Forensic Analysis on WhatsApp/Linkedin

[1] Bhoomi Dangar, [2] Dr.Ravi Sheth, [3] Mr.Priyank Parmar
[1]MTech Student, [2]Assistant Professor, [3]Assistant Professor,
[1,2,3] School of Information Technology, Artificial Intelligence and Cyber Security,
[1,2,3] Rashtriya Raksha University, Gandhinagar, Gujarat, India.

Abstract: The fast growth in usage and application of Social Networking structures reason them to a capability purpose through cyber criminals to conduct malicious sports activities which includes identification theft,piracy,unlawful buying and selling, unlawful income, sexual harassment, cyber harassment, and cyber-terrorism. Many SN structures are extending their services to mobile structures, making them an essential supply of evidence in cyber research cases. On this paper, I observe 2 popular SN packages: WhatsApp and LinkedIn on Android and iOS structures, to uncover the remnants of user activities that may be of forensic interest. This paper makes a speciality of performing a forensic evaluation on social networking applications broadly used on Smartphone's along with WhatsApp and LinkedIn. The subject of this research is an analysis of the artifacts produced by the WhatsApp and LinkedIn application on Android. This study gives analysts and professionals the benefit of helping to find digital proof of WhatsApp on Android. WhatsApp and LinkedIn app artifacts on Android, such as user account records, message exchange documentation, and user uploaded activity traces were successfully described in the results of this analysis.

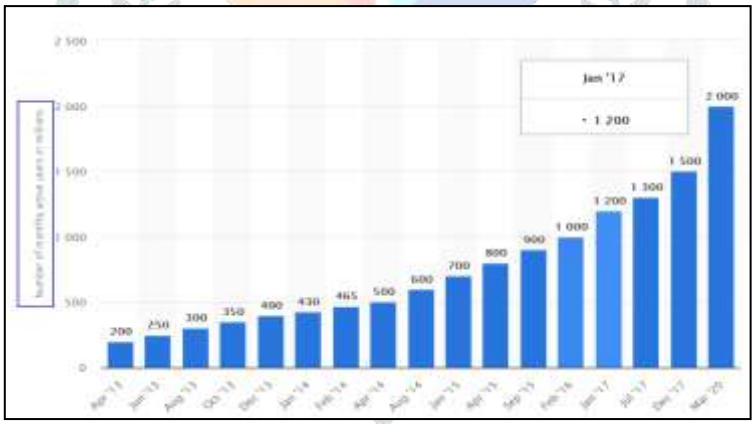
IndexTerms **- Cyber Security, Digital Forensic, Mobile forensic, WhatsApp Forensic, LinkedIn Forensic**

.

I. INTRODUCTION

Cyber Security takes facts that digital forensics has located through various cases and creates approaches to prevent virtual forensic investigations; cyber security is largely proactive.Further, virtual forenscis exists due to failed or susceptible cyber security approaches. Mobile Forensic is branch of digital forensics regarding restoration of digital proof of records from a mobile tool beneath in forensically sound situations.

We have seen the speedy evolution of brand new form of online communication which we call social networking. In cyber investigation cases, many SN systems increase their offering to mobile structure, making them a vast source of evidence. It is also important for forensics to consider the possible forms of evidence for user SN operations available on mobile devices.



[Figure: number of month-to-month active WhatsApp users global from April 2013 to March 2020]

It is impossible to separate WhatsApp from misuse. For those with a criminal motive, which include drug kidnapping, cyber-bullying, trafficking, and so on, A magnet can be used by number of users and end-to-stop encryption technology. There are several cases involving applications for IM or WhatsApp. (1)

LinkedIn is for finding and connecting with business connections. LinkedIn has over 500 million registered users. You can make a copy of the member login details pertaining to the use of industrial tools. As an example, Oxygen Forensics. There's additionally a methods to try this manually.

The investigator wants to do mobile forensics in a case related to phone devices. One of the forensic virtual divisions that discover ways to behavior proof healing from a telephone is mobile /telephone forensic. The investigator will use forensic devices with a forensically-tested approach to conduct forensic evaluation of phone gadgets, so the findings of the analysis are actual earlier than the regulation and may be used as proof. (2)

To pick out crimes, it is largely essential to apply appropriate forensic strategies to get better the ones traces and evidence.

This look at considers social networks in WhatsApp and LinkedIn as a topic for re-research. Study the last artifacts at the WhatsApp/ LinkedIn app and show evidence of collection which consist of tales, posting pictures, tagging others, and profile information on the Android platform, respectively.

II. LITERATURE REVIEW

Rusydi Umar, Imam Riadi and Guntur Maulana Zamroni have proposed a research paper. In order to deal with a case involving Android devices and WhatsApp, they need to do research on the efficiency of the latest forensic equipment.This study analyzed current forensic tools using criteria from NIST and WhatsApp items for engaging in forensic evaluation on WhatsApp. According to the results, Belkasoft proof has the best quality index range, WhatsApp Key/DB Extractor has the lowest cost, and Oxygen Forensic has the highest WhatsApp artefact quality. The purpose of this analysis was to test forensic tools. Primarily based on NIST parameters and additional parameters supplied by researchers, WhatsApp DB/Key Extractor, Belkasoft proof and Oxygen Forensic is probably evaluated in terms of the capability to carry out WhatsApp forensic assessment on Android. The studies used the methods. They have a look at are divided into four methods: simulation of experiments, forensic analysis, outcome of analysis, and conclusion(3)

Social Networking Forensic Objects Analysis has also included the study of artifacts left behind on computer networks and resources by social networking platforms that help extract these artifacts. The method of retrieving and restoring WhatsApp and LinkedIn chat objects from the hard drive of a computer was addressed in other research. The database stores information, including names, identification numbers, and telephone numbers, about each friend on the list. Forensics in social media requires the application of cyber forensics and methods of digital analysis to: Gather understanding from social media networks such as WhatsApp, LinkedIn, etc. Information on the location of the source of electronic proof to combat a case in the court of law are stored, examined and maintained.

In WhatsApp forensic blog, proposed by **fabio sangiacomo** - May 15, 2012.they explain one tool which is whatsapp extract (4).and how it is used in android and ios Smartphone.we can extract encrypted database of whatsapp by rooting or no rooting the Smartphone. Only an encrypted file (/sdcard/WhatsApp/Databases/msgstore.db.crypt) can be obtained from the SD card if you choose to prevent the device from rooting. If you root the device, you can easily access the plain databases (msgstore.db and wa.db). The database for Android is divided into two files: Wa.db stores all contact information (ID, phone number, status, and so on), whereas msgstore.db stores messages, including attachments.

When you connect your iPhone to your computer, iTunes will automatically synchronise and backup the iPhone's content. Furthermore, the backup is not encrypted by default. So, even if the UFED physical analyzer is not used, it may be possible to find a massive amount of data about his iPhone on a suspect's computer. The iPhone Backup Extractor interprets this data and allows you to extract as many files as you want. The data source we are searching for is Application/net.whatsapp.WhatsApp/Documents/ChatStorage.sqlite. (5)

Ambreen F.A.H1 and **C.N. Kayte** have proposed a research paper. They mentioned the forensic evaluation of the artifacts left on the Smartphone by way of WhatsApp Messenger and facebook, and we confirmed how these artifacts can provide a lot of evidence data. Specially, they've proven a way to interpret the statistics saved into the contacts and Chat databases are used to reconstruct the list of contacts as well as the chronology of messages exchanged by users. More importantly, they've demonstrated the significance of correlating the artifacts produced by hats amongst themselves. App Messenger that enables you to acquire records that cannot be inferred by examining them separately. (6)

Igor Mikhailov's Whatsapp forensic artifacts blog, , if you need to know what varieties of WhatsApp forensic artefacts exist in numerous running structures and where they can be observed, you've got come to the right location. This weblog is purely about WhatsApp forensics and the expertise that may be won via forensic studies on a phone. And this weblog is right there in simple sight, absolutely on Whatsapp.:Where in and how to gather forensics objects. An investigator needs to have superuser (root) privileges to do away with WhatsApp gadgets from an Android tool or be able to extract a physical memory dump from the report machine via different method (for example, the use of software vulnerabilities of a selected device). Documents within the program are located within the telephone's memory within the section where person records is saved. This part, mostly, is known as Userdata. The subdirectories and application documents are found beneath the direction /data/data/com.whatsapp/. The wa.db and msgstore.db databases are the primary documents containing WhatsApp items on Android. (7)

In digital forensic blog **Oleg Skulkin** and **Igor Mikhaylov** proposed article for LinkedIn. How to purchase a LinkedIn account was examined in the paper .This method no longer necessitates the usage of forensics software program; however it's far vital to attend 24 hours before the LinkedIn member archive document is available for down load. (8)

WhatsApp has end-to-end encryption, which ensures they're unreadable if everybody, which includes regulation enforcement and WhatsApp itself, intercepts them. extra substantially, at the WhatsApp server, WhatsApp communications are in no way saved. With this sort of safety constructed into the utility,it is not surprising that it is regularly the option of communication channel for users with sinister agendas. The most complete WhatsApp information extraction and decryption tools in the marketplace are supplied through Oxygen Forensics.

In WhatsApp From Mobile Devices, However, the data is accessible in a decrypted format on an Apple iOS or Android Smartphone. In today's mobile device exams involving WhatsApp and other applications, the challenges investigators frequently face how to overcome a device with a display lock or device encryption. In a essential iTunes backup system, all WhatsApp statistics may be removed in terms of iOS computers.However, we also suggest a physical extraction method for Android devices to retrieve WhatsApp proof files. On a broad variety of Android devices, we offer a wide range of physical selection methods that are effective. Note, always search the SD card for a WhatsApp backup while reviewing an Android device (9)

2.1 Table :- Evaluation of Most efficient Identification Techniques

Research proposed by	Research on	Methods	Tools used	Limitation
Rusydi Umar, Imam Riadi and Guntur Maulana Zamroni (3)	efficiency of the latest forensic equipment	1)Simulation of experiments 2)forensic analysis 3)outcome of analysis 4)conclusion	1)WhatsApp Key/DB Extractor 2)Oxygen Forensic 3)Belkasoft	The result shows that Belkasoft Proof has the highest index number, WhatsApp Key/DB Extractor has cost superiority, and Oxygen Forensic has WhatsApp artifact superiority.
fabio sangiacomo (5)	explain one tool which is whatsapp extract	1)by rooting or 2)No-rooting Smartphone	Whatsapp Extract	1)If you choose to avoid the rooting of the device ,you will be only able to get an encrypted file from the SD card (/sdcard/WhatsApp/Databases/msgstore.db.crypt). 2)Conversely, if you root the device, you will easily reach the plain databases (/data/data/com.whatsapp/databases/msgstore.db and wa.db).
Ambreen F.A.H1 and C.N. Kayte (6)	How wp and fb's artifacts can provide a lot of evidence data.	1)Identification of evidence 2)Collection 3)Examination	Wp's and FB's different artifacts	
Igor Mikhailov (7)	Whatsapp forensic artificats	1)investigator needs to have superuser privileges (root) or be able to extract a physical memory dump of the file system	Wp's different paths	This post is focused on WhatsApp forensics and what data can be obtained from a device during forensic analysis
Oleg Skulkin &Igor Mikhaylov (8)	LinkedIn Forensic	How to acquire a LinkedIn account	This method does not require the use of forensics tools	it is required to wait for 24 hours while the archive file with the LinkedIn member will be available for download
Oxygen Forensics (9)	Whatsapp forensic	Decryption of Backup	Oxygen Forensic Detective	This tool offers only decryption methods.

III. **Conclusion**

In this paper, we discussed the forensic evolution of artifacts left on Smartphone's via WhatsApp and LinkedIn; we tested how these artifacts can provide many records of evidentiary cost. In step with the evolution table, present gear and research have a few boundaries, such as a complicated shape, time-consuming set up, a paid version to be had, and simplest manual and decryption techniques. And most important they haven't do analysis related to status or stories hence there is requirement to find some useful status information from Whatsapp and LinkedIn for forensic analyst.

References

[1] *With Islamic State using instant messaging apps,FBI seeks access to data.* **B.Bennet.** 2015, Los Angeles Times.

[2] *"Guidelines on mobile device forensics".* **R. Ayers, W.jansen, and S.Brothers.** 85, 2014, NIST special publication, Vol. 1.

[3] *A Comparative study of forensic Tools For WhatsApp Analysis using NIST Measurements.* **Rusydi Umar, Imam Riadi and Guntur Maulana Zamroni.** 12, 2017, International Journal of Advanced Computer Science and Applications(IJACSA), Vol. 8.

[4] **ztedd.** https://forum.xda-developers.com/t/tool-whatsapp-xtract-backup-messages-extractor-database-analyzer-chat-backup.1583021/. *forum.xda-developers.com.* [Online] April 5, 2012.

[5] **sangiacomo, fabio.** https://blog.digital-forensics.it/2012/05/whatsapp-forensics.html. [Online] May 15 , 2012.

[6] *Forensic Analysis of Social Applications.* **Ambreen F.A.H1, C.N. Kayte.** IOSR Journal of Computer Engineering (IOSR-JCE) , pp. 39-44. ISSN.

[7] **Mikhailov, Igor.** https://www.group-ib.com/blog/whatsapp_forensic_artifacts. *https://www.group-ib.com/.* [Online] 11 7, 2019.

[8] **Igor Mikhaylov, Oleg Skulkin.** https://www.digitalforensics.com/blog/how-to-acquire-a-linkedin-account/. *digitalforensics.com.* [Online]

[9] **Forensics, By Oxygen.** https://blog.oxygen-forensic.com/whatsapp-forensics/. [Online] January 29, 2019.