MAC OS X (Macintosh Operating System)

Md. Zahid Hasan Juel

North South University
zahid.juel@northsouth.edu

***Abstract* - Market share of the Apple computers are continuously increasing day by day and Apple provides an OSX as a default operating system in their computers. The time has already arrived when digital forensic examiner needs sound and efficient digital forensic techniques for Mac OSX to collect evidences related cybercrime. The information source for artifacts may be application such as Apple Mail, iMesseges, FaceTime or third party application such as third party browsers (chrome, firefox), office applications (Microsoft office), Team Viewer and Skype. Among these mentioned sources, browser contains the very potential information. In the research paper, potential artifacts are collected for Safari browser using digital forensics of plist files, browsing history, recovery of deleted history, bookmarks, downloads, last session, top sites and user notification. The outcome of this research will serve to be a significant resource for law enforcement, computer forensic investigators, and the digital forensics research community.**

***Index Terms*—Mac OSX, safari browser, digital forensics, artifacts, Apple.**

I. INTRODUCTION

For years, the Windows OS has been the mainstay of enterprise computing, a common fixture in an ever-changing technology landscape. Though Windows continues to dominate the enterprise market, Apple is taking bigger bites out of its market share as the OS X ecosystem becomes an increasingly popular business choice [2]. 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 [3]. In fact, research suggests that 96% of businesses now support Macs in the workplace [2]. The increasing popularity of Apple Macintosh hardware, particularly that using Intel x86-compatible processors, provides new challenges and data gathering opportunities for forensic examiners [1]. 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 [5]. 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. The aim and objective of the research paper is to identify the source of information to collect artifacts with the various tool and techniques which will definitely help the investigator to analyze the real time case to
Mac OSX.

The rest of the paper is organized as follows - the related research paper review is discussed in section II, digital forensic process and configuration of laboratory setup is discussed in section III and artifacts analysis and recovery related to safari browser is discussed in section IV. Section V discussed about private browsing traces and section VI discussed about other source of information to

extract artifacts. The research paper is concluded with comments in section X.

II. 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 [1] - 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 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, Log analysis, and deleted data recovery from the local database file. The research paper is more focused on the Mac Applications database and log analysis for the potential artifacts like FaceTime log recovery, iMessages, Private Browsing artifacts from Safari Browser and number of other artifacts and its location changed in recent version of the OS X.

III. PROCESS AND CONFIGURATION OF SETUP:

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 [6]. So as a Computer Forensic Investigator, one has to conduct their work properly subject to the procedures, law and judiciary. 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.

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.

IV. MAC OS X SAFARI BROWSER

Safari is a web browser developed by Apple and it contains the very potential information related to cybercrime. it is very important for the digital forensic examiner to know the various tools and techniques to retrieve or recover evidences related to cybercrime. Following section discuss various source of information with forensics techniques to extract important evidences.

A. ANALYSIS OF PLIST

FILE Property list (plist) file stores the user and application preference information and application's session, user's information and many more artifacts depending upon the type and usage of the application. In case of safari browser, plist file stored at given location. :

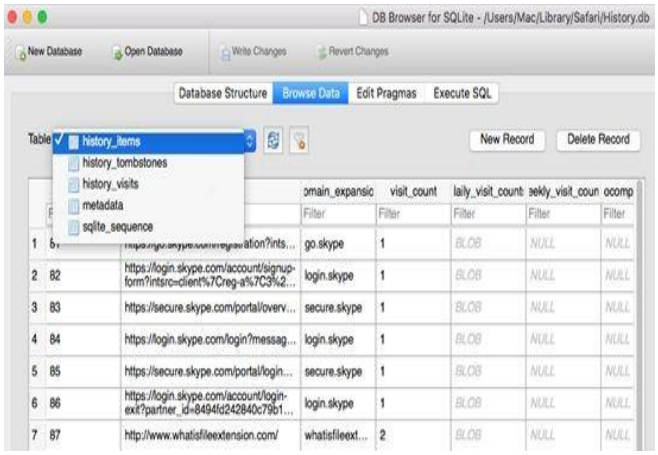
/Users/Mac/Library/Preferences/com.apple.Safari.plist

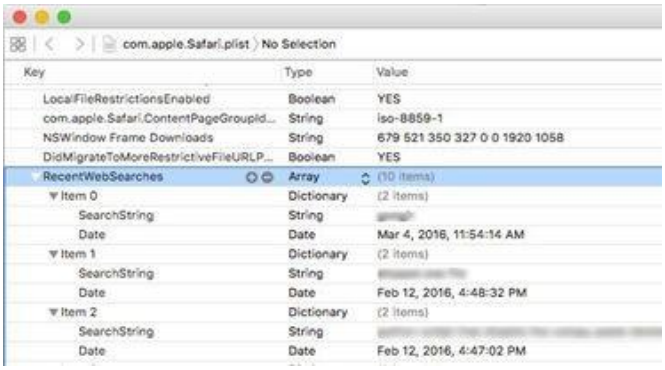
B. RECENT WEB SEARCH

Web searches reveal the information about the user mentality, what suspect want, what are the key words and behavior. Plist file contains the number of attributes and its value. Figure 1 shows the items recently searched with timestamp

C. BROWSING HISTORY

Browsing history stores in the SQLite database





(figure 2) format at given location: /Users/Mac/Library/Safari/History.db History.db file stores the number of artifacts in the different table names withindatabase file.

Figure 1 Recent Web Searches

Figure 2 List of table in Safari

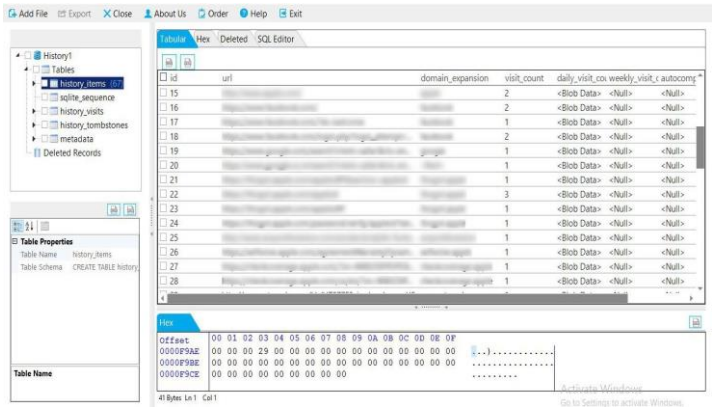
history database file

D. DELETED HISTORY RECOVERY

Safari stores browsing history in SQLite file format. History files stores at the location /Users/Mac/Library/Safari as a History.db file name. This file will play an important role to recover the history deleted by the suspect. Using Sqlite forensic explorer tool, (http://www.acquireforensics.com/products/sqlite-forensic-e xplorer/) swe can recover the history. Figure 3 and 4 shows the recovered database tables History_visits and history_items. Here time format used by OSX to stored data is UNIX Standard time format.

Figure 3. History items

V. PRIVATE BROWSING TRACES



Private browsing data will not be stored in the computer. As an investigator we can succeed to analyze the private browsing history of the Safari browser. The method mention below is not supported to latest Mac OS 10.11.X. It supports up to version 10.10.X. Safari manages the database named WebpageIcons.db. We can get the history of the private browsing (figure 5) from this file. This file is not actually intended for the private history but due to Safari's bug it can help us. In the PageURL table of the WebpageIcons.db database, file not shows the time stamp directly for the each visit but investigator should co-relate its time stamp with the other table named iconInfo.

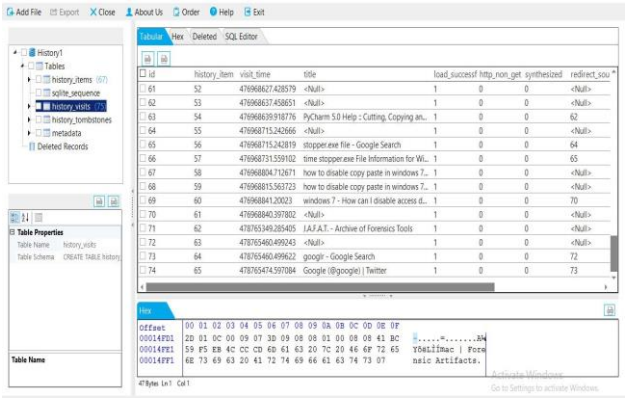


Figure 4 History visits

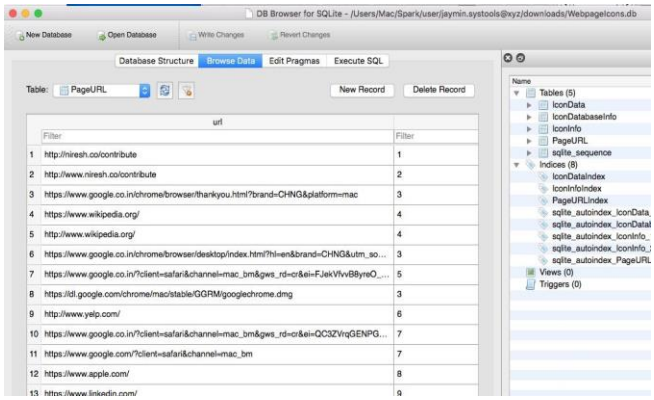


Figure 5 Private Browsing Histories

Favicon Icon is also enough to prove suspects web visits on private browsing as shown in figure 6.

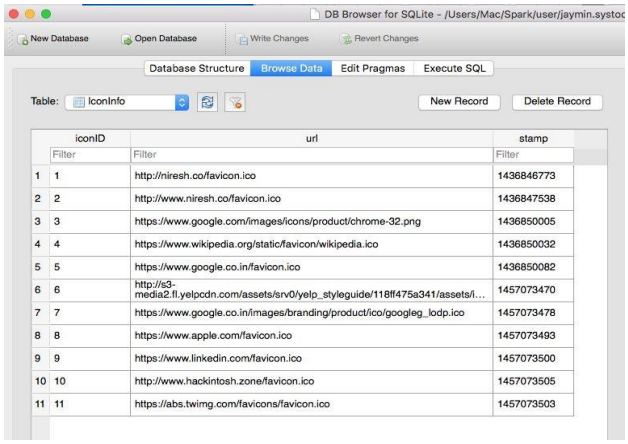


Figure 6 Private Browsing Traces With The Favicon Icon

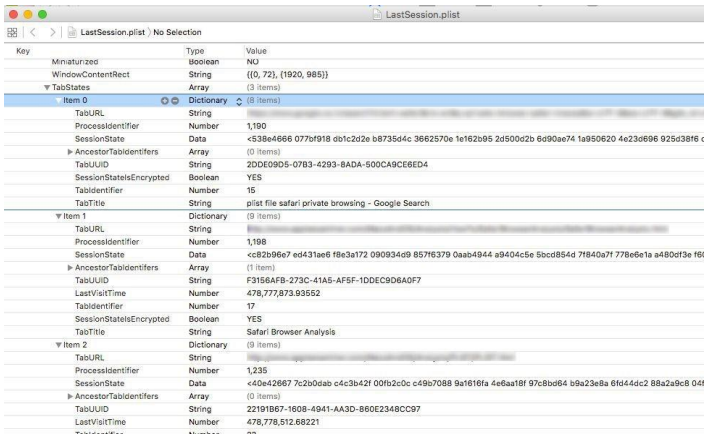
VI. FEW MORE ARTIFACTS OF SAFARI

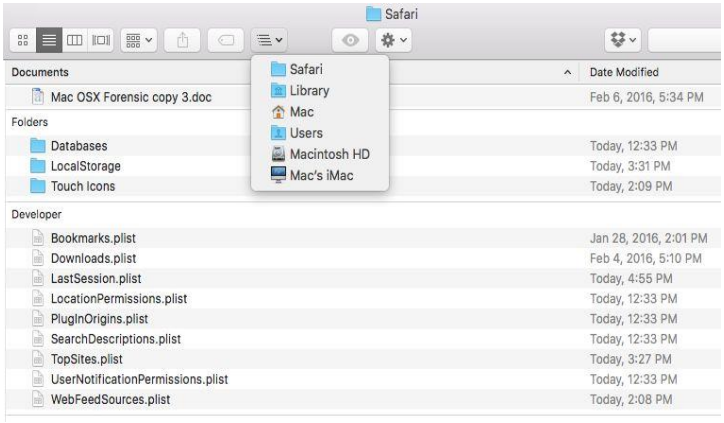
Except History there are other information which is stored in plist file at location /Users/Mac/Library/Safari such as, Bookmarks, Downloads, Last Session, Top sites, User notification shown in figure - 7

Figure 7 Files, which contains the more artifacts

A. LAST SESSIONS

Last browser's session detail stores in LastSessions.plist file with the visited links.





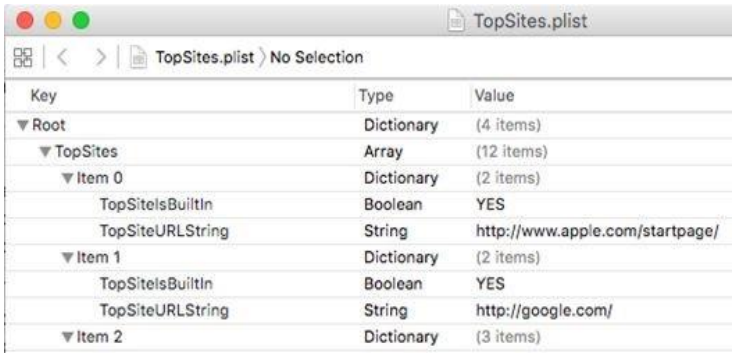
Importance of analyzing this file is to investigate last opened tabs history figure 8.

Figure 8 Last sessions with the tabs

B. TOP SITES

Top sites, which are visited by users and fixed a link short cut on the home page, are shown in the TopSite.plist file as shown in figure 9.

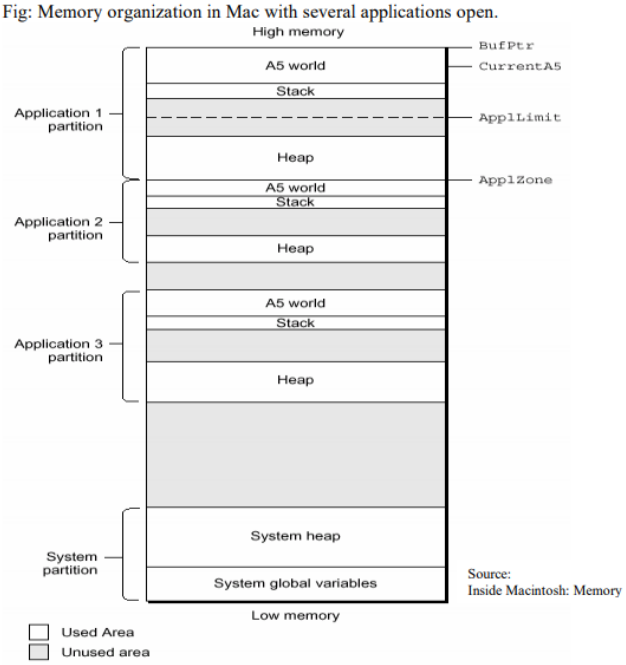
Figure 9 Top sites



VII. Memory Management of MAC OS X

When the Macintosh Operating System starts up, it divides the available RAM into two broad sections. It reserves for itself a zone or partition of memory known as the system partition. The system partition always begins at the lowest addressable byte of memory (memory address 0) and extends upward. All memory outside the system partition is available for allocation to applications or other software components. In system software version 7.0 and later (or when MultiFinder is running in system software versions 5.0 and 6.0), the user can have multiple applications open at once. When an application is launched, the Operating System assigns it a section of memory known as its application partition. In general, an application uses only the memory contained in its own application partition.

Fig: Memory organization in Mac with several applications open.

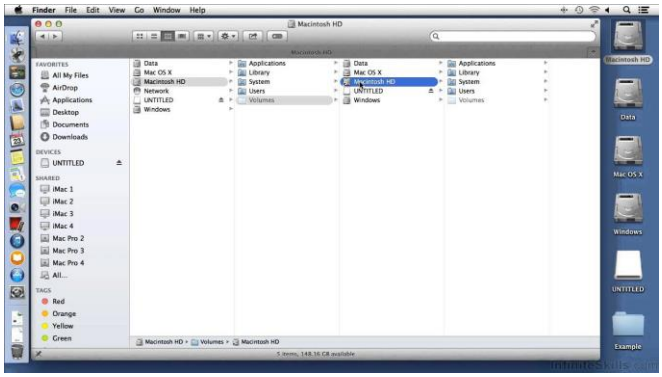


VIII. File Management in MAC OS X

Apple File System replaces HFS Plus as the default file system for iOS 10.3 and later, and for macOS High Sierra and later. Apple File System offers improved file system fundamentals as well as several new features, including cloning, snapshots, space sharing, fast directory sizing, atomic safe-save, and sparse files.

Using high-level APIs in Foundation, such as FileManager and FileHandle, to interact with files takes advantage of the new behavior provided by Apple File System automatically, without requiring changes your code.

If you need to interact with the file system directly, without using any frameworks or the operating system, read Apple File System Reference.



XI. MAC OS X securities used

File Quarantine

In 2009, when Apple released OS X 10.6 Snow Leopard, the new operating system included a rudimentary anti-malware feature. While the official name is File Quarantine, people in the security industry tend to call it XProtect, after one of its configuration files, `Xprotect.plist`. We explained how this works back when it was released. Unlike a true anti-virus, File Quarantine looks for a limited number of very specific types of malware. And it only detects this malware if it's downloaded to a Mac via Safari or Chrome, received as an email attachment by Mail, or sent via a Messages file transfer (and a few other apps).

The only thing a user sees is a banal setting in **System Preferences** > **App Store**. Make sure that Install system data files and security updates is checked to ensure that your Mac updates the File Quarantine exclusion list. If your Mac does detect something nefarious, you'll see an alert.

Gatekeeper

Added to OS X 10.7.5 and 10.8 (Lion and Mountain Lion), Gatekeeper is a technology that

uses *code signing* to verify the authenticity and integrity of applications you launch on your Mac. Every developer can request a certificate from Apple to "sign their code." This cryptographic certificate allows OS X to ensure that an app you run is not only from a registered developer, but also that it hasn't been modified.

There are some limits though. As Apple explains: "Developer ID signature applies to apps downloaded from the Internet. Apps from other sources, such as file servers, external drives, or optical discs are exempt, unless the apps were originally downloaded from the Internet."

So you're protected when you download apps, but not if someone manually installs an app on your Mac, or if you copy it from an external or network drive. And this certificate system can go wrong. In November, Mac users suddenly found they could not launch apps from the Mac App Store, because of an expired certificate.

With Gatekeeper, users have three options. In **System Preferences** > **Security** > **General**, you can choose whether you want your Mac to open apps from the Mac App Store only, from the Mac App Store and registered developers, or from Anywhere, bypassing Gatekeeper entirely. It's a good idea to choose one of the first two options, though if you test applications, you'll need to pick the third.

X. 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.