OS X Artifact Analysis

Bhavana Maddu, P.V.R.D Prasad Rao

Abstract--- Recent day's apple computers have been trend to new generation. As the usage of apple products is increasing day by day, the market has increased more for apple devices. Apple computers has default MAC OS operating system. Even though mac is secure it also experiences cyber related crimes. The cybercrimes across the world has been increased more but there are limited open source forensics tools for MAC along with different operating systems to analyse the cybercrime. A Digital forensic investigator collects the atrifacts from the evidence and analyse using digital forensic techniques. Mac uses different methodologies for investigating a cybercrime. Artifacts plays key role in analyzing the crime by finding the traces. Artifacts are related to system, user and third party applications (chrome, Firefox, Skype, Team Viewer etc.) This research paper helps to find out the black listed software's that are installed in Mac computers.

Keywords: Mac OS X, OS X forensics, Mac forensics, Digital forensics, Artifact Analysis.

1. INTRODUCTION

MAC OS is the operating system that is only used on Apple systems. Earlier windows operating systems are the most used among MAC, Linux but now usage of MAC has increased. In recent years incidents related to Mac environment has increased due to the usage of MAC computers is continuously increased by individuals and business people. The Apple Macintosh (or Mac) was first introduced to the public in 1984. In 2001 March, a new version of Mac OS has released by Apple which is called Mac OS X here X means 10. It has been marketed as Mac OS X till 2012 then it is marketed as OS X till 2016 and later it is marketed as macOS. It is a UNIX'S based operating system[1]. Apple has named their operating systems after big cats until Mac OS 10.8 MOUNTAIN LION and from OS X 10.9 mavericks it started naming after places in California. Even the operating system is more advanced than earlier versions, Apple software has maintained same ease-of-use for people.

1.1 Comparison between Mac, Windows and Linux[2]

Features	Mac	Windows	Linux
File systems	APFS	NTFS	EXT3
Registry	Mac stores all the application information in plist files.	Windows registry is a master database stores settings and all the users related information with passwords.	Linux does not have specific registry. It stores all the application settings under different user in same hierarchy.
Security	Mac can only be installed on Apple computers. So, it has more security.	It is most used system. So, Windows systems are more vulnerable to attacks.	Linux is an open source operating system so, it less vulnerable than windows.
Compatibility	Limited applications are compatible to Mac OS.	Compatible with different types of applications.	You can program the s/w because it is open source.
GUI	Graphical designers are more attracted because of their GUI.	Windows is user friendly.	Needs more computer knowledge in order to work them.
Cost	Apple devices are more costly than windows.	Windows devices are less costly than Mac.	Linux is an open source operating system.

Table 1 Comparison

1.2 Importance of Mac computers

Mac OS does not have any serial keys you can install the OS any number of times on the systems. Mac computers are more secure than windows because Mac is UNIX based operating system. Due to this Mac OS is less prone to attacks than compared to windows. Apple itself develops both hardware and software so these are less prone to system crashes compared to Windows. Apple Company takes care of their computers look and internals are constructed beautifully. Apple releases its new version for free to download and install for the supported Macs. It has pre-installed software's like FaceTime, Numbers, iMovies, pages, GarageBand etc[3]. Mac computers have an App store which contains different Apps for free and paid. Every download from App Store requires an admin authenticity to allow the application to download. Mac provide different features like Time Machine, File Vault2 and many others. Time Machine is used to take backup of their system all you need to do is connect a drive and turn on Time Machine. Whenever the drive is accessible it automatically takes the backup of the system. File Vault2 which is used to encrypt the whole disk to provide security.

1.3 Phases of Digital Forensics

Different methodologies are needed for digital forensic investigator to investigate the case related to Mac. The digital forensics process has five phases to investigate the case. They are Identification & Acquiring, Preservation, Analysis, Reporting and Presentation[4].

Identification & Acquiring: The digital forensic examiner who is present at the cybercrime scene should be well trained to identify the evidence, where it is stored, how

Revised Manuscript Received on March 10, 2019.

Bhavana Maddu, M.Tech Student, Department of Computer Science and Engineering, Koneru Lakshmaiah Educational Foundation, Vaddeswaram, Guntur District. (bhavana.kdy@gmail.com)

Dr. P.V.R.D Prasad Rao, Professor, Department of Computer Science and Engineering, Koneru Lakshmaiah Educational Foundation, Vaddeswaram, Guntur District. (pvrdprasad@kluniversity.in)

data is stored in the evidence and what operating system is used. The examiner need to identify the appropriate recovery methodologies and tools to be used to extract the data. The examiner needs to acquire the evidence properly in the presence of authority and conduct imaging or cloning to the evidence.

Figure 1 Digital Forensics Phases

Preservation: The evidence should be preserved by ensuring its integrity and chain of custody. All the steps should be documented while capturing the data and any changes made to evidence also be documented. At the end integrity of data should be proved in the court of law.

Analysing: In this phase the data present in the evidence is examined, processed, interpreted and the deleted data is recovered. It produces a final conclusion like how the incident has occurred based on the evidence that has found at the crime scene.

Reporting: Report means producing how the crime has occurred in a document format. This document contains the process used to analyse, tools used to recover, chain of custody etc. The report should be in simple and understandable manner.

Presentation: The evidence and the report should be produced in the court of law in an acceptable manner. The judge should be able to relate the original crime and the report that is submitted to the court and be able to punish the offender.

2. LITERATURE WORK

Dr Digvijaysinh Rathod – research paper has mainly focused on the safari artifacts like browser history, recent web search, and last sessions.

Philip Craiger, Paul K. Burke - research paper focused more on the available artifacts from the system and user data. But the user deleted logs and history are necessary to recover.

Dr Digvijaysinh Rathod- in this research paper he mainly focused on the potential artifacts log analysis, Apple Mail, FaceTime etc.

Which are minimal for forensic investigation. So we need to focus on the installation of software's, system log, Log analysis, Database files, user interactions and many other things to check the system is secure or not.

3. ARTIFACT

Artifacts are the locations within a computer system which holds important information related to the activities performed by the user on the computer. Artifacts provides digital evidence for the cybercrime happened. Artifacts locations and information varies from different operating systems and versions[5]. The digital forensic investigator need to identify and process these artifacts to prove the cybercrime. These Artifacts plays a major role in identifying the traces and root cause of a cybercrime.

4. EXPERIMENTAL SETUP

The laboratory setup that is used for this forensic analysis is MacBook Pro with operating system macOS High Sierra (10.13.4) , Processor 2.6 GHz intel core i5, Memory 8 GB 1600 MHz DDR3, Storage 256 GB. The application that is used for this analysis is Xcode version 9.4.1, TextEdit[1].

5. METHODOLOGY & RESULTS:

Digital Forensics mainly focuses on three stuffs like data theft, malware infection, and deleted data whenever the cybercrime has occurred. Data theft can be occurred by USB, mail attachments etc. if a data theft is occurred then the digital forensic investigator mainly focuses on the USB logs, mail logs to identify from where the data has been theft. If malware has infected to system then the digital forensic investigator mainly focuses on Activity monitor and by commands. If the data is deleted from system the digital forensic investigator mainly focuses on trash, Time Machine backup, tools.

5.1 Scenario

The MNC firm called WebEx which works in the area of iOS application development. IT audit team found certain black listed software's & devices are installed in their workstations. The legal team conduct a raid & seize the potential evidence from the premises. In response to the complaint of data theft, forensic investigation file of one of the machine was given to the accused was seized. Now the task of forensic analysts to find out the potential artefacts to prove the scenario.

5.1.1 System Logs

System log files main folder

System log file folder contains all the log files related to the user activities[6]. This is the path ***/var/log*** which displays all the log files.

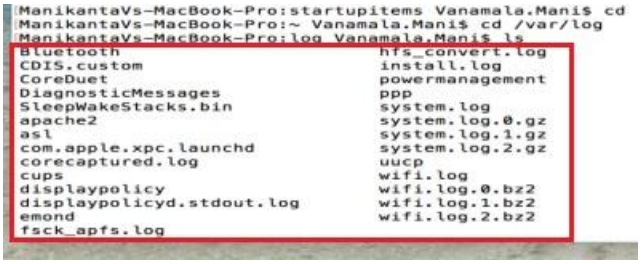


Figure 2 system log files folder

Audit log:

The audit logs gives information related to security, user login/logoff data. These logs record user log in and log off data. These logs will hold information about when a user is created or removed from a system. These logs are identified by StartTime. Endtime in the format:

YYYYMMDDHHMMSS.YYYYMMDDHHMMSS. Each file is known as a trail file.

This is the path */**var/audit*** which displays audit logs.

.crash_recovery – This is the recovered Log file which is not attained due to crash. This audit file has Audit recovery record as it was the first record.

.current – it displays the current active trail file.

.not_terminated – It displays the Active audit trail file and audit file was not terminated properly.

```
sh-3.2# ls -la
total 1920
drwx------  25 root  wheel     850 Dec 31  2000 .
drwxr-xr-x  29 root  wheel     986 Jul 20  2011 ..
-r--r-----   1 root  wheel   20783 Apr 21 19:46 20010101000041.not_terminated
-r--r-----   1 root  wheel   36889 Jul 20  2011 20110720234522.20110721005114
-r--r-----   1 root  wheel   49461 Jul 23  2011 20110721005225.20110723185309
-r--r-----   1 root  wheel    3329 Jul 23  2011 20110723190438.20110723233706
-r--r-----   1 root  wheel   68052 Jul 29  2011 20110723235732.crash_recovery
-r--r-----   1 root  wheel   77490 Aug 17  2011 20110808154524.20110817130302
-r--r-----   1 root  wheel    9159 Aug 17  2011 20110817130504.20110817135301
-r--r-----   1 root  wheel   34906 Aug 21  2011 20110817135326.20110821160014
-r--r-----   1 root  wheel   36105 Aug 30  2011 20110821160203.crash_recovery
-r--r-----   1 root  wheel   16150 Sep  9  2011 20110903075028.20110910000317
-r--r-----   1 root  wheel  114098 Oct 13  2011 20110910000443.20111013121941
-r--r-----   1 root  wheel   57344 Nov 11 17:42 20111013211334.crash_recovery
-r--r-----   1 root  wheel   52442 Dec 19 20:06 20111112184257.20111220010601
-r--r-----   1 root  wheel   47358 Jan 14 10:03 20111220010712.20120114150319
-r--r-----   1 root  wheel   88328 Feb 15 20:15 20120114150406.20120216011539
-r--r-----   1 root  wheel    2887 Feb 15 20:32 20120216012756.crash_recovery
-r--r-----   1 root  wheel   44673 Feb 17 23:25 20120216123741.20120218042511
-r--r-----   1 root  wheel   48692 Mar 16 19:13 20120218042553.crash_recovery
-r--r-----   1 root  wheel   27454 Mar 24 09:52 20120317000535.20120324135232
-r--r-----   1 root  wheel   54550 Apr  9 18:57 20120324135529.crash_recovery
-r--r-----   1 root  wheel    2741 Apr  9 19:02 20120409230117.crash_recovery
-r--r-----   1 root  wheel   49737 Apr 20 08:30 20120409230908.crash_recovery
lrwxr-xr-x   1 root  wheel      40 Dec 31  2000 current -> /var/audit/20010101
```

Figure 3 Audit Log

Apple Unified Logs

Apple Unified logs are stored in directories

The files that are stored in this ***/var/db/diagnostics*** directory are saved with .tracev3. To open these files we need different utility that is called log[12]. These are binary files which contain others files as well as log.tracev3 files.

```
total 197584
drwxr-xr-x   2 root  wheel       68 Sep 27 19:03 Events
drwxr-xr-x  31 root  wheel     1054 Nov 13 19:44 FaultsAndErrors
drwxr-xr-x   2 root  wheel       68 Sep 27 19:03 Oversize
drwxr-xr-x   2 root  wheel       68 Sep 27 19:03 SpecialHandling
drwxr-xr-x   2 root  wheel       68 Sep 27 19:03 StateDumps
drwxr-xr-x  16 root  wheel      544 Nov 13 19:44 TTL
-rw-r-----   1 root  wheel  10586976 Nov  6 06:08 logdata.Persistent.20161106T045449.tracev3
-rw-r-----   1 root  wheel  10549904 Nov  6 17:03 logdata.Persistent.20161106T112151.tracev3
-rw-r-----   1 root  wheel   2331488 Nov  6 19:17 logdata.Persistent.20161106T221230.tracev3
-rw-r-----   1 root  wheel   6667976 Nov  7 19:18 logdata.Persistent.20161107T002825.tracev3
-rw-r-----   1 root  wheel   3605360 Nov  7 21:56 logdata.Persistent.20161108T003223.tracev3
-rw-r-----   1 root  wheel  10586760 Nov  9 23:11 logdata.Persistent.20161109T001242.tracev3
-rw-r-----   1 root  wheel   3068952 Nov 10 20:57 logdata.Persistent.20161110T051134.tracev3
-rw-r-----   1 root  wheel  10587272 Nov 11 17:55 logdata.Persistent.20161111T023347.tracev3
-rw-r-----   1 root  wheel   3177928 Nov 11 20:21 logdata.Persistent.20161111T230548.tracev3
-rw-r-----   1 root  wheel  10573896 Nov 12 12:10 logdata.Persistent.20161112T012527.tracev3
-rw-r-----   1 root  wheel   5564952 Nov 12 19:32 logdata.Persistent.20161112T185153.tracev3
-rw-r-----   1 root  wheel  10602712 Nov 13 11:58 logdata.Persistent.20161113T003205.tracev3
-rw-r-----   1 root  wheel   9023072 Nov 13 19:37 logdata.Persistent.20161113T170327.tracev3
-rw-r-----   1 root  wheel    520040 Nov 13 19:59 logdata.Persistent.20161114T004307.tracev3
-rw-r-----   1 root  wheel   1212268 Nov 13 19:43 logdata.statistics.0.txt
```

Figure 4 Diagnostics Files

The files that are stored in ***/var/db/uuidtext*** directory contains main.tracev3 log file references.

```
drwxr-xr-x  12 root  wheel   384 Jul 25 17:51 00
drwxr-xr-x  14 root  wheel   448 Jul 25 17:51 01
drwxr-xr-x   8 root  wheel   256 Oct 30 11:56 03
drwxr-xr-x  15 root  wheel   480 Nov  6 11:34 03
drwxr-xr-x  11 root  wheel   352 Oct 27 23:09 04
drwxr-xr-x  15 root  wheel   480 Oct 30 11:56 05
drwxr-xr-x   9 root  wheel   288 Oct 30 15:56 06
drwxr-xr-x  16 root  wheel   512 Jul 27 14:47 07
drwxr-xr-x  18 root  wheel   576 Oct 30 15:56 08
drwxr-xr-x  10 root  wheel   320 Jul  2 11:15 09
drwxr-xr-x  10 root  wheel   320 Oct 30 11:30 0A
drwxr-xr-x  19 root  wheel   608 Oct 30 11:56 0B
drwxr-xr-x  10 root  wheel   320 Nov  5 12:35 0C
drwxr-xr-x  12 root  wheel   384 Jul 25 15:25 0D
drwxr-xr-x  15 root  wheel   480 Jan  1  2018 0E
drwxr-xr-x  12 root  wheel   384 Oct 30 11:56 0F
drwxr-xr-x  12 root  wheel   384 Jul 11 17:21 10
drwxr-xr-x  18 root  wheel   576 Oct 30 15:56 11
drwxr-xr-x  12 root  wheel   384 Oct 27 23:10 12
drwxr-xr-x  13 root  wheel   416 Oct 30 15:56 13
drwxr-xr-x  13 root  wheel   416 Nov  5 12:06 14
```

Figure 5 uuidtext

Software Installation

The installhistory.plist file contains installation history of software's and updates, it also displays date and time of the software installation and updates

This is the Path: ***/library/receipts/installhistory.plist*** which displays all the installations.

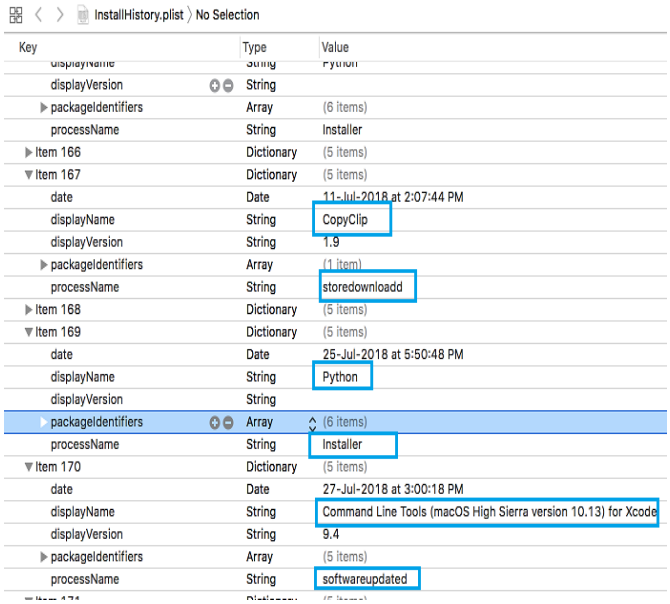


Figure 6 Install history plist

5.1.2 System preferences

System preferences files:

System preferences contains all preferences settings .plist files. That should remain same regardless of which user is currently logged in.

This is the path ***/library/preferences*** which displays all the .plist files.

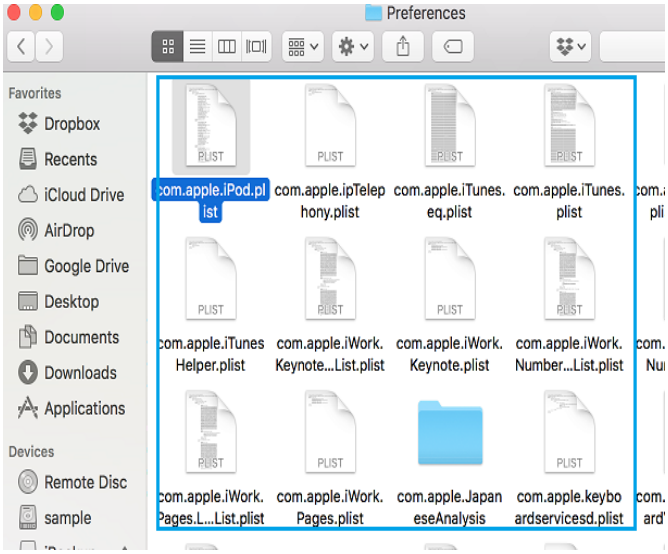


Figure 7 Preference plists

Global preferences:

The glolbalpreferences.plist files holds information related to local time zone, geographical coordinates, etc.

This is the path ***/library/preferences/.globalpreferences.plist*** which displays the preferences.

com.apple.TimeZonePref.Last_...	Array	(10 items)
Item 0	String	16.48333
Item 1	String	80.6
Item 2	String	0
Item 3	String	Asia/Kolkata
Item 4	String	IN
Item 5	String	Tādepalle
Item 6	String	India
Item 7	String	Tādepalle
Item 8	String	India
Item 9	String	DEPRECATED IN 10.6
AppleTextDirection	Number	0

Figure 8 Global Preferences plist

Login window info:

This loginwindow.plist file shows the users last logged in details like username, it also displays date and time when the user logged in.

This is the path ***/library/preferences/com.apple.loginwindow.plist*** which displays the last logged in user details.

com.apple.loginwindow.plist 〉 No Selection

Key	Type	Value
Root	Dictionary	(6 items)
OptimizerLastRunForSystem	Number	16,86,25,152
GuestEnabled	Boolean	NO
lastUserName	String	Vanamala.Mani
OptimizerLastRunForBuild	Number	3,59,20,096
lastUser	String	loggedIn
SHOWFULLNAME	Boolean	NO

Figure 9 Loginwindow plist

Bluetooth preferences:

Bluetooth preferences holds information about deceives that are connected to the system using Bluetooth. It givens information like device name, last updated etc.

This is the path ***/library/preferences/com.apple.bluetooth.plist*** which displays all the paired Bluetooth devices.

com.apple.Bluetooth.plist

com.apple.Bluetooth.plist 〉 No Selection

Key	Type	Value
UplaodStatus	Number	2
CoreBluetoothCache	Dictionary	(0 items)
PersistentPorts	Dictionary	(3 items)
PANDevices	Array	(0 items)
BluetoothStats	Dictionary	(11 items)
DeviceCache	Dictionary	(10 items)
6c-ab-31-3f-60-25	Dictionary	(17 items)
6c-e9-07-1d-0e-02	Dictionary	(4 items)
c8-3d-d4-66-21-3a	Dictionary	(4 items)
98-e0-d9-94-44-54	Dictionary	(19 items)
Manufacturer	Number	15
ClassOfDevice	Number	36,70,284
LastServicesUpdate	Date	30-May-2015 at 9:42:10 PM
LastInquiryUpdate	Date	30-May-2015 at 9:42:05 PM
Name	String	Desiraju's MacBook Air
ModelIdentifier	String	MacBookAir7,2
LMPSubversion	Number	16,741
PageScanPeriod	Number	0
LastNameUpdate	Date	30-May-2015 at 9:42:02 PM
Services	Data	<040b7374 7265616d 74797065 6481e803 84014084 84
0783 - Is Portable	Number	1
ExtendedFeaturesPage1	Data	<00000000 00000007>
LMPVersion	Number	6
PageScanRepetitionMode	Number	1

Figure 10 Bluetooth preference plist

5.1.3 Network Artifacts

This plist file holds information related to the network like known networks that the Mac system has connected.it displays the last connected date, name of the Wi-Fi, ID of the particular device etc.

This is the path ***/Library/Preferences/SystemConfiguration/com.apple.airport.preferences.plist*** which displays the network information.

wifi.ssid.<42687051 2d4d5451 7...	Dictionary	(20 items)
wifi.ssid.<43686172 616e2043 6...	Dictionary	(20 items)
Captive	Boolean	NO
CaptiveBypass	Boolean	NO
ChannelHistory	Array	(4 items)
Closed	Boolean	NO
CollocatedGroup	Array	(14 items)
Disabled	Boolean	NO
LastConnected	Date	27-Dec-2016 at 11:35:02 AM
NetworkWasCaptive	Boolean	NO
Passpoint	Boolean	NO
PersonalHotspot	Boolean	NO
PossiblyHiddenNetwork	Boolean	NO
RoamingProfileType	String	Single
SPRoaming	Boolean	NO
SSID	Data	<43686172 616e2043 68657272 79>
SSIDString	String	Charan Cherry
SecurityType	String	Open
ShareMode	Number	1

Figure 11 network preference plist

Published By:
Blue Eyes Intelligence Engineering
& Sciences Publication

5.1.4 USER ARTIFACTS

Login items:

Loginitems.Plist file has the information related to the applications automatically start when the user is logged in to user account. The accounts maybe like iTunes, Google Drive, Dropbox etc.

This is the Path ***%%users.homedir%%/library/preferences/com.apple.loginitems.plist*** where you can see all the logged in accounts of the user.

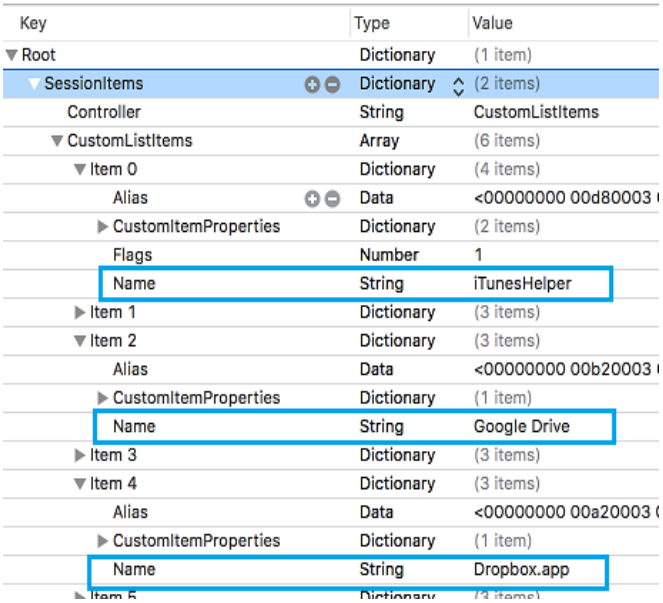


Figure 12 Login Items

5.1.5 Users directories/Users

To know how many users are there for a particular system. This is the path ***/Users/**** which displays the available users. For GUI go to users.

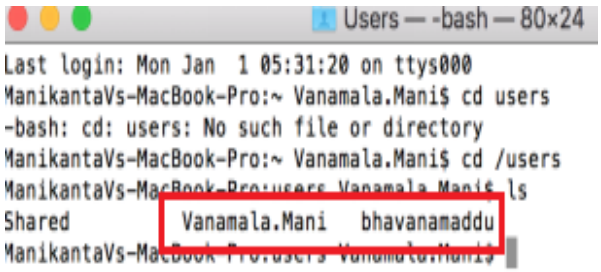


Figure 13 users command line

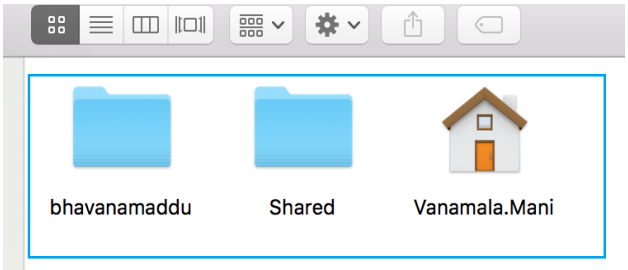


Figure 14 users GUI

5.1.6 Downloads Directory

This is the directory which stores all downloads that are done by the user using different browsers and from the Apple Mail app which is default for the mac systems.

This is the path ***%%users.homedir%%/Downloads/**** which displays all downloads available in the download directory.

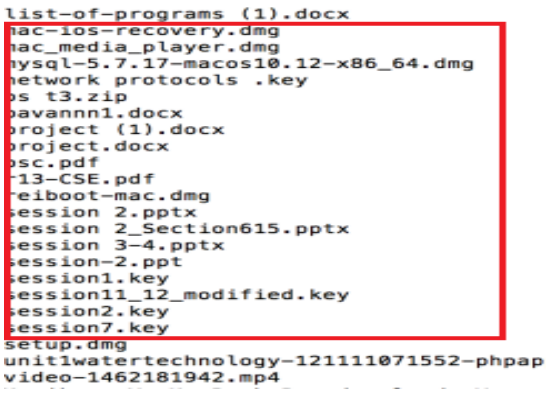


Figure 15 Downloads Directory

5.1.7 Documents Directory

The Document directory stores all the documents created by user like pages, numbers, and keynotes.

This is the path ***%%users.homedir%%/Documents/**** where it displays all the available documents that are stored in the document directory.

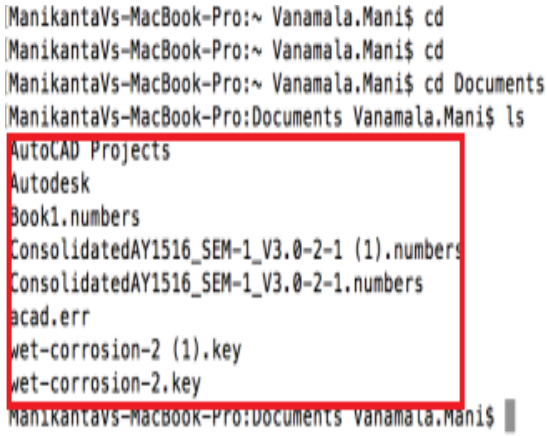


Figure 16 Documents Directory by command

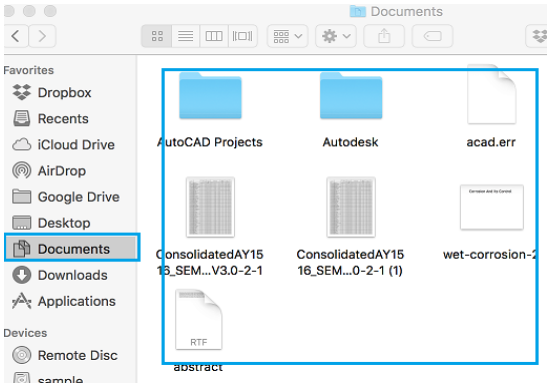


Figure 17 Documents Directory GUI

5.1.8 Desktop Directory:

Desktop directory contains folders, photos and different applications which are stored by user on the desktop.

This is the path ***%%users.homedir%%/Desktop/**** where it display's all the available folders and applications etc.

```
esfs-Mac:~ esf$ cd Desktop/
esfs-Mac:Desktop esf$ ls
Screen Shot 2018-06-21 at 4.25.45 PM.png
chrome extensions.png
cookie.png
cookie1.png
cookie2.png
ss.jpeg
esfs-Mac:Desktop esf$
```

Figure 18 Desktop Directory by command

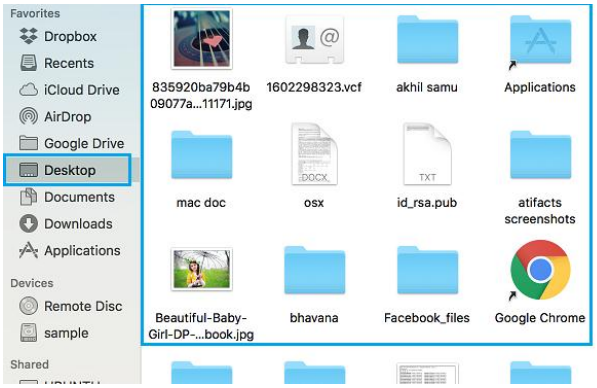
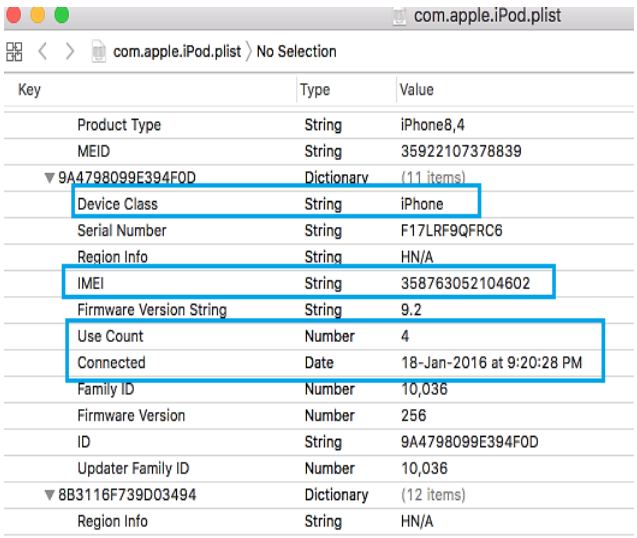


Figure 19 Desktop Directory GUI

5.1.9 Attached iDevices:

Attached iDevices holds the information about the iDevices that are connected to the particular Mac system. It gives information about IMEI number, time, use count, device class.

This is the path ***%%users.homedir%%/Library/Preferences/com.apple.iPod.plist*** which displays all the idevices that are connected to the Mac system.



Key	Type	Value
Product Type	String	iPhone8,4
MEID	String	35922107378839
▼9A4798099E394F0D	Dictionary	(11 items)
Device Class	String	iPhone
Serial Number	String	F17LRF9QFRC6
Region Info	String	HN/A
IMEI	String	358763052104602
Firmware Version String	String	9.2
Use Count	Number	4
Connected	Date	18-Jan-2016 at 9:20:28 PM
Family ID	Number	10,036
Firmware Version	Number	256
ID	String	9A4798099E394F0D
Updater Family ID	Number	10,036
▼8B3116F739D03494	Dictionary	(12 items)
Region Info	String	HN/A

Figure 20 Attached iDevices

5.1.10 Time Machine info:

Time Machine is used to take backup of their system all you need to do is connect a drive and turn on Time Machine. Whenever the drive is accessible it automatically takes the backup of the system backup info. It also stores these backups.

This is the path ***/library/preferences/com.apple.timemachine.plist*** which displays the backup if any backup is taken.

5.1.11 System info MISC

Current time zone:

This holds information related to the time zone of a particular system. This is the path ***/usr/lib/cron/jobs*** which displays the information related to current time zone of the Mac system.

6. ACKNOWLEDGEMENT

This work is supported by the Department of Science and Technology, India through the fund sanctioned for improvement of Science & Technology infrastructure, at department of CSE, K.L University, by order number SR/FST/ESI-332/2013.

7. CONCLUSION

According to our research the digit of security threats on Mac computers has been increasing from the last decade, especially linked with malware and intruders. Though, the techniques & research to deal with these incidents have been minimal. Mac has certain limitations that vary from one version to another version. These forensically sound artifacts are used to know whether the system has any malicious content or activities performed by the user. This paper mainly focuses on the persistent artifacts. This paper recognized where the potential evidences are stored and how forensic investigator can pull that juicy information from the Mac computers.

8. REFERENCES

1. Digvijaysinh rathod "MAC OSX: iMessage, Face Time, Apple Mail Application Forensics " journal of information, knowledge and research in computer engineering issn: 0975 – 6760| nov 16 to oct 17| volume – 04, issue – 02
2. Ali Zar, Shakeel Tufail, Saad Ali, Rabbiya "comparison of windows linux and mac os" slideshare
3. ONLINE "10 REASONS TO GET AN APPLE MAC INSTEAD OF A WINDOWS PC" SLIDESHOW ON BUSINESSINSIDER
4. Karen Ryder "Computer Forensics - We've Had an Incident, Who Do We Get to Investigate" SANS Institute InfoSec Reading Room, 2018
5. Bhanu Prakash Kondapally "Forensically Important Artifacts in Windows Operating systems" security community.
6. Macworld Staff "Display info in the login window" article macworld
7. Jaron Bradley "OS X incident Response: Scripting and analysis" Text Book
8. "Mac OS" Article Encyclopaedia Britannica

Published By:
Blue Eyes Intelligence Engineering
& Sciences Publication

9. Paul K. Burke “Mac Forensics: Mac OS X and the HFS+ File System “ semanticsscholar
10. Hai-Cheng Chu “Testifying the digital artifacts for Line application program under MAC OS X from the aspects of witness experts” Wiley online library.
11. Charles B.Leopard, Neil C.Rowe and Michael R.Mccarrin “Testing Memory Forensics Tools For the Macintosh Os X operating system” Journal of Doigital Forensics Security and Law.
12. "New macOS Sierra (10.12) Forensic Artifacts – Introducing Unified Logging" Blog mac4n6
13. Sarah Edwards "Reading Mac BSM Audit Logs" wordpress
14. Eby Prasad, S Dija” Towards Live Forensics Acquisition and analysis of MAC Os Systems” IEEE.
15. Philp Craiger, Paul Burke “Mac OS X Forenscis” Text Book
16. Top of Form
17. Bottom of Form