MAC OSX: iMessage, Face Time, Apple Mail Application Forensics

[1]*Dr. DIGVIJAYSINH RATHOD*

[1]Assistant Professor, Institute of Forensic Science, Gujarat Forensic Sciences University Gandhinagar, Gujarat (India)

digvijay.rathod@gfsu.edu.in

ABSTRACT : *The days of an operating system avoiding attacks simply by not being Windows is long behind us. Attacks against Mac OSX and Linux have both increased considerably and cyber security is a necessity across the board for all operating systems—not just for Windows—to avoids the consequences of attack. Mac OSX obviously required unique methodology to investigate apple's systems. There are very few forensics tools and techniques related to Mac OSX are available in the market. In the research paper, potential artifacts are collected from the inbuilt application of the OSX such as Messages (chat application for Mac OSX) - iChat , VOIP application - FaceTime, Apple Mail, USB artifacts Logs analysis and Wireless network history. This detailed analysis carried with manual approaches only. The outcome of this research will serve to be a significant resource for law enforcement, computer forensic investigators, and the digital forensics research community.*

KEY WORDS: Mac OSX, Digital forensics, iChat, FaceTime, Apple mail, Log analysis, Apple, USB artifacts.

1. Introduction

The business appetite for Mac devices is growing. Between 2011 and 2014, Apple sold over three million commercial units in the US alone. It's now thought that Apple's share of desktop computers is around 17% and growing by the day [1]. In fact, research suggests that 96% of businesses now support Macs in the workplace [2]. While this accounts for a small minority when compared with Microsoft Windows, OS X has become the operating system of preference for many individuals. As a result, it cannot be ignored as a possible target during forensic investigation. The days of an operating system avoiding attacks simply by not being Windows is long behind us. Attacks against Mac OS X and Linux have both increased considerably in 2016 and cyber security is a necessity across the board for all operating systems—not just for Windows—to avoids the consequences of attack [3]. Mac OSX obviously required unique methodology to investigate apple's systems. There are very few forensics tools and techniques related to Mac OSX are available in the market. Digital devices such as computer, mobiles, embedded devices, network devices contain very crucial and sensitive information. So it is necessary to handle this in well-structured manner. Digital forensics more focuses on the data only. Data such as volatile data, stored data, informative raw data etc. can be easily tempered by itself or by human (whether it's intentionally or unintentionally). Once it gets tempered or loss, it is difficult to prove in the judiciary [4]. So as a Computer Forensic Investigator, one has to conduct their work properly subject to the procedures, law and judiciary [5]. The Digital forensic process has mainly four phases Acquisition, Identification, Evolution and Presentation. In Acquisition phase, evidence was acquired in acceptable manner with proper approval from authority. It is followed by Identification phase whereby the tasks to identify the digital components from the acquired evidence and converting it to the format understood by human. The Evaluation phase comprise of the task to determine whether the components identified in the previous phase, is indeed relevant to the case being investigated and can be considered as a legitimate evidence. In the final phase, Admission, the acquired & extracted evidence is presented in the court of law [6].

The aim and objective of the research paper is to identify the source of information to collect potential artifacts are collected from the inbuilt application of the OSX such as Messages (chat application for Mac OSX) - iChat , VOIP application - FaceTime, Apple Mail, USB artifacts, Photo application, Logs analysis, Console commands, Address book, Software update and install history and Wireless network history

The rest of the paper is organized as follows - the related research paper review is discussed in section II, artifacts analysis, recovery and configuration of experimental setup is discussed in section III. Forensics of iMessages (Chat Application for OSX), Facetime (A VOIP Application), Apple mail, USB artifacts, OSX log analysis and wireless network history discussed in section IV, V, VI, VII, VIII, IX and X respectively. The research paper is concluded with comments in section XI.

2. Literature survey

Philip Craiger, Paul K. Burke [7] - research paper focused more on the available artifacts from the system and user data. But it is necessary to recover the user deleted logs and history of the OSX Applications to analyze the potential artifacts. Rob Joyce, Judson Powers, and Frank Adelstein [6] - Number of OSX Application forensic has been mentioned in paper limits the some artifacts related to FaceTime deleted history, Private browsing history for the Safari.

There are number of research has been already carried out for MAC OSX Forensic. Most of the papers are focused on the artifacts locations. Log files, Database files, User data all are important in forensic analysis of the Mac. In parallel, one should have to analyze the detailed applications analysis such as iChat, mail , VOIP, photo and wireless network history etc.

3. Artifacts Analysis, Recovery and configuration

Mac OSX has number of inbuilt application for Office, system preferences, entertainment, communications, email clients and third party software [8] such as Apple Mail, iMesseges, FaceTime, iTunes, iCloud, Safari, Photos, Contacts, Calendar, Notes and KeyChain. Third party applications are available for Mac OSX [9] such as third party browsers (Chrome, Firefox), Office Applications (Microsoft Office), Team Viewer and Skype etc. Forensically these inbuilt and third party applications have significant importance. While applying forensic techniques, forensic examiner should considered network connections, console commands, logs of the applications, system preferences, hidden directories, folders and files, spotlight, deleted contents, diagnostic reports, crash reporter, shutdown logs, and software installation Logs to collect evidences related to cybercrime.

The configuration of laboratory to perform the forensics of Mac OSX is: Machine configuration for Mac OSX forensic is iMac (27-inch, Late 2009), Operating System El Capitan (10.11.3), Processor 3.06 GHz Intel Core 2 Duo , Memory 4 GB 1067 MHz DDR3, Storage 1 TB HDD and configuration of Yosemite Virtual Machine is Host Operating System Windows 7, Host Machine RAM: 16 GB, Allocated RAM: 12 GB, Host OS Processor: Intel i7 (3.40 GHz). Some other tools such as SQLite Browser, SQLite forensic Explorer, iHex (Hex Editor) used for forensics purpose.

Int the next section we discussed forensics of inbuilt and third party application.

4. Messages (Chat Application for OSX)

Messages also known as iMesseges is the popular instance messenger application for both iOS and MAC OSX. iMesseges works together in all apple devices having same Apple Id and also can be associated with mobile number [10]. The chat database file is available at path /Users/Mac/Library/Messages/chat.db and we used Sqlite browser to view the chat database (chat.db). The database contains attachments (figure 1) flag: value is 0 or 1, which means that the message contain any attachment or not. Message from (is_from_me) gives information about sender and receiver. Message Delivered flag is_delivered - 1(Delivered) / 0(Not delivered) : shows message has been delivered to recipients or not. Message read flag (is_read) : 1(Read) / 0(Not read) : show the status of message, read or not. Audio flag - is_played: 1(Played) / 0(Not played) : show that status of audio message , played or not.

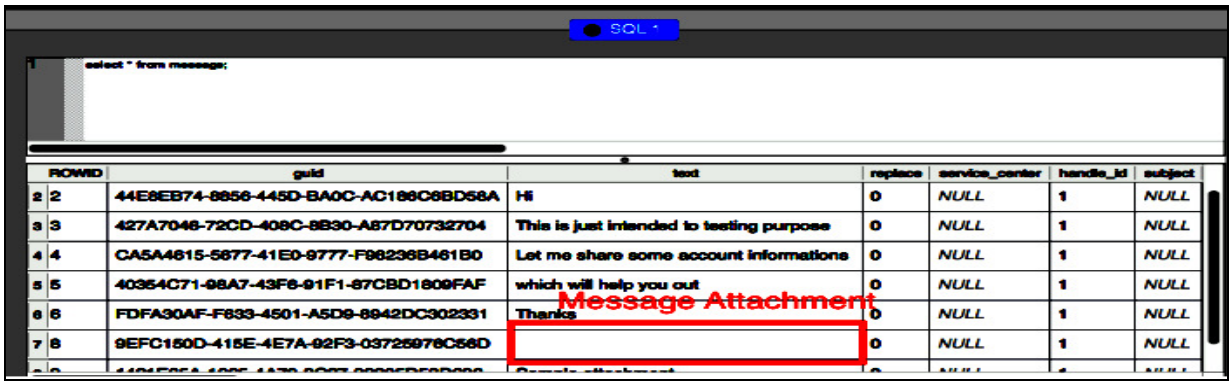

Figure 1 Attachment shows the blank row

The Attachments of the message can be found at location: /Users/Mac/Library/Messages/Attachments/0d/13/6D9A2CE4-CDDF-4E74-9581-1279E9BF2C18 <UniqueNumber-MayDiffersFromMachinetomachine>/ <Attachment_name> iChat file is automatically generated separately for each conversations. This file can be found from location: /Users/Mac/Library/Messages/Archive/<Date>/<prefix_ name>.ichat to collect evidence. Recovery of deleted messages is an important task that forensic examiner needs to perform. We intentionally deleted messages to discuss the procedure to recover the deleted messages. We used Sqlite browser to view that database file and we found that deleted messages is not available in the database file.

We used SQLite forensic explorer tool [11] to recover the deleted message. We noticed during the research that file size of the database file after deletion of messages will be same as before deletion. It shows that we can find

the deleted message from the spaces available within a same file and SQLite forensic explorer does same thing to recover deleted data. Recovered result shown in figure – 2.

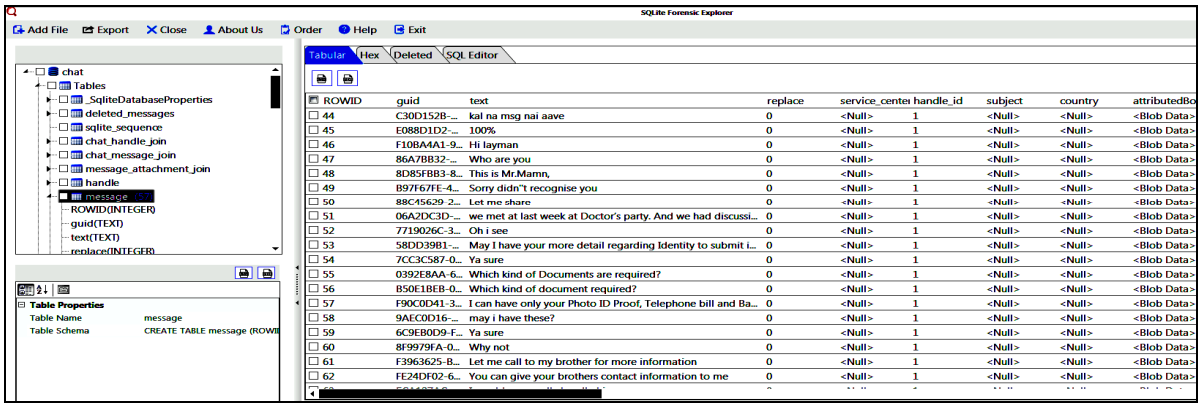

Figure 2 SQLIte Forensic Explorer DB File Recovered Result

5. FaceTime (VOIP Application)

FaceTime is an inbuilt utility for VOIP (Voice over IP) [12] Communication service. It provides videos and audio call utility to users. It is available in all apple devices including iPhones; iPads and all OSX configured computers. To investigate user's communication logs, forensic investigator needs to check out log files related to it. In the case of FaceTime analysis only one log file is generated at location:
/Users/Mac/Library/Logs/FaceTime/FaceTime.log
This log file can be opened in console logs utility of OSX as well as any text editors. It contains all internal logs; some of them are very useful and it needs to extract the important logs as artifacts like communication type (audio or video), Timestamps, Apple id and mobile numbers.
To analyze the important artifacts from the log file, we have developed Facetime_log_analysis.py command line python utility. This utility analyze the FaceTime log file recovered from the MAC machines hard drive and shows recently deleted call history (figure 3) from FaceTime Application.

```
**********   Received    **********
Call type    ====>       audio

Call from    ====>       +919662108081
Date         ====>       2016-02-06
Time         ====>       12:05:54
TimeStamp    ====>       +0530
**************************************
**********   Received    **********
Call type    ====>       audio

Call from    ====>       +919662108081
Date         ====>       2016-02-06
Time         ====>       12:09:52
TimeStamp    ====>       +0530
**************************************
**********   Received    **********
Call type    ====>       audio

Call from    ====>       +919662108081
Date         ====>       2016-02-06
Time         ====>       12:59:55
TimeStamp    ====>       +0530
```

Figure 3 Deleted History Recovered for the FaceTime

6. Apple Mail

Almost all OSX user uses Apple mail client. Number of evidences like emails, attachments, Apple notes (If synchronization to mail is enabled) can be found from it. The location of mail folder is: /Users/Mac/Library/<Mail>, location of all email messages is: /Users/Mac/Library/Mail/V3/4F5438F6-1CA9-4A68-ABF0-A7A71652B41C<Varies by Machine to machine>/[Gmail].mbox/All Mail.mbox/7B91AEB6-50E1-427E-B02C-D4EEBC1051A1/Data/Messages/ <name>.emlx. Separate folder for Inbox, Outbox, Sent items, Trace and all other user created folders are resides under the data directory itself. Location of the Email Attachments:/Users/Mac/Library/Mail/V3/4F5438F6-1CA9-4A68-ABF0A7A71652B41C/[Gmail].mbox/ AllMail.mbox/7B91AEB6-50E1-427E-B02C-D4EEBC1051A1/Data/Attachments/
As mentioned in the case of iMesseges, recovery of the data is very crucial and important factor in the process of investigation of digital artifacts. Email data and its header contains the artifacts such as senders and receivers IP Addresses, Application used to send the email, message id, Time stamps and other details contain by email headers. Unlike iMesseges, each email message stores separately in emlx file. When email from the Apple Mail user interface has been deleted then it automatically removes own entry from the list of emlx file. If investigator wants to recover the deleted email files then one needs to create an image of entire hard disk and has to look for the specific file format (emlx).

7. USB Artifacts

For the Mac OSX Forensic Investigator, analysis of USB Artifacts is equally important. It can be a difficult if user has logged out from the system or shutdown the system. To quick searching of USB

related artifacts like time stamp, USB id, Manufacture id, Product id and Product version, Investigator needs to open up the console window and search for USBMSC or manually go through /private/var/log/system.log. Collected USB artifacts shown in (figure 4)

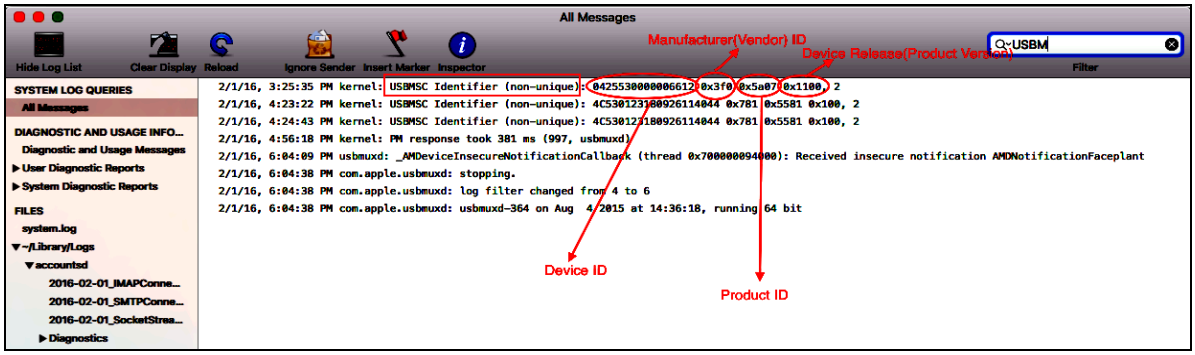

Figure 4 USB Artifacts

We wrote python script usb_history.py to fetch USB history from large system log file and result shown in figure 5.

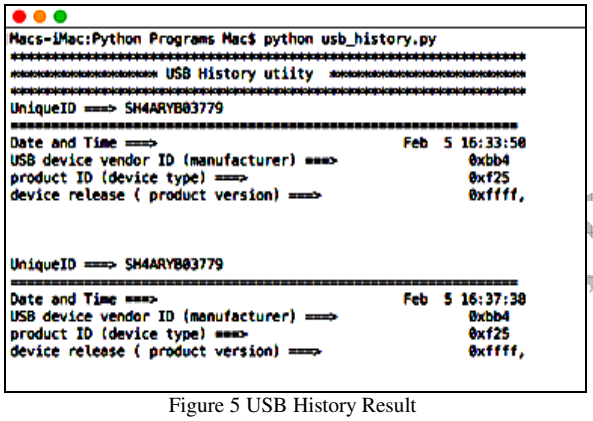

Figure 5 USB History Result

8. OSX Log Analysis

User and software activity logged in three different types of log files. The important things to notice over here are time stamps and message generated by the system. All events happened like volumes, network related activity, user activity, installation log, FaceTime call logs, USB logs, Bluetooth and many more can be analyzed from log files.

There are three types of logs e.g System log, User log and Application specific log file and location of the respected files are - System Logs : ! /private/var/log/ and !/Library/Logs; User logs: ~ /Users/Mac/ Library/Logs; Application specific log : ~ /Users/Mac/Library/Application Support , ! /Application

9. Log Format and Viewer

Log is an important location for evidences for investigator and logs are in the readable format. It is availablein standard Unix format : MMM DD HH:MM:SS Host Swervice: Message. This log can be analyzed by using OSX inbuilt applications like terminal.app or console.app (figure 6).

Figure 6 Console app to view logs in OSX

10. Wireless Network History

Wireless Network history with the SSID, Time, Security type and many other seventeen attributes are available. File Locations: /Library/Preferences/SystemConfiguration/ com.apple.airport. preferences.plist (figure 7) and /Library/Preferences/SystemConfiguration/ com.apple.network.identification.plist (figure 8)is an important for investigator

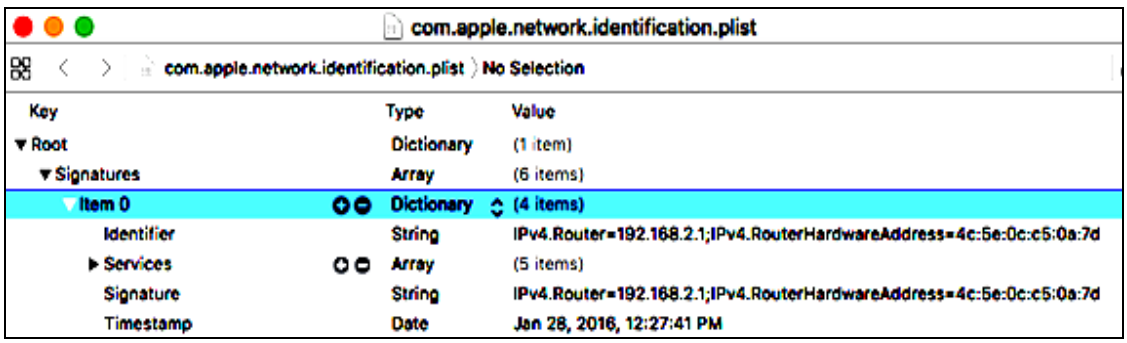

Figure 7 Wireless configuration artifacts

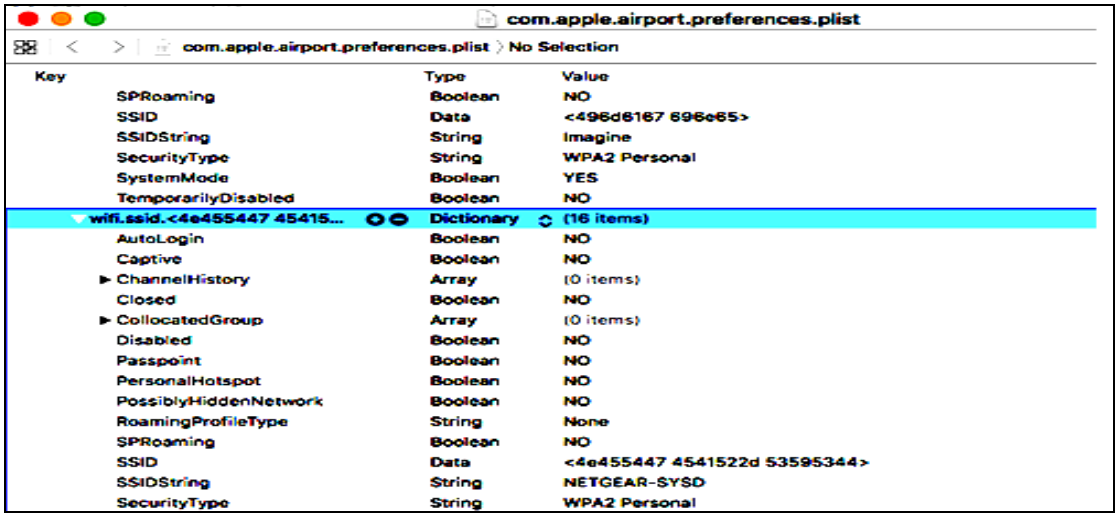

Figure 8 Wireless configuration artifacts

Above figures shows the plist files attributes such as, SSID String: NETGEAR-SYSD Security type: WPA2 Personal and Personal Hotspot: 0

11. Conclusion

Popularity of Mac OSX is continuously increasing day by day and cybercrime criminal uses or target the Mac OSX to commit the internet related crime. As file system and technology used in Mac OSX and Windows OS is different, those digital forensic techniques applicable to Window OS cannot be applicable Mac OSX. Safari web browser is proved by the Apple and most of the Mac users use safari to access internet. By considering this fact, web browser forensics is the most important for digital forensic examiners. As safari is the leading web browser for Mac OSX and in this research paper, we discussed various source of information such as Messages (Chat Application for OSX), Facetime (A Voip Application), Apple Mail , Usb Artifacts, OSX log analysis and wireless network history. The outcome of this research will serve to be a significant resource for law enforcement, computer forensic investigators, and the digital forensics research community.

References

[1.] Macs dent the enterprise, but not by much , By Esther Shein Contributing Writer, Computerworld, MAR 24, 2016, http://www.computerworld.com/article/3047597/apple-mac/macs-dent-the-enterprise-but-not-by-much.html

[2.] State of Mac Security 2016 Enterprise Mac management , Avecto Whitepaper https://www.avecto.com/media/1325/report-state-of-mac-security.pdf

[3.] Internet Security Threat Report VOLUME 21, APRIL 2016 , https://www.symantec.com/content/dam/symantec/docs/reports/istr-21-2016-en.pdf

[4.]

[5.] N Beebe, Advances in Digital Forensics V, Fifth IFIP WG 11.9 International Conference on Digital Forensics, Orlando, Florida, USA, January 26-28, 2009, Revised Selected Papers

[6.] Taylor, R. W., T.J. Caeti, K. Loper, E.J. Fritsch, and J. Liederbach (2006) Digital Crime and Digital Terrorism. Englewood Cliffs, NJ: Prentice Hall.

[7.] André Årnes, Anders Flaglien, Inger Marie Sunde, Ausra Dilijonaite, Jeff Hamm, Jens Petter Sandvik, Petter Bjelland, Katrin Franke and, Stefan Axelsson, Cybercrime Law, 2017, DOI: 10.1002/9781119262442.ch3

[8.] Philip Craiger, Paul K. Burke, "Mac Forensics : Mac OS X and the HFS+ File System," Department of Engineering Technology University of Central Florida.

[9.] Rob Joyce, Judson Powers, and Frank Adelstein. Mac Marshal: A Tool for Mac OS X Operating System and Application Forensics. In Proceedings of the 2008 Digital Forensic Research Workshop, 2008. URL: http://www.dfrws.org/2008/proceedings/p83-joyce_pres.pdf.

[10.] Survey: Macs, iPhones, and iPads Become the Apple of Enterprises' and Educational Organizations' Eye, http://www.jamfsoftware.com/resources/survey-macs-iphones-and-ipads-usagesoars/

[11.] Use Messages with your Mac, https://support.apple.com/en-in/HT202549

[12.] Sqlite Forensics Explorer, http://www.sqliteviewer.org/.

[13.] Use FaceTime with your iPhone, iPad, or iPod touch, https://support.apple.com/en-in/HT204380