, whereas the file and folder of Android installed devices are located in com.snapchat.android_preferences.xml, folder received_image_snaps ,folder images and folder com.android.chrome. (Cindy Wu, Christopher Vance,Robert Boggs,Terry Fenger,2013).

2.2 Digital Forensics

It is an applied computer science and technology to check and analyze electronic and digital evidences in order to view the correlation between one evidence and others, so the cybercrimes cases can be investegated and the crimminals can be arrested and be responsible on the crimes they did [15]. There are some phases to conduct scientific procedures. They are preservation, collection, validation, identification, analysis, interpretation, documentation and presentation.[16].

2.3 Mobile Forensics

Mobile forensic is one of sub-disciplines of digital forensics. It works on how to recover digital evidences or other data from mobile phones; it is under sound forensic with scientific methods [17]. Commonly, digital forensic investigation begins with dialed numbers, responses to received phone

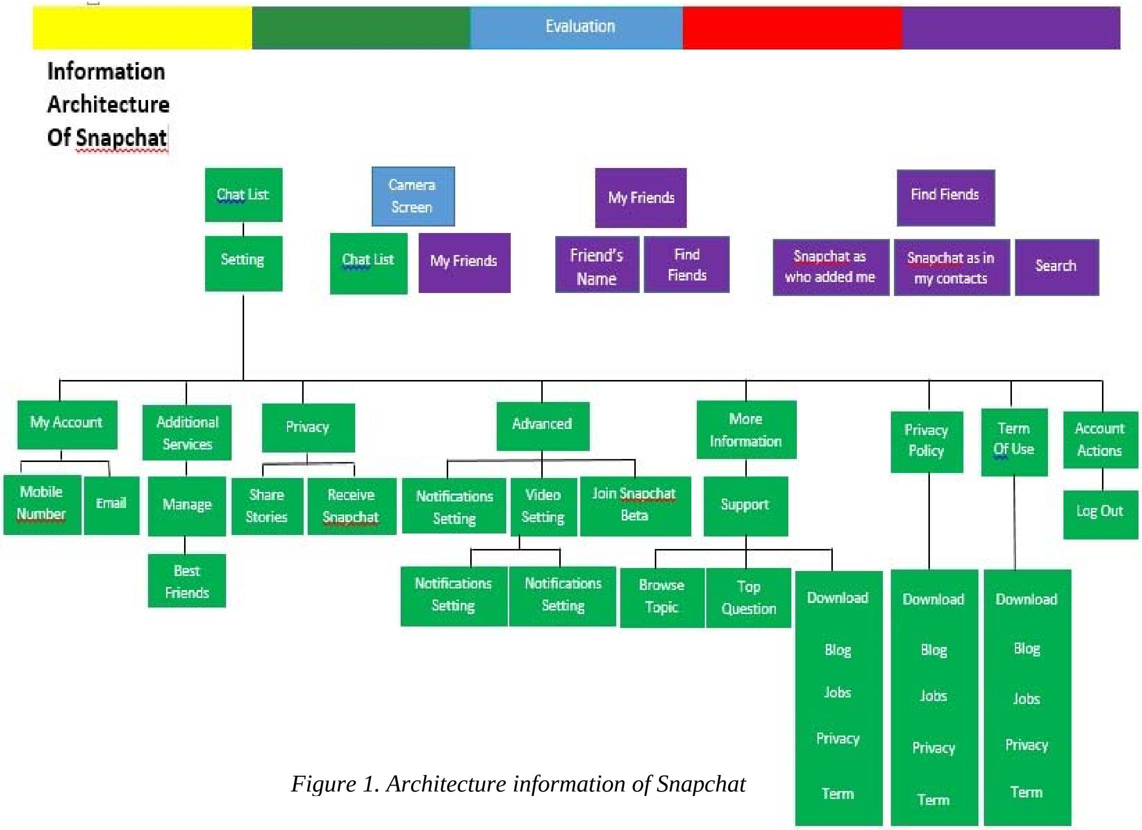


Figure 1. Architecture information of Snapchat

calls; accepted or rejected, saved phone numbers, and texts of messages; the sent text, received text, or even the removed ones [18]. In perspective of digital forensic, it can conduct an investigation based on mobile gadgets to find out many digital evidences of the users, and other purposes related to recovery of additional information as evidence [19].

2.4 Snapchat

Snapchat is a unique mobile messaging application. The users can share and send their personal images and videos and it automatically will remove the postings in few seconds later [2]. Here is the architecture information of Snapchat as shown in figure 1.[20].

2.5 Digital Evidences on Snapchat

Digital evidences of instant messaging application on smartphones are useful for several investigations and law processes in courts [21]. According to the researcher's opinion, digital evidence of Snapchat is information in digital form obtained form the application and digital gadgets. It contains information such as images, videos, chatting transcript, time, and etc. The phase of digital evidence analysis supposed to be done to handle common condition that is possibly faced by investigators. The phase involves digital evidences, especially the smartphones and other related electronic gadgets in the case field [22]. Integrity test of file data was very important to be conducted by digital investigators to verify that the file is genuine [28].

2.6 XML Records

XML stands for Extensible Markup Language. XML is a mark up language such HTML, but it has fixed format. World wide web Consortium (W3C) is a consortium having task to develop standards of world wide web. It means eXtensibel Markup Language is a simple text-based format to present information structured information such as document, data, configuration,

book, transaction, invoice, and other related things. XML can also communicate the structured information to the users.[23].

2. METHODOLOGY

A scientific activity is related to a system of how something works to understand a research subject or object [24]. In this research, the researcher implemented phases to reveal the answers related to problems of Snapchat application as shown in figure 2.

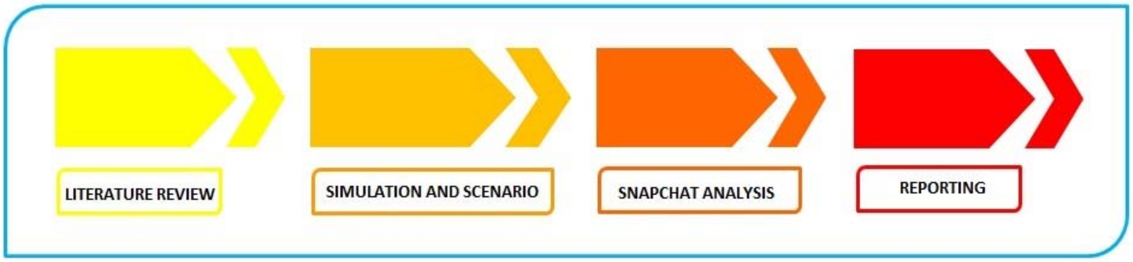


Figure 2. The phases of research

3.1. Literary Review

Literary review is a technique of data collection with study review on books, literatures, notes, and reports relating to the solved problems.[25].The researcher conducted data searching related to research object with questing references on books, articles, journals, papers, and websites relating to mobile forensic, Snapchat Architecture, and XML Records and others.

3.2. Simulation and Scenario of Snapchat Investigation

A simulation is a process required to operate a model to imitate real behavior of the system. It aims to prove the research problems ofthis research.The simulation would be conducted in a Digital Forensic Laboratory of Semarang Branch Office located at the Semarang Police Academy. The simulation required two smartphones (iOS and Android), then both smartphones were simulated to connect each other to chat and send images and videos, as well as video call. The next phase was acquisition toward both smartphones. After the acquisition, then analysis process was conducted. Finally, the report of the evidence was written.

3.2.1. Equipments of the Simulation

Equipments and tools required for the simulation were:

1. Apple iPhone 6 (A1549)
2. Samsung GSM SM-N7505 Galaxy Note 3 Neo
3. AccessData's Forensic Toolkit
4. Cellebrite UFED
5. SQLite DB browser
6. Windows and Linux platforms for analysis

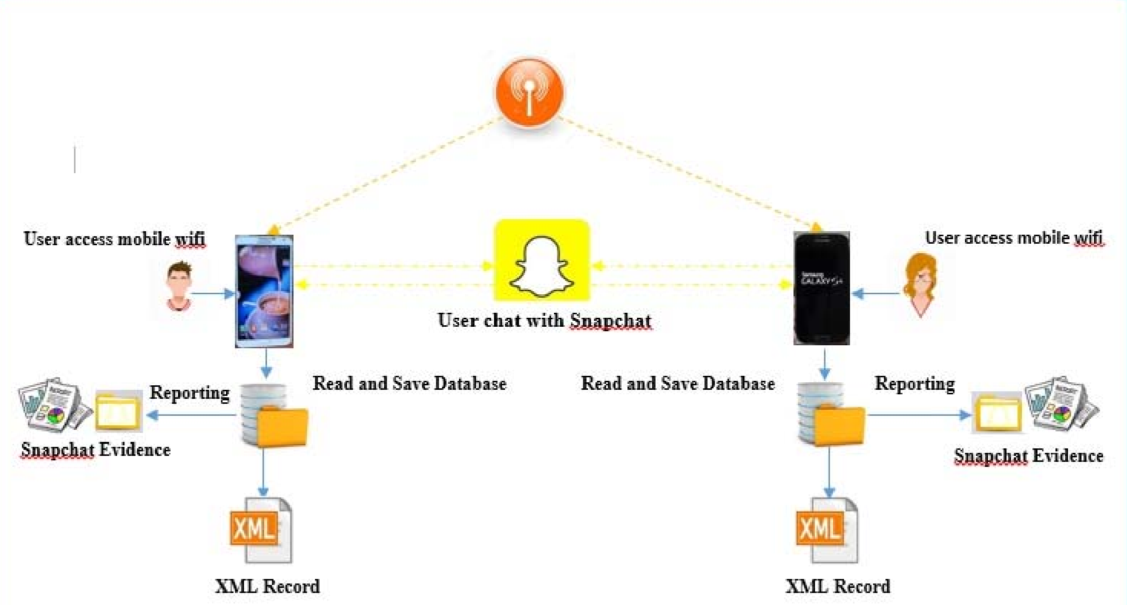


Figure 3. Phases of Simulation Scenario

3.2.2. Scenario of the Simulation

The scenario was designed to achieve what is expected by the researcher, so it requires phases as shown in figure 3.

Ths phases were as follow:

a. IOS and Android-based Smartphones connected to internet to communicate each other on Snapchat.
b. The communication on Snapchat included chatting, sending images and videos, as well as video calls based on the simulation.
c. In the next phase, acquisition/imaging on both smartphones were done. It used Celebrite UFED to obtain digital evidences for obtaining imaging for the next analysis.
d. In this phase, analysis of Snapchat Evidence on both smartphones was conducted to obtain required digital evidence.
e. The last phase was analysis on XML Records toward the evidence to obtain important information relating to Snapchat.

3.2.3. Simulation on Connection

For further understanding and research on forensic cases, especially researcher did simulations were:

Figure 3. Phases of Simulation Scenario

a. Downloading dan Installing Snapchat
b. Signing up
c. Searching and adding friends
d. Capturing image or video (Snap)
e. Editing Snap
f. Saving Snap
g. Setting the time
h. Posting Snap
i. Viewing Snaps sent by friends
j. Using replay Snap feature
k. Sending text (Instant Chat)
l. Conducting a video chat
m. Blocking and removing friends
n.

3.3. Acquisition

There are 3 extraction techniques atau acquisitions used on the gadgets such as Physical Collection, Logical Collection, and File System Extraction.

3.4. Analysis

The analysis of digital evidences was aimed at obtaining digital evidence on data which was suspected as the evidence of a cybercrime, especially “sexting” using Cellebrite UFED Physical.

3.5. The Report of Evidence Investigation

Reporting is one of important phases on digital forensic activities, so whatever that have been done during the investigation, finally the aspect that ı form of data presentation and report. [26].

4. RESULT

4.1. Simulation

The simulation was conducted at Forensic Laboratory of Semarang Branch Office located at the Semarang Police Academy. It is located at Jl. Sultan Agung No 131 Candi Baru Semarang, Indonesia.

4.2. Process of Evidence Acquisition

The Acquisition was an imaging process to obtain data, especially from the smartphones used for cybercrimes.

On the process of digital evidence collection, there were 3 extraction techniques which would be used on the smartphones. They were Physical Extraction, Logical Extraction, and File System Extraction.

To make sure that the process is valid and authentic from file backup, so the score of hash were as shown in table 1 for iPhone 6 and table 2 for Samsung Note 3:

Table 1. Hash Score of iPhone 6

#	Name	Info
1	FileDump	Path Apple_iPhone 6(A1549).zip Size(bytes) 3602663100 MD5 DCE77B4EB09FB49EE1131ACB2 F4590B7

Table 2. Hash Score of Samsung Note 3

#	Name	Info
1	Backup	Path Samsung GSM_SM-n7505 Galaxy Note Neo.zip Size(bytes) 2157634254 MD5 29213643670F6D204C9B59B7575D 5CBF

After conducting acquisition on iPhone 6 and Samsung Note 3, then the researcher did analysis toward acquisition result. From the acquisition process on both smartphones, produce data as shown in table 3.

Table 3. Result of Acquisition Process on the Smartphones

Name	Extraction		
	Physical	Logical	File System
iPhone 6	-	3.11 GB	3.35 GB
Samsung Note 3	29.5 GB	1.01 GB	2.00 GB

The extraction that has been done was with UFED Cellbrite; for extraction with logical and file sytem, the obtained data from the acquisition was not to large. It was different with the physical extraction on Samsung note 3 data; it resulted 29.5 GB. The data was much different using extraction logical and file system. It would be helpful in analyzing more complicated data, and the obtained data would be much more.

The result of file system extraction on iOS conducted with UFED Cellbrite showed 3 important aspects on evidence identification of extraction summary result. Firstly, this Case Information was the information on the case that will be analyzed in tem of case number, evidence number, number of police report, as well as date, case name, case request, brand and type of the smartphones. Both devices were the identification of evidence relating to information of the hardware/smartphones. Inside device inf, it showed information of the smartphone's vendor., IMEI (Internasional Mobile Station Equipment Identity), ICCID (Integrated Circuit Card Identifier), phone model, phone serial, unique ID, version and MSISDN (Mobile Subscriber ISDN), wifi Address, Phone data/time, apple ID and other related information. The third one, it was device content and data files providing short information on content and data, both the existed file and the removed ones.

Whereas on Android, it used physical extrcation data that was obtained much more. The result of extraction summary on Android on case information and device info covering information on bluetooth device name, Android ID, bluetooth MAC address, OS version, detected phone model, android fingerprint, detected phone vendor, MAC address, ICCID, IMSI, phone activation, time, factory number, locale language, country name, time zone, IMEI and others. Then device content and data file covered information on existed and removed content number and data File, but it had more categories; there were around 29 categories of data name.

4.3. Artifact, Structure, and File Storage Location of Snapchat on iOS

After obtaining the digital evidence, the next phase was conducting artifact searching analysis relating to Snapchat application on iOS. From the research result, it was gained some artifacts relating to Snapchat as shown in table 4.

Table 4. Data from Snapchat Artifact

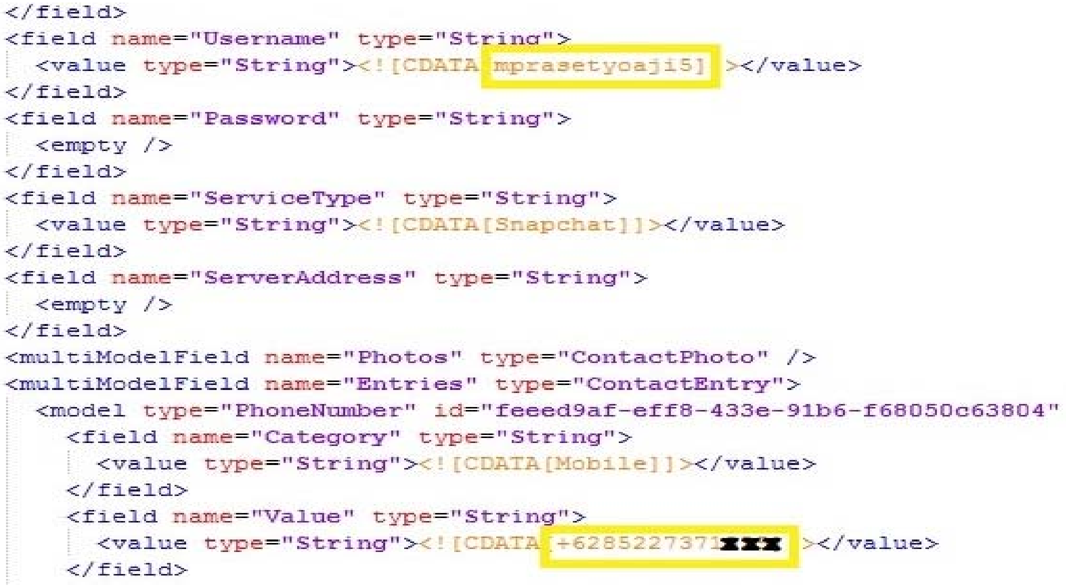
No	Folder Name	Total
1	Call Log	1
2	Chats	6
3	Contacts	177
4	Installed Applilactions	3
5	Log Entries	1
6	SMS Messages	2
7	User Accounts	1
8	File	13

The obtained artifact wer 204 files. They included information such as call log, chatting, location of Snapchat installation, user account and other Snapchat file on structure file and location of

Snapchat file. The folder of structure and Snapchat file was in com.toyopagroup.picaboo, com.toyopagroup.picaboo.sharedan group.snapchat. picaboo.

Then the folder was analyzed to seek evidences relating to the case, so the further anlysis were conducted. The analysis were such user account analysis, as well as other analysis on chatting transcription, images, and videos.

From the XML files that have been analyzed, it was found file user account in the name of mprasetyoaji5 and its phone number; it was +62085227371XXX, then the account chat with account nandamargi as shown in figure 4.



```
</field>
<field name="Username" type="String">
  <value type="String"><![CDATA mprasetyoaji5] ></value>
</field>
<field name="Password" type="String">
  <empty />
</field>
<field name="ServiceType" type="String">
  <value type="String"><![CDATA[Snapchat]]></value>
</field>
<field name="ServerAddress" type="String">
  <empty />
</field>
<multiModelField name="Photos" type="ContactPhoto" />
<multiModelField name="Entries" type="ContactEntry">
  <model type="PhoneNumber" id="feeed9af-eff8-433e-91b6-f68050c63804"
    <field name="Category" type="String">
      <value type="String"><![CDATA[Mobile]]></value>
    </field>
    <field name="Value" type="String">
      <value type="String"><![CDATA +6285227371XXX ></value>
    </field>
```

Figure 4 . Screenshoot File XML Account Snapchat from iOS

From the artifact of chatting result on Snapchat between an account named mprasetyoaji5 and nandamargi, the data were:

Start Time: 11/1/2016 11:51:01 AM(UTC+7)
Last Activity: 11/2/2016 12:29:30 AM(UTC+7)
Participants: mprasetyoaji5
mprasetyoaji5,nandamargi
From: From: nandamargi
Timestamp: 11/1/2016 11:47:24 PM(UTC+7)
Source App: Snapchat
Body:
<Snapchat Image/Video>

The chatting result done by mprasetyoaji5 and nandamargi has been started since November 1 2016 at 11:51:01 AM (UTC+7) and ended on November 2, 2016 at 12:29:30 AM(UTC+7). They have conducted chatting 5 times and 1 called log.

The result of XML file analysis on iOS with file system extraction on Snapchat, the analysis did not found chatting result between mprasetyoaji5 and nandamargi. It because the files were really removed automatically as the Snapchat regulation.

4.4. Artifact, Structure and Location of Snapchat File Storage Location on Android.

To obtain digital evidences on Android, especially the evidences relating to artifact of Snapchat, the main aspect required was where the the application was located. Here is the location file of Snapchat installed on Android based gadgets:Phone Samsung GSM SM-N7505 Galaxy Note 3 Neo,Snapchat vesion : Snapchat 9.39.5.0, location folder:com.snapchat.android,permissions file Accounts, Audio, Camera, Locations, Messages, Microphone,Network, Personal Info, Phone Calls,Social and Info Storage.

After finding out the folder where Snapchat is located, then we can seek the files relating to the application. After physical acquisition, the obtained data are 4074 files relating to Snapchat. Here are the file structure and Snapchat artifact:

1. **Structure of Android File**

   Here are the Snapchat file structure in Android:
   a. com.snapchat.android
   b. com.snapchat.android/cache
   c. com.snapchat.android/databases
   d. com.snapchat.android/app_webview
   e. com.snapchat.android/files
   f. com.snapchat.android/files/media_cache
   g. com.snapchat.android/files/catory_icons
   h. com.snapchat.android/files/stickers

2. **Artifact of Android Folder**

   Here are table 5 the artifact of Android :
   Table 5. Artifact of Android Folder

No	Folder name	Total
1	Application Usage	18
2	Chat	8
3	Contacts	146
4	Emails	1
5	Installed Applications	1
6	Passwords	2
7	SMS Messages	3
8	User Accounts	1
9	Files	3894

From the artifacts on Samsung Note 3, it was gained *user account* in the name of nandamargi with its *password, phone number ,mobile verivication send to number, login username, mobile verification key* and email name. Here is data XML relating to *user account* named nandamargi. In the next phase, the researcher would analyze result of chatting transcription between nandamargi and another account named mprasetyoaji5 that became the target to analyze. In the the analysis result of attachments:

#1: chats\Snapchat\attachments1\h1a81hurcs00h1478018825539AoqX5.jpg.decrypted

#2: chats\Snapchat\attachments1\h1a81hurcs00h1478018825547bnIGa.jpg

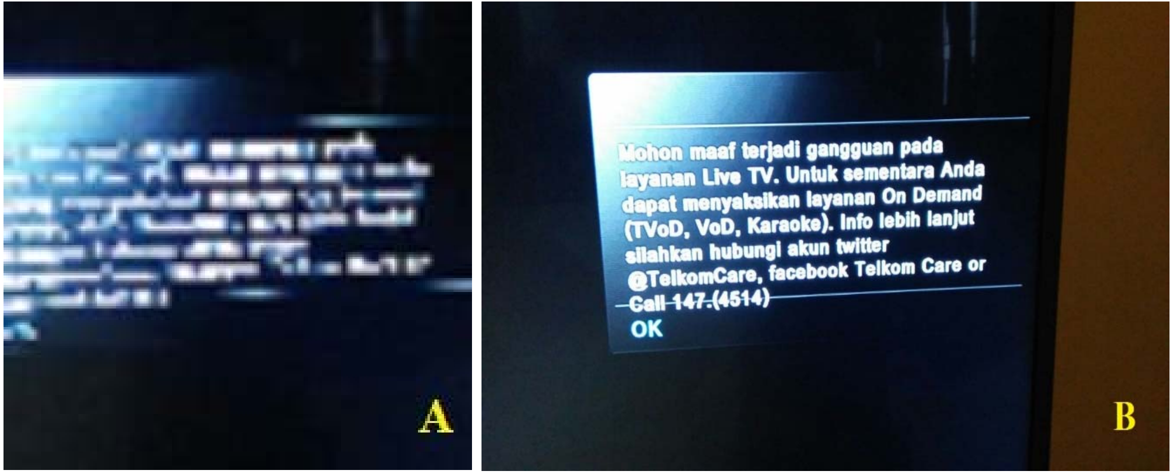
From the attachments, we can view a file; it was a .jpg file extended .decrypted with the .jpg file, but both files have similiar number if we compare to other files. It proved that the research conducted by rhikman was true; it was not all files. Then the question is whether only the file image or comunication file between nandamargi and mprasetyoaji5, it was obtained a quite interesting file as follow:

From: From: nandamargi nandamargi
Timestamp: 11/1/2016 11:47:09 PM(UTC+7)
Source App: Snapchat

4.5. Correlation between XML Records and File Name

File of *image attachments* named h1a81hurcs00h1478018825547bnIGa.jpg was located at /com.snapchat/cache/stories/my/thumbnail/h1a81hurcs00h1478018825547bnIGa.jpg.nomedia.

File *.nomedia* was an empty file located in a folder, so the file was invisible in the gallery on Android system. While a file named *decrypt* was ab .As shown in figure 5A extension file .nomedia.



Mohon maaf terjadi gangguan pada layanan Live TV. Untuk sementara Anda dapat menyaksikan layanan On Demand (TVoD, VoD, Karaoke). Info lebih lanjut silahkan hubungi akun twitter @TelkomCare, facebook Telkom Care or Call 147 (4514)
OK

Figure 5. Figure 5A File image h1a81hurcs00h1478018825547bnIGa.jpg.nomedia and Figure 5B Original image IMG-20161031-WA0003

Then compare the original image in figure 5B named IMG-20161031-WA0003; it showed that the original image was clearer.

Therefore, ths research is able to answer that files having correlation is the hidden file as viewed in both files below:
Filename = h1a81hurcs00h1478018825539AoqX5.jpg.decrypted
Filename = h1a81hurcs00h1478018825547bnIGa.jpg

4.6. Correlation between XML Records and Video

The video file attachments named sesrh_dlw211478021363262REmYp.mp4 and file sesrh_dlw211478021363262REmYp.mp4.DELETED.nomedia extended to .nomedia, the video is able to be recovered. Here is the location of video on Snapchat installed in Android : /USERDATA(ExtX/root/data/com.snapchat.android/cache/snaps/tosend/video/sesrh_dlw21147802136

3262REmYp.mp4.nomedia. The correlation between file on XML Record and video is not found yet by the writer. He has not found satisfiying answer, the viwed information is that related file is because of .nomedia extension.

4.7. Research Comparison

Here is table 7 on analysis of some related researches conducted by other researchers and the writer himself:

4.8. Acknowledgement

After finishing the investigation of this research, we present our gratitude to The Center of Forensic Laboratory (PULABFOR) of Mabes Polri (The Headquarter of Indonesian Police), The Center of Forensic Laboratory (PUSLABFOR) of Semarang Branch Office, The Center of Digital Forensic Studies (PUSFID), Universitas Islam Indonesia, and Universitas Muhammadiyah Purwokerto as the supporting institutions of this research.

4.9. Future Works

It is expected to conduct further researches in the future to investigate image and video on Snapchat with physical acqusition in iOS device to gain more files and to find the correlation between XML Records and name of video files with better analysis technique.

5. CONCLUSION

The investigation process conducted on Aplle 6 and Samsung Note 3, relating to the research on Snapchat application concludes:

The important file of iOS is com.topoya.picaboo.plist and user.plist, Whereas the structure in Android device is com.snapchat.android_preferences.xml.

iOS devices use file acquisition system, the files of both image and video are not found, but there is file showing the removed images and videos. In Android Device, the file of both images and videos can be found, as well as Metadata track; it can be viewed clearly.

The writer started this research for answering a question whether or not the Snapchat file is permanently removed. A fact has been revealed that chatting file on iOS with forensic method still leaves notes, although the image and videos are fully detected. Whereas the devices with Android uses physical acquisition on image or video files; they are not permanently removed, they are hidden with .nomedia extension, so they are not displayed/viewed in gallery.

Table 7. Research Comparison

Topic	Richard Hickman Research	Mukhlis Prasetyo Aji Research
Snapchat Strukture	✓ Samsung Galaxy S3 with folder structure as follow: shared_prefs folder are several XML files: CameraPreviewActivity.xml,com.google.android.gcm.xml, com.snapchat.android_preferences.xml, and SnapPreviewActivity.xml. ✓ iPhone is not reviewed.	✓ Samsung Galaxy Note 3 with folder structure as follow:: ✓ com.snapchat.android,com.snapchat.android/cache ✓ ,com.snapchat.android/databases,com.snapchat.android/app_webview,com.snapchat.android/files,com.snapchat.android/files/media_cache,com.snapchat.android/files/category_icons,com.snapchat.android/files/stickers ✓ iPhone 6 with folder structure as follow: com.toyopagroup.picaboo,com.toyopagroup.picaboo.share,group.snapchat.picaboo
Correlations XML Records and Image Name	✓ Samsung Galaxy S3 image name, there is an extension .nomedia with name: :h1a81hurcs00h1365528700423.jpg.nomedia ✓ iPhone is not reviewed.	✓ Samsung Note 3 (in the image name, there is image extension decripted with the name:: h1a81hurcs00h1478018825539AoqX5.jpg.decrypted ✓ iPhone 6 is as follow: the image name has not been available yet.
Correlations XML Records and Video Name	✓ Samsung Galaxy S3 (there was no research on video) ✓ iPhone is not reviewed.	✓ Samsung Note 3 (there is extension DELETED.Nomedia in video name), the name is: ✓ sesrh_dlw211478021363262REmYp.mp4.DELETED.nomedia ✓ iPhone 6 is as follow: video name is not found yet.

REFERENCES:

[1] We Are Social's. [online]. digital-in-2016.Available from wearesocial.com: http://www.slideshare.net/wearesocialsg/digital-in-2016/215. [Accessed: Maret 20, 2016].

[2] Snapchat.com. [Online].Getting Started . Retrieved from snapchat.com: https://support.snapchat.com/en-GB/article/getting-started1. [Accessed: Juni 1, 2016].

[3] A.Poltash, N. (2014). Snapchat and Sexting: A Snapshot of Baring Your Bare Essentials. Richmodn Journal of Law & Technology, article14.

[4] Thistlethwaite, F. (2015, Augustus 10). life style. Retrieved from express.co.uk: http://www.express.co.uk/life-.

[5] Hickman, R. (2014, January 23). Snapchat Image Recovery. Retrieved from decipherforensics.com: http://www.decipherforensics.com/snapchat/.

[6] Hoog. (2011). Android Forensics: Investigation, Analysis and Mobile Security for Google Android. Amsterdam: Syngress.

[7] Mitra,A(2015). Social Forensics in Mobile Phones – Analysis of the temporal dimension of Evidence Storage. Unpublished doctoral dissertation,University of Bristol, United Kingdom.

[8] Khan,Z.C.,Mashiane,T.,andShozi,N.A.,(2015) Snapchat Media Retrieval for Novice Device Users.The Proceedings of the 10th International Conference on Cyber Warfare and Security.pp-162.

[9] Walnycky, D., Baggili, I., Marrington, A., Moore, J., & Breitinger, F. (2015). Network and device forensic analysis of Android social-messaging applications. Digital Investigation, 14, S77–S84. http://doi.org/10.1016/j.diin.2015.05.009.

[10] Roesner,R.,Gill.T.,and Kohno,T.(2014).Sex, Lies,or Kittens? Investigating the Uses of Snapchat's Selft-Destructing Messages. Financial Cryptography and Data Security, pp.64-76.

[11] Mahajan,A.,Dahia,Ms.,& Sanghvi,P.H.(2013). Forensic Analysis of Instant Messenger Applications on Android Devices. International Journal of Computer Applications ,68(8).

[12] Cindi,Wu,Vance,C., Bogss,R,. and Fenger.T,(2013)Forensic Analysis of Data Trancience Applications in iOS and Android.1401 Forensic Science Drive,Marshall University.

[13] Raghavan,S.(2014)A Framework for Identifying Associations in Digital Evidence Using Metadata. Unpublished doctoral dissertation,Queensland University of Technology,Brisbane.

[14] Alink,W.(2005). XIRAF: An XML-IR Approach to Digital Forensics.Unpublished master's thesis, University of Twente.Netherlands.

[15] Al-Azhar, M. N. (2012). Digital Forensic: A Practical Guide of Computer-based Investigation: Salemba Infotek.

[16] Palmer, G. L. (2001). A Road Map for Digital Forensic Research. Report for the Firsh Digital Forensic Research Workshop (DFRWS), Technical Report DTR-T0010-01.

[17] Harril,D.C. (2007). A Small Scale Digital Device Forensics Ontology. Small Scale Digital Device Forensics Journal, Vol 1, No 1.

[18] Punja, S.G.,and Mislan,R.P.(2008). Mobile Device Analysis. Small Scale Digital Device Forensics Journal, Vol 2,No 1.

[19] Nuril.A., Riadi.I. ,and Lutfhi.A. (2016). Forensic SIM Card Cloning Using Authentication Algorithm. Int. J. of Electronics and Information Engineering, Vol.4, No.2, PP.71-81.

[20] Kim,H.(2014).Snapchat chat Interface Analysis Report.Spring Semester Interface Design. Retrieved April 16, 2017, from https://www.slideshare.net/SeunghunYoo93/snap-chat-interface-analysis-report.

[21] Walnyeky,D. (2015). Network and device forensic analysis of Android sosial-messaging applications. DFRWS, 1741-2876.

[23] World Wide Web Consortium.(n.d) w3 .org: Electronic references. Retrieved Maret 20, 2016, from https://www.w3.org/XML/

[23] Ruuhwan,Riadi,I. and Prayudi,Y.(2016).A Properness Analysis of Integrated Digital Forensics Investigation Framework for Smartphone-based Investigation.pp Vol 7, No 4.

[24] Ruslan, R. (2008). Management of Public Relations & Communication Media:. Jakarta: PT Raja Garfindo Persada.

[25] Nazir, M. (1988). Research Methodology. Jakarta: Ghalia Indonesia.

[26] Prayudi,Y.”Investigation Report”.[Online]. Available https://catatanforensikadigital.wordpress.com/2015/11/22/laporan-investigasi/. [Accesed:September 22,2015].

[27] Kuncoro, A.P.,Riadi,I. and Luthfi,A.(2017). Mobile Forensics Development of Mobile Banking Application using Static Forensic. International Journal of Computer Applications. Volume 160 – No 1.

[28] Kurniawan .A, Riadi,I. and Luthfi,A.(2017). Forensic analysis and prevent of cross site Scripting in single victim attack using open Web application security project (owasp) Framework. Journal of Theoretical and Applied Information Technology.Vol.95.No 6.