Digital Foot-Printing of Artifacts of Web Based Applications on Windows

***Omraj Gautam**

Abstract

Internet Security has become a notable concern in today's world, due to the reason that the security can not only be compromised via illegal activities such as malware threat, money laundering, child-abuse material, drug trafficking, fraud, etc. but also via Internet activity tracking. Hence crime over internet has become a serious problem now-a-day. Various web applications are used to perform various different activities over the Internet such as, searching for information, online shopping, email communication, etc. Aside from such common usage of web applications also desire to chat over Internet in a secure manner so as to protect their privacy, as web applications are designed in such a manner that they tend to store certain information related to the users and their activities.

Web Based applications have changed the way people communicate with one another. They are becoming widely popular amongst the individuals, corporates and also among the criminals due to its secure and cheap services. Since these applications are available on multiple operating systems therefore it has become very necessary to investigate the artefact location of these application on multiple platforms. In this research we have focused on artefact analysis of five common web applications on Windows. Real chats and calls were performed on these applications. The artefacts were extracted from volatile memory of these operating systems. We were able to identify artefacts like messages, call details, transferred images and login credentials. Our results showed that memory forensics was the best way for identification of artefacts from these web applications because they have end to end encryption because of which over the network acquisition was not possible. In this thesis we have also highlighted the differences between the artefacts in these applications.

Index Terms- Digital Forensics, Volatile Memory, Web Application Forensics, Live and Dead Forensics

I. Introduction

Earlier before the use of social media applications the communication between people was limited mainly to sending and receiving text messages but with the advent of the internet and social media, the communication system has drastically changed over the years for people. Social media platform has opened up an opportunity to share an opinion with a far wider audience. Instant messaging or web-based chatting applications are becoming very popular among individuals and corporate sectors

due to their secure and cheap services. These web chat applications allow users to communicate in real time as they have easily accessible web interfaces.

Moreover, many popular instant messaging applications have built-in advanced features such as private/encrypted chat, file transfer, status following, user-friendly interface, secure peer to peer technology, multiple device platforms, and many more features. Web-Based applications are distinguished by its simplicity and accessibility to users on multiple platforms like Windows, Linux and Mac OS where users don't have to install and learn to use specialized chat software and this provides them instantaneous access and only a web browser is needed to chat. The users will always get the latest version of a chat service because no software installation or update is needed. WhatsApp Messenger, Telegram, and Skype are examples of some of the most commonly used instant messaging applications used on Android smartphones and also on Windows, Linux and Mac OS and they can be directly opened on a web browser.

WhatsApp Messenger is a widely used instant messaging application with more than 1 billion users. It allows users of Android, IPhone, windows and Nokia smartphone users exchanges text, audio and video messages for free and it can also be used on a computer with Windows, Mac OS, and Linux OS because of it does not require separate software it can directly open on a web browser.

It is free of cost which is its biggest advantage and also it is user-friendly because of which it is used by young generation as well as old generation people and also those people who are not tech savvy. And also, it does not have any advertisement and the chats are encrypted. All these advantages make WhatsApp a very useful instant messaging application with that it is also misused by some people for committing cybercrime. People share fake messages, video, and obscene content.

Telegram Messenger

It is a messaging app which works just like WhatsApp or Facebook over the internet. It allows users to send messages for free by using a Wi-Fi connection on mobile data allowance (providing you have enough data). Its web client allows users to enjoy all the features of Telegram App right in your web browser and also it supports private messaging.

Skype

Skype is a telecommunications application that specializes in providing video chat and voice calls between computer, tablets, mobile devices, the Xbox One console and smartwatches via the internet and it also provides instant messaging services which also users to transmit text, video, audio and images and also skype supports conference calls. It can be used on Windows, Linux and Mac OS.

The increased usage and need of social media have raised the risks associated with it which if not taken into account can contribute to major losses as social media usage is not limited to personal matters but is also used for business advertising and selling purposes.

Digital Forensics is a branch of forensic science which includes the identification, recovery, investigation and validation and presentation of facts regarding digital evidence found on the computer or similar digital storage devices.

Memory forensics is a branch of digital forensics which is useful in identifying artefacts of web chats stored in physical memory of the computer.

The Physical memory of the computer i.e. RAM (Random Access Memory) is the heart of the computer system. It contains information about all the carried out on your PC. It is the hardware in a computing device where the operating system, application programs and data in current use are kept so that they can be quickly reached by the device processor. Random Access Memory is volatile which means that data is retained in RAM as long as the computer is on, but it is lost when the computer is turned off. It plays a very important role in memory forensics.

Memory Forensics refers to the analysis of the volatile data from the computer's memory dump. It is used by cybersecurity professionals to investigate and identify attacks or malicious behaviors that do not leave easily detectable trait on hard drive data. Volatile data is the data stored in the temporary memory on a computer while it's running. When the computer is powered off, the volatile data is lost immediately. Volatile data includes data like browsing history, chat messages and clipboard content and also a list of all the processes that have been carried out on the PC. This situation is desirable when the investigator arrives at the site where the computer is still on and the instant messaging application like Skype, WhatsApp, Telegram, is still on. For analysis of this volatile data, memory is collected. A memory dump also is known as a core dump or system dump is a snapshot capture of computer memory data from a specific instant. A memory dump contains valuable forensics data about the state of the computer system before an incident such as a crash or security compromise. Memory dump contains RAM data that can be used to identify the cause of an incident and other key detail about what happened.

Along with the rapid growth of instant messaging applications, cybercrime has become a major concern to public security. For instance, the private /encrypted chat function could be used by terrorist for communicating with one another.

In this case, memory forensics can provide valuable information about open network connections and recently executed commands or processes. In many cases critical data pertaining to attacks or threats will exist solely in system memory-examples includes network connections, account credentials, chat messages, encryption keys, running processes, injected code fragments and internet history which is non-cacheable. As attack methods become increasingly sophisticated, memory forensic tools and skill have become very necessary in many areas of instant messaging because information like running process list, open network connections, encrypted data, passwords, and malicious codes reside in physical memory.

II. AIM & OBJECTIVE

The aim and objective of the research are very important for directing actions and activities. The aim of this research is to analyze and compare artefacts of the five instant messaging applications

WhatsApp, Skype, Telegram, on Windows, Linux and Mac OS. Based on the above-formulated aim, the following objectives are created:

- To identify artefacts of WhatsApp, Telegram, and Skype on Windows, Linux, and Mac OS.
- To Compare artefacts of this application on Windows, Linux and Mac OS.
- To find out the similarities and differences of the artefacts of this app on Windows, Linux and Mac OS

III. Forensic Significance

The forensic significance of this research is that most of the important user information could be retrieved from all the operating system through memory forensics.

It also showed that during LIVE memory acquisition maximum artefacts could be recovered. After shutting down maximum information is lost.

IV. Challenges

- The research in RAM forensics has been performed on a virtual machine environment i.e., VMware. This has been done to reduce the captured memory size and make the process of analysis and acquisition of the RAM less cumbersome. But since this method is a simulation of the real-world environment so we do not get the whole picture.
- VMware does not directly support the installation of Mac OS. So, we do need to download a patch tool to make it compatible for installation in VMware.
- Since in VMware a simulated environment is created so actual Apple drivers are not present because of which installation of memory forensic tools like Rekall forensics and osxpmem was not possible.
- In Ubuntu, also because of lack of some system requirement it was not possible to install memory forensic tool like Rekall forensics in it.
- Since the size of virtual memory is very low i.e., 2 Gb because of the which the chances of data being overwritten increases.
- Over the network acquisition of artefacts was not possible as all the applications had end to end encryption.
- Carrying out a smooth audio and video call was also not possible.

V. Literature Review

The topic of research is based on comparing artefacts of web-based applications on Windows. Several literature sources which include journal, articles, online or web- based articles and certain books and the research work of many qualified academicians and authors is included and reviewed for the development of theoretical knowledge.

In the study conducted by Nicolás Villacís Vukadinović the authors propose the analysis of the WhatsApp clients revealed the presence of several artifacts of value for digital forensics investigators. The main source of artifacts is the WhatsApp log file, present throughout all WhatsApp clients. Within this log file, different data can be found, such as timestamps of user actions, and browser user agent information.

In the study conducted by Diogo Barradas, Tiago Brito, David Duarte, Nuno Santos, and Lu´ıs Rodrigues, described a forensic study over the digital artifacts left behind in memory by popular web applications. This study concludes that it is possible to retrieve communication records from IM/email applications, in various settings and system configurations.

In the study conducted by Majeed (2017) remnants of Facebook, Viber and Skype were explored on the Windows 10 platform. The potential locations were explored and examined to find out the location of artefacts and their details. An effort was made to recover items from unallocated space, which also includes those that were permanently deleted from Windows.

A related study of Forensic Analysis of Social Media on Windows 10 was conducted by Majeed (2013). In the paper the study on location of artefacts of the frequently used

applications like Facebook, Skype and Twitter were done on the Windows 10 platform. Some of the differences were also highlighted in this paper found with previous version of Windows i.e., Windows 8.1. The information about the usage of the above-mentioned social media applications was found in both the relevant databases and the registry entries.

In relation to forensic analysis of WhatsApp messenger on android smartphones a study was conducted by Anglano C et.al (2014) which provided a complete description of all the artifacts generated by WhatsApp messenger. By using the results generated a reconstruction of list of contacts and the chronology of the messages that have been exchanged by the user can be done. Through this the information like when a specific contact has been added, deleted contacts and their time of deletion, when the messages have been deleted, when these have messages have been exchanged and the users between whom the messages had been exchanged can be determined.

IMO is a mobile application which allows making audio and video calls, chat messages, share photos and videos and group chatting and an increased usage of these application has become important source of computer forensic investigation. The paper by Ababneh, et. al (2017) provided a forensic prospective for investigation of IMO App on Android and Windows systems. Real chats and calls were

performed in different scenarios and artefacts were extracted from NAND flash memory in Android and the main memory (RAM) in Windows platform. The results showed that important data can still be recovered even after deleting chats and uninstalling the app. Another research was conducted on IMO chat application by

M.A.K. Sudozai et.al (2018). A thorough study of important artifacts of IMO chat application was conducted on both android and iOS platforms. The novel aspect of the work is the extensive analysis of the encrypted traffic generated by IMO. Along with this a new method of using a firewall to explore the obscured options of connectivity, in a way, which is independent of the protocol used by the IMO client and server. The results of this research determine that IMO traffic flows can be correctly detected and different events of its chat and related activities can be determined. And the comparison of IMO network traffic was done on both Android and iOS platform and subtle differences were reported.

Ovens & Morison (2016) stated that digital forensic analysis is based on the systematic extraction of information from hardware and software. The hardware approach is easy to implement because it helps in detaching the android device chip and then the files are extracted to the respective storage location. In addition to this Walnycky et.al. (2015), conducted a network and device-based forensic analysis for extracting the artefacts from Android social messaging applications. The research indicated that it is easier for the digital forensic experts to identify the criminals through extraction of messages from the smartphone using network and device forensics.

The artefacts extracted from the social messaging applications include chats, logs, information about the location of person and all significant information which was transferred during the communication. Further, Simpao et.al., (2015) present that the smartphones majorly remain in the proximity of customers and they are widely used as compared to the computers or desktops which are not available in the proximity. The quantities of digital evidence available in smartphones is higher as compared to the data available over computers and other devices.

The process of acquiring artefacts is intricate, but easier at the ends of cybercriminals or hackers because they are using the social media applications or messengers to dupe the customers. Satrya, Daely, & Shin (2016) conducted an android forensic analysis through focusing on the private chats that are present on the social messengers. The authors used different versions of the android operating system for conducting their digital experimental and found that there are numerous vulnerabilities that prevail over the social messengers when considering the transfer of personal information. Lack of encryption over these platforms is a serious threat that is experienced by customers which could further lead them to the dangers like theft of intellectual property and social security numbers. In addition to this study, the works of Majeed and Saleem (2017) present the forensic analysis of social media applications by using Windows 10 operating system. The identified that modern version of Windows operating system is more efficient in tackling threats and cybersecurity breaches as compared to the previous versions. The authors considered using social

media applications like Facebook, Skype and Twitter for conducting their studies and led to the finding that there are numerous risks prevailing over users while messaging and communicating through these platforms.

It cannot be denied that the social media applications like Facebook, Instagram or Twitter have high attraction power which keeps users engaged and involved to a great extent. However, Sgaras, Kechadi & Le-Khac (2012) explains that the greater involvement of individuals over social media messaging applications creates a negative effect on their personal security and well-being. They tend to share more information which is traded by companies for their economic and monetary benefits. About two times, Facebook was responsible for the breach of nearly a million users which included their personal information, pictures, statuses, promotional advertisement preferences, etc.

As mentioned by Al Mutawa et.al., (2011) in their study, the use of digital forensics has been supportive in identifying the artefacts that are transferred when communication takes place over the social media applications. This extraction of artefacts has become the foundational basis for developing tools and strategies that could protect the users from losing their credentials and improves the authenticity of their communication platforms.

The findings of Anglano (2014), on the forensic analysis of WhatsApp messenger over the android operating system indicated that the chronology of messages is reconstructed through the use of digital forensic tools. There is enough scope for the researchers to recover deleted contacts, the time at which they were deleted as well as the messages that were deleted ever in the history of specific WhatsApp number. Entire history of conversation over this communication platform is retrieved through the use of digital forensic tools and decoding.

With rise of sophisticated communication systems, the risks over loss of credentials and hacking of entire computer systems have increased as was explained by Al Mutawa, Baggili & Marrington, (2012). The potential threats over the database of these communication applications have increased and this has increased the responsibility of companies to improve their security features. The forensic analysis of such communication applications is helpful in identifying the encryption algorithms, their durability as well as their authenticity in resolving the security issues. Further, Simon, & Sla (2010) explained that contents of the memory and written pieces of information are not acquired easily unless there is effective forensic analysis technique applied. The social network applications have a large chat database which is accessed in the analysis for retrieving the artefacts and consequently the information that was transferred between two or more users.

Ababneh, Awwad & Al-Saleh (2017) presented that smartphone forensics is an emerging branch of digital forensics that is useful in reducing the threats and negative consequences when the messenger applications are hacked or breached. The users of IMO messaging application have presented several security issues especially when engaged in video and audio calls, while sharing photos or when chatting through messages. The increased usage has subjected users to several threats which are hidden and have potential of completely disrupting the security of users. However,

Cahyani et.al. (2017) mentioned that applications like WhatsApp, Line, Skype, Viber and IMO are supportive in providing spontaneous messages and information irrespective of the distance and location of the users. There is no limit over the number of messages, but higher dependency on internet connection.

The engagement of such huge customer base is attractive for the hackers and unethical practitioners. However, the forensic or digital analysis helps in acquiring chat evidences that could help in reducing the threats and consequently improving the security of the messaging application.

According to the views of Kitsaki et.al. (2018) the messaging applications include different types of sensitive information as they consider that they have complete ownership of their information. It was identified that the handling of sensitive information is ineffective when it comes to the works of smart applications and therefore, the forensic analysis techniques have to be implemented for extracting information with maximum efficiency. The encryption algorithms are to be designed in a way that there is higher security and safety provided to the credentials of users. However, Ghafarian and Wood (2018) conducted research on forensic data recovery through the physical memory using Skype application. It was identified that despite the popularity of Skype for its cheap services and highly secure features, there is not much safety provided to users especially in the presence of cybercriminals and hackers. The forensic examination of Skype communication presented that data like active processes, hidden processes and terminated processes along with all the files open over Skype are retrieved through the use of forensic tools. The extraction of artifacts is easier with the use of volatile memory forensics and for checking the durability of the messaging application.

VI. Tools & Technologies

1. Windows Operating System

Windows is a closed source operating system developed by Microsoft to overcome the limitations of the MS-DOS operating system on November 20, 1985. It dominates the world's personal computer (PC) market with 90% of the users. It uses an NTFS file system and a FAT file system which has been inherited from old DOS and has exFAT as its later extension. The active and the most popular versions of Windows have been Windows XP, Windows 7, Windows 8 and Windows 10. Windows 10 is the latest version released on July 29, 2015. Windows 10 is the most widely used version of Windows because of its uniqueness.

The most distinguished feature of Windows 10 is that it supports universal apps (Universal windows app are those program that can be used across all Microsoft compatible devices). Windows 10 also introduced revised user interface to handle transitions between a mouse- oriented interface and a touchscreen-optimized interface based on available input devices, both of these interfaces include an updated Start menu which incorporates elements of Windows 7 's traditional Start menu with tiles of Windows 8. It has also introduced a Microsoft Edge web browser, a virtual desktop system, Task view (it is a window and desktop management feature, support for fingerprint and face recognition

login, new security features for enterprise environment and it also contains Windows Defenders tool with the latest security patch.

The latest version of Windows 10 is the October 2020 Update, version "20H2," which was released on October 20, 2020. is the most advanced version of Windows 10 which contains some unique features which make it more user-friendly because of which it was used for the research.

2. Belkasoft RAM capture

It is a free volatile memory forensic tool which helps in extracting the entire content of the volatile memory even if it protected by anti-debugging or anti-dumping system. It is equipped with separate 32-bit and 64-bit kernel drivers which allows the tool to operate at a privileged kernel and also minimizes the footprint of the tool as much as possible.

The memory dump is stored with. mem extension and later it the memory dump can be used for further analysis.

Belkasoft Live RAM Capturer is compatible with all versions and edition of Windows including XP, Vista, Windows 7,8, 10, 2003 and 2008 server.

3. Ftk Imager

The Ftk Imager is a forensic tool which creates a bit-by-bit image, including unallocated space and slack space. It helps to examine files and folders on hard drives, network drives, CDs/DVDs and reviews the content of forensic images or memory dump. It is used for live memory capture but it cannot analyze the captured memory dump. It stores the memory dump with. mem extensions which later can be analyzed using a WxHexEditor tool or some other tool.

4. Strings

The string is a command line utility of Sysinternals Suite which uses a set of command that prints out any ASCII or Unicode strings in the input file. It is used by forensic examiners to get a sense of the functionality of an unknown program. User prompts, error messages, and status messages can give hints, but should not be used as proof or lack or any functionality. It is also used for conversion of data from the memory dump into a user readable form.

5. wxHexEditor

It is a free memory forensic tool which is used for analysis of data from the memory dump. It has two parts on the right side the information from the string value is displayed and the hex values of the strings which can be analyzed are displayed on the left side. It is present for all Windows, Linux and Mac OSX.

6. Ubuntu

For this research Ubuntu version, 18.10 was used for this research. It is an open-source Linux operating system which powers millions of PCs and laptops around the world. The major advantages of Ubuntu OS are:

I. Ubuntu contains all essential applications like an office suite, browsers and media apps in its software center.

II. Ubuntu is an opensource software which is freely available to download, use and share. It cannot exist with its worldwide community of voluntary developers.

III. Ubuntu has a built-in firewall and virus protection software which makes it the most secure operating system. The long-term releases give users five years of security patches and updates.

IV. Ubuntu is freely accessible to everyone regardless of nationality, gender or disability. It completely translated into 50 languages and also includes essential assistive technologies.

7. Lime

LIME is a memory forensic tool which contains a Loadable Kernel Module (LKM) which help to acquire memory from Linux and Linux-based devices. It is a first memory forensic tool which helps in the complete acquisition of memory. It also helps to minimize the interaction between user and kernel space processes while taking the memory dump. It helps to create memory dump which is more forensically sound than any other tool which is used for Linux memory acquisition.

8. MAC OS X

Mac OSX is the operating system that resides on Apple's desktop and portable computer line up. It is built upon a Unix core. It is easy to use highly advanced extremely stable and an excellent OS for productivity and creation.

9. VMware Workstation

VMware Workstation Pro is one of the desktop applications in which virtualization is available. It helps to create a simulated environment for running multiple operating systems like Windows, Linux and Mac OSX on a single PC. It used to build a test or demo software for any device by IT professionals, developers, and businesses

The benefit of using VMware Workstation Pro is that

i. It helps to run multiple OSs on a single PC

VMware Workstation Pro helps to run multiple operating systems like Windows, Mac, and Linux at once on your PC. It creates a complete simulated environment with configurable virtual networking and network condition to create a real Linux, windows virtual machine and other desktop server and tablet environment.

ii. It helps to develop and test for any platform

Hundreds of operating systems are supported by the Workstation pro and also it works with cloud and container technologies like Docker and Kubernetes.

iii. It helps to connect with VMware vSphere

VMware Workstation helps to control and manage both physical host and virtual machines by securely connecting with vSphere, ESXi or other servers of the workstation to launch. To maximize productivity and to enable easy transfer of virtual machine from your local PC VMware hypervisor is used.

iv. It helps to Secure and Isolate Environments

It helps to helps to run a secure second operating system by using forensic tools to investigate vulnerabilities of the operating system and also by using different privacy settings, tools, and network configuration. It contains one of the most secure hypervisors which delivers powerful features for cybersecurity professional.

VII. Environment Setup

In this research we investigate WhatsApp, Telegram, and Skype on Windows, Linux and Mac OS X. The workstation we used is a Lenovo laptop with Intel i5 processor with 2.20 GHz Base speed and 4GB RAM with a virtual machine that runs Windows 10, Ubuntu 18.10 and Mac OS X 10.14 with all the application running on them.

The following list summarizes the tools and applications that are utilized in our investigation:

a. Windows 10 with version 20H2 (OS Version 10.0.19042)

b. Ubuntu 18.10 (Cosmic Cuttlefish)

c. Mac OS Mojave (version 10.14)

d. Belkasoft RAM Capturer for taking the memory dump in Windows 10

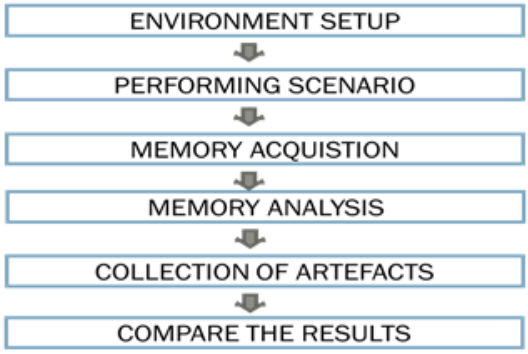
e. Strings 64 for analysis of memory dump

f. WxHexEditor

g. LIME master for collecting the memory dump in Ubuntu

h. Google Chrome Version 87.0.4280.88 (Official Build) (64-bit)is installed on all the three operating systems.

VIII. Research Methodology



EXTRACTION OF ARTEFACTS.

This section focusses on extraction of artefacts of WhatsApp, Telegram, and Skype on Windows operating system.

I. Performing Scenarios

After installing the web browser opened the web applications (WhatsApp, Telegram and Skype) were opened in it and account was created on them and then interactive activities were performed like audio calls, video calls, sharing images and sending messages.

II. Memory Acquisition

It is a process in which we do acquisition of memory by collecting the RAM dump. Three RAM dumps of each application were taken.

In first scenario, a live RAM dump was taken. Which means that RAM dump was collected keeping all the tabs of the application running.

In second scenario, a dead RAM dump was taken. Which means a RAM dump was collected after closing all the tabs of the application and browsing of the browser.

In third scenario, RAM dump was taken after shut down and restarting the host machine. After collecting all the RAM dumps for all the browsers. Its analysis was done using manual and automatic techniques.

III. Memory Analysis

After collecting the RAM dump the collected memory dump was analyzed using tools like Strings64 for windows, LIME for Linux and VMEM for MacOS

IV. Collection of Artefacts

The collection of artefacts was done by searching them from the memory dump by using appropriate keywords

V. Comparing the results

After collecting the artefacts, the results are compared with that obtained from other operating systems.

IX. Result and discussion

Here some particular scenario for investigating web-based applications had been tested. We performed some activities on the applications like URLs search, chats, sharing images, audio and video calls, contact information and then three RAM dumps of each application were taken, Live RAM dump, Dead RAM Dump, after shutdown RAM dump and then some tools and techniques were used to identify the artefacts.

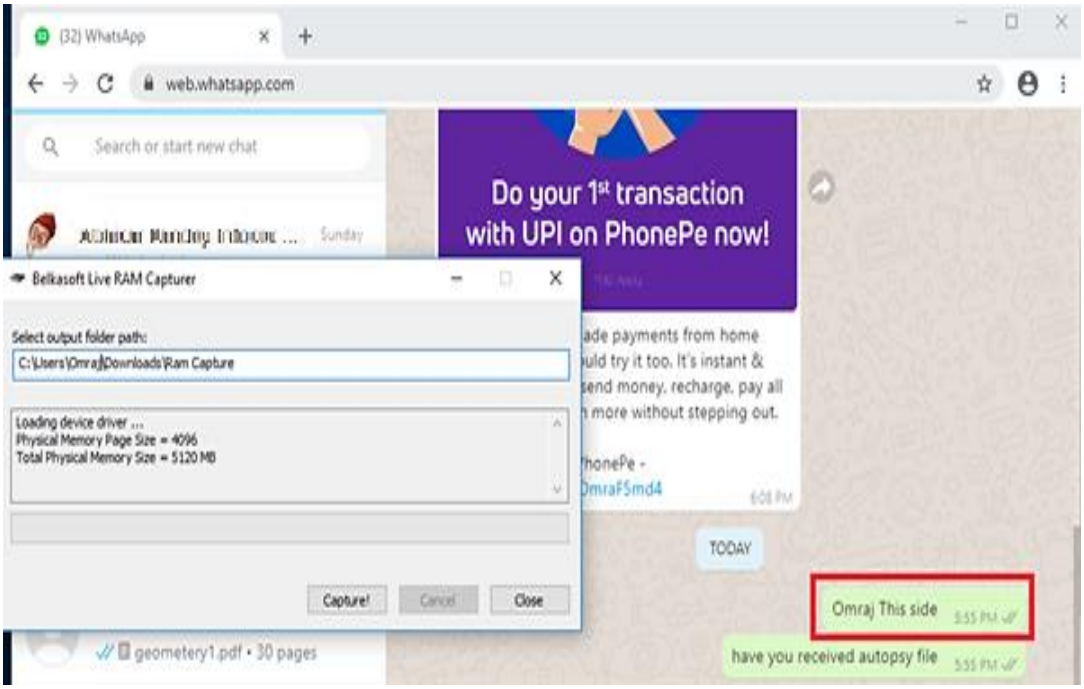
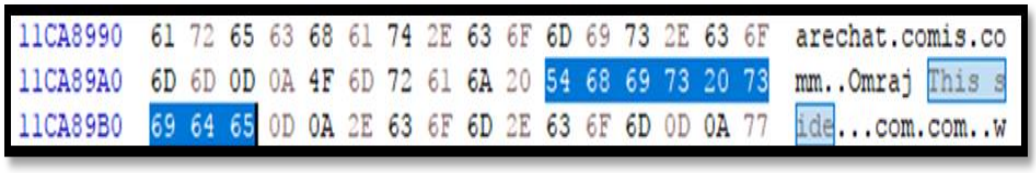


Figure 1. – Windows WhatsApp Chat

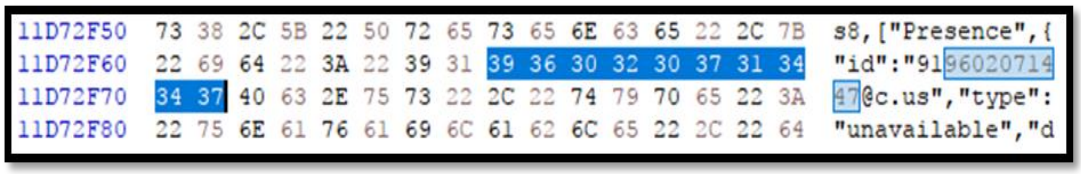
A. Live RAM Analysis

- **Chat Messages**



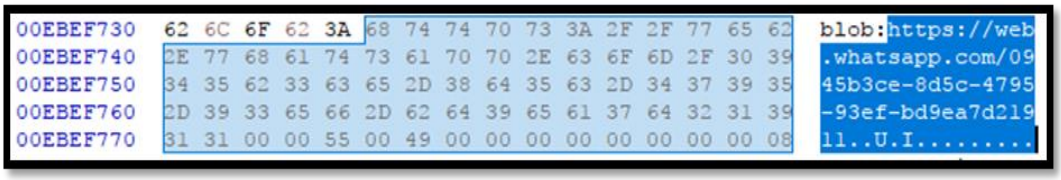
It shows the message along with day and date

- **Phone number**



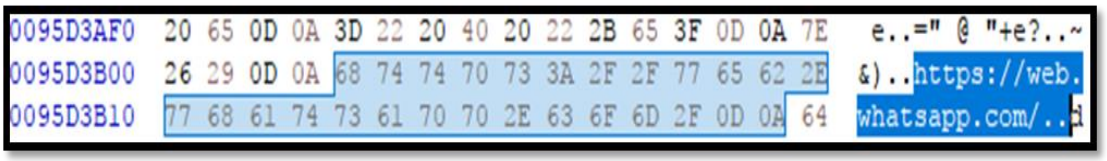
It show the contact information i.e. phone numbers of people in the contact list

- **Images**



It Shows the image shared on WhatsApp.

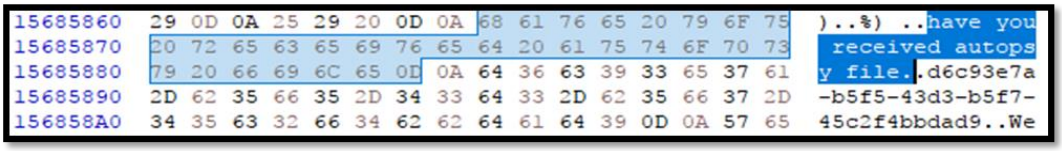
- **URL**



It shows the URL which indicate that web WhatsApp was opened on Windows.

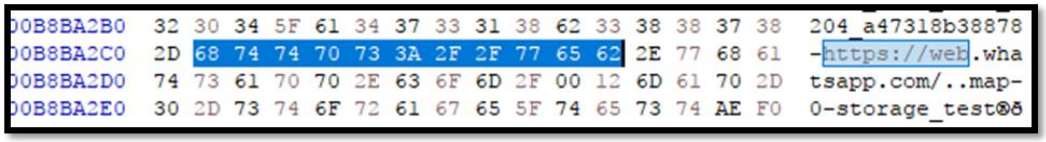
B. DEAD RAM ANALYSIS

- **Chat messages**



Complete chat messages were not recovered only a part of it was found.

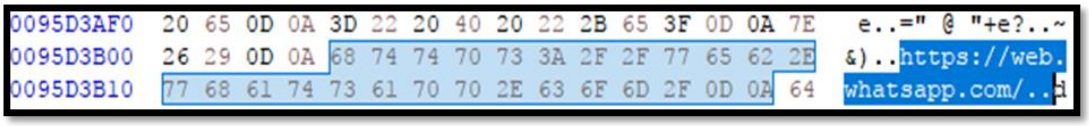
- **URL**



It show the URL which indicate that Web WhatsApp was opened on Windows

C. AFTER SHUT DOWN

- **URL**



Only URL could be recovered after shut down.

DISCUSSION

All the web applications showed a similar pattern in revealing artefacts during analysis in all the three operating systems. The live RAM dump has been successful in revealing almost all the operating system and only a minute difference was observed in the trend, no images could be recovered from telegram messenger in Ubuntu and Mac OS X.

During the Dead RAM only chat messages and URL could be recovered. And also, not complete messages were recovered only a part of it was found.

While doing the RAM analysis after shutdown almost not artefact was found.

The table below shows a list of all the artefacts that can be found in all the web applications.

Table 1 List of Artefacts Found In All the Applications

INSTANT MESSAGING APPLICATION	LIVE ARTEFACTS	DEAD ARTEFACTS	AFTER SYSTEM SHUTDOWN
WhatsApp	Chats Images Phone number URL	Chats URL	URL
Telegram	Chats Images Phone number URL	Chats URL	URL
Skype	Chats Skype Id URL call	Chats URL Skype id	URL

From the above table, it can be clearly seen that

- Live RAM analysis - Almost all the artefacts were found excepts password in some browsers
- Dead RAM analysis - Number of artefacts found reduced profoundly and there was dissimilarity observed in the artefacts found in different browsers.
- After Shutdown hardly revealed anything except URL artefacts.

WINDOWS

Table 2: LIST OF ARTEFACTS FOUND IN ALL THE APPLICATIONS IN WINDOWS

Artefacts	WhatsApp			Telegram			Skype		
	L	D	AS	L	D	AS	L	D	AS
URL	✓	✓	✓	✓	✓	✓	✓	✓	✓
Chats	✓	✓	✗	✓	✓	✗	✓	✓	✗
Phone Number	✓	✗	✗	✓	✗	✗	✓	✗	✗
Images	✓	✗	✗	✓	✗	✗	✓	✗	✗
Call details	✗	✗	✗	✗	✗	✗	✓	✗	✗
Skype ID	-	-	-	-	-	-	✓	✓	✗

UBUNTU

Table 3: LIST OF ARTEFACTS FOUND IN ALL THE APPLICATIONS IN UBUNTU

Artefacts	WhatsApp			Telegram			Skype		
	L	D	AS	L	D	AS	L	D	AS
URL	✓	✓	✓	✓	✓	✓	✓	✓	✓
Chats	✓	✓	✗	✓	✓	✗	✓	✗	✗
Phone Number	✓	✗	✗	✓	✗	✗	✗	✗	✗
Images	✓	✗	✗	✓	✗	✗	✓	✗	✗
Call details	✗	✗	✗	✗	✗	✗	✓	✗	✗
Skype id	-	-	-	-	-	-	✓	✓	✗

MAC OS

Table 4: LIST OF ARTEFACTS FOUND IN ALL APPLCATIONS IN MAC OS X

Artefacts	WhatsApp			Telegram			Skype		
	L	D	AS	L	D	AS	L	D	AS
URL	✓	✓	✓	✓	✓	✓	✓	✓	✓
Chats	✓	✓	✗	✓	✓	✗	✓	✓	✗
Phone no.	✓	✗	✗	✓	✗	✗	✗	✗	✗
Images	✓	✗	✗	✗	✗	✗	✗	✗	✗
Call details	✗	✗	✗	✗	✗	✗	✓	✗	✗
Skype Id	-	-	-	-	-	-	✓	✗	✗

X. CONCLUSION

This research is focused on analyzing the artefact of the five most commonly used web application, WhatsApp, Telegram, and Skype on Windows, Linux and Mac OS X. These web applications are used widely all over the world because of their easy user interface. And since these devices have support on multiple operating systems, therefore, it is necessary to find artefacts of these applications in the different operating system.

As our study was limited to the scenarios, we considered the following conclusion can be made- Almost all the artefacts were found during RAM dump analysis in all the application. While during Dead RAM dump analysis very few artefacts were revealed than Live RAM analysis. After restart RAM dump analysis revealed almost no artefacts except the URL. This trend was also similar in all the applications.

Amongst the three operating systems, the best results were given by the Windows operating system where maximum artefacts were found during Live RAM analysis.

Similar artefacts were found on all the operating system during Dead RAM analysis and after shut down.

A very small difference was observed in the artefacts found during live RAM analysis in all the operating system.

In Instant messaging forensic, it can be said that if there is a machine with some evidential value then following things should be considered - If the tabs of are open, then it would be best to take the RAM dump. Keeping all the tabs open as it has been established from the study that Live RAM dump analysis reveals a maximum number of artefacts in all the applications. If the browsing window is found closed, then however a difference in the trend of findings was observed. It still revealed some important artefacts like URL and partially recovered chat messages which can provide some lead in the investigation but surely it was not as revealing as live RAM dump analysis. Thirdly, if the system is found in "shutdown" mode then most of the private browser artefacts are lost.

XI. FUTURE WORK

- We kept our study limited to forensic aspect but security aspect can also be studied of the above applications. More applications are hitting the market regularly, they can also be included in the scope of the study.
- The artefacts were collected after installing the operating system in a virtual machine accordingly the same techniques could be followed to collect artefacts on a live operating system.
- The acquisition of artefacts can also be done by using private browsing as in this research normal browsing mode was used.

***Research Scholar**
Department of Advance Research
University of Technology
Jaipur (Raj.)

REFERENCES

[1] Ababneh, A., Awwad, M. A., & Al-Saleh, M. I. (2017, August). IMO forensics in Android and windows systems. In 2017 8th International Conference on Information, Intelligence, Systems & Applications (IISA) (pp. 1-6). IEEE.

[2] Al Mutawa, N., Al Awadhi, I., Baggili, I., & Marrington, A. (2011, December). Forensic artifacts of Facebook's instant messaging service. In 2011 International Conference for Internet Technology and Secured Transactions (pp. 771-776). IEEE.

[3] Al Mutawa, N., Baggili, I., & Marrington, A. (2012). Forensic analysis of social networking applications on mobile devices. Digital Investigation, 9, S24-S33.

[4] Al-Saleh, M. I., & Forihat, Y. A. (2013). Skype forensics in android devices. International Journal of Computer Applications, 78(7).

[5] Anglano, C. (2014). Forensic analysis of WhatsApp Messenger on Android smartphones. Digital Investigation, 11(3), 201-213.

[6] Cahyani, N. D. W., Ab Rahman, N. H., Glisson, W. B., & Choo, K. K. R. (2017). The role of mobile forensics in terrorism investigations involving the use of cloud storage service and communication apps. Mobile Networks and Applications, 22(2), 240-254.

[7] Chin, E., Felt, A. P., Greenwood, K., & Wagner, D. (2011, June). Analyzing inter-application communication in Android. In Proceedings of the 9th international conference on Mobile systems, applications, and services (pp. 239-252). ACM.

[8] Dodge Jr, R. C. (2008, January). Skype fingerprint. In Proceedings of the 41st Annual Hawaii International Conference on System Sciences (HICSS 2008) (pp. 484-484). IEEE.

[9] Ghafarian, A., & Wood, C. (2018, July). Forensics Data Recovery of Skype Communication from Physical Memory. In Science and Information Conference (pp. 995-1009). Springer, Cham.

[10] Kitsaki, T. I., Angelogianni, A., Ntantogian, C., & Xenakis, C. (2018, November). A forensic investigation of Android mobile applications. In Proceedings of the 22nd Pan-Hellenic Conference on Informatics (pp. 58-63). ACM.

[11] Mahajan, A., Dahiya, M. S., & Sanghvi, H. P. (2013). Forensic analysis of instant messenger applications on android devices. arXiv preprint arXiv:1304.4915.

[12] Majeed, A., & Saleem, S. (2017). Forensic Analysis of Social Media Apps in Windows

[13] 10. NUST Journal of Engineering Sciences, 10(1), 37-45.

[14] Norouzizadeh Dezfouli, F., Dehghantanha, A., Eterovic-Soric, B., & Choo, K. K. R. (2016). Investigating Social Networking applications on smartphones detecting Facebook, Twitter, LinkedIn and Google+ artefacts on Android and iOS platforms. Australian journal of forensic sciences, 48(4), 469-488.

[15] Ovens, K. M., & Morison, G. (2016). Forensic analysis of kik messenger on ios devices. Digital Investigation, 17, 40-52.

[16] Raji, M., Wimmer, H., & Haddad, R. J. (2018, April). Analyzing Data from an Android Smartphone while Comparing between Two Forensic Tools. In SoutheastCon 2018 (pp. 1-6). IEEE.

[17] Satrya, G. B., Daely, P. T., & Shin, S. Y. (2016, July). Android forensics analysis: Private chat on social messenger. In 2016 Eighth International Conference on Ubiquitous and Future Networks (ICUFN) (pp. 430-435). IEEE.

[18] Schrittwieser, S., Frühwirt, P., Kieseberg, P., Leithner, M., Mulazzani, M., Huber, M., & Weippl, E. R. (2012, February). Guess Who's Texting You? Evaluating the Security of Smartphone Messaging Applications. In NDSS.

[19] Sgaras, C., Kechadi, M. T., & Le-Khac, N. A. (2012). Forensics acquisition and analysis of instant messaging and VoIP applications. In Computational forensics (pp. 188-199). Springer, Cham.

[20] Simon, M., & Slay, J. (2010, February). Recovery of skype application activity data from physical memory. In 2010 International Conference on Availability, Reliability and Security (pp. 283-288). IEEE.

[21] Simpao, A. F., Lingappan, A. M., Ahumada, L. M., Rehman, M. A., & Gálvez, J. A. (2015). Perioperative smartphone apps and devices for patient-centered care. Journal of medical systems, 39(9), 102.

[22] Zhang, H., Chen, L., & Liu, Q. (2018, March). Digital Forensic Analysis of Instant Messaging Applications on Android Smartphones. In 2018 International Conference on Computing, Networking and Communications (ICNC) (pp. 647-651). IEEE.