Comparisons of Forensic Tools to Recover Ephemeral Data from iOS Apps Used for Cyberbullying

Aimee Chamberlain and M A Hannan Bin Azhar
School of Engineering, Technology and Design
Canterbury Christ Church University
Canterbury, United Kingdom
e-mail: aimee.chamberlain@yahoo.co.uk; hannan.azhar@canterbury.ac.uk

***Abstract*—Ephemeral 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, such as cyberbullying where evidence could be useful. 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 forensically sound recovery of evidential data, in relation to cyberbullying, from three popular ephemeral applications using an iOS mobile device. Examinations were performed to evaluate two popular mobile forensic tools, Oxygen and MOBILedit, using parameters from the National Institute of Standards and Technology's (NIST) mobile tool test assertions and test plan. The results from the investigation recovered various artefacts from the mobile device as well as revealing some interesting forensic data related to cyberbullying.**

Keywords— Mobile forensics; NIST measurements; Oxygen Forensics; MOBILedit forensic; Ephemeral APPS; Cyberbullying.

I. INTRODUCTION

Mobile phones are an essential part of modern-day life. According to the Global System for Mobile Communications [1], there were 5 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.

Criminals usually use mobile phones to communicate with each other. They may use regular chatting applications, but there is a growing opportunity within the mobile application market for criminals to use ephemeral applications, which allow users to send messages/multimedia, etc., to each other with the messages only lasting for a certain period of time [2]. Barker [3] reported that criminals are moving away from dark web interactions and on to ephemeral applications, such as WhatsApp, Snapchat, Telegram, etc. 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 [4].

Since ephemeral applications only hold data for a certain period of time, an individual or group could easily send a hateful message to somebody and there would be no evidence of it. Moreover, more serious issues can be hidden through these types of applications, such as self-harm, and sexting. Charteris et al. [5] reported that out of 276 primary and secondary school professional staff that observed the application 'Snapchat' [6] being used at school, a total percentage of 26.9% of professionals reported Snapchat was used for bullying/harassment, sending inappropriate images/text, sexting, and self-harm. The results were from a viewpoint of teachers, counsellors, etc., which means there may have been a lot more students suffering from the same issues, but they did not come forward. According to Cook [6], 11% parents reported their children had been a victim of cyberbullying in 2011, an increase followed of 15% in 2016, and another increase followed of 18% in 2018. It appears that as the cyber world evolves and develops, the rate of cyberbullying increases.

With all the opportunities for new crimes to be committed through growing technology, it is crucial to ensure that the law enforcement agencies have the appropriate software and methods to deal with these crimes. There is a gap in literature in relation to comparisons of tools to recover evidential data, specifically focusing on ephemeral applications relating to cyberbullying. This paper will attempt to fill this gap by comparing two popular forensics tools, Oxygen [7] and MOBILedit [8] in recovering ephemeral data from popular mobile apps used for cyberbullying. Furthermore, this paper focuses on an iOS device, as there is already a large body of research on forensic investigations into Android devices [4][9][10].

The remainder of the paper will be organised as follows: Section 2 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 3, including logical acquisition and analysis of mobile forensic data and tool comparisons. Section 4 will cover the results of the analysis. Finally, Section 5 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

 ISBN: 978-1-61208-743-6

focusing on particular pieces of data within the mobile device. There is also work completed on non-ephemeral applications, such as Ovens et al. [11] conducted a forensic analysis on Kik Messenger on iOS. While there has 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.

Al-Hadadi et al. [12] 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.

Azhar et al. [13] conducted a forensic experiment of two ephemeral messaging applications: 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 compared ephemeral applications on Android platforms. The investigation more looked into packages and files within the application itself instead of using a mobile forensic tool. Performing similar investigatory analysis on an iOS platform would be an interesting study as a future work.

Umar et al. [14] tested three different forensic tools on a Samsung Galaxy S4 GT-I9500 using the application WhatsApp. The tools included WhatsApp DB/Key Extractor (open source), Belkasoft Evidence (trial version and proprietary) and Oxygen Forensic (proprietary). The forensic tools were tested against the NIST Mobile Device Tool Test Assertions and Test Plan ver. 2. Researchers in [14] forensically tested the mobile device using the tools, each either completed a logical or physical acquisition. WhatsApp DB/Key extractor performed a logical acquisition and Belkasoft Evidence was used alongside it to open the result from the acquisition. The results showed that the WhatsApp contact list was recovered, as well as a text message artefact including the sender and recipient of the message, as well as the time stamp. Belkasoft Evidence performed a logical acquisition, the acquisition was unable to recover the WhatsApp contact list but found multimedia and document artefacts. Oxygen forensic could perform both physical and logical acquisition. Oxygen forensic recovered the WhatsApp contact list as well as a text message artefact including the sender and recipient information, content of the message and a time stamp.

As can be seen from this brief review of the literature, there is a significant gap in extraction of ephemeral artefacts on iOS platforms and there has not been any research reported primarily focusses on artefacts related to cyberbullying. This paper will contribute to investigate in these aspects to fill the gap.

III. METHODOLOGY

The focus of the investigation was recovering data from ephemeral applications due to their uses by Internet "trolls" [15], also known as digital bullies. This paper is going to investigate how much data can be recovered from these types of applications from two different tools as listed in Table 1; the mobile device and applications are listed in Table 2.

TABLE I. FORENSIC TOOLS

Name	Forensic tools	
	Cost	***Version***
Oxygen Forensic Detective Enterprise	APPROX £1,100-£2000	10.3.0.100
MOBILedit Forensic Express	APPROX £76 for one mobile device, £1,150 for full license	6.1.0.15480

TABLE II. MOBILE DEVICE AND APPLICATIONS

Mobile used	Ephemeral Apps	
	App Name	***Version***
iPhone 6s NOT-JAILBROKEN	Snapchat	10.55.1
	Cyberdust	5.6.1.1049
	Confide	8.3.1

The investigation was carried out according to the four good practice guidelines of the Association of Chief Police Officers (ACPO) [16]. For example, the third principle of the guidelines state that an audit trail should be recorded throughout the investigation in a manner which a third party could recreate the steps taken in the investigation.

A. Ephemeral Apps for Cyberbullying

The three applications as listed in Table 2 were all chosen for different reasons. Snapchat is one of the most popular ephemeral applications. According to Omnicore [17], more than 25% of mobile phone users are on Snapchat, with 71% of the users being aged between 17 to 24. 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.

The next application, 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 [18]. 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. For the

 ISBN: 978-1-61208-743-6

investigation's purpose, only the secure messaging feature was used, where messages were encrypted and deleted after 24 hours. A total of eleven messages were exchanged. Two of the messages were picture messages. The username for the mobile owner was linked directly to the mobile number.

The final application, Confide [19], 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. For the investigation purpose, this application was used to test the message encryption and data recovery from the application. A total of seven messages were exchanged. Like Cyberdust, here also the username for the mobile owner was linked directly to the mobile number.

B. Forensic Tools

Forensic tools used in the investigation were Oxygen Forensic Detective Enterprise [7] and MOBILedit Forensic Express [8]. Both tools have reputations to be able to forensically examine mobile devices and are widely used by professional investigators [20]. Oxygen is a more well used tool within Law enforcement, military operations and professional investigatory cases, with uses of the tool in over 100 countries [7]. MOBILedit Forensic is also popular, but it is used a little less, it is used in approximately 70 countries and is used in military investigations and law enforcement [8]. The mobile device was extracted on both tools using logical acquisition and then the analysis was conducted in forensic workstations. Oxygen Forensic Detective Enterprise was running on Windows 7 Enterprise version 6.1.7601. The MOBILedit was running on a Windows 10 Home version 10.0.17134. Both tools were tested against NIST test assertions from 'MDT-CA-01' to 'MDT-CA-09' as detailed in [21]. Throughout the investigation, nine NIST test assertions were closely followed and the forensic tools were tested according to the measurements.

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 ephemeral applications 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.

IV. RESULTS

The results analyse the key findings from the methodology. The results are presented with regards to the four categories: Oxygen Forensic Detective Enterprise; MOBILedit Forensic Express, Evaluation of findings and NIST measurements.

A. Oxygen Forensic Detective Enterprise

A list of applications on the mobile device was found in the 'Applications' tile using Oxygen. Snapchat was the first application to be investigated [4]. Figure 1 shows Snapchat data. Four areas were highlighted within the figure. This included the login user name '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.

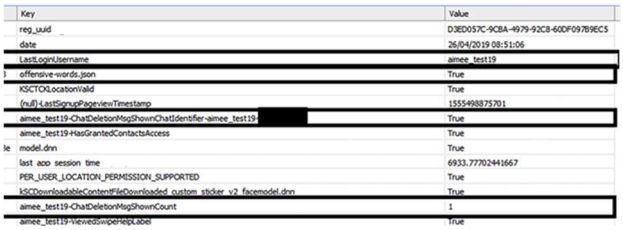

Figure 1. Snapchat artefacts in Oxygen.

The next application investigate was Cyberdust [18]. 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'.

 ISBN: 978-1-61208-743-6

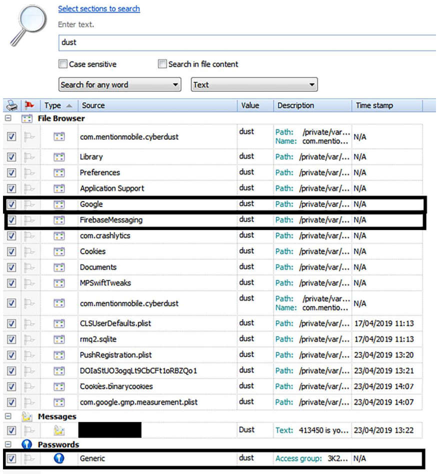

Figure 2. Cyberdust general search Oxygen

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 [22]. 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.

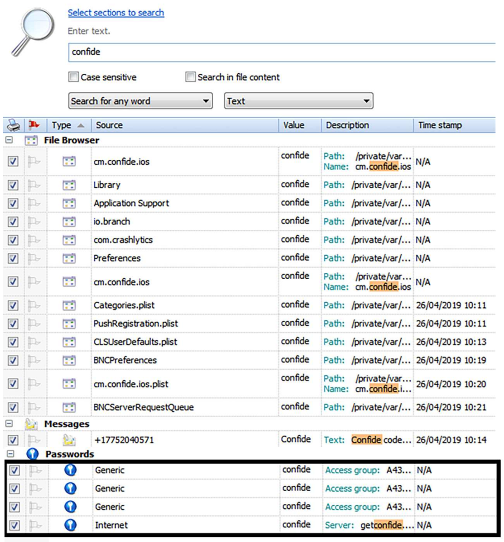

Figure 3. Confide general search Oxygen.

The last application investigated was Confide [19]. 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 weren't visible and were secure for the user's account.

B. MOBILedit Forensic Express

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 [4]. 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.

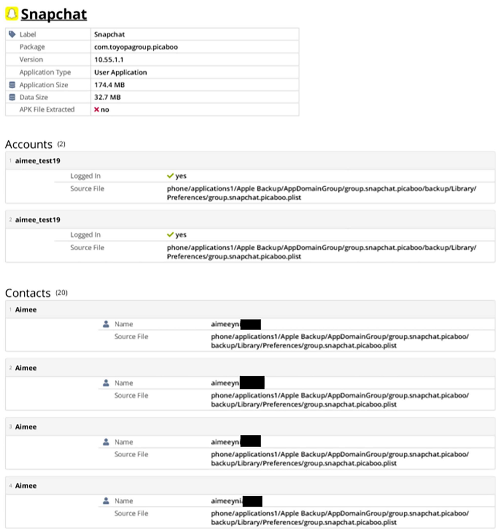

Figure 4. Snapchat data in MOBILedit.

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 had 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 [18]. Figure 5 shows Cyberdust pplication 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

 ISBN: 978-1-61208-743-6

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.

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.

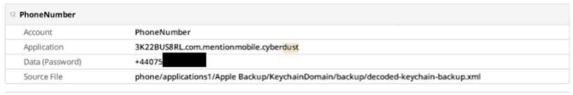

Figure 6. Phone number recovery in Cyberdust.

The last application MOBILedit investigated on the mobile device was Confide [19]. 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.

Figure 7. Confide application data MOBILedit.

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. Evaluation of findings

Both tools used in the mobile investigation output slightly different results. While neither recovered messages from the ephemeral applications 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 ephemeral applications 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.

D. NIST Measurements

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 3.

TABLE III. NIST TEST RESULTS

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

Oxygen provided the user with a "Select All" individual data objects (MDT-CA-02) while completing the

logical/filesystem acquisition, it also provided the ability to "Select Individual" data objects (MDT-CA-03) for acquisition; in both of these cases MOBILedit failed. In another test case (MDT-CA-04), where Oxygen had a success over MBOILedit was 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 (MDT-CA-09) and hash values for the data objects (MDT-CA-09).

V. CONCLUSION

To conclude, this forensic investigation was successful in how it was carried out, it followed professional ACPO guidelines [16], the tools were tested against NIST measurements, and the whole investigation was forensically sound. However, no full ephemeral messages were recovered with either of the tools, but other significant artefacts were found which proved rather interesting to the investigation and to potential cyberbullying cases. 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. On reflection, a physical acquisition may have provided a much more thorough investigation to recover deleted data, but that can be tested in future work. Also, in the future more tools can be compared in recovering evidential data from a wide range of ephemeral applications.

REFERENCES

[1] 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: 07- Aug- 2019].

[2] 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.

[3] 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: 07- Aug- 2019]

[4] T. Alyaha and F. Kausar, "Snapchat Analysis to Discover Digital Forensic Artefacts on Android Smartphone", 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.

[5] J. Charteris, S. Gregory, Y. Masters and M. Maple, "Snapchat at school – 'Now you see it…': Networked affect – cyber bullying, harassment and sexting", Innovation, Practice and Research in the Use of Educational Technologies in Tertiary Education 33rd International Conference, University of South Australia, Adelaide, Australia, pp. 111-114, November 2016.

[6] S. Cook, *Cyberbullying facts and statistics for 2016-2018*, 2018. [Online]. Available from: https://www.comparitech.com/internet-providers/cyberbullying-statistics/ [Accessed: : 07- Aug- 2019]

[7] Oxygen Forensics, *Oxygen Forensic Detective Enterprise*, [Online]. Available from: https://www.oxygen-forensic.com/en/products/oxygen-forensic-detective-enterprise [Accessed: : 07- Aug- 2019].

[8] MOBILedit Forensic, *MOBILedit Forensic Express*, [Online]. Available from: https://www.mobiledit.com/online-store/forensic-express [Accessed: : 07- Aug- 2019].

[9] D. Walnycky, I. Baggili, A. Marrington, J. Moore and F. Breitinger, "Network and device forensic analysis of Android social-messaging applications", The Proceedings of the Fifteenth Annual DFRWS Conference, USA, pp. S77-S84, August 2015.

[10] V. Vijayan, *Android Forensic Capability and Evaluation of Extraction Tools*, 2012. [Online]. Available from: https://www.academia.edu/1632597/Android_Forensic_Capability_and_Evaluation_of_Extraction_Tools [Accessed : 07- Aug- 2019]

[11] K. M. Ovens and G. Morison, Forensic analysis of kik messenger on ios devices. Digital Investigation, vol. 17, pp. 40-52, 2016.

[12] 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.

[13] 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.

[14] 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.

[15] Panda Security, *What is an online troll?*, 2017. [Online]. Available from: https://www.pandasecurity.com/mediacenter/security/what-is-an-online-troll/ [Accessed: 07- Aug- 2019].

[16] 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: 07- Aug- 2019].

[17] Omnicore , *Snapchat by the Numbers: Stats, Demographics & Fun Facts*, [Online]. Available from: https://www.omnicoreagency.coma/snapchat-statistics/ [Accessed: 07- Aug- 2019].

[18] Dust, *The APP that protects your assests*, [Online]. Available from: https://usedust.com/ [Accessed: 07- Aug- 2019].

[19] Confide, *Your Confidential Messenger*, [Online]. Available from: https://getconfide.com/ [Accessed: 07- Aug- 2019]

[20] Forensic Focus, *MOBILedit Forensic Express From Compelson*, 2018. [Online]. Available from: https://forensicfocus.com/c/aid=229/reviews/2018/mobiledit-forensic-express-from-compelson/ [Accessed: 07- Aug- 2019]

[21] National Institute of Standards and Technology, *Mobile Device Tool Test Assertions and Test Plan, 2016*. [Online]. Available from: https://www.nist.gov/sites/default/files/documents/2017/05/09/mobile_device_tool_test_assertions_and_test_plan_v2.0.pdf [07- Aug- 2019].

[22] FireBase Messaging, *Firebase Cloud Messaging*, [Online]. Available from: https://firebase.google.com/docs/cloud-messaging [Accessed: 07- Aug- 2019]

 ISBN: 978-1-61208-743-6