Research Article

A comparative study of WhatsApp forensics tools

Khalid Alissa[1,2] · Norah A. Almubairik[1] · Lamyaa Alsaleem[1] · Deema Alotaibi[1] · Malak Aldakheel[1] · Sarah Alqhtani[1] · Nazar Saqib[1] · Samiha Brahimi[1] · Mubarak Alshahrani[3]

© Springer Nature Switzerland AG 2019

Abstract

With the increasing number of mobile phones and mobile applications, there is a noticeable rise in cybercrimes. Hence, an urgent need for mobile forensics. Before starting investigation, the investigator should choose one of the acquisition types; physical acquisition, logical acquisition or manual acquisition. The current mobile acquisition tools use these methods to produce an image of the entire mobile content, files of specific datatypes, or data of a certain application. Unfortunately, the resultant output does not facilitate investigating cases related to specific mobile application, since the tool might acquire more than what is needed which requires investigators to filter data manually, or acquire all the application's data without sufficient analysis. Both cases are effort and time consuming. This study analyzes and compares currently available forensics tools that are designed to extract WhatsApp data only. The comparative study is based on two aspects; National Institute of Standards and Technology (NIST) Mobile Device Tool Test Assertions and researchers' requirements. The results of the comparative study showed a shortage in the current WhatsApp forensics tools as they do not satisfy all NIST Test Assertions. Additionally, several researchers' requirements such as: creating projects, comprehensive analysis, applying filters and validating the extracted files, were not met in the studied tools.

Keywords Comparative study · Digital forensics · Mobile forensics · WhatsApp

1 Introduction

Mobile devices have become an integral part of everyone's life, it has various types, models, operating systems and sizes that enable it to carry out diverse tasks and activities. Mobile devices have divergent categories, such as business, sport, entertainment, communication and many others. Recently, there is a notable shift to mobile device communication since different messaging applications were developed with variety of features. Among all messaging applications, WhatsApp is accredited to be the most popular application worldwide [1]. Although Fig. 1 shows that WhatsApp and Facebook Messenger have the same score, the statistics of Department of Criminal Evidence in Saudi Arabia states that more than 80% of the digital crimes in Saudi Arabia are committed using WhatsApp.

WhatsApp is well-known for its diverse features, it enables text messaging, videos, images and voice notes transmission, video and audio calls. All these features can be utilized by variety of fields and users, for evil or for good purposes. Therefore, WhatsApp is considered a gold mine for forensics evidences and artifacts due to the vast amount of data it stores [1, 3].

From digital forensics point of view, the advancement of technology enables digital crimes to be committed by diverse means and methods, such as mobile devices.

✉ Khalid Alissa, kAlissa@kacst.edu.sa; Norah A. Almubairik, naalmubairik@iau.edu.sa; Lamyaa Alsaleem, 2150006354@iau.edu.sa; Deema Alotaibi, 2150004996@iau.edu.sa; Malak Aldakheel, 2160007006@iau.edu.sa; Sarah Alqhtani, 2150001193@iau.edu.sa; Nazar Saqib, nasaqib@iau.edu.sa; Samiha Brahimi, sbrahimi@iau.edu.sa; Mubarak Alshahrani, Mob.mob1409@gmail.com | [1]College of Computer Sciences and Information Technology, Imam Abdulrahman Bin Faisal University, Dammam, Saudi Arabia. [2]National Center for Satellite Technologies, King Abdulaziz City for Science and Technology (KACST), Riyadh, Saudi Arabia. [3]Ministry of Interior, Public Security, Dammam, Saudi Arabia.

SN Applied Sciences (2019) 1:1320 | https://doi.org/10.1007/s42452-019-1312-8

Received: 4 August 2019 / Accepted: 18 September 2019 / Published online: 3 October 2019

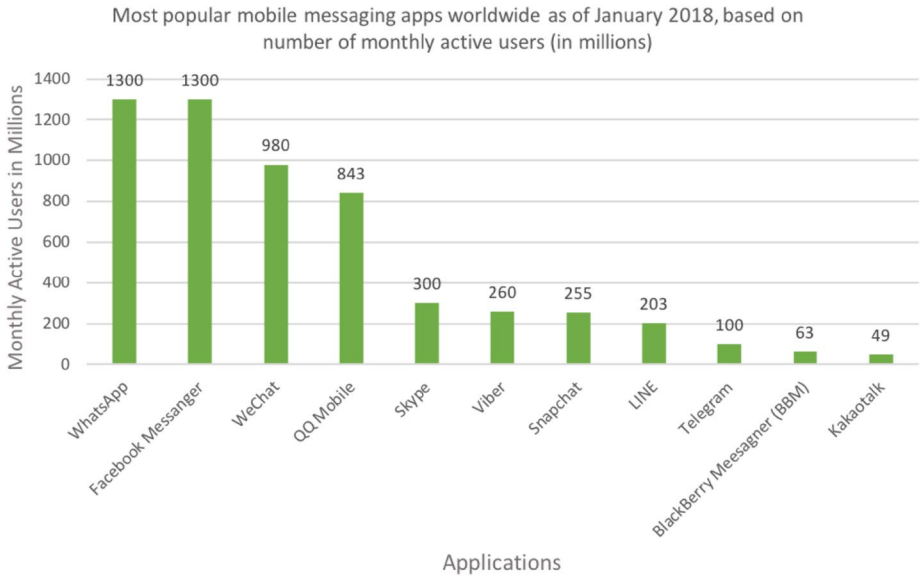

Fig. 1 Mobile messaging applications statistics [2]

Hence, in investigation cases where many mobile features and applications are involved, it is reasonable to acquire an image of the whole mobile content to carefully analyze it and search for evidences. In contrast, acquiring a whole image of the mobile device while it is certain that the crime is committed by a specific application, is a time, effort and resource consuming.

In WhatsApp cases, many investigators use Cellebrite UFED or XRY tools to make an image of the whole mobile content, or specific set of data (e.g., SMS, pictures, videos, etc.) then investigate all the extracted files to locate and analyze WhatsApp related files [4, 5]. Imaging the whole mobile without being able to extract WhatsApp evidences directly slows down the investigation process.

The use of digital forensic tools that are designed to acquire an image of the entire mobile content to investigate WhatsApp cases, is effort and time consuming. Due to the increasing cases and crucial need to accelerate the investigation process, there is a need for a WhatsApp specific forensic tool. Fortunately, there are some digital forensics tools that are designed to acquire WhatsApp data only from the suspect's devices, yet, they lack significant features. This paper aims to compare between existing WhatsApp forensics tools and asses its capabilities against NIST Test Assertions and researchers' defined criteria. This paper will identify the best acquisition method that ensures the protection of the memory and other evidences from any alteration during the investigation process. Then it will compare the existing WhatsApp Forensics tool and address its deficiencies and how comprehensive and forensically sound are the current mobile WhatsApp forensic tools.

The rest of the paper is organized as follow; Sect. 2 provides background information on mobile digital forensics. Section 3 define the structure of WhatsApp and discusses the main ideas used in WhatsApp forensics. Section 4 shows a systematic comparative study between the available WhatsApp forensics tool. Section 5 conclude the paper.

2 Digital and mobile forensics

The former director of the Defense Computer Forensics Laboratory, Ken Zatyko, defined digital forensics as "the application of computer science and investigative procedures for a legal purpose involving the analysis of digital evidence after proper search authority, chain of custody, validation with mathematics, use of validated tools, repeatability, reporting and possible expert presentation" [6]. Typically, every digital forensics investigator has to follow the investigation model to examine any case. According to Kruse and Heiser [7], authors of Computer Forensics: Incident Response Essentials, computer forensics is "the preservation, identification, extraction, documentation, and interpretation of computer media for evidentiary and/or root cause analysis." The computer investigation model shown in Fig. 2 organizes the different computer forensics elements into a logical flow. The phases can be summarized as follows:

- *Assess the situation* Analyze the scope of the investigation and the action to be taken.
- *Acquire the data* Gather, protect, and preserve the original evidence.
- *Analyze the data* Examine and correlate digital evidence with events of interest that will help you make a case. This step can be supported by the use of data-

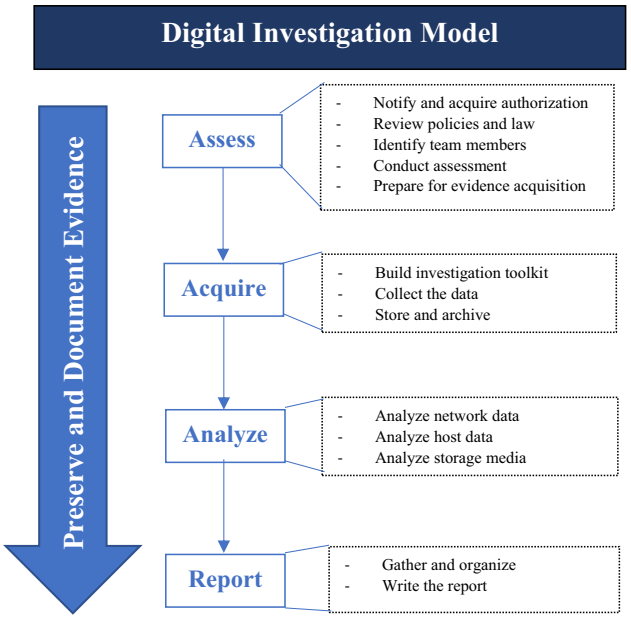

Fig. 2 Digital investigation model. (Adopted from [8])

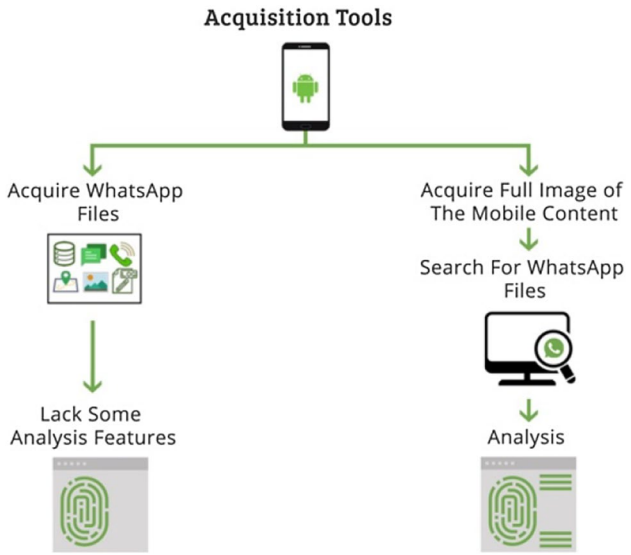

Fig. 3 The acquisition of specific application data processes

mining and machine learning techniques [9]. In fact, this combination is becoming a promising research area.

- *Report the investigation* Gather and organize collected information and write the final report.

Digital forensics has diverse branches such as computer forensics, network forensics, malware forensics, database forensics and mobile forensics [10]. There is a noticeable raise in mobile devices cases in courts [11], which triggers an urgent need of mobile forensics to suppress cybercrimes involving mobiles [12, 13]. Therefore, this section introduces mobile forensics and its acquisition types.

Mobile forensics is defined by NIST as "the science of recovering digital evidence from a mobile device under forensically sound conditions using accepted methods" [10]. Mobile forensics is considered challenging by its nature because of the increasing number of diverse mobile devices types that have various features, which span more than voice calls and texts messaging [10]. The diversity of features which are supported by mobile devices allows the investigators to acquire large amount of worthy evidences, like chat logs, multimedia files, contacts and application data [12]. Accordingly, digital forensics investigators can acquire evidences in three methods. The three methods are physical acquisition, logical acquisition and manual acquisition [12, 14]. Each of these methods differs in the technique used to acquire data and the amount of collected data [14].

1. Physical acquisition is the process of recovering the binary representation, which allows the recovery of all files, including deleted files [6].
2. Logical acquisition concerns with retrieving data of interest, such SMS, pictures and text [6]. Additionally, Srivastava and Tapaswi [6] introduces sparse acquisition which is the same as the logical acquisition but with an additional capability of retrieving fragments of deleted data.
3. Manual acquisition is the process of viewing the mobile device content and document it by taking pictures [6]. Manual acquisition is chosen when both physical and logical acquisition cannot be done [6].

As mentioned, many cases require investigating specific application rather than the whole phone content which requires the use of a logical or a sparse acquisition.

In order to seize application data, investigators can go with two-steps process. Firstly, taking a full image for the whole mobile device content. Secondly, separating and filtering the extracted files to eventually find the intended software application data. On the other hand, investigators can simply apply one-step process using specialized forensics acquisition tools, as long as there is a tool that supports acquiring the required software application data without the need to take a full mobile image. The processes are illustrated in Fig. 3.

In the latter method, acquiring the files of interests pertaining specific application is not always available in the forensics tools. Although most of the available tools support logical acquisition which acquires specific data of interest, not all of them support acquiring data related to specific application without retrieving the data belongs

to the rest. This situation falls under the logical or sparse acquisition but with more specification.

3 WhatsApp forensics

There are different tools that support WhatsApp data acquisition which are discussed in the following section. Generally, the goal of these tools is to access WhatsApp data stored in the device's protected area. The working mechanism of these tools are based on two methodologies which are: rooting the Android device or downgrading WhatsApp application. Since these two methodologies are related to WhatsApp application data acquisition, understanding their concepts, depends on understanding the structure of WhatsApp application.

This section, firstly, discusses WhatsApp application structure. Then, it illustrates the two main mechanisms that WhatsApp application acquisition tools rely on to acquire WhatsApp artifacts, which are rooting and downgrading.

WhatsApp is a free instant messaging application that allows its users to easily send and receive text messages, photos, videos, audios and many other file types. It is widely adopted since it substitutes SMS messages, expensive audio and video calls by offering same services but being free of charges [1, 15]. WhatsApp client software is available for Android, iOS and Windows platforms.

Technically, people always think about the way messages traverse from their phones through the server to the receiver, without paying attention what might be done to these messages in their phones. In fact, when the sender clicks send, the message is stored in the sender's device, transmitted to the server, received by the receiver and stored in the receiver's device [15], Fig. 4 depicts the transmission process.

Forensics investigators care about the places where the messages are stored, so it can be acquired and analyzed. According to WhatsApp Terms of Service [17], the sent messages will be stored in WhatsApp servers temporarily, until the receiver received the message, then it will be deleted. In cases where receiver does not receive the message, meaning the receiver were not online, WhatsApp server will store the message for a period of 30 days, then the message will be deleted [17].

Regarding the forensics value of the server, it definitely holds a great deal of evidences, but for a short period of time. Moreover, investigators need to deal with the company that owns WhatsApp and privacy policy to retrieve whatever evidences left in WhatsApp server, if the receiver did not receive them.

All stated conditions make investigating the server hard and time-consuming task, and here comes the importance of investigating sender's or receiver's devices as they hold the sent and received messages.

Forensically speaking, WhatsApp client stores multiple artifacts with high evidentiary values to be seized for investigation purposes, such as log files and databases. Therefore, it is critical that the investigator focuses on criminal's device to extract WhatsApp data, and it is a vital aspect for the forensics tool to be capable of extracting and analyzing all of these artifacts. Such artifacts are stored in various files and databases at different locations. Some of them are stored in the Android phone internal memory and the others are stored in the Secure Digital (SD) card [15]. Some of these important artifacts are the databases shown in Fig. 5.

Figure 5 shows a hierarchy that illustrates WhatsApp databases' structure that are stored in the internal memory. Starting with the first database, msgstore.db, which is known as the chat database. From its name, it stores detailed information about the exchanged messages in its different types, text and multimedia. msgstore.db consists of three tables, namely, messages, chat_list and sqlite_sequence, each of them has different role [15]:

- *Messages table* it is the most detailed table, it keeps a record for each exchanged message, whether it is sent or received. Such record contains two sets of information, the message content and its metadata (e.g., message type and media hash) and other mes-

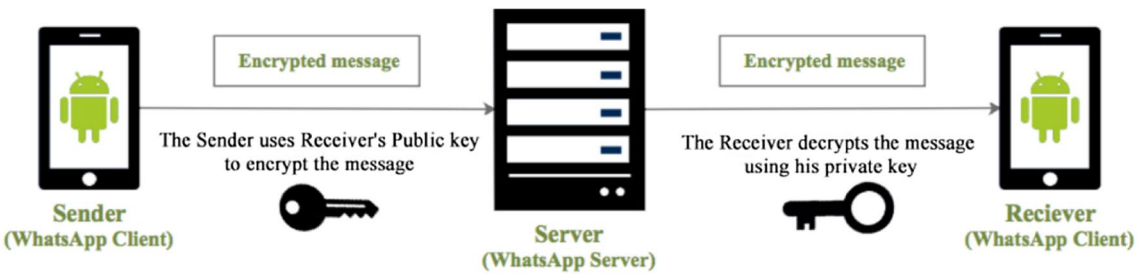

Fig. 4 WhatsApp transmission [16]

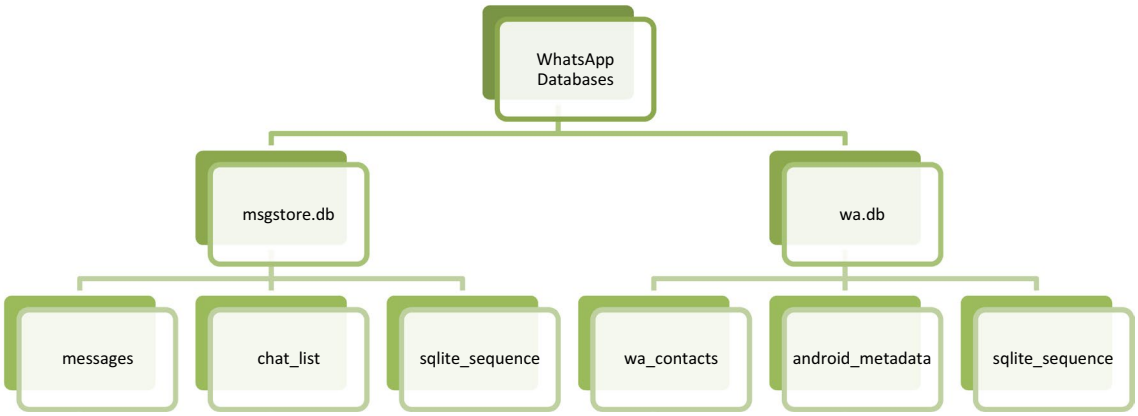

Fig. 5 WhatsApp databases structure

sage's attributes such as the communication partner, message status, timestamp, etc. [15].

- *Chat_list table* It is responsible for storing records regarding conversations, each record pertains a contacted user [15].
- *Sqlite_sequence table* It is an automatically generated table that is responsible for storing a row for each table that has an autoincrement integer primary key variable. Specifically, it has two columns that store table name and the last value of an autoincrement integer. The main functionality of this table is to keep track of the integer values and prompt a SQLITE_FULL error whenever an autoincrement variable reached its largest [18]. Being a table that holds information needed for the database to function properly made such table yields no evidentiary value in term of investigating WhatsApp cases.

The second database is wa.db, which is the contacts database. Mainly, it consists of three tables, wa_contacts, android_metadata and sqlite_sequence. However, the first table is the most important table to be discussed in this database in term of investigation since the other tables do not have evidentiary values. wa_contacts table stores a record for each added contact. Such record contains contact's WhatsApp ID, contact's name, contact's number and other information. Moreover, wa.db database is synchronized with the phonebook. Whenever a contact is added to the phonebook, it will be added in this database with a value of is_whatsApp_user field, this field is in wa_contacts table. It stores a value of 1 or 0 to denote whether the added contact is a WhatsApp user or not, respectively [15].

Since WhatsApp's files are stored in the internal memory of the sender's and receiver's devices, the investigator has to reach carefully. Thus, they commonly apply one of the two methods, rooting Android device or downgrading WhatsApp application, which are both explained in this section.

WhatsApp data is stored in the mobile device's protected area, which makes it difficult for investigators to acquire its data. Therefore, investigators seek to gain a root access in order to access this area and acquire all the required data [19]. To do so, they might need to use a custom operating system that allows rooting the device using a third-party software such as, CyanogenMod and SuperSU. According to Vidas a, Zhang and Christin [19] Android is constituted of six partitions which are system, user data, cache, boot, and recovery. The system partition contains the original operation system that android boots from [20]. While the recovery partition contains the flashed custom operating system, which allows the investigator to boot Android device from the recovery partition instead of the system partition. Therefore, the rooting process only deals with the recovery partition, which guarantees that the data stored in other partitions are not modified, and all the data can be acquired easily [21].

Some of the available WhatsApp forensics acquisition tools discussed in the following section extract WhatsApp files by downgrading, which is the process of reverting the current version of WhatsApp to an older version, specifically version 2.11.431 [22].

The reason behind downgrading WhatsApp to that exact version, lies solely on the fact that 2.11.431 version is the last version that supports Android Debugging Bridge (ADB) backup, meaning, the current version of WhatsApp does not allow Android devices to use ADB backup [22].

ADB is a command line tool provided by Android that allows Android users to communicate with Android phone through variety of ways, such as, transferring files, installing apps, debugging and restoring files [23]. The restore and backup command is only available for Android users with version 4.0 and above, and it allows Android users to back up their Android files to their preferred storage

destination [23]. Thus, the investigators downgrade WhatsApp in order to use ADB to extract WhatsApp files and databases, unencrypted, along with the cipher key [24].

To sum up, rooting mechanism deals with the recovery partition which ensures high possibility of preserving the integrity of the data resides in the user data partition [21]. However, it is device-dependent process. On the other hand, downgrading mechanism deals directly with the user data partition which contains all the evidential data, further, this mechanism requires an expert investigator since a small mistake will let them loss all the data [24], moreover, WhatsApp recent versions does not allow ADB backup nor allow downgrading, which makes tools rely on this method obsolete.

Rooting or downgrading Android mobile phone are two of the most deployed mechanisms in WhatsApp forensics tools, the subsequent section presents a comparative study of these tools.

4 Comparative study of WhatsApp forensics tools

This section mainly discusses and compares between four WhatsApp forensics tools, which are currently found in the field based on the researchers findings, namely, SalvationDATA WhatsApp Forensics, Elcomosft WhatsApp Explorer, Guasap and WhatsApp Key/DB Extractor. The comparative study is based on two main aspects, NIST Mobile Device Tool Test Assertions and Test Plan, and researchers-specified criteria.

To prove the reliability of WhatsApp application forensics tools, the researchers examined several well-known standards and test plans to select the most relevant one. It was found that NIST Mobile Device Tool Test Assertions and Test Plan [25] is the most relevant test plan to WhatsApp forensics tools. Specifically, NIST provides several core and optional test assertions that are general for all types of mobile device tools and not precise to a specific-application forensics tool. This led to the need of omitting the optional test assertions that are unrelated to the characteristics of WhatsApp Forensics Tools to improve readability. Thus, the researchers used such selected test plan as the first aspect of comparison. Table 1 illustrates the selected NIST Test Assertions.

Since NIST assertions were developed to encompass all mobile forensics acquisition tools, the scope of assertion MDT-CA-01 and MDT-CA-02 is wider than the acquisition scope required for WhatsApp tools, which makes these two assertions not applicable to WhatsApp case. MDT-CA-03 is about selecting individual data objects, which illustrates the mechanism followed by WhatsApp

Table 1 NIST specification

NNIST test assertions	Description
Core test assertions	
MDT-CA-01	If a mobile device forensics tool provides the user with an "*Acquire All*" data objects acquisition option, then the tool shall complete the logical/file system acquisition of all data objects without error
MDT-CA-02	If a mobile device forensics tool provides the user with a "*Select All*" individual data objects, then the tool shall complete the logical/file system acquisition of all individually selected data objects without error
MDT-CA-03	If a mobile device forensics tool provides the user with the ability to "*Select Individual*" data objects for acquisition, then the tool shall complete the logical/file system acquisition for each exclusive data object without error
MDT-CA-04	If connectivity between the mobile device and forensics tool is disrupted for a logical/file system acquisition, then the tool shall notify the user that connectivity has been disrupted
MDT-CA-05	If a mobile device forensics tool completes logical/file system acquisition of the target device without error, then the tool shall have the ability to present acquired data objects in a useable format via either a preview-pane or generated report
MDT-CA-06	If a mobile device forensics tool completes logical/file system acquisition of the target device without error then the tool shall have the ability to present subscriber and equipment related information (e.g., IMSI, IMEI, MEID/ESN, MSISDN) in a useable format
MDT-CA-07	If a mobile device forensics tool completes logical/file system acquisition of the target device without error then all supported data elements: PIM data (address book, calendar, notes), call logs, SMS, MMS, chat logs, stand-alone files (audio, pictures, video), application, social media and Internet related data (bookmarks, browsing history), email and GPS data shall be presented in a useable format
MDT-CA-08	If the mobile device forensics tool completes logical/file system acquisition of the target device without error, acquired data containing non-Latin characters shall be presented in their native format
MDT-CA-09	If the mobile device forensics tool completes logical/file system acquisition of the target device without error, hash values are reported for acquired data objects or overall case file
MDT-CA-10	If the logical/file system generated case file or individual data objects are modified via third-party means, then the tool shall provide protection mechanisms disallowing or reporting data modification

acquisition tools in the sense that these tools acquire some data objects, such as some pictures, videos and audios that belong to WhatsApp, rather than selecting or acquiring all data objects, such as all pictures, videos and audios, which include data objects unrelated to WhatsApp. As mentioned, NIST optional assertions were omitted due to its non-relevance to WhatsApp case, while all core assertions were included and measured in term of applicability and functionality.

However, to reach more comprehensive results about the tools, more specific comparison features are needed. Thus, the researchers had defined stand-alone features related to WhatsApp forensics tools, precisely to be used as the second aspect of comparison. The selected features are the following, *supported platforms* where the tool is installed on, *supported Android versions*, supporting of downgrading, *financial cost*, *extracted files types, supporting analysis, supported acquisition types*, *supporting hashing*, *supporting acquisition of Arabic characters*, *the methodology used for data extraction* and *the ability to generate a project for each set of files related to a case*.

The selection of these specific features was not random, in contrary, it was decided after conducting an analytical study about the required features. Specifically, the researchers considered several reasons. One reason is to measure the tool inclusiveness, compatibility, scope and effectiveness. The analysis feature was considered in term of adding bookmark, searching, filtering and exporting specific files, the existence of these options all together will eventually facilitate the investigation process. Moreover, it is important to check for hashing support to validate the integrity of the extracted files through the chain of custody. Further, the researchers considered the extraction of Arabic characters since this project is motivated by the number of WhatsApp cases in Saudi Arabia and Arabic is the native language there. In addition, the researchers considered the project arrangement feature since it arranges the investigators' work, allows adding working on multiple images related to one project, and provides easy reference for cases.

The first tool is 'Guasap forensics'. It is a Graphical User Interface (GUI) tool that allows digital forensics investigators to extract WhatsApp databases and multimedia independently [26]. It is available for download on Windows and Linux OSs [26]. It can extract WhatsApp files from all versions of Android from Petite Four to the current version, Pie, by rooting the mobile device [26]. It also extracts WhatsApp messages in any language, which is a powerful feature that satisfies NIST MDT-CA-08 test assertion [26]. The Graphical User Interface of Guasap forensics provides the following functionalities [26]:

1. Checks if the device is rooted or not.
2. Roots the device.
3. Extracts WhatsApp multimedia.
4. Extracts encrypted database.
5. Extracts WhatsApp log.

In addition, this tool generates a report that summarizes all the following results: the Android version, mobile brand, whether the device is rooted or not, the MD5 hash value of the extracted databases and a detailed log information, in one condensed HTML format [26]. The ability of Guasap forensics to calculate the hash value of the extracted databases meets NIST MDT-CA-09 test assertion.

It is worth mentioning that Guasap has two types of licenses, free open source in the Github of QuantiKa14, and a professional version in their formal website [26]. The latter differs from the previous with one functionality, which is the ability to generate a report [26]. To conclude, Guasap is compatible with NIST MDT-CA-08 and MDT-CA-09 Test Assertions since it displays non-Latin characters in their native format and calculate the MD5 hash value of the databases respectively. The rest of the test assertions are not applicable, meaning they don't exist in Guasap.

The second tool is 'Elcomosft WhatsApp Explorer' It is a Windows based, commercial, and Graphical User Interface (GUI) tool that extracts WhatsApp database from Android smartphones, iOS system backups (iTunes and cloud), and WhatsApp proprietary cloud backups on Google Drive and iCloud Drive. It supports the Android version from 4.0 to 6.0.1 when a downgrading mechanism is used, and if the root access is gained, it supports till version 7.1.1 [27]. Once it gains the root access, it extracts the database from its protected area. Otherwise, it downgrades WhatsApp to version 2.11.431 to make a backup using Android Debug Bridge (ADB), once the backup is done, it reinstalls the original WhatsApp version. Specifically, it extracts the text, images, videos, contacts and the device information. Furthermore, it provides features which are analyzing the acquired data and view it clearly and easily, filtering and searching the acquired data as shown in Table 3 [22].

As Table 2 shows, Elcomosft WhatsApp Explorer is compatible with MDT-CA-03, NIST MDT-CA-05, NIST MDT-CA-06, NIST MDT-CA-07, and NIST MDT-CA-08. Since it only acquires the data and view it in a very useful format, it does not offer a feature to take a pre-acquired image and investigate it, as MDT-CA-10 states. Furthermore, it does not satisfy the MDT-CA-09 which is an integrity requirement.

The third tool in this review is 'WhatsApp DB/key extractor'. It is a free command line tool that can be installed in several platforms, specifically, Windows, Linux and Mac. It supports multiple Android versions, from 4.0 to 7.0,

Table 2 Comparison based on NIST test assertions

NNIST test assertions	WhatsApp forensics tools			
	Guasap	Elcomosft WhatsApp explorer	WhatsApp key/DB extractor	Salvation-Data
Core test assertions				
MDT-CA-01	–	–	–	–
MDT-CA-02	–	–	–	–
MDT-CA-03	√	√	√	√
MDT-CA-04	*	*	*	√
MDT-CA-05	×	√	×	×
MDT-CA-06	×	√	×	×
MDT-CA-07	×	√	×	×
MDT-CA-08	√	√	√	√
MDT-CA-09	√	–	*	×
MDT-CA-10	×	×	×	×

√, Succeeded; ×, Failed; –, Not applicable; *, no available information

namely, Ice Cream Sandwich, Jelly Bean, KitKat, Lollipop, Marshmallow or Nougat [28]. WhatsApp DB/key extractor is capable of extracting WhatsApp DBs along with the decryption key of non-rooted Android devices [28]. Mainly, it can extract msgstore.db and wa.db databases [8]. Further, it has a point of strength in which it supports non-Latin languages [8] (e.g. Arabic) which meets NIST MDT-CA-08. To seize WhatsApp data, it relies on the downgrading methodology.

Although WhatsApp DB/key has worthy features, it has some notable limitations that show its fail of critical NIST Assertions which affects its usability. First of all, it does not have the ability to extract videos, audios and documents [7] which are worthy media files that might be a rich source of evidences. Thus, such limitation might have a great consequences on the investigation process. Although it has the ability to extract images, it results in low quality images with a fixed resolution of 56 × 100 pixels [7]. Besides, this tool is limited to extraction only, and needs an integration of analysis tools to provide the highest value [8]. In addition to all the mentioned limitations, the tool is compatible only with NIST MDT-CA-03 and MDT-CA-08, which means it satisfies two out of eight assertions since MDT-CA-01 and MDT-CA-02 are not applicable.

The fourth tool is 'SalvationDATA WhatsApp Forensics tool'. It is a free graphical user interface tool that can be installed on all Windows versions, it almost supports all smartphones Operating System (OS), and it is capable of decrypting encrypted WhatsApp backups. This tool extracts all WhatsApp databases and recovers logs and deleted messages [9]. SalvationDATA succeeded in NIST MDT-CA-03, MDT-CA-04 and MDT-CA-08, but failed in the rest test assertions.

Table 3 Comparison based on researchers-specified requirements

Comparative features	WhatsApp forensics tools			
	Guasap	Elcomosft WhatsApp explorer	WhatsApp key/DB extractor	Salvation-Data
Works on Windows platform	♦	♦	♦	♦
Works on Linux platform	♦	◊	♦	◊
Works on Mac platform	◊	◊	♦	◊
Support multiple Android versions	♦	♦	♦	♦
Support Android Version 9	♦	◊	◊	◊
Downgrading WhatsApp	◊	♦	♦	♦
Free	♦	◊	♦	♦
Commercial	♦	♦	◊	♦
Extracts text	♦	♦	♦	♦
Extracts images	♦	♦	♦	◦
Extracts videos	♦	♦	◊	◊
Extracts contact	♦	♦	♦	♦
Extracts deleted messages	♦	*	*	♦
Support analysis	□	♦	◊	◊
Logical acquisition	♦	♦	♦	♦
Support acquisition of Arabic characters	♦	♦	♦	◊
Hashing	♦	◊	◊	◊
Project arrangement option	◊	◊	◊	◊

♦, supported; ◊, not supported; □, partially supported; *, no available information

This tool uses downgrading mechanism to allow the retrieval of plaintext form of WhatsApp encrypted data, by downgrading the current WhatsApp version to v.2.11.431, this version does not force encryption on its backup, so investigator can do backup after the downgrading and get unencrypted backup and a key generated with the backup [24]. After the downgrading is done successfully, investigators can analyze the unencrypted backup or input the generated key with the encrypted backup, which is taken prior the downgrading, to the tool for the decryption. The tool generates unencrypted WhatsApp backup to be inserted to another tool for analysis [24].

Table 2 summarizes the comparison results based on the selected NIST Test Assertions. The agenda below the table explains the symbols used in the table.

Table 3 summarizes the comparison of the studied WhatsApp forensics tools based on the researchers-specified features. The agenda below the table explains the symbols used in the table.

As shown from NIST comparison, Table 2, MDT-CA-01 and MDT-CA-02 are not applicable to all of the studied WhatsApp forensics tools. Moreover, only one tool, Guasap, satisfies MDT-CA-09 which is an important option for the chain of custody to maintain the evidences integrity. Additionally, all the tools failed to satisfy MDT-CA-10.

As for the strengths, all the tools satisfy MDT-CA-03 and MDT-CA-08. The results of the other test assertions are varied among the tools. However, as shown from the conducted analysis, Elcomosft WhatsApp Explorer is the most compatible tool with NIST among the others since it passed five out of eight test assertions.

On the other hand, Table 3 shows that all the studied tools support multiple features. Nevertheless, all of them lack critical features that WhatsApp Forensics Tools must have to provide the greatest value for WhatsApp forensics investigations.

Starting with the positive side, all of the tools support multiple Android versions. Also, all of them provides a free version except Elcomosft WhatsApp Explorer. Further, Guasap and Elcomosft both are capable of extracting all types of data, text and multimedia, but not WhatsApp SalvationData and Key/DB Extractor.

As for the downsides, WhatsApp Key/DB Extractor is the only tool that can be installed and run on all the three platforms, Windows, Linux and Mac. Although the majority support multiple Android versions, only Guasap supports the latest version (version 9). Moreover, none of them support analysis except Elcomosft WhatsApp Explorer, which supports all analysis features but lacks bookmark option. Regarding the hashing feature, only Guasap satisfied this criterion. Further, none of these tools provides project management option.

Based on the conducted analysis, it is clearly shown that there is a deficiency in the current WhatsApp Forensics Tools as they do not satisfy all the required features to facilitate the investigation process.

Three out of four of the mentioned tools use downgrading methodology, which mainly interacts with users' data, this interaction raises the surface of data loss since it requires experience and cautious. Moreover, analysis, hashing, reporting and comprehensive data extraction are only supported in some of the tools. More importantly, none of the mentioned tools arrange the case files in project bases.

These reasons justify the need of developing a comprehensive tool that meets all the needed features, and satisfies the applicable NIST assertions. Such tool will assist the investigator by accelerating the investigation process with less effort.

To summarize, investigating WhatsApp files can be done in two methods, the first method is acquiring the whole device and then selecting the files that related to WhatsApp. The second method is to use a tool that allows direct extraction of WhatsApp data, such as Guasap, Elcomosft WhatsApp Explorer, WhatsApp Key/DB Extractor and SalvationData. Although there are various types of WhatsApp forensics tools, there is no tool that satisfies all the applicable NITS core assertions nor encompasses all the needed features specified by the researchers. Therefore, there is a need to develop a WhatsApp Forensics Tool that compensates the deficiencies found in the existing tools.

5 Conclusion

This research thoroughly analyzed and compared currently available WhatsApp forensics tools. The aim is to Address the problem faced when investigating WhatsApp cases, which is the complex acquisition and analysis of the case data. In fact, increases the efforts and time consumed by the investigators.

Foremost, the researchers scanned the field for the existing WhatsApp forensic tools. The research revealed four main tools, namely, SalvationDATA WhatsApp Forensics, Elcomosft WhatsApp Explorer, Guasap and WhatsApp Key/DB Extractor. Secondly, a detailed comparative study was conducted. The study consists of analysing the functionalities and the forensic analysis features supported by each tool. The comparison was based on two main aspects, NIST test assertions and test plan, and researchers-based criteria.

The results showed that these tools lack critical features, either in terms of the researchers-based criteria, NIST test assertions and test plan or the used key access method. Such result justifies the need for a comprehensive

WhatsApp forensic tool that compensates the deficiencies found in the previous tools and preserve the evidences' integrity.

Compliance with ethical standards

Conflict of interest The authors declare that they have no conflict of interest.

Human and animal rights This article does not contain any studies with human participants or animals performed by any of the authors.

References

1. Gudipaty LP, Jhala KY (2015) WhatsApp forensics: decryption of encrypted whatsapp databases on non rooted android devices. Inf Technol Softw Eng 5(2):1
2. Statista (2018) Most popular mobile messaging apps worldwide. Statista. https://www.statista.com/statistics/258749/most-popular-global-mobile-messenger-apps/. Accessed 4 Oct 2018
3. Magnet Forensics (2014) The rise of mobile chat apps: recovering evidence from kik messenger, Whatsapp and BBM (White Paper), 11 November 2014. https://www.magnetforensics.com/mobile-forensics/the-rise-of-mobile-chat-apps-recovering-evidence-from-kik-messenger-whatsapp-bbm/. Accessed 15 Oct 2018
4. Smarterforensics (2014) Explaining Cellebrite UFED data extraction processes. https://smarterforensics.com/wp-content/uploads/2014/06/Explaining-Cellebrite-UFED-Data-Extraction-Processes-final.pdf. Accessed 2 Oct 2018
5. Leahy Center for Digital Investigation, 19-11-2014. https://www.champlain.edu/Documents/LCDI/Windows_OS_Tutorial_Final_PDF.pdf. Accessed 5 Oct 2018
6. Srivastava H, Tapaswi S (2015) Logical acquisition and analysis of data from android mobile devices. ProQuest 23(5):450–475
7. Kruse W, Heiser J (2001) Computer forensics: incident response essentials. Addison Wesley, Boston
8. Pande J, Prasad A (2016) Digital forensics. Uttarakhand Open University, Haldwani
9. Raburu G, Omollo R, Okumu DO (2018) Applying data mining principles in the extraction of digital evidence. IJCSMC 7(3):101–109
10. Anglano C (2014) Forensic analysis of WhatsApp Messenger on Android smartphones. Digit Investig 11(3):201–213
11. Maxim C, Sherali Z, Zubair B, Andrew W (2017) Mobile forensics: advances, challenges, and research opportunities. IEEE Secur Priv 15(6):42–51
12. WhatsApp (2017) WhatsApp security white paper, 19 December 2017. https://www.whatsapp.com/security/WhatsApp-Security-Whitepaper.pdf. Accessed 5 Dec 2018
13. WhatsApp (2016) Terms of service, 25 August 2016. https://www.whatsapp.com/legal/#privacy-policy. Accessed 21 Oct 2018
14. SQLite (2004) Database file format. SQLite, 18-6-2004. https://www.sqlite.org/fileformat.html#the_sqlite_sequence_table. Accessed 20 Nov 2018
15. Bill N, Amelia P, Christopher S (2015) Guide to computer forensics and investigations: processing digital evidence. Cengag Learning, Boston
16. Hassan M, Pantaleon L (2017) An investigation into the impact of rooting android device on user data integrity. In: 7th IEEE international conference on emerging security technologies
17. Levin J (2015) Android internals a Confectioner's Cookbook. Technologeeks, Cambridge
18. Vidas T, Zhang C, Christin N (2011) Toward a general collection methodology for Android devices. Elsevier, Amsterdam, pp S14–S24
19. Oleg A (2017) Extracting WhatsApp conversations from Android Smartphones, 2 February 2017. https://blog.elcomsoft.com/2017/02/extracting-whatsapp-conversations-from-android-smartphones/. Accessed 14 Oct 2018
20. Android (2018) Android debug bridge (adb), Android, 24 September 2018. https://developer.android.com/studio/command-line/adb
21. SalvationDATA (2018) WhatsApp forensics: decryption of encrypted databases and extraction of deleted messages on non-rooted Android Devices, 8 February 2018. https://blog.salvationdata.com/2018/02/08/whatsapp-forensics-decryption-of-encrypted-databases-and-extraction-of-deleted-messages-on-non-rooted-android-devices/. Accessed 1 Oct 2018
22. National Institute of Standards and Technology (2016) Mobile device tool test assertions and test plan, 1 Febrauray 2016. https://www.nist.gov/sites/default/files/documents/2017/05/09/mobile_device_tool_test_assertions_and_test_plan_v2.0.pdf. Accessed 1 Oct 2018
23. quantika14, "Guasap Forensic," quantika14. https://quantika14.com/guasap-forensic/
24. Elcomsoft desktop, mobile and cloud forensics, "Elcomsoft Explorer for WhatsApp". https://www.elcomsoft.com/exwa.html. Accessed 14 Oct 2018
25. TripCode (2016) WhatsApp-Key-DB-Extractor, GitHub, 21 October 2016. https://github.com/EliteAndroidApps/WhatsApp-Key-DB-Extractor. Accessed 18 Sept 2018
26. Umar R, Riadi I, Zamroni GM (2017) A comparative study of forensic tools for WhatsApp analysis using NIST measurements. Int J Adv Comput Sci Appl 8(12):69–75
27. Umar R, Riadi I, Zamroni GM (2018) Mobile Forensic tools evaluation for digital crime investigation. Int J Adv Sci Eng Inf Technol 8(3):949–955
28. SalvationDATA (2018) SalvationDATA WhatsApp forensics free tool official release, 8 March 2018. https://blog.salvationdata.com/2018/03/08/salvationdata-whatsapp-forensics-free-tool-official-release/. Accessed 1 Oct 2018

Publisher's Note Springer Nature remains neutral with regard to jurisdictional claims in published maps and institutional affiliations.