FORENSIC ANALYSIS OF GROUPME ON ANDROID AND IOS SMARTPHONES

by

Tanvi M. Gandhi

A Thesis

Submitted to the Faculty of Purdue University

In Partial Fulfillment of the Requirements for the Degree of

Master of Science

Department of Computer and Information Technology

West Lafayette, Indiana

August 2021

THE PURDUE UNIVERSITY GRADUATE SCHOOL
STATEMENT OF COMMITTEE APPROVAL

Dr. Marcus Rogers, Chair

Department of Computer and Information Technology

Dr. John Springer

Department of Computer and Information Technology

Dr. Umit Karabiyik

Department of Computer and Graphics Technology

Approved by:

Dr. John A. Springer

Chair of the Graduate Education Committee

ACKNOWLEDGMENTS

I wish to gratefully acknowledge my advisor Dr. Marcus Rogers for his constant help, support and mentorship throughout my time at Purdue, and Dr. K and Dr. Springer for their time and guidance as my thesis committee.

I also want to thank my parents, brother and friends, without whose encouragement, love and support I could not imagine getting through graduate school.

TABLE OF CONTENTS

LIST OF TABLES

LIST OF FIGURES

LIST OF ABBREVIATIONS

ADB	Android Debugging Bridge
AVD	Android Virtual Device
AXIOM	Advanced eXpress Input Output Module
CFTT	Computer Forensics Tool Testing
Covid-19	Coronavirus Disease of 2019
DF	Digital Forensics
DFIF-IoT	Digital Forensics Investigation Framework for IoT
DFU	Device Firmware Update
FBI	Federal Bureau of Investigation
FORZA	FORensics ZAchman framework
FTK	Forensic ToolKit
IM	Instant Messaging
IoT	Internet of Things
NIST	National Institute of Standards and Technology
OS	Operating System
QC Chipset	Qualcomm Chipset
ROM	Read-Only Memory
SD Card	Secure Digital Card
SMS	Short Message Service
PC	Personal Computer
TWRP	Team Win Recovery Project
UFED	Universal Forensic Extraction Device
URL	Uniform Resource Locator

ABSTRACT

Author: Gandhi, Tanvi Milind. MS

Institution: Purdue University

Degree Received (Expected): August 2021

Title: Forensic Analysis of GroupMe's Android Application

Committee Chair: Dr. Marcus Rogers

The growing popularity of instant messaging has led to the conception of several new applications over the span of the past decade. This has opened up an attack surface for cybercriminals to target susceptible app users. GroupMe is a free IM app widely used by students and so far, no comprehensive forensic analysis has been performed to aid forensic practitioners in recovering evidence from GroupMe on smartphones. This research performs a detailed analysis of the digital artifacts left by the app on Android and iOS devices. This was achieved by installing the app on two mobile phones (Samsung Galaxy S7 Edge and iPhone 6), and identifying each artifact created by performing a series of actions in the app ranging from sending texts, to sharing images and documents, along with their location. Using Cellebrite UFED and Magnet AXIOM, a significant number of artifacts were accurately recovered mainly from the "GroupMe.sqlite" and "GroupMe.sqlite-wal" databases. Out of the 335 artifacts populated on the iPhone, 317 were correctly recovered by both UFED and AXIOM, resulting in an accuracy of 94.62%. No GroupMe related artifacts could be recovered from the Android device. This was due to several physical imaging and rooting limitations imposed by the Samsung SM-935A model, which was used during the study.

CHAPTER 1. INTRODUCTION

This chapter provides an introduction to the study by presenting the background of the research problem as well as of GroupMe, including the primary research question, its scope as well as significance in the field of digital forensics (DF). Additionally, the assumptions, limitations and delimitations of the study have also been discussed.

1.1 Background

Contemporarily, technology seems to be driving every single industry in the world, and smartphones have become more of a necessity than a luxury for every individual to own. It is estimated that by 2021, the number of active smartphone users will rise to 3.8 billion (O'Dea, 2020). The most widely used mobile operating systems today are iOS and Android, which together occupy about 99.45% of the smartphone market worldwide (*Mobile Operating System Market Share Worldwide*, 2020). This popularity, however, can be viewed as a double-edged sword. While smartphone applications provide a wide range of extremely powerful features, users are largely dependent on third party applications to share information rather than the default apps which come installed with the OS itself (Majid ALThebaity, Shailendra Mishra, Manoj Kumar Shukla, 2020), and are often misused by criminals to aid in illegal activities. This can lead to the smartphone being the center of a criminal investigation. Thakur, Hayajneh, and Tseng (2019) comment in their study that since mobile phones have comparatively weaker defense mechanisms than PCs, social media networks being accessed through smartphones can be especially vulnerable platforms for criminals to exploit.

Specifically targeting Instant Messaging (IM) applications, Clement (2019) has provided some statistics on the number of active, unique users of each app, which demonstrates the vast use of IM in the United States. Some of the most popularly used instant messaging applications include Facebook Messenger, Snapchat and WhatsApp, with approximately 106, 46 and 26 million users respectively.

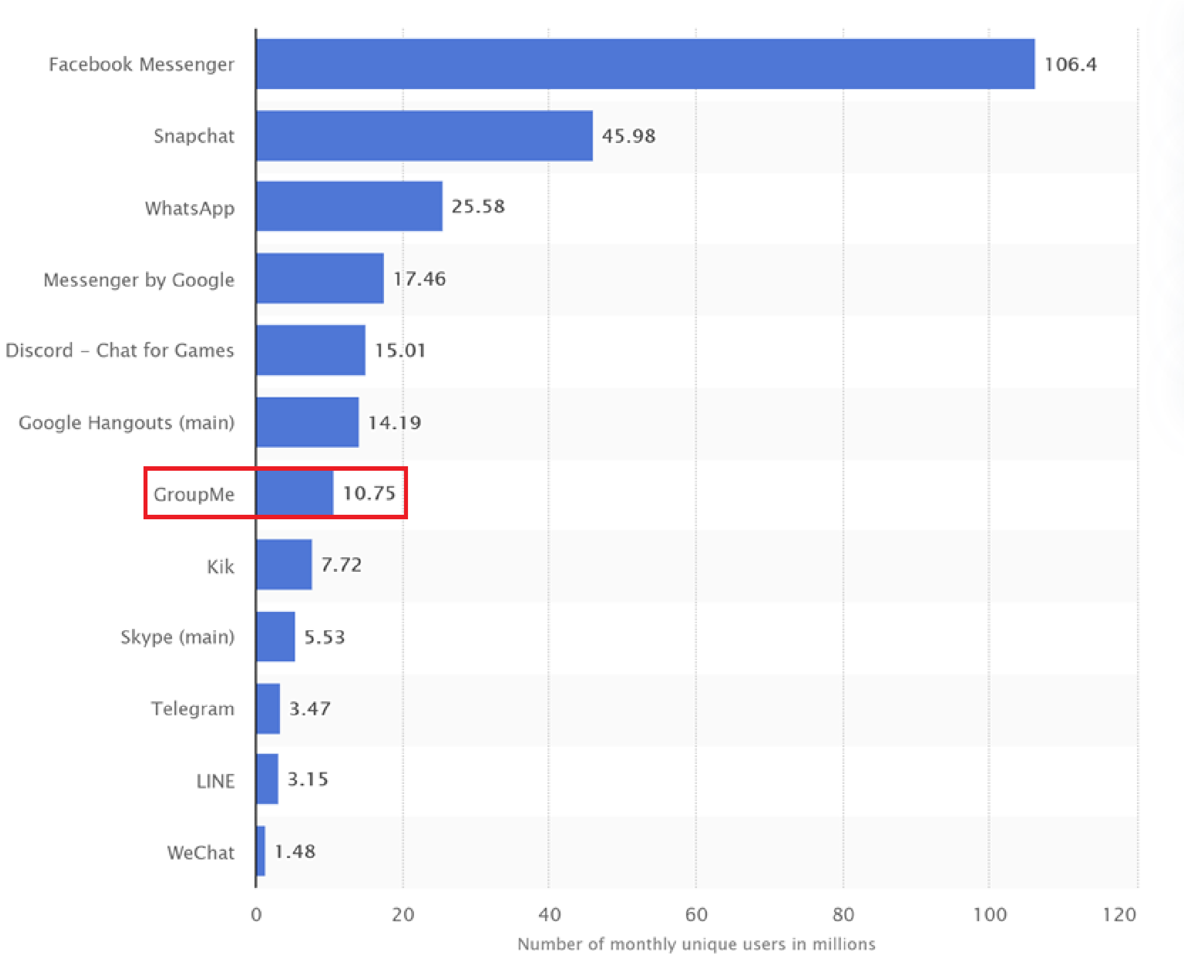


Figure 1.1. Number of IM App Users in the US as of September 2019 (Clement, 2019)

One such upcoming application is GroupMe, which is a free IM app available on Android, iOS and Windows smartphones, along with a web version which can be accessed through PC browsers. It is currently owned by Microsoft, though it was created independently in 2010 and acquired by Skype in 2011. According to Clement (2019), GroupMe has over 10.75 million unique users as of 2019 in the United States alone, a large majority of which are students. GroupMe provides several useful features including private and group messaging, creating groups with up to 500 members, taking audience polls in group chats as well as making group video calls. Moreover, there is an option called “GroupMe SMS” which allows users to create, manage and communicate in group chats through SMS, which means even if they currently do not have the app installed or do not have internet, they can still participate in discussions, although complex group activities like participating in polls and sharing calendar events are not supported.

Along with being able to browse the web and share unlimited photos, videos and documents, users can add text over photos shared in chats to create “Memes” directly in chat, which is another feature that instantly draws students and teenagers towards the app. As defined by Gruger (n.d.) in the Merriam-Webster dictionary, a meme is “an amusing or interesting item (such as a captioned picture or video) or genre of items that is spread widely online especially through social media”. GroupMe also has a Campus Connect feature, which allows students to select their university campus and then choose to join or create group chats specifically for students from the same university to participate in social or cultural events, or simply meet other like-minded students. Additionally, since the Covid-19 pandemic and the increased number of courses being delivered online, several students have started using GroupMe for class collaboration and information sharing among themselves.

Due to its immense popularity with the young, GroupMe, like other IM apps, can be targeted by criminals to indulge in illegal acts, requiring a forensic investigation of the device. An example of one such incident from the past is the 2016 cyberbullying case where a group of Black freshmen from the University of Pennsylvania were added to a racist group chat on GroupMe without their consent (Ozio, 2016). After identifying that the source of the messages was in the Tulsa region, the FBI were consulted by the university, following which the FBI interviewed several students from various Oklahoma universities who were members of the groups (Indani, 2017). Two students revealed that they were added to the groups by a student from the Tulsa Community College, and upon obtaining a search warrant for his phone and investigating it, it was proven that he was responsible for initiating the cyberbullying incident since he had created the groups and started sharing racist content on them (Snyder, 2016).

1.2 Problem Statement

Android and iOS applications leave behind a range of digital footprints which can be identified as evidence and used by forensic investigators to piece together a case (Alyahya & Kausar, 2017). Every application has its own unique way of storing data and app artifacts on the internal storage as well as SD card (if applicable) of the phone, and it is highly unlikely that any one forensic tool has the capacity to be able to locate each artifact for every application accurately. Since no previous research has been performed from this perspective on the GroupMe application, this research will include identifying all possible relevant artifacts created by the app on Android and iOS smartphones along with its significance and location on the filesystem. This will assist a forensic practitioner in an investigation by providing information on which artifact can be located where, along with what information it can provide them with.

1.3 Research Question

This research aims to answer for following question:

1. What digital artifacts created by GroupMe can be forensically recovered using UFED and AXIOM from Android and iOS smartphones?

1.4 Assumptions

The assumptions for this study include:

- The smartphone involved in the investigation is running Android or iOS as the mobile OS.
- GroupMe is installed and has a valid user account set up on it.
- The smartphone is not encrypted/locked by the user and investigators have full access to the OS and filesystem.

1.5 Limitations

The limitations for this study include:

- The current study focused only on Android and iOS operating systems, not desktop/web clients for laptops or PCs.

- The current study only focused on performing analyses on 2 devices, a Samsung Galaxy S7 edge running Android version 7 and an iPhone 6 running iOS 12.5.1.
- The tool used for imaging was limited to UFED4PC and analysis was done using UFED Physical Analyzer and Axiom Examine.
- UFED Reader was used for parts of the analysis using a report (.ufdr) created by UFED Physical Analyzer.
- No cloud data analysis or volatile memory analysis was performed, only data on the filesystem was analyzed.
- Any data stored on external SD cards was not be considered in the proposed methodology, only data stored on the internal filesystems of the devices was included.

1.6 Delimitations

The delimitations for this study include:

- A valid mobile number and email address is necessary to create a new GroupMe account.
- The number being used for account creation must have a valid SMS plan since there is no other method (email/call) for verifying the account.
- An active internet connection is required while setting up the account, to send direct messages and to participate in most group chats (except GroupMe SMS).
- To use the GroupMe SMS feature, a valid SMS plan is necessary.

1.7 Summary

This chapter provided a background of the rise of smartphone and IM app use in recent years, along with a brief description of the GroupMe application. It also discussed the scope of the study as well as significance of researching this application in particular. GroupMe is a widely used app by students and as per PlayStore downloads, has over 10 million Android users. Due to its involvement in various criminal activities over the years, it is important from an investigative point of view to be able to discover digital artifacts created by the app in order to recover valuable evidence. Along with stating the research question and elaborating on its goals, Chapter 1 listed out the assumptions, limitations and delimitations governing this research study.

CHAPTER 2. REVIEW OF LITERATURE

In Chapter 2, a brief background on the Digital Forensics and Mobile Forensics domain has been provided, following which some pre-existing techniques, methodologies and tools developed by researchers to perform forensic analysis of IM apps have been discussed. Some of the current research being performed on GroupMe has also been discussed.

2.1 Digital Forensics

Digital Forensics (DF) is that subcategory of the forensic sciences which deals with helping law enforcement agencies solve crimes which have been committed by using computers or computing devices as tools (Vukadinovic, Seigfried-Spellar, Rogers, & Karabiyik, 2019). It is an extremely diverse field which has found applications in various scenarios ranging from investigative activities and forensic science laboratories to critical infrastructure protection, counter-terrorism and military and intelligence operations (Casey, 2019). DF dates back to the later part of the 1970's, and Pollitt (2010) describes the conception and growth of the digital forensics discipline right from 1976 in the form of four phases or "epochs" which are (1) Pre-history, (2) Infancy, (3) Childhood and (4) Adolescence. In the past four decades, this discipline has matured considerably, with several frameworks which have been developed by researchers to make the process somewhat aligned and standardized.

Carrier and Spafford (2004) presented an event based investigative framework with the goal of standardizing the digital forensics investigation process, which until the time was quite isolated and not unified. Building on this, Ieong (2006) proposed FORZA, which is an investigative framework which helped in bridging the gap between forensic practitioners and legal advisors and prosecutors. Taking into consideration the ever expanding nature of technology, the type of devices being involved in DF investigations are quite diverse. Kebande and Ray (2016) developed a three step process to carry out systematic analyses of IoT devices called the DFIF-IoT (Digital Forensics Investigation Framework for IoT), while Ryu, Sharma, Jo, and Park (2019) proposed a conceptual framework to assist forensic investigators analyze IoT data using a blockchain infrastructure. Despite the structural differences that may exist among these frameworks, they share a common goal, which is to guide a forensic practitioner through an investigation in a systematic fashion. Satpathy and Mohanty (2020) have summarized the the three basic goals, or three A's of any DF methodology, which are: (1) Acquiring evidence without modifying the source, (2) Authenticating the acquired evidence to ensure that it has not been changed, and (3) Analyzing the acquired data.

2.2 Mobile Forensics

Mobile forensics is a sub-category of DF, and pertains to the acquisition and analysis of data from mobile devices (Reddy, 2019). When it comes to Mobile Forensics, the National Institute of Standards and Technology (NIST) has provided various different models to ensure a smooth investigative procedure. Ayers et al. (2014) provides an extensive document describing the hardware structure of mobile phones and the manner in which information is stored in each component. The authors also propose a methodology, commonly known as the "NIST Methodology" or "NIST Framework", which is a four step process including (1) Acquisition, which includes identification of the mobile device, selecting appropriate tools and extraction of forensic images; (2) Examination, which includes loading the acquired evidence into appropriate tools and identifying potential evidence; (3) Analysis, which includes applying forensic tools to study the acquired data to reach certain conclusions; and (4) Reporting, which encompasses consolidating the analysis and presenting the findings. Even though they go hand in hand with each other, there are some notable differences between the Examination and Analysis steps. As explained by Ayers et al. (2014), Examination uncovers digital evidence that may be hidden or obscured by separating useful information from irrelevant data. On the other hand, Analysis entails studying the results obtained from the examination process in detail to understand their significance to the case. In another presentation, Ayers (2009) discusses NIST's Computer Forensics Tool Testing (CFTT) Program, which is used as a standard for measuring the capability and assurance of mobile forensic tools to ensure that the results provided by them are reliable and accurate. It not only helps in maintaining a standard for tools, but also enables interested people in understanding the tool capabilities in their entirety.

Moreover, Ayers et al. (2014) have classified mobile device tools into five categories, based on the techniques used for extraction, which are: (1) Manual extraction, which includes extracting all the data from the phone which is visible directly through the screen to the user, (2) Logical extraction, which includes extracting visible data as well as deleted data which is present on the mobile filesystem, (3) Hex dump/JTAG, which includes creating a bit-by-bit copy of the device to provide more detailed information than the previously discussed methods, (4) Chip-off, which is a method by which data is acquired directly from the NAND flash memory and usually requires an expert to perform, and (5) Micro read, which involves manually interpreting data stored on the phone's memory chip.

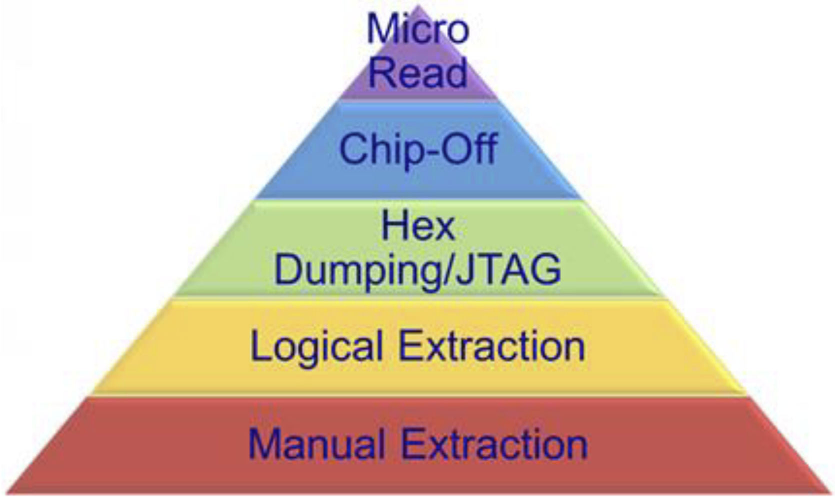


Figure 2.1. Ayers et al. (2014) Tool Classification

2.2.1 Android Forensics

Android is the most prevalent mobile operating system as of 2020, occupying about 73% of the mobile market (*Mobile Operating System Market Share Worldwide*, 2020). Tayeb and Varol (2019) have performed a review of popular pre-existing methodologies for Android forensics and provided a consolidated model. The steps they have suggested are: (1) Identification, (2) Preservation, (3) Acquisition, (4) Examinations and Analysis, and (5) Presentation. It can be noted these are quite similar to the generic mobile forensics steps provided by NIST, but Tayeb and Varol (2019) go on to provide a detailed acquisition process (step 3) which is divided into three stages: (1) File System Acquisition, (2) Memory Acquisition, and (3) Environmental Acquisition. However, for an investigator to be able to acquire maximum data from the Android filesystem, it is sometimes necessary to gain “root” access. As explained by Boueiz (2020), Android is based on the Linux operating system, which uses a single tree hierarchy of directories (folders) with Root at the top. This means that without superuser (root) access, it may not be possible to retrieve data from certain directories. Rooting can be performed on a device after unlocking its bootloader, which is defined by Nazario (2013) as a piece of software that boots up each time a phone is started up. It it responsible for making sure that the operating system is booted properly so the phone can function normally. It also has a security layer to verify that only an operating system that passes its approval process can be loaded, which needs to be bypassed to be able to root a phone, which is why unlocking it becomes necessary Nazario (2013).

2.2.1.1 Rooting an Android Phone There are several techniques to root Android devices, including one-click mobile applications like Framaroot, KingoRoot, BaiduRoot, Clockwork (CWM) and Towelroot, or PC softwares like Android Toolkit (Junaid, 2019). All of the aforementioned tools enable root without wiping existing data from the device, however, do not specify the techniques they use to enable the root. This often results in susceptibility to spyware and adware, and cannot be considered forensically sound. Alternatively, more reliable rooting methods are available, one of which uses Odin, a developer tool for Samsung mobile phones that can be used for rooting, installing custom ROMs, restoring a bricked device, etc. (Morgan, 2019). Paired with CF Autoroot, which is a root tool compatible with Odin, it is possible to root an Android phone without wiping its current contents (*Will CF-Auto-Root wipe the device*, 2013). Another trustworthy rooting technique uses TWRP (Team Win Recovery Project), which is a custom recovery that enables a user to flash unauthorized or 3rd party software or mods to their device. TWRP can be used to install Magisk, a framework that enables systemless root. Systemless root essentially means that Magisk will create a boot partition in the target device and make all modifications to it instead of the actual device (*What is Magisk?*, n.d.). For these methods, if the bootloader of the target device is not already unlocked, involves manually unlocking the bootloader to be able to install the custom ROM, which in most cases results in the device being completely formatted (Boueiz, 2020).

While rooting a device can provide a significant enhancement in the amount of data which can be retrieved, it also raises concern on user data privacy, and from a forensic perspective, it could also alter some of the data, which can lead to questions regarding its authenticity (Almehmadi & Batarfi, 2019). An investigator can weight the pros and cons of rooting and then make an informed decision on whether or not to use this technique in their investigation.

2.2.2 iOS Forensics

iOS is the operating system used by Apple's iPhones, iPads and iPod Touch devices (Epifani & Stirparo, 2016), and is the second most popularly used mobile OS, occupying approximately 27% of the worldwide smartphone market (*Mobile Operating System Market Share Worldwide*, 2020). Applications on iOS devices run in a structure composed of four layers, where: (1) Layer 1 provides direct access to the kernel and memory, (2) Layer 2 consists of services written in the "C" programming language, (3) Layer 3 is responsible for managing graphics as well as media, and (4) Layer 4 provides a high level interface to connect users with the mobile app (Al-Hadadi & AlShidhani, 2013). Apart from traditional extraction techniques, iTunes backups are also a commonly used method for data acquisition and analysis of iPhones. The backups are treated as logical images and can be analyzed using tools like Reincubate iPhone Backup Extractor (Knox, Moghadam, Patrick, Phan, & Choo, 2020), Oxygen Forensic Analyst and iPhone Analyzer (Igor Mikhaylov, 2016), etc. An interesting point to note about iTunes backups is that if they are encrypted, they would have more information in them than unencrypted ones (*About encrypted backups on your iPhone, iPad, or iPod touch*, 2021). This includes data like saved passwords, health data, WiFi settings, call history and website history. Thus, forensic tools provide the option to encrypt backups with a default password, just to be able to extract more data from them.

2.3 IM App Forensics

Instant Messaging can be defined as a service that enables people to monitor the online presence of fellow users and also exchange messages and files with those users (Low & Wilson, 2003). It can be said that IM existed all the way back in the 1960s, like MIT's Compatible Time-Sharing System (CTSS) which enabled up to thirty people to log in and chat simultaneously, or the Zephyr Notification Service, also created at MIT, which used UNIX to locate users and send messages (Petronzio, 2012). However, IM as we know it today (i.e., real time text chat through the internet), was first seen in the form of ICQ in 1996 and AOL in 1997. Developed by Mirabilis, ICQ was an IM utility which users could download for free on their computers as a client (Jeff Tyson, 2001). AOL, too, allowed users to chat in online chat rooms, and subsequently acquired Mirabilis (along with ICQ) in 1998 (Jeff Tyson, 2001).

A considerable amount of research has been done to perform thorough analyses of digital artifacts created by several IM apps. While there are several categories under which these studies can be synthesized together (based on tools used, based on methodologies/frameworks followed), for the sake of this review, they will be categorized based on the application under consideration since each application has a unique way of creating and storing artifacts on smartphones. Thus, it does not make sense to merely compare the performance of tools or methodologies while ignoring the application they are being used on.

In a comparative study between the WhatsApp Key/DB Extractor and Belkasoft Evidence Center (BEC) tools, Yadav, Prakash, Dayal, and Singh (2019) performed an analysis on artifacts extracted from the WhatsApp database using both the tools on four separate android phones. The focus was on evaluating which tool performed better in terms of accurately reconstructing the database to retrieve deleted messages which may be of importance to a forensic investigator. BEC was found to be 98.13% successful, whereas WhatsApp Key/DB Extractor showed a significantly lower success rate of 43.92%. In another study aimed at WhatsApp forensic analysis, Zamroni and Riadi (2019) proposed a methodology with four stages (Activities Simulation, Forensic Analysis, Forensic Results Analysis, and Conclusion) to extract digital artifacts using an unrooted Samsung C9 Pro smartphone. The authors used a combination of BEC, Oxygen Forensic, Magnet

AXIOM, and WhatsApp Key/DB Extractor tools and successfully extracted artifacts including chat messages, call logs, contact lists, and files shared by the user.

Applications with encrypted databases and end-to-end encryption for one to one conversations are posing significant challenges to law enforcement during digital investigations. Rathi, Karabiyik, Aderibigbe, and Chi (2018) have discussed techniques to decrypt the databases and perform a detailed analysis of digital artifacts collected from four encrypted IM apps (WhatsApp, Viber, We Chat and Telegram). They used three separate phones, two of which were unrooted, and one was rooted and acquired artifacts like call logs, contacts, text messages, images, videos and geo-location information using ADB (Android Debugging Bridge) with other open source tools. Moreover, they have shown how each of the apps store data in the Android file system as well as discussed challenges faced in the forensic analysis process.

In a more detailed article, Anglano, Canonico, and Guazzone (2017) have studied Telegram very closely. The authors proposed an interesting methodology to perform a forensic analysis of the app which was performed on virtualized smartphones in lieu of physical devices to provide generality and reproducibility of results. Using this method, the authors were able to retrieve a large number of artifacts including a reconstructed list of contacts, the chronology and contents of messages, files, properties of groups and channels in which the user has been involved as well as complete call logs. Due to its generalized nature, this process can be applied to any Android application and can also facilitate anyone to validate the results obtained in the study.

An analysis of Facebook performed by Majid ALThebaity, Shailendra Mishra, Manoj Kumar Shukla (2020) leveraged both quantitative and qualitative methods of research to first recover and classify artifacts like text messages, login information, friends' information, and user account details. Following this, a description of each artifact was provided to the reader. FTK imager was used to make an image of the Android device and examine the SQLite databases of the Facebook app. In another study conducted by Yudhana, Riadi, and Anshori (2019), the Facebook Messenger app was forensically analyzed based on the NIST methodology using Magnet AXIOM and Oxygen Forensics Suite 2014. While both the tools provided similar artifacts (user accounts, conversation texts, images), the authors found the data obtained from AXIOM more detailed and fruitful than from Oxygen Forensics Suite.

Al-Rawashdeh, Al-Sharif, Al-Saleh, and Shatnawi (2020) have performed a post mortem memory forensics analysis of the Kik application by employing their own investigative methodology which uses memory dumps for NAND flash memory as well as heap memory of the device. Once both the memories for Kik Messenger are dumped, the researchers have created eight unique scenarios and designed an experiment for each, to identify relevant artifacts. The tools used included Android Studio with the Android Virtual Device (AVD) Manager tool to provide the Android Virtual Device Emulator. Additionally, the Android Debug Bridge was used to install the Kik app. Through the results, the authors were not only able to find all the sent and received messages through the account, but were also successful in proving that every message had been stored in plain text in the database at least once.

In another forensic analysis performed on IMO, which is an IM app that facilitates messaging and calling, Sudozai, Saleem, Buchanan, Habib, and Zia (2018) proposed a methodology for recovering digital artifacts on Android as well as iOS devices. Their methodology consists of five main steps, which are: (1) Analysis of IMO functionalities, (2) Application Installation, (3) Account Configuration, (4) Experiments for IMO functionalities, and (5) Information Extraction and Analysis. The mobile devices they used for their analysis were a rooted Samsung Galaxy 6.0 running Android version 6.0.1 and a jail-broken Apple iPhone 5 running iOS 9.3.3 and were able to recover several types of artifacts including phonebook entries, email Ids, call logs, chat logs and even the contents of the chats.

2.4 GroupMe

Previous research for the GroupMe Android application exists primarily in the field of education. Gronseth and Hebert (2019) discuss the effect of using GroupMe as a method of delivery in online classes on the engagement of students in the higher education context whereas Ly (2020) focuses on the development of the writing style of students using GroupMe to participate in online class discussions. No research in the forensic domain has been performed on GroupMe to the best of the author's knowledge. To bridge this gap, the focus of this research will be drawing inspiration from the pre-existing literature and performing an analysis of the digital artifacts created by GroupMe on Android and iOS smartphones, as well as describing their significance to forensic investigators.

2.5 Summary

This chapter provided a literature review relevant to digital forensics as well as mobile forensics, including Android and iOS smartphones. Moreover, it included an elaboration of research conducted on IM apps similar to GroupMe including WhatsApp (Rathi et al., 2018; Yadav et al., 2019; Zamroni & Riadi, 2019), Facebook Messenger (Yudhana et al., 2019), Facebook (Majid ALThebaity, Shailendra Mishra, Manoj Kumar Shukla, 2020), Telegram (Anglano et al., 2017; Rathi et al., 2018), Kik (Al-Rawashdeh et al., 2020) and IMO (Sudozai et al., 2018). These articles helped in providing the researchers with a better understanding of the structure in which data is locally stored by IM apps on Android and iOS devices. Additionally, valuable insights could be drawn from the various proposed methodologies to analyze the artifacts, and the comparison of tools helped in selecting the right tools for this research.

CHAPTER 3. METHODOLOGY

This chapter provided the proposed methodology to perform a detailed forensic analysis of GroupMe on Android and iOS smartphones. Since no pre-existing forensic research had been performed specifically on this application, a new methodology built upon the NIST guidelines (Ayers et al., 2014) was followed to satisfy the goals of the study.

3.1 Hypotheses

The hypotheses which were tested in this study were the following:

- H_1: The accuracy of recovered artifacts will be the same using UFED and AXIOM on the Android device.
- H_2: The accuracy of recovered artifacts will be the same using UFED and AXIOM on the iOS device.

3.2 Research Environment

The objective of this study was to identify the location and analyze the digital artifacts created by GroupMe in the Android and iOS filesystems. The smartphones used for this research consisted of a Samsung Galaxy S7 Edge (Android 7.0) and an iPhone 6 (iOS 12.5.1). The model number for the Samsung phone was SM-G935A, which is the US variant carrier locked to AT&T. The workstation setup included a Dell Optiplex 7060 running Windows 10 Education and a Dell XPS 15 laptop running Windows 10 Home. The Optiplex workstation was used for imaging since it had Purdue's active license for UFED4PC, whereas the XPS workstation was used for all the examinations and analyses.

UFED4PC (Version 7.42.0.82) was used for image acquisition, and the acquired images were then analyzed using Cellebrite UFED Physical analyzer (7.42.0.50) and Reader (Version 7.42.0.50) and Magnet AXIOM (4.11.0.24063) for both Android and iOS devices. These tools were selected since they are considered to be industry standard tools that have provided reliable results in forensic studies in the past (Anglano et al., 2017; Majid ALThebaity, Shailendra Mishra, Manoj Kumar Shukla, 2020; Zamroni & Riadi, 2019). For iPhones, iTunes backups were not used as the extraction method since they only provide logical backups, whereas we are interested in a deeper layer, which physical extraction using UFED provides us with. Moreover, UFED has been integrated with the CheckM8 exploit for iOS, which enables the tool to perform complete forensically sound file system extractions which are compatible with 85% of the iOS devices in the market (*Cellebrite UFED iOS - Cellebrite*, 2020).

3.3 Research Design

The research methodology followed in this study consisted of two broad phases: (1) Pre-Investigative, and (2) Investigation. Even though the same general phases were followed for Android as well as iOS devices, there were some minor differences in the methodologies for both. The results obtained were contrasted thereafter. An outline of the methodology used is provided below, followed by flow charts depicting each phase.

3.3.1 Pre-Investigative Phase

This phase is called "pre-investigative" since in an actual investigative scenario, a forensic practitioner would not be performing these steps. They would receive a seized device in the same state as ours would be in after the completion of this phase. The steps included in this phase are presented in the form of a flow chart in Figure 3.1, and then discussed in detail.

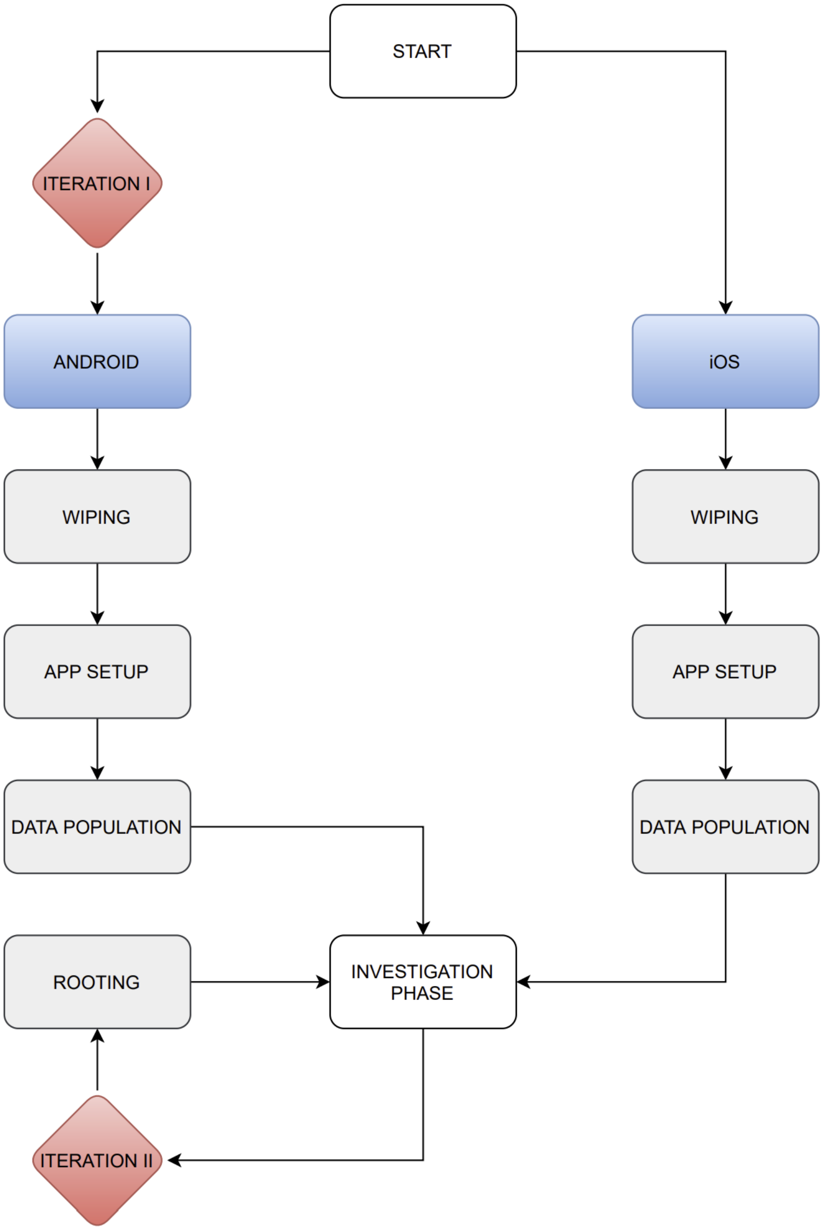


Figure 3.1. Schematic Representation of Pre-Investigative Phase

3.3.1.1 Wiping Both the devices were wiped back to their factory state.

1. Android - This was done by navigating to *Settings* → *General Management* → *Reset* → *Factory Data Reset* and clicking on the “Reset Device” option.

2. iOS - This was done by navigating to *Settings → General → Reset → Erase All Content*. Upon getting prompted, the apple ID and password linked to the device were entered for confirmation.

3.3.1.2 App Setup The latest version of GroupMe was installed on both devices and a new user account was set up. Prior to this, a new Google account was created, and the email address associated with it was used to set up the GroupMe account. An AT&T sim card was also acquired and the number associated with it was used to verify the GroupMe user account.

1. Android - GroupMe (Version 5.59.6) was downloaded through the Play Store. A user account with the name “Purdue Forensics”, was created.
2. iOS - GroupMe (Version 5.48.1.8) was downloaded through the App Store. A user account with the name “Jane Doe” was created.

3.3.1.3 Data Population Both the devices were populated with GroupMe app data by using common functionalities of the app in accordance with the NIST data population guidelines (NIST, 2016). These guidelines suggest that three main factors must be considered while preparing any device for data population, which were ensuring that the device: (1) did not have any pre-existing user data; (2) had valid network connectivity; and (3) did not have any pre-existing personally identifiable information. Since the devices used in this study had already been reset to factory state, and a valid sim card with a data plan had been inserted in both devices, all three conditions were satisfied.

When prompted by the app to provide permissions (location, storage, camera, phone, contacts, microphone), all permissions were provided. A total of 335 actions were performed during data population on each of the two devices. The type of action performed as well as a short description on how to perform each one is provided in Table 3.1 below. The hypothetical scenario created included the user adding 5 friends as contacts on GroupMe and chatting with them about school work and graduating from college soon. Details of which action was performed in which chat in the hypothetical scenario has been provided in Appendix Table A.1 for the Samsung phone and Appendix Table A.2 for the iPhone.

Table 3.1. *Data Population Guidelines*

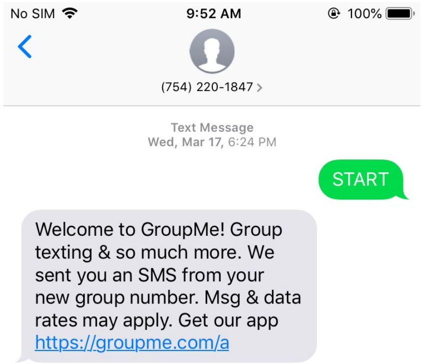
Type of Action	Description	File Formats
Text Messages (Total: 250)	This included sending (100) and receiving (150) text messages in private and group chats.	
Media Items (15)	Photos and videos were shared in private and group chats. This included clicking new photos and videos through the app as well as sharing others from the phone's storage.	JPEG (3), PNG (3), GIF (3), MP4 (3), M4V (3)
Integrated Videos (5)	YouTube videos through the built-in feature to share YouTube videos were sent (3) and received (2) in the form of URLs within private and group chats.	
Liking Messages (20)	Text messages sent by other users were "liked" by clicking the heart icon beside them in private and group chats.	
Shared Locations (4)	The user's current location (2) as well as other (2) locations on the map were shared in private and group chats	
Documents (10)	Supported documents were shared in private and group chats.	DOC (2), PDF (3), PPTX (1), XLS (1), TXT (2) XLSX (1)
Adding Contacts (5)	This included adding new contacts in the app by the phone number of the recipient.	
Blocking Contacts (1)	One particular contact was blocked by the user.	
New Group (1)	A new group was created and some members were added to it.	
Exiting a Group (1)	One of the groups that the user was a member of was exited (this sends the group to an Archive).	

Polls (2)	This included creating new polls in group chats and sharing them with the participants.	
Calendar Event (2)	New calendar events were created in private (1) and group (1) chats and shared with other participants.	
Memes (4)	This included creating a new meme using the apps built in feature and sharing it in private as well as group chats.	JPEG (2), PNG (2)
Skype Calls (2)	Skype call invitations were created and received using the Skype button provided in each chat.	
Searches (2)	This included searching for a chat by contact name and searching for texts within a private or group chat.	
GroupMe SMS (3)	A new group was created via SMS, a new member was added to it through SMS and messages were exchanged in the group chat (instructions below).	
Hiding Messages (1)	This included "hiding" a particular text message sent to another user on your device by long pressing the text and selecting "hide message" (does not delete it).	
Hiding Chats (2)	Two private chats were hidden by long pressing on them and selecting "hide chat"(this moves the chats to an Archive).	
Unhiding Chats (1)	1 of the hidden chats sent to Archives was unhidden by selecting it and clicking "Unhide".	
Editing Personal Information (1)	The Display Name of the user under *Settings* → *Profile Information* was changed.	
Campus Connect (3)	Purdue University was selected as the relevant campus and several group actions were performed including joining a pre-existing campus group as well as creating a new one for Purdue (instructions below).	

The populated artifacts discussed in the table above were grouped in accordance with how the author expected GroupMe to categorize and store its artifacts. For example, it was expected that text messages, documents, media items, etc., would create unique types of artifacts that would be treated as separate data types by the tools used for examination and analysis. However, during analysis it was found that GroupMe actually treated these artifacts differently, which has been discussed in detail in the Investigation Phase.

GroupMe SMS - The instructions for using GroupMe SMS provided by *What are GroupMe SMS Commands?* (n.d.) were used in this study and have been explained below. Before being able to send or receive messages through SMS, some settings within the app needed to be altered. In the app, upon navigating to *Settings* → *Notifications* → *Receive messages via SMS*, Turn on SMS Mode was selected. This activated GroupMe SMS, and was turned off after the population was done to be able to receive notifications through the app again. Screenshots of each action listed below performed on the iPhone have also been provided for reference.

- Creating a new group: The word "START" was sent to +1 754-220-1847 via SMS to create a new group (Figure 3.2). Thereafter, a text from another number (+1 806-476-4236) stating that the group was successfully created was received (Figure 3.3).

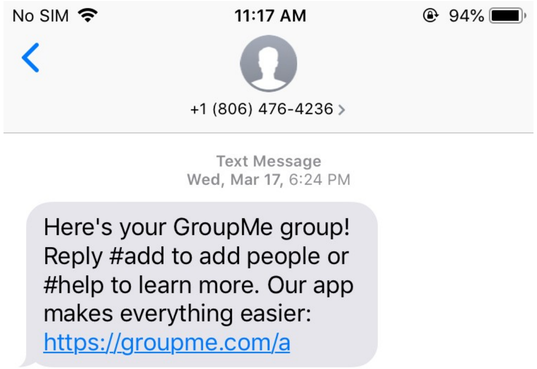


Text Message
Wed, Mar 17, 6:24 PM

START

Welcome to GroupMe! Group texting & so much more. We sent you an SMS from your new group number. Msg & data rates may apply. Get our app https://groupme.com/a

Figure 3.2. Creating a New Group



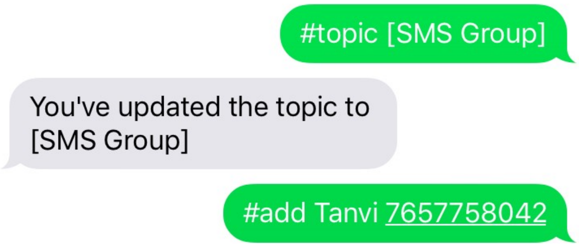
Text Message
Wed, Mar 17, 6:24 PM

Here's your GroupMe group! Reply #add to add people or #help to learn more. Our app makes everything easier: https://groupme.com/a

Figure 3.3. Group Creation Successful

- Setting a name for the group: By sending "#topic" followed by the desired group name in the conversation, the group name was set to SMS Group (Figure 3.4).

- Adding a new member: By sending "#add" followed by the name and phone number of the targeted recipient, a new member was added to the group (Figure 3.4).



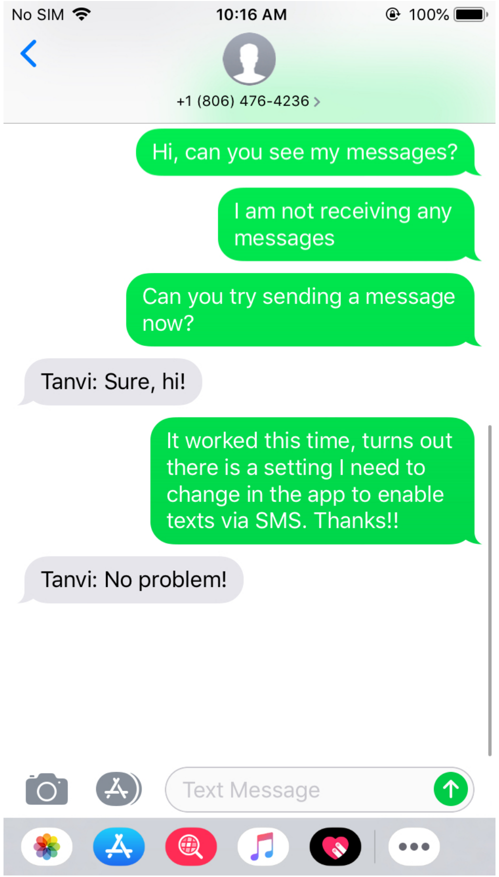
#topic [SMS Group]

You've updated the topic to [SMS Group]

#add Tanvi 7657758042

Figure 3.4. Setting Group Name & Adding a Member

- Sending and receiving messages: Whatever messages were sent in this conversation without being preceded by "#" were sent as messages to all the recipients in the group. Any messages they sent to the chat were also received in the same conversation (Figure 3.5).



Hi, can you see my messages?

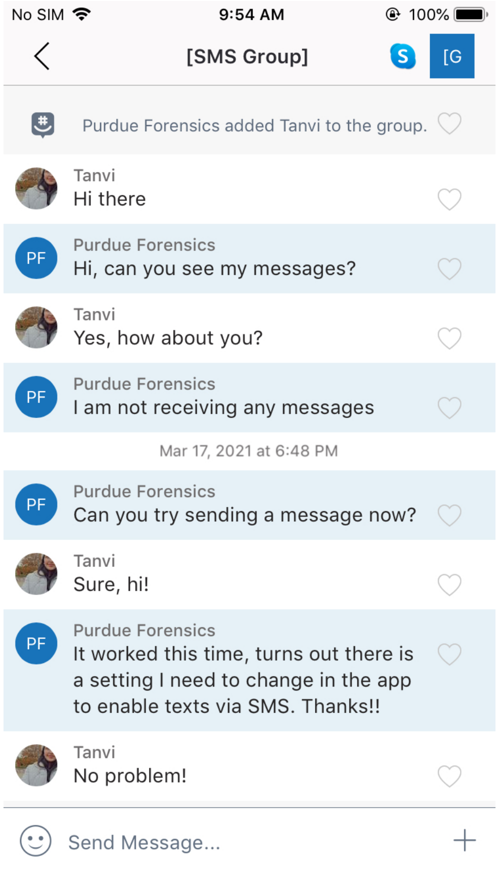
I am not receiving any messages

Can you try sending a message now?

Tanvi: Sure, hi!

It worked this time, turns out there is a setting I need to change in the app to enable texts via SMS. Thanks!!

Tanvi: No problem!



Purdue Forensics added Tanvi to the group.

Tanvi
Hi there

PF Purdue Forensics
Hi, can you see my messages?

Tanvi
Yes, how about you?

PF Purdue Forensics
I am not receiving any messages

Mar 17, 2021 at 6:48 PM

PF Purdue Forensics
Can you try sending a message now?

Tanvi
Sure, hi!

PF Purdue Forensics
It worked this time, turns out there is a setting I need to change in the app to enable texts via SMS. Thanks!!

Tanvi
No problem!

Figure 3.5. Messages in SMS

Figure 3.6. Messages in App

After all these steps were completed, SMS Notifications were turned back off in the app so it could be used normally, following which the group created using SMS was visible even in the app as a regular group chat (Figure 3.6).

Campus Connect - To start using this feature, “Campus Connect” was selected in the app menu, and a valid Purdue University email address was entered upon being prompted. After verifying the email address, the Purdue University campus community was successfully opened in GroupMe and a list of pre-existing groups was displayed. To join any of these groups, the group was simply selected and “Join Group” was clicked. To create a new group within the Community, the “+” icon at the top of the screen was clicked and after entering a name for the new group, “Create” was clicked. Any groups joined or created through Campus Connect were visible as regular groups on the main chat screen in the app.

3.3.1.4 Rooting This step was carried out only in the **second iteration** (after investigation phase had been completed once) for the **Android device**, in an attempt to obtain superuser privileges since no useful information could be retrieved in the first iteration. The important thing to note here is that for most rooting techniques to work, the device’s bootloader must be in an unlocked state. If the bootloader of the target device is locked, most rooting methods will attempt to unlock it first, which could potentially erase all the data on the device. Doing this would be forensically unacceptable, since all the evidence from the phone could be erased in the process.

Upon researching the Samsung Galaxy S7 Edge device being used in study, it was found that for this particular model (SM-G935A), which is the AT&T variant, it is impossible to unlock the bootloader (Malani, 2016; *TWRP recovery for AT&T SAMSUNG S7 Edge (SM-G935A)*, 2018). This is because the bootloader for this model is based on QC (Qualcomm) chipsets, which does not allow bootloader unlocking for the AT&T devices. As opposed to this, the international variants of the same model, which end in W8/F/K/L/S/FD use Exynos chipsets which have unlocked bootloaders and can be rooted without losing data.

Moreover, one click rooting tools like Towelroot and Kingoroot were not opted for since as discussed earlier, they do not reveal the process used for rooting, and often rely on some exploits to get root access. The problem with this is that most of these exploits get quickly patched by manufacturers, rendering these apps ineffective (*Spyware: KingRoot, KingoRoot, iRoot, etc*, 2018). Moreover, according to an XDA developer gatesjunior (2017), some of these apps alter existing data and install adware onto the device, which would create new data and artifacts and consequently make the data obtained forensically unsound. Due to these factors, it was not possible to achieve successful rooting for the Android phone, and the analysis will be done without the results expected from rooting.

3.3.2 Investigation Phase

This phase is based on the NIST guidelines provided by Ayers et al. (2014), which is a four step process including Acquisition, Examination, Analysis and Reporting. These are the steps that an investigator would follow in an actual investigative scenario after obtaining the seized devices, thus it has been referred to as the "Investigation Phase". Figure 3.7 shows a flow chart of the different steps including the tools used in each one.

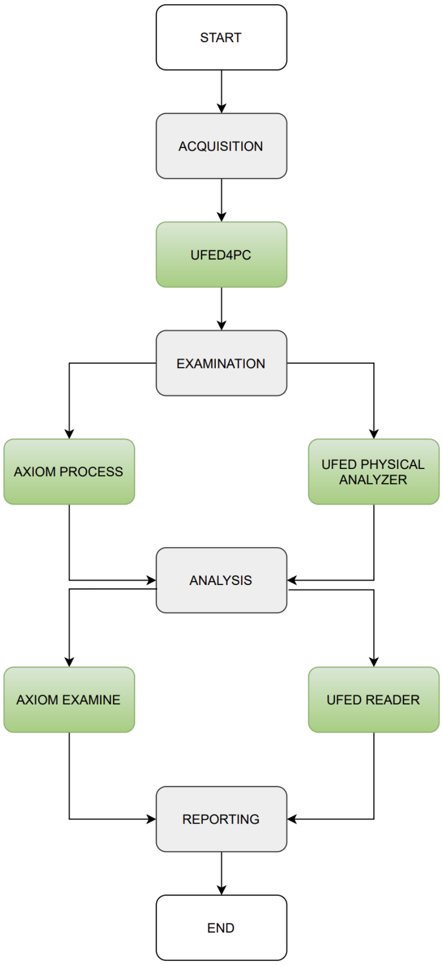


Figure 3.7. Schematic Representation of Investigation Phase

3.3.2.1 Acquisition A forensic image of both devices was created following the steps provided by the vendors after data population. According to McKemmish (2008), a forensically sound acquisition process is defined as “a transparent digital forensic process that preserves the original meaning of the data for production in a court of law”. UFED4PC was used for imaging both, the Android as well as iOS device.

1. Android - UFED4PC has several available extraction techniques for Android phones, including Advanced Logical, File System and Physical. As discussed before, physical imaging techniques are capable of extracting maximum amount of data from a device, thus physical imaging using UFED4PC was attempted to image the Samsung phone.

   UFED Physical Extraction - The different physical imaging options offered by the tool were ADB (Android Debugging Bridge), Advanced ADB and Boot Loader. All 3 of these techniques were attempted to image the device following all the on screen instructions, but all 3 failed. The error message displayed was “Device not supported”, despite the official Cellebrite release notes stating that this model (SM-G935A) was included in the list of supported devices (*UFED Ultimate & UFED In Field*, 2018). Upon some further troubleshooting through the tool, it was discovered that it does not guarantee physical extraction of devices with security patches further than November 2016. The security patch of the device being used was from June 2017, which was most likely the reason of failure to perform any physical extractions using UFED. Another suspected cause is that, according to another Cellebrite source *Supporting new extraction methods and devices* (2019), bootloader decryption and unlocking technologies are only supported for Samsung Exynos versions, not the QC versions, which was preventing successful physical extraction for the SM-935A model being used in this study. The difference between Exynos and Qualcomm chipsets has been discussed in the Rooting section of the Pre-Investigative Phase.

   UFED Advanced Logical Extraction - Since physical extraction using UFED was not possible, the next best option, which is Advanced Logical imaging, was pursued. UFED’s Advanced Logical acquisition technique is a combination of logical and file system extractions, which allows users to overcome long and convoluted extractions, saving time and effort while still maintaining forensically sound data (*Supporting new extraction* *methods and devices*, 2019). After selecting the Advanced Logical option on screen, the target directory for the extracted files was selected and the device was connected to the workstation using a USB cable. Following this, all on screen instructions provided by the tool were followed. Once the tool identified the device, the user was prompted to select the extraction source as well as data types to be extracted. Since the device used in the study did not have a memory card inserted, the source was selected as “Device”, and all data types were selected to be extracted. In a few minutes, a window stating that extraction was successful popped onto the screen. Upon opening the directory with extracted files, the resultant files including a “.ufdx”, “.ufd” and “.dar” were found. This verified that the extraction process had been successfully completed.

<u>AXIOM Process</u> - Despite having a successful advanced logical image from UFED, another attempt at acquiring a physical image was made using AXIOM Process as a last resort. AXIOM has two options for acquisition, Full and Quick. According to *A technical look at Phone Extraction* (2019), Full extraction provides a physical image, whereas Quick provides a logical one. When the Samsung phone being used in the study was attempted to be imaged by AXIOM, the “Full Image” (physical) option was greyed out as unavailable. According to the “Magnet AXIOM User Guide” (2020), Full Image extraction for Android devices only works for rooted devices, and since this device was not rooted, it was not possible for AXIOM to perform physical acquisition on it either. Since an advanced logical image from UFED was already acquired, it was futile to perform another logical acquisition using AXIOM, thus this attempt was not pursued.

Thus, the advanced logical image acquired from UFED4PC was the one used in the next stages for Examination and Analysis for the Samsung device.

2. iOS - UFED4PC has 4 imaging options for iOS devices which are Logical, Advanced Logical, Camera and Screenshot. Further, Advanced Logical acquisition has various options including File System, Full File System and Full File System (Checkm8). The iPhone (A1549) used in this study was imaged using the Full File System (Checkm8) extraction for iOS. This technique has built-in checkm8 integration, which allows forensic examiners to perform full file extractions from unlocked (known screen pass code or none

set) iOS devices without making any changes to the original file system (*Cellebrite UFED iOS - Cellebrite*, n.d.). Checkm8 is a Boot ROM exploit which, according to Yu, Zhuge, Cao, Shi, and Jiang (2020), can be considered as one of the most important exploits ever discovered for jailbreaking iOS devices.

Device Firmware Update (DFU) Mode - Prior to imaging, the iPhone needs to placed in DFU mode. This mode allows users to make low-level changes to the software running the device, and is required for successful jailbreaking (Costello, 2019). Once the device was connected to the workstation using a USB cable, and File System extraction in UFED was selected, instructions on how to place the device in DFU mode were displayed. Following them successfully placed the iPhone in DFU mode, after which the “Continue” button in UFED was enabled to carry out the actual imaging process.

UFED File System Extraction - After placing the device in DFU mode and clicking the “Continue” button, the target directory for extraction was selected and then on-screen instructions were followed for imaging. When prompted to select the data types desired to be extracted, all were selected. After a few minutes, a screen that stated extraction was complete appeared on the screen, and upon checking the selected target directory, the resultant files including a “.ufdx”, “.ufd” and “.dar” were found.

3.3.2.2 Examination This step included converting and loading a copy of the evidence, i.e., the forensic images created during Acquisition in the appropriate format using the appropriate tools. Since this study included the comparison of two tools (UFED Cellebrite and Magnet AXIOM) for examination and analysis of artifacts obtained, it was necessary to ensure that the extracted forensic images for both phones were in formats compatible with both tools.

Since UFED4PC was used as the acquisition tool, the resultant “.ufd” file was directly opened as a case using UFED Physical Analyzer. Once all the data was loaded, the entire case was then exported as a UFED report, so that it could be conveniently accessed from any device without the official Cellebrite license. This was done by clicking Generate Report in the top tab of the Physical Analyzer and selecting the UFDR option, along with the desired target directory.

This created a file in ".ufdr" format in the target directory which can be accessed using just the UFED Reader on any computer or laptop.

The procedure for creating a case file compatible with AXIOM was slightly different, since acquisition was done using a different tool. AXIOM Process was launched and a new case was created. After entering all the case details and desired target directory, the evidence source had to be selected. Since an image had already been acquired using UFED4PC, "Load Evidence" was selected, and then the type of evidence was selected as "Image". The ".dar" file previously created during Acquisition was selected as the input image, and Finish was clicked when the process was completed. Among all the output files written to the target directory, one "Case.mfdb" file was created, which is the case file format compatible with AXIOM Examine, and can be opened in it directly to analyze case data. It must be noted that during examination using AXIOM, none of the custom add-on artifacts were used to perform custom parsing of mobile applications.

These techniques for creating tool compatible case files are common for Android and iOS devices, and were performed separately for the images acquired from both devices. As discussed in the literature review, Examination also encompasses uncovering digital evidence by separating useful information from irrelevant data, so that the resulting data can be properly analyzed. For this study, this included identifying the locations and sections where GroupMe data was properly categorized by the respective tools. This has been discussed in detail for both devices below.

1. Android - The steps taken to identify useful case information for the Samsung phone using UFED Reader and AXIOM Examine will be explained in this section.

   UFED Physical Analyzer (PA) - The ".ufd" image corresponding to the Samsung device was opened using UFED PA for examination. Upon exploring the Analyzed Data and File Systems sections in tool, no direct categorization of GroupMe artifacts was found in any of their subsections. On taking a closer look under *Analyzed Data* → *Application* → *Installed Applications*, it was discovered that GroupMe was not recognized as an installed application by UFED, and consequently none of the GroupMe artifacts had been categorized as such, which meant that an investigator would not be able to directly locate and analyze them using this tool. To be thorough, the list of databases identified by the tool were examined using the built-in SQLite browser, but no GroupMe databases were found here either, which meant that an investigator would not even be able go in by hand using UFED to study the GroupMe SQLite databases.

AXIOM Examine - For examination using this tool, the ".mfdb" image file corresponding to the Samsung device used in the study was opened using AXIOM Examine. Unfortunately, just like before, no GroupMe artifacts were successfully recognized by AXIOM. All sections in artifact view including Chat, Documents, Mobile, Operating System and Refined Results were thoroughly examined, but none of them contained any artifacts identifiable as GroupMe. Thus, just like with UFED, an investigator would not be able to directly locate and analyze them using AXIOM.

It is more likely than not that the reason for this limitation is because the Samsung device could not be rooted, and thus a physical image of it could not be acquired. Advanced logical images have limitations in the amount of data they can extract from Android phones, which is probably why both, UFED as well as AXIOM were unable to recognize GroupMe as an application and failed to categorize any of its artifacts.

2. iOS - The steps taken to identify useful case information for the iPhone using UFED Reader and AXIOM Examine will be explained in this section.

   UFED Physical Analyzer (PA) - Upon opening the correct ".ufd" file associated with the iPhone in UFED PA, a preliminary examination of all subsections under the Analyzed Data section provided some information regarding GroupMe like contacts, some chats and account information. A more detailed look was taken at the *Analyzed Data* → *Application* → *Installed Applications* section, where GroupMe was present under Social Media Apps. The GroupMe icon in this section was selected, and the "Run AppGenie" option was clicked. UFED's AppGenie is a new research tool engine that is capable of recovering data from 3rd-party apps more efficiently than existing techniques. Once this module was run for GroupMe, a new subsection called Manual Data Collection appeared under Analyzed Data. This contained GroupMe data that was specifically extracted by AppGenie and had the following categorizations: Chats, Contacts, Locations, and User Accounts. On navigating to these locations, a forensic investigator would be able to further analyze the identified artifacts. The analysis of these artifacts has been discussed in Table 3.2 in the Analysis step.

AXIOM Examine - The relevant “.mfdb” file associated with the iPhone was opened through AXIOM Examine. Once the entire case was successfully loaded, it was viewed in Artifact Mode. All the relevant GroupMe related artifacts were found under the Chat section, and were classified as: GroupMe Accounts, GroupMe Groups, and GroupMe Messages.

On the surface, while this might have seemed like insufficient information in comparison to the number and type of populated items, upon analyzing them in the upcoming sections, it was discovered that this was because GroupMe had a unique way of treating some of its artifacts, and thus they have been categorized in seemingly unexpected ways.

3.3.2.3 Analysis In this step, all the artifacts identified during examination were analyzed to understand their significance to the case, and those that could potentially be used to support or disprove the hypotheses being tested by the study were recorded.

1. Android - As discussed in the examination section, neither UFED, nor AXIOM were able to find any artifacts related to and classified as GroupMe related. An investigator could attempt to manually search through database files, log files and caches to find GroupMe related artifacts, but that would be equivalent to going in by-hand to examine a raw image file. The scope of this study does not include analysis of that kind, and is limited to analysis of artifacts identified by the selected tools only.

2. iOS - Based on the preliminary data obtained from Examination, a more detailed breakdown and analysis for the iPhone was performed using UFED Reader and AXIOM Examine separately. The results obtained from each have been discussed as well as tabulated below. For every artifact recovered using these tools, the timestamp for it was also obtained.

   It was observed during analysis that both UFED and AXIOM used the unique User IDs to refer to group chat members instead of their actual names, so in order to identify the senders and receivers in every chat, first the Contacts artifacts were examined and each participant name was mapped with their unique User IDs. Similarly, each group chat also had its unique Group ID which was used by the tools to reference groups instead of their names. The User IDs and Group IDs retrieved from the iPhone by both tools have been tabulated in Appendix Table B.1.

UFED Reader Analysis - The ".ufdr" file corresponding to the iPhone was opened in UFED Reader for analysis. During Examination, several types of GroupMe data and their locations had been noted, and these were methodically analyzed in this step. As previously mentioned, certain data related to contacts, some chats and account information were found before running AppGenie on GroupMe. These were the first to be analyzed. Thereafter, all the data obtained through AppGenie was analyzed. It is important to note that there was a lot of data that was overlapping; for example, GroupMe contacts were found through AppGenie as well as without it. In general, the data obtained through AppGenie was more comprehensive and provided greater details about the artifacts discovered. For example, all 156 entries for Contacts obtained without AppGenie were completely blank or had random character strings in them, whereas the Contacts obtained through AppGenie had intelligible contact details with contact names and User IDs. For the Chats artifacts, even though the same number of unique artifacts were obtained with and without AppGenie, the latter provided the option of chat groupings. These groupings were available by Conversation IDs, Group IDs and User IDs, which could make it extremely convenient for investigators to filter through chats shared in specific groups or private conversations. The following Table 3.2 shows the source, artifact type, navigation path and artifact details of the analyzed data. The last column specifies if it was obtained through AppGenie or without.

Table 3.2. *Artifacts Recovered using UFED for iPhone*

Artifact Type	**Artifact Details**	**Extraction Source**	**Navigation Path**	**App Genie**
Contacts (156)	None of the contacts had any decipherable information. Most of the entries were blank, while others had a string of random characters in them. However, the column with the Deleted flag was checked for each one, which meant that UFED had marked all 156 of these as deleted contacts.	Database: GroupMe.sqlite Table: zgmrelationship	Analyzed Data → Contacts → GroupMe	No
Chats (9, with total 319 messages)	A total of 9 conversations were recovered which consisted of 319 messages altogether. These included all the attachments shared in the respective chats as well as messages exchanged through GroupMe SMS.	Database: GroupMe.sqlite Table: zgmmessage	Analyzed Data → Messages → Chats (Filter Source Column by GroupMe)	No
User Accounts (1)	The correct email address and mobile number associated with the GroupMe account were recovered, as well as the current name on the account. A unique User ID (91976822) for the account owner was also discovered.	Plist file at: com.groupme. iphone-app.plist	Analyzed Data → User Accounts & Details → User Accounts (Filter Source Column by GroupMe)	No
Chats (51, with total 641 messages)	AppGenie had created separate groupings of chats for easier filtering, which was why such a seemingly high number of messages of visible. Groupings were available by Conversation IDs, Group IDs and User IDs. All the data that was obtained through chats discussed above was present here as well. Additionally, the unique User IDs of all other participating members were also obtained.	Cache file at: Library/Caches/ com.groupme. iphone-app/ Cache.db	Analyzed Data → Manual Data Collection → Chats	Yes

Contacts (27)	A total of 27 contacts along with their unique User IDs were discovered, out of which 15 were duplicates. The reason for some contacts appearing more than once was that they were being pulled from 2 different database tables.	Database: GroupMe.sqlite -wal Tables: zgmmember, zgmrelationship	Analyzed Data → Manual Data Collection → Contacts	Yes
Locations (131)	This contained the location coordinates that were recorded from where the GroupMe app had been opened and used.	Cache file at: Library/Caches/ com.groupme. iphone-app/	Analyzed Data → Manual Data Collection → Locations	Yes
User Accounts (1)	The correct email address and mobile number associated with the GroupMe account were recovered, along with the name associated with the account. The same User ID (91976822) for the account owner as found before was also discovered.	Database: GroupMe.sqlite -wal Table: zgmrelationship	Analyzed Data → Manual Data Collection → User Accounts	Yes
GroupMe SMS	All messages exchanged in the group created via GroupMe SMS were obtained as native text messages as well.	DarArchive/root/ private/var/ mobile/Library/ SMS/sms.db-wal	Analyzed Data → Messages → Chats (Filter Source Column by Native Messages)	No

On analyzing all of the artifacts in the aforementioned table, it was discovered that GroupMe was storing its data and artifacts in a manner different from what was expected by the author. While populating data, it was expected that the text messages, media items, documents, polls, integrated videos, shared locations, calendar events, memes and Skype calls would be treated as separate types of artifacts. In reality, however, GroupMe treats them all as simple text artifacts shared through chats. Moreover, logs of new members joining a group chat, members accepting or rejecting calendar invites, responding to polls, calendar events beginning and ending, and members exiting groups were also found as "System Events" in the form of messages in their respective chats. However, upon opening up the "GroupMe.sqlite" database using the built in database viewer, it was found that there was also a table called "zgmattachment" which had a column named "ztype", that flagged each entry as either File, Location, Image, Video, Event or Poll. By cross-referencing the value in the “zmessage” column for each entry with the “message #” column under the Chats category mentioned in Table 3.2, an investigator can verify if the message sent was actually a location, file, media item, poll or calendar event.

Yet, under artifact view, UFED had displayed all of these artifacts under the Chats category, and then provided a URL to open each one to view in detail in a web browser. This was why more than the expected count (250) of text messages were found. Out of the 319 messages recovered from *Analyzed Data* $\rightarrow$ *Messages* $\rightarrow$ *Chats*, only 250 were actual text messages, and the others were messages containing URLs to the other types of artifacts which were just discussed. The exact same thing was observed for the messages found through AppGenie. As explained in the table, chats found through AppGenie were grouped into various categories, causing duplicates. The category grouped by User IDs was identified as the one containing all the text messages, related artifacts and system events, and had exactly 319 messages in it, which was the same as chats recovered without AppGenie.

To find evidence of new groups created by the user, the category of AppGenie chats grouped by Group IDs was examined. This contained entries for all the groups the user was a member of, including those created using GroupMe SMS, along with specific details like the unique User ID of the group creator, User IDs of members, etc. By filtering the “ID” column by the user’s unique User ID, all the groups created by them were obtained. This included groups they may have created or joined in Campus Connect as well.

Evidence of messages exchanged through GroupMe SMS were found in Chats as well as native text messages. No logs of messages being “liked” by the user was discovered in any of the text artifacts. Further, no evidence of any chats or individual messages being hidden or unhidden could be found using UFED.

Since the contacts obtained without AppGenie were empty and marked as Deleted, they were ignored. Only the contacts obtained through AppGenie were considered in analysis. 12 unique contacts were found, which were more than the expected number (5). Upon analysis, it was discovered that the reason for this was that GroupMe does not consider only contacts explicitly added by the user as “contacts”. Every member that was present in any group that the user had been in was counted as a “contact” by GroupMe, which is why 12 unique contacts were discovered. No logs or flags to prove that any contact was blocked by the user was found in any of the contacts artifacts.

As explained in the User Accounts row in the table above, the name of the user that was recovered was the most recent name set in the app for the user. No evidence for any previous names used before changing it to the present one was found. Additionally, no logs for in-app searches performed by the user were found.

AXIOM Examine Analysis - The ".mfdb" file created previously was loaded using AXIOM Examine for detailed analysis. All the previously identified artifact types from the Examination step were analyzed during this step. Table 3.3 provides concise details regarding each one, with more detailed explanations below the table.

Table 3.3. *Artifacts Recovered using AXIOM for iPhone*

Artifact Type	**Artifact Details**	**Extraction Source**	**Navigation Path**
Contacts (5)	A total of 5 contacts along with their respective unique User IDs were found.	Database: GroupMe.sqlite Table: zgmrelationship	Artifacts View → Chat → GroupMe Contacts
Chats (319 messages)	A total of 319 messages were recovered. These included all the attachments shared in the respective chats as well as messages exchanged through the GroupMe SMS feature.	Database: GroupMe.sqlite Tables: zgmmessage, zgmchat	Artifacts View → Chat → GroupMe Messages
User Accounts (1)	The correct email address and mobile number associated with the GroupMe account were recovered, along with the name associated with the account. A unique User ID (91976822) for the account owner was also discovered.	Plist file at: com.groupme. iphone-app.plist	Artifacts View → Chat → GroupMe Accounts
Groups (4)	A list of all the groups that the user is currently a member of was found with all the details including unique Groups IDs, date and time of creation, and User IDs of all its members.	Database: GroupMe.sqlite Tables: zgmmember, zgmchat	Artifacts View → Chat → GroupMe Groups

GroupMe SMS	All messages exchanged in the group created via GroupMe SMS were found as native text messages as well.	Database: sms.db-wal	Artifacts View → Chat → iOS iMessage/SMS

It was now already known that GroupMe considers media items, documents, polls, shared locations, integrated videos, calendar events, memes and Skype calls as text artifacts. Just like UFED, AXIOM also stores logs of new members joining a group chat, members accepting or rejecting calendar invites, responding to polls, calendar events beginning and ending, and members exiting groups as system events in the form of messages in their respective chats. Thus, of the 319 chat messages discovered using this tool, exactly 250 were the actually intended text messages, and the remaining 69 belonged to the other types of data that have just been discussed.

Upon navigating to *Artifacts View → Chat → GroupMe Groups*, all the groups that the user was a member of, including groups in Campus Connect as well as GroupMe SMS were found. Each one contained details regarding the User ID of the group creator, User IDs of members, and date and time of creation. By filtering the “Creator ID” column by the user’s unique User ID, all the groups created by them were obtained. It is important to note that only the groups that the user was presently a part of were found, not any groups that they may have potentially been a part of and then exited.

Very similarly to what was found in UFED, evidence of messages exchanged through GroupMe SMS were found in Chats as well as native iOS text messages. No logs of “liked” messages, or chats and individual messages being hidden or unhidden were found either.

AXIOM extracted all contacts that had been added by the user along with their respective User IDs. Unlike UFED, it did not consider all group members present in groups that the member is a part of as contacts. No logs or flags to prove that any contact was blocked by the user was found in any of the contacts artifacts.

Although all the correct user account information including email address and mobile number were discovered, the name on the account was the most recent one set in the app for the user. No evidence for any previous names, or logs for in-app searches performed by the user were found.

3.3.2.4 Reporting This step included consolidating the analysis and comparing the results obtained from various sources with the expected results. The accuracy of tools used on the iPhone was also calculated, whereas reliability was only theoretically discussed. The details of whether the hypotheses were supported or rejected, as well as screenshots of all obtained artifacts are discussed in the next chapter, which is Results.

3.4 Summary

This chapter provided the detailed methodology which was followed for the research study along with stating its hypotheses. Elaborate flow charts to visualize the methodology phases have also been included. Apart from providing the hardware and software specifications of the environment and tools which were used, this chapter included the systematic examination and analysis of the artifacts recovered during the study.

CHAPTER 4. RESULTS

This chapter provided screenshots and further details of the analysis discussed previously. Each of the hypotheses being tested by the study were also discussed to check whether they were supported by these results or not.

4.1 Hypothesis One

The first hypothesis stated that the accuracy of recovered artifacts using UFED and AXIOM would be the same on the Android device. This hypothesis could not be tested since both, UFED Physical Analyzer as well as Axiom Examine were unable to find any GroupMe related artifacts from the advanced logical image created by UFED4PC. For the hypothesis to be proven or disproved, comparison of artifacts acquired from a physical image of the Samsung phone would be required.

4.2 Hypothesis Two

The second hypothesis stated that the accuracy of recovered artifacts using UFED and AXIOM would be the same on the iOS device. The following Table 4.1 presents a summary of the artifacts found from the iPhone using both AXIOM and UFED.

Table 4.1. *Artifact Comparison for UFED and AXIOM for iPhone*

Artifact	Recovered		Expected
	UFED	AXIOM	
Text Messages	250	250	250
Media Items	15	15	15
Integrated Videos	5	5	5
Liked Messages	0	0	20
Shared Locations	4	4	4
Documents	20	20	20

Contacts	12	5	5
New Group Creation	1	1	1
Exiting Group	1	1	1
Polls	2	2	2
Calendar Events	2	2	2
Memes	4	4	4
Skype Call Invites	2	2	2
Searches	0	0	2
GroupMe SMS	3	3	3
Hidden Messages	0	0	1
Hidden Chats	0	0	2
Unhiding Chats	0	0	1
Editing Personal Info	0	0	1
Campus Connect	3	3	3
Total	324	317	335

Even though their methods of presenting information was extremely different from each other, UFED and AXIOM were able to recover almost the same number of artifacts. The table above has been organized according to the types of artifacts expected by the researchers during data population. As we have discussed during the analysis, GroupMe actually had a different way of storing these artifacts. It was observed that the total number of artifacts recovered from UFED was higher than that of AXIOM (observe Contacts), but AXIOM was actually more successful in identifying the contacts correctly. Only 5 new contacts were added during data population, but UFED recovered 12, which included all group members that the user was in a group with, even if they were not added as contacts, whereas AXIOM recovered only the expected 5. This could be significant to a case during an investigation since if a particular group member in a chat that the user is a member of were to commit any illegal activities, UFED might report this person as a Contact, even if they were not. This could result in the user coming under suspicion for being friends with the perpetrator, even if they did not even personally know them.

- Accuracy: This was calculated as a percentage of the number of artifacts correctly recovered using the tool over the number of expected artifacts. Since the number of contacts correctly identified by UFED were also 5, the total number of correctly recovered artifacts by both tools were approximately equal, (i.e. 317/335). Thus, this hypothesis was successfully supported by this study.

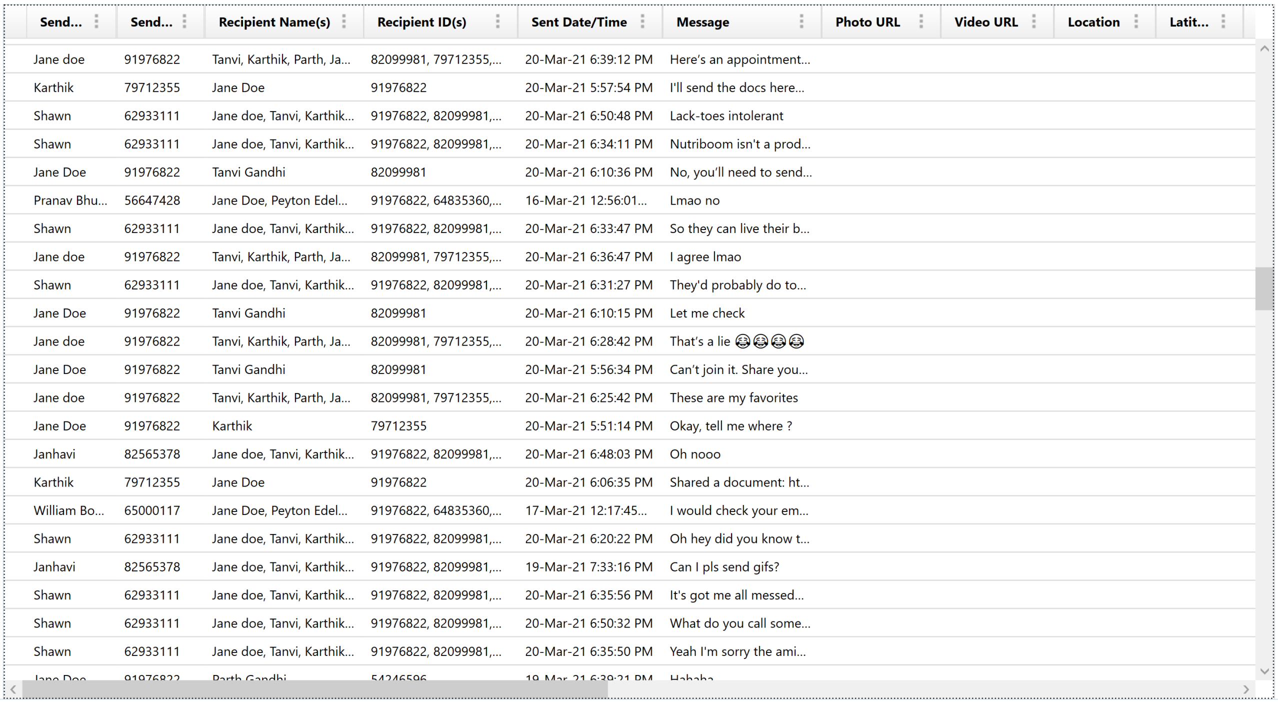
  AXIOM Accuracy: 94.62%
  UFED Accuracy: 94.62%

- Reliability: This would ideally be calculated as a measure of the number of artifacts each tool could correct identify more than once. This would require several repetitions of the entire methodology, which was not possible given the time constraint, thus the reliability of the tools was not calculated during this study.

Based on the data in Table 4.1, screenshots of artifacts obtained from both tools for the iPhone are provided below. AXIOM provides a view in which all text artifacts are present together without any grouping, thus, upon filtering specific columns, it was possible to record screenshots of all the populated artifacts with the accurate number of each. However, UFED groups text artifacts by the chats/conversations they were a part of, so it was not possible to take screenshots of all similar types of artifacts together by filtering. Thus, all the UFED screen captures provided below contain some of the artifacts, but not all that had been recovered.

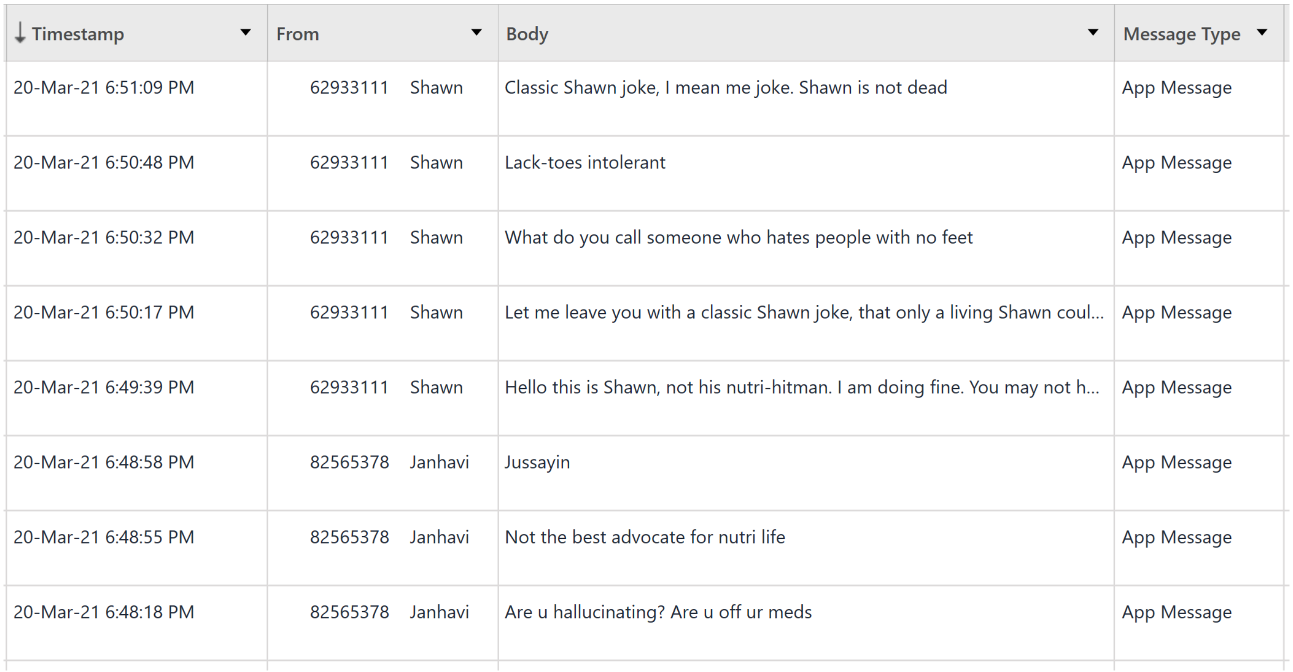
4.2.1 Text Artifacts

Text artifacts include text messages, media items, polls, integrated videos, shared locations, documents, calendar events, memes, Skype calls. They also include System Events like logs of new members joining a group chat, members accepting or rejecting calendar invites, responding to polls,calendar events beginning and ending, and members exiting groups.
Figure 4.1 and Figure 4.2 show how text messages were being displayed by AXIOM and UFED respectively. AXIOM has special flags to denote if the artifact is a message, photo, video or shared location.



Send...	Send...	Recipient Name(s)	Recipient ID(s)	Sent Date/Time	Message	Photo URL	Video URL	Location	Latit...
Jane doe	91976822	Tanvi, Karthik, Parth, Ja...	82099981, 79712355,...	20-Mar-21 6:39:12 PM	Here's an appointment...				
Karthik	79712355	Jane Doe	91976822	20-Mar-21 5:57:54 PM	I'll send the docs here...				
Shawn	62933111	Jane doe, Tanvi, Karthik...	91976822, 82099981,...	20-Mar-21 6:50:48 PM	Lack-toes intolerant				
Shawn	62933111	Jane doe, Tanvi, Karthik...	91976822, 82099981,...	20-Mar-21 6:34:11 PM	Nutriboom isn't a prod...				
Jane Doe	91976822	Tanvi Gandhi	82099981	20-Mar-21 6:10:36 PM	No, you'll need to send...				
Pranav Bhu...	56647428	Jane Doe, Peyton Edel...	91976822, 64835360,...	16-Mar-21 12:56:01...	Lmao no				
Shawn	62933111	Jane doe, Tanvi, Karthik...	91976822, 82099981,...	20-Mar-21 6:33:47 PM	So they can live their b...				
Jane doe	91976822	Tanvi, Karthik, Parth, Ja...	82099981, 79712355,...	20-Mar-21 6:36:47 PM	I agree lmao				
Shawn	62933111	Jane doe, Tanvi, Karthik...	91976822, 82099981,...	20-Mar-21 6:31:27 PM	They'd probably do to...				
Jane Doe	91976822	Tanvi Gandhi	82099981	20-Mar-21 6:10:15 PM	Let me check				
Jane doe	91976822	Tanvi, Karthik, Parth, Ja...	82099981, 79712355,...	20-Mar-21 6:28:42 PM	That's a lie 😂😂😂😂				
Jane Doe	91976822	Tanvi Gandhi	82099981	20-Mar-21 5:56:34 PM	Can't join it. Share you...				
Jane doe	91976822	Tanvi, Karthik, Parth, Ja...	82099981, 79712355,...	20-Mar-21 6:25:42 PM	These are my favorites				
Jane Doe	91976822	Karthik	79712355	20-Mar-21 5:51:14 PM	Okay, tell me where ?				
Janhavi	82565378	Jane doe, Tanvi, Karthik...	91976822, 82099981,...	20-Mar-21 6:48:03 PM	Oh nooo				
Karthik	79712355	Jane Doe	91976822	20-Mar-21 6:06:35 PM	Shared a document: ht...				
William Bo...	65000117	Jane Doe, Peyton Edel...	91976822, 64835360,...	17-Mar-21 12:17:45...	I would check your em...				
Shawn	62933111	Jane doe, Tanvi, Karthik...	91976822, 82099981,...	20-Mar-21 6:20:22 PM	Oh hey did you know t...				
Janhavi	82565378	Jane doe, Tanvi, Karthik...	91976822, 82099981,...	19-Mar-21 7:33:16 PM	Can I pls send gifs?				
Shawn	62933111	Jane doe, Tanvi, Karthik...	91976822, 82099981,...	20-Mar-21 6:35:56 PM	It's got me all messed...				
Shawn	62933111	Jane doe, Tanvi, Karthik...	91976822, 82099981,...	20-Mar-21 6:50:32 PM	What do you call some...				
Shawn	62933111	Jane doe, Tanvi, Karthik...	91976822, 82099981,...	20-Mar-21 6:35:50 PM	Yeah I'm sorry the ami...				
Jane Doe	91976822	Parth Gandhi	54246596	19-Mar-21 6:39:21 PM	Hahaha				

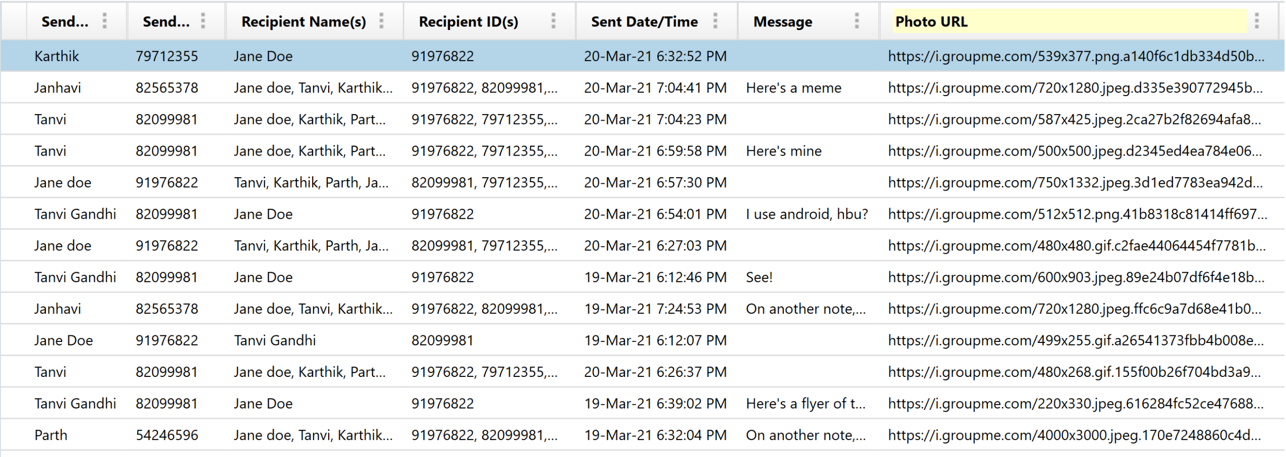
Figure 4.1. Text Messages from AXIOM



↓ Timestamp	From	Body	Message Type
20-Mar-21 6:51:09 PM	62933111 Shawn	Classic Shawn joke, I mean me joke. Shawn is not dead	App Message
20-Mar-21 6:50:48 PM	62933111 Shawn	Lack-toes intolerant	App Message
20-Mar-21 6:50:32 PM	62933111 Shawn	What do you call someone who hates people with no feet	App Message
20-Mar-21 6:50:17 PM	62933111 Shawn	Let me leave you with a classic Shawn joke, that only a living Shawn coul...	App Message
20-Mar-21 6:49:39 PM	62933111 Shawn	Hello this is Shawn, not his nutri-hitman. I am doing fine. You may not h...	App Message
20-Mar-21 6:48:58 PM	82565378 Janhavi	Jussayin	App Message
20-Mar-21 6:48:55 PM	82565378 Janhavi	Not the best advocate for nutri life	App Message
20-Mar-21 6:48:18 PM	82565378 Janhavi	Are u hallucinating? Are u off ur meds	App Message

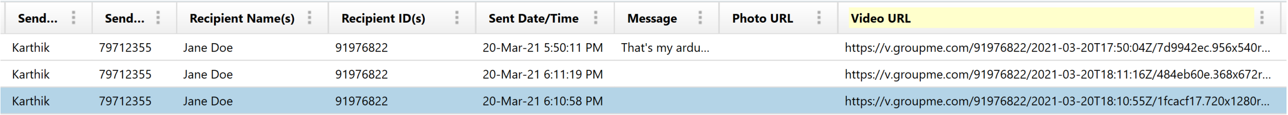
Figure 4.2. Text Messages from UFED

Figure 4.3 shows all 9 images as well as 4 memes that were recovered using AXIOM, and Figure 4.4 shows the 3 videos recovered from the chats. Figure 4.5 on the other hand, shows one example of how media items are displayed by UFED. On selecting the particular artifact, a side panel opens with a URL to the relevant item.



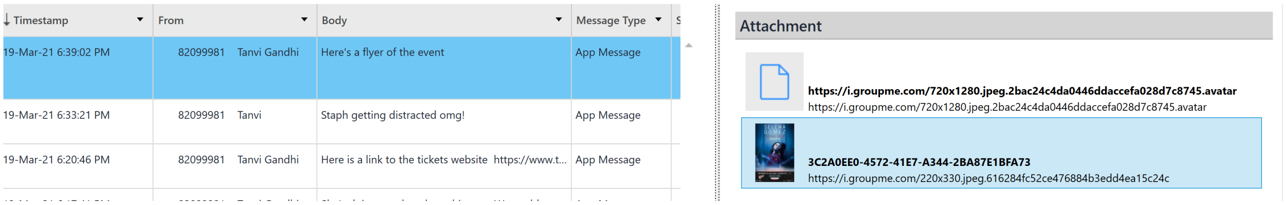
Send...	Send...	Recipient Name(s)	Recipient ID(s)	Sent Date/Time	Message	Photo URL
Karthik	79712355	Jane Doe	91976822	20-Mar-21 6:32:52 PM		https://i.groupme.com/539x377.png.a140f6c1db334d50b...
Janhavi	82565378	Jane doe, Tanvi, Karthik...	91976822, 82099981,...	20-Mar-21 7:04:41 PM	Here's a meme	https://i.groupme.com/720x1280.jpeg.d335e390772945b...
Tanvi	82099981	Jane doe, Karthik, Part...	91976822, 79712355,...	20-Mar-21 7:04:23 PM		https://i.groupme.com/587x425.jpeg.2ca27b2f82694afa8...
Tanvi	82099981	Jane doe, Karthik, Part...	91976822, 79712355,...	20-Mar-21 6:59:58 PM	Here's mine	https://i.groupme.com/500x500.jpeg.d2345ed4ea784e06...
Jane doe	91976822	Tanvi, Karthik, Parth, Ja...	82099981, 79712355,...	20-Mar-21 6:57:30 PM		https://i.groupme.com/750x1332.jpeg.3d1ed7783ea942d...
Tanvi Gandhi	82099981	Jane Doe	91976822	20-Mar-21 6:54:01 PM	I use android, hbu?	https://i.groupme.com/512x512.png.41b8318c81414ff697...
Jane doe	91976822	Tanvi, Karthik, Parth, Ja...	82099981, 79712355,...	20-Mar-21 6:27:03 PM		https://i.groupme.com/480x480.gif.c2fae44064454f7781b...
Tanvi Gandhi	82099981	Jane Doe	91976822	19-Mar-21 6:12:46 PM	See!	https://i.groupme.com/600x903.jpeg.89e24b07df6f4e18b...
Janhavi	82565378	Jane doe, Tanvi, Karthik...	91976822, 82099981,...	19-Mar-21 7:24:53 PM	On another note,...	https://i.groupme.com/720x1280.jpeg.ffc6c9a7d68e41b0...
Jane Doe	91976822	Tanvi Gandhi	82099981	19-Mar-21 6:12:07 PM		https://i.groupme.com/499x255.gif.a26541373fbb4b008e...
Tanvi	82099981	Jane doe, Karthik, Part...	91976822, 79712355,...	20-Mar-21 6:26:37 PM		https://i.groupme.com/480x268.gif.155f00b26f704bd3a9...
Tanvi Gandhi	82099981	Jane Doe	91976822	19-Mar-21 6:39:02 PM	Here's a flyer of t...	https://i.groupme.com/220x330.jpeg.616284fc52ce47688...
Parth	54246596	Jane doe, Tanvi, Karthik...	91976822, 82099981,...	19-Mar-21 6:32:04 PM	On another note,...	https://i.groupme.com/4000x3000.jpeg.170e7248860c4d...

Figure 4.3. Media Items (Images) and Memes from AXIOM



Send...	Send...	Recipient Name(s)	Recipient ID(s)	Sent Date/Time	Message	Photo URL	Video URL
Karthik	79712355	Jane Doe	91976822	20-Mar-21 5:50:11 PM	That's my ardu...		https://v.groupme.com/91976822/2021-03-20T17:50:04Z/7d9942ec.956x540r...
Karthik	79712355	Jane Doe	91976822	20-Mar-21 6:11:19 PM			https://v.groupme.com/91976822/2021-03-20T18:11:16Z/484eb60e.368x672r...
Karthik	79712355	Jane Doe	91976822	20-Mar-21 6:10:58 PM			https://v.groupme.com/91976822/2021-03-20T18:10:55Z/1fcacf17.720x1280r...

Figure 4.4. Media Items (Videos) from AXIOM



Timestamp	From	Body	Message Type
19-Mar-21 6:39:02 PM	82099981 Tanvi Gandhi	Here's a flyer of the event	App Message
19-Mar-21 6:33:21 PM	82099981 Tanvi	Staph getting distracted omg!	App Message
19-Mar-21 6:20:46 PM	82099981 Tanvi Gandhi	Here is a link to the tickets website https://www.t...	App Message

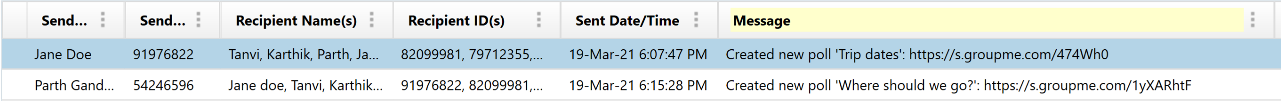
Attachment

https://i.groupme.com/720x1280.jpeg.2bac24c4da0446ddaccefa028d7c8745.avatar
https://i.groupme.com/720x1280.jpeg.2bac24c4da0446ddaccefa028d7c8745.avatar

3C2A0EE0-4572-41E7-A344-2BA87E1BFA73
https://i.groupme.com/220x330.jpeg.616284fc52ce476884b3edd4ea15c24c

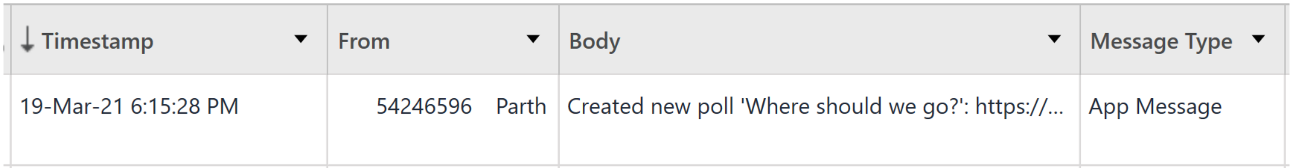
Figure 4.5. Media Items from UFED

In Figure 4.6, we can see the creator and recipient details, as well as title of both the polls created during data population. Similarly, Figure 4.7 shows an example of one of the polls created during data population retrieved by UFED.



Send...	Send...	Recipient Name(s)	Recipient ID(s)	Sent Date/Time	Message
Jane Doe	91976822	Tanvi, Karthik, Parth, Ja...	82099981, 79712355,...	19-Mar-21 6:07:47 PM	Created new poll 'Trip dates': https://s.groupme.com/474Wh0
Parth Gand...	54246596	Jane doe, Tanvi, Karthik...	91976822, 82099981,...	19-Mar-21 6:15:28 PM	Created new poll 'Where should we go?': https://s.groupme.com/1yXARhtF

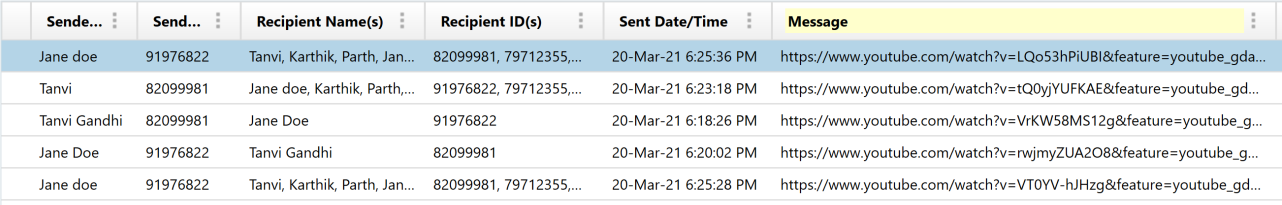
Figure 4.6. Polls from AXIOM



↓ Timestamp	From	Body	Message Type
19-Mar-21 6:15:28 PM	54246596 Parth	Created new poll 'Where should we go?': https://...	App Message

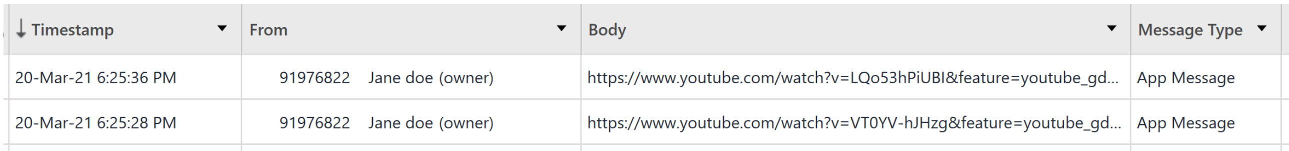
Figure 4.7. Polls from UFED

Figure 4.8 and Figure 4.9 provide details about the YouTube links shared in the chats recovered by AXIOM and UFED respectively. Again, despite having recovered all 5, only a few examples of the artifact recovered by UFED are displayed since it was not possible to filter out the specific artifacts due their groupings.



Sende...	Send...	Recipient Name(s)	Recipient ID(s)	Sent Date/Time	Message
Jane doe	91976822	Tanvi, Karthik, Parth, Jan...	82099981, 79712355,...	20-Mar-21 6:25:36 PM	https://www.youtube.com/watch?v=LQo53hPiUBI&feature=youtube_gda...
Tanvi	82099981	Jane doe, Karthik, Parth,...	91976822, 79712355,...	20-Mar-21 6:23:18 PM	https://www.youtube.com/watch?v=tQ0yjYUFKAE&feature=youtube_gd...
Tanvi Gandhi	82099981	Jane Doe	91976822	20-Mar-21 6:18:26 PM	https://www.youtube.com/watch?v=VrKW58MS12g&feature=youtube_g...
Jane Doe	91976822	Tanvi Gandhi	82099981	20-Mar-21 6:20:02 PM	https://www.youtube.com/watch?v=rwjmyZUA2O8&feature=youtube_g...
Jane doe	91976822	Tanvi, Karthik, Parth, Jan...	82099981, 79712355,...	20-Mar-21 6:25:28 PM	https://www.youtube.com/watch?v=VT0YV-hJHzg&feature=youtube_gd...

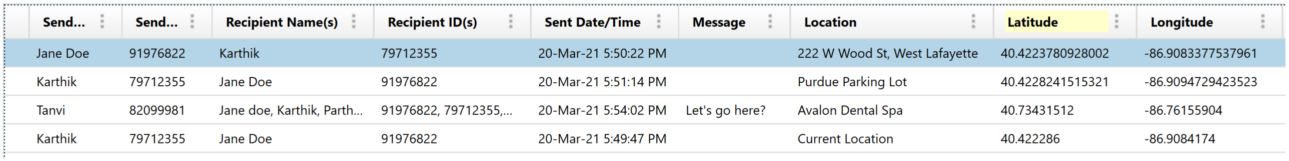
Figure 4.8. Integrated YouTube Video Links from AXIOM



↓ Timestamp	From	Body	Message Type
20-Mar-21 6:25:36 PM	91976822 Jane doe (owner)	https://www.youtube.com/watch?v=LQo53hPiUBI&feature=youtube_gd...	App Message
20-Mar-21 6:25:28 PM	91976822 Jane doe (owner)	https://www.youtube.com/watch?v=VT0YV-hJHzg&feature=youtube_gd...	App Message

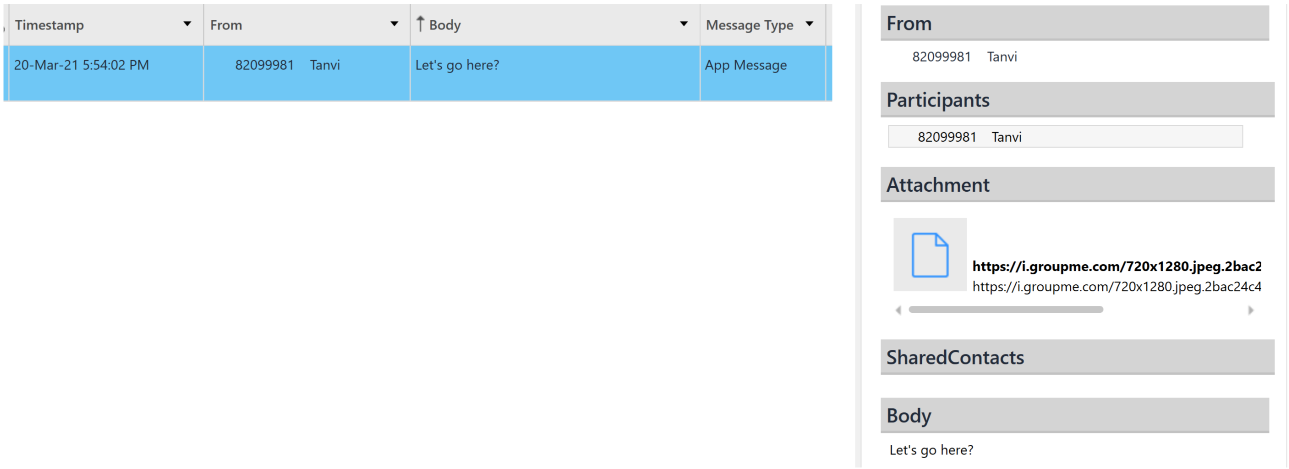
Figure 4.9. Integrated YouTube Video Links from UFED

Figure 4.10 shows all 4 of the shared locations that were recovered using AXIOM, and Figure 4.11 on the other hand, shows one example of how shared locations are displayed by UFED. Upon selecting the particular artifact, a side panel opens with a URL to the relevant item as shown in the screenshot.



Send...	Send...	Recipient Name(s)	Recipient ID(s)	Sent Date/Time	Message	Location	Latitude	Longitude
Jane Doe	91976822	Karthik	79712355	20-Mar-21 5:50:22 PM		222 W Wood St, West Lafayette	40.4223780928002	-86.9083377537961
Karthik	79712355	Jane Doe	91976822	20-Mar-21 5:51:14 PM		Purdue Parking Lot	40.4228241515321	-86.9094729423523
Tanvi	82099981	Jane doe, Karthik, Parth...	91976822, 79712355,...	20-Mar-21 5:54:02 PM	Let's go here?	Avalon Dental Spa	40.73431512	-86.76155904
Karthik	79712355	Jane Doe	91976822	20-Mar-21 5:49:47 PM		Current Location	40.422286	-86.9084174

Figure 4.10. Shared Locations from AXIOM



Timestamp	From	Body	Message Type
20-Mar-21 5:54:02 PM	82099981 Tanvi	Let's go here?	App Message

From

82099981 Tanvi

Participants

82099981 Tanvi

Attachment

https://i.groupme.com/720x1280.jpeg.2bac2
https://i.groupme.com/720x1280.jpeg.2bac24c4

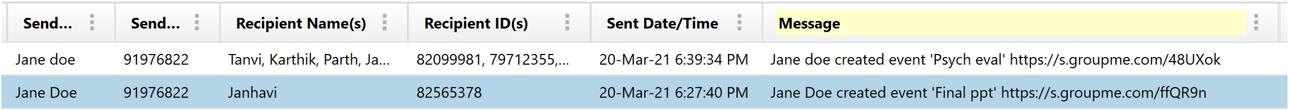
SharedContacts

Body

Let's go here?

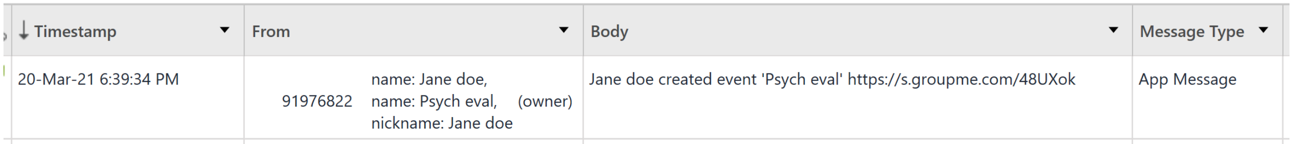
Figure 4.11. Shared Locations from UFED

Similarly to the shared location artifacts, an example of UFED displaying a calendar event is shown in Figure 4.13, whereas details of both calendar events recovered by AXIOM are illustrated in Figure 4.12.



Send...	Send...	Recipient Name(s)	Recipient ID(s)	Sent Date/Time	Message
Jane doe	91976822	Tanvi, Karthik, Parth, Ja...	82099981, 79712355,...	20-Mar-21 6:39:34 PM	Jane doe created event 'Psych eval' https://s.groupme.com/48UXok
Jane Doe	91976822	Janhavi	82565378	20-Mar-21 6:27:40 PM	Jane Doe created event 'Final ppt' https://s.groupme.com/ffQR9n

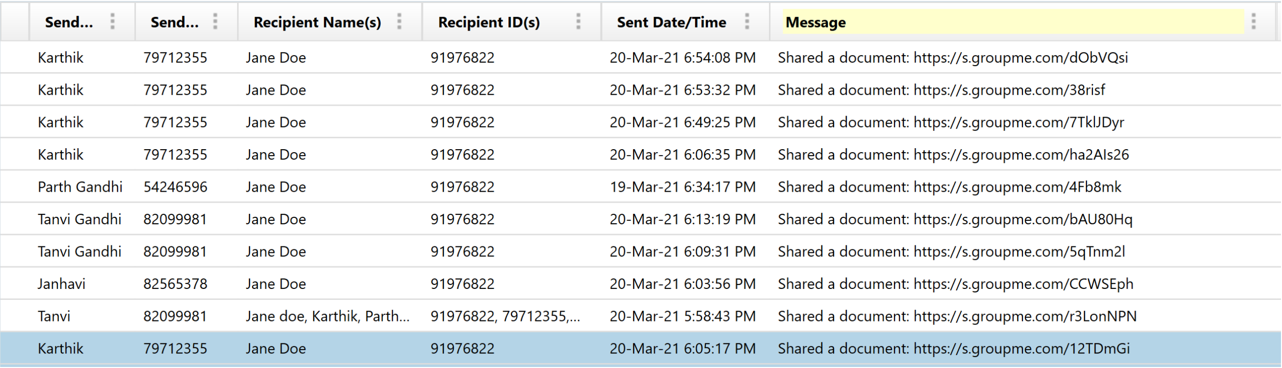
Figure 4.12. Calendar Events from AXIOM



Timestamp	From	Body	Message Type
20-Mar-21 6:39:34 PM	91976822 name: Jane doe, name: Psych eval, (owner) nickname: Jane doe	Jane doe created event 'Psych eval' https://s.groupme.com/48UXok	App Message

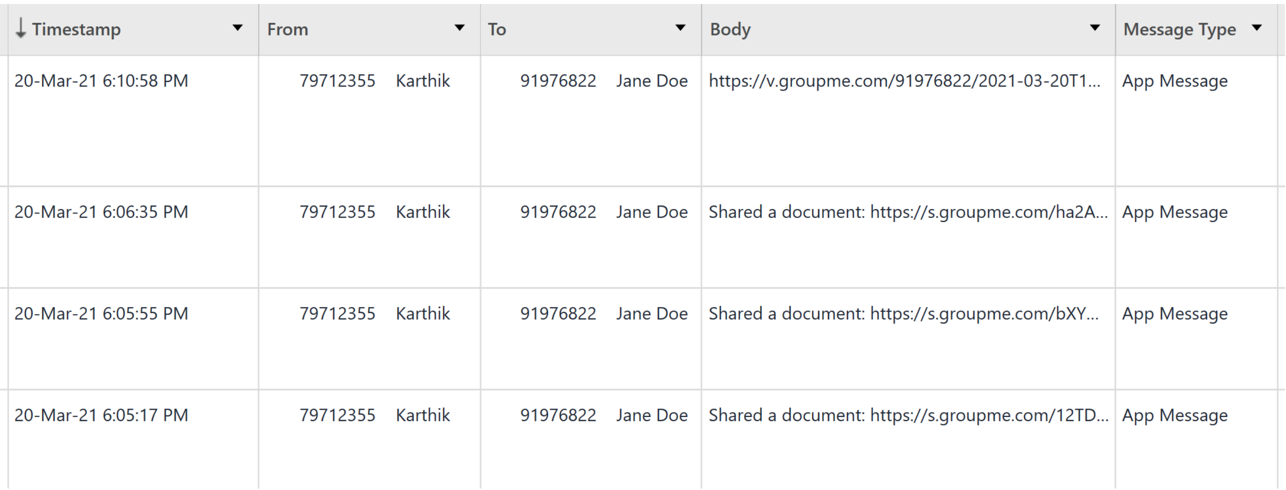
Figure 4.13. Calendar Events from UFED

All the documents recovered through AXIOM are displayed in Figure 4.14, and some of the documents recovered through UFED are similarly displayed in Figure 4.15.



Send...	Send...	Recipient Name(s)	Recipient ID(s)	Sent Date/Time	Message
Karthik	79712355	Jane Doe	91976822	20-Mar-21 6:54:08 PM	Shared a document: https://s.groupme.com/dObVQsi
Karthik	79712355	Jane Doe	91976822	20-Mar-21 6:53:32 PM	Shared a document: https://s.groupme.com/38risf
Karthik	79712355	Jane Doe	91976822	20-Mar-21 6:49:25 PM	Shared a document: https://s.groupme.com/7TklJDyr
Karthik	79712355	Jane Doe	91976822	20-Mar-21 6:06:35 PM	Shared a document: https://s.groupme.com/ha2AIs26
Parth Gandhi	54246596	Jane Doe	91976822	19-Mar-21 6:34:17 PM	Shared a document: https://s.groupme.com/4Fb8mk
Tanvi Gandhi	82099981	Jane Doe	91976822	20-Mar-21 6:13:19 PM	Shared a document: https://s.groupme.com/bAU80Hq
Tanvi Gandhi	82099981	Jane Doe	91976822	20-Mar-21 6:09:31 PM	Shared a document: https://s.groupme.com/5qTnm2l
Janhavi	82565378	Jane Doe	91976822	20-Mar-21 6:03:56 PM	Shared a document: https://s.groupme.com/CCWSEph
Tanvi	82099981	Jane doe, Karthik, Parth...	91976822, 79712355,...	20-Mar-21 5:58:43 PM	Shared a document: https://s.groupme.com/r3LonNPN
Karthik	79712355	Jane Doe	91976822	20-Mar-21 6:05:17 PM	Shared a document: https://s.groupme.com/12TDmGi

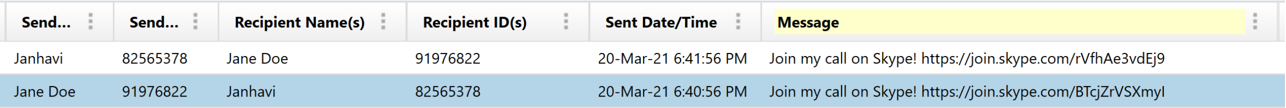
Figure 4.14. Documents from AXIOM



↓ Timestamp	From	To	Body	Message Type
20-Mar-21 6:10:58 PM	79712355 Karthik	91976822 Jane Doe	https://v.groupme.com/91976822/2021-03-20T1...	App Message
20-Mar-21 6:06:35 PM	79712355 Karthik	91976822 Jane Doe	Shared a document: https://s.groupme.com/ha2A...	App Message
20-Mar-21 6:05:55 PM	79712355 Karthik	91976822 Jane Doe	Shared a document: https://s.groupme.com/bXY...	App Message
20-Mar-21 6:05:17 PM	79712355 Karthik	91976822 Jane Doe	Shared a document: https://s.groupme.com/12TD...	App Message

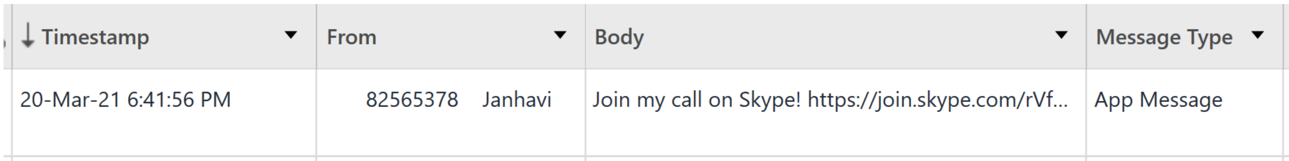
Figure 4.15. Documents from UFED

Artifacts showing the Skype call invites shared through chats on the iPhone recovered by AXIOM and UFED are shown in Figure 4.16 and Figure 4.17 respectively.



Send...	Send...	Recipient Name(s)	Recipient ID(s)	Sent Date/Time	Message
Janhavi	82565378	Jane Doe	91976822	20-Mar-21 6:41:56 PM	Join my call on Skype! https://join.skype.com/rVfhAe3vdEj9
Jane Doe	91976822	Janhavi	82565378	20-Mar-21 6:40:56 PM	Join my call on Skype! https://join.skype.com/BTcjZrVSXmyl

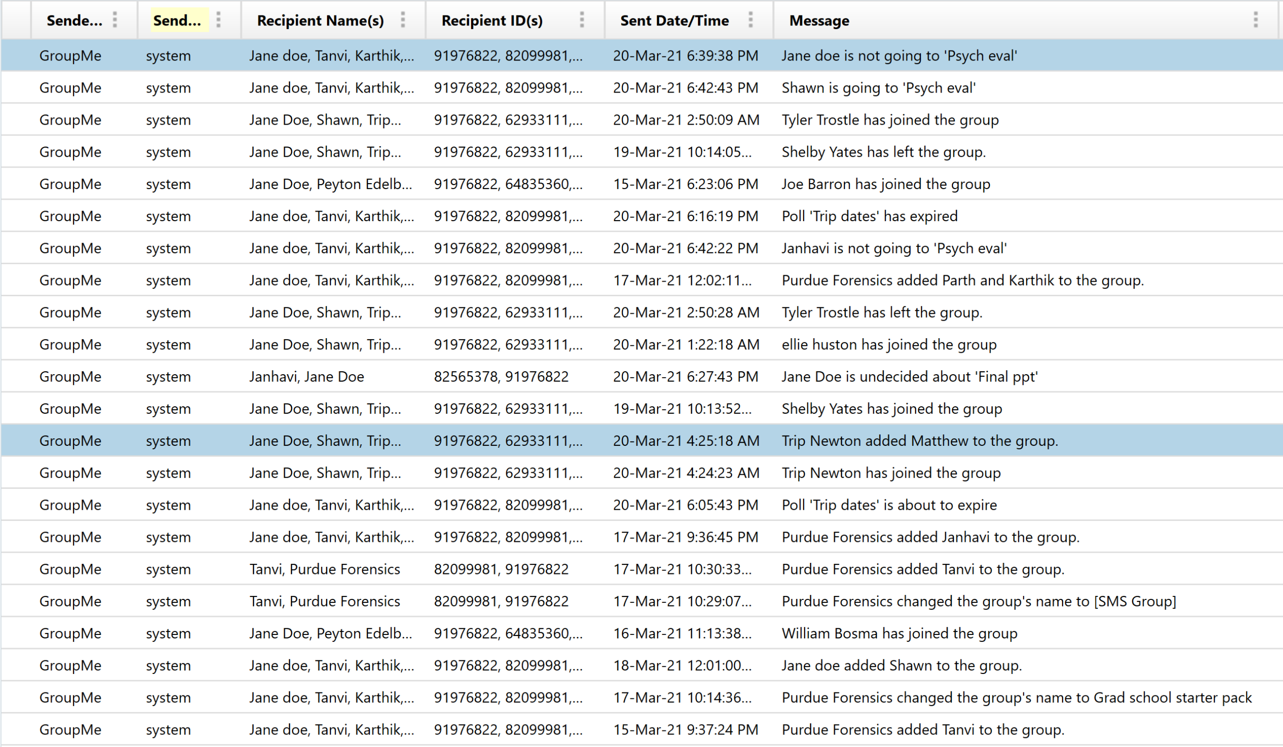
Figure 4.16. Skype Call Invite from AXIOM



↓ Timestamp	From	Body	Message Type
20-Mar-21 6:41:56 PM	82565378 Janhavi	Join my call on Skype! https://join.skype.com/rVf...	App Message

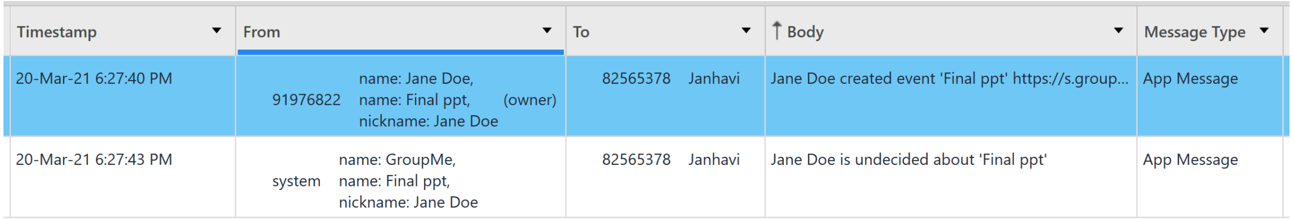
Figure 4.17. Skype Call Invite from UFED

Finally, some of the system events generated by GroupMe that include logs of new members joining a group chat, members accepting or rejecting calendar invites, responding to polls, calendar events beginning and ending, and members exiting groups that were recovered by AXIOM are shown in Figure 4.18. In a similar fashion, some of the system events retrieved by UFED are shown in Figure 4.19.



Sende...	Send...	Recipient Name(s)	Recipient ID(s)	Sent Date/Time	Message
GroupMe	system	Jane doe, Tanvi, Karthik,...	91976822, 82099981,...	20-Mar-21 6:39:38 PM	Jane doe is not going to 'Psych eval'
GroupMe	system	Jane doe, Tanvi, Karthik,...	91976822, 82099981,...	20-Mar-21 6:42:43 PM	Shawn is going to 'Psych eval'
GroupMe	system	Jane Doe, Shawn, Trip...	91976822, 62933111,...	20-Mar-21 2:50:09 AM	Tyler Trostle has joined the group
GroupMe	system	Jane Doe, Shawn, Trip...	91976822, 62933111,...	19-Mar-21 10:14:05...	Shelby Yates has left the group.
GroupMe	system	Jane Doe, Peyton Edelb...	91976822, 64835360,...	15-Mar-21 6:23:06 PM	Joe Barron has joined the group
GroupMe	system	Jane doe, Tanvi, Karthik,...	91976822, 82099981,...	20-Mar-21 6:16:19 PM	Poll 'Trip dates' has expired
GroupMe	system	Jane doe, Tanvi, Karthik,...	91976822, 82099981,...	20-Mar-21 6:42:22 PM	Janhavi is not going to 'Psych eval'
GroupMe	system	Jane doe, Tanvi, Karthik,...	91976822, 82099981,...	17-Mar-21 12:02:11...	Purdue Forensics added Parth and Karthik to the group.
GroupMe	system	Jane Doe, Shawn, Trip...	91976822, 62933111,...	20-Mar-21 2:50:28 AM	Tyler Trostle has left the group.
GroupMe	system	Jane Doe, Shawn, Trip...	91976822, 62933111,...	20-Mar-21 1:22:18 AM	ellie huston has joined the group
GroupMe	system	Janhavi, Jane Doe	82565378, 91976822	20-Mar-21 6:27:43 PM	Jane Doe is undecided about 'Final ppt'
GroupMe	system	Jane Doe, Shawn, Trip...	91976822, 62933111,...	19-Mar-21 10:13:52...	Shelby Yates has joined the group
GroupMe	system	Jane Doe, Shawn, Trip...	91976822, 62933111,...	20-Mar-21 4:25:18 AM	Trip Newton added Matthew to the group.
GroupMe	system	Jane Doe, Shawn, Trip...	91976822, 62933111,...	20-Mar-21 4:24:23 AM	Trip Newton has joined the group
GroupMe	system	Jane doe, Tanvi, Karthik,...	91976822, 82099981,...	20-Mar-21 6:05:43 PM	Poll 'Trip dates' is about to expire
GroupMe	system	Jane doe, Tanvi, Karthik,...	91976822, 82099981,...	17-Mar-21 9:36:45 PM	Purdue Forensics added Janhavi to the group.
GroupMe	system	Tanvi, Purdue Forensics	82099981, 91976822	17-Mar-21 10:30:33...	Purdue Forensics added Tanvi to the group.
GroupMe	system	Tanvi, Purdue Forensics	82099981, 91976822	17-Mar-21 10:29:07...	Purdue Forensics changed the group's name to [SMS Group]
GroupMe	system	Jane Doe, Peyton Edelb...	91976822, 64835360,...	16-Mar-21 11:13:38...	William Bosma has joined the group
GroupMe	system	Jane doe, Tanvi, Karthik,...	91976822, 82099981,...	18-Mar-21 12:01:00...	Jane doe added Shawn to the group.
GroupMe	system	Jane doe, Tanvi, Karthik,...	91976822, 82099981,...	17-Mar-21 10:14:36...	Purdue Forensics changed the group's name to Grad school starter pack
GroupMe	system	Jane doe, Tanvi, Karthik,...	91976822, 82099981,...	15-Mar-21 9:37:24 PM	Purdue Forensics added Tanvi to the group.

Figure 4.18. System Events from AXIOM

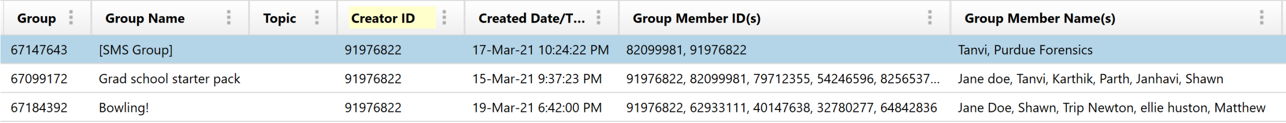


Timestamp	From	To	Body	Message Type
20-Mar-21 6:27:40 PM	91976822 name: Jane Doe, name: Final ppt, (owner) nickname: Jane Doe	82565378 Janhavi	Jane Doe created event 'Final ppt' https://s.group...	App Message
20-Mar-21 6:27:43 PM	system name: GroupMe, name: Final ppt, nickname: Jane Doe	82565378 Janhavi	Jane Doe is undecided about 'Final ppt'	App Message

Figure 4.19. System Events from UFED

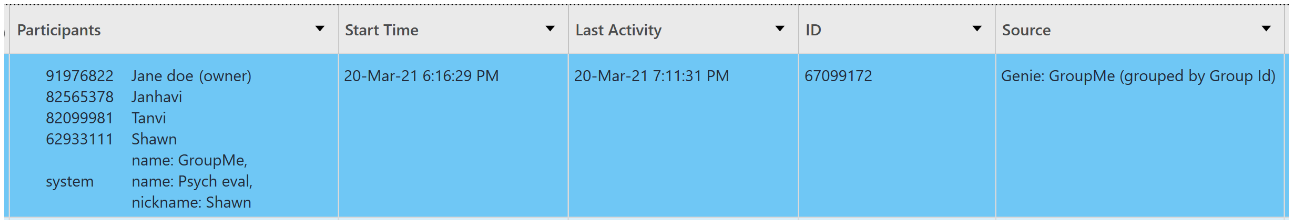
4.2.2 New Group Creation

Upon navigating to the GroupMe Groups tab in AXIOM and filtering the Creator ID with the user's ID, the 3 groups created by the user are obtained as shown in Figure 4.20. Of these, one is a regular group, one was created through GroupMe SMS, and one was created through Campus Connect. Similarly for UFED, upon grouping all text artifacts by GroupId, we can find the group owner (creator) is the user as shown in Figure 4.21.



Group	Group Name	Topic	Creator ID	Created Date/T...	Group Member ID(s)	Group Member Name(s)
67147643	[SMS Group]		91976822	17-Mar-21 10:24:22 PM	82099981, 91976822	Tanvi, Purdue Forensics
67099172	Grad school starter pack		91976822	15-Mar-21 9:37:23 PM	91976822, 82099981, 79712355, 54246596, 8256537...	Jane doe, Tanvi, Karthik, Parth, Janhavi, Shawn
67184392	Bowling!		91976822	19-Mar-21 6:42:00 PM	91976822, 62933111, 40147638, 32780277, 64842836	Jane Doe, Shawn, Trip Newton, ellie huston, Matthew

Figure 4.20. New Groups Created by User from AXIOM

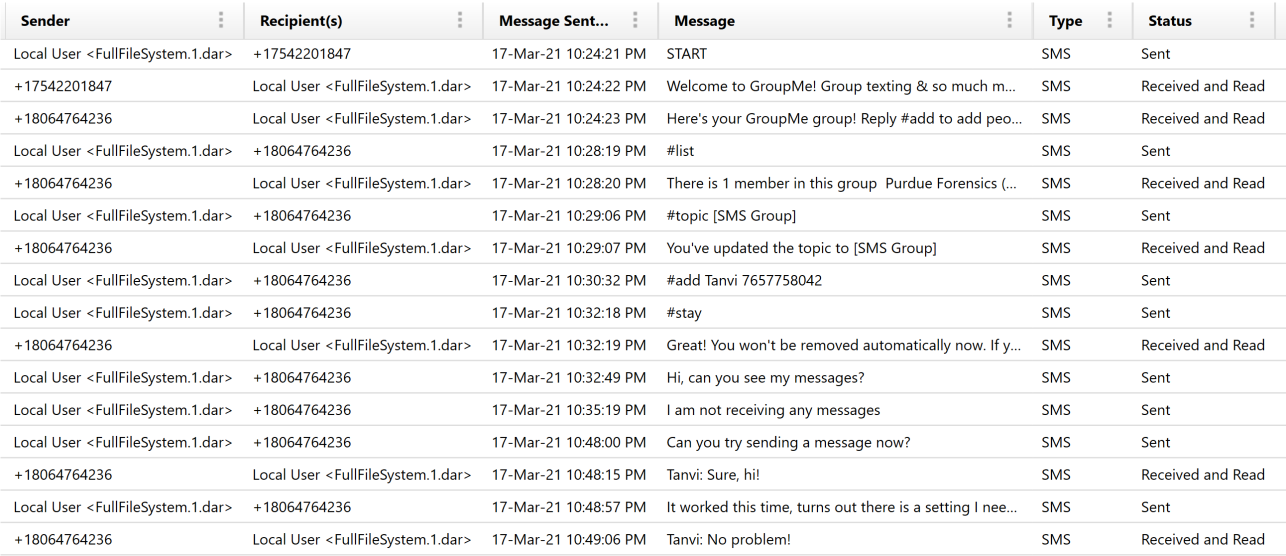


Participants	Start Time	Last Activity	ID	Source
91976822 Jane doe (owner) 82565378 Janhavi 82099981 Tanvi 62933111 Shawn system name: GroupMe, name: Psych eval, nickname: Shawn	20-Mar-21 6:16:29 PM	20-Mar-21 7:11:31 PM	67099172	Genie: GroupMe (grouped by Group Id)

Figure 4.21. New Groups Created by User from UFED

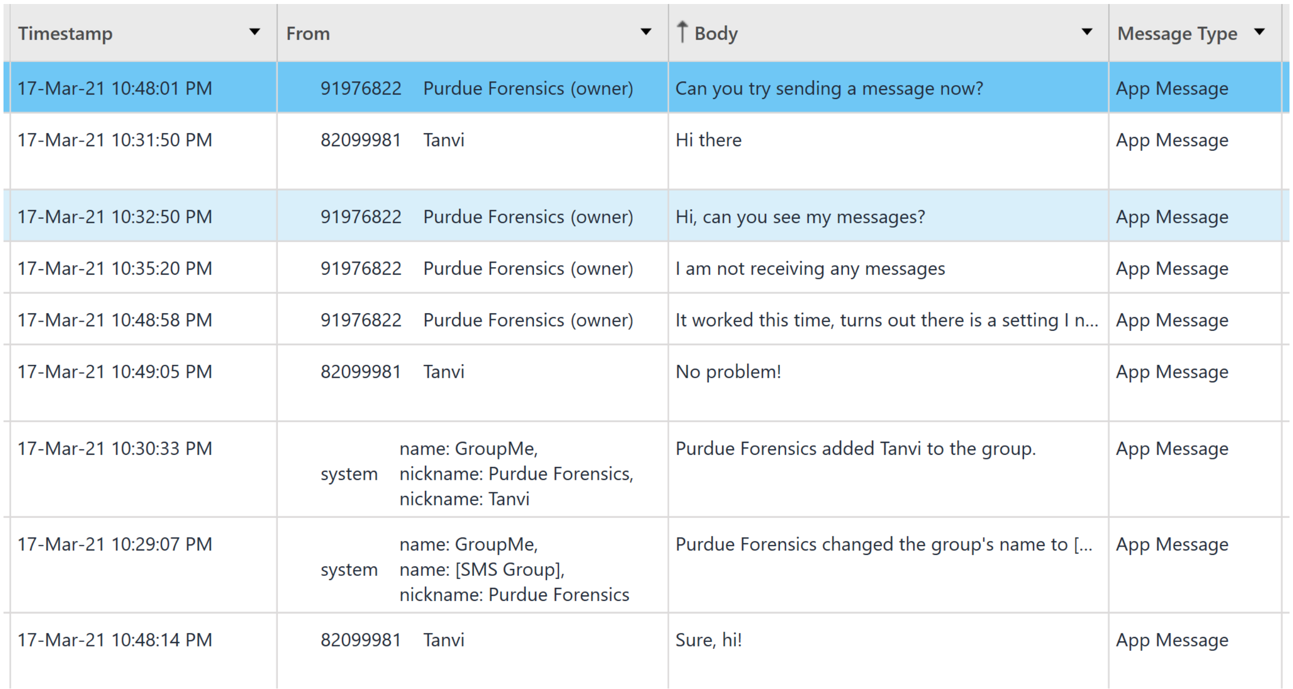
4.2.3 GroupMe SMS

All the artifacts related to GroupMe SMS recovered by AXIOM are illustrated in Figure 4.22, and those through UFED in Figure 4.23. The ones through AXIOM were screen captured through SMS logs, thus they include the system messages of adding members, changing the group name, etc., while the ones from UFED were recorded through the GroupMe Chats directly.



Sender	Recipient(s)	Message Sent...	Message	Type	Status
Local User <FullFileSystem.1.dar>	+17542201847	17-Mar-21 10:24:21 PM	START	SMS	Sent
+17542201847	Local User <FullFileSystem.1.dar>	17-Mar-21 10:24:22 PM	Welcome to GroupMe! Group texting & so much m...	SMS	Received and Read
+18064764236	Local User <FullFileSystem.1.dar>	17-Mar-21 10:24:23 PM	Here's your GroupMe group! Reply #add to add peo...	SMS	Received and Read
Local User <FullFileSystem.1.dar>	+18064764236	17-Mar-21 10:28:19 PM	#list	SMS	Sent
+18064764236	Local User <FullFileSystem.1.dar>	17-Mar-21 10:28:20 PM	There is 1 member in this group Purdue Forensics (...	SMS	Received and Read
Local User <FullFileSystem.1.dar>	+18064764236	17-Mar-21 10:29:06 PM	#topic [SMS Group]	SMS	Sent
+18064764236	Local User <FullFileSystem.1.dar>	17-Mar-21 10:29:07 PM	You've updated the topic to [SMS Group]	SMS	Received and Read
Local User <FullFileSystem.1.dar>	+18064764236	17-Mar-21 10:30:32 PM	#add Tanvi 7657758042	SMS	Sent
Local User <FullFileSystem.1.dar>	+18064764236	17-Mar-21 10:32:18 PM	#stay	SMS	Sent
+18064764236	Local User <FullFileSystem.1.dar>	17-Mar-21 10:32:19 PM	Great! You won't be removed automatically now. If y...	SMS	Received and Read
Local User <FullFileSystem.1.dar>	+18064764236	17-Mar-21 10:32:49 PM	Hi, can you see my messages?	SMS	Sent
Local User <FullFileSystem.1.dar>	+18064764236	17-Mar-21 10:35:19 PM	I am not receiving any messages	SMS	Sent
Local User <FullFileSystem.1.dar>	+18064764236	17-Mar-21 10:48:00 PM	Can you try sending a message now?	SMS	Sent
+18064764236	Local User <FullFileSystem.1.dar>	17-Mar-21 10:48:15 PM	Tanvi: Sure, hi!	SMS	Received and Read
Local User <FullFileSystem.1.dar>	+18064764236	17-Mar-21 10:48:57 PM	It worked this time, turns out there is a setting I nee...	SMS	Sent
+18064764236	Local User <FullFileSystem.1.dar>	17-Mar-21 10:49:06 PM	Tanvi: No problem!	SMS	Received and Read

Figure 4.22. GroupMe SMS Artifacts from AXIOM

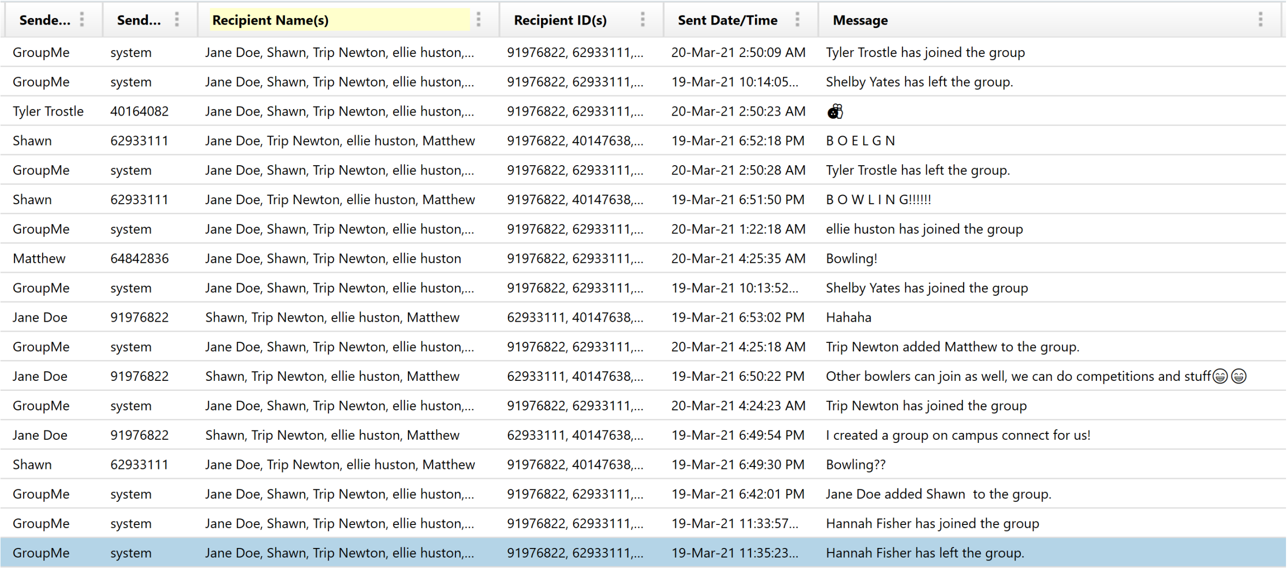


Timestamp	From	Body	Message Type
17-Mar-21 10:48:01 PM	91976822 Purdue Forensics (owner)	Can you try sending a message now?	App Message
17-Mar-21 10:31:50 PM	82099981 Tanvi	Hi there	App Message
17-Mar-21 10:32:50 PM	91976822 Purdue Forensics (owner)	Hi, can you see my messages?	App Message
17-Mar-21 10:35:20 PM	91976822 Purdue Forensics (owner)	I am not receiving any messages	App Message
17-Mar-21 10:48:58 PM	91976822 Purdue Forensics (owner)	It worked this time, turns out there is a setting I n...	App Message
17-Mar-21 10:49:05 PM	82099981 Tanvi	No problem!	App Message
17-Mar-21 10:30:33 PM	system name: GroupMe, nickname: Purdue Forensics, nickname: Tanvi	Purdue Forensics added Tanvi to the group.	App Message
17-Mar-21 10:29:07 PM	system name: GroupMe, name: [SMS Group], nickname: Purdue Forensics	Purdue Forensics changed the group's name to [...	App Message
17-Mar-21 10:48:14 PM	82099981 Tanvi	Sure, hi!	App Message

Figure 4.23. GroupMe SMS Artifacts from UFED

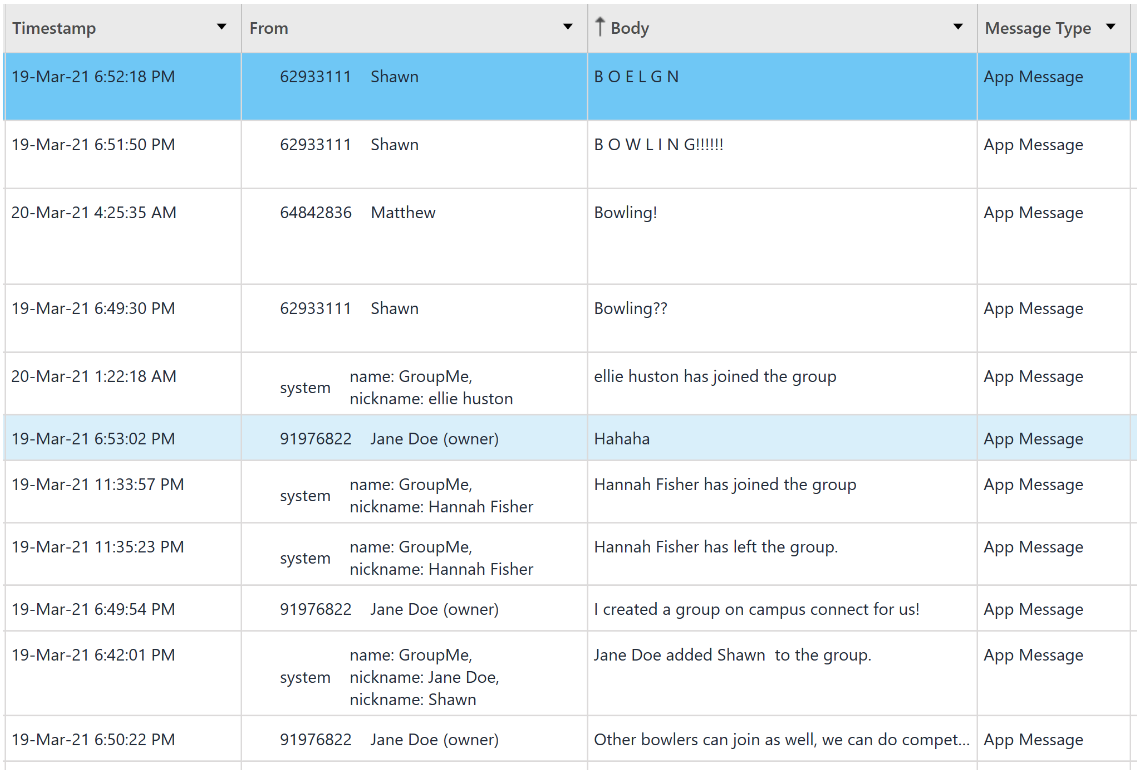
4.2.4 Campus Connect

Figure 4.24 and Figure 4.25 illustrate the messages exchanged through the campus connect group created by the user, recovered through AXIOM and UFED respectively. Following that, Figure 4.26 and Figure 4.27 display the messages exchanged through the pre-existing group that the user had joined in the Campus Connect community, recovered through AXIOM and UFED respectively.



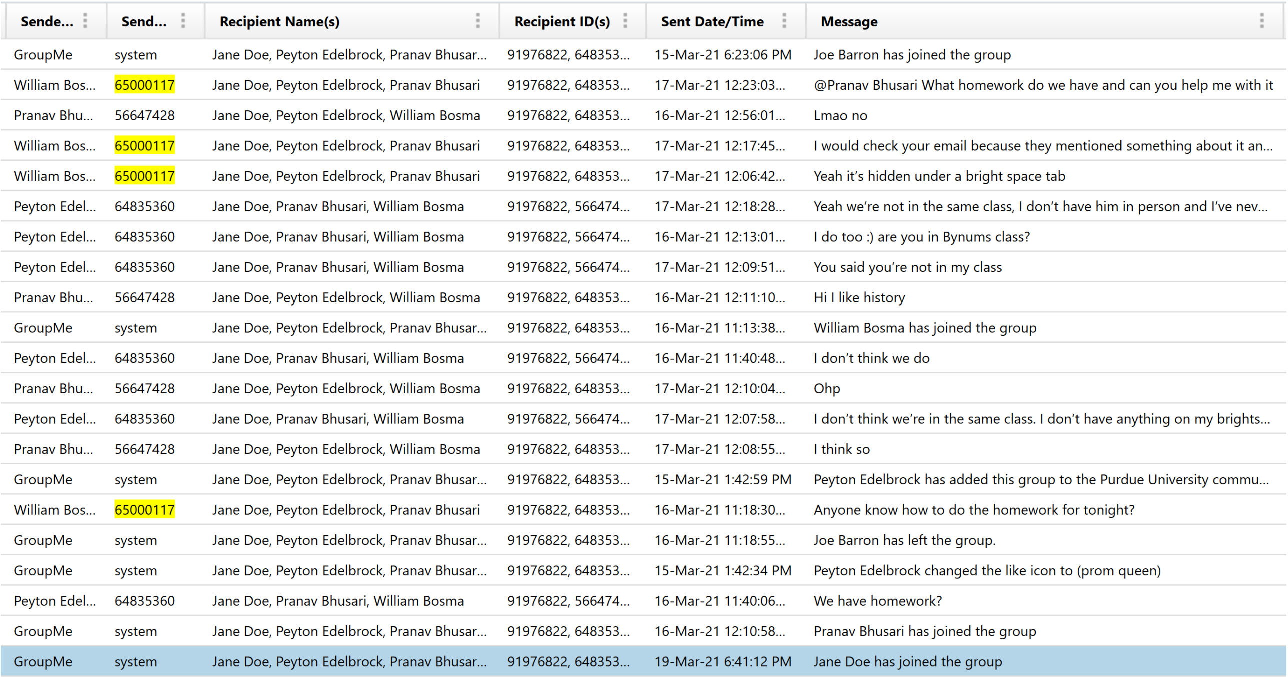
Sende...	Send...	Recipient Name(s)	Recipient ID(s)	Sent Date/Time	Message
GroupMe	system	Jane Doe, Shawn, Trip Newton, ellie huston,...	91976822, 62933111,...	20-Mar-21 2:50:09 AM	Tyler Trostle has joined the group
GroupMe	system	Jane Doe, Shawn, Trip Newton, ellie huston,...	91976822, 62933111,...	19-Mar-21 10:14:05...	Shelby Yates has left the group.
Tyler Trostle	40164082	Jane Doe, Shawn, Trip Newton, ellie huston,...	91976822, 62933111,...	20-Mar-21 2:50:23 AM	🎳
Shawn	62933111	Jane Doe, Trip Newton, ellie huston, Matthew	91976822, 40147638,...	19-Mar-21 6:52:18 PM	B O E L G N
GroupMe	system	Jane Doe, Shawn, Trip Newton, ellie huston,...	91976822, 62933111,...	20-Mar-21 2:50:28 AM	Tyler Trostle has left the group.
Shawn	62933111	Jane Doe, Trip Newton, ellie huston, Matthew	91976822, 40147638,...	19-Mar-21 6:51:50 PM	B O W L I N G!!!!!!
GroupMe	system	Jane Doe, Shawn, Trip Newton, ellie huston,...	91976822, 62933111,...	20-Mar-21 1:22:18 AM	ellie huston has joined the group
Matthew	64842836	Jane Doe, Shawn, Trip Newton, ellie huston	91976822, 62933111,...	20-Mar-21 4:25:35 AM	Bowling!
GroupMe	system	Jane Doe, Shawn, Trip Newton, ellie huston,...	91976822, 62933111,...	19-Mar-21 10:13:52...	Shelby Yates has joined the group
Jane Doe	91976822	Shawn, Trip Newton, ellie huston, Matthew	62933111, 40147638,...	19-Mar-21 6:53:02 PM	Hahaha
GroupMe	system	Jane Doe, Shawn, Trip Newton, ellie huston,...	91976822, 62933111,...	20-Mar-21 4:25:18 AM	Trip Newton added Matthew to the group.
Jane Doe	91976822	Shawn, Trip Newton, ellie huston, Matthew	62933111, 40147638,...	19-Mar-21 6:50:22 PM	Other bowlers can join as well, we can do competitions and stuff😁😁
GroupMe	system	Jane Doe, Shawn, Trip Newton, ellie huston,...	91976822, 62933111,...	20-Mar-21 4:24:23 AM	Trip Newton has joined the group
Jane Doe	91976822	Shawn, Trip Newton, ellie huston, Matthew	62933111, 40147638,...	19-Mar-21 6:49:54 PM	I created a group on campus connect for us!
Shawn	62933111	Jane Doe, Trip Newton, ellie huston, Matthew	91976822, 40147638,...	19-Mar-21 6:49:30 PM	Bowling??
GroupMe	system	Jane Doe, Shawn, Trip Newton, ellie huston,...	91976822, 62933111,...	19-Mar-21 6:42:01 PM	Jane Doe added Shawn to the group.
GroupMe	system	Jane Doe, Shawn, Trip Newton, ellie huston,...	91976822, 62933111,...	19-Mar-21 11:33:57...	Hannah Fisher has joined the group
GroupMe	system	Jane Doe, Shawn, Trip Newton, ellie huston,...	91976822, 62933111,...	19-Mar-21 11:35:23...	Hannah Fisher has left the group.

Figure 4.24. Campus Connect Artifacts from AXIOM



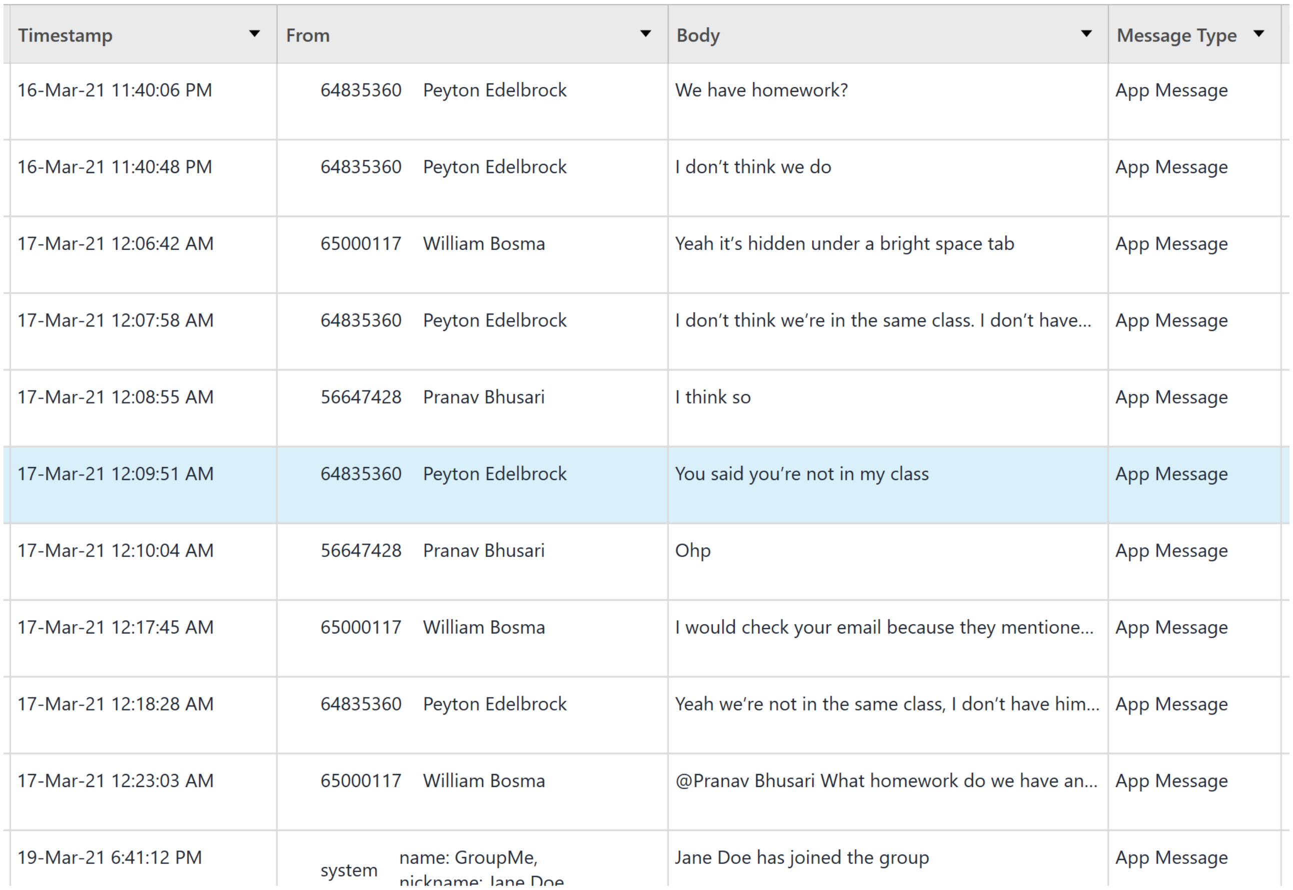
Timestamp	From	Body	Message Type
19-Mar-21 6:52:18 PM	62933111 Shawn	B O E L G N	App Message
19-Mar-21 6:51:50 PM	62933111 Shawn	B O W L I N G!!!!!!	App Message
20-Mar-21 4:25:35 AM	64842836 Matthew	Bowling!	App Message
19-Mar-21 6:49:30 PM	62933111 Shawn	Bowling??	App Message
20-Mar-21 1:22:18 AM	system name: GroupMe, nickname: ellie huston	ellie huston has joined the group	App Message
19-Mar-21 6:53:02 PM	91976822 Jane Doe (owner)	Hahaha	App Message
19-Mar-21 11:33:57 PM	system name: GroupMe, nickname: Hannah Fisher	Hannah Fisher has joined the group	App Message
19-Mar-21 11:35:23 PM	system name: GroupMe, nickname: Hannah Fisher	Hannah Fisher has left the group.	App Message
19-Mar-21 6:49:54 PM	91976822 Jane Doe (owner)	I created a group on campus connect for us!	App Message
19-Mar-21 6:42:01 PM	system name: GroupMe, nickname: Jane Doe, nickname: Shawn	Jane Doe added Shawn to the group.	App Message
19-Mar-21 6:50:22 PM	91976822 Jane Doe (owner)	Other bowlers can join as well, we can do compet...	App Message

Figure 4.25. Campus Connect Artifacts from UFED



Sende...	Send...	Recipient Name(s)	Recipient ID(s)	Sent Date/Time	Message
GroupMe	system	Jane Doe, Peyton Edelbrock, Pranav Bhusar...	91976822, 648353...	15-Mar-21 6:23:06 PM	Joe Barron has joined the group
William Bos...	65000117	Jane Doe, Peyton Edelbrock, Pranav Bhusari	91976822, 648353...	17-Mar-21 12:23:03...	@Pranav Bhusari What homework do we have and can you help me with it
Pranav Bhu...	56647428	Jane Doe, Peyton Edelbrock, William Bosma	91976822, 648353...	16-Mar-21 12:56:01...	Lmao no
William Bos...	65000117	Jane Doe, Peyton Edelbrock, Pranav Bhusari	91976822, 648353...	17-Mar-21 12:17:45...	I would check your email because they mentioned something about it an...
William Bos...	65000117	Jane Doe, Peyton Edelbrock, Pranav Bhusari	91976822, 648353...	17-Mar-21 12:06:42...	Yeah it's hidden under a bright space tab
Peyton Edel...	64835360	Jane Doe, Pranav Bhusari, William Bosma	91976822, 566474...	17-Mar-21 12:18:28...	Yeah we're not in the same class, I don't have him in person and I've nev...
Peyton Edel...	64835360	Jane Doe, Pranav Bhusari, William Bosma	91976822, 566474...	16-Mar-21 12:13:01...	I do too :) are you in Bynums class?
Peyton Edel...	64835360	Jane Doe, Pranav Bhusari, William Bosma	91976822, 566474...	17-Mar-21 12:09:51...	You said you're not in my class
Pranav Bhu...	56647428	Jane Doe, Peyton Edelbrock, William Bosma	91976822, 648353...	16-Mar-21 12:11:10...	Hi I like history
GroupMe	system	Jane Doe, Peyton Edelbrock, Pranav Bhusar...	91976822, 648353...	16-Mar-21 11:13:38...	William Bosma has joined the group
Peyton Edel...	64835360	Jane Doe, Pranav Bhusari, William Bosma	91976822, 566474...	16-Mar-21 11:40:48...	I don't think we do
Pranav Bhu...	56647428	Jane Doe, Peyton Edelbrock, William Bosma	91976822, 648353...	17-Mar-21 12:10:04...	Ohp
Peyton Edel...	64835360	Jane Doe, Pranav Bhusari, William Bosma	91976822, 566474...	17-Mar-21 12:07:58...	I don't think we're in the same class. I don't have anything on my brights...
Pranav Bhu...	56647428	Jane Doe, Peyton Edelbrock, William Bosma	91976822, 648353...	17-Mar-21 12:08:55...	I think so
GroupMe	system	Jane Doe, Peyton Edelbrock, Pranav Bhusar...	91976822, 648353...	15-Mar-21 1:42:59 PM	Peyton Edelbrock has added this group to the Purdue University commu...
William Bos...	65000117	Jane Doe, Peyton Edelbrock, Pranav Bhusari	91976822, 648353...	16-Mar-21 11:18:30...	Anyone know how to do the homework for tonight?
GroupMe	system	Jane Doe, Peyton Edelbrock, Pranav Bhusar...	91976822, 648353...	16-Mar-21 11:18:55...	Joe Barron has left the group.
GroupMe	system	Jane Doe, Peyton Edelbrock, Pranav Bhusar...	91976822, 648353...	15-Mar-21 1:42:34 PM	Peyton Edelbrock changed the like icon to (prom queen)
Peyton Edel...	64835360	Jane Doe, Pranav Bhusari, William Bosma	91976822, 566474...	16-Mar-21 11:40:06...	We have homework?
GroupMe	system	Jane Doe, Peyton Edelbrock, Pranav Bhusar...	91976822, 648353...	16-Mar-21 12:10:58...	Pranav Bhusari has joined the group
GroupMe	system	Jane Doe, Peyton Edelbrock, Pranav Bhusar...	91976822, 648353...	19-Mar-21 6:41:12 PM	Jane Doe has joined the group

Figure 4.26. Campus Connect Artifacts from AXIOM



Timestamp	From	Body	Message Type
16-Mar-21 11:40:06 PM	64835360 Peyton Edelbrock	We have homework?	App Message
16-Mar-21 11:40:48 PM	64835360 Peyton Edelbrock	I don't think we do	App Message
17-Mar-21 12:06:42 AM	65000117 William Bosma	Yeah it's hidden under a bright space tab	App Message
17-Mar-21 12:07:58 AM	64835360 Peyton Edelbrock	I don't think we're in the same class. I don't have...	App Message
17-Mar-21 12:08:55 AM	56647428 Pranav Bhusari	I think so	App Message
17-Mar-21 12:09:51 AM	64835360 Peyton Edelbrock	You said you're not in my class	App Message
17-Mar-21 12:10:04 AM	56647428 Pranav Bhusari	Ohp	App Message
17-Mar-21 12:17:45 AM	65000117 William Bosma	I would check your email because they mentione...	App Message
17-Mar-21 12:18:28 AM	64835360 Peyton Edelbrock	Yeah we're not in the same class, I don't have him...	App Message
17-Mar-21 12:23:03 AM	65000117 William Bosma	@Pranav Bhusari What homework do we have an...	App Message
19-Mar-21 6:41:12 PM	system name: GroupMe, nickname: Jane Doe	Jane Doe has joined the group	App Message

Figure 4.27. Campus Connect Artifacts from UFED

4.3 Summary

This chapter consisted of consolidating the findings of the study and providing details of all the recovered artifacts in the form of screen captures from both the forensic tools (AXIOM and UFED) used in the study. It also contained a brief description of the two hypotheses being tested in the study and a note on whether or not they were supported by the obtained results.

CHAPTER 5. DISCUSSION AND FUTURE WORK

The objective of this study was to determine which forensic artifacts, if at all, could be recovered from the GroupMe mobile application. Specifically, this study explored examining the application on Android (before and after rooting) and iOS operating systems using two separate tools. The Android device used was a Samsung Galaxy S7 Edge (Android 7.0) and the iOS device used was an iPhone 6 (iOS 12.5.1). Out of the two hypotheses being tested in the study, H_1 could not be tested, while H_2 was successfully supported.

GroupMe is among some of the the most popular instant messaging applications worldwide and is available on most major mobile operating systems, including Android iOS and Windows. According to Clement (2019), it has over 10.75 million unique users as of 2019 in the United States alone, a large majority of which are students. The findings of this study will aid investigators in future investigations involving the use of GroupMe to locate several artifacts, including text messages, media files, documents, etc. when analyzing a suspect's Android or iOS smartphone.

After examining and analyzing the iPhone using both tools (UFED and AXIOM), it was found that most of the relevant artifacts were found in either the “GroupMe.sqlite” or “GroupMe.sqlite-wal” databases, or in certain plist or cache files. These would be the locations an investigator could primarily focus on to get a bulk of the data from the suspect's device. Even though this study focused on analysis using only AXIOM and UFED, other forensic tools like XRY, BlackLight or FTK could also be used by following the methodology proposed in this study. An important point to note here would be that GroupMe groups artifacts related to several different data types as text artifacts, thus if an investigator is looking specifically for photos, videos, GIFs, or even documents, they would be found as text/chat artifacts, with URLs to the relevant item. The same would apply for shared locations, polls and calendar events shared within the chat. Another consideration that an investigator could keep in mind during the analysis is that for the most part, the forensic tools used in this study use the unique User IDs to refer to group chat members instead of their actual names, so in order to identify the senders and receivers in every chat, they would have to first examine the Contacts artifacts and map each participant name with their User IDs. While most of the populated artifacts were recovered by both tools

(317/335), no evidence of liked messages, in-app searches, hidden messages and chats, and altered user account information could be found through this study.

Significant challenges were faced during imaging and rooting the Samsung Galaxy S7 Edge device during this study. The proposed methodology expected a physical image of the device to be created for maximum possible data recovery. However, since the security patch of the device was from June 2017 and it was found that UFED did not guarantee physical extraction of devices with security patches further than November 2016, all attempts at a physical extraction failed. Thus, an advanced logical image was created, which was unable to provide the expected evidence related to GroupMe. Moreover, rooting this device proved to be extremely challenging since it was a US model carrier (SM-G935A), which uses a Qualcomm chipset that does not allow bootloader unlocking which is required to root, as opposed to the international variants which use the Exynos chipsets. This means that an investigator could also potentially face the same problem if the suspect's phone was a US model, (i.e., whose model number ended in A/P/T/V/0/AZ/T1/R6/R7/R4/VL/U). In that case, it would be extremely difficult to gain root access to the device, which could also result in failed physical imaging, since tools like UFED internally try to root devices to extract evidence from them.

5.1 Future Research

Although a substantial amount of information was recovered from the iPhone during this study, and several useful facts about Android device imaging and rooting were discovered and presented, there are still questions that remain unanswered. Future work that can extend this study could include analyzing GroupMe on the Desktop/Web client for PCs. The data stored on cloud, and even the volatile (RAM) memory of the suspect's device could be examined for new artifacts which are not present in the filesystem. Also, Android devices with SD cards could be included in a similar study to compare if the GroupMe artifacts recovered from the internal storage differ from those that would be stored on the SD card. Moreover, future work could include developing a technique to safely root US models of these Samsung phones so that future investigations would not be forced to reach a dead end due to lack of new information.

Some further research could also be conducted to improve the performance metrics being used in this study. The accuracy metric in this study is calculated as a percentage of the number of artifacts correctly recovered using the tool over the number of expected artifacts. This has led to the accuracies of both tools being used for iOS analysis to produce the same accuracy, whereas UFED had actually incorrectly classified 7 group participants as Contacts. The current accuracy metric does not take into account incorrectly classified artifacts, which should ideally be factored in while measuring the performance of a tool. Since the accuracy metric used for this study was decided prior to the actual experiment, it would have been incorrect to alter it to accommodate the results obtained. However, if the author were to make a suggestion for a more unbiased accuracy metric, it would be to subtract the number of incorrectly classified artifacts from the total number of correctly identified ones and then calculate the percentage of the resultant sum over the number of expected artifacts.

Additionally, this experiment could be repeated multiple times in order to test out the Reliability measure, since due to time constraints, this could not be done during this study.

REFERENCES

About encrypted backups on your iphone, ipad, or ipod touch. (2021, January). https://support.apple.com/en-us/HT205220. (Accessed: 2021-7-14)

Al-Hadadi, M., & AlShidhani, A. (2013). Smartphone forensics analysis: A case study. *IJCEE*, 576–580.

Almehmadi, T., & Batarfi, O. (2019, May). Impact of android phone rooting on user data integrity in mobile forensics. In *2019 2nd international conference on computer applications information security (ICCAIS)* (pp. 1–6).

Al-Rawashdeh, A. M., Al-Sharif, Z. A., Al-Saleh, M. I., & Shatnawi, A. S. (2020, April). A Post-Mortem forensic approach for the kik messenger on android. In *2020 11th international conference on information and communication systems (ICICS)* (pp. 079–084).

Alyahya, T., & Kausar, F. (2017, January). Snapchat analysis to discover digital forensic artifacts on android smartphone. *Procedia Comput. Sci.*, *109*, 1035–1040.

Anglano, C., Canonico, M., & Guazzone, M. (2017, December). Forensic analysis of telegram messenger on android smartphones. *Digital Investigation*, *23*, 31–49.

Ayers, R. (2009). Mobile device Forensics-Tool testing. *National Institute of Standards and Technology May*, *6*, 1–23.

Ayers, R., Brothers, S., & Jansen, W. (2014, May). *Guidelines on mobile device forensics* (Tech. Rep.). National Institute of Standards and Technology.

Boueiz, M. (2020, June). Importance of rooting in an android data acquisition. In *2020 8th international symposium on digital forensics and security (ISDFS)* (pp. 1–4).

Carrier, B., & Spafford, E. (2004). An event-based digital forensic investigation framework. *Digital Investigation*.

Casey, E. (2019, November). The chequered past and risky future of digital forensics. *Aust. J. Forensic Sci.*, *51*(6), 649–664.

Cellebrite UFED iOS - cellebrite. (n.d.). https://www.cellebrite.com/en/ufed-unlock-iphone-x/. (Accessed: 2021-6-28)

Cellebrite UFED iOS - cellebrite. (2020). https://www.cellebrite.com/en/ufed-unlock-iphone-x/. (Accessed: 2020-11-13)

Clement, J. (2019, September). *Leading mobile messengers in the U.S. 2019, by users.* https://www.statista.com/statistics/350461/mobile-messenger-app-usage-usa/. (Accessed: 2020-11-5)

Costello, S. (2019, December). *iphone DFU mode: What it is and how to use it.* https://www.lifewire.com/using-iphone-dfu-mode-2000656. (Accessed: 2021-6-28)

Epifani, M., & Stirparo, P. (2016). *Learning iOS forensics.* Packt Publishing Ltd.

gatesjunior. (2017, February). *KingRoot malware / adware root !!* https://forum.xda-developers.com/t/kingroot-malware-adware-root.3563090/. XDA Forums. (Accessed: 2021-7-13)

Gronseth, S., & Hebert, W. (2019, January). GroupMe: Investigating use of mobile instant messaging in higher education courses. *TechTrends*, *63*(1), 15–22.

Gruger, W. (n.d.). *Meme.* https://www.merriam-webster.com/dictionary/meme. (Accessed: 2020-11-5)

Ieong, R. S. C. (2006, September). FORZA – digital forensics investigation framework that incorporate legal issues. *Digital Investigation*, *3*, 29–36.

Igor Mikhaylov, O. S. (2016, June). *itunes backup forensic analysis.* https://www.digitalforensics.com/blog/itunes-backup-forensic-analysis/. Digital Forensics Corp. (Accessed: 2020-11-13)

Indani, E. (2017, February). *FBI zeroes in on ringleaders of racist GroupMe incident.* https://www.thedp.com/article/2017/02/fbi-has-new-developments-in-investigations-into-racist-groupme-messages. (Accessed: 2020-11-4)

Jeff Tyson, A. C. (2001, March). *How instant messaging works.* https://computer.howstuffworks.com/e-mail-messaging/instant-messaging.htm. HowStuffWorks. (Accessed: 2020-11-13)

Junaid, B. (2019, June). *Root android phone without losing data with android data recovery.* https://www.droidguides.com/root-android-phone-without-losing-data/. (Accessed: 2021-6-22)

Kebande, V. R., & Ray, I. (2016, August). A generic digital forensic investigation framework for internet of things (IoT). In *2016 IEEE 4th international conference on future internet of things and cloud (FiCloud)* (pp. 356–362).

Knox, S., Moghadam, S., Patrick, K., Phan, A., & Choo, K.-K. R. (2020, July). What's really 'happning'? a forensic analysis of android and iOS happn dating apps. *Comput. Secur.*, *94*, 101833.

Low, S., & Wilson, G. (2003, January). *Instant messaging* (No. 20030018726:A1).

Ly, Q. C. (2020). The case for GroupMe: Rhetorical thinking thrives among students using app. *Journal of Literacy and Technology*, *21*(1).

Magnet AXIOM user guide [Computer software manual]. (2020).

Majid ALThebaity, Shailendra Mishra, Manoj Kumar Shukla. (2020, August). Forensic analysis of third-party mobile application. *Helix - The Scientific Explorer*.

Malani, S. (2016, March). *How to root samsung galaxy devices using CF auto root and odin.* `https://nerdschalk.com/root-samsung-galaxy-devices-cf-auto-root-odin/`. (Accessed: 2021-6-26)

McKemmish, R. (2008). When is digital evidence forensically sound? In *Advances in digital forensics IV* (pp. 3–15). Springer US.

Mobile operating system market share worldwide. (2020, October). `https://gs.statcounter.com/os-market-share/mobile/worldwide`. (Accessed: 2020-11-8)

Morgan, H. (2019, December). *How to root samsung android phone with odin root.* `https://www.androiddata-recovery.com/blog/root-with-odin`. (Accessed: 2021-6-22)

Nazario, K. (2013, June). *What is a bootloader & why you need to unlock it on android devices.* `https://www.technorms.com/25689/android-bootloader-locked-unlocked-guide`. (Accessed: 2021-6-26)

NIST. (2016). Mobile device data population setup guide [Computer software manual].

O'Dea. (2020, August). *Smartphone users worldwide 2016-2021.* `https://www.statista.com/statistics/330695/number-of-smartphone-users-worldwide/`. (Accessed: 2020-11-5)

Ozio, R. (2016, November). *Black freshmen at penn target of threatening racist messages.* https://penntoday.upenn.edu/news/black-freshmen-penn-target-threatening-racist-messages. (Accessed: 2020-11-4)

Petronzio, M. (2012, October). *A brief history of instant messaging.* https://mashable.com/2012/10/25/instant-messaging-history/. (Accessed: 2020-11-12)

Pollitt, M. (2010). A history of digital forensics. In *Advances in digital forensics VI* (pp. 3–15). Springer Berlin Heidelberg.

Rathi, K., Karabiyik, U., Aderibigbe, T., & Chi, H. (2018, March). Forensic analysis of encrypted instant messaging applications on android. In *2018 6th international symposium on digital forensic and security (ISDFS)* (pp. 1–6).

Reddy, N. (2019). Mobile forensics. In N. Reddy (Ed.), *Practical cyber forensics: An Incident-Based approach to forensic investigations* (pp. 205–239). Berkeley, CA: Apress.

Ryu, J. H., Sharma, P. K., Jo, J. H., & Park, J. H. (2019, August). A blockchain-based decentralized efficient investigation framework for IoT digital forensics. *J. Supercomput.*, *75*(8), 4372–4387.

Satpathy, S., & Mohanty, S. N. (2020). *Big data analytics and computing for digital forensic investigations*. CRC Press.

Snyder, S. (2016, November). *Tulsa u. student possibly linked to racist texts sent to penn freshmen.* https://www.inquirer.com/philly/news/20161117_Tulsa_U__student_possible_source_of_racist_texts_sent_to_Penn_freshmen_last_week.html. (Accessed: 2020-11-5)

Spyware: KingRoot, KingoRoot, iroot, etc. (2018). https://www.reddit.com/r/androidroot/comments/78914h/spyware_kingroot_kingoroot_iroot_etc/. (Accessed: 2021-7-13)

Sudozai, M. A. K., Saleem, S., Buchanan, W. J., Habib, N., & Zia, H. (2018, June). Forensics study of IMO call and chat app. *Digital Investigation*, *25*, 5–23.

Supporting new extraction methods and devices. (2019, February). https://www.cellebrite.com/en/productupdates/supporting-new-extraction-methods-and-devices/. (Accessed: 2021-6-27)

Tayeb, H. F., & Varol, C. (2019, June). Android mobile device forensics: A review. In *2019 7th international symposium on digital forensics and security (ISDFS)* (pp. 1–7).

A technical look at phone extraction. (2019, October). `https://privacyinternational.org/long-read/3256/technical-look-phone-extraction`. (Accessed: 2021-6-27)

Thakur, K., Hayajneh, T., & Tseng, J. (2019, March). Cyber security in social media: Challenges and the way forward. *IT Prof.*, *21*(2), 41–49.

TWRP recovery for AT&T SAMSUNG S7 edge (SM-G935A). (2018, January). `https://forum.xda-developers.com/t/twrp-recovery-for-at-t-samsung-s7-edge-sm-g935a.3739128/`. XDA Forums. (Accessed: 2021-6-26)

UFED ultimate & UFED in field (Tech. Rep.). (2018, May).

Vukadinovic, N. V., Seigfried-Spellar, K. C., Rogers, M. K., & Karabiyik, U. (2019, May). WhatsApp forensics: Locating artifacts in web and desktop clients.

What are GroupMe SMS commands? (n.d.). `https://support.microsoft.com/en-us/office/what-are-groupme-sms-commands-ac9d4331-e213-413e-af70-f9081203ca4c`. (Accessed: 2021-7-1)

What is magisk? (n.d.). `https://www.xda-developers.com/what-is-magisk/`. (Accessed: 2021-6-22)

Will CF-Auto-Root wipe the device. (2013, November). `https://forum.xda-developers.com/t/will-cf-auto-root-wipe-the-device.2516234/`. XDA Forums. (Accessed: 2021-6-22)

Yadav, S., Prakash, S., Dayal, N., & Singh, V. (2019). Forensics analysis of WhatsApp in android mobile phone. In *Proceedings of the international conference on advances in electronics, electrical & computational intelligence (ICAEEC).*

Yu, M., Zhuge, J., Cao, M., Shi, Z., & Jiang, L. (2020, February). A survey of security vulnerability analysis, discovery, detection, and mitigation on IoT devices. *Future Internet*, *12*(2), 27.

Yudhana, A., Riadi, I., & Anshori, I. (2019, January). IDENTIFICATION OF DIGITAL EVIDENCE FACEBOOK MESSENGER ON MOBILE PHONE WITH NATIONAL INSTITUTE OF STANDARDS TECHNOLOGY (NIST) METHOD. *Jurnal Ilmiah Kursor*, *9*(3).

Zamroni, G. M., & Riadi, I. (2019, May). Instant messaging forensic analysis on android operating system. *Kinetik: Game Technology, Information System, Computer Network, Computing, Electronics, and Control*, *4*(2), 137–148.

APPENDIX A. HYPOTHETICAL SCENARIO FOR DATA POPULATION

Table A.1. *Android - Samsung Galaxy S7 Edge*

Participant/ Group Name	Tanvi Sent/Rec		Parth Sent/Rec		Vaishali Sent/Rec		Neesha Sent/Rec		Graduation Sent/Rec		Birds		PU Soccer		Grad 2021	
Artifact																
Text Messages	31	34	3	2	26	20	4	1	25	84	5	4	3	3	3	2
Media Items	2	5			1	1			3	3						
Integrated Videos	1	1			2				1							
Liked Messages	1				2				17							
Shared Locations	1	1							1	1						
Documents		5			1	2				2						
Blocked Contact?	No		No		No		Yes									
Polls									1				1			
Calendar Events	1									1						
Memes					1				2	1						
Skype Calls	1				1											
Hidden Chat?	No		Yes		No		No									

Exited Group?					No	No	Yes	No
Hidden Messages				2				
SMS Group?					No	Yes	No	No
Campus Connect?					No	No	Yes	Yes

Table A.2. *iOS - iPhone 6*

Participant/ Group Name	Tanvi Sent/Rec	Parth Sent/Rec	Karthik Sent/Rec	Janhavi Sent/Rec	Grad School Starter Pack Sent/Rec	SMS Group	CGT 164	Bowling
Artifact								
Text Messages	18 16	5 3	8 6	28 9	34 96	4 4	13	3 3
Media Items	1 3	2	4		3 2			
Integrated Videos	1		2 1		1			
Liked Messages	1		2	2	15			
Shared Locations			1 2		1			
Documents	5		3	1 1				
Blocked Contact?	No	No	Yes	No				
Polls					2			

Calendar Events				1	1			
Memes	1				2 1			
Skype Calls								
Hidden Chat?	No	Yes	No	No				
Exited Group?					No	No	Yes	No
Hidden Messages	2							
SMS Group?					No	Yes	No	No
Campus Connect?					No	No	Yes	Yes

APPENDIX B. RETRIEVED MEMBER AND GROUP IDS FOR IPHONE

Table B.1. *Participant and Group IDs for iPhone Retrieved from AXIOM and UFED*

Participant/Group Name	**User ID**	**Group ID**
Jane Doe	91976822	
Tanvi	82099981	
Parth	54246596	
Janhavi	82565378	
Shawn	62933111	
Karthik	79712355	
Grad School Started Pack		67099172
SMS Group		67147643
CGT 164		67085198
Bowling		67184392