Research Article

Forensic Analysis of Social Networking Applications on an Android Smartphone

Anoshia Menahil,¹ Waseem Iqbal¹,¹ Mohsin Iftikhar,² Waleed Bin Shahid,¹ Khwaja Mansoor,³ and Saddaf Rubab¹

¹Department of Information Security, National University of Sciences and Technology (NUST), Islamabad 44000, Pakistan

²School of Computing and Mathematics, Charles Sturt University, Australia

³Faculty of Computing and AI, Department of Cyber Security, Air University, Islamabad 44000, Pakistan

Correspondence should be addressed to Waseem Iqbal; waseem.iqbal@mcs.edu.pk

Received 20 February 2021; Revised 15 March 2021; Accepted 1 July 2021; Published 23 July 2021

Academic Editor: Ernestina Cianca

Copyright © 2021 Anoshia Menahil et al. This is an open access article distributed under the Creative Commons Attribution License, which permits unrestricted use, distribution, and reproduction in any medium, provided the original work is properly cited.

Smartphone users spend a substantial amount of time in browsing, emailing, and messaging through different social networking apps. The use of social networking apps on smartphones has become a dominating part of daily lives. This momentous usage has also resulted in a huge spike in cybercrimes such as social harassing, abusive messages, vicious threats, broadcasting of suicidal actions, and live coverage of violent attacks. Many of such crimes are carried out through social networking apps; therefore, the forensic analysis of allegedly involved digital devices in crime scenes and social apps installed on them can be helpful in resolving criminal investigations. This research is aimed at performing forensic investigation of five social networking apps, i.e., Instagram, LINE, Whisper, WeChat, and Wickr on Android smart phones. The essential motivation behind the examination and tests is to find whether the data resides within the internal storage of the device or not after using these social networking apps. Data extraction and analysis are carried out using three tools, i.e., Magnet AXIOM, XRY, and Autopsy. From the results of these experiments, a considerable amount of essential data was successfully extracted from the examined smartphone. This useful data can easily be recovered by forensic analysts for future examination of any crime situation. Finally, we analyzed the tools on the basis of their ability to extract digital evidences from the device and their performance are examined with respect to NIST standards.

1. Introduction

Smartphones have gone through a progressive advancement over the last two decades. From being a prized possession, they have become an outright need as they are used for a lot more than just calls and messages. Smartphones enable users to enjoy a comfortable internet experience by browsing, emailing, and staying connected through different social media apps. The use of social media apps has witnessed a momentous surge, and they are being used by people of all age groups, by businesses, academia, media, hacktivists, law enforcement agencies (LEAs), and even terrorist organizations for a wide variety of purposes [1]. During the last 12 months, the use of social media has continuously increased by 1 million every day [2]. According to the Digital 2020

Global Overview, the usage of social media has increased by 12 percent from 2019 and 99 percent of that surge was due to smartphone apps [2].

For most teenagers, the most popular usage of mobile phone is socializing. These online interactions are mostly productive; however, the online interactions have resulted in increased number of bullying, threatening, and humiliating others as well [3]. It is estimated that 73% of students feel that they have been harassed in their lives and 44% say they have been harassed during the last 30 days [4]. Easy access to social media platforms opens a door for a new type of bullying.

Social networking apps (SNAs) allow users to create a profile, upload personal information such as pictures, videos, and location, and share that information through private messaging or public posts. This phenomenon gives criminals

FIGURE 1: Statistics of the usage of the Internet and social media.

an open opportunity to influence the user's personal information thus giving rise to cybercrimes via SNAs [5]. These apps can also be exploited for cyber bullying, stalking, sexual harassment, and insults [6, 7]. Since all information about user activities is stored within the phone's internal memory, these smartphones have become an important source of evidence and artifacts during crime investigations linked to these SNAs. These gathered artifacts enable users and investigators to find out the PII (personally identifiable information) [8] that is stored in the device and is useful to be presented in the court of law.

The increase in cybercrimes using smartphones and SNAs [9] has created an opportunity to use forensic tools and techniques to investigate these criminal activities. The forensic analyst requires an up-to-date understanding of what kind of artifacts can possibly be recovered so that they can be presented in the court of law. Moreover, the increased demand for more and more advanced smartphones has created fierce competition among equipment manufacturers. New smartphones are continuously launched in the market that has resulted in a frequent change of mobile phones by users based on factors such as better OS, file structure, data storage, user experience, and many more [10]. Therefore, forensic examiners are struggling to keep up with new procedures and tools.

Many studies have been conducted on Facebook and WhatsApp forensic and other well-renowned apps as mentioned in literature, so there is a need for forensics analysis of other social media apps (Instagram, LINE, WeChat, Whisper, and Wickr) which are getting popular these days. With expanded use of smartphones for social networking as highlighted in Figure 1, a lot of knowledge on forensic artifacts depicting user behaviour is generated through these social networking apps [2] which are stored within the phones. Several situations involving significant accidents might occur that may end up in the court. Forensic investigators can use those activities as evidence in investigating such incidents.

Keeping this scenario in mind, we have focused on inspecting the phone forensically and looking for the artifacts generated and stored in different locations in the phone, via the forensic tools. Such artifact findings are capable of tying the perpetrator to the incident; thus, forensic examination

FIGURE 2: NIST forensic analysis process.

of these apps can provide a ready reckoner to the digital forensic investigator of Android phone analysis.

Thus, focusing on this requirement, our research aims at performing the following actions:

- (i) Identification, extraction, and analysis of the artifacts recovered from the popular social networking apps on an Android smartphone in a way that can be presented in the court of law
- (ii) Analysis of each app using three different tools, i.e., Magnet AXIOM, Autopsy, and XRY
- (iii) Presentation of the analysis of the tools to showcase their ability to extract digital evidences from the device and their performance is examined with respect to NIST standards

We have used three forensic tools to perform experiments on five popular social media apps including Instagram [11], LINE [12], Whisper [13], WeChat [14], and Wickr [15]. Data from these apps is acquired and analyzed during three stages (before data deletion, after data deletion, and after app uninstall) using Magnet AXIOM [16], Autopsy [17], and XRY [18]. Furthermore, we have also categorized the tools on the basis of total artifacts recovered and NIST standards on smartphone extraction tools [19]. We have also devised some additional parameters that can be used

TABLE 1: Literature study of forensic investigation on mobile applications.

App	Platform used	Artifacts	Remarks
Snapchat [34]	iOS and Android	IOS images and videos are fully detected. Android images and videos not fully detected	No correlation found between _le on XML record and recovered video.
Wickr [35]	Android	No artifacts found	After analyzing app on rooted and nonrooted devices, Wickr was proved as an antiforensic app
WhatsApp, Viber [36]	Froyover 2.2, GingerBread v2.3.x, and IceCreamSandwich v4.0.x	WhatsApp: message, timestamps, and names of files sent and received. Viber: no file found through the analyzer	Research does not focus on the artifact discovery when data was deleted
WhatsApp [37]	Android	Phone numbers, messages, media files, contact cards, and profile pictures	They successfully developed a tool to acquire data from phone
20 applications [38]	Android v4.4.2, iOS 7.1.2	Snapchat, Tinder, Wickr, and BBM: data not recovered	Main focus was on the network traffic analysis
ChatSecure [39]	Android	Recovered messages, video, and audio that have been shared. No deleted data recovered	Artifact extraction done only from the volatile memory. An algorithm was designed to decrypt the encrypted chat secure database
Kik Messenger [40]	Android v4.4,5.0	Chat messages (send/received), contacts, and media that have been exchanged are recovered	Device backup was created through the logical acquisition
Instagram [41]	iPhone 6s (iOS 10.3.0)	User information, activity history, and application settings recovered from the iPhone backup file	Backup created through logical acquisition. Only the file folder was considered for the artifacts
WhatsApp [42]	Android v5.0.1	Text messages, images, video, and documents recovered	Calculate and compare the Belkasoft Evidence (trial version) and WhatsApp Key/DB Extractor tools on the basis of artifacts recovered from WhatsApp
Telegram [43–45]	Android, Windows	Android gives messages and cache info after exploring databases. App package was not recovered in Windows phone	Analysis was done on 5 scenarios that were divided into 17 smaller scenarios but these scenarios were not discussed properly. Reference [44] did not analyze the whole _le system (part analysis has been done). Reference [45] claimed that commercial tools like Internet Evidence Finder, UFED Physical Analyzer, and Oxygen Forensic Analysis did not have the capability to acquire artifacts from Telegram Messenger for the Windows phone but did not discuss the clear experimental evidence
KaKaoTalk [44, 46]	Android	Kakao encrypted database was decrypted to gain access to messages and contact information	Reference [41] discussed the security measures against password guessing attack to protect the encrypted databases. Reference [44] did not analyze the whole file system (part analysis has been done)
Instagram and Path [47]	iPhone 5s	Followers, hashtags, and some account information recovered from Instagram. Path did not disclose any important data of user activities	Discussed and proved the importance of write blocker while acquiring data from a device
Cubby, IDrive [48]	Android v5	Recovered register id and password, timestamps, uploaded files with timestamps, and downloaded files with timestamps and recovered encryption technique	Some locations were identified that were vulnerable to attacks

TABLE 1: Continued.

App	Platform used	Artifacts	Remarks
Facebook, Twitter, Myspace [49]	Android, iPhone, and Blackberry	Recovered some information from iPhone and Android. Nothing recovered from Blackberry	Logical backup copies of three smartphones. No artifacts from internal memory were discussed
Snapchat [33]	Android	Unexpired and expired recoverable	Scenario-based discussion. Scenarios are difficult to implement because of high cost

for forensic analysis. The artifacts suggested by our study can be helpful in forensic investigation of cybercrimes on SNAs.

The rest of the paper is organized in 6 sections. Section 1 presents the preliminary concepts and definitions used in this paper. Section 2 presents the literature related to mobile app forensics on different operating systems (OSs). In Section 3, the methodology of the research is explained. Section 4 covers the artifacts recovered from all five apps using Magnet AXIOM, Autopsy, and XRY. Section 5 discusses the results gathered from three tools and evaluates the tools according to total artifacts recovered, NIST parameters [19, 20], and additional parameters derived during this research to judge the tool's capabilities. Conclusions and future work are presented in Section 6.

2. Preliminary Concepts

This section presents a brief overview of preliminary concepts that are going to be used/referred throughout this article.

2.1. Android Operating System. Currently, Android OS is the most commonly used OS in mobile phones with an 88% share in the worldwide smartphone industry. It is therefore essential to explore Android using various methodologies and methods [21]. For forensic investigators, the folder structure of an Android phone can be an extremely interesting region. So, they should understand where the information/evidence can be found. It is therefore helpful to understand the structure of data storage [22].

A unique Id (Uid) is assigned to each app in Android. Each app runs in a separate process so as no application can access the data of other app. A unique app id for a specific app is stored in the app package. Phone application can store app data in many ways [23]. Through app forensic analysis, an investigator can comprehend the usage of the app and find the user data. App analysis is important because nearly all of them use typical function, i.e., messages, calls, contacts, and internet surfing [24]. This data can tell a lot about the user as to when they were in a specific location or to whom they have communicated and their future planning, etc.

2.2. Digital Evidence and Forensic Process. In 2006, Carrier and Spafford [25] defined a digital evidence as the data that approve or disapprove the hypothesis made about the digital events. Forensic investigation is done by collecting, preserving, and analyzing the evidence to present in the court of law. Mobile phones continuously transmit the data through

wifi, Bluetooth, etc. It is too difficult to preserve data without altering it so it is important to record and document every single detail during the whole process.

According to the National Institute of Standards and Technology (NIST), the forensic process [26] includes a 4-step procedure, i.e., preservation, acquisition, analysis, and presentation. Figure 2 describes the NIST forensic process.

2.2.1. NIST Standards on Smartphone Extraction Tools. NIST releases some parameters and methods to calculate the performance of forensic tools based on the outcomes of the assessment plan conducted by NIST. Every assertion creates at least one experiment comprising of a test convention and the normal test outcomes. The test convention indicates point-by-point techniques for setting up the test, executing the test, and estimating the test outcomes [19]. NIST claims that in forensic cases, expanding the quantity of cell phones every year creates problems. Hence, to quantify the capability of forensic tools available, a method is required. NIST offers 42 parameters and methods based on the results of each test plan to assess the performance of forensic devices.

The objective of the computer forensic tool testing (CFTT) venture at the NIST is to build up an approach for testing forensic tools. This is done by establishing unique and common rules governing the requirements of the tools. NIST records the estimation parameters of the forensic tools on two composed reports entitled "smartphone tool specification" [19] and "smartphone tool test assertions and test plan" [20]. The estimation parameters are partitioned into two parts: core and optional. Specifications for smartphone devices are in two parts. Smartphone tool core requirements ([SPT-CR-01] to [SPT-CR-06]) are the requirements that will be met by all the acquisition tools. Smartphone tool optional requirements ([SPT-RO-01] to [SPT-RO-15]) require that all tools shall comply with the requirements that the stated feature or choices that tool offers. Test assertions are developed using these requirements. Test assertions are defined as general proclamations of conditions that can be tested after a test has been carried out.

2.3. Digital Investigation Tools. There are tools that are designed to acquire and analyze the digital image from the mobile devices. Competency of the forensic acquisition and analysis of these tools can differ from one another so it is important for the analyst to have the knowledge of different tool expertise levels. The output comparison and verification between tools can help the examiner to choose the tool he needs to use for the case. We have used the following three tools in our analysis.

FIGURE 3: Research methodology: a detailed flow chart of actions performed during forensic analysis.

2.3.1. Magnet AXIOM. AXIOM is a complete digital investigation tool developed by Magnet Forensics. It is used to recover digital evidence from different sources, i.e., computers, smartphones, third-party images, and cloud. This platform contains two apps to acquire and analyze data. The *AXIOM* process is used to acquire and process the data acquired from the smartphone, and *AXIOM Examine* performs the examination and analysis over the acquire data. For the purpose of this research, we have used the fully functional trial version [16].

2.3.2. Autopsy. Autopsy is an open source digital investigation platform that is commonly used by law enforcement and forensic examiners to analyze the digital image in order to get the evidence from it. In this research, we are using Autopsy as a second analyzing tool to make certain of all the evidence recovered from the acquired images [17].

2.3.3. XRY. XRY is a digital investigation platform. It is an instinctive and competent software app that runs on the Windows OS. It allows an examiner to extract high-quality

FIGURE 4: Application scenario.

TABLE 2: Experimental tools (SNA stands for social networking app).

Sr.	Experimental tools and software	Description
1	Samsung Galaxy J7	Android 8.0.1
2	Workstation	Windows 10, 64 Bit, Intel i5
3	USB cable	Connect the mobile phone to the workstation
4	SQL DB browser [58]	Version 3.11.0
5	Instagram [11]	SNA v87.0.0.18.99
6	LINE [12]	SNA v9.4.5
7	Whisper [13]	SNA v7.28.6
8	WeChat [14]	SNA v7.0.3
9	Wickr [15]	SNA v5.10.2

data securely from different digital devices and platforms. Acquisition and analysis can be performed through this tool. It allows an examiner to extract logical or physical data according to the case [18].

2.4. Root for Physical Acquisition. Forensic examination requires a detailed recovery of artifacts for thorough analysis, even though rooting is not needed for physical acquirement in some cases where patch is offered by the acquisition tool such as XRY, Cellebrite, and Magnet AXIOM. On the other hand, rooting the device helps in eliminating the limitations that the cell carriers or system OEMs have imposed. A rooted interface offers effective user data extraction and access to internal directories for the device. The partitions and system folders are kept hidden with no access for a nonrooted phone. However, many Android smartphone manufacturers permit to legally root your devices [27]. Moreover, integrity of user data from rooted Android devices during data acquisition is a main concern as forensic analyst extract valuable data from Android phones by rooting [27]. Furthermore, authors in [28] prove that rooting of Android devices has legal validity and the evidence extracted as a result of the rooting process is effective and credible evidence of conviction in criminal proceedings.

3. Related Work: Application Forensics

Some research work has been done in the field of mobile application forensics. Some of the analysis is done on the device general activities, event logs, and device logs [29, 30], whereas others emphasized on the installed applications on the device. Andriotis et al. [31] related the usage of smartphone with numerous crimes like confidential information sharing on public mediums, uploading images over the cloud and child pornography etc. [32]. Information was collected from phone log files, wifi logs, event logs, Bluetooth logs, and databases containing the browsing history. Snapchat was analyzed in [33] by Infosecurity Group and by Aji et al. [34] on two smartphones using Android and iOS. They acquired the data from the smartphone's internal memory through 3 extraction techniques: physical, logical, and file system. Extraction was performed with UFED Cellebrite. Chatting file, images, and videos were detected from XML records found on the iOS smartphone; however, the Android device data was not permanently deleted but hidden with nomedia extension.

In [35], Mehrotra et al. aimed to authenticate the founder's claim that the Android application Wicker enables the user to exchange self-destructive messages and files. They examined both rooted and not rooted Android phone data acquired through *Titanium Backup Android app v6.1.1* and *Helium Backup Android app*. No artifacts or trace of data exchange was found. Mahajan et al. [36] analyzed the artifacts of two apps, *WhatsApp* and *Viber*. Data was extracted through *UFED* from 3 versions of Android OS. Both the apps were examined through *UFED Analyzer*. The chat list, chat messages, and sessions along with timestamps were found in the WhatsApp "msgstoredb" file, and contact information was found in the "wadb" file. For *Viber*, all information that

TABLE 3: Forensic tool description.

Sr.	Forensic tools	Version	Description
1	Magnet AXIOM	4.0	Proprietary
2	Autopsy	4.14.0	Open source
3	XRY	8.2	Proprietary

TABLE 4: Proposed categories for artifacts.

Categories	Artifacts
DB	Databases recovered Text messages Images incoming
Media/text exchanged	Images outgoing, videos incoming, videos outgoing, audio incoming Audio outgoing, GIFs/emojis incoming GIFs/emojis outgoing Stories, posts uploaded
Timeline	Posts liked/reply Group information Timing of posts/status Friend list Profile picture, date of birth Email address ID Location Name Phone number Profile images Phone app activity
Calls	Audio calls, video calls Private chats
Timestamps	Stories/posts/statuses upload Friends added

include send and receive messages, contact lists, and timestamps was found through manual search. Mathavan and Meeran [37] performed forensic analysis on *WhatsApp*. The internal memory of an Android phone was analyzed to find out the artifacts such as send/receive messages, images, videos, logs, and contact information. Walnycky et al. [38] selected 20 social messaging apps based on the number of downloads and keyword results from Google Play Store. Network traffic was captured and saved by using *Wireshark* and examined through *NetworkMiner* and *NetWitness Investigator*. This research concluded that four apps, i.e., *Snapchat*, *Tinder*, *Wicker*, and *BBM* are secure as they encrypt network traffic through HTTPS encryption using an SSL certificate.

Anglano et al. [39] analyzed *ChatSecure* on Android phones. *UFED Physical Analyzer* was used to analyze data. *ChatSecure* database was decrypted through *LiME*. Messages and media shared during conversation were been recovered, whereas the deleted data was not recovered. Adebayo et al. [40] analyzed *Kik* app installed on three Android mobile devices. The device backup was created with *Titanium*

FIGURE 5: Artifacts retrieved from Instagram using Magnet AXIOM.

Backup, and the SQLite DB browser was used to analyze the recovered databases. In another study, *Instagram* was analyzed by Ryu et al. [41] on iPhone 6s using *EditPlus3 Plist*, *iBackupBot iPhone Backup Extractor*, *iBackup Viewer*, and *iPhone Tracker DB*. User information, activity history, and application settings were recovered from the iPhone backup file. Umar et al. [42] analyzed *WhatsApp* for digital evidence. The application was installed on Samsung Galaxy S4 GT-I9500 Android version 5.0.1, and acquisition was done through ADB. For analysis, two tools were used: *WhatsApp key/DB Extractor* and *Belkasoft Evidence*. Text messages, images, videos, and documents were recovered. From the results generated by tools, *Belkasoft* was concluded as best among the two. Telegram app was analyzed in [43, 44] on different versions of Android phones and Windows phones [45]. Android gave messages and cache info after exploring DBs. No package related to the app was found on the Windows phone.

In a few other studies [44, 46], *KaKaoTalk* was analyzed on Android phones. The *Kakao* encrypted database was decrypted to gain access to messages and contact information in the researches. *Facebook*, *Skype*, *Viber*, *Windows Live Messenger*, and *WhatsApp* were analyzed in [50] on iPhone. The backup contains all the information related to these apps even after uninstallation. In [51], *Facebook*, *WhatsApp*, *Hike*, *Viber*, and *Imo* were analyzed on an Android phone. Loca-

tions of artifacts were discussed in this research. In [52], the security mechanisms of *WhatsApp*, *Viber*, *Tango*, *Voupi*, *For-fone*, *HeyTell*, *EasyTalk*, and *WowTalk* were discussed when they were installed on Android v2.3 and iOS v2.3. In [53–55], *LINE Messenger*, *BlackBerry Messenger*, and *IMO Messenger* app were analyzed respectively on Android phones and iPhone. The content shared between two parties through private conversation was discussed. *Twitter*, *POF Dating*, *Snapchat*, *Fling*, and *Pinterest* were analyzed in [56] installed on Android v5. Message content and account information were discussed. Forensic analysis of *Snapchat* and *Burner* was done in [57] on both iOS and Android smartphones. Table 1 summarizes some previous studies on forensic analysis on mobile apps.

4. Methodology

The overall methodology adopted in research comprises four steps. These steps are illustrated in Figure 3.

4.1. Scenario Building. In the first stage, investigation scenarios are set up by performing common user activities on apps. Apps are installed on the phone from Google Play Store. Accounts are created for each app and activities, i.e., pictures/videos uploaded, comments, scrolling over newsfeed, stories uploaded, messages (text/audio/video/images) sent

FIGURE 6: Artifacts retrieved from LINE using Magnet AXIOM.

or received, and video calling (LINE), are performed for the application according to their capabilities. The scenario followed in this research is explained in Figure 4.

4.2. Acquisition. Data from phone memory is acquired through two different tools *Magnet AXIOM (process)* and *XRY*. Data from phone memory is acquired in three stages.

- (i) Application is installed and working
- (ii) Application is installed and data has been deleted
- (iii) Application and data both have been deleted

In the first stage, all the data remains on the phone as the app is working. In the next stage, some data is deleted by the analyst, and in the last stage, all data is deleted and the app is uninstalled from the phone. Data is acquired from the device in a controlled environment in order to ensure the integrity of the data. In order to get maximum data from the internal memory of the device, data is acquired through the physical acquisition of the device after rooting.

4.3. Analysis. In the analysis phase, every app is analyzed by the content of the app folder located in the data/data directory. The analysis generally involves data found in the specific app's file folder and database folder but not limited to them. Another folder found in the data/data/app_folder named "Shared Preference" contains some .xml files having

app-related data. The same information is recovered by all three tools. Cache stores all the activity information and images/videos seen by the user while using the app and is recovered by all three tools.

4.4. Tool Evaluation. Tools are evaluated on the basis of their capability to recover digital artifacts from every said app, NIST standards on smartphone extraction tools [19] and some additional parameters from the investigator after conducting research. The result of this research can be used as a recommendation to investigators to handle the cases associated with these apps.

In order to analyze the data generated by these apps (Figure 4), the internal storage of the smartphone is examined after every experiment. The information generated by apps is stored in the inner phone memory that is ordinarily out of reach to users. Therefore, appropriate tools and techniques should be adopted so as to obtain and access this part of the memory. The hardware used in the research is a Samsung smartphone, USB cable, and computer for the retrieval and analysis of data. The description of experimental tools is provided in Table 2. Forensic tools that are used during the experiments are described in Table 3.

Artifacts recovered have been categorized into six fields in this research. The main categories are DB (databases), media/text exchange, timeline, account/user information, calls, and timestamps. The DB category contains the artifacts recovered from the databases present in the app folder. The

Partner Name	Message Text	Status
Hero_Singing	[REDACTED]	Received
Twisted Dr	[REDACTED]	Received
Twisted Dr	[REDACTED]	Sent
Hero_Singing	Hy	Sent
Twisted Dr	[REDACTED]	Received
Twisted Dr	[REDACTED]	Sent
Coolio_Ocean	Hy	Sent
[REDACTED]	[REDACTED] spiness	Received
Bright_Aluminum	Hy	Sent
Bright_Aluminum	Are you [REDACTED]	Received
Bright_Aluminum	Yup	Sent
Bright_Aluminum	[REDACTED]	Received
Brave Heart	[REDACTED]	Received
[REDACTED]	[REDACTED]	Received

(a)

Name	Type	File ext...	Size (b...	Created
2ef4b292-4546-4f5d-a387-1a9d98450661	File		4,142,994	
b229bd4d-6f80-435f-94c1-5dd2e1c4c3dc	File		3,333,213	

(b)

Name	Type	File ext...	Size (b...	Created
w1517247768051	File		36,929	
w1517820253580	File		62,768	
w1518335770143	File		76,622	
w1518377807121	File		59,507	
w1518378197117	File		103,911	

(c)

ENCE (21)				Column view	Stoned_Pallyi
User Name	Text	Ima			
stadium_status	If y	http:			
JoeEggs	Just	http:			
Cloud_calmi	I h	http:			
luna_blood	I ju	http:			
Stoned_Pallyi	No	http:			
seyredhead	Wa	http:			
Stoned_Pallyi	Alt	http:			
Jr_Moonlight	The	http:			
Stoned_Pallyi	Gu	http:			
Outlaw_Little	If i	http:			

(d)

FIGURE 7: Artifacts retrieved from Whisper using Magnet AXIOM.

☐ FTSSChatRoomMembers	Table
☐ FTSSContactLabels	Table
☐ FTSSIndexContact	Table
☐ FTSSIndexContact_content	Table
☐ FTSSIndexContact_docsize	Table
☐ FTSSIndexContact_idx	Table
☐ FTSSIndexFavorite	Table
☐ FTSSIndexFavorite_config	Table
☐ FTSSIndexFavorite_content	Table
☐ FTSSIndexFavorite_data	Table
☐ FTSSIndexFavorite_docsize	Table
☐ FTSSIndexFavorite_idx	Table

(a)

☐ FTSSIndexFriend_content	Table
☐ FTSSIndexFriend_data	Table
☐ FTSSIndexFriend_docsize	Table
☐ FTSSIndexFriend_idx	Table
☐ FTSSIndexGame	Table
☐ FTSSIndexGame_config	Table
☐ FTSSIndexGame_content	Table
☐ FTSSIndexGame_docsize	Table
☐ FTSSIndexGame_idx	Table
☐ FTSSIndexMessage	Table
☐ FTSSIndexMessage_config	Table
☐ FTSSIndexMessage_content	Table
☐ FTSSIndexMessage_data	Table
☐ FTSSIndexMessage_docsize	Table
☐ FTSSIndexMessage_idx	Table
☐ FTSSIndexMiniGame	Table
☐ FTSSIndexMiniGame_content	Table

(b)

/IDENCE (1)				Column view	video_send_pr
Name	Type	File extension	Size (b...		
video_send_preprocess_tmp_1518695915279.mp4	File	.mp4	1,734,114		

Textual information of video shared during chat

(c)

Name	Type	File extension	Size (b...	Create
.nomedia	File	.nomedia	0	
msg_42170202151819a6b51fff9104.amr	File	.amr	2,627	

Textual information of audio shared during chat

(d)

FIGURE 8: Artifacts retrieved from WeChat using Magnet AXIOM.

5.1. Forensic Analysis of Apps through Magnet AXIOM. This section discusses the artifacts recovered from the applications using Magnet AXIOM.

FIGURE 10: Artifacts retrieved from Instagram using Autopsy.

5.1.1. Instagram. The artifacts recovered from Instagram through Magnet AXIOM are described in Figure 5 under three conditions: before data deletion, after deleting some data, and after app uninstallation. Firstly, the app is analyzed while no data has been deleted from the device. Figure 5(a) shows that the messages sent and received are recovered with message time, type, sender, and receiver information. Figure 5(b) shows that the stories uploaded by the user on its Instagram account are recovered. An image is taken again after deleting some data, i.e., images, text messages, and images/video uploaded on the Instagram account. Figure 5(c) shows that 80 percent of text messages are successfully recovered and only textual information of images and video calls is recovered such as the name of other party and timestamps. After app uninstallation, no data is recovered related to the Instagram app analyzed by Magnet AXIOM.

5.1.2. LINE. As we examined naver.line.db, there are 32 tables from which only 6 tables are of interest from the forensic point of view. The contact table has the relation with call_history.db as the user that was making the call can only be rec-

ognized by the contact table. The id of the caller would be matched from the m_id in the contact table. So, the caller can be verified. LINE gives an end-to-end encryption for data. The public key for every contact is stored in e2ee.db in an encrypted format. After deletion, some messages and media shared through private messages were not recovered. Only a few contacts were recovered. No data related to the LINE application was recovered after app uninstallation. The detailed analysis of LINE is shown in Figure 6. Figure 6(a) shows that LINE contacts, m_ids (unique IDs for every contact), messages, and calls shared between both parties with timestamps are recovered from the database (naver_line.db) store in the app package. Messages recovered with the sender/receiver and message type with timestamps are shown in Figure 6(b). Figures 6(c) and 6(d) show the recovery of media files (videos) and audio image, respectively, transferred during the chat session with timestamps.

5.1.3. Whisper. The forensic analysis of Whisper resulted in some data being retrieved. The retrieved data contains

FIGURE 11: Artifacts retrieved from LINE using Autopsy.

puid	user	ts	url	location	are	text	er	text	ima	searc	mage	ate	hearts
6e36a57d-6a...	Stoned_Pallyi	1517247778480	http://cdn-clie	Somewhere	de	Guardian Ang...	0	0	NULL	NULL	0	NULL	2
6e36a57d-6a...	Stoned_Pallyi	1517820264094	http://cdn-clie	Somewhere	de	Don't want to ...	0	0	NULL	NULL	0	NULL	1
6e36a57d-6a...	Stoned_Pallyi	1518335779428	http://cdn-clie	Narowal, Punj...	de	At home after...	0	0	NULL	NULL	0	NULL	4
6e36a57d-6a...	Stoned_Pallyi	1518377814526	http://cdn-clie	Somewhere	de	No one will re...	0	0	NULL	NULL	0	NULL	2
6e36a57d-6a...	Stoned_Pallyi	1518378205078	http://cdn-clie	Narowal, Punj...	de	Best time is th...	0	0	NULL	NULL	0	NULL	2
05650f44a5f3...	Jr_Moonlighte	1518606069000	http://cdn-clie	Lake Odesso, ...	de	That avklov...	0	0	NULL	NULL	0	NULL	1564
05652f90e525...	Platinum_Su...	1518629339000	http://cdn-clie	Raleigh, North...	de	Which fictiona...	0	0	NULL	NULL	0	NULL	349
05650e88de0...	Whale_Gome...	1518606065000	http://cdn-clie	Escondido, Ca...	de	I just spent 3...	0	0	NULL	NULL	0	NULL	1277
05651be5f9e...	stadium_status	1518606070000	http://cdn-clie	Al Muraytibah...	de	If you could pi...	0	0	NULL	NULL	0	NULL	443
05650f17219b...	Not.ee	1518606068000	http://cdn-clie	Fond du Lac, ...	de	Men of quality...	0	0	NULL	NULL	0	NULL	1081
05651bf53b8e...	will_not_send...	1518606030000	http://cdn-clie	Commerce Cit...	de	What's one lif...	0	0	NULL	NULL	0	NULL	413
0564bece9fc...	jheez	1518606064000	http://cdn-clie	Leeds, Englan...	de	So here I am...	0	0	NULL	NULL	0	NULL	624
05650f267fc1...	JoeEggs	1518606068000	http://cdn-clie	Preston, Engl...	de	Just get heard...	0	0	NULL	NULL	0	NULL	653
05651be9149...	ponev	1518606069000	http://cdn-clie	Somewhere	de	My poor fbi a...	0	0	NULL	NULL	0	NULL	630
05651bf869ed...	lordofkings	1518606071000	http://cdn-clie	Media, Penns...	de	I don't unders...	0	0	NULL	NULL	0	NULL	492
05651bd9714...	sexyredhead	1518606069000	http://cdn-clie	Arlington, Tex...	de	Walked out to...	0	0	NULL	NULL	0	NULL	539

(a)

Listing

DM-0.raw\data\sh.whisper\files\me

Table Thumbnail

Page: 1 of 1 Pages: Go to Page: Images: 1-5 Medium

w1517247768051

w1517820253580

w1518335770143

w1518377807121

w151837819711

(b)

sid	gt	wid	im	unread
Filter	Filter	Filter	Filter	Filter
Stoned_Pallyi	f7cd5caa-193f...	05647311ac9	Hy	0
Stoned_Pallyi	7b427077-e3...	05647311ac9	Hy	0
Stoned_Pallyi	2b04ea54-4d...	0564eb18c85	Hy	0
Stoned_Pallyi	43323422-5df...	0564eb18c85	Hy	0
Stoned_Pallyi	f5750d95-cc8...	0564eb18c85	Hi	0
Stoned_Pallyi	4d71fe5a-3ba...	0564eb18c85	?	0
Stoned_Pallyi	6366803a-a2c...	0564eb18c85	...	0
Stoned_Pallyi	33913be3-8f9...	0564eb18c85	...	0
Stoned_Pallyi	a9bbfda2-9b8...	0564eb18c85	...	0
Stoned_Pallyi	e15b966a-59...	0564eb0cb5c	...	0
Stoned_Pallyi	a1a54f8c-d9a...	0564e7b5334	...	0
Stoned_Pallyi	d9c5bad0-b05...	0564e6e1122	...	0
Stoned_Pallyi	e3dc1f22-579...	0564eb18c85	...	0
Stoned_Pallyi	637be4be-99c...	0564eb18c85	...	0
Stoned_Pallyi	92d27e37-8f2...	0564eb18c85	...	0
Stoned_Pallyi	a8c2db3e-f86...	0564f4e2450	...	0
Stoned_Pallyi	eebaf71a-9f6...	0564f4f98c62	...	0

(c)

2ef4b292-4546-4...

b229bd4d-6f80-4...

(d)

FIGURE 12: Artifacts retrieved from Whisper using Autopsy.

information of user accounts, content created or liked by the user, groups he/she follows, private messages shared with friends, location information and other activities. After deletion, all the text messages were recovered and a textual preview of media shared through private messages was recovered. After app uninstallation, no data related to the Whisper app was recovered. The detailed analysis of Whisper

is shown in Figure 7. Figure 7(a) shows the retrieved text messages shared between the user with its friends with time-stamps and location information. Textual information of images received by the user is recovered as shown in Figure 7(b). Figure 7(c) shows the retrieved information about the posts uploaded by or replied by the user with time-stamps, hearts, and location information. Figure 7(d) shows

FIGURE 13: Continued.

(g)

(h)

FIGURE 13: Artifacts retrieved from WeChat using Autopsy.

the posts shared while the user was online with timestamps, Whisper content, and location information.

5.1.4. WeChat. WeChat data files are stored within the parent company Tencent's [59] directory MicroMsg folder. WeChat's database EnMicroMsg.db is encrypted using SqlCipher [60]. Some information was retrieved from the index file named FTS5IndexMicroMsg.db, as shown in Figure 8(a). After data deletion, some messages/media files were recovered in a textual format as shown in Figure 8(b). After app uninstallation, only textual information of media files, i.e., video files as shown in Figure 8(c) and audio files (as shown in Figure 8(d)), was recovered from the smartphone. The detailed analysis of WeChat is shown in Figure 8.

5.1.5. Wickr. Wickr is known as an antiforensic app. It is highly encrypted and claims that no data can be recovered from a device or from network analysis for forensic investigation. All conversations are stored in a highly encrypted database. Wickr does not store any other data within the internal memory of the phone. The detailed analysis of Wickr is shown in Figure 9. By exploring the base.apk file (extracted base.apk file through the .zip archive extractor. In this file, some artifacts have been recovered from classes.dex and classes2.dex files. .dex files were decompiled through Java Decompiler.), it was found that the database wickr_db.db is encrypted with SQLCipher [60] as shown in Figure 9(a). Figure 9(b) shows the WickrDBAdapter File Recover wickr.db Schema that contains account information, contact info, messages sent/received, timestamps, and keys. Figure 9(c) shows that the file folder contains some .wic files that are encrypted. By exploring base.apk, it was found that the ds.wic file is used to store cache data and passwords. Figure 9(d) shows the WickrDBKey.class where it was found that sk.wic contains the key for database. Kck.wic and kcd.wic are also encrypted files that must have contained videos/audio that were sent by the user because these files were deleted after video and audio information sent by the user was deleted (shown in Figure 9(e)). Figure 9(f) shows

that the video sent by the user is recovered from the cache folder.

5.2. Forensic Analysis of the App through Autopsy. This section discusses the artifacts recovered from the apps using Autopsy.

5.2.1. Instagram. Autopsy recovered almost the same data recovered by AXIOM. AXIOM gives the text thread detail with the text/media shared. This is not the case in Autopsy. Autopsy gives the text content and information in the database (have to save the database and open in SQLite browser) shared in DM. The user's activity has been recorded in the cache folder and recovered with timestamps. Video's parts are also recovered in the form jpeg image. After the cache clears, stories and cache data were not recovered. 50 percent of text messages were recovered after deletion from direct.db with date and time information. Images shared during the chat were not recovered. Textual information of media that has been sent or video call done by the user is recovered after data deletion. No data was recovered after app uninstallation. The detailed analysis is shown in Figure 10. Figure 10(a) shows that messages sent through DM are recovered. Figure 10(b) shows that images sent through DM are recovered. Figure 10(c) shows the stories recovered as pending media. Figure 10(d) shows that the images uploaded as the story are recovered after deletion.

5.2.2. LINE. naver_line.db contains the information of text messages shared during private chat, chat history, chat members, and contacts. Autopsy did not recover any text messages after deletion. Deleted images from the timeline have been recovered. Voice message detail recovers after deletion. No data was recovered after app uninstall. The detailed analysis is shown in Figure 11. Figure 11(a) shows the recovered chat history with timestamps and contact information. Figure 11(b) shows that Autopsy recovered the post hidden from the timeline with the option "Hide posts." Backup data of a chat including text messages, media type shared, and call (audio, video) information are recovered as shown in

FIGURE 14: Artifacts retrieved from Instagram using XRY.

Figure 11(c). Profile pictures of all the friends have also been recovered as shown in Figure 11(d). Figure 11(e) shows that voice messages were recovered with timestamps. The video shared through chat was recovered in .jpeg image format as shown in Figure 11(f).

5.2.3. *Whisper*. Artifacts recovered from the *c.db* database's *c* table are the information of private conversation of the user. After deletion, images received while private chatting; Whisper post; event information recovered with the sender name, location, age, gender, and content that has been sent; and some messages with sender and receiver ids and timestamps are recovered after deletion. No artifact was recovered after app uninstallation. The detailed analysis is shown in Figure 12. Figure 12(a) shows the list of every conversation

with the timestamp being stored. The column titled *pid* has the receiver user id and the column *sid* contains the user id of the sender. Figure 12(b) shows that Whisper posted on the timeline were recovered. Figure 12(c) shows that Whisper posted by the people while the user was active is recovered with timestamps and locations. Figure 12(d) shows that images received during chat is recovered.

5.2.4. *WeChat*. WeChat artifacts recovered through Autopsy are stated in this section. The detailed analysis is shown in Figure 13. Figure 13(a) shows the messages recovered from the *FTS5IndexMessage_content* table when it was open in the SQLite browser. Figure 13(b) shows that the audio messages shared during private chat are recovered with timestamps. Figure 13(c) shows that the images received during

(a)

sqlite_master	(70)	Table:
android_metadata	(1)	contacts
contacts	(44)	Live Records:
chat	(4)	44
chat_member	(1)	Deleted Records:
chat_history	(6)	0

RECORD NUMBER	DELETED RECORD	m_id	contact_id	contact_key	name
4	False	u5e4dde96fe64c89f	[NULL]	[NULL]	Saadia Mera
5	False	u1a428e3301c4149	[NULL]	[NULL]	Alina
6	False	u3278634b9922d7	[NULL]	[NULL]	salma
7	False	u7ff34aa728b937e	[NULL]	[NULL]	riffat
8	False	ue4a2e4c65013d9a	[NULL]	[NULL]	Azka

(b)

(c)

(d)

(e)

(f)

(g)

sqlite_master	(3)	Table:
android_metadata	(1)	call_history
call_history	(0)	Live Records:
sqlite_sequence	(1)	0
		Deleted Records:
		2

RECORD NUMBER	DELETED RECORD	id	call_type	caller_mid	contact_id
1	True	1	FCC	u365fa8994a6191f8	[NULL]
2	True	1	FCC	u365fa8994a6191f8	[NULL]

(h)

FIGURE 15: Artifacts retrieved from LINE using XRY.

FIGURE 16: Artifacts retrieved from Whisper using XRY.

FIGURE 17: Artifacts retrieved from WeChat using XRY.

chat are recovered. Figure 13(d) shows that the phone number against which the account was created is recovered in plain text. Textual information of the video shared is recovered after deletion as shown in Figure 13(e). Figure 13(f) shows that images received through private chat are recovered after deletion. Figure 13(g) shows that textual

information of videos is recovered after app uninstallation. Figure 13(h) shows that images shared and uploaded by the user are recovered after app uninstall.

5.2.5. *Wickr*. From analyzing the image from Autopsy, the textual information of the video file is recovered from the

TABLE 5: Comparison of tools on the basis of digital artifacts recovered from SNAs. The (✓) symbol defines that artifact is recovered from the tool, (●) is the symbol for textual information/audio-video not playable, and (▲) defines partially recovered.

[illegible]

TABLE 7: Location and Artifacts Recovered from Instagram before Data Deletion.

Location	Artifacts recovered	AXIOM	Autopsy	XRY
/data/com.instagram.android/databases/ direct.db	Text messages and sender id with timestamps	(✓)	(✓)	(✓)
/data/com.instagram.android/databases/ direct.db	Text messages received with receiver_id with time stamp	(✓)	(✓)	(✓)
/data/com.instagram.android/databases/ direct.db	http link to the accounts recovered	(●)	(●)	(●)
/data/com.instagram.android/databases/ direct.db-journal	Messages from other accounts previously logged in	(✓)	X	X
/data/com.instagram.android/databases/ direct.db/thread	Every thread info, thread id, sender/receiver ids, account info, messages seen/pending, and type of message	(✓)	(✓)	(●)
/data/com.instagram.android/databases/ direct.db/messages	All the information of message sender, receiver ids, name, type, and content	(✓)	(●)	(✓)
/data/com.instagram.android/databases/direct.db-journal	Send images recovered with date & time and sender/receiver name	(✓)	(●)	(✓)
/data/com.instagram.android/databases/direct.db-journal	Information of received media recovered (type, date time)	(✓)	(●)	(●)
/data/com.instagram.android/databases/direct.db-journal	Link of media shared from newsfeed/explorer through DM	(✓)	(✓)	(✓)
/data/com.instagram.android/databases/video.db	Videos and jpeg thumbnails watched by user on news feed with time/date	(✓)	(✓)	(●)
/data/com.instagram.android/databases/video.db	Videos and jpeg thumbnails watched by user on explorer with time/date	(✓)	(✓)	(●)
media/0/Android/data/com.instagram.android/files/videos/VID_20190319_182811_473_session_0	Video shoot through Instagram cam and uploaded by the user	(✓)	(●)	(✓)
/data/com.instagram.android/files/	Text stories	(✓)	(✓)	X
/data/com.instagram.android/files/	Video stories (playable)	(✓)	(●)	X
media/0/Android/data/com.instagram.android/files/rendered_videos	Video shoot through Instagram cam is being segmented in audio and video files	(✓)	(✓)	(✓)
/data/com.instagram.android/cache/ images	Images viewed by the user on newsfeed with date and time	(✓)	(●)	(✓)
/data/com.instagram.android/cache/ images	Images viewed by the user on explorer with date and time	(✓)	(●)	(●)
media/0/Android/data/com.instagram.android/cache/ExoPlayerCacheDir/videocache	Video information watched by users is recovered	(✓)	(✓)	(✓)

TABLE 7: Continued.

Location	Artifacts recovered	AXIOM	Autopsy	XRY
/data/com.instagram.android/cache/	Stories viewed by a user with date and time	(✓)	(●)	(✓)
/data/com.instagram.android/cache/original_images	Images shared through DM	(●)	(●)	(●)
/data/com.instagram.android/shared_prefs/token_store.xml	Token key recovered	(✓)	(✓)	(✓)
/data/com.instagram.android/shared_prefs/2138581153_insta_video_call_notifications.xml	Live session info of user's followers/following	(✓)	(✓)	(✓)
/data/com.instagram.android/shared_prefs/rti.mqtt.ids.xml	Connection key	(✓)	(✓)	(✓)
/data/com.instagram.android/shared_prefs/rti.mqtt.ids.xml	Device key	(✓)	(✓)	(✓)
/data/com.instagram.android/shared_prefs /com.instagram.android_preferences.xml	Last login_nonce recovered	(✓)	(✓)	(✓)
/data/com.instagram.android/shared_prefs /2138581153_USER_PREFERENCES.xml	Recent user searches recovered	(✓)	(✓)	(✓)
/data/com.instagram.android/shared_prefs/2138581153_usersBootstrapServices.xml	List of the follower and following account recovered with timestamps	(✓)	(✓)	(✓)
/media/0/Pictures/Instagram/	Contain all pictures uploaded by the user	(✓)	(✓)	(✓)
/media/0/Movies/Instagram/	Video uploaded by the user	(✓)	(●)	(●)

cache folder. Wickrdb is encrypted database and all the file folder is encrypted. No information regarding communication has been recovered from Wickr.

5.3. Forensic Analysis of Applications through XRY. This section discusses the artifacts recovered from the applications using XRY.

5.3.1. Instagram. The image has also been taken from XRY from all the said cases. After the app uninstalls, the app name was recovered with information that the app deleted on what time and date on the data/data folder. The detailed analysis is shown in Figure 14. Figure 14(a) shows that the database direct.db contains the messages and sent images. Figure 14(b) shows that the thread information of the chat through DM is recovered. Figure 14(c) shows the cache data stored in the cache folder of the app package. Figure 14(d) shows that Cache images are recovered in XRY after a cache clears. After deletion, XRY recovered the messages deleted within 24 hrs with text/media information (type, timestamps) as shown in Figure 14(e). Remnants of the video uploaded on the account are recovered after deletion as shown in Figure 14(f).

5.3.2. LINE. The LINE package is analyzed before any data was deleted using XRY. After LINE uninstallation, the app existence proof is present in location data/data which contains the application name jp.naver.line.android, date, and time of app deletion. The detailed analysis is shown in Figure 15. Figure 15(a) shows that the files shared through private chat have been recovered. Contact details, chat record, and information shared between two parties including text messages, media, and call info with timestamps were

recovered from naver_line.db as shown in Figure 15(b). Figure 15(c) shows that e2ee.db stores private and public keys encrypted with a unique id and timestamp. Images uploaded by the user on LINE's timeline were also recovered as shown in Figure 15(d). The profile picture of friends was recovered as shown in Figure 15(e). The video uploaded on the timeline by the user was recovered as shown in Figure 15(f). Messages that have been deleted with the content information (text, video, and audio) with sender and receiver ids and timestamps are recovered as shown in Figure 15(g). Figure 15(h) shows that call history details were recovered after deletion from call_history.db images and videos that were uploaded by a user on the timeline are also recovered after deletion.

5.3.3. Whisper. Whisper app analyzed by XRY recovered the stated artifacts for all cases. The detailed analysis is shown in Figure 16. Figure 16(a) shows the c.db that contains all the messages that are transmitted between the user and the other users with their ids and timestamps. w.db contains the list of all those people that have posted at the time of the user's connectivity and group user joined as shown in Figure 16(b). Posts uploaded by the user are recovered as shown in Figure 16(c). Images sent by the user were recovered as shown in Figure 16(d). Figure 16(e) shows the cache folder containing the posts viewed by a user with timestamps. Deleted chats are recovered from c.db with the sender and receiver names and timestamps as shown in Figure 16(f). The deleted group's information was recovered. The images sent by the user and then deleted are recovered. The file with the name whisper is recovered after app uninstallation.

5.3.4. WeChat. Artifacts recovered from WeChat through XRY is stated below. The first analysis has been done before

TABLE 8: Location and artifacts recovered from LINE and Whisper before data deletion.

Location	Artifacts recover	AXIOM	Autopsy	XRY
/data/jp.naver.line.android/databases/naver_line.db/contact	Contact data recovered with timestamps (m_id, contact_id, name, and status)	(✓)	(✓)	(✓)
/data/jp.naver.line.android/databases/naver_line.db/group_home	group_id and memebars_id are recovered	(✓)	(✓)	(✓)
/data/jp.naver.line.android/databases/naver_line.db/group	Group name against their id's is recovered	(✓)	(✓)	(✓)
/data/jp.naver.line.android/databases/naver_line.db/members	0,1 indicated if the requested user accepts to be a member or not	(✓)	(✓)	X
/data/jp.naver.line.android/databases/naver_line.db/chat	Chat_id, message content, and timestamp recovered	(✓)	(✓)	(✓)
/data/jp.naver.line.android/databases/naver_line.db/chat_history	Sender/recover id, message content, date, time, message type recovered (audio, video, text, doc, and location)	(●)	(✓)	(✓)
/data/jp.naver.line.android/databases/naver_line.db/chat_notification	Chat_id	(✓)	(✓)	(✓)
data/media/0/Android/data/jp.naver.line.android/storage/toyboxing/line	User email recover	X	X	(✓)
/data/jp.naver.line.android/databases/naver_line_myhome	Post information uploaded by the ser on LINE timelines	(●)	(✓)	(✓)
/data/jp.naver.line.android/databases/call_history.db	caller_id, time, date, and duration of call (audio, video) recovered	(✓)	(✓)	(✓)
data/jp.naver.line.android/databases/e2ee.db	LINE has end-to-end encryption. E2ee.db stores public keys	(✓)	(✓)	(✓)
data/media/0/Android/data/jp.naver.line.android/storage/mo	Images transferred during chat is recovered with timestamp	(●)	(●)	(✓)
data/media/0/Android/data/jp.naver.line.android/storage/mo	Videos transferred during chat is recovered with timestamp	(✓)	(●)	(●)
data/media/0/Android/data/jp.naver.line.android/storage/mo	Audio messages transferred during chat is recovered with timestamp	(●)	(●)	(●)
data/media/0/Android/data/jp.naver.line.android/storage/write	Images uploaded by the user on LINE timeline recovered with timestamps	(✓)	(✓)	(✓)
/data/media/0/Android/data/jp.naver.line.android/storage/write	Hidden post recovered	X	(✓)	X
/media/0/Android/data/jp.naver.line.android/cache/mm	The video viewed by the user on LINE timeline recovered	(✓)	(●)	(✓)
/data/jp.naver.line.android/shared_prefs/Extended_My_Profile.xml	User's date of birth recovered	(✓)	(✓)	(✓)
/data/jp.naver.line.android/shared_prefs/ServiceInfoManager.xml	Server key for the profile and encryption standard	(✓)	(✓)	(✓)
data/com.whisper.andrid/database/c.db	Private conversion details recovered with timestamps	(✓)	(✓)	(✓)
data/com.whisper.andrid/database/c.db/m	Text messages with timestamps and member_id recovered	(✓)	(✓)	(✓)
data/com.whisper.andrid/database/w.db	Information about the groups joint by the user with time/date and URL	(✓)	(✓)	(✓)
data/com.whisper.andrid/database/w.db/n	Notification received by the user (hearts to whisper/reply to whisper)	(✓)	(✓)	(✓)
data/com.whisper.andrid/database/w.db/w	Whisper posted by people nearby with timestamps	(✓)	(●)	(●)
the /data/sh.whisper/files/me/	Whispers that has been posted by the user (textual preview) recovered	(✓)	X	(●)
/data/sh.whisper/files/whisper-chat/.	Files sent/received by the user to other people recovered	(●)	(●)	(●)
/data/sh.whisper/cache/picasso-cache	All the whisper that has been seen by the user	(✓)	(●)	(✓)
/data/sh.whisper/shared_prefs/com.mixpanel.android.mpmetrics.MixpanelAPI_c39eea2c9ad72a79d1688ca82c50cb94.xml	Whisper app installation data, time, Uid, user location, gender, and date of birth. List of groups that have been joined by the user	(✓)	(✓)	(✓)

TABLE 9: Location and artifacts recovered from WeChat and Wickr before data deletion.

Location	Artifacts recovered	AXIOM	Autopsy	XRY
data/com.tencent.mm/MicroMsg/71a0c06fe86c4efd9b0b6e1112d906/EnMicroMsg.db	Encrypted database. Did not reveal any information	(✓)	(✓)	(✓)
/data/com.tencent.mm/shared_prefs/com.tencent.mm_preferences.xml	u_id, device info, username, and login mobile number are recovered	(✓)	(✓)	(✓)
/data/com.tencent.mm/MicroMsg/71a0c06fe86c4efd9b0b6e1112d906/FTS5IndexMicroMsg.db/FTS5MetaMessage	Messages between U_id of contacts and talkers (receiver of user's messages) with timestamps	(✓)	(✓)	(✓)
/data/com.tencent.mm/MicroMsg/71a0c06fe86c4efd9b0b6e1112d906/FTS5IndexMessagecontant	Text messages recovered	(✓)	(✓)	(✓)
/media/0/tencent/MicroMsg/71a0c06fe86c4efd9b0b6e1112d906/voice2/0b/50/msg_01000602111819a6b51aaa6106.amr	Audio sent by the user is recovered	(✓)	(●)	(✓)
/media/0/tencent/MicroMsg/71a0c06fe86c4efd9b0b6e1112d906/video/videoCompressTmp	Video sent by the user is recovered	(●)	(✓)	(✓)
/data/app/com.mywickr.wickr2-1/base.apk/classes.dex/WickrDBAdapter.class	This file revealed that wickr_db is encrypted by SQLite Cipher (AES-256 full database encryption)	(✓)	(✓)	(✓)
	Recovered from			
/data/app/com.mywickr.wickr2-1/base.apk/classes.dex/WickrDBAdapter.class	WickrDBAdapter.class. DB saves account information, contact info, messages with timestamps, and keys	(✓)	(✓)	(✓)
/data/com.mywickr.wickr2/files	Encrypted .wic files "ds.wic," "sk.wic," Kck.wic, and kcd.wic recovered	(✓)	(✓)	(✓)
/data/app/com.mywickr.wickr2-1/base.apk/classes.dex/WickrDBKey.class	WickrDBKey.class described that "sk.wic" stores the encrypted key of database	(✓)	(✓)	(✓)
/data/com.mywickr.wickr2/files	Kck.wic and kcd.wic must have contained media files (images, video, and audio) because these files were deleted automatically after media of Wickr deleted	(✓)	(✓)	(●)

TABLE 10: Artifacts recovered from Magnet AXIOM after data deletion and app uninstallation.

	Instagram	LINE	Whisper	WeChat	Wickr
	80% of text messages deleted	Call history	Text messages (send/received) recovered	50% of text messages	Encrypted database
	Textual information of shared media	Group member detail	Hearts and replay notification	Image uploaded on the timeline	Video from the cache folder
After data deletion	Account information	Textual preview of video uploaded after deletion	Group data	Video uploaded on the timeline	-
	Uploaded pictures recovered	Textual preview of images	Image sent	Video shared during the chat	-
	-	-	Posts by the user	Images sent recovered during the chat	-
After Apps Uninstall	-	An empty folder names LINE	-	Video uploaded	-
	-	-	-	Image uploaded	-
	-	-	-	Image send during the chat	-

TABLE 11: Artifacts Recovered from Autopsy after Data Deletion and App Uninstall.

	Instagram	LINE	Whisper	WeChat	Wickr
	50 % of Text messages deleted	Hidden/deleted image recovered	Text messages recovered	SSID of chat parties	Encrypted database
	Account information	Call history	Heart and replay notification	Image uploaded on the timeline	Video from the cache folder
After Data Deletion	—	Group member detail	Group data	Video uploaded on the timeline	—
	—	Textual preview of the video uploaded after deletion	Image send	Video shared during the chat	—
	—	Textual preview of images	Posts by user	Images shared during the chat	—
	—	—	—	Image captured by WeChat	—
After app uninstallation	A filename with deletion date/time	—	—	Profile picture	—
	—	—	—	Video uploaded	—
	—	—	—	Image uploaded	—
	—	—	—	Private chat image	—
	—	—	—	Image sent during the chat	—

data deletion. No message information has been recovered as all the databases are encrypted. The detailed analysis is shown in Figure 17. After the deletion of some data, no text messages were recovered. Images and videos uploaded were recovered after deletion. After app uninstallation, all the media files and their information were recovered. Encrypted databases and cache files were not recovered. The profile picture, images, and videos uploaded and shared through private chats are all recovered.

5.3.5. *Wickr*. No data recovery from Wickr could be managed except from the metadata from the base.apk file. After app uninstallation, the location data/data contain the filename com.mywickr.wickr2 with the deleted status being yes.

Detailed information of artifacts that were recovered after three scenarios is discussed in Table 5. The (✓) symbol defines that artifact are recovered from the tool, (●) is the

symbol for textual information/audio-video not playable, and (▲) defines partially recovered. Table 6 describes the artifacts recovered from SNAs before data deletion, after data deletion, and after app uninstallation according to categories proposed in Table 4. The details of artifacts recovered and their location are presented in Tables 7–13. Tables 7–9 state the artifacts recovered from apps and their locations before any data is deleted from apps. Similarly, Tables 10–12 show the artifact information recovered after data deletion and after app uninstallation from every app using all three tools.

6. Results Analysis and Tool Evaluation

This section presents an analysis and discussion on the output of forensic analysis of five SNAs. A comparison of tools on the basis of their capabilities is also presented.

TABLE 12: Artifacts recovered from XRY after data deletion and app uninstallation.

After data deletion	Instagram	LINE	Whisper	WeChat	Wickr
	Text messages deleted within 24 hrs	Group member detail	Text messages recovered	Image uploaded on the timeline	Textual info of the image
	Account information	Call history	Heart and replay notification	Video uploaded on the timeline	—
	Textual preview of the shared image	Video uploaded after deletion	Group data	Video shared during the chat	—
	Video uploaded after deletion	Textual preview of images	Image sent	Images shared during the chat	—
After app uninstallation	—	—	Posts by the user	Images received in private chat	—
	—	—	—	Image captured by WeChat	—
	Filename with deletion date/time	Filename with deletion date/time	Filename	Profile picture	The app filename recovered
	—	—	—	Video uploaded	—
	—	—	—	Image uploaded	—
	—	—	—	Private chat image	—
	—	—	—	Encrypted database info	—
	—	—	—	App filename	—
	—	—	—	Image sent	Image sent
	—	—	—	—	—

6.1. Analysis of Apps

6.1.1. Instagram. During investigation of the internal storage of the Android phone for Instagram app data, many artifacts are recovered that can help the investigation. The database folder that contains all the messages, i.e., text message, video, audio, emojis, or the link to online media that have been transferred to or from the user is being recovered unencrypted with the information of date and time. The posts that are uploaded on the account and stories are also recovered with date/time information. The cache folder stores all the online activity done by the user. Every post, picture, story, or video seen by the user get recorded in the cache folder. The shared preference folder contains an .xml file that stored user's account information in plain text format. The number of accounts logged in the app during specific time period are recovered through their login nonce. The information stored in these files contain live sessions attended and last search made etc. After the messages and posts are deleted, data from the database is deleted but some of the messages are being recovered from the .db journal file. The posts have also been recovered after deletion. After the uninstallation of the app, only the pictures that had been uploaded by the user are recovered. If we clear the cache of our phone, photos, videos, and Instagram stories cannot be recovered.

6.1.2. LINE. Different artifacts are recovered from the LINE app. The main focus of our research is on four folders stored inside the local memory of the smartphone. By examining the internal memory of the smartphone, it was determined that the app stores some artifacts on different locations in the app folder. These artifacts are related to its activity within the internal memory. We can understand the DB schema and can recover the critical information of LINE app activity from the database folder. Note that the importance and the

location of the artifacts can be examined during any criminal investigation. It was discovered that LINE manages the directories within its app folder. LINE app stores the cache for transferred, downloaded, and uploaded files in the app cache. From the examination of local memory and databases of the app, we can recover the information (message/media transferred, cache copies) within the DB table in a plain text form with the exception of the password. All the contacts are recovered from the database folder even after deletion. We realize that app data is stored in a different location and different forms can be interesting in a forensic investigation.

6.1.3. Whisper. Whisper post is originally a message sent by user publicly and it includes the name of the sender, message, date/time when it was posted, the link of the image, location, the likes (hearts) it received, and replies to these posts. The name of the user is not a unique identifier in a whisper; that means that the same username can be used by different users and can also be changed anytime by the user. The user phone does not store the images of the post in the app but these images are cached by the phone and stored in the device. Links of posts are also stored on the phone but not all the images are available on these links. Post location information can also be determined in Android with the longitude and latitude for each post. The heart and reply counter keeps the info of likes on a post. Whisper messages are privately sent or received by the user. All the messages with timestamps, media type, and other party information are recovered even after the deletion of some messages or the deletion of the whole thread. Like Whisper posts, in whisper messages, the username is also not a unique identifier so it became difficult to confirm the exact identity of the other party. There is no way to confirm if the message has been received or read by the other person or not. Whisper stores its information against the Mac address of the phone. It does

TABLE 13: Comparison between tools on the basis of the number of artifacts recovered.

Tools	Artifacts	Instagram			LINE			Whisper			WeChat			Wickr		
		Send/receive	Recover		Send/receive	Recover		Send/receive	Recover		Send/receive	Recover		Send/receive	Recover	
Magnet AXIOM	Text messages	Incoming	10	12	10	7		20	20		10	8		5	0	
		Outgoing	10	10	10	8		20	20		10	8		5	0	
	Images	Incoming	5	0	5	0		2	2		4	1		2	0	
		Outgoing	5	5	2	0		2	2		1	1		2	0	
		Stories	1	1	-	-		-	-		-	-		-	-	
		Uploaded	4	4	4	4		5	5		2	2		-	-	
	Videos	Incoming	-	-	1	0		-	-		1	0		1	0	
		Outgoing	-	-	1	1		-	-		1	1		1	1	
		Stories	1	1	-	-		-	-		-	-		-	-	
		Uploaded	1	1	1	1		-	-		1	1		-	-	
Autopsy	Audio Calls	Incoming	-	-	1	1		-	-		1	1		-	-	
		Outgoing	-	-	1	1		-	-		1	1		-	-	
	Video calls	Incoming	1	1	1	1		-	-		1	1		-	-	
		Outgoing	1	1	1	1		-	-		1	1		-	-	
	Audio	Incoming	1	0	1	0		-	-		1	0		1	0	
		Outgoing	1	1	1	1		-	-		1	1		1	0	
	Text messages	Incoming	10	8	10	8		20	20		10	8		5	0	
		Outgoing	10	7	10	6		20	20		10	8		5	0	
	Images	Incoming	5	0	5	0		2	2		4	2		2	0	
		Outgoing	5	3	2	0		2	2		1	0		2	0	
Autopsy	Videos	Stories	1	1	-	-		-	-		-	-		-	-	
		Uploaded	4	4	4	5		5	5		2	2		-	-	
		Incoming	-	-	1	0		-	-		1	1		1	0	
		Outgoing	-	-	1	1		-	-		1	1		1	1	
	Audio calls	Stories	1	1	-	-		-	-		-	-		-	-	
		Uploaded	1	1	1	1		-	-		1	1		-	-	
		Incoming	-	-	1	1		-	-		1	1		-	-	
		Outgoing	-	-	1	1		-	-		1	1		-	-	
	Video calls	Incoming	1	1	1	1		-	-		1	1		-	-	
		Outgoing	1	1	1	1		-	-		1	1		-	-	
Autopsy	Audio	Incoming	1	0	1	0		-	-		1	0		1	0	
		Outgoing	1	1	1	1		-	-		1	1		1	0	

TABLE 13: Continued.

Tools	Artifacts	Instagram			LINE			Whisper			WeChat			Wickr		
		Send/receive	Recover		Send/receive	Recover		Send/receive	Recover		Send/receive	Recover		Send/receive	Recover	
XRY	Text messages	Incoming	10	8	10	7	20	18	10	8	5	0				
		Outgoing	10	8	10	8	20	18	10	8	5	0				
	Images	Incoming	5	0	3	0	2	0	2	2	2	0				
		Outgoing	5	0	3	0	2	2	4	4	2	0				
		Stories	1	0	-	-	-	-	-	-	-	-				
		Uploaded	4	4	3	3	5	5	1	1	-	-				
	Videos	Incoming	-	-	2	0	-	-	1	0	1	0				
		Outgoing	-	-	2	0	-	-	1	1	1	0				
		Stories	1	0	-	-	-	-	-	-	-	-				
		Uploaded	1	1	1	1	-	-	1	1	-	-				
	Audio calls	Incoming	-	-	1	1	-	-	1	1	-	-				
		Outgoing	-	-	1	1	-	-	1	1	-	-				
	Video calls	Incoming	1	1	1	1	-	-	1	1	-	-				
		Outgoing	1	1	1	1	-	-	1	1	-	-				
	Audio	Incoming	1	0	1	0	-	-	1	0	1	0				
		Outgoing	1	1	1	1	-	-	1	1	1	1				

TABLE 14: Ranking of tools according to digital artifact recovery.

Tools	Instagram		LINE		Applications				WeChat		Wickr		Total recovered artifacts	Index calculated	Ranking
	<i>T</i>	<i>R</i>	<i>T</i>	<i>R</i>	<i>T</i>	<i>R</i>	<i>T</i>	<i>R</i>	<i>T</i>	<i>R</i>	<i>T</i>	<i>R</i>			
Magnet AXIOM	41	37	40	26	49	49	36	27	18	1	140		76.00%		1
Autopsy	41	28	40	26	49	49	36	28	18	1	132		71.70%		2
XRY	41	24	40	24	49	43	36	30	18	0	121		65.70%		3

not have any email id or password and not any phone number needed to register into the platform. However, there is an email registration option that is present in new versions of the app. The user needs to install the app and can start posting and messaging. A username is given by the app. All the whispers can be seen. Turn on the location and the user can see all the whispers that have been posted by the people near its location. If the user uninstalls the app and reinstalls it, it recovers its own account and all the data and activities that have been carried out by the user on that account. But if the user uninstalls the app and restarts its phone and reinstalls the app, its account is gone forever. The user will be registered against another name and gets a new account.

6.1.4. WeChat. From the analysis of the internal memory of the phone, it was revealed that WeChat [14] created the directory Tencent [59] to store its data in the internal memory. The Tencent directory contains all the files including databases, caches, and media information that has been shared or uploaded on the timeline by the user. WeChat [14] cares about privacy more than most social networking apps because of some critical features, i.e., payments. EnMicroMsg.db is a database within this directory which is encrypted. It uses SQLCipher [60] to encrypt its database. All previous researches about WeChat describe that EnMicroMsg.db contains messaging information of the user and describes the method to decrypt this database. A script [61] needs to run with SQLCipher to decrypt the said database. That method is successful for the Android phone's previous versions. For WeChat version 6 or more running on Android version 6.0.x or higher, the database EnMicroMsg.db is not decrypted through the methods described in [61, 62]. Since lower versions of WeChat cannot be installed on Android versions higher than 5, so, the information within this database is not possible to recover. In [62], the previous versions of WeChat were installed on Android 4.4.2 and decrypted successfully using the same methods described in [63, 64]. So, it was determined that the encryption in the latest version of WeChat in Android 6.0.1 or higher is different from the previous version and it is not possible to recover data from it. An index file named FTS5IndexMicroMsg.db contains the information about the contact and plain text messages. The Meta_messages table contains the unique ids of the user; the talker with a timestamp and message_content table contain the content of the messages. The main issue is that we cannot tell who sends which message to whom and when. This database is also encrypted in a later version of WeChat.Media that has been shared through messages and uploaded by the user on the timeline which is recovered from the com.tencent/media/0/MicroMsg folder. It contains the jpeg images, mp4 videos, and audio file transfer during the chat. After data deletion, this folder contains these files stored in this location. The shared preference folder contains critical information, i.e., username and the phone number through which the account was created when the account was created. If we clear the phone cache, it was discovered that the user automatically logs out from the

TABLE 15: Comparison of tools according to NIST standards.

Type	Features	Magnet AXIOM	XRY	Autopsy
Core requirements	SPT-CR-01	(✓)	(✓)	(▲)
	SPT-CR-02	(✓)	(X)	(▲)
	SPT-CR-03	(✓)	(X)	(▲)
	SPT-CR-04	(✓)	(✓)	(✓)
	SPT-RO-05	(✓)	(✓)	(✓)
	SPT-RO-06	(✓)	(✓)	(✓)
Optional requirements	SPT-RO-08	(✓)	(✓)	(✓)
	SPT-RO-09	(✓)	(✓)	(▲)
	SPT-RO-13	(✓)	(✓)	(▲)
	SPT-RO-14	(✓)	(✓)	(X)
	SPT-CA-01	(✓)	(✓)	(X)
	SPT-CA-02	(✓)	(✓)	(▲)
Core assertion	SPT-CA-03	(✓)	(X)	(▲)
	SPT-CA-04	(✓)	(✓)	(✓)
	SPT-CA-05	(✓)	(✓)	(✓)
	SPT-CA-06	(✓)	(✓)	(✓)
	SPT-CA-07	(✓)	(✓)	(✓)
	SPT-CA-24	(✓)	(✓)	(✓)
	SPT-CA-25	(✓)	(✓)	(✓)
	SPT-CA26	(✓)	(✓)	(●)
	SPT-CA27	(✓)	(●)	(●)
	SPT-CA29	(✓)	(✓)	(▲)
Optional assertion	SPT-CA30	(✓)	(✓)	(▲)
	SPT-CA31	(✓)	(X)	(▲)
	SPT-AO25	(✓)	(✓)	(✓)
	SPT-AO26	(✓)	(✓)	(✓)
	SPT-AO27	(X)	(●)	(●)
	SPT-AO31	(✓)	(✓)	(●)
	SPT-AO37	(✓)	(●)	(✓)
	SPT-AO38	(✓)	(●)	(✓)
	SPT-AO39	(●)	(●)	(●)

account and he needs to log in again with the username and password.

6.1.5. Wickr. Wickr secures the internal information by encrypting the local storage. Wickr's delicate information, i.e., id keys, account data, and messages, is stored in an encrypted storage in the phone. This information in the storage container is decrypted only when the user is logged in the account and can be used for any activity. When a user logs off, the container is encrypted again with Klds and expelled from the persistent memory. Klds is put away in an encoded configuration with the goal that it might be recuperated upon the following client login. The key used to encode and decode Klds is taken from the client's passphrase utilizing script [65]. Klds is put away in an encoded configuration with the goal that it might be recuperated upon the following client login. The key used to encode and decode Klds is taken from the client's passphrase utilizing script. Successful login for this

TABLE 16: Comparison of tools according to additional parameters.

Additional parameters		Magnet AXIOM	Autopsy	XRY
Processing time (physical acquisition + processing)	4–8 hrs (fast)			(✓)
	8–12 hrs (medium)		(✓)	
	12–16 hrs (slow)	(✓)		
User friendly	Portable case file	(✓)	X	X
	GUI	(✓)	(✓)	(✓)
	Artifact connectivity	(✓)	X	X
	Categorization	(✓)	(✓)	X
	DB	(✓)	(✓)	(✓)
Artifacts	Media/text exchanged	(✓)	(✓)	(●)
	Timeline	(✓)	(●)	(●)
	Account/user information	(✓)	(●)	(✓)
	Calls	(✓)	(✓)	(✓)
Keyword search option	Timestamps	(✓)	(✓)	(✓)
Accuracy		(✓)	(✓)	(●)

situation is equivalent to having the capacity to effectively unscramble Klds and get to an encrypted container material. Those clients who wish to dependably remain signed in to Wickr basically store the secret word-determined key in stage gave secure capacity. Along these lines, delicate material is constantly encoded when the Wickr application is not dynamic [66]. The metadata about how and where Wickr app stores its information is identified while exploring the base.apk file. By exploring the files stored within the .apk file, it was determined that the information related to messages with timestamps and media type is stored in a database named wickr_db. The key through which wickr_db is encrypted is also encrypted and stored within the phone. The database can be decrypted only if the user will log in to the account with the username and password. These phrases with a random number decrypt the key and the key decrypts the database. It was also discovered that a database is encrypted through SQLCipher by the SQL helper class present in the WickrDbAdapter.class file. Two files sk.wic and ds.wic are also encrypted. By analyzing the file in the .apk file of Wickr app, it was discovered that the ds.wic file contains the cache data of Wickr and sk.wic which contain the key of the database which is also encrypted.

6.2. Tools Evaluation. Three tools are used in this research—Magnet AXIOM, Autopsy, and XRY. Magnet AXIOM and XRY have the capability to extract the data from the smartphone and present the artifacts in a human-understandable format. Autopsy just analyzes the already-extracted image. The tools are evaluated on the basis of three factors.

- (i) Number of artifacts recovered by the tool
- (ii) NIST standard tool assessment document [19, 20]
- (iii) Additional parameters

The result of this research can be used as recommendations to investigators to handle the cases associated with

these apps. The overall ranking of tools according to digital artifacts recovery is presented in Table 14.

6.2.1. Number of Artifacts Recovered by a Tool. All three tools are analyzed on the basis of their capability to recover digital artifacts from five SNAs. These numbers give us the validation of the performance of tools. Details of the number of artifacts recovered from every app using these tools are shown in Table 13. Tools are ranked according to the capability of artifacts to be recovered by them. The index number has been calculated according to the formula stated in (1) as follows:

$$P = \frac{\sum Nr}{(Nt)} * 100, \quad (1)$$

where P is the percentage of useful extractions, Nr is the number of recovered artifacts, and Nt is the total number of artifacts

The index number for every application is calculated according to equation (1). The Magnet AXIOM index is calculated by dividing the number of artifacts recovered (R) from all five applications through Magnet AXIOM with a total number of artifacts (T) sent times 100, and the result index is 76 percent. The indexes of Autopsy and XRY are also calculated in the same way. Autopsy is ranked second in as an image analysis tool with an index of 71.7 percent and XRY is ranked third with an index of 65.7 percent.

6.2.2. NIST Standard Tool Assessment Document. NIST published an assessment plan to measure the performance of a tool [19, 20]. It is important to develop the method that can standardize the tool according to its capabilities. NIST releases some factors and methods to calculate the performance of a forensic tool based on the outcomes of the assessment plan conducted by NIST. In Table 15, tools are compared against the core requirements, optional requirements, core assertions, and optional assertions of

smartphone examination tools where the (✓) symbol defines that tool supports the factor, symbol (●) defines partially supporting, symbol (X) defines not supporting, and symbol (▲) defines not applying for a specific tool. According to the NIST parameter of smartphone examination tools, Magnet AXIOM did fulfill most of the requirements.

6.2.3. Additional Parameters. Finally, the performance of tools is evaluated on the basis of some parameters that were defined during this research and tool performance capability can be judged by these parameters. These six parameters are

- (i) Processing time
- (ii) User friendliness
- (iii) Compatibility
- (iv) Artifacts recovery
- (v) Keyword search option
- (vi) Accuracy

Table 16 gives a detailed comparison of the tools according to these parameters where the (✓) symbol defines the tool that supports the factor, symbol (●) defines partly supporting, symbol (X) defines not supporting, and symbol (▲) defines not applicable for a specific tool. According to the combined results of defined tool evaluation factors (no. of artifacts a tool recovers, NIST parameter of smartphone analysis tools, and additional parameters) and on the basis of overall performance, Magnet AXIOM is the number one followed by XRY and Autopsy.

7. Conclusions and Future Work

Various tools are available commercially and proprietary through which data acquisition and forensic analysis can be done. In this research, Magnet AXIOM and XRY are used to acquire data from five social networking apps in three different scenarios: before any data deleted from the app, after some data deleted, and after app uninstall. The outcomes of research explain that a large number of artifacts of Instagram, LINE, Whisper, and WeChat are recovered from the smartphone internal memory. Wickr, on the other hand, discloses very little information. Potential artifacts have been categorized to utilize them to create a report. Tools are analyzed with respect to their capabilities, NIST standards for smartphone analysis tools, and few additional parameters defined during this study. The results of this analysis report that among the three tools, Magnet AXIOM is ranked no. 1 with an index no. of 76.0% followed by Autopsy at 71.5% and XRY at rank 3 with an index of 65.5%. According to the NIST parameter of smartphone analysis tools and additional parameters on the basis of overall performance, Magnet AXIOM is the number one followed by XRY and Autopsy. In the future, a new version of Android Smartphones can be analyzed for application forensics as almost every 3 month, a new version or software update is released for Android. This leaves a lot of areas to further research the apps on the latest version and analyze the security flaws.

New apps like *Omele*, *Periscope*, and *Azar* which are becoming popular within teenagers need some attention from forensic investigators. Every tool has some weaknesses, and for the better and accurate results, forensic investigators can use the combination of different tools in his investigation to get more reliable results by using the unique capability of every single tool.

Data Availability

No data were used to support this study.

Conflicts of Interest

The authors declare that there are no conflicts of interest regarding the publication of this paper.

Acknowledgments

The authors of this paper are extremely thankful to the Department of Information Security, National University of Sciences and Technology (NUST), Islamabad, Pakistan, for its support in the research.

References

- [1] Global social media research summary September 2019 <https://www.smartinsights.com/social-media-marketing/social-mediastrategy/new-global-social-media-research/>.
- [2] DataReportal – Global Digital Insights, 2021, March 2021 <https://datareportal.com/reports/digital-2020-october-global-statshot>.
- [3] “51 critical cyberbullying statistics in 2020,” <https://www.broadbandsearch.net/blog/cyber-bullying-statistics>.
- [4] “The-Annual-Bullying-Survey-2017-1.pdf,” December 2019 <https://www.ditchthelabel.org/wp-content/uploads/2017/07/The-Annual-Bullying-Survey-2017-1.pdf>.
- [5] N. Jain and V. Shrivastava, “Cyber crime changing everything—an empirical study,” *International Journal of Computer Application*, vol. 1, no. 4, 2014.
- [6] M. Sharma and S. Kaur, “Cyber crimes becoming threat to cyber security,” *IASR Journals*, vol. 2, no. 1, 2019 https://www.academia.edu/39618017/Cyber_Crimes_Becoming_Threat_to_Cyber_Security.
- [7] U. Sharma, S. Ghisingh, and E. Ramdinmawii, “A study on the cyber, crime and cyber criminals a global problem,” *Journal: International Journal of Web Technology*, vol. 3, pp. 172–179, 2014.
- [8] R. A. Grimes, *What Is Personally Identifiable Information (PII)? How to Protect It under GDPRCSO* Online August 2019; <https://www.csoonline.com/article/3215864/how-to-protect-personally-identifiable-information-piiunder-gdpr.html>.
- [9] H. Saini, Y. S. Rao, and T. C. Panda, “Cyber-crimes and their impacts: a review,” *International Journal of Engineering Research and Applications*, vol. 2, no. 2, pp. 202–209, 2012.
- [10] H. Mahalik, R. Tamma, and S. Bommesetty, *Practical Mobile Forensics*, Packt Publishing Ltd, 2016.
- [11] Instagram, App Store, 2010, August 2019. <https://apps.apple.com/us/app/instagram/id389801252>.

- [12] LINE Free Calls, *Messages-Apps on Google Play* Googlecom August 2019 <https://play.google.com/store/apps/details>.
- [13] *Whisper Apps on Google Play* Googlecom August 2019 <https://play.google.com/store/apps/details>.
- [14] *WeChat Apps on Google Play* Googlecom August 2019 <https://play.google.com/store/apps/details>.
- [15] *Wickr Me Private Messenger Apps on Google Play* Googlecom August 2019 <https://play.google.com/store/apps/details>.
- [16] Magnet AXIOM Digital Investigation Platform|*Magnet Forensics* Magnet Forensics August 2019 <https://www.magnetforensics.com/products/magnet-axiom/>.
- [17] *Autopsy* Sleuthkit.org August 2019 <https://www.sleuthkit.org/autopsy/>.
- [18] MSAB, *MSAB The Pioneers of Mobile Forensics* MSAB August 2019 <https://www.msab.com/>.
- [19] R. P. Ayers, *Smart Phone Tool Specification*|NIST, Computer Forensic Tool Testing, 2017, August 2019. <https://www.nist.gov/publications/smart-phone-tool-specification>.
- [20] NIST, *Smart Phone Tool Test Assertions and Test Plan*, NIST, US Department of Commerce, 2010.
- [21] *Android (Operating System)*, Wikipedia, 2019.
- [22] A. Hoog, *Android Forensics-Investigation*, Syngress, 2011.
- [23] "Application sandbox|android open source project," 2019, September 2019 <https://source.android.com/security/app-sandbox>.
- [24] B. Reaves, J. Bowers, S. A. Gorski Iii et al., "droid: assessment and evaluation of android application analysis tools," *ACM Computing Surveys (CSUR)*, vol. 49, no. 3, pp. 1–30.
- [25] B. D. Carrier and E. H. Spafford, "Categories of digital investigation analysis techniques based on the computer history model," *Digital Investigation*, vol. 3, pp. 121–130, 2006.
- [26] R. Ayers, S. Brothers, and W. Jansen, *NIST Special Publication 800-101 Guidelines on Mobile Device*, Obtenido de National Institute of Standards and Technology, 2014, <http://nvlpubs>.
- [27] A. Verma, "What is rooting? Is rooting my android smart-phone illegal? Fossbytes," November 2017; <https://fossbytes.com/what-is-rooting-meaning-android-legal>.
- [28] T. Almeahmadi and O. Batarfi, *Impact of Android Phone Rooting on User Data Integrity in Mobile Forensics*, IEEE, 2021.
- [29] S. Park, S. Park, and K. Ma, "An automatic user activity analysis method for discovering latent requirements: usability issue detection on mobile applications," *Sensors*, vol. 18, no. 9, p. 2963, 2018.
- [30] F. Rebhi, *Development of a Tool for Analysis and Visualization of Android Logs*, Ecole Nationale des Sciences de l'Informatique (ENSI), Tunisie, 2013, <https://hal.inria.fr/hal-00922034>.
- [31] P. Andriotis, G. Oikonomou, and T. Tryfonas, "Forensic analysis of wireless networking evidence of android smartphones," in *2012 IEEE International Workshop on Information Forensics and Security (WIFS)*, pp. 109–114, IEEE, 2012.
- [32] P. Stephenson, "A comprehensive approach to digital incident investigation," *Information Security Technical Report*, vol. 8, no. 2, pp. 42–54, 2003.
- [33] C. G. Nolte, *Privacy in Social Networks – Economic Options for Regulation*, ResearchGate, 2017, https://www.researchgate.net/publication/324517531_Privacy_in_social_networks_-_economic_options_for_regulation.
- [34] M. P. Aji, I. Riadi, and A. Lutfhi, "The digital forensic analysis of Snapchat application using XML records," *Journal of Theoretical & Applied Information Technology*, vol. 95, no. 19, 2017.
- [35] T. Mehrotra and B. Mehtre, "Forensic analysis of Wickr application on android devices," in *2013 IEEE International Conference on Computational Intelligence and Computing Research*, pp. 1–6, IEEE, 2013.
- [36] A. Mahajan, M. Dahiya, and H. Sanghvi, "Forensic analysis of instant messenger applications on android devices," 2013, <http://arxiv.org/abs/13044915>.
- [37] T. Mathavan and M. A. Nagoor, "Acquisition and analysis of artifacts from instant messenger on android device," *International Journal of Engineering Research & Technology*, pp. 1210–1212, 2014.
- [38] D. Walnicky, I. Baggili, A. Marrington, J. Moore, and F. Breiteringer, "Network and device forensic analysis of Android social-messaging applications," *Digital Investigation*, vol. 14, pp. S77–S84, 2015.
- [39] C. Anglano, M. Canonico, and M. Guazzone, "Forensic analysis of the chatsecure instant messaging application on android smartphones," *Digital investigation*, vol. 19, pp. 44–59, 2016.
- [40] O. S. Adebayo, S. A. Sulaiman, O. Osho, J. Alhassan, and S. Abdul-hamid, *Forensic Analysis of Kik Messenger on Android Devices*, ResearchGate, 2017, https://www.researchgate.net/publication/321268908_Forensic_Analysis_of_Kik_Messenger_on_Android_Devices.
- [41] J. H. Ryu, N. Y. Kim, B. W. Kwon, S. K. Suk, J. H. Park, and J. H. Park, "Analysis of a third-party application for mobile forensic investigation," *Journal of Information Processing Systems*, vol. 14, no. 3, 2018.
- [42] R. Umar, I. Riadi, and G. M. Zamroni, "Mobile forensic tools evaluation for digital crime investigation," *International Journal on Advanced Science, Engineering and Information Technology*, vol. 8, no. 3, pp. 949–955, 2018.
- [43] G. B. Satrya, P. T. Daely, and M. A. Nugroho, "Digital forensic analysis of Telegram Messenger on Android devices," in *2016 International Conference on Information & Communication Technology and Systems (ICTS)*, pp. 1–7, IEEE, 2016.
- [44] G. B. Satrya, P. Daely, and S. Y. Shin, "Android forensics analysis: private chat on social messenger," in *2016 Eighth International Conference on Ubiquitous and Future Networks (ICUFN)*, pp. 430–435, IEEE, 2016.
- [45] J. Gregorio, A. Gardel, and B. Alarcos, "Forensic analysis of telegram messenger for Windows phone," *Digital Investigation*, vol. 22, pp. 88–106, 2017.
- [46] J. Choi, J. Park, and H. Kim, "Forensic analysis of the backup database file in KakaoTalk messenger," in *2017 IEEE International Conference on Big Data and Smart Computing (Big-Comp)*, pp. 156–161, IEEE, 2017.
- [47] R. Al Mushcab and P. Gladyshev, "Forensic analysis of instagram and path on an iPhone 5s mobile device," in *2015 IEEE Symposium on Computers and Communication (ISCC)*, pp. 146–151, IEEE, 2015.
- [48] A. A. Abbasi, S. Saleem, and R. Zulqarnain, "Forensic investigation of smartphone cloud storage applications," *NUST Journal of Engineering Sciences*, vol. 10, no. 1, pp. 30–36, 2017.
- [49] N. Al Mutawa, I. Baggili, and A. Marrington, "Forensic analysis of social networking applications on mobile devices," *Digital Investigation*, vol. 9, pp. S24–S33, 2012.
- [50] Y. C. Tso, S. J. Wang, C. T. Huang, and W. J. Wang, "iPhone social networking for evidence investigations using iTunes forensics," in *Proceedings of the 6th International Conference on Ubiquitous information management and Communication*, ACM, p. 62, 2012.

- [51] V. V. Rao and A. Chakravarthy, "Forensic analysis of android mobile devices," in *2016 International Conference on Recent Advances and Innovations in Engineering (ICRAIE)*, pp. 1–6, IEEE, 2016.
- [52] S. Schrittwieser, P. Frühwirt, P. Kieseberg et al., *Guess Who's Texting You? Evaluating the Security of Smartphone Messaging Applications*, NDSS Citeseer, 2012.
- [53] V. Jain, D. R. Sahu, and D. S. Tomar, "Evidence gathering of LINE messenger on iPhones," *International Journal For Innovative Engineering and Management*, vol. 4, no. 2, pp. 1–9, 2015.
- [54] I. Riadi, Sunardi, and A. Firdonsyah, "Forensic investigation technique on Android's BlackBerry Messenger using NIST framework," *International Journal of Cyber-Security and Digital Forensics*, vol. 6, no. 4, pp. 198–205, 2017.
- [55] M. K. Tri, I. Riadi, and Y. Prayudi, "Forensics acquisition and analysis ethod of IMO messenger," *International Journal of Computer Applications*, vol. 179, pp. 9–14, 2018.
- [56] A. Azfar, K. K. R. Choo, and L. Liu, "An Android social app forensics adversary model," in *2016 49th Hawaii International Conference on System Sciences (HICSS)*, pp. 5597–5606, IEEE, 2016.
- [57] C. Wu, C. Vance, R. Boggs, and T. Fenger, *Forensic Analysis of Data Transience Applications in iOS and Android*, Marshall Forensic Science, 2013.
- [58] DB Browser for SQLite, *Sqlitebrowserorg* August 2019 <https://sqlitebrowser.org/>.
- [59] Tencent, *Tencentcom* August 2019 <https://www.tencent.com/en-us/>.
- [60] "SQLCipher-Zetetic," August 2019 <https://www.zetetic.net/sqlcipher/>.
- [61] ppwwyyxx, "wechat-dump," 2018, September 2019 <https://github.com/ppwwyyxx/wechat-dump>.
- [62] F. Darus, *How to Decrypt WeChat EnMicroMsg.db Database? Forensic Focus*, 2014, <https://www.forensicfocus.com/articles/decrypt-wechat-enmicromsgdb-database/>.
- [63] S. Wu, Y. Zhang, X. Wang, X. Xiong, and L. Du, "Forensic analysis of WeChat on Android smartphones," *Digital Investigation*, vol. 21, pp. 3–10, 2017.
- [64] Z. Dai, Sufatrio, T. W. Chua, D. K. Balakrishnan, and V. L. Thing, *Chat-App Decryption Key Extraction through Information Flow Analysis*, IOS Press, 2017.
- [65] H. Md and M. Warnier, *Cyber Crime in Privately Held Information Systems: Personal Data at Stake*, IEEE, 2014.
- [66] Z. Whittaker, *Wickr Technical White Paper*, 2019, September 2019 <https://www.documentcloud.org/documents/3461863-Wickrtechnical-white-paper.html>.