Received: 14 November 2019 | Revised: 6 July 2020 | Accepted: 16 July 2020 | Published on: 20 August 2020

DOI: 10.1002/spy2.128



RESEARCH ARTICLE

WILEY

# Examining artifacts generated by setting Facebook Messenger as a default SMS application on Android: Implication for personal data privacy

**Morris Ntonja**[1] | **Moses Ashawa**[2]

[1]Ministry of Interior and Coordination of National Government, Mombasa, Kenya

[2]Centre for Electronic Warfare, Information and Cyber, Cranfield University, Shrivenham, UK

**Correspondence**
Moses Ashawa, Centre for Electronic Warefare Information and Cyber, Cranfield University, Shrivenham, SN6 8LA UK.
Email: m.ashawa@cranfield.ac.uk

**Abstract**

The use of mobile devices and social media applications in organized crime is increasingly increasing. Facebook Messenger is the most popular social media applications used globally. Unprecedented time is spent by many interacting globally with known and unknown individuals using Facebook. During their interaction, personal information is uploaded. Thus, crafting a myriad of privacy trepidation to users. While there are researches performed on the forensic artifacts' extraction from Facebook, no research is conducted on setting Facebook Messenger applications as a default messaging application on Android. Two Android mobile devices were used for data generation and Facebook Messenger account was created. Disc imaging and data partition were examined and accessed to identify changes in the orca database of the application package using DB browser. The data were then generated using unique words which were used for conducting key searches. The research discovered that mqtt_log_event0.txt of the Com.Facebook.orca/Cache directory stores chat when messenger is set as a default messaging app. The research finding shows that chats are recorded under messages tab together with SMS of data/data/com.facebook.orca/databases/smstakeover_db and data/data/com.facebook.orca/databases/threads_db. This indicates that only smstakeover_db stores SMS messaging information when using messenger application. It is observed that once the user deletes a sent SMS message, the phone number and the deleted time stamp remained in the data/data/com.facebook.orca/databases/smstakeover_db database in the address_table are recoverable. The results suggest that anonymization of data is essential if Facebook chats are to be shared for further research into social media content.

**KEYWORDS**

database, default SMS application, Facebook Messenger, SMS take over, third-party application, timestamp

# 1 | INTRODUCTION

Without any iota of doubt, smartphones have resulted in a variety of free or low-cost social media and instant messaging applications. Due to the convenience, broad reach, affordability, and anonymity status attached some of these platforms; many criminals tend to utilize them to pursue their activities since they find them as most "secure". Indeed, many government security agencies across the world have blamed them for facilitating criminal activities. For example, in Europe, it has been blamed as a platform that facilitates terrorist propaganda, hate speech, child sexual exploitation, copyright breaches, and financial scams.[1] One significant criminal activity affecting national security in many countries across the world is terrorism which is influenced by instant messaging applications. Instant messaging software such as Fetion, Skype Messenger, Facebook Instant Messenger, Yahoo Messenger, eBuddy, and WhatsApp Instant Messaging are the most popular and commonly used IM applications.[38,39] A research paper authored by Avis[2] indicated that criminals and violent extremists could use social media applications as a platform for; information exchange, carrying out recruitment and training, planning attacks, conducting fundraising, and spreading of terrorist's propaganda in developing countries. Kenya being a developing country has indeed experienced some occurrences where terrorists have orchestrated their activities through social media applications. For example, during the year 2013 Westgate mall attack, Alshabaab terrorists used the Twitter application to post real-time tweets as they executed the attack.[3]

A report published by Citizen Support Mechanism (CSM) an initiative of National Counter Terrorism Centre in Kenya, which is authored by Ekumbo and Angira,[4] indicated that terrorists have continued to use social media applications to pursue their interests in Kenya and other countries including but not limited to recruitment and training personnel. According to the report, once the recruits have been identified and radicalized, they are encouraged to use encrypted messaging platforms for communication since they provide anonymity and also not easily tracked by security agents. The recruits are advised to shun the mainstream communication media such as the use of mobile networks at all cost since it is prone to interception. For instance, according to the report, investigations of three terror suspects who were arrested while on their way to join Alshabaab terror group operating in Somali revealed that they had been radicalized and recruited through Whatsapp as suicide bombers and jihadists. Following these findings, it can be suggested that the investigation of social media applications and particularly instant messenger applications is crucial for digital forensic investigators in Kenya. This research provides an overview of investigating Facebook Messenger application on the Android operating system.

Statistics on social media indicate that Facebook is the most popular social network worldwide controlling 85.14% of world social media users. Facebook also leads in UK and Kenya where it controls 81.71% and 85.43 of total mobile social media users correspondingly. The study of Martin Brinkmann in[5] wrote that Facebook would soon be phasing out Facebook mobile website (m.facebook.com) which allows Facebook users to use chat functionality in favor of Facebook Messenger application. The research of Jung et al[6] also noted that Facebook was disabling the mobile website messaging functionality to push people to use Facebook Messenger. Indeed today users cannot use Facebook mobile website to message unless they have installed Facebook messenger or are otherwise willing to switch to the Desktop view which may be slow on mobile devices. This implies that in a near future Facebook messenger could be one of the most popular mobile instant messaging applications. It could also be suggested that criminals could also exploit it as a communication avenue. A number of new features that were introduced in the Facebook messenger application in the year 2016. These features included SMS integration, Switch account, contacts syncing, and secret conversations. Existing literature on Facebook Messenger Artifacts indicated that Investigations have been done on forensic artifacts that can be recovered from the Facebook messenger. However, these investigations have not addressed the artifacts generated by setting the application as default SMS application on an android smartphones which are the most popular in the world. After considering these research gaps, the aim of this research is to determine if there are recoverable forensic artifacts generated by setting Facebook Messenger as a default SMS application on an Android 6.0.1 Marshmallow running on Samsung S5 device.

## 1.1 | Digital forensics

It is no doubt that the world is experiencing significant technological innovation and advancement particularly in the development of computing and digital devices. The tremendous growth in the usage of digital devices has led to the emergence of an exponentially growing branch of forensic science called digital forensics. The study of Raghav and Saxena[7] define digital forensics as a branch of forensic science that focuses on recovery and investigation of raw data residing in

electronic or digital devices. Arguably, this can be considered as a shallow definition as the definition misses the significant aspects of Digital forensics such as preservation, presentation, and repeatability. Digital forensics is broad and more than just recovery and investigation. Also, the research published by Palmer[8] of Digital Forensics Research Workshop (DFRW) defined Digital forensics as; "The use of scientifically derived and proven methods toward the preservation, collection, validation, identification, analysis, interpretation, documentation, and presentation of digital evidence derived from digital sources for the purpose of facilitating or furthering the reconstruction of events found to be criminal, or helping to anticipate unauthorized actions shown to be disruptive to planned operation". Palmer definition can be considered as the most definitive as it includes all the aspects of digital forensics. Digital Forensics is about the application of repeatable forensically sound scientific methods. The underlined principle is that the original evidence must be preserved.

Significantly, Pollitt[9] points out that digital forensics has grown over the years along with the fast development of computers and variety of other digital devices. As a result, digital forensics has progressed to create other branches based on the kind of digital device being investigated. For example, there are branches like computer forensics where computers are involved, network forensics where network evidence is required and mobile forensics where mobile phones are being forensically examined and many other areas of specialities. According to Kamvar and Baluja and Thulin and Velhelmson,[10,11] these specialities are widely applied in the investigation of digital crime incidents. Pointedly, the author notes that mobile phones are often considered to be more private than a computer; therefore, they are very vital in forensic investigations. What is more, as they are frequently encountered in most criminal cases, mobile forensics comes as a fundamental field of digital forensics.

Mobile forensics can be defined as a branch of digital forensics using a set of scientific methodologies in extracting, analyzing, and presenting digital evidence from mobile devices in a legal context[12] while the forensically sound procedure is widely used to show the validity of the evidence in digital forensics community, this may not always be easy in mobile forensics. According to National Cybersecurity University,[13] this is because some mobile forensic tools require a communication vector with the mobile phone hence a standard write blocking during extraction is not possible. What is more, other mobile extraction methods may involve installing a bootloader or removing the chip from the mobile phone before the extraction process. Nonetheless, in instances where extraction is not possible without altering the settings of the mobile phone, proper procedures must be followed and the method used and changes observed must be tested, validated, and adequately documented for evidence to be admissible in court(ibid). According to Lohrmann,[14] the ever-evolving mobile phone industry has resulted in the development of smartphones that are as powerful as personal computers. The author argues that in near future smartphones will probably replace computers. Indeed, in the modern world, smartphones have become repositories of sensitive data as they are being used to perform a variety of tasks such as calling, messaging, and geolocation, emailing, and banking transactions among many other tasks. Variety of artifacts can be recovered from mobile phones including SMS, Call history, Web browser history, MMS, multimedia files, documents, deleted data, address book, E-Mail, GPS locations, calendar, and social networking applications data.[15]

Facebook Messenger is an instant messaging application that allows users to share messages, videos, photos, location, create group chats, play games, and send money using debit card details.[16] The study of[17] also noted additional more features including feature to play games among the users. Facebook Messenger was initially developed as Facebook chat extension to the Facebook application website in the year 2008. In the year 2011, Facebook chat was revamped to a standalone application for android and IOS devices called Facebook Messenger.[18] Facebook Messenger has become second most popular third-party mobile messaging application, which is widely used to share text messages, videos, locations, photos, audios, and also in making VOIP calls between different users.[19] Variety of user information valuable to forensic investigators can be retrieved from the application using different examination techniques and tools. These artifacts could range from locations, debit card details, phone numbers, photos, time stamps, and sender and recipient details.

## 1.2 | Mobile forensics processes

The research of Raghav and Saxena[7] notes that mobile phones have become dynamic systems that pose numerous challenges to digital forensic examiners. Furthermore, he points out that the rapid increase of variety of mobile phones from different manufacturers has made it challenging for the digital forensic community to develop a single process or a tool to examine all mobile phones as each investigation is distinct. Even so, William[18] has presented a general mobile forensics approach that is broken down into five phases as shown in Figure 1.

The study of William[18] mentions that this phase begins after the examination request is made and it involves preparation of paperwork and forms required for: chain of custody documentation, device owner information, device model,

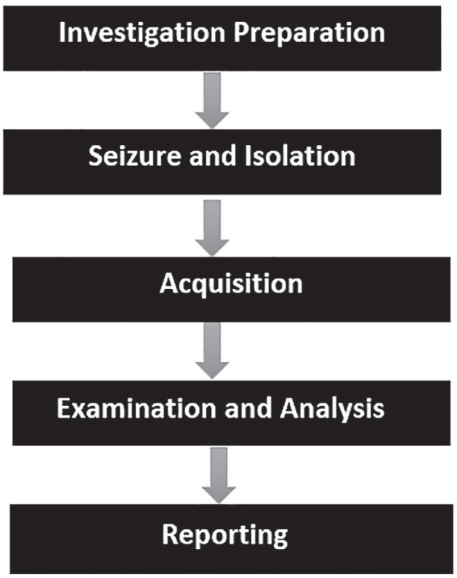



**FIGURE 1** Phases in mobile forensics[18]

device IMEI number, carrier and the associated number, nature of the incident the device was involved in, examination request details and so on. The study of Murphy et al[20] also identifies other critical elements and considerations related to the mobile phone examination in this phase such as removable and external storage devices as well as other potential sources of evidence like biological evidence and fingerprints.[7] Highlight that preparation phases can also involve research on the mobile phone based on its model, operating system, version, and identification of suitable procedures and tools to be used.

The research of Cynthia and Murphy[20] describes this phase as a critical phase that requires careful steps in ensuring evidence preservation. The study of Dogan and Akbal[21] notes two challenges that forensic examiners face while seizing mobile phone for examination. First, he noted that investigators face the challenge of the potential risk of evidence modification as mobile phones are networked devices. According to the author, mobile phones can communicate through Bluetooth, WFI, and Telecommunication systems. Therefore, when a mobile phone is seized at a crime scene and is switched off, it is imperative that the investigator place it in Faraday bag to avoid the evidence change in case the device powers on automatically. Faraday bags are made to isolate the mobile phone from the network. Second, when a mobile phone is recovered from a crime scene and is found to be switched on and locked with a password, PIN, fingerprint, or facial recognition the examiner will be required to bypass the lock. This phase links to the acquisition phase which involves the extraction of data from the device. Acquisition method is determined depending on device make, model, and installed operating system. It is crucial that acquisition be done using a tested method which is forensically sound and repeatable.

The examination and analysis process employs the use various software tools to extract data of interest from the acquired image or files. Significantly, as no single tool can parse all the data from the mobile phone, it is vital that the examiner have sound knowledge of file systems structures to recover all the data that tools cannot process. According to Domingues et al,[22] this phase is followed by verification process to determine the accuracy of the acquired data by comparing the extracted data to the data on the mobile phone to identify any possible discrepancies. It also uses a variety of tools to compare the results to identify any differences using hash values to identify if data on the images has changed since acquisition. The reporting phase involves documentation of all processes indicating what was done during the acquisition and examination processes. The research of Ayers et al[23] pointed out that the documentation should be in form of contemporaneous notes. The investigator notes can include details such as the case background, the status of the device when received, tools used among other notable findings of the case investigation. The findings should be concise, clear, and repeatable in a manner acceptable in court. Timeline and Link analysis tools are essential in assisting investigators to establish patterns across multiple devices being investigated. After documentation and reporting the data extracted should be preserved and archived in a usable format for future references and record keeping as per jurisdiction requirements.

The following contributions are made by this article:

- This article identified both qualitative and quantitative artifacts as potential evidence when Facebook Messenger as an instant messaging (IM) application is set as a default messaging application and their potential impacts on social

media. The metadata obtained in the research can be a crucial resource of how social media texts can be collected by cyber criminals for attacks. This metadata can also be used for sociological and linguistic research.

- Forensically, our research shows that some information such as the phone number and deleted timestamp recoverable when a user deletes SMS when using messenger as a default Messaging application on Android 6.0.1. Our results showed flags that can indicate whether an Identified phone number was the one that messenger received SMS from or one that Messenger sent SMS to. It proved that it is possible to retrieve the timestamps when Messenger Send or Receives SMS. This flag indicates an SMS sent or received by the messenger has been deleted during digital forensic investigation.
- We demonstrated how virtualization using Bluestack windows application can be used in conducting Android applications research by setting Facebook Messenger as the default SMS application. To the best of our knowledge, this experiment has never been conducted elsewhere before now.

The remainder of the paper is organized as follows: Section 2 summarizes the related approaches in the literature on forensic data extraction and social media privacy issue. Section 3 describes the proposed method for setting Facebook Messenger as a default messaging applications and extracting the artifacts accordingly. The experimental design and results were provided in sections 4 and 5, respectively. A comparison with some related work was discussed in section 6 while section 7 was devoted to conclusion and future.

## 2 | RELATED WORK

### 2.1 | Forensic data extraction from instant messaging applications

A number of researchers have carried out significant studies on data extraction from messaging applications. The research of Gruschka et al[32] performed a data extraction from instant messaging applications focusing on WhatsApp and Facebook. While social medial and instant messaging applications are used for good intentions, criminals use it to perpetrate evil.[29-31] The amount of information contained by these applications can be used to address digital-related crime cases in the court of law. In the research of Chu et al[25] approach involved investigating Facebook application artifacts in windows XP computer volatile memory (RAM), browser cache files, virtual machine image, and snapshot files as well as iPhone and android file system dump. Their investigation on the two mobile devices involved logical acquisition using XRY and Oxygen forensic tools. Logical acquisition was conducted on Huawei installed with unrooted Android 2.1 and also on iPhone running iOS 4.3 which was not jail-broken. This research established artifacts such as chat messages, contacts, and photos from the Facebook application.

The study of Corcoran et al[26] conducted further investigation titled Messaging Application Analysis for Android and iOS platforms. Their investigation involved experimenting with Android smartphone HTC EVO 3D which was rooted to allow access to the operating system files. Their methodology involved resetting the phone to its factory settings to remove any previous user applications and then acquiring both physical and logical images of the smartphone when the applications were not installed. The phone was then installed with seven applications among them Facebook Messenger and then the image was acquired. The final step involved generating applications data and then acquiring the image which was analyzed to identify application artifacts. Results from the artifact analysis indicated that they found chat conversations, locations, and contacts. However, they did not explain the locations from which they recovered these artifacts. Furthermore, their research was based on Android 4.0.3 Ice Cream Sandwich as well as older version of Facebook Messenger and did not properly focus on all the artifacts that can be retrieved from the Facebook Messenger. Besides, their research appears to have been outdated as the current Facebook Messenger version has new settings and features (Figure A1).

### 2.2 | Social media and data privacy issue

Data privacy in relation to how data is shared with the third party is becoming a big challenge in data protection.[32-35] During social media registration, a lot of users' data is collected ranging from name to date of birth, even location. This data can be exploited for negative when accessed by cybercriminals. On documenting Facebook privacy data, the study

of Tahiri[27] published investigation involved the installation of Facebook Messenger on rooted Samsung Galaxy J1 phone. Logical acquisition on Facebook Messenger files was performed using ADB pull command and files were analyzed using SQLite Browser. The result showed that some of the user's data were accessed by a third party.

Investing open data challenges at Facebook, the research of Bronson et al[36] identified how the application stores huge volume of artifacts which can be relied upon during investigation. The electronic evidence contains hash codes that link to data identification.[37] Credibility of electronic evidence in relation to data associated with social media applications can be verified. Evidence that are modified can also be used to extend further forensic investigations.

# 3 | METHODOLOGY

## 3.1 | Research question

A number of new features of interest to digital forensics community on Facebook Messenger were implemented in the year 2016. None of the existing researches on Facebook Messenger has addressed the implications of these new features to mobile forensic investigations. After considering these features, the following research question was formulated.

"Are there recoverable artifacts generated by setting Facebook Messenger as a default SMS application on Android 6.0.1 Marshmallow running on Samsung S5 device?"

To answer the research question above, the following research objectives were set:

1. Establish changes that could indicate that messenger has been enabled as a default SMS application in Android and how its records Chat and SMS messages in its user interface. Facebook Messenger was set as a default SMS application and changes that occur to its relevant application package files were noted in comparison with the control experiment. Furthermore, SMS and normal chat conversation were tested to examine how they are recorded in both messenger app and its relevant databases.
2. Identify artifacts left when messenger receives SMS when set as a default Messaging application. To achieve this objective, a clean Messenger application was set to receive SMS from four different mobile network numbers to have much data to populate the databases. SMS deletion was also considered. The messenger databases of interest were then compared with the control experiment.
3. Identify SMS artifacts left when a user disables Messenger as a default messaging application. To achieve this objective, the relevant application databases will be examined to determine if they have any traces of artifacts that can be recovered once the application is disabled as a default SMS client and the user has logged out. Does disabling erase all the User activity data if any?

## 3.2 | Resources

This research could be carried out using variety of devices and would involve experimentation with a number of both high-end and low-end mobile phones which would require a substantial financial implication. Furthermore, the project would involve establishing how the Facebook Messenger application behaves in all the Android versions. While this is not possible due to a fixed budget, one or two mobile devices were selected for experimentation and virtualization was used as an alternative to more devices where needed. A forensic workstation running Windows 10 having memory of 8 GB and core i5 processor was used for extraction and analysis of the experimental data. The workstation had a good processing capacity to allow running of required tools. Tools and devices used for the experiment are listed in Tables 1 and 2, respectively. These tools are both mobile forensic and non-mobile forensic tools and will be used for extraction and analysis of the experimental data. The list of tools and experimental devices used in this work are listed in Tables 1 and 2, respectively.

# 4 | EXPERIMENTATION

The workstation was set-up using a Windows 10 Enterprise Compaq Desktop computer with Intel Core i5 processor and 4 GB RAM, respectively. The workstation was installed with up to date versions of the selected tools (Table 1). Preliminary

**TABLE 1** List of used tools

| Hardware/Software | Version |
|---|---|
| Android SDK | 27.0.1 |
| *Windows ADB* | Adb 1.0.40, |
| *XRY* | 7.6 |
| *DB Browser for SQLite* | 3.10.1 |
| *Odin* | 3.12.7 |
| SuperSSu by Chainfire | 3.13.4 |
| Windows Powershell | PS 5.1.17134 |
| *Bluestacks* | 4 |
| *WinHex* | 18.5 |
| FTK Imager | 3.1.1.8 |

**TABLE 2** Devices used for the experiment

| Device | OS | Operator |
|---|---|---|
| Samsung S5 | Android | Not applicable |
| Nexus 4 | Android | Not applicable |
| 5 SIM cards | Not applicable | giffgaff |
| Samsung USB cable | Magnetic Moment | Not applicable |
| Facebook messenger | Not applicable | Not applicable |

experiments were performed to determine the nature of default Android applications using Bluestack before the actual experimentation was carried out using Android smartphone. In the experimental setup, LG Nexus 4 Android 5.1.1 and Samsung Galaxy S5 Model SM-G900F running Android version 6.0.1 Marshmallow was the two mobile devices used for the experiment. The devices were installed with Facebook Messenger application version 181.0.0.12.78 within the experimentation period from o6 September 2018 and. The experimental setup summarized as shown in Figure 2. LG Nexus 4 running Android 5.1.1 Lollipop was used for data generation. This device is solely used for data generation and was not extracted. Samsung Galaxy S5 Model SM-G900F running Android version 6.0.1 Marshmallow was extracted after data generation using ADB and XRY for validation of the results. Four SIM cards were used to generate data in LG Nexus 4 Android 5.1.1 device. The reason for using the four SIM is to have much data to populate the Facebook Messenger databases.

During the preliminary experiment, the **Data_0.vdi** image which contained the Android file hierarchy containing cache, data, local, and misc partitions were extracted. We then performed another preliminary experiment to determine the nature of Android Facebook Messenger application files in the **Data.vdi.** Examination on **Data.vdi** and **Data_0.vdi** indicated the images contain EXT4 android file system with an MBR partitioning style containing **com.facebook.orca** database with smstakeover_db. The two preliminary experiments have provided an overview of location of Facebook Messenger files. Facebook Messenger version 181.0.0.12.78 was downloaded from play store and configured as default SMS App to ensure that the messenger uses same configuration during data generation. To prevent autoupdate of the Facebook Messenger during data generation and extraction, the auto-update service was disabled throughout the entire experimentation process. During data extraction process, different command from the power shell was executed to list the connected devices, to start the connected devices, to switch to root user, and then navigate to data partition which stores Facebook Messenger application data in a package named **com.facebook.orca** respectively. The **-ls -l** command was then executed to recursively list the content of the data partition. Command **ls -l | grep com.facebook.orca** was executed to only view the details of the Facebook Messenger package. The messenger application on Samsung Galaxy S5 was accessed and was used to initiate SMS conversation with LG Nexus 4. Samsung Galaxy s5 was put to flight mode and restarted to allow messenger application package to be extracted. Messenger data was then extracted using the ADB tool commands.

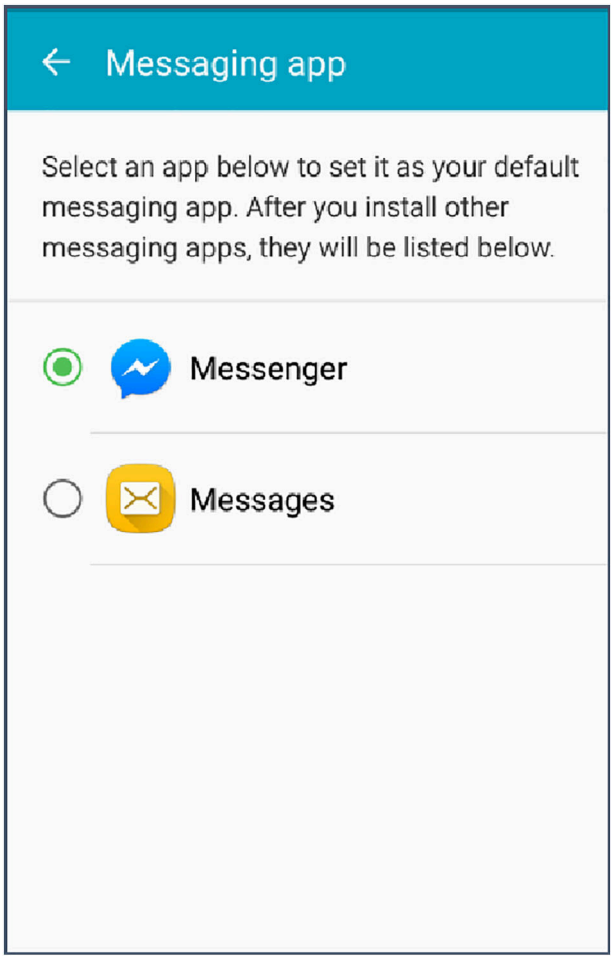



**FIGURE 2** Configuring third-party app as a Default SMS App

The SIM card in Samsung S5 was maintained throughout the experiments and it was not changed to ensure consistency of the experimental data. All the SIM cards have unique subscriber number which will be useful in conducting keyword search during analysis. The Gmail accounts have been set up using one of the researchers' name mixed with numbers which are unique to each email. This was useful during keyword searching of all used emails. The Facebook Messenger was thereafter activated by first registering dummy Facebook accounts and then activating messenger accounts using the registered email on Facebook. The same credentials were used as set up for Facebook Messenger using login by Facebook option. This option was considered because it gives more user anonymity as opposed to using mobile number to register the messenger account. In addition, most mobile website Facebook users will need to register on messenger to send and read messages from their friends. Furthermore, criminals will make dummy Facebook accounts using dummy emails and use them to login to messenger hence maintaining their anonymity status. Three dummy Facebook Messenger contacts were created to be used as friends and also to be used to login to Messenger application for user data generation as seen in Table 3.

## 4.1 | Preliminary experiment A

The focus of this experiment was to determine the nature of default android applications using Bluestack Emulator before actual experimentation using an Android smartphone. Bluestack Emulator was setup on the workstation were the Gmail account was registered. A Gmail account was particularly registered for this purpose as there was no consideration for any analysis the Gmail account used was given the researcher's name. Android folder from Engine directory was exported to Preliminary Experiment 1 directory on the workstation Desktop for analysis using Winhex. The image was examined for main Android system partitions. The main Android partitions such as cache, data, local, and misc were present. Data partition was accessed to identify the default preinstalled applications.

**TABLE 3** Facebook messenger account set-up and SIM cards details

| **LG Nexus 4** | | **Samsung S5** | |
|---|---|---|---|
| Device Information | LG Nexus 4 Android 5.1.1 Lollipop | Device Information | Samsung Galaxy S5 Model SM-G900F running Android version 6.0.1 Marshmallow. |
| Google play account | Email: ashwa.mos940@gmail.com | Google play account | Email: ashwa.mos940@gmail.com |
| Messenger Account | Login by Facebook option: Email: morrisn402@gmail.com | | Login by Facebook option: Email: morriston940@gmail.com |
| SIM Numbers used | 07803097096<br>07803097100<br>07751577520<br>07749068990 | SIM Number used: | 07753462734 |

### 4.1.1 | Preliminary experiment B

During this experiment, Facebook Messenger account was created when there was no user activity generated. Android folder from Engine directory was exported to Preliminary Experiment 2 directory on the workstation Desktop for analysis using Winhex. Two Virtual Disk Image (VDI) images; **Data.vdi** and **Data_0.vdi** were opened in their respective order as they were differencing virtual hard disks to read a differencing VMDK/VHD/VDI image. The image was examined for main Android file system partitions and to identify the change after installation of Facebook Messenger. Data partition (/data) was accessed to identify the change in android application packages after the installation of Facebook Messenger account. DB browser for SQLite was used to access data/com.facebook.orca/databases.

The database directory was observed to contain SQLite databases which are important for this research as they hold all the application user data. For this research, **smstakeover_db** will be Key as the experiments will be conducted to establish if it stores any forensically important artifacts. However, other databases will be analyzed for variety of other experimental artifacts. The two preliminary experiments have provided an overview of the location of Facebook Messenger files. The preliminary experiment 2 has formed a foundation for experimentation phase of this research. Secondly, the experiment has established Facebook Messenger application database files. The experiment has shown that indeed there exists a database file **smstakeover_db** that has potential of storing SMS evidence.

### 4.1.2 | Configuration of Facebook Messenger as a default SMS App and data generation

As explained in the experimentation section, Facebook Messenger in both Nexus 4 and Samsung s5 device Facebook Messenger was configured as default Messaging application. This was to ensure that messenger uses same configuration during data generation. To prevent autoupdate of the Facebook Messenger application during data generation and extraction, the application autoupdate was disabled throughout the entire experimentation process.

The data was generated on Samsung Galaxy S5 using Nexus 4 phone by enabling device rooting. In the forensic workstation, PowerShell was enabled to location of portable adb tool (**PS C:\platform-tools_r28.0.1-windows\platform-tools>**) by connecting the rooted devices using micro-USB cable to the workstation. The connected devices were listed by executing the PowerShell command. /**adb.exe shell.** We then switched to the root user to enable access to the Facebook Messenger data partition.

To ignore other partitions and concentrate to view only the Facebook Messenger packages, **ls -l | grep com.facebook.orca** command was executed. The entire com.facebook.orca package contents to the experiments directory in the workstation was then copied by navigating to the **PS C:\platform-tools_r28.0.1-**

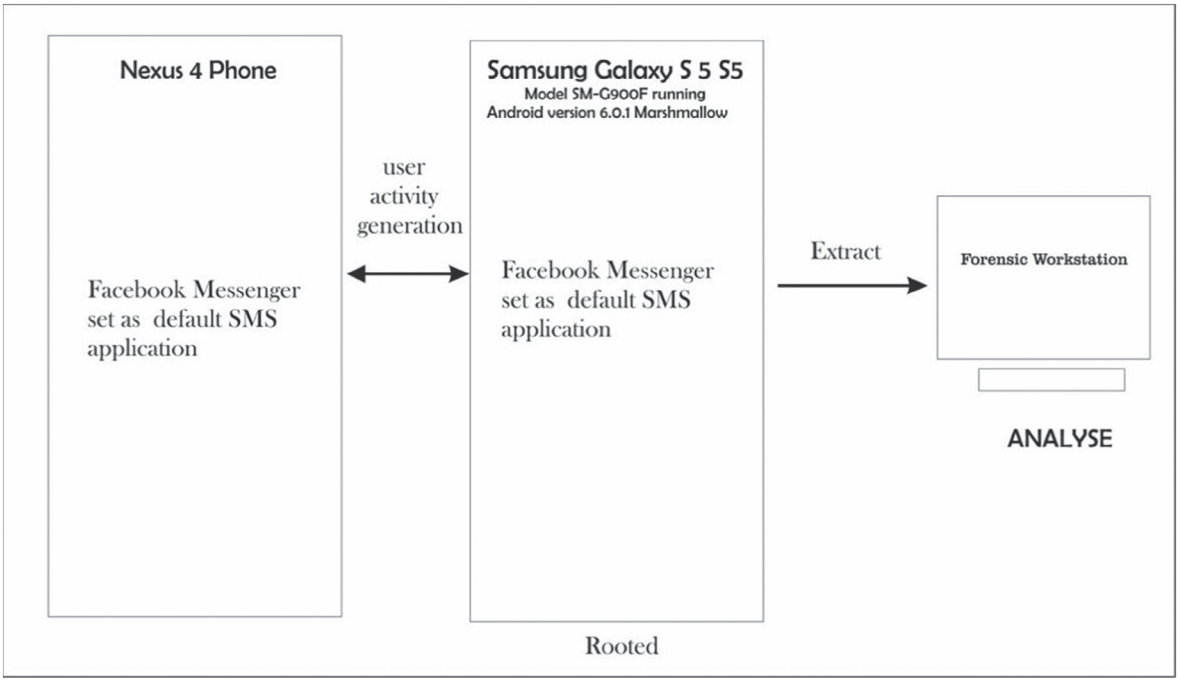



**FIGURE 3** Summary of the Experimental setup and flow

**windows\platform-tools> and** execute command **/.adb.exe pull /storage/0403-0201/com.facebook.orca/ /Desktop/Experiments** (Figure 3).

## 4.2 | Control experiment

The focus of the control experiment was to generate a clear messenger package contents with empty databases that would serve as a comparative basis during analysis for other experiments containing user data. During this experiment, the used devices were reset to factory settings to clear any existing user data. The USB debugging mode was then activated, and the devices were rooted respectively. Facebook Messenger version 181.0.0.12.78 was installed and accessed using the registered user credentials as shown in Table 3. At this stage, no user data was generated. The devices were connected to the forensic workstation using micro-USB cable for extraction using the ADB tool. The rest of the approach for data generation were same as those in the preliminary experiments (Figure A2).

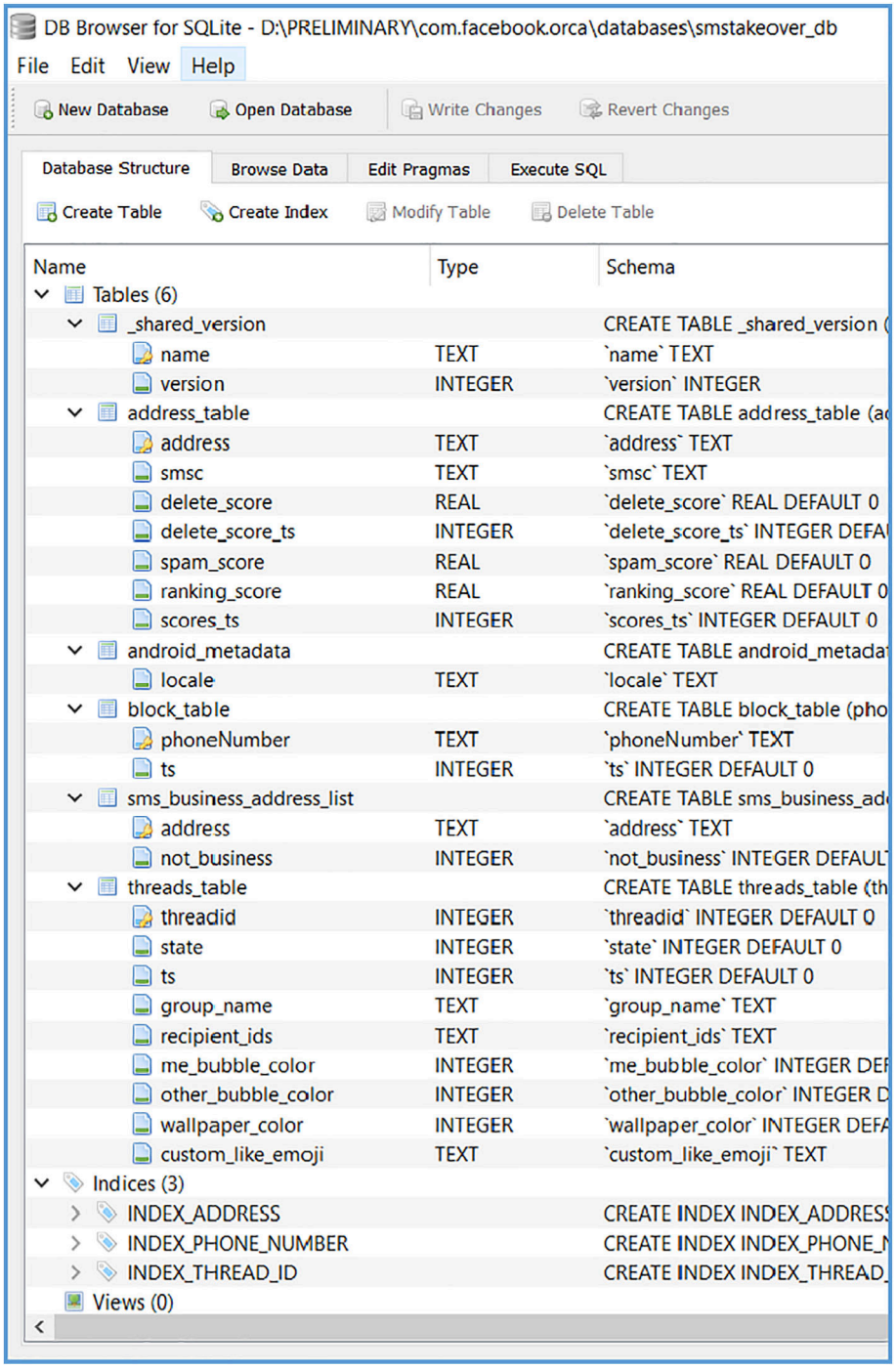
### 4.2.1 | Data generation

User data was generated by the use of animal and their baby names in this format (animalname-babyname). The generated unique words were used in conducting keyword searches during data analysis. Although Samsung S5 Device was used as set up in Control experiment, additional setting of enabling Messenger as a default messaging app was introduced by enabling the USB debugging mode. The Samsung Galaxy S5 was rooted and set up with SIM card (0775****734) and SD card. The Facebook **smstakeover_db** database was extracted using DB Browser for SQLite (Figure 4).

To determine messages sent from Galaxy S5 to different contacts, the devices were accessed to send SMS Messages to four numbers. The following is a list of Messages sent:

07749068990:12/09/2018| 14:30 **Hamster-pup.**
07803097096:12/09/2018| 14:32 **Hippopotamus-calf.**
07803097100:12/09/2018| 14:38 **Kangaroo-joey.**
07751577520:12/09/2018| 14:39 **Hare-leveret.**

**FIGURE 4** Structure of smstakeover_db database




The device was then set to flight mode to isolate it from its environment. After engaging with on SMS conversation with contacts, Galaxy s5 was disabled as default MP. The messenger application on LG Nexus 4 was accessed and was used to initiate SMS conversation with Samsung Galaxy S5. XRY was then used to complete the logical extraction. The results obtained are discussed in the next section.

## 5 | RESULTS AND DISCUSSION

Analysis on cache folder indicated the following contents of Com.facebook.orca/Cache as extracted using FTK Imager. Com.facebook.orca/Cache contains com.facebook.orca/cache/notification_log_event0.txt. This

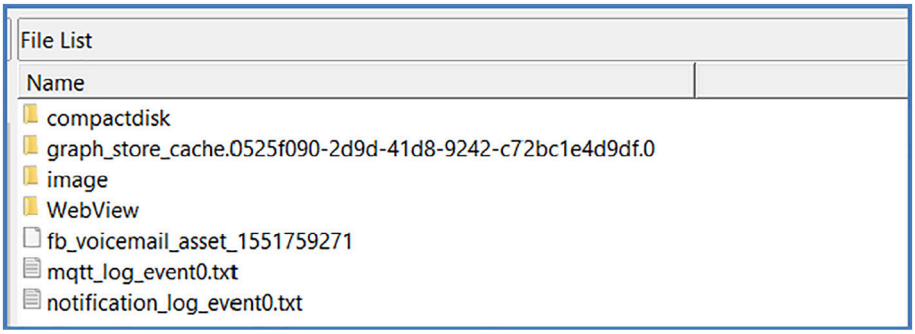



**FIGURE 5** Content of com.facebook.orca/Cache

text log file contains application messaging events with a message request snippet Fetcher. Examination on com.facebook.orca/databases indicated two SMS databases of interest to the research. These were com.facebook.orca/databases/smstakeover_db and com.facebook.orca/databases/smstakeover_db-journal respectively. Examination on com.facebook.orca/databases/smstakeover_db indicated that the database contained six tables as shown in Figure 5; while **com.facebook.orca/databases/smstakeover_db-journal** was encrypted and could not be opened using DB Browser for SQlite.

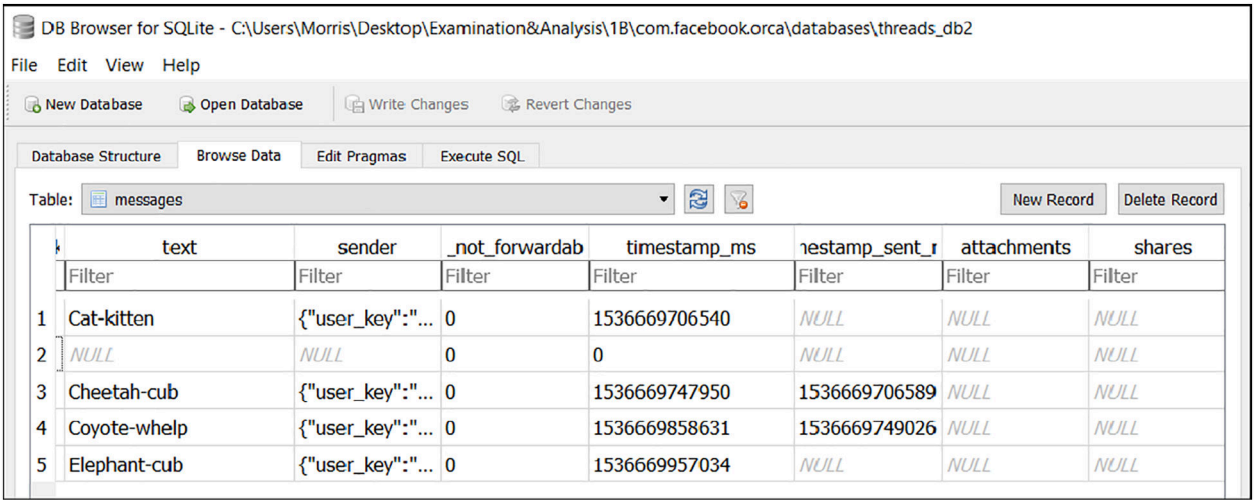
## 5.1 | Facebook Messenger' records in the interface

Examination on the messenger home screen indicated the chat messages are recorded under messages tab together with SMS. The SMS conversation indicated a purple theme icon attached to the profile picture. The purple color of this icon did not appear to change despite the customization of SMS colors by the user. On the other hand, normal chat messages indicated white color theme and the colors cannot be customized by the user. Due to the prior literature knowledge that **com.facebook.orca/databses/threads_db** stores chat messages; it was important to examine this database to identify if it has any evidence of SMS conversation. Analysis of this database indicated that the messages table was populated with only chat messages with timestamps stored in Unixepoch format as shown in Figure 6; storing SMS messages recorded in this database. Both SMS and messenger normal chat conversations are recorded under messages tab. The SMS conversations are identified by a purple theme small icon attached to the main profile picture. The purple color of this icon did not appear to change despite the customization of SMS colors by the researcher. Normal chat message conversations do not have the purple theme small icon attached to the main profile picture. Therefore, using this difference, investigators can easily tell when messenger has been used for SMS messaging. However, this is possible only when the user has not deleted the SMS messages in the .orca database.

Analysis of data/data/com.facebook.orca/databases/smstakeover_db and data/data/com.facebook.orca/databases/threads_db indicates that only smstakeover_db stores SMS messaging information when using messenger application. Examination and comparison were only done on the data/data/com.facebook.orca/ cache folder and there were no search queries conducted on the identified threads_db and smstakeover_db databases since their comparison was adequate answer to the intended research objective. This research set precedence for investigation of Facebook Messenger application when set as a default SMS application in Smartphones running Android operating system. While the objective of this research was adequately achieved, there are some areas of this thesis as well as other potential related areas that would require further investigation. Further research can be carried on examining com.facebook.orca/app_gatekeepers, the smstakeover_db Database rollback journal (smstakeover_db-journal).

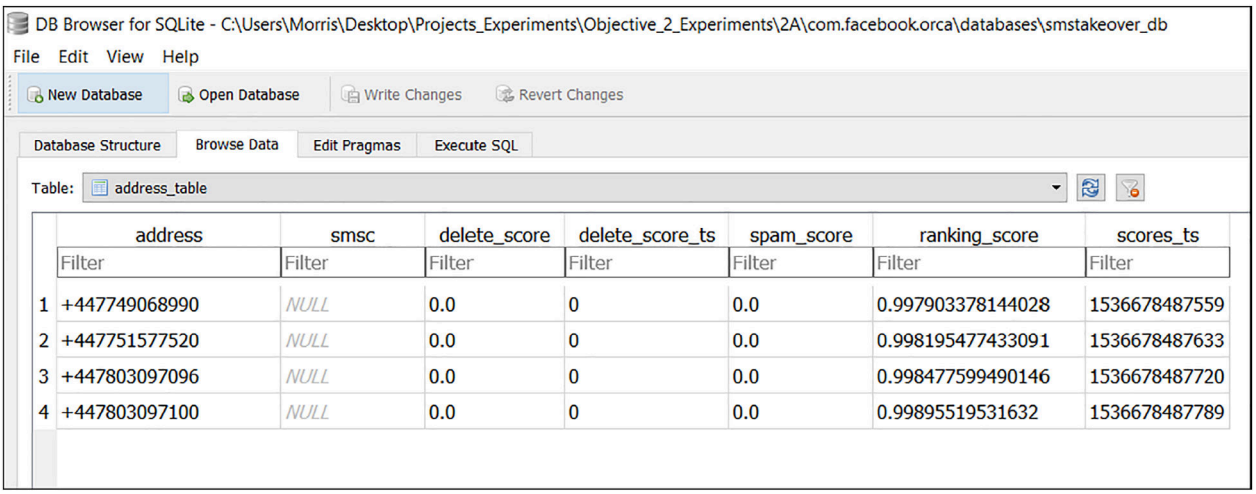
## 5.2 | Messenger set as a default messaging application

During the examination of the databases, it was noted that the smstakeover_db was populated with some data from the received SMS. For the experiments, the messenger smstakeover_db was analyzed then compared with the control experiment and the preceding experiments to identify any evidentiary trails left when it is used to receive SMS. Since




| | text | sender | _not_forwardab | timestamp_ms | nestamp_sent_r | attachments | shares |
|---|---|---|---|---|---|---|---|
| | Filter | Filter | Filter | Filter | Filter | Filter | Filter |
| 1 | Cat-kitten | {"user_key":"... | 0 | 1536669706540 | NULL | NULL | NULL |
| 2 | NULL | NULL | 0 | 0 | NULL | NULL | NULL |
| 3 | Cheetah-cub | {"user_key":"... | 0 | 1536669747950 | 1536669706589 | NULL | NULL |
| 4 | Coyote-whelp | {"user_key":"... | 0 | 1536669858631 | 1536669749026 | NULL | NULL |
| 5 | Elephant-cub | {"user_key":"... | 0 | 1536669957034 | NULL | NULL | NULL |

**FIGURE 6** Messages stored as text in /data/data/com.facebook.orca/databases/threads_db




| | address | smsc | delete_score | delete_score_ts | spam_score | ranking_score | scores_ts |
|---|---|---|---|---|---|---|---|
| | Filter | Filter | Filter | Filter | Filter | Filter | Filter |
| 1 | +447749068990 | NULL | 0.0 | 0 | 0.0 | 0.997903378144028 | 1536678487559 |
| 2 | +447751577520 | NULL | 0.0 | 0 | 0.0 | 0.998195477433091 | 1536678487633 |
| 3 | +447803097096 | NULL | 0.0 | 0 | 0.0 | 0.998477599490146 | 1536678487720 |
| 4 | +447803097100 | NULL | 0.0 | 0 | 0.0 | 0.99895519531632 | 1536678487789 |

**FIGURE 7** Smstakeover_db database address_table columns using DB Browser for AQLite

the address_table was populated with data it was important to examine its columns and the nature of the data stored (Figure 7).

The scores_ts column the timestamps are stored in 13 characters non-human readable "unixepoch" format. While comparison of the smstakeover_db databases was enough to determine the artifacts left when messenger receives SMS it was also necessary to see if the scores_ts column unixepoch timestamps could indicate those of receiving time as noted during experimentation and subsequently determine if **scores_ts** column indicate time when the SMS was received. Therefore, conversion to human readable format was essential. For conversion the SQLite datetime function was used. The SQL command Select **address, scores_ts, datetime (scores_ts/1000, "unixepoch")** was run on a copy of the database; from address_table, the result of running this command can be seen in Figure 8.

Alternatively, SQL update function can be used to update the scores_ts to a human-readable format using datetime function by executing the command **Update address_table set scores_ts = datetime(scores_ts/1000, "unixepoch")**. Executing this command resulted in a change in the database since the column scores_ts was updated to human-readable format permanently and therefore was performed on a copy of the database. Both of these commands work by dividing the date by 1000 to give seconds since the 13 characters record the date in Milliseconds and then updating the scores_ts to human-readable format (Figure 9).

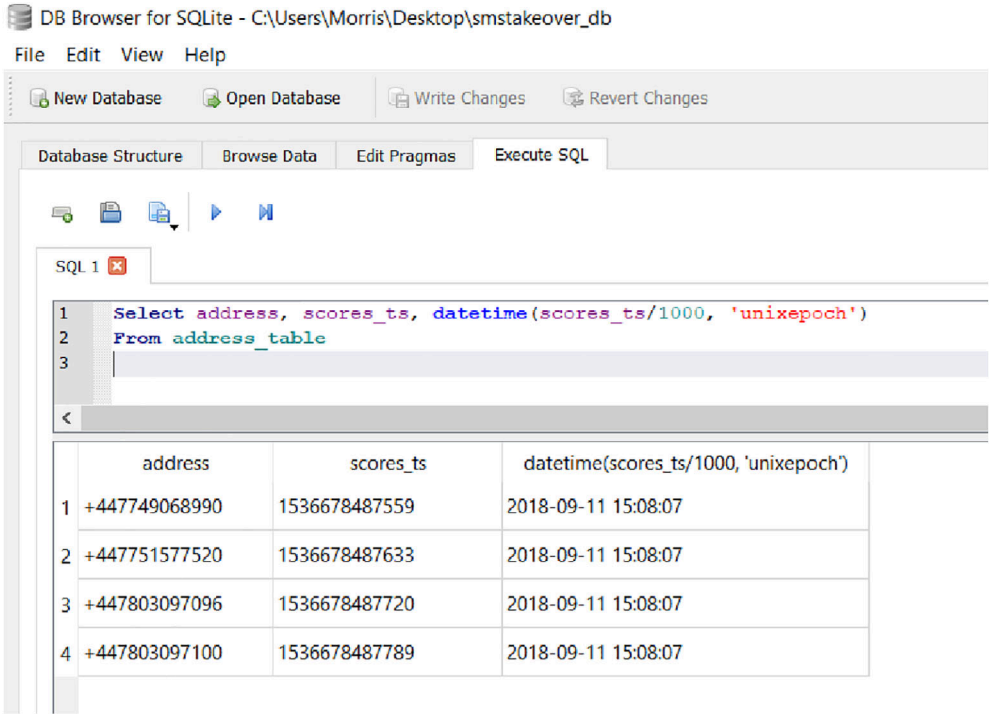



**FIGURE 8** Converting and updating the address table scores_ts column timestamps

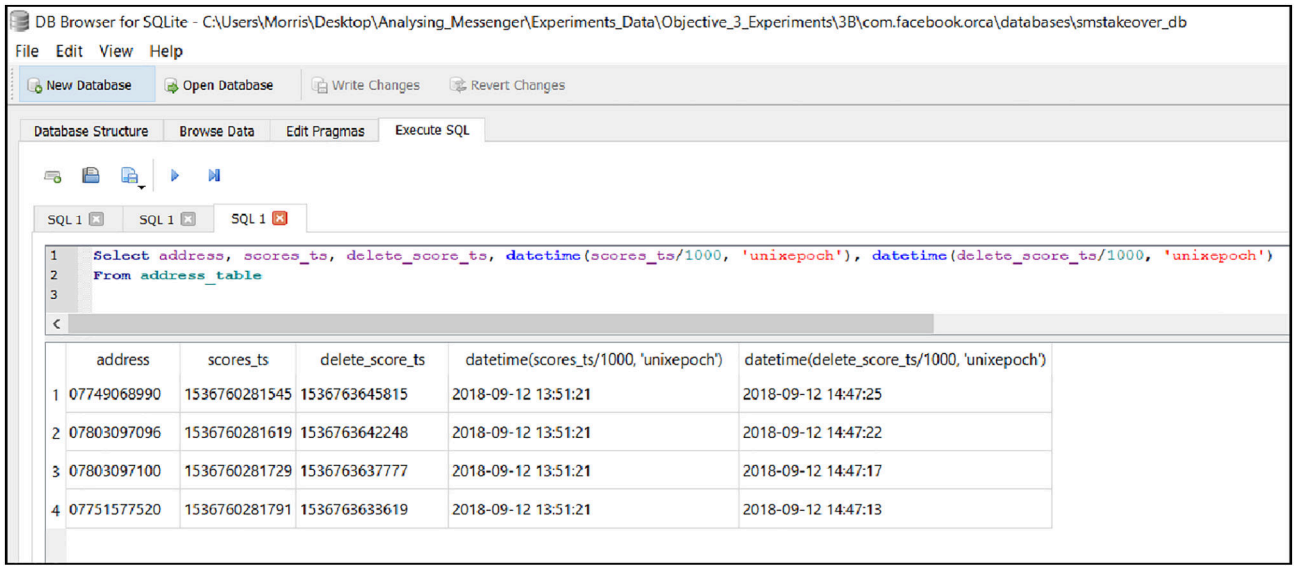



**FIGURE 9** The delete_score_ts and scores_ts are stored in UNIX epoch format

## 5.3 | Artifacts left when messenger sends SMS as a default messaging application

The result shows that it is possible to identify some artifacts related to SMS messages sent when messenger application is set as a default SMS application in android. These artifacts include; the phone number which sent the SMS, the date the SMS was sent as well as the date and time when the SMS was deleted by the user from the Messenger application. The changes observed when the SMS was deleted are recorded. It was observed that once the user deletes a sent SMS message the phone number and the deleted time stamp still remained in the data/data/com.facebook.orca/databases/smstakeover_db database in the address_table table and was recoverable. This is significant strength for examiners since the phone number was still recoverable despite the message having been deleted as seen in Figure 10.

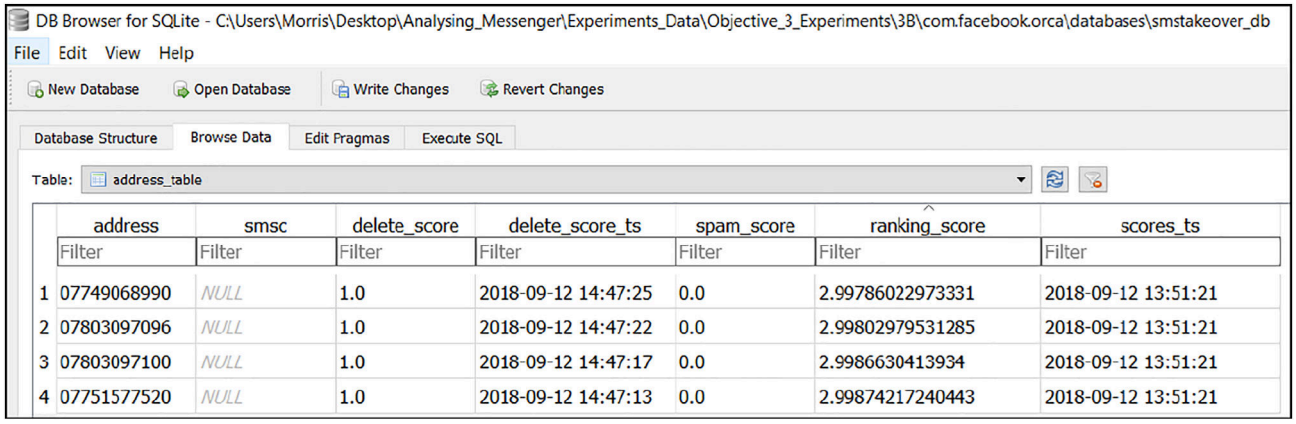



**FIGURE 10** Scores_ts and delete_scores_ts from the addres_tables

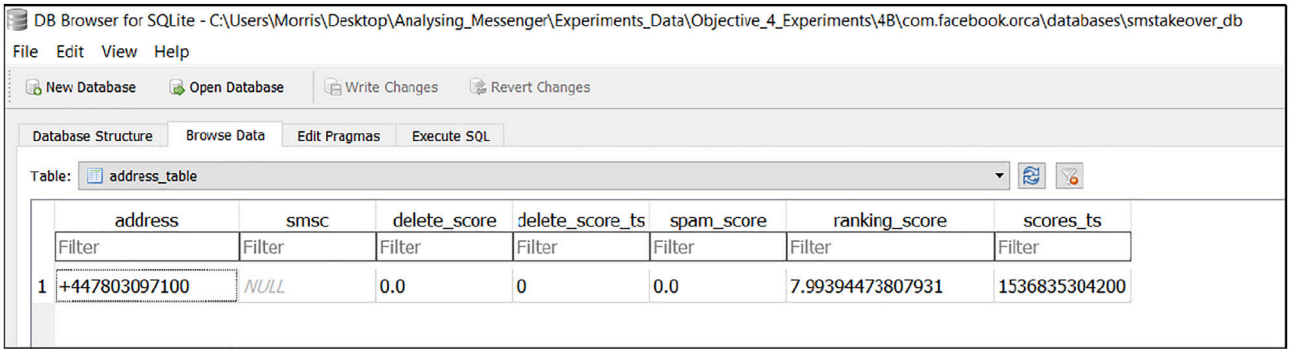



**FIGURE 11** Smstakeover_db_address_table after disabling messenger as a default messaging application

The scores_ts column in the address_table of data/data/com.facebook.orca/databases/smstakeover_db database however appeared to only give the correct date on when the SMS messages were sent. It also seemed to indicate the time as when the first SMS was sent and this time was incorrectly placed to other SMS messages sent. This implied that this timestamp was not correct and therefore should not be relied upon by the investigators. On the other hand, the delete_score_ts column timestamp conversion results shown the exact time when the sent message was deleted by the user as recorded during experimentation and therefore provided a reliable timestamp for the examiner. For the deleted sent SMS messages, the value on ranking_score column in smstakeover_db was observed to be random decimal number each starting with value 2.99. This could be used as a flag to indicate SMS sent from the messenger. However, as limitation to the research, this finding could not be validated as it would require repeated experiments to confirm this finding. While this can be appreciated as a positive finding of these experiments, it was discovered that it is not possible to recover these artifacts from the live smstakeover_db database once the user uninstalls the Messenger application.

## 5.4 | Artifacts left when a user disables messenger as a default messaging application

A major strength of the collated results of the experiments under this objective is that they showed that the user SMS data is not usually cleared when messenger is disabled as a default messaging application as seen in Figure 11.

This finding is significant as it can help investigators recover SMS data from messenger when the user has used and disabled the application as default messaging application. Analysis of smstakeover_db indicated that it contained some data regarding the SMS conversation. It was also noted that for the SMS conversations between two numbers the value on ranking_score column in smstakeover_db database (address_table) was a random decimal number each starting with value 7.99. This could be suggested as a flag for identifying contacts that have engaged in SMS conversation using messenger application.

## 6 | COMPARISON WITH SOME RELATED WORK

Facebook artifacts generation methodology proposed in Reference 24 was based on keyword search image to identity Facebook Messenger artifacts while their investigation seems outdated as at now, their research was only based on Facebook chat in computer and ignored mobile devices which are now most likely to be used in accessing chat applications. Virtualization approach in Reference 25 established artifacts such as chat messages, contacts and photos from the Facebook application through jail breaking. As proposed in Reference 26 obtained results from the artifacts analysis indicated that they found chat conversations, locations, and contacts.

However, they did not explain the locations from which they recovered these artifacts. Furthermore, their research was based on Android 4.0.3 Ice Cream Sandwich as well as older version of Facebook Messenger and did not properly focus on all the artifacts that can be retrieved from the Facebook Messenger. Besides, their research appears to have been out-dated as the current Facebook Messenger version has new settings and features. Using rooted approach as proposed in Reference 27 identified the location of Facebook Messenger artifacts in Android. Our work, however, focused on setting Facebook Messenger as a default SMS messaging application.

As noted in section one, SMS feature was announced as an optional setting that would allow Facebook Messenger users to send, receive and read their SMS and MMS from their Messenger application without having to switch to the default SMS Messages application in their Android mobile phones. As the author pointed, the objective of introducing SMS feature was to shift away messenger users from their default mobile phone Messages application and see them spend more time in the Messenger application. Derek Walter in Reference 28 claimed that the Messenger application does not save or store any of the SMS in its servers. Indeed, from the experimentation results, it has been shown that it is true that Messenger does not store any SMS in its servers.

However, from the experimentation results, it is clear that Messenger does store some of the SMS artifacts which include the phone number which SMS was sent to or was received from as well as the accompanying time stamps when Facebook Messenger has been enabled as a default messages application in Android 6.0.1. Noteworthy, these artifacts appeared to be wiped out once the user uninstalls and then reinstalls or otherwise logs out the application by clearing data and cache. This finding is important for the digital forensic community and particularly mobile forensics field since it has shown that Facebook Messenger is capable of storing some SMS artifacts and therefore should not be overlooked especially in cases when there are no recoverable SMS artifacts during mobile device examination and the device user had Facebook Messenger application installed and being active.

Due to the prior literature knowledge that **com.facebook.orca/databses/threads_db** stores messenger chat messages it was important to examine this database to identify if it has any evidence of SMS conversation. Analysis of this database indicated that the messages table was populated with only chat messages with timestamps stored in Unixepoch format as shown in Figure 6. Although both SMS and messenger normal chat conversations are recorded under messages tab, The SMS conversations are identified by a purple theme small icon attached to the main profile picture. The purple color of this icon did not appear to change despite the customization of SMS colors by the researcher. Therefore, using this difference, investigators can easily tell when messenger has been used for SMS messaging. However, this is possible only when the user has not deleted the SMS messages. Result on analysis of **data/data/com.facebook.orca/databases/smstakeover_db and data/data/com.facebook.orca/databases/threads_db** indicated that only smstakeover_db stores SMS messaging information when using messenger application. The smstakeover_db address_table constituted most of the recoverable artifacts including the phone number, the SMS deletion timestamp, and other unique data that could distinguish SMS conversations using the messenger application.

## 7 | CONCLUSIONS

Android is the most popular smartphone operating system used by many people across the world. Besides, android can be described as an open ecosystem allowing its users to customize some of its default features and settings. One android setting that can be easily customized by user is the default SMS application. Messages app is by default set as Android messaging app allowing users to send and receive SMS as well as MMS. However, Messages app can be changed to other messaging applications such as Facebook Messenger, Textra, GoSMS, hangouts, Signal among variety of other instant messaging applications that can be downloaded from Google play store by Android smartphone user. It is crucial that mobile forensic investigators pay attention to the kind of SMS artifacts that these android applications can store. Therefore,

it is important that the many instant messaging applications which can be set as default messaging applications in Android be investigated to identify the nature of SMS artifacts they store. This is because they could store crucial artifacts that may not be recoverable through Android device exploitation using existing mobile forensic tools and therefore could provide essential information during cases. This research has provided a foundation for research on instant messaging applications that can be set as default SMS application on Android devices. Facebook Messenger is one of the popular android instant messaging applications with over 1.3 billion monthly active users globally.

By devising a research question; are there recoverable forensic artifacts generated by setting Facebook Messenger as a default SMS application on Android 6.0.1 Marshmallow running on Samsung Galaxy S5 device? This thesis has investigated the artifacts generated by setting Facebook Messenger as default messaging application in Android 6.0.1 Marshmallow. As it has been demonstrated by the research XRY tool could not parse Facebook Messenger data in android 6.0.1 running on Samsung Galaxy S5 device. This, therefore, calls for the use of alternative tools. The research has shown that it is possible to recover some artifacts from Messenger when set as a default messaging application in Android. These artifacts included; the phone number either sending or receiving SMS, the sent, or received timestamp. The research has also shown that some unique flags can be used to tell if messenger application was used to either send or receive SMS message. Finally, the research has shown that when a messenger application is uninstalled or logged out by clearing user data and cache then the SMS information is wiped from the application. The study demonstrated that Facebook Messenger does not store actual SMS message content but stores the phone number which it sends or receives SMS from. By implication, the privacy of users is at stake. In countries where SIM cards are registered, users' biodata are attached to the phone number of the user. Thus, if the phone number can be stored by Facebook Messenger, this will facilitate pointing out where other personal information of the user can be accessed during digital forensic investigation.

Further research can be carried out focusing primarily on multimodality which could increase alternatives for consolidating visual materials such as emoji and photographs in the Facebook Messenger application when sett as a default messaging application.

## ACKNOWLEDGMENTS

The authors would like to thank the anonymous reviewers. This work is fully supported by the Kenya Ministry of Interior, Kenya.

## ORCID

*Moses Ashawa* https://orcid.org/0000-0002-1016-0791

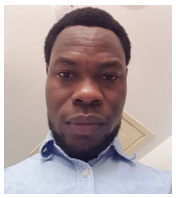
## REFERENCES

1. Watanabe H, Bouazizi M, Ohtsuki T. Hate speech on twitter: a pragmatic approach to collect hateful and offensive expressions and perform hate speech detection. *IEEE Access*. 2018;6:13825-13835.
2. Kolajo T, Daramola O. Leveraging big data to combat terrorism in developing countries. Paper presented at: 2017 Conference on Information Communication Technology and Society (ICTAS), pp. 1-6, 2017.
3. Mohamed I, Bartoo P, Wendo N. Use of twitter as an alternative narrative for Alshabab during the 2013 Westgate mall terror attack in Nairobi, Kenya. *Scholars J Arts Human Soc Sci*. 2016;4:409-414.
4. Andreadis S, Gialampoukidis I, Kalpakis G, et al. A monitoring tool for terrorism-related key-players and key-communities in social media networks. Paper presented at: 2017 European Conference in Intelligence Security Informatics EISIC2017, p. 166, 2017.
5. Ndyave ZC, Kyobe M. Mobile bully-victim behaviour on Facebook: the case of south African students. Paper presented at: 10th Annual IEEE Information Technology, Electronics and Mobile Communication Conference, pp. 743-749, 2019.
6. Jung I, Kim H, Hong DK, Ju H. Protocol reverse engineering to facebook messages. Paper presented at: International Conference on Intelligent Systems, Modelling and Simulation (ISMS), pp. 539-542, 2013.
7. Raghav S, Saxena AK. Mobile forensics: guidelines and challenges in data preservation and acquisition. Paper presented at: SCOReD2009 - Proceedings of 2009 IEEE Student Conference on Research and Development, pp. 5-8, 2009.
8. Palmer G. A road map for digital forensic research. Paper presented at: Digital Forensic Research Conference (DFRWS), 2001, pp. iii-42. http://dfrws.org/sites/default/files/session-files/a_road_map_for_digital_forensic_research.pdf. Accessed December 2018
9. Pollitt M. A History Of Digital Forensics. https://pdfs.semanticscholar.org/0d15/132439fc1de82724dd06effff5a782eefeac.pdf. Accessed August 6, 2018.
10. Kamvar M, Baluja S. Deciphering trends in mobile search. *Computer*. 2019;40(8):58-62.
11. Thulin E, Vilhelmson B. More at home, more alone? Youth, digital media and the everyday use of time and space. *Geoforum*. 2019;100:41-50.
12. Kessler GC. Are mobile device examinations practiced like "forensics". *Digit Evid Electron Sign Law Rev*. 2015;12:3-9.

13. National Cyber Security University. Computer And Mobile Forensics Investigations. https://www.nationalcybersecurityuniversity.com/courses/computerforensics. Accessed February 2019.
14. Lohrmann D. Will a Smartphone Replace Your PC. http://www.govtech.com/blogs/lohrmann-on-cybersecurity/will-a-smartphone-replace-your-pc.html. Accessed January 2019
15. Forensic-Access. Digital Forensics Services for Mobile Phones & Portable Devices. 2019. https://www.forensic-access.co.uk/mobile-phone-digital-forensics/. Accessed August 6, 2018.
16. Ali MM, Mohammed KM, Rajamani L, Framework for surveillance of instant messages in instant messengers and social neworking sites using data mining and ontology. Paper presented at: IEEE TechSym 2014 IEEE Students' Technology Symposium. pp. 297-302, 2014.
17. Zhang Y, Bai Y, Chen L, et al. Influence maximization in messenger-based social networks. Paper presented at: 2016 IEEE Global Communications Conference, GLOBECOM 2016, pp. 1-6, 2016.
18. William B. *Android Forensics*. 1st ed. La Vergne, TN: Lightning Source; 2018:3-90.
19. Statista. Mobile internet traffic share in selected countries 2018. https://www.statista.com/statistics/430830/share-of-mobile-internet-traffic-countries/. Accessed January 2019.
20. Murphy C, Zia H, Majeed A, et al. Forensic analysis of three social media apps in windows 10. Paper presented at: 2015 12th International Conference on High-Capacity Optical Networks and Enabling/Emerging Technologies, HONET-ICT 2015, pp. 1-5, 2016.
21. Dogan S, Akbal E. Analysis of mobile phones in digital forensics. Paper presented at: 2017 40th International Convention on Information and Communication Technology, Electronics and Microelectronics (MIPRO), pp. 1241-1244, 2017.
22. Domingues P, Frade M, Andrade LM, Silva JV. Digital forensic artifacts of the your phone application in windows 10. *Digit Investig*. 2019;30:32-42.
23. Ayers R, Jansen W, Brothers S. Guidelines on mobile device forensics (NIST special publication 800-101 revision 1). *NIST Spec Publ*. 2014;1(1):85.
24. Al Mutawa N, Al Awadhi I, Baggili I, Marrington A. Forensic artifacts of Facebook's instant messaging service. Paper presented at: 6th International Conference on Internet Technology and Secured Transactions, pp. 771-776.
25. Chu HC, Deng DJ, Park JH. Live data mining concerning social networking forensics based on a facebook session through aggregation of social data. *IEEE J Sel Areas Commun*. 2011;29(7):1368-1376.
26. Corcoran K, Read A, Brunty J, Fenger T. Messaging application analysis for android and iOS platforms. 1st ed. Huntington, WV: Marshall University Forensic Science Center, pp. 16-18.
27. Tahiri S. *Mastering Mobile Forensics*. 1st ed. Birmingham, UK: Packt Publishing Ltd; 2016.
28. Ashawa M, Ogwuche I. Forensic data extraction and analysis of left artifacts on emulated android phones: a case study of instant messaging applications. *Seizure*. 2017;19:16.
29. Tsai M, Zhang Y. How the Innovation Diffusion of Facebook Changed Internet Usage and Expression of Public Opinion in Taiwan: Using Voters' Internet and Facebook Usage during the 2016 Taiwanese Presidential Election as an Example. Paper presented at: 2017 Portland International Conference on Management of Engineering and Technology (PICMET), Portland, OR, 2017. pp. 1-8. https://doi.org/10.23919/PICMET.2017.8125347.
30. Umair A, Nanda P, He X. Online social network information forensics: a survey on use of various tools and determining how cautious facebook users are? Paper presented at: The 16th IEEE International Conference On Trust, Security And Privacy In Computing And Communications (TrustCom 2017), 11th IEEE International Conference on the Big Data Science & Engineering (IEEE BigDataSE 2017), 14th IEEE International Conference on Embedded Software and Systems (ICESS 2017), pp. 1139-1144, 2017.
31. Rathnayake C, Suthers DD. Dissidents versus allegiants on facebook: an examination of facebook page networks related to channel 4 war crime videos on Sri Lanka. Paper presented at: Proceedings of the Annual Hawaii International International Conference on Systems Science 2016, March, pp. 2246-2255, 2016.
32. Gruschka N, Mavroeidis V, Vishi K, Jensen M. Privacy issues and data protection in big data: a case study analysis under GDPR. Paper presented at: 2018 IEEE International Conference on Big Data, Big Data2018, pp. 5027-5033, 2019.
33. Mo R, Liu J, Yu W, et al.. A differential privacy-based protecting data preprocessing method for big data mining. Paper presented at: 2019 18th IEEE International Conference On Trust, Security And Privacy In Computing And Communications/13th IEEE International Conference On Big Data Science And Engineering (TrustCom/BigDataSE), Rotorua, New Zealand, pp. 693-699, 2019. https://doi.org/10.1109/TrustCom/BigDataSE.2019.00098
34. Dev Mishra A, Beer Singh Y. Big data analytics for security and privacy challenges. Paper presented at: International Conference on Computing Communication & Automation (ICCCA-2016), pp. 50-53, 2017.
35. Kamakshi P. A survey on privacy issues and privacy preservation in spatial data mining. Paper presented at: 2014 International Conference on Circuits, Power and Computing Technologies, ICCPCT 2014, pp. 1759-1762, 2014.
36. Bronson N, Lento T, Wiener JL. Open data challenges at Facebook. Paper presented at: International Conference on Data Engineering ICDE2015, May. pp. 1516-1519, 2015.
37. Yang Y, Li C, Sun G. A time-space attribute-based evidence fixing method in digital forensics. Paper presented at: 2016 Third International Conference on Trustworthy Systems and their Applications (TSA) 2016, pp. 127-131, 2016.
38. Ashawa M, Ogwuche I. Forensic data extraction and analysis of left artifacts on emulated android phones: a case study of instant messaging applications. *Circ Comp Sci*. 2017;2(11):8-16.
39. Wanda P, Hantono BS. Model of secure P2P mobile instant messaging based on virtual network. Paper presented at: 2014 International Conference on Information Technology Systems and Innovation (ICITSI), November 2014, pp. 81-85.

## AUTHOR BIOGRAPHIES

**Morris Ntonja** received the BSc (Hons) in Computer Forensics from Kenyatta University, Kenya, in 2013, MSc degree in Digital Forensics from Cranfield University, UK, in 2018. He is currently working with the Ministry of Interior, Kenya, as digital forensic investigator. His keen interests include mobile forensics, OSINT, binary level image analysis, malware analysis, and reverse engineering.



**Moses Ashawa** received the BSc (Hon) in computer Science from Benue State University Makurdi, Nigeria, in 2013, MSc degree in Computer Security and Digital Forensics (Distinction) from the University of Bedfordshire, UK, in 2017. From 2015 to 2018, he was a System Analyst at the Federal Ministry of Communication and Technology, Nigeria. He is currently a PhD student at the Centre for Electronic Warfare, information, and Cyber in Defense and Security, Cranfield University, UK. His keen interests include mobile forensics, malware analysis and detection, and machine learning.

**How to cite this article:** Ntonja M, Ashawa M. Examining artifacts generated by setting Facebook Messenger as a default SMS application on Android: Implication for personal data privacy. *Security and Privacy*. 2020;3:e128. https://doi.org/10.1002/spy2.128

## APPENDIX

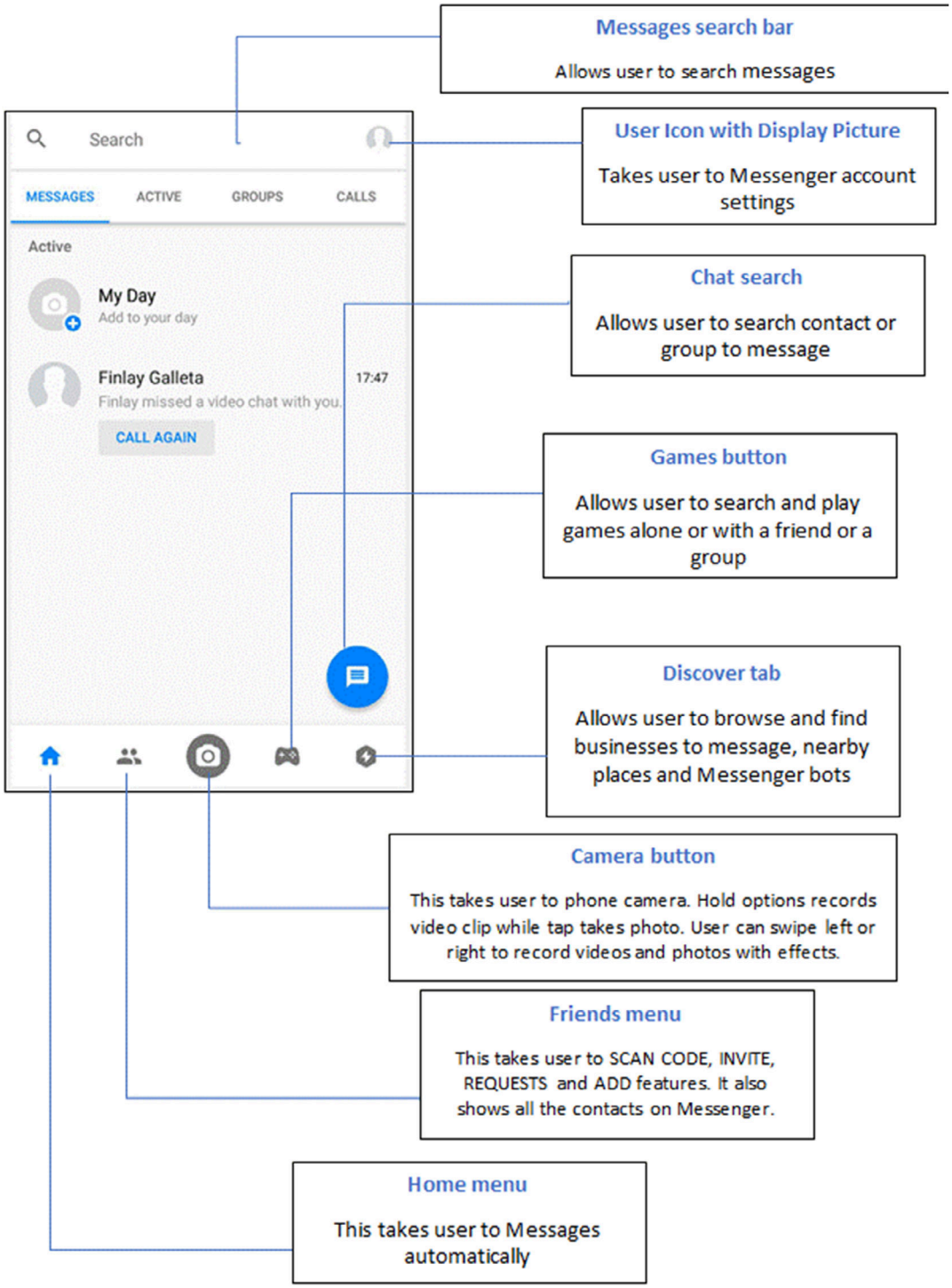



**FIGURE A1** Facebook Messenger features

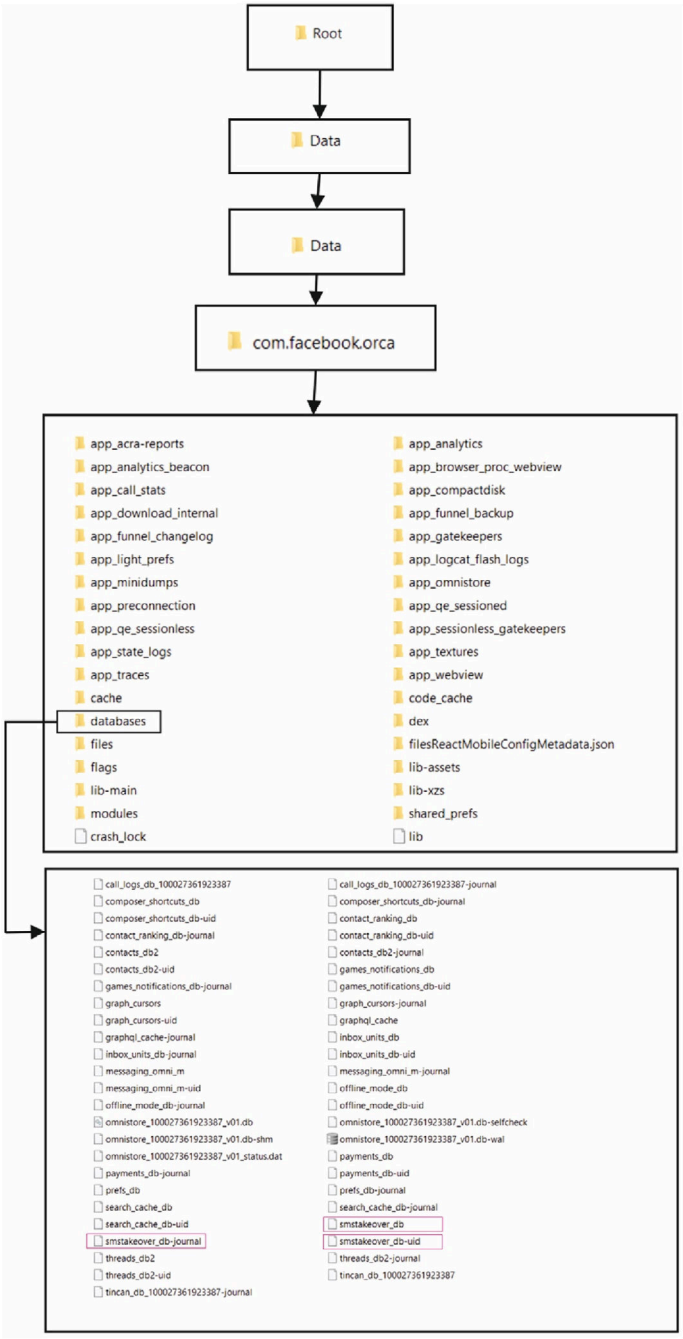



**FIGURE A2** Structure of empty messenger application