

# Forensic Investigations of Popular Ephemeral Messaging Applications on Android and iOS Platforms

M A Hannan Bin Azhar, Rhys Cox and Aimee Chamberlain

School of Engineering, Technology and Design

Canterbury Christ Church University

Canterbury, United Kingdom

e-mail: [hannan.azhar@canterbury.ac.uk](mailto:hannan.azhar@canterbury.ac.uk); [rhys-1998@hotmail.co.uk](mailto:rhys-1998@hotmail.co.uk); [aimee.chamberlain@yahoo.co.uk](mailto:aimee.chamberlain@yahoo.co.uk);

**Abstract**—Ephemeral messaging applications are growing increasingly popular on the digital mobile market. However, they are not always used with good intentions. Criminals may see a gateway into private communication with each other through this transient application data. This could negatively impact criminal court cases for evidence, or civil matters. To find out if messages from such applications can indeed be recovered or not, a forensic examination of the device would be required by the law enforcement authority. This paper reports mobile forensic investigations of ephemeral data from a wide range of applications using both proprietary and freeware forensic tools. Both Android and iOS platforms were used in the investigation. The results from the investigation uncovered various artefacts from the iOS device including account information, contacts, and evidence of communication between users. The Android device uncovered evidence of communications, and several media files assumed to be deleted within a storage cache in the Android file system. The forensic tools used within the investigations were evaluated using parameters from the National Institute of Standards and Technology's (NIST) mobile tool test assertions and test plan.

**Keywords**— *Mobile forensics; Digital forensics; NIST measurements; Oxygen Forensics; Ephemeral messaging apps; EMAs.*

## I. INTRODUCTION

The growth of ephemeral messaging applications (EMAs) is also posing a problem to the enforcement of law, with apps being proving a concern for activities like cyberbullying [1] or even high-end criminal activity like terrorism [2]. Criminals may use regular chatting applications, but there is a growing opportunity within the mobile application market for criminals to use ephemeral messaging applications, which allow users to send messages/multimedia etc. to each other with the messages only lasting for a certain period of time [3]. Barker [4] reported that criminals are moving away from dark web interactions and onto EMAs such as Facebook Messenger, Snapchat, and Wire etc. It is thought this is happening because data in these applications is known to delete itself, which is prime for criminal communications. For example, Snapchat allows users to send 'Snaps' to each other containing pictures, which are deleted once the recipient user closes the message [5].

It is not just criminals using EMAs. Mobile phones are an essential part of modern-day life. According to the Global System for Mobile Communications [6], there were five billion mobile users in the world by the second quarter of 2017, with a prediction that another 620 million people will become mobile phone users by 2020, together that would account for almost three quarters of the world population. Due to the increasing popularity in mobile phones, there is naturally an increasing concern over mobile security and how safe communication between individuals or groups is. It is known that EMAs can be used in civil concerns such as evidence of liability in business [7]. Most notably, the United States department of justice imposed heavy restrictions on the use of EMAs by employees in 2018 as part of a scheme to reduce illegal bribery within businesses [8]. The rationale for the use of the applications was reported to be more complex than covering tracks, and that employees themselves had started to turn to using them of their own accord for reasons such as more reliable service. From this, it is clear that the use of EMAs is moving from the use of criminals and privacy advocates, to the general populace as well.

The two most popular EMAs on the mobile market currently are Snapchat and Facebook Messenger. According to Constine [9], Snapchat has a daily user total of 190 million users. According to Noyes [10], Facebook messenger has an average daily user intake of 2.1 billion users. The statistics show a high intake of users within these EMAs. With the ever-growing ephemeral market, it is vital to both civil matters and criminal cases to find out just how truthful the applications are about data being deleted and unrecoverable.

With all the opportunities for new crimes to be committed through growing technology, it is crucial to ensure law enforcement agencies have the appropriate software and methods to deal with these crimes. This paper will report forensic investigations of two mobile phones: one on an Android and the other on iOS platforms. The Android device was rooted; however, the iPhone was not jail broken. This will give an interesting insight to the investigation as different amounts of data may be recovered according to if the device is rooted or not. This paper will be using a variety of forensic tools to extract the mobile devices as well as comparing and examining each tool according to the NIST Measurements Mobile Device Tool Test Assertions and Test Plan [11]. The main contributions include a taxonomy of tools for forensic

analysis of mobile platforms, along with hands-on tests of these tools on several Android and iOS messaging apps. The paper's results cover the relative effectiveness of the forensic frameworks, as well as various interesting security findings among the mobile apps.

The remainder of the paper will be organised as follows: Section II will discuss existing research in relation to mobile phone forensics, including forensic tools and ephemeral data. The methodology used during the analysis process will be discussed in Section III. Results and analysis will be reported in Section IV. Finally, Section V will conclude the paper and include possible future work.

## II. LITERATURE REVIEW

There is already a vast amount of research on mobile forensics in general, which includes comparing forensic tools, performing different types of mobile acquisitions and focusing on particular pieces of data within the mobile device. There is also work completed on non-EMAs, such as Ovens et al. [12] conducted a forensic analysis on Kik Messenger on iOS. While there have been similar studies in a wide range of apps, the focus of this review is to highlight the findings in extraction of artefacts from the apps, which are specifically ephemeral.

One study undertaken by Sathe et al. [13] provided a broad overview of the available forensic acquisition methods for mobile device forensics, including several freeware options. The study undertook comprehensive analysis of both physical and logical data acquisition options and compared those options via several categories, i.e., Cost, Accuracy, Data Integrity, Training required, OS reliance, Root required etc., all of which would prove useful for identifying the practicality of the tools/techniques in professional scenarios, as well as the forensic soundness of the techniques in question, a pertinent characteristic when dealing with more disruptive techniques, such as those which require root access, as any alteration to the data stored within a device/image may well remove the reliability of a given piece of evidence in the eyes of the court. The results of the study showed that of the chosen forensic tools, AFLogical, Andriller and Dr. Fone toolkit, each provided evidence data in areas, which the other was lacking, leading to the conclusion that the use of multiple forensic tools in a given mobile forensic investigation may well be ideal.

Azhar et al. [14] conducted a forensic experiment of two EMAs: Telegram and Wickr using Autopsy and logically acquiring a database file, as well as performing a RAM dump. Results showed that the application 'Wickr' stored received messages in encrypted "wic" files. The RAM dump recovered username information from Wickr and artefacts from Telegram. This investigation was an Ephemeral application comparison using Android platforms. The investigation more looked into packages and files within the application itself instead of using a mobile forensic tool. This would be interesting for future work as well as perhaps performing the same investigatory analysis on an iOS device.

Al-Hadadi et al. [15] forensically investigated a mobile device, an iPhone 4 running iOS 5.0.1 previously jailbroken by the mobile phone owner, as a part of a real legal case. The

case was from the Sultanate of Oman, and the aim of the investigation was to forensically examine the iPhone to determine if the device had been hacked and sent messages over the application 'WhatsApp' out to the owner's contact list. In the investigation, the ISP report of the device was observed and examined, and two forensic tools were used to extract and examine mobile data, one tool being the Universal Forensic Extraction Device's (UFED) physical analyser Cellebrite, and the other being the Oxygen Forensic Suite. The credibility of both tools is highly regarded by computer forensic experts. Results showed that Cellebrite recovered more forensic evidence than Oxygen, including call log artefacts, SMS messages, web history, etc.

Another study, by Umar et al. [16] investigated the specific forensic evidence recoverable from the use of WhatsApp, a popular secure messaging application. The study took a rooted mobile device with Android 5.0.1 and used it in communications with a second device in order to simulate the standard daily use of the application. The mobile device was then forensically analysed by 3 different mobile forensic tools: WhatsApp DB/Key extractor, Belkasoft Evidence and Oxygen Forensic Detective 6.4.0.67. In addition to comparing the results of each tool's analysis, the tools were assessed by various levels of the NIST Mobile device tool test assertions [11], a set of test requirements and guidelines produced to assist in the evaluation of mobile forensic tools. Each tool was assessed by all the baseline assessments and a select number of the optional assessments, before comparing the tools by the number of assessments they passed. The results of the study revealed that Oxygen Forensic Detective provided the most forensically valuable data, managing to identify evidence of the test data in both logical and physical extraction, and passed the most assessment parameters put against it by the NIST guidelines, failing only five out of the twenty-two assertions and functionality tests.

A study undertaken by Naughton et al. [17] provided an investigation into data left by specific apps on mobile and personal devices. Said study utilised two mobile devices, using Android and IOS respectively, alongside a windows 10 based laptop using an Android emulator. The applications selected for the study included various shared and device/OS specific apps, including two ephemeral apps: Snapchat and Instagram. Each device was used to gather forensically valuable data before undergoing forensic analysis, after which the data would be deleted to simulate a criminal covering their tracks and would undergo analysis once more. The study showed detailed information of what each forensic tool could recover from the test devices, with subcategories for each specific application, device and file type. While less focussed on the tools utilised during analysis, this study put heavy focus into the realism of the forensic analysis within the experiment, going as far to consult digital forensic specialists and 15 separate police forces within England and Wales to ensure the experiment would prove as realistic a scenario as possible, a level of justification lacking in every other study found. The results of the study showed that the laptop and the iPhone provided the most forensically valuable data through analysis, and, more relevantly, that both EMAs used in the study, Snapchat and Instagram, provided no recoverable data that the

chosen forensic tools, Cellebrite UFED and Autopsy, could identify.

As can be seen from this brief review of the literature, there is not much reported literature in extraction of ephemeral artefacts especially on iOS platforms. This paper will contribute to investigate artefacts recovery from both iOS and Android using wide range of EMAs. Comparisons will be made in evaluation of artefacts recovered using various tools following the guidelines by the NIST Measurements Mobile Device Tool Test Assertions and Test Plan [11]. The paper's results cover the relative effectiveness of the forensic frameworks, as well as various interesting security findings among several Android and iOS messaging apps.

### III. METHODOLOGY

Methodology section will detail choice of devices, chosen applications, forensics tools used and investigation process including the testing methodologies using NIST measurements. The investigation was carried out according to the four good practice guidelines of the Association of Chief Police Officers (ACPO) [18]. For example, the third principle of the guidelines state that an audit trail should be recorded throughout the investigation in a manner, such that a third party could recreate the steps taken in the investigation and get the same results.

#### A. Chosen Devices

The two mobile devices used within the investigation was an iOS device: iPhone 6s [19], and an Android device: Vodafone VF695 [20]. According to Jkielty [21], there is just a 2.3% difference in UK in the market share between Android and iOS devices, with the iOS market having the edge. Vodafone was running an Android 4.4.2 (KitKat) OS and iPhone had iOS 9. To investigate wide range of exploits, one of the phones was rooted (Android). Having the root level access, it was hoped to gain more access to recover detail artefacts, including deleted files. In case of root level access, while forensic soundness can be questioned, the artefacts could still be valuable giving clues to further direction of investigation, which eventually may lead to gather concrete evidences to be presented in court with sufficient justification.

#### B. Ephemeral Applications

A wide range of ephemeral messaging apps were selected for the investigation as listed in Table I. Some applications are more popular (Snapchat for iOS and Facebook Messenger for Android) than the others but they all varied in their ephemeral features and target audiences. Details of these applications are given next.

1) *iOS Applications*: Applications as listed for iOS in Table I were all chosen for different reasons. Snapchat is one of the most popular EMAs. According to Omnicore [28], more than 25% of mobile phone users are on Snapchat, with 71% of the users being aged between 17 to 24. Cyberdust, was chosen due to the difference in its ephemeral features compared to other apps. The encrypted messages within the app delete themselves between users after 24 hours of it being sent [23]. The application also has other uses, such as a “watchdog” feature where users can check their email

addresses to see if any data breaches have been completed. Another feature is known as “Stealth Search”, where users can search the Internet privately, supposedly without any cookie trackers or trace remnants. This application was selected for the investigation as it creates ephemeral data, and it has many different functions, which allows the user to use the application for multi-purpose functions.

TABLE I. MOBILE DEVICE AND APPLICATIONS

Mobile used	Ephemeral Messaging Apps	
	App Name	Version
iPhone 6s	Snapchat [22]	10.55.1
	Cyberdust [23]	5.6.1.1049
	Confide [24]	8.3.1
Vodafone VF695	Facebook Messenger [25]	215.1.0.21.101
	Signal [26]	4.39.4
	Wire [27]	3.30
	Confide [24]	5.9.5

The final application, Confide [24], was chosen because of its end to end message encryption between users. Furthermore, the application does not allow screenshots to be taken from users. The messages between users are self-destructing once the recipient has read the message, and the user can only read the message by swiping down on the message on the screen to view it. Furthermore, the user can adjust the settings to change the ephemeral nature of the messages, if a message is not opened within 48 hours, the content of the message will delete itself regardless. All of these features would create an interesting investigation, as the application advertises very strong messaging security, so it would be intriguing to test the security through this forensic investigation.

2) *Android Applications*: Like iOS, Confide was also used for the Android investigation. Among other applications, Facebook Messenger is one of the most popular EMAs on the market with a similar popularity to Snapchat, as used on the iOS device. According to Google Play[29], as of March 2020 Facebook Messenger has over one billion downloads on the Android market. Facebook Messenger has a recent implementation of a new feature, which is a secret conversations function. It can facilitate encrypted and ephemeral communications between two parties, utilising the signal messaging protocol as previously used in the application ‘Signal’ description. The ephemeral features exist as a set of optional timers, with 11 delay options between 5 seconds and a day.

Signal is an open source encrypted messaging application with ephemeral capabilities, developed by the company of the same name. As a company, Signal is responsible for producing an encryption-based messaging protocol, also by the same name, which is utilised by multiple other secure messaging applications like WhatsApp and Facebook Messengers secret conversations feature [30]. Signal’s ephemeral capabilities come in the form of an optional timer to set for messages, with 11 different settings between five

seconds and one week delays for removal. All of this information makes it a perfect EMA for forensic investigation.

The next application was Wire, which is a secure messaging application developed by Wire Swiss [27] and includes ephemeral messaging features. The application is targeted for use in business, with a majority of its promotional descriptions detailing secure communications between teams of employees, and further detailing its free version as ideal for home or family use. The ephemeral capabilities of Wire exist as a set of 6 optional timers between 10 seconds and 4 weeks delay. Its popularity is around twice as much as Confide, with over 1 million downloads on the Google play store.

### *C. Forensic Tools*

Oxygen Forensic Detective Enterprise [31] version 10.3.0.100 is a commercial forensic tool that was used to extract and examine both the iOS and the Android phone. Oxygen Forensic Detective is a specialised mobile forensics tool developed by Oxygen Forensics Inc and utilised by professional digital forensic investigators in law enforcement. The specific extraction capabilities for the tool range depending on the device being analysed, but in general it provides several options for extraction depending on the individual device requirements, and provides highly detailed and clear visual representations of the data both in the applications user interface and in the reports it can produce. Various viewers are built into Oxygen Forensic Detective, allowing users to view the contents of files such as SQL databases within the program and make reports specifically from the contents [31].

MOBILedit Forensic Express [32] version 6.1.0.15480 is a commercial forensic tool that was used to extract and examine the iPhone device. MOBILedit can create a logical and physical acquisition of a mobile device and can recover deleted files as well as retrieve mobile data. It is used widely across law enforcement in over 70 countries and is also used in military investigations [32].

Andriller version 3.0.3 [33] is an Android specific proprietary forensic tool developed by the software team of the same name and allows for data extraction from both rooted and unrooted Android devices. This tool was used to extract and examine the Android device. Data extracted from suitable devices is extracted to a directory of the users choosing in the form of several different reports, and folders for shared storage data. Various utility tools come alongside the extraction capabilities, such as a screenshot function, lockscreen decoders and specific database decoders for a specific list of supported applications and sources. For the purposes of this experiment a trial licence was acquired to use the full version for a time period of 30 days.

FTK Imager version 4.1.1.1 is a freeware disk analysis tool produced by AccessData [34] as part of their Forensic Toolkit product range. This forensic tool was used to extract and examine the Android phone. While only a free version of the products AccessData have produced, FTK Imager is still a versatile tool for extracting disk and RAM images, as well as analysing existing forensic images. Lacking elaborate methods of displaying extracted data, FTK displays the filesystem of the chosen image files and provides both

plaintext and hexadecimal viewing panes to display file contents. While not intrinsically advertised as a mobile forensic tool, FTK Imager is still capable of analysing an existing image file extracted from a mobile device and could serve as a mobile forensic analysis tool if necessary.

Autopsy 3.0.8 [35] was used to analyse a forensic image file. Autopsy is the graphical frontend for a set of Linux forensics tools called the Sleuthkit. This contains tools that allow for the recovery of deleted data. Autopsy also allows for the processing of unallocated space, which is an important part of the analysis as ephemeral messaging functions rely on the deletion of data. Artefacts such as deleted files sent as attachments to messages can be recovered using Autopsy [14].

Kali Linux is not a forensic tool, instead an operating system that was used for forensic analysis on the Android device. It can produce disk and mobile devices images through the use of the DD command, which serves to create a bit for bit copy of a file or directory. Accessing a mobile device to utilise this method of imaging requires several other tools, Android debug bridge and BusyBox, on top of rooting the device to allow direct access to the mobile devices root directory. As a result, imaging a mobile device with this method is highly questionable in its forensic soundness, however it is still a viable technique in the event a device requires imaging without specialised tools and equipment. While not being assessed as a forensic tool, given its only functionality is copying data bit for bit, both Autopsy and FTK Imager would be using image files produced by Kali Linux for their analysis as an example of full data extraction and analysis with freeware tools [36][37].

### *D. NIST Measurements*

NIST, otherwise known as the National Institute of Standards & Technology, is an institution based on technological and scientific advancement. They provide data and professional standards of technology for multiple scientific fields, including the forensic sciences. To ensure the quality and functionality of the tools, equipment and practices utilised [11]. NIST produced a set of standards detailing ten baseline functionality standards and twenty-two optional standards for assessing tools on their suitability for mobile forensic extraction and examination. The main goal of the guidelines is to determine a tool's ability to accurately acquire specific data objects populated onto the feature phone, smart phone, tablet or credit cards. Before proceeding with the examination of the target mobile device for this research, the tools would be assessed with the ten baseline test assertions, MDT-CA-01 through to MDT-CA-10. For example, the first test assertion, MDT-CA-01, indicates if a mobile device forensic tool provides the user with an "Acquire All" data objects acquisition option then the tool should complete the logical or filesystem acquisition of all data objects without error. An accurate acquisition copies means that the bytes of the acquired data object are identical to the bytes of the data object on the device. The NIST guidelines also have some optional assertions focussing on physical extraction ability of a tool, which were omitted for the tests as all versions of the tools used for analysis lacked those features by default.

### E. Testing Methodology

The iPhone 6s was extracted and examined first using Snapchat on the iPhone device. For this application, three contacts were added and two of those contacts had communication sending picture messages, as well as written messages back and forth. Ten picture messages were exchanged, three written messages were marked as 'saved', while one of other messages was not saved. The username for the mobile owner was 'aimee\_test19'. For the Snapchat, the ephemeral artefacts were the picture messages for the investigation.

Cyberdust had a total of eleven messages exchanged. Two of the messages were picture messages. The username for the mobile owner was linked directly to the mobile number of the device instead of an account like Snapchat.

Confide had a total of seven messages exchanged on the iPhone device. Like Cyberdust, here also the username for the mobile owner was linked directly to the mobile number. For the investigation's purpose, only the secure messaging feature was used, where messages were encrypted and deleted after 24 hours.

Oxygen Forensic outputs a GUI home page, which displays the kinds of information that has been extracted, allowing an investigator to navigate around the mobile contents easily. The 'Applications' tile was selected to investigate the three Ephemeral applications mentioned previously, including any data the applications held of the user, conversation data, etc. Once the 'Applications' tile was examined, the 'Passwords' tile was selected and examined. This was to see if any passwords were stored within the three EMAs to test the general security of the applications.

The same extraction process was completed in MOBILedit Forensic Express [8]. Unlike Oxygen, MOBILedit outputs the mobile device extraction into a report. However, there was a contents page produced within the report. There was also a separate section for both 'Applications' and 'Passwords' similarly to Oxygen. Both of those sections were examined. In the next stage of the examination, a general keyword search was made within the Oxygen and MOBILedit in search for artefacts. The keywords searched included 'Snapchat', 'Dust' and 'Confide'. This was completed in case any other information relating to the applications was extracted and missed previously. The application names were used for the searches, as in a real-life scenario the digital forensic investigator may not know the contents of the messages and may be left with no other search options other than the application names.

Next, the Android device was extracted and examined by the nominated forensic tools. Assessment of the supported messaging capabilities within each application was performed and then messaging transcripts for each of the applications were produced, detailing the messages and attachments sent between the Android phone and a personal phone. Each application would be used to produce five distinct text-based messages, exchanges of specifically named image files, and then exchanges of distinct audio messages and document files for the apps that supported audio and file-based attachments.

Once the test data was created to the specifications of the transcripts, the device was then forensically analysed, first by the proprietary forensic tools and then the freeware forensic tools. The forensically valuable artefacts were recorded through screenshots and were extracted, if necessary, to identify contents, in the case of the media file attachments. Once thorough analysis of the device was performed with all four chosen tools, the applications were then uninstalled from the device to simulate anti-forensic activity, after which a second stage of analysis was then performed to see if any of the artefacts recovered in the first stage of analysis were still recoverable in a forensically valuable form.

## IV. RESULTS

This section covers the key findings from the analysis described in Section III. The results will be broken down into multiple sections: iOS results from forensic tools used to extract the iPhone 6s, Android results from the forensic tools used to extract the Android Vodafone VF695.

### A. Oxygen Forensic for iOS

A list of applications on the mobile device was found in the 'Applications' tile using Oxygen. Snapchat was the first application to be investigated. Figure 1 shows Snapchat data. Four areas were highlighted within the figure. This included the login username 'aimee\_test19', that was used to log into Snapchat and detection of an 'offensive words' used in messages. The next highlighted section was the evidence that there was messaging communication between a user 'aimee\_test19' and another user. The final highlighted section shows a chat deletion message count with a value of one, which indicates that a message was deleted by the user, which was a true case. A general search of the extracted mobile device was conducted using the search feature on Oxygen Forensics. The findings included general application data within the file browser, such as the Snapchat library, stickers, etc.

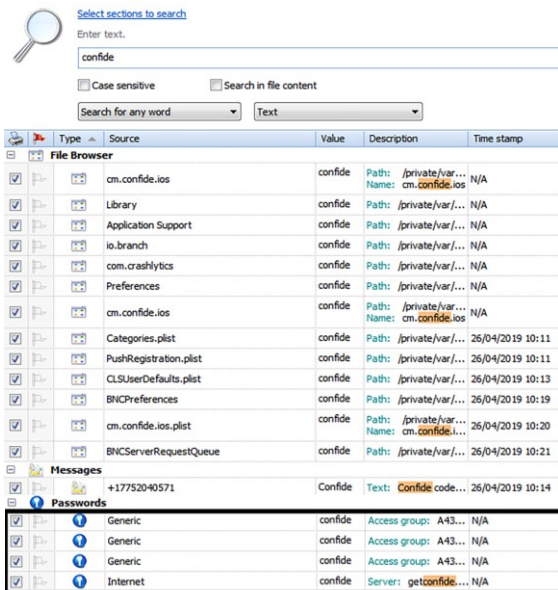
Key	Value
reg_suid	D3ED057C-9CBA-4979-92C8-60F09789ECS
date	26/04/2019 08:51:06
LastLoginUsername	aimee_test19
offensive-words.json	True
KSCFOGLocationValid	True
(null)-LastSignupPageViewTimestamp	1555498875701
aimee_test19-ChatDeletionMsgShownChatIdentifier-aimee_test19	True
aimee_test19-HasGrantedContactsAccess	True
model.dnn	True
last app session time	6933.77702441667
PER_USER_LOCATION_PERMISSION_SUPPORTED	True
kSCDownloadableContentFileDownloaded_custom_sticker_v2_facemodel.dnn	True
aimee_test19-ChatDeletionMsgShownCount	1
aimee_test19-viewedSwipeHeptLabel	True

Figure 1. Snapchat artefacts in Oxygen.

The next application investigated was Cyberdust. Previously, Snapchat appeared in the 'Applications' tile on Oxygen displaying itself as a normal application. However, with Cyberdust only the application folder was recognised, and Cyberdust was not acknowledged as a full application like Snapchat, however the folder proved there was evidence of an application called Cyberdust being present on the mobile device. This could be because the application did not require a username and password to log in, rather the user's mobile



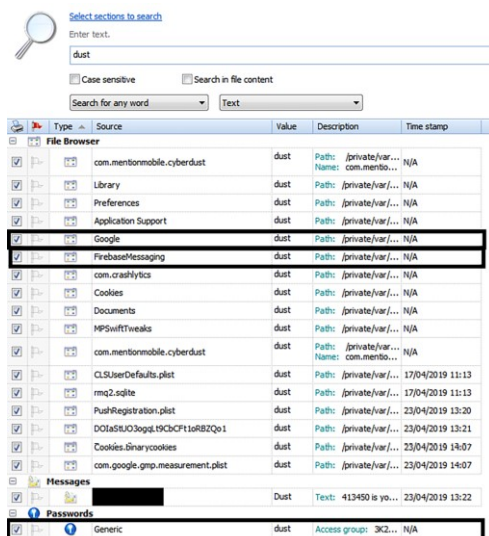
number instead, which therefore meant the phone did not identify it as an application in the same way as Snapchat, where it requires a username and password. Figure 2 shows results from a general search of the word ‘dust’.



The screenshot shows the Oxygen Forensic Examiner interface. At the top, a search bar contains the word 'dust'. Below the search bar, there are checkboxes for 'Case sensitive' and 'Search in file content'. The search results are displayed in a table with columns: Type, Source, Value, Description, and Time stamp. The results are categorized into File Browser, Messages, and Passwords. The Passwords section is highlighted with a red box, showing four entries: Generic, Generic, Generic, and Internet.

Type	Source	Value	Description	Time stamp
File Browser	cm.confide.ios	confide	Path: /private/var/... Name: cm.confide.ios	N/A
File Browser	Library	confide	Path: /private/var/...	N/A
File Browser	Application Support	confide	Path: /private/var/...	N/A
File Browser	io.branch	confide	Path: /private/var/...	N/A
File Browser	com.crashlytics	confide	Path: /private/var/...	N/A
File Browser	Preferences	confide	Path: /private/var/...	N/A
File Browser	cm.confide.ios	confide	Path: /private/var/... Name: cm.confide.ios	N/A
File Browser	Categories.plist	confide	Path: /private/var/...	26/04/2019 10:11
File Browser	PushRegistration.plist	confide	Path: /private/var/...	26/04/2019 10:11
File Browser	CLSUerDefaults.plist	confide	Path: /private/var/...	26/04/2019 10:13
File Browser	BMCPreferences	confide	Path: /private/var/...	26/04/2019 10:19
File Browser	cm.confide.ios.plist	confide	Path: /private/var/... Name: cm.confide.ios	26/04/2019 10:20
File Browser	BMCServerRequestQueue	confide	Path: /private/var/...	26/04/2019 10:21
Messages	+17752040571	Confide	Text: Confide code...	26/04/2019 10:14
Passwords	Generic	confide	Access group: A43...	N/A
Passwords	Generic	confide	Access group: A43...	N/A
Passwords	Generic	confide	Access group: A43...	N/A
Passwords	Internet	confide	Server: getconfide...	N/A

Figure 2. Cyberdust general search Oxygen



The screenshot shows the Oxygen Forensic Examiner interface. At the top, a search bar contains the word 'dust'. Below the search bar, there are checkboxes for 'Case sensitive' and 'Search in file content'. The search results are displayed in a table with columns: Type, Source, Value, Description, and Time stamp. The results are categorized into File Browser, Messages, and Passwords. The Passwords section is highlighted with a red box, showing one entry: Generic.

Type	Source	Value	Description	Time stamp
File Browser	com.mentionmobile.cyberdust	dust	Path: /private/var/... Name: com.mento...	N/A
File Browser	Library	dust	Path: /private/var/...	N/A
File Browser	Preferences	dust	Path: /private/var/...	N/A
File Browser	Application Support	dust	Path: /private/var/...	N/A
File Browser	Google	dust	Path: /private/var/...	N/A
File Browser	FireBaseMessaging	dust	Path: /private/var/...	N/A
File Browser	com.crashlytics	dust	Path: /private/var/...	N/A
File Browser	Cookies	dust	Path: /private/var/...	N/A
File Browser	Documents	dust	Path: /private/var/...	N/A
File Browser	MPSwiftivals	dust	Path: /private/var/...	N/A
File Browser	com.mentionmobile.cyberdust	dust	Path: /private/var/... Name: com.mento...	N/A
File Browser	CLSUerDefaults.plist	dust	Path: /private/var/...	17/04/2019 11:13
File Browser	mq2.sqfile	dust	Path: /private/var/...	17/04/2019 11:13
File Browser	PushRegistration.plist	dust	Path: /private/var/...	23/04/2019 13:20
File Browser	DOIaSLUQ3ogg19ChCP1tR8ZQ1	dust	Path: /private/var/...	23/04/2019 13:21
File Browser	Cookies.Binarycookies	dust	Path: /private/var/...	23/04/2019 14:07
File Browser	com.google.gmp.measurement.plist	dust	Path: /private/var/...	23/04/2019 14:07
Messages	[REDACTED]	Dust	Text: 413490 is yo...	23/04/2019 13:22
Passwords	Generic	dust	Access group: 3K2...	N/A

Figure 3. Confide general search Oxygen.

The results from the file browser show private folder pathway names. This acknowledges the existence of the application itself within the mobile device, but it does not have definitive messages between two users. However, as Figure 2 highlights, both ‘Google’ and ‘FireBaseMessaging’ were in the private folders. FireBase, formerly known as Google Cloud Messaging, is a cross-platform cloud solution for messaging [38]. This means that the data from the application could be deleted on the mobile device itself, but data may be uploaded elsewhere in the cloud and therefore access could be

granted through that, but this needs to be explored further. For this investigation however, it was proven that the application, Cyberdust, was a messaging application, but there was no evidence of messages between two users. Additionally, Figure 2 highlights a ‘Generic’ password in the search. This shows that the application has stored a password, most likely the user’s password, but has encrypted it with a token.

The last application investigated was Confide. Similarly, to Cyberdust, there was little evidence to prove the application Confide existed under the ‘Applications’ tile. Unlike Snapchat, the only data Confide showed within the Applications tile was a private pathway. Figure 3 shows results from a general search of the word ‘Confide’. The results showed general application files in private folders within the file browser. The number ‘+17752040571’ in Figure 3 is a verification text message from the application itself to verify the user’s account. Even though there was evidence that the Confide was installed in the phone, no application specific communication between users or user log in details was recovered. There were however, four passwords that were linked to the application Confide. Three being generic and one being an Internet password. The passwords could have been the user login password, but the passwords were encrypted. Therefore, the passwords were not visible and were secure for the user’s account.

## B. MOBILedit Forensic Express for iOS

The next part of the investigation was to examine the mobile device and the applications under examination using MOBILedit Forensic Express. Once the report generated from MOBILedit, the next step in the investigation was to navigate to the applications section of the report focusing on Snapchat, Cyberdust and Confide. The first application investigated was Snapchat. Figure 4 shows the accounts used to log in to Snapchat and the list of contacts and the pathways to ‘plist’, where the contact’s information was stored.

Figure 4 proves that the mobile device was linked to a Snapchat account with the username ‘aimee\_test19’, and both victim and suspect were likely to have communication as the names (username blackened out) appeared on the contact log of the phone. This finding would let further interrogation to the suspect during the investigation. Similarly to Oxygen, MOBILedit also found general application artefacts under private folders, but nothing significant that contributed to the investigation. The next application that was looked at within MOBILedit was Cyberdust. Figure 5 shows Cyberdust application data and the account the mobile device linked to the application. As Figure 5 displays, one account was evidently linked from the mobile device to the application. This proves the mobile user did use the application and also had an account. However, there were no account details recovered from that section of the report and unlike Snapchat, no contacts were found either, when the user did in fact have one contact on the application. However, this may be because the user contact was directly through a mobile number, which was already in the mobile user’s general phone contact list. Therefore, the contact may not have been stored on the application itself.

<b>Snapchat</b>	
Label	Snapchat
Package	com.toyosnapgroup.picaboo
Version	10.55.1.1
Application Type	User Application
Application Size	174.4 MB

<b>Accounts (2)</b>	
aimee_test19	<p>Logged in <span>✓ yes</span></p> <p>Source File phone/applications1/Apple Backup/AppDomainGroup/group.snapchat.picaboo/backup/Library/Preferences/group.snapchat.picaboo.plist</p>
aimee_test19	<p>Logged in <span>✓ yes</span></p> <p>Source File phone/applications1/Apple Backup/AppDomainGroup/group.snapchat.picaboo/backup/Library/Preferences/group.snapchat.picaboo.plist</p>

<b>Contacts (20)</b>	
Aimee	<p>Name aimeeyn [REDACTED]</p> <p>Source File phone/applications1/Apple Backup/AppDomainGroup/group.snapchat.picaboo/backup/Library/Preferences/group.snapchat.picaboo.plist</p>
Aimee	<p>Name aimeeyn [REDACTED]</p> <p>Source File phone/applications1/Apple Backup/AppDomainGroup/group.snapchat.picaboo/backup/Library/Preferences/group.snapchat.picaboo.plist</p>
Aimee	<p>Name aimeeyn [REDACTED]</p> <p>Source File phone/applications1/Apple Backup/AppDomainGroup/group.snapchat.picaboo/backup/Library/Preferences/group.snapchat.picaboo.plist</p>
Aimee	<p>Name aimeeyn [REDACTED]</p> <p>Source File phone/applications1/Apple Backup/AppDomainGroup/group.snapchat.picaboo/backup/Library/Preferences/group.snapchat.picaboo.plist</p>

Figure 4. Snapchat data in MOBILedit.

<b>Dust</b>	
Label	Dust
Package	com.mentionmobile.cyberdust
Version	1049
Application Type	User Application
Application Size	42.8 MB
Data Size	15.1 MB
APK File Extracted	✗ no

<b>Accounts (1)</b>	
Account	<p>Source File phone/applications0/com.mentionmobile.cyberdust/backup/Library/Preferences/com.mentionmobile.cyberdust.plist</p>

Figure 5. Cyberdust application in MOBILedit.

Some data was recovered from the ‘Passwords’ section within the generated report as shown in Figure 6. The “Password” had the label of “PhoneNumber”. The data itself was the mobile user’s unencrypted phone number. No other data was found in the passwords section of the report. Since the phone number was stored by the application, it shows evidence of a user account on the mobile device.

<b>PhoneNumber</b>	
Account	PhoneNumber
Application	3K22BUS8RL.com.mentionmobile.cyberdust
Data (Password)	+44075 [REDACTED]
Source File	phone/applications1/Apple Backup/KeychainDomain/backup/decoded-keychain-backup.xml

Figure 6. Phone number recovery in Cyberdust.

The last application MOBILedit investigated on the mobile device was Confide. Figure 7 displays Confide within the application list generated by MOBILedit. Unlike Snapchat and Cyberdust, the generated report displayed no information on contacts or accounts within Confide. Similar to the finding by Oxygen, Figure 6 suggests that there was little evidence that the mobile device had an account with the application.

<b>Confide</b>	
cm.confide.ios	
APK File Extracted: ✗ no	
User Application	Version: 360 Application Size: 24.0 MB Data Size: 276.0 kB

Figure 7. Confide application data MOBILedit.

<b>Passwords from Keychain (Synchronized Accounts Passwords) (7)</b>	
0759 [REDACTED]	<p>Account 0755 [REDACTED]</p> <p>Application com.apple.cinetwork</p> <p>Uri getconfide.com</p> <p>Data (Password) Top [REDACTED]</p> <p>Source File phone/applications1/Apple Backup/KeychainDomain/backup/decoded-keychain-backup.xml</p>

Figure 8. Phone number and password artefacts in Confide.

Figure 8 displays the mobile number and the password artefact recovered from the application. The account was the mobile user’s unencrypted phone number, and the password was the user password for the created account for the application. The password was also unencrypted. This suggested that the application have stored the user password unsafely.

### C. NIST Measurements for iOS

MOBILedit met all nine NIST measurement requirements tested in this research, while Oxygen did not, yet Oxygen did meet most of them. Comparisons of all nine test cases have been reported in Table II. MOBILedit provided the user with a “Select All” individual data objects (MDT-CA-02) while completing the logical or filesystem acquisition, it also provided the ability to “Select Individual” data objects (MDT-CA-03) for acquisition; in both of these cases Oxygen failed.

TABLE II. NIST TEST RESULTS (iOS)

Measurements tested	NIST test assertions applications Were the requirements met? (Y = Yes N = No)	
	Oxygen Forensic Detective Enterprise	MOBILedit Forensic Express
MDT-CA-01	Y	Y
MDT-CA-02	N	Y
MDT-CA-03	N	Y
MDT-CA-04	N	Y
MDT-CA-05	Y	Y
MDT-CA-06	Y	Y
MDT-CA-07	Y	Y
MDT-CA-08	Y	Y
MDT-CA-09	Y	Y

In the fourth test case (MDT-CA-04), where MBOILedit had a success over Oxygen, during data acquisition when

connectivity between the mobile and tool was disrupted; a notification was given to alert the user. Both tools could successfully present all supported data elements in useable formats via preview pane or generated report, as required by NIST measurement test id MDT-CA-05. Both tools also reported other test cases, such as reporting equipment related information and hash values for the data objects (MDT-CA-09).

#### D. Oxygen Forensic for Android

The mobile device extracted using Oxygen showed some interesting forensic evidence. A physical acquisition was performed on the device using Oxygen, and it was found that the most relevant pieces of the recovered data were found in Wire, which had records of every single communication stored within a log file by the name of “internalLog0.log” (Figure 9), and a storage cache (Figure 10) for various media files including the image and document files received and the audio message sent, despite those attachments being shown as deleted in application. All three of the identified files could be extracted, and the audio file could be played to hear the original contents of the message.

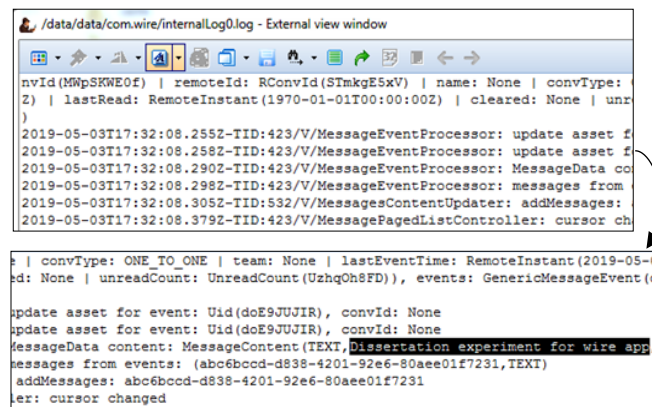


Figure 9. internalLog0.log Wire communications in Oxygen

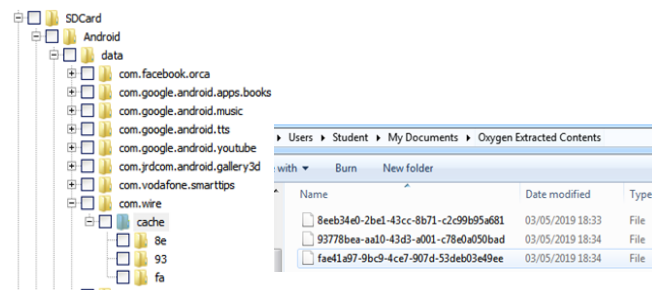


Figure 10. Wire cache and media files in Oxygen

The remaining items of recovered evidence were that of account data, recovered from various log or config-based files within the application data areas of the device storage. This data revealed the username, account ID and mobile number for the registered Facebook Messenger account and the

mobile number for the Signal account (Figure 11). Analysis of messenger and Signal program files revealed no data relevant to the conversations undertaken, nor any account information. Keyword search analysis of the image provided few results as shown in Figure 12.



Figure 11. Messenger and Signal in Oxygen

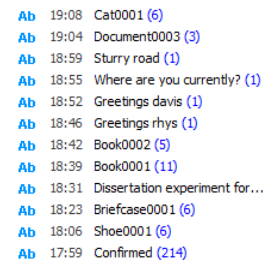


Figure 12. Full Oxygen keyword search results



Figure 13. Confide account data in Oxygen



Figure 14. Wire account data in Oxygen

Analysis of the Confide program files displayed no data relevant to the conversations but did contain a config file detailing the email registered to the confide account as well as the sign-up date, username and account ID (Figure 13). For



Wire, the username, account ID, mobile number and email address for the registered account were also found (Figure 14).

Analysis of the Wire program files revealed an SQL database named “ZGlobal.db” containing the locations of media files sent/received by the target device within a cache, specifically the jpg image received (Book0002.jpg), the Audio message sent (“Audio test 1”) and the document file received (Document0003.doc), as shown in Figure 15.

lastUsed	timeout	eric_key	path
1556904819119	604800000	7pKk3N9yCRImVu4mWQskog==	/storage/sdcard0/Android/data/com.wire/cache
1556904828355	604800000		/data/data/com.wire/files/assets
1556904828883	604800000		/data/data/com.wire/cache
1556904852623	604800000		/data/data/com.wire/files/assets
1556904858305	604800000		/storage/sdcard0/Android/data/com.wire/cache
1556904862714	604800000		/data/data/com.wire/cache
1556961781250	604800000	sOQ1y300nOChjzTnUj2yrA==	/storage/sdcard0/Android/data/com.wire/cache

name	file_name	length
image/jpeg	Book0002.jpg	304256
image/jpeg		61437
		61456
audio/pcm-s16le;rate=44100;channels=1		
audio/mp4	74436cf-97bb-4252-9863-e9bfa1758b7d.m4a	24065
		24096
application/vnd.openxmlformats-officedocument.wordprocessingml.document	Document0003.docx	11930

Figure 15. Oxygen analysis of ZGlobal.db

Only the images sent by each application were consistently found as they were within device storage. Attempts to extract the media files from the Wire directory using the cache file paths and file names provided by the ZGlobal.db database were successful, and each file could be carved from the image, however both “Book0002.jpg” and “Document0003.doc” were encrypted and could not be opened. The Audio message file on the other hand was unencrypted and once extracted could be played to hear the original message.

### E. Oxygen Anti-forensic for Android

Upon completing prior testing with the applications installed, all four apps were uninstalled via the Google play store and the device was imaged again for analysis. Both Facebook messenger and Signal were absent from the messengers section of the GUI after uninstallation leaving the account data absent from extraction. The program files for all four applications had also been removed from the file system, however the Wire media cache remained semi intact as recovered data. Searching for the Wire media files by cache name and manually searching for the cache in recovered space did reveal the image and audio message files (Figure 16).

Name	Date modified	Type	Size
_3778B-1	03/05/2019 18:34	File	12 KB
_AE41A-1	03/05/2019 18:34	File	24 KB
_EEB34-1	03/05/2019 18:33	File	64 KB

Figure 16. Oxygen extracted deleted Wire media files

Both the identified image and audio files could be extracted, and the audio message could be played to hear its

original content. Each application transcript, as well as the email address and mobile number associated with the applications, was then inputted into the search bar, with the results of the search being far less than the prior analysis (Figure 17).

Today - Sunday, 19 May 2019

Ab	18:20	447511724562 (27)
Ab	18:09	corrxhs98@gmail.com (15)
Ab	18:06	93778bea-aa10-43d3-a001... (2)
Ab	18:01	8eeb34e0-2be1-43cc-8b71... (3)
Ab	17:55	f4e1a97-9bc9-4ce7-907d... (4)
Ab	17:50	74436cf-97bb-4252-9863... (2)
Ab	17:38	Document0003 (1)
Ab	17:33	Book0002 (2)
Ab	17:26	Book0001 (22)
Ab	17:18	Confirmed (184)

Figure 17. Oxygen Anti-forensics image keyword search result

```
<?xml version='1.0' encoding='utf-8' standalone='yes'?><map> <string  
name='accessToken'>vZpM7HferfowIwL7yJka3m8TgqudeAvXChkku10G6p9goNStwx  
name='PREFIX_SERIALIZATION_EXTENSION_KEY'>S7JR8tYngucvkV48BuAVTKSiWiVq9/Bca  
&quot;email:&quot;;&quot;c0rxhy598@gmail.com&quot;;&quot;SignUpdate&quot;;&quot;  
[,&quot;destinationhashes&quot;];&quot;groupids&quot;:[,&quot;email&quot;];&quot;  
[,&quot;email:&quot;c0rxhy598@gmail.com&quot;;&quot;verified&quot;:true,&quot;  
1:260&quot;;&quot;username&quot;:&quot;tkpvqshhb&quot;;&quot;FirstName&quot;:&quot;  
[,&quot;installations&quot;:&quot;  
  
<string  
u10G6p9goNStwxTzBzbiC</string> <string  
AVTKSiWiVq9/BcaxOw0</string> <string name='currentUser'  
ate&quot;;&quot;2019-04-21T13:48:34Z&quot;;&quot;Phones&quot;:&quot;  
rEmails&quot;:  
ed&quot;:true,&quot;Type&quot;:&quot;,&quot;Primary&quot;:&quot;true&quot;];&quot;userId&quot;  
ame&quot;;&quot;Davis&quot;;&quot;Features&quot;:&quot;
```

Figure 18. Oxygen Anti-forensics image recovered Confide.xml

```
k?xml version='1.0' encoding='utf-8' standalone='yes' ?><map>  
  <string name=afdf-906f3f9a9d520a0":&quot;assets&quot;:l_&quot;phone&quot;:&quot;  
+447511724562&quot;:&quot;handle&quot;:&quot;davis4722&quot;:&quot;managed_by_c  
:&quot;name&quot;:&quot;davis&quot;:&quot;davis&quot;:&quot;accent_id&quot;:}&lt;/string>  
<boolean name='skip_terminating_state' value='true' /> <int name='updateba  
name='push_token'>FhgUpTtURcAPASIBeltttXzooQqFdG5PuffFoByjaukkuwRskE  
TY4e_12I7ukysvmwobxqsYSGb7x2kxMQGNhhx</string> <long name='lastUpdateSyn  
value='true' /> <boolean name='databases_renamed' value='true' /> <strin  
play&utm_medium=organic</string></map>
```

The second screenshot shows the XML output after the first modification. The `<string name="logging_in_user">` tag has been added, and the `<boolean name="first_time_with_teams" value="false"/>` tag has been removed. The `<string name="push_token">` tag now contains a long alphanumeric string.

```
<string name="logging_in_user">&quot;i&quot;:&quot;b1149364-604f-494d-&quot;  
t;managed_by&quot;:&quot;wire&quot;:&quot;email&quot;:&quot;coxrhy598@gmail.  
}&lt;/string> <boolean name='first_time_with_teams' value='false' />  
AqvkkumRSKSEJPG-VZCBXu14LBVnyvW5A3ADP7-C12oJy_wITZE6FL3dtacRHrZE-  
update_databasesync' value='1556737659933' /> <boolean name='Update-  
</string name='USER_REFERENCE_TOKEN'>utm_source=google-
```

Figure 19. Oxygen Anti-forensics image Wire account data

The Wire messages that had previously appeared within internalLog0.log did not exist, leaving no trace of the text-based communications, however, searches for the mobile number and email address revealed both a recovered copy of the Confide.xml file (Figure 18) and showed a deleted file that appeared to display all the account details for Wire (Figure 19).

#### F. Autopsy and FTK for Android

An Autopsy case file was produced for the Android device and both DD extracted partitions were added as evidence. Analysis of the image files provided similar evidence as Oxygen Forensic Detective: the Confide.xml config file containing the registered email address was discovered, as well as the “ZGlobal.db” database containing cache locations for the Wire media files. Further analysis with a keyword search of the application transcripts also revealed the same data, with the sent media files and entire Wire transcript being identified. Extraction of the media files also proved the same, with both the jpg file and Document

file remaining encrypted but the mp4 file remaining audible. The Autopsy analysis differed only in the absence of identified Signal account data and in a lack of Mobile number/Account ID data for Facebook messenger.

FTK Imager was run and both partition images were added as image files for analysis; however, the volume containing the application data stored within mmcblk0.dd was unavailable in analysis. As a result, accessing the “Confide.xml”, “ZGlobal.db” and “internalLog0.log” files was impossible. However, partition mmcblk1 was complete and as a result it was possible to access the Wire media cache and extract the media files to the same effect as Oxygen and Autopsy.

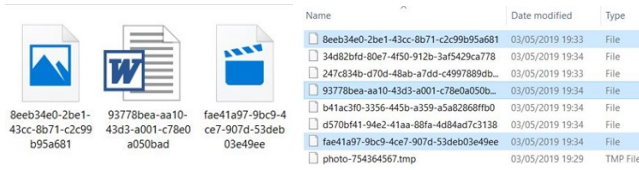


Figure 20. Extracted Wire cache files via Autopsy (Left) and FTK Imager (Right)

### G. Autopsy and FTK Anti-forensics Results for Android

Autopsy revealed only slightly fewer results, once again similar to the Oxygen Forensic Detective results. Keyword searches for both the test data transcripts and for the known account details failed to find the “internalLog0.log” file, which had stored the Wire conversations, however it did still manage to find both the deleted “Confide.xml” file and the deleted Wire file containing its account details. Analysis of the Wire cache was also possible, and revealed more deleted records that Oxygen seemed to, enabling the extraction of the media files once again. Both the jpg image file and document files remained unreadable, and the mp4 audio message remained unencrypted and fully audible (Figure 21).

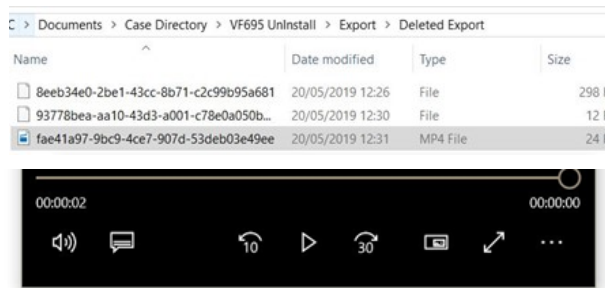


Figure 21. Autopsy extracted deleted Wire media files

FTK Imager revealed identical results as before, when apps were not deleted. The mmcblk0 partition still appeared partially unreadable, making analysis of partition specific files impossible, but access to the deleted Wire cache was still possible to identify and extract the cache contents. The extracted files behaved as they had before, with all except the mp4 file being encrypted or otherwise unreadable.

### H. Andriller Results for Android

The results from Andriller were negligible compared to those in Oxygen, with only account data and Facebook messages being shown in the main report, and no storage data being extracted despite the option being selected before extraction was performed. The account data recovered provided no actual account details, and instead just provided evidence that Facebook messenger and signal were installed, and the Facebook messages extracted were only the unencrypted messages sent between the original Nokia 1 device and the personal device, on top of the account confirmation messages, as shown in Figure 22. Andriller revealed no forensically valuable evidence relevant to the uninstalled applications, account data that was previously extracted was absent and once again was missing shared storage data for manual analysis.

Index	Sender	Sender Account	Message	Recipients	Time
9		David Shaw	Confirmed	Olivia Cox	2019-04-26 14:35:48 UTC
10		Olivia Cox	Dissertation experiment for Facebook Messenger app	David Shaw	2019-04-26 14:33:45 UTC
12		Messenger	What's new To view this link, use the latest version of the Messenger app.	David Shaw	2019-04-26 14:29:13 UTC
13		Messenger	Say hi to the new Messenger! We've simplified your messaging experience into three views - Chats, Feed Tap below to see what's new	David Shaw	2019-04-26 14:29:13 UTC

Figure 22. Andriller Facebook messages extraction

### I. NIST Measurements for tools used for Android

As the baseline test assertions, MDT-CA-1 to 10 are the lowest levels of functionality that NIST determined a mobile forensics analysis tool should have, Oxygen Forensic Detective managed to meet all of the test assertions except MDT-CA-10 (Table III). However, some of the assertions in the other tools such as FTK, Autopsy and Andriller were not relevant and therefore could not be tested.

TABLE III. ANDROID PROPRIETARY TOOLS

NIST Test Guidelines: Oxygen Vs. Andriller		
NIST Base Guidelines	Oxygen Forensic Detective	Andriller 3.0.3
MDT-CA-01	Pass	N/A
MDT-CA-02	Pass	N/A
MDT-CA-03	Pass	Pass
MDT-CA-04	Pass	Fail
MDT-CA-05	Pass	Pass
MDT-CA-06	Pass	Pass
MDT-CA-07	Pass	Pass
MDT-CA-08	Pass	Pass
MDT-CA-09	Pass (Inconsistently)	Fail
MDT-CA-10	N/A	N/A

TABLE IV. ANDROID FREEWARE TOOLS

NIST Test Assertions: FTK Imager Vs. Autopsy		
NIST Base Guidelines	FTK Imager 4.1.1.1	Autopsy 4.8.0
MDT-CA-01	N/A	N/A
MDT-CA-02	N/A	N/A
MDT-CA-03	N/A	N/A
MDT-CA-04	N/A	N/A
MDT-CA-05	Pass	Pass
MDT-CA-06	Fail	Fail
MDT-CA-07	Fail	Pass
MDT-CA-08	Pass	Pass
MDT-CA-09	Fail	Pass
MDT-CA-10	N/A	Pass

As shown in Table IV, being purely analysis tools, both Autopsy and FTK Imager were unable to be assessed by MDT-CA-1 to 4 by default. Andriller failed two of the seven applicable assertions, MDT-CA-4 & MDT-CA-9; Autopsy failed one of the six applicable assertions, MDT-CA-6, and FTK Imager failed three of the five applicable assertions, MDT-CA-6/7/9. Considering both the failed assertions, and the assertions that could not be applied due to a lack of tool functionality, Oxygen Forensic Detective is by far the most reliable by the standards set by NIST, with Andriller second, Autopsy third and FTK Imager fourth.

#### J. Comparison of tools for iOS

For iOS, both tools used in the mobile investigation output slightly different results. While neither recovered messages from the EMAs tested, both of them recovered artefacts elsewhere. Oxygen and MOBILedit successfully recovered data on all applications: Snapchat, Cyberdust and Confide. While different artefacts and data were detected, the fact that no physical copies of messages were recovered in any application, using either of the forensic tools, proves how efficient EMAs are at protecting user privacy. Oxygen detected offensive words being sent/received, this would be useful within a cyberbullying case, even though the message itself was not recovered. The evidence detected of communication between the mobile user and another contact would also prove useful as the application would be able to tell detectives who the mobile user had been in contact with. This would also be useful in a cyberbullying case, as there would be evidence the ‘bully’ had contact with the victim.

Furthermore, the detection of Cloud messaging within Cyberdust suggested that although physical messages were not recovered within the application, the messages could have been uploaded elsewhere to a Cloud network and access could be gained through the network. This would provide a chance for messages to perhaps be recovered in a cyberbullying case.

For Confide, Oxygen displays the password in encrypted format, while the MOBILedit shows it in unencrypted format. MOBILedit also recovered an unencrypted version of the registered mobile number, which Oxygen could not. For the Snapchat, MOBILedit detected account data, such as the

mobile user’s username and the contact list within the application. However, MOBILedit failed to detect other evidences, such as offensive words, evidence of communication between the mobile user and another contact, and the evidence of a message being deleted.

#### K. Comparison of tools for Android

The application analysis performed revealed that, for the most part, the EMAs are secure enough to keep evidence of user activity and message contents from being identified. Considering the successfully identified/extracted data, the NIST assessments and the overall forensic soundness of the tools and reliant imaging techniques therein, in the case of FTK and Autopsy, Oxygen Forensic Detective appears to be the most capable and reliable tool of the four, able to both non-invasively image suspect devices and analyse the extracted images in detail up to the relevant baseline specifications set by NIST. Furthermore, the evidence analysis shown by Oxygen was rivalled only by Autopsy, which while impressive for a fully freeware tool still required a pre-created image in order to perform analysis. The second freeware analysis tool, FTK Imager, was lacking in its analysis due to an inability to properly analyse the mmcblk0 partition, which contained the majority of the identifiable evidence. As a result, use of FTK Imager as a backup to proprietary tools would be ill advised when Autopsy is far more accessible as an immediate download, instead of FTK Imager’s request-based download, and provides more analysis functionality. While not entirely limited to DD images for analysis, without a prior image being obtained through a dedicated imaging tool both FTK Imager and Autopsy would be reliant on the invasive and potentially forensically unsound technique of rooting and DD extracting a device image, which potentially justifiable in court given the right situation still carries great risk of being thrown out as compromised evidence. Despite the potentially evidence unsafe methods required by the freeware tools, both FTK Imager and Autopsy provided more forensically valuable data than Andriller, which did not extract any filesystem data required for the in-depth analysis.

#### V. CONCLUSION

In this paper, experiments were performed to assess the forensically valuable artefacts that could be recovered from EMAs using various proprietary and freeware tools. The results show that with the rooted Android phone, more artefacts were recovered compared to iOS phone, which was not jailbroken. On iOS platform, no full ephemeral messages were recovered with either of the tools, but other significant artefacts were found, which proved rather interesting to the investigation. One significant finding was that of the Snapchat’s ‘offensive words’ detection, which may help aid evidence in cyberbullying cases to prove inappropriate language may have been used towards a victim. In forensic investigations, the investigators have to look very deep into the data and have a lot of patience, as one small piece of evidence could change the case, such as the offensive word. For iOS, a physical acquisition may have provided a much more thorough investigation to recover deleted data.

The forensic analysis conducted on the Android device also did not recover full ephemeral communications on the applications examined, except for the application 'Wire'. A log file was recovered containing full vocal communication sent and received on the application. Facebook Messenger was acknowledged as an application, and some details of the user were also stored, however no evidence of communication was found. This was interesting, as Snapchat (which is of similar popularity to Facebook Messenger) managed to recover some evidence of communication between two users using a logical acquisition on Oxygen, but it seems Oxygen could not find such communication on Facebook Messenger. This could contradict the fact physical acquisitions are supposed to recover more information. However, it could be the way the application is designed in itself. It does appear that Facebook Messenger has a more secure design, in which messages cannot be recovered even through a physical acquisition.

During experimentation of Android device, automatic tool analysis and analysis of application files revealed that from all four EMAs varying amounts of account data were recovered, of which Confide and Wire provided the most valuable data, then Facebook messenger and then Signal with the least. From this, a moderate range of recoverable forensic evidence has been identified for the four chosen EMAs, displaying where they may be recovered from and what data the evidence specifically relates to. During the anti-forensic investigation, when apps were deleted from the Android phone, some valuable artefacts were recovered. For example, the media files in Wire could still be recovered but the log file was not.

Furthermore, the use of the proprietary and freeware forensic tools, combined with the NIST assessments, provides insight into the capabilities and level of professional functionality that each tool holds, allowing for greater understanding of the available tools in Android and iOS based mobile device analysis and what these tools can do with regard to the extraction and analysis of ephemeral data. In total this study fills the gaps of knowledge that resides in the analysis of both popular EMAs and analysis of those applications via freeware forensic tools to the standard proprietary options. Further research on this topic should focus on better filling the gaps of knowledge regarding the recovery of ephemeral communication data from applications not included in this study, or further research on the applications used within this study to identify if app specific decryption capabilities could assist in identifying ephemeral communications from the applications that did not yield communication evidence.

#### REFERENCES

- [1] A. Chamberlain and M.A.H.B. Azhar, "Comparisons of Forensic Tools to Recover Ephemeral Data from iOS Apps Used for Cyberbullying", The Fourth International Conference on Cyber-Technologies and Cyber-Systems, CYBER 2019, Porto, Portugal.
- [2] R. Graham, "How Terrorists Use Encryption", Combating Terrorism Center at West Point. Available from: <https://ctc.usma.edu/how-terrorists-use-encryption/> [Accessed: 01- June- 2020].
- [3] C. Cotta, A.J. Fernandez-Lelva, F. Fernandez de Vega and F. Chavez, "Application Areas of Ephemeral Computing: A Survey", in Transactions on Computational Collective Intelligence: David Camacho, University of Malaga, pp. 155-157, 2016.
- [4] I. Barker, "Cyber criminals turn to messaging apps following dark web crackdown", Betanews, 2017. [Online]. Available from: <https://betanews.com/2017/10/25/criminals-turn-to-messaging/> [Accessed: 01- June- 2020].
- [5] T. Alyaha and F. Kausar, "Snapchat Analysis to Discover Digital Forensic Artefacts on Android Smartphone", in 8th International Conference on Ambient Systems, Networks and Technologies, ANT-2017 and the 7th International Conference on Sustainable Energy Information Technology, SEIT 2017, 16-19 May 2017, Madeira, Portugal, pp. 1035-1040, 2017.
- [6] GSMA, "Number of Mobile Subscribers Worldwide Hits 5 Billion", [Online]. Available from: <https://www.gsma.com/newsroom/press-release/number-mobile-subscribers-worldwide-hits-5-billion/> [Accessed: 01- June- 2020].
- [7] D. L. Fisher, M.J. Hamilton and J.K. Southwick, "When Electronic Records Disappear But Legal Issues Linger", Law360, Portfolio Media, Inc., Available from: <https://www.pepperlaw.com/publications/when-electronic-records-disappear-but-legal-issues-linger-2018-09-06/> [Accessed: 01- June- 2020].
- [8] J. Graham, "WhatsApp, Wickr Seen by Justice Dept. as Tools to Erase Evidence", Available from: <https://biglawbusiness.com/whatsapp-wickr-seen-by-justice-dept-as-tools-to-erase-evidence/> [Accessed: 01- June- 2020].
- [9] J. Constine, "Snapchat revives growth in Q1 beat with 190M users", Available from: <https://techcrunch.com/2019/04/23/snapchat-q1-2019-earnings/> [Accessed: 01- June- 2020].
- [10] D. Noyes, "The Top 20 Valuable Facebook Statistics", Available from: <https://zephoria.com/top-15-valuable-facebook-statistics/> [Accessed: 01- June- 2020].
- [11] National Institute of Standards and Technology, "Mobile Device Tool Test Assertions and Test Plan", 2016. [Online]. Available from: [https://www.nist.gov/system/files/documents/2017/05/09/mobile\\_device\\_tool\\_test\\_assertions\\_and\\_test\\_plan\\_v2.0.pdf](https://www.nist.gov/system/files/documents/2017/05/09/mobile_device_tool_test_assertions_and_test_plan_v2.0.pdf) [Accessed: 01- June- 2020].
- [12] K. M. Ovens and G. Morison, "Forensic analysis of kik messenger on ios devices", Digital Investigation, vol. 17, pp. 40-52, 2016.
- [13] S. C. Sathe and N. M. Dongre, "Data acquisition techniques in mobile forensics", in 2018 2nd International Conference on Inventive Systems and Control (ICISC), pp. 280-286. doi: 10.1109/ICISC.2018.8399079.
- [14] M. A. H. B. Azhar and T. Barton, "Forensic Analysis of Secure Ephemeral Messaging Applications on Android Platforms", Jan. 2017, doi: 10.1007/978-3-319-51064-4.
- [15] M. Al-Hadadi and A. AlShidhani, "Smartphone Forensics Analysis: A Case Study", International Journal of Computer and Electrical Engineering, vol. 5, pp. 577-579, 2013.
- [16] R. Umar, I. Riadi and G. Zamroni, "Mobile Forensic Tools Evaluation for Digital Crime Investigation", International Journal on Advanced Science, Engineering and Information Technology, vol. 8, pp. 949-955, 2018.
- [17] P. Naughton and M. A. H. B. Azhar, "An Investigation on Forensic Opportunities to Recover Evidential Data from Mobile Phones and Personal Computers. The Second International Conference on Cyber-Technologies and Cyber-Systems", CYBER 2017, Barcelona, Spain.
- [18] ACPO, "ACPO Good Practice Guide for Digital Evidence", 2012. [Online]. Available from: <https://www.digital-detective.net/digital-forensics->



- documents/ACPO\_Good\_Practice\_Guide\_for\_Digital\_Evidence\_v5.pdf [Accessed: 01- June- 2020].
- [19] iPhone 6s, “Wikipedia for iPhone 6s”, [Online]. Available from: [https://en.wikipedia.org/wiki/IPhone\\_6S](https://en.wikipedia.org/wiki/IPhone_6S) [Accessed: 01- June- 2020].
- [20] Vodafone VF695, “User manual of Vodafone VF695”, [Online]. Available from: <https://www.vodafone.com/content/dam/vodcom/devices/smart-first/User%20Manual%20-%20English.pdf> [Accessed: 01- June- 2020].
- [21] Jkielty, “Android v iOS market share”, 2019, DeviceAtlas, [Online]. Available at: <https://deviceatlas.com/blog/android-v-ios-market-share> [Accessed: 01- June- 2020].
- [22] Snapchat, “Snapchat APP for mobile”, [Online]. Available from: <https://www.snapchat.com/l/en-gb/> [Accessed: 01- June- 2020].
- [23] Dust, “The APP that protects your assests”, [Online]. Available from: <https://usedust.com/> [Accessed: 01- June- 2020].
- [24] Confide, “Your Confidential Messenger”, [Online]. Available from: <https://getconfide.com/> [Accessed: 01- June- 2020].
- [25] Facebook Messenger, “Wikipedia for Facebook Messenger”, [Online]. Available [https://en.wikipedia.org/wiki/Facebook\\_Messenger](https://en.wikipedia.org/wiki/Facebook_Messenger) [Accessed: 01- June- 2020].
- [26] Signal Messenger, “Wikipedia for Signal Messenger”, [Online]. Available [https://en.wikipedia.org/wiki/Signal\\_Messenger](https://en.wikipedia.org/wiki/Signal_Messenger) [Accessed: 01- June- 2020].
- [27] Wire App, “Wikipedia for Wire App”, [Online]. Available [https://en.wikipedia.org/wiki/Wire\\_\(software\)](https://en.wikipedia.org/wiki/Wire_(software)) [Accessed: 01- June- 2020].
- [28] Omnicore, “Snapchat by the Numbers: Stats, Demographics & Fun Facts”, 2020. [Online]. Available from: <https://www.omnicoreagency.com/snapchat-statistics/> [Accessed: 01- June- 2020].
- [29] Messenger, “Messenger - Android Apps on Google Play”, [Online], Available at: <https://play.google.com/store/apps/details?id=com.facebook.orca> [Accessed: 01- June- 2020].
- [30] J. Evans, “WhatsApp Partners With Open WhisperSystems To End-To-End Encrypt Billions Of Messages A Day.” [Online]. Available from <https://techcrunch.com/2014/11/18/end-to-end-for-everyone/> [Accessed: 01- June- 2020].
- [31] Oxygen Forensics, Oxygen Forensic Detective Enterprise, [Online]. Available from: <https://www.oxygen-forensic.com/en/products/oxygen-forensic-detective-enterprise> [Accessed: 01- June- 2020].
- [32] MOBILedit Forensic, MOBILedit Forensic Express, [Online]. Available from: <https://www.mobiledit.com/online-store/forensic-express> [Accessed: 01- June- 2020].
- [33] Andriller, Android Forensic Tools, [Online]. Available from: <https://www.andriller.com/> [Accessed: 01- June- 2020].
- [34] FTK Imager, AccessData. [Online], Available from: <https://accessdata.com/product-download> [Accessed: 01- June- 2020].
- [35] Autopsy. [Online], Available from: <https://www.sleuthkit.org/autopsy/> [Accessed: 01- June- 2020].
- [36] Andrioid Tools, “Android Forensics: imaging android filesystem using ADB and DD”, [Online], Available from: <https://www.andreafortuna.org/2018/12/03/android-forensics-imaging-android-file-system-using-adb-and-dd/> [Accessed: 01- June- 2020].
- [37] M. Lohrum, “Live imaging an Android device”, [Online] Available from: <http://freeandroidforensics.blogspot.com/2014/08/live-imaging-android-device.html> [Accessed: 01- June- 2020].
- [38] FireBase Messaging, “Firebase Cloud Messaging”, [Online]. Available from: <https://firebase.google.com/docs/cloud-messaging> [Accessed: 01- June- 2020].