Xournals

Academic Journal of Forensic Sciences

ISSN: 2581-4273 | Volume 05 | Issue 01 | April-2022

Retrieved Data Comparison of WhatsApp and Signal Application

Preeti Ansari[1], Ritika Sharma[2]

Available online at: www.xournals.com

Received 24th June 2021 | Revised 28th October 2021 | Accepted 14th February 2022

Abstract:

Digital forensic is a scientific study which identify, extract, analyze and present the evidence which was found in digital devices. The WhatsApp, the Signal is a mobile application which allows user to transfer messages, images, audio, videos, location etc. The Smart phones are merely used in criminal activities and can be used for digital evidence as a part of an investigation. The Digital Forensic Tools used by the investigators were not actually designed for the forensic application. Data retrieval tools are generally use as the method of restoring data partially or completely from damaged, failed, corrupted storage media. This paper focuses on data recovery and also comparison of extracted data from the WhatsApp and the Signal application.

Keywords: *Mobile forensic, WhatsApp, Signal, MSAB XRY, Cellebrite UFED, Data Extraction.*

Authors:

1. *Assistant Professor, Renaissance University, Indore, Madhya Pradesh, INDIA*

Introduction

The Cyber Forensics has faced major obstacles in the last few years. Cybercrime is rising day by day and the contest in the case of cyber criminals is never-ending since the internet was established. The low cost of digital equipment's are not only attracting the common man but also criminals to use them and so crimes are swiftly increasing.

The Mobile Forensics is the collection of digital evidence retrieved from a mobile phone. Here is an immense demand to extract data from smartphones today as the crime rate is rapidly increasing. There are different tools to restore the data. In terms of investigation, smartphones frolic a crucial part as they are routinely found in crime scenes. The capability to access the data relies on the internal memory of the mobile phone while extraction of the evidence **(Al Hidaifi, 2018).** The personal computers that have a limited number of major operating system vendors, there are countless manufacturers of smartphones and mobile devices with their own proprietary technology and formats **(Aziz *et al*., 2015).**

In the modern era, cell phone evidence is playing a vital role in cases of homicides, suicide, sexual assault, human trafficking, narcotics etc. Forensic evidence is recovered from phone memory, sim cards and memory cards using different forensic tools so the data can be extracted, decoded, analyzed and reported. The android cell phone can behave like a small PC and it contained information regarding cell phone, address book, messenger, photo & video camera, GPS navigator, web client and platform for 3rd party applications. Before packing cell phones should be put either in Faraday bags or switched on airplane mode to keep away the cell phone from network signals. In the case where neither the faraday bag nor airplane mode option is available, then the battery of the cell phone can be removed and packed separately in the sample parcel.

Related Work

WhatsApp

WhatsApp allows users to share messages, images, documents, audios, videos, location, making face calls. WhatsApp Inc. was founded by Jan Koum and Brian Acton in 2009. This messenger is applicable for, Androids, Blackberry, iOS, Windows phones, and Symbian **(Sahu, 2014).**

There is no restriction of exchanging no. of tweets in this application but the latest version allows only 30 images or videos to send at a time. It only requires WhatsApp installed on the device, internet and internal storage.

In early versions of WhatsApp, experts found that chat records managed by the WhatsApp messenger are unsafe, as per the researcher's backup storage of chat, document and media details do not end to end encrypted and can be accessed by anonyms. As the news hit the internet, security researchers started researching with WhatsApp database to retrieve the conversation alike erased ones from the tweets but this messenger respond earlier and rise with an encryption mechanism to save the database **(Sahu, 2014).**

Figure No. 1: WhatsApp users graph from year 2010 -2021 (backlinko.com, 2021)

Signal Application

The Signal messenger application was founded by "Signal Technology Foundation and Signal Messenger LLC February 2018''. It allows users to send one-to-one and group messages, documents, images, audios, videos, audio and face calls and user location. It also has the option of 'disappearing messages' which means messages sent and received in the conversation will disappear within 5 seconds to 1 week after they have been seen. Signal privacy features also have 'screen security' in which one can block others to take screenshots of a chat. Other feature includes 'Safety no.' in the security of encryption with that chat by comparing no. on their phones or can scan the code of their phone. One can also change chat colour.

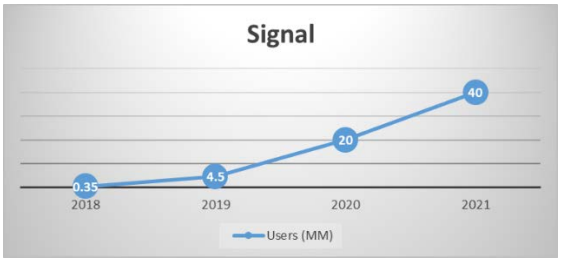

Figure No. 2: Signal Application users graph from year 2018-2021 (www.businessofapps.com)

Tools Used for Data Extraction

Analysis with XRY

XRY is a commercial mobile forensic tool made by Swedish company MSAB and so-termed as MSAB XRY. It provides an extraction method to analyze and recover data from Smartphone, tablets and GPS navigation systems. It can extract the erased data from the devices. Some applications from which data can be easily extracted are WhatsApp, Facebook, Instagram and Snapchat.

MSAB XRY is complete software- cum- hardware solution which allows the user or the experts to do a physical acquisition to retrieve deleted data as well as allows the user or expert to do logical acquisition of data and generate the forensic report for legal purposes. It helps to extract more data in less time duration with great support towards different chipsets.

XRY Logical - XRY Logical is an expeditious retrieved method to access live, deleted and file system data from the device found in the scene of the crime by interfacing directly with the OS of the device.

XRY Physical - XRY Physical salvage the erased files out of the devices as well as it also permits the user to beat the firewall on a locked device.

Figure No. 3: MSAB XRY version 9.3.1

Analysis with Universal Forensic Extraction Device

Cellebrite UFED Physical Analyser is a cell phone forensic investigation software /hardware toolkit designed by ‘’Cellebrite Mobile Synchronization Inc. an Israel Company established in 1999’’. UFED is used for data acquisition and analysis of a range of cell phones of different chipsets. It came with a suite of applications peripheral accessories for the best result. UFED software 4 pc provide the user with the advanced capability to perform data -Extraction, Decoding and Analysis from the huge range of cell phone on a platform. It is a commercial tool available for logical acquisition and can retrieve even erased files from mobile devices, Sim-card, mass storage and drone. UFED can easily restore files from SMS, Emails, Calendars, Audio, Videos, Images, Contacts, Call logs, phone Details and SIM Card Details including applications present in the device.

Figure No. 4: Cellebrite UFED version 7.42.0.82

Smartphones processor is also known as the Chipset. It is a component that helps in controlling everything which is going on in your smartphone. And it also ensures that the mobile phone functions correctly. The Chip Set Method is used for the extraction of data from a mobile device without removing the chip from inside the phone. The chip stored all the data of the mobile phone. In any case, if the device is damaged but found the chip safely, the data could be easily extracted from that chip this is present inside the mobile devices. The chip contains its individual IMEI no. which is its unique characteristic of individual devices. The IMEI no. is stored in the “About Phone” setting of mobile phone or we can search it by simply dialling ***#06#.** By this code the IMEI no. will appear and through that no. one could easily find the detail of cell phone in “IMEI.info”.

Types of Chipset used in Android and Apple smartphones are Qualcomm's Snapdragon, MediaTek, Exynos, TSMC used in iPhone.

Materials and Methodology

Materials required in XRY Forensic Workstation are XRY forensic tool kit, Smartphone, Licensed pen drive and hard drives.

Materials required in Cellebrite UFED Forensic Workstation are tool kit, cables (C-type, B-type, iPhone cable) Smartphone, Licensed pen drive and hard drives.

Phone Setting

1. For extraction go to the system manager of mobile devices
2. About phone
3. Tap 7 times to software version for USB debugging in developer option
4. Enable “stay awake”
5. Option on USB devices
6. Setup screen lock select “none

Operating Instructions for XRY Mobile Forensic workstation

1. Ensure that the power supply of the equipment is stabilized and uninterrupted

2. Extraction of data

Switch on the XRY Mobile Forensic Workstation and wait for the system to initialize. Open the XRY application software by clicking on the XRY extraction icon. Remove sim card if any from the mobile phone. Connect the mobile phone with XRY Mobile Forensic Workstation and wait for drivers to be installed. Browse and create a case folder and name the folder. Search for the model of the mobile phone in the XRY database and follow the instructions. Go for physical extraction if supported otherwise perform logical extraction. For extraction of data from sim card, search for a sim card in XRY database and follow the instructions. Wait for the extraction to be completed.

3. Analysis and examination

After completing the extraction process, open the case folder and open XRY extraction file. Select and open the file category according to the query of the case i.e. calls, messages, documents, multimedia, email etc. Search the relevant files and tag important the relevant files found**.**

4. Report generation

Click on the Export option in the toolbar and enter the name to save the file and other required options. Check the report export option and create the report folder and click OK. After completion of report generation, shut down the MSAB XRY Workstation **(www.msab.com).**

Operating Instructions for Cellebrite UFED

1. Ensure that the power supply of the equipment is stabilized and uninterrupted

2. Extraction of data

Switch on the Cellebrite UFED Forensic Workstation and wait for the system to initialize. Open the UFED application software by clicking on the UFED extraction icon. Connect the mobile phone with the Cellebrite UFED Forensic Workstation and wait for drivers to be installed. Browse and create a case folder and name the folder. Select the device by clicking on the “autocorrect” option if not found then click on browse device. Then select the option Android backup APK downgrade. Select File system or advanced logical option. Press continue to Android backup APK downgrade. Your device information appears check and press continue. Select applications from which data extraction should be done. Wait for the extraction to be completed.

3. Analysis and examination

After completing the extraction process, open the case folder and open UFED extraction file. Select and open the file category according to the query of the case i.e. calls, messages, documents, multimedia, email etc. Search the relevant files and tag important the relevant files found.

4. Report generation

Click on the Export option in the toolbar and enter the name to save the file and other required options. Check the report export option and create the report folder and click OK. After completion of report generation, shutdown the Cellebrite UFED Workstation **(Khan, and Mansur, 2018).**

Observation

The observation table shows the result of retrieved data.

Table No. 1: The Result of Retrieved Data

OBSERVATION TABLE				
WHATSAPP APPLICATION DATA			**SIGNAL APLLICATION DATA**	
SAMPLES	MSAB XRY SOFTWARE	UFED SOFTWARE TOOL	MSAB XRY SOFTWARE	MSAB XRY SOFTWARE
SAMPLE 1- VIVO V17Pro	Successful	Successful	Unsuccessful	Unsuccessful
SAMPLE 2- iPhone 7 A12bionic	Successful	Successful	Unsuccessful	Unsuccessful
SAMPLE 3- Realme2Pro	Successful	Unsuccessful	Unsuccessful	Unsuccessful
SAMPLE 4- Samsung note10Lite	Successful	Successful	Unsuccessful	Unsuccessful
SAMPLE 5- VIVO 1820	Successful	Successful	Unsuccessful	Unsuccessful
SAMPLE 6- One Plus 7	Successful	Successful	Unsuccessful	Unsuccessful
SAMPLE 7- Oppo F9 Pro	Successful	Successful	Unsuccessful	Unsuccessful
SAMPLE 8- Oppo A7	Unsuccessful	Successful	Unsuccessful	Unsuccessful
SAMPLE 9- Samsung Galaxy A21	Unsuccessful	Successful	Unsuccessful	Unsuccessful
SAMPLE 10- Samsung Galaxy J7	Successful	Successful	Unsuccessful	Unsuccessful

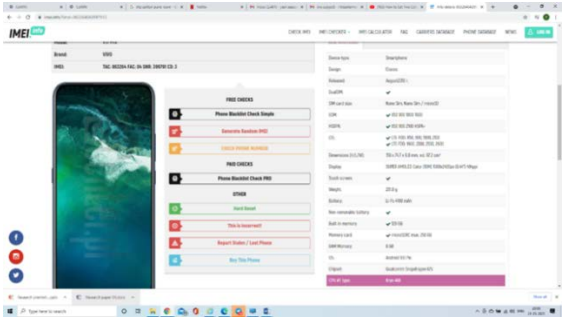

Figure No. 5: Above snap shows the device (Vivo v17 pro) having chipset QUALCOMM Snapdragon along with sample 3 Realme2pro, Sample5 Vivo1820, Oneplus7, Oppo f9 pro, Oppoa7ha Qualcomm Snapdragon chipset.

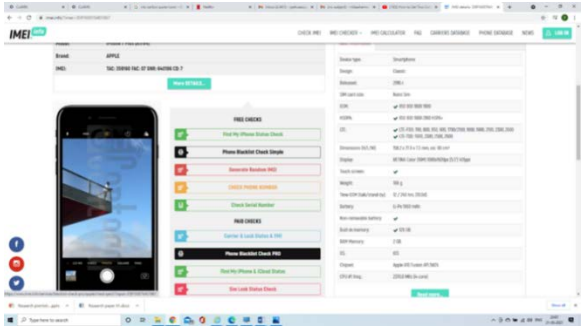

Figure No. 6: Above picture shows the device having Chipset Apple A10 APL1W24.

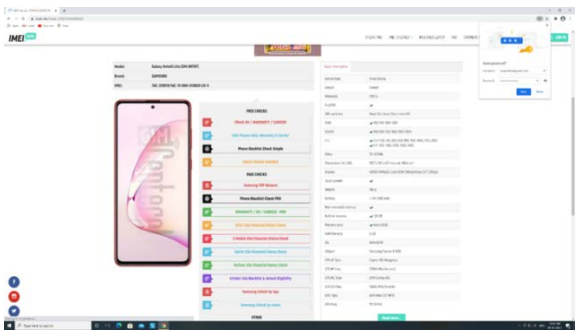

Figure No. 7: Above snap shows the device (Samsung note 10 Lite) having chipset Exynos M3 Mongoose along with Sample 9 (Samsung Galaxy A21), Sample 10 (Samsung Galaxy J7)

Extraction glimpse of UFED and MSAB XRY

Data extraction of WhatsApp and Signal Application:

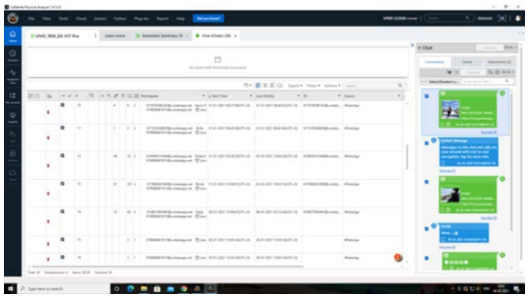

Figure No. 8: This picture shows retrieved data of WhatsApp by UFED.

Chipset Qualcomm Snapdragon

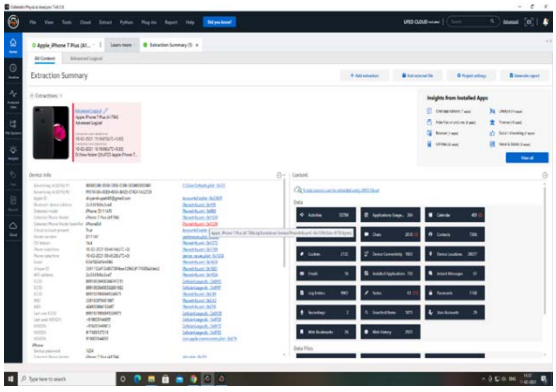

Figure No. 9: This picture shows retrieved data of WhatsApp by UFED

Chipset Apple A10 APL1W24

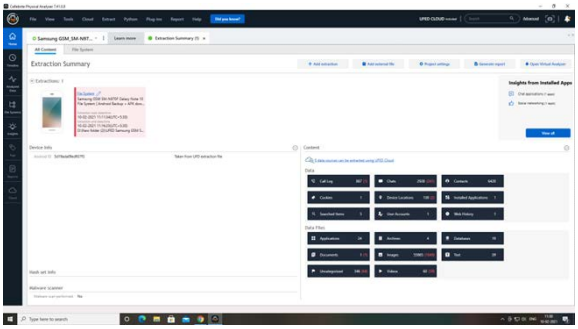

Figure No. 10: This picture shows retrieved data of WhatsApp by UFED

Chipset EXYNOS

"Attached snap describes us how even using Cellebrite UFED tool signal source data is inaccessible and how vulnerable WhatsApp security standards are which are easily trackable.''

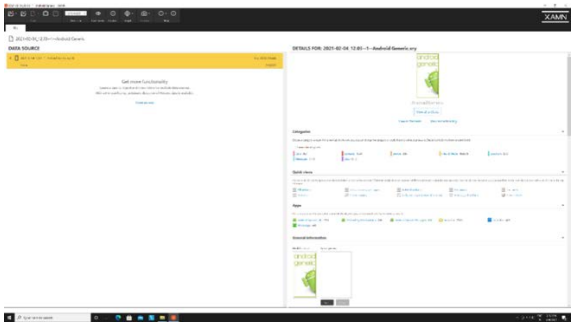

Figure No. 11: This picture shows retrieved data of WhatsApp by MSAB XRY

Chipset Qualcomm Snapdragon

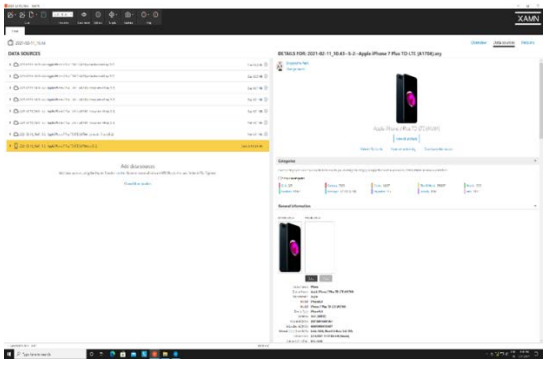

Figure No. 12: This picture shows retrieved data of WhatsApp by MSAB XRY

Chipset Apple A10 APL1W24

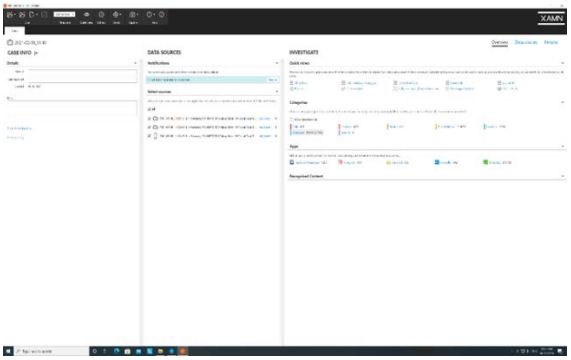

Figure No. 13: Above snap shows Retrieved Data of WhatsApp by MSAB XRY

Chipset EXYNOS M3 Mongoose

Results and Discussion

WhatsApp data were successfully extracted except sample-3 (device name – Realme 2pro chipset-snapdragon) in UFED but no Signal app data has been extracted through MSAB XRY and Cellebrite UFED.

Conclusion

Doing this acquisitions and analysis technical methods like UFED, XRY are challenging, it should be time consuming and advanced version of software like as advancing in technology, this paper shows successful extraction of retrieved WhatsApp data in most of the devices but Signal data is unsuccessful in all the devices by MSAB XRY and UFED. The latest version of XRY 9.3.1 and UFED 7.42.0.82 can't retrieve the signal data.

In future work, a study will consider comparing the signal application data by the proposed tool for successful physical and logical retrieval of data with these commercial tools to get the best results for investigation.

References:

"Signal Revenue & Usage Statistics (2021)." *Business of Apps*, 7 June 2021, www.businessofapps.com/data/signal-statistics.

"WhatsApp 2021 User Statistics: How Many People Use WhatsApp?" *Backlinko*, 2021, backlinko.com/whatsapp-users.

"XRY - Mobile Data Extraction Software." MSAB, 12 June. 2021, www.msab.com/product/xry-extract.

Al Hidaifi, Saleh. "Mobile Forensics: Android Platforms and WhatsApp Extraction Tools." International Journal of Computer Applications, vol. 179, no. 47, 2018, pp. 25–29. Crossref, doi:10.5120/ijca2018917264.

Aziz, Normaziah A., et al. "Mobile Device Forensics: Extracting and Analysing Data from an Android-Based Smartphone." *2015 Fourth International Conference on Cyber Security, Cyber Warfare, and Digital Forensic (CyberSec)*, 2015. *Crossref*, doi:10.1109/cybersec.2015.32.

Khan, Azimuddin, and Zakir Hussain Mansur. *"Comparative Study of Various Digital Forensics Logical Acquisition Tools for Android Smartphone's Internal Memory: A Case Study of Samsung Galaxy S5 and S6." International Journal of Advanced Research in Computer Science, vol. 9, no. 1, 2018, pp. 357–69. Crossref, doi:10.26483/ijarcs.v9i1.5303.*

Sahu, Shubham. "An Analysis of WhatsApp Forensics in Android Smartphones." *International Journal of Engineering Research*, vol. 3, no. 5, 2014, pp. 349–50. *Crossref*, doi:10.17950/ijer/v3s5/514.