Mac OSX Digital Forensic Analysis

SHILU DOLLYBEN NARENDRABHAI[1] & CHANDRESH PAREKH[2]
[1]P.G. Student in M.Tech.(Cyber Security) of Raksha Shakti University – Lavad, Dahegam, Gandhinagar.
[2]Assistant Professor, Department of IT & Telecommunication Raksha Shakti University – Lavad, Dahegam, Gandhinagar.

Received: March 03, 2019 Accepted: April 13, 2019

ABSTRACT: : *Popularity of Mac OSX is constantly growing 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 is different Historical digital forensics has been mainly focused on systems with high market share. Yet, even today, digital forensics in Mac OS X has been conducted in a limited scope other than memory forensics such as disk forensics technology with common API and/or existing technique reuse. Additionally, it is necessary to have advanced analysis of Mac OS X artifacts. Records historical file system activity over time. Our study analysis to provides simple access to Spotlight metadata maintained by the operating system, yielding efficient file content search and exposing metadata such as digital camera make and model. It can also help investigators to assess FileVault encrypted home directories. Support tools are under development to interpret files written by common Mac OS applications such as Safari, Mail, and iTunes.*

Key Words: *Digital Forensics as a Service, Digital Forensics, Mac OSX ,Mac OS X forensics, computer forensics.*

1. INTRODUCTION

These Mac OSX Digital Forensic Analysis The Sleuth Kit is a Unix and Windows based tool which helps in forensic analysis of computers. It comes with various tools which helps in digital forensics. These tools help in analyzing disk images, performing in-depth analysis of file systems, and various other things. Forensic investigator is investigating a crime and has collected a suspect's Mac OSX data. Moreover, the forensic investigator has obtained a file system image from the Mac OSX, We note that it is a common practice in forensics that the forensic investigator can retrieve the file system image. There could be thousands of files on the device. The forensic investigator aims to identify the files on the device that could contain certain types of evidentiary data, We call the problem evidence identification problem, and we formally describe it as follows: Given an image of a device's file system and a type of evidentiary data, the evidence identification problem is to identify the files (if any) that contain the type of evidentiary data. In this work, we focus on solving the evidence identification problem for Mac OSX. Moreover, we focus on the evidentiary data including assess FileVault encrypted, historical file system activity over time text input as they were shown to be useful digital evidence in real-world crime investigations. Although we focus on these types of evidentiary data, our techniques can be easily extended to other types of data such as Mac OS applications such as Safari, Mail, and iTunes.If a forensic investigator is interested in analyzing such data for potential evidence. 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 research on mac osx forensic analysis and recovery related to is discussed in. research quespaladin versioniso for mac os image files section IV.Digital forensic Analysis Mac OSX vs Windows OS Comparison Section V The research paper is concluded with comments in section VI discussed about other source of information to extract artifacts.

2. RELATED WORK

Existing forensic tools with explicit support for Mac OS X are few, and typically focus on low-level file system forensics. Guidance Software's EnCase, AccessData's FTK, and some versions of the open source Sleuth Kit can read Apple HFSþformatted disk images; EnCase can also perform a limited snapshot of live OS X machines. Black Bag's Mac Forensics Software and subrosasoft's MacForensicsLab also focus on file-based data recovery and extraction of files of evidentiary value(BlackBagTechnologiesInc. Subrosasoft'sMacForensicsLab). Cyber Security Technologies's live forensic tool, OnLineDFS, supports Mac OS X but does not take advantage of Mac-specific forensic data (OnLineDFS). In addition, with OS X's Unix underpinnings, Unix-based tools and scripts allow an expert examiner to gather generic information about

files and processes.

Dr. DigvijaysinhRathod et al[1] 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 they have discussed various source of information such as Recent web search, browse history, recovery of deleted history, last session, downloads, bookmarks , last session and ,top sites to collect artifacts related to internet activities on Mac OSX.

ShiluDollybenNarendrabhai et al[2]A standardized procedure of investigation process is vital for conducting forensic investigations. The pursuit of a perfect model for digital forensic science will likely never cease. In this research work, the evolution of digital forensic process models was discussed and these models were classified into three types. The first type defines a general process for the entire investigation process. The second type refines and enhances the previous models by improving compatibility with more situations. The third type makes use of new methods, techniques and/or tools in the investigative process to deal with new problems encountered in modern investigations.

Philip Craiger, et al[3] they have scratched the surface of Mac OS X forensics. They have to limit the scope of our coverage due to space limitations and the fact that there are variations in how Mac OS X behaves that are relevant to forensic processing. research with different versions demonstrated that there are several changes in each version (major and/or minor) of Mac OS X that require a new plan of attack to perform forensically sound examinations. Because of these variations it is important that a forensic examiner have a document that lists the protocols for each major and minor version of Mac OS X. This helps ensure that improper procedures are not used that may taint the evidence, for instance, by writing to the suspect's hard drive.

3. RESEARCH ON MAC OSX FORENSIC ANALYSIS

Mac OSX Digital Forensic Analysis extracts and analyzes OS X-specific forensic information from a seized disk image,(Mac OSX Digital Forensic Analysis could also operate in a ''live'' forensics setting – executing directly on the running machine to be analyzed – but our initial attention son after-the-fact analysis.)With a focuson interpreting and analyzing files written by the operating system and commonOSXapplications,Mac OSX Digital Forensic Analysis willprovide insightintoucreativitiesthatisnotpossible–orissubstantiallymoretediousto obtain – with low-level disk image tools. MEGA uses the open source Sleuth Kit tools to extract partition information and files, allowing MEGA to read dd (raw), EnCase, and FTKformat disk images (Carrier). Most of MEGA's extraction and analysis work is performed by executing command-line tools – both The Sleuth Kit and our own custom tools. Mac OSX Digital Forensic Analysis performs its tasks in a forensically sound, reproducible manner, including fully documenting the investigativeprocesswithits ownauditlog.ItcanalsoproduceRTF, PDF, or HTML formatted reports of the data gathered, along with investigators' notes. The initial ''triage'' mode in Mac OSX Digital Forensic Analysis allows an investigator to quickly assess the operating system(s) installed on a Mac OS X diskimageormachine–bothbootablepartit ionsandvirtualmachine images within the file systems. This information allows the forensic examiner to quickly pinpoint the disk partitions most likely of interest and to apply operating system-specific for a machine with two Windows virtual machines. Once triage is complete, employs command-line analysis tools on files automatically extracted from the disk image, then presents the results graphically. designed to be extensible, allowing new analysis tools to be created and added dynamically (e.g., to extract ''recent addresses'' from a new type of e-mail client)

4. PALADIN VERSION7 ISO USED IN IMAGE FILE OF MAC BOOK OS

Apple PList file Tools Magnet IEF , Autopsy ,FTK Imager Since FTK has released a newer version of their software (version 6.0.1). We have decided to update our findings from the previous projects by comparing Access Data's Forensic Toolkit (FTK) v.6.0.1, Guidance Software's EnCase v7.10, and Magnet's Internet Evidence Finder (IEF) v6.7. We are also going to look at the differences between each tool's corresponding imaging software such as FTK Imager, EnCase's imaging option, and Magnet's new imaging software Magnet ACQUIRE.

The following tools are industry-standard and widely used by law enforcement and the private sector. These tools are proven to be reliable and produce consistent defensible results. No tool can cover everything - it is common to use multiple tools for a case. Some of these tools can be used to create forensic images as well. Access Data's FTK Forensic Tool Kit: A powerful digital analysis program that processes and indexes data

from a variety of sources and formats. It allows us to take a forensic image of a computer and process it. Once processed, an examiner can conduct searches, filter data, and view deleted data. FTK is often used to cull data prior to ingestion in eDiscovery platforms such as Relativity. FTK is capable of reporting findings in Excel format, PDF, HTML, and more. It is incredibly powerful and versatile and the preferred industry tool.

Simulation and results Analysis

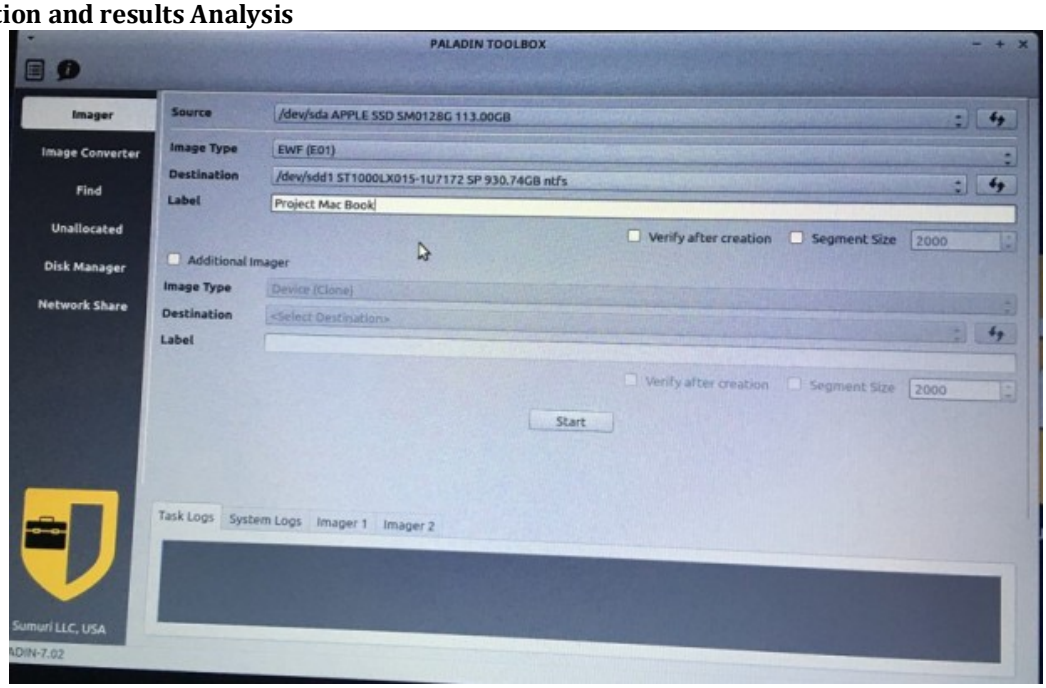

Figure 1: Select the tools for analysis

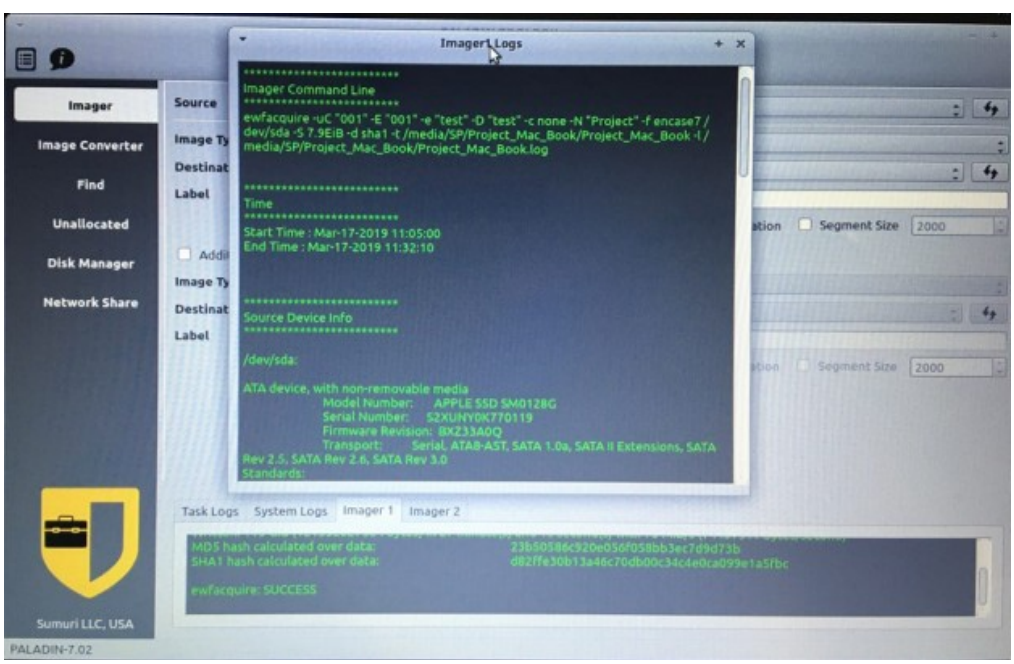

Figure 2: Show the experiment using imagert logs

Guidance Software's EnCase: Much like FTK, EnCase processes and indexes data for searches and analysis. Many examiners use one or the other – even both. Your IST forensic collections team is certified in FTK.

Magnet's Axiom: Previously known as IEF (Internet Evidence Finder), Axiom is the leading web data analysis tool. Axiom processes forensic images and other data sources and parses data related to web activity such as web history, web cookies, downloaded history, web chat, webmail, and more. Axiom also

simplifies the process of analyzing commonly encountered system artifacts like USB history and document history. Axiom allows for reporting in load files, PDF, Excel, HTML, and more.

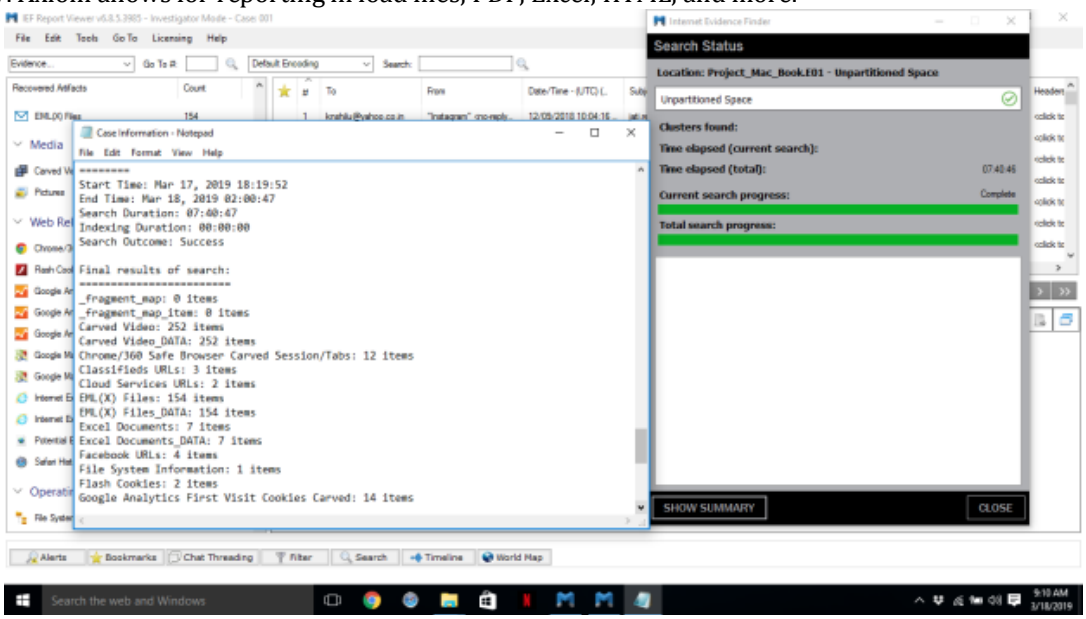

Figure 3: Summery Search Data

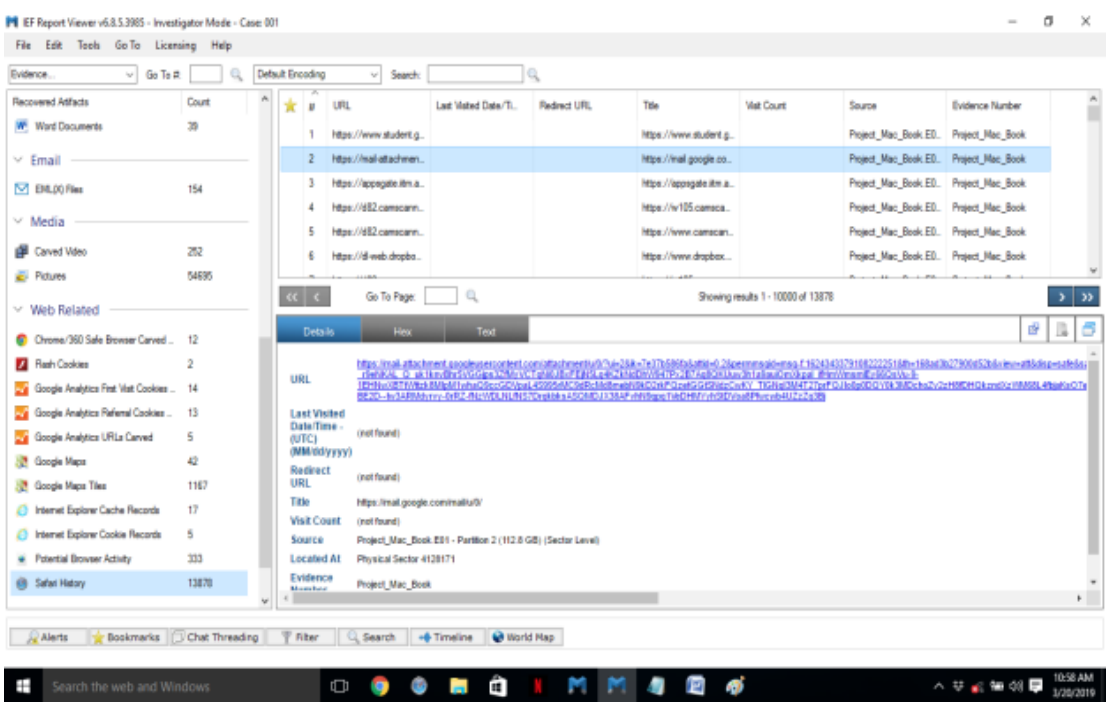

Figure 4: Browser Data, Artifacts

Oxygen Forensic Suite: A mobile device forensic program. Generally lacking in comparison to Cellebrite, Oxygen is capable of extraction and analysis of mobile devices. Oxygen stores extracted mobile phone data in .OFB format which then is usually converted to a Cellebrite friendly format.

Autopsy: A free, light weight digital forensic platform. Capable of processing, carving, and searching.

e ISSN 2348 –1269, Print ISSN 2349-5138
Cosmos Impact Factor 4.236

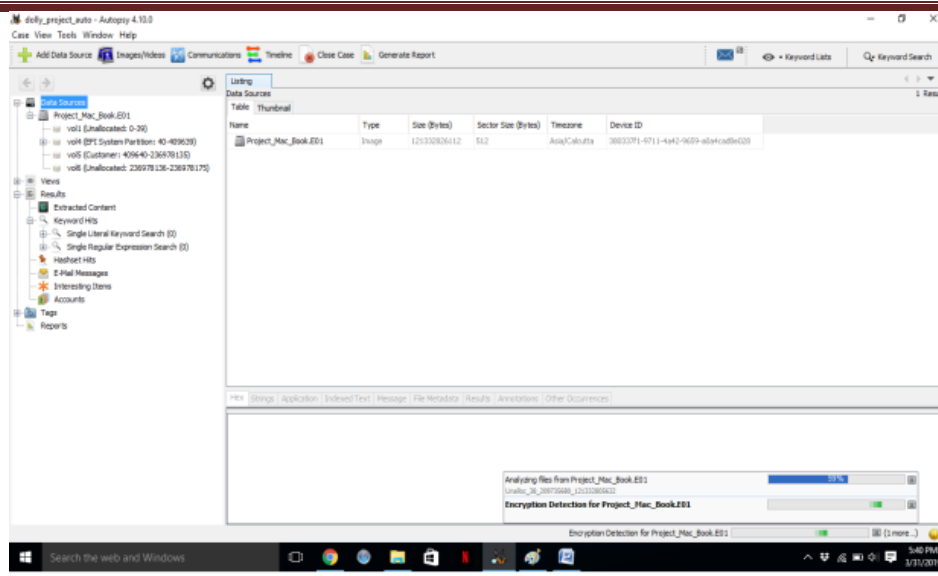

Figure 5: Select the process project for Encryption Detection for project_mac_Book.E01

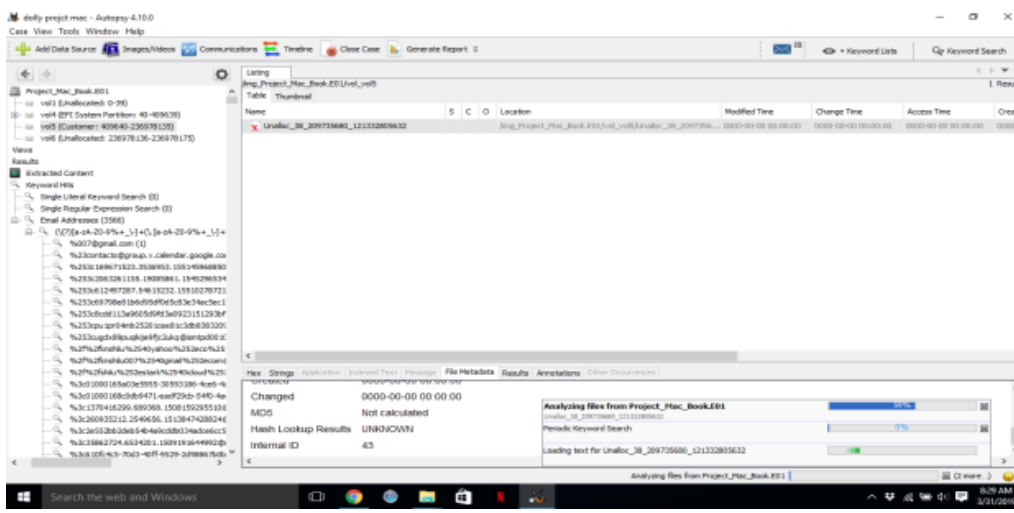

Figure 6: Select the process project for Email Encryption Detection for project_mac_Book.E01

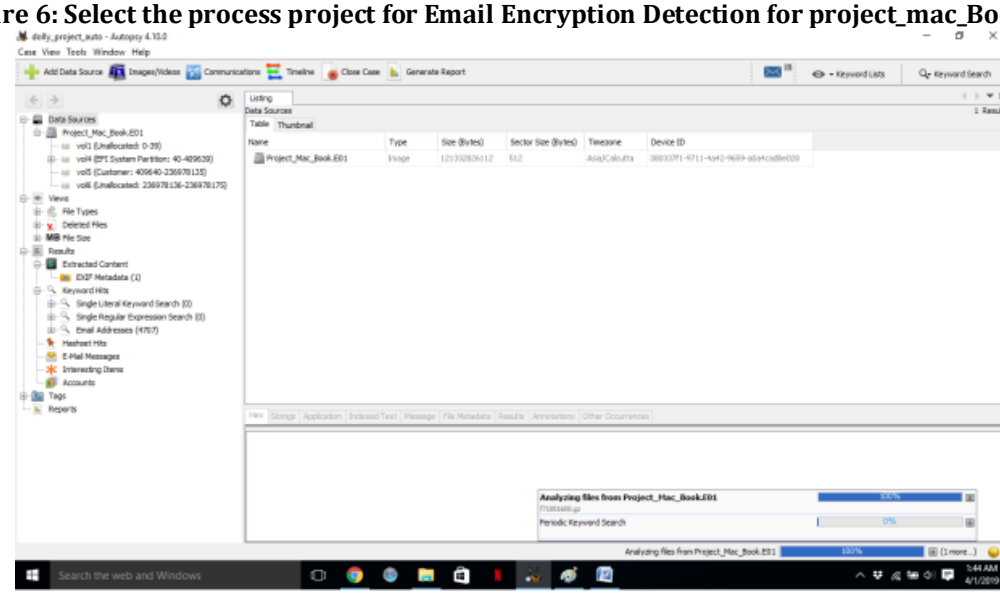

Figure 7: Select the process project for Encryption Detection for project_mac_Book.E01

Aid4Mail: A versatile email preservation and conversion tool. Aid4Mail allows us to pull email from a variety of sources and domains. Once collected, Aid4Mail can convert the data into a .PST file for ingestion into Relativity.

BlackBag'sBlackLight: A powerful forensic analysis platform much like FTK and EnCase, BlackLight can handle evidence from multiple sources. The big difference between BlackLight and the other tools is its ability to parse Apple computer (Mac) images with more intelligent parsing.

Griffeye: A new forensic software tool that processes data and enables intelligent analysis through the use of custom parsers and photo recognition AI. Offers various custom analytic tools within the platform.Digital Forensics is the process of recovering and investigating data from digital devices. The techniques and tools used in this field can be very useful when used as part of a wider 'cyber incident' response plan. We love free and open source tools - especially for Digital Forensics where licensing costs can be prohibitively expensive. Accordingly, we have put together a free/open source tool kit which we have been busy experimenting with before we use it 'in the field'! HDD Acquisition – FTK Imager Lite Download If a system is powered-on, a decision needs to be taken whether to image the system 'live' (which will change data, but can be useful in crypto-malware type situations), or to 'pull the plug' and image the hard drive with a forensic write blocker (to prevent changing data). Whichever method is used, ensure a thorough record is kept of all actions taken. FTK Imager Lite allows selecting of specific disks to image, along with specifying a file type to save as, and a location such as the 'HDD Dump' drive, or a network location. The RAW format 'dd' is the most widely-compatible when saving. If a system is BitLocker-enabled, this makes imaging the disk slightly harder. However, imaging can be done with BitLocker still enabled, and decrypted after, or after decrypting the powered-on computer NB: this changes data. Examination of RAM - Volatility Download. Volatility is both free and open-source, and provides a command-line framework for analysing the contents of a RAM dump. It provides profiles for reading RAM dumps from Windows/Linux/OSX systems, and runs either portable or installed. Running this from a high-spec analysis machine is recommended to make examination quicker. Volatility can do the following, given a RAM dump file: Show running processes Extract running .exe files , List active network connections , List loaded DLLs , Recover encryption keys And much more. Volatility also has many user-created plugins and extra libraries for enhanced functionality - available for free. Using Volatility, interesting network connections or potentially-malicious programs can be displayed from the RAM dump. Suspicious .exe files could even be extracted and put into a sandbox/analysis environment if needed. RAM capture and HDD image video on YouTube.

5. Digital forensic Analysis Mac OSX VS Windows OS Comparison

One of the quickest ways to troll IT security professionals is to proclaim that either Microsoft Windows computers or Apple Macs have better security. In reality, both OSes are adequately secure when operated with their default security settings along with their vendor's best practice recommendations, but after decades of intense competition for passionate consumers, the subject borders on a technical religious war. You won't gain many friends by claiming both are secure. Getty Images Insider exclusive: With that said, not everyone knows what makes the two most popular OSes secure out of the box. Below is an overview of each OS followed by a comparison of the base security features found in each. We didn't include other solid enterprise features that aren't built into the OS and enabled by default.

a. Boot-up protections :

Microsoft Windows 10: Microsoft has long led the way with pre-boot, boot, and post-boot protections. Some of the defenses were borrowed from other open-source operating system initiatives, some from industry-wide initiatives, and many others self-invented. Today, Microsoft places many of them under the larger branding umbrella of Windows Defender System Guard. Boot protections, in particular, are known as Secure Boot.With Secure Boot, everything starts pre-boot by requiring computers to have the updated, more secure, Unified Extensible Firmware Interface (UEFI) and Trusted Platform Module (TPM) chips installed on the motherboard and used. Both chips require cryptographic approval before they will accept new code or configuration settings, and both allow the boot process to be cryptographically measured and verified. Earlier verified components often securely store the previously verified hash of later components, which must match, before the booting process can continue normally. Microsoft also refers to these processes as Measured Boot or Trusted Boot.If anything, like a rootkit, tries to modify the pre-boot or OS booting process, one of these two chips will be alerted and either stop the attempted modification or give the user a critical warning upon next use. If you remember all the press about rootkits and boot malware and wonder why we don't hear about them as much anymore, it's because of pre-boot and boot protection processes like these. Mark it as one of the few significant successes against hackers and malware.Both UEFI and TPM are open standards that any vendor or OS may use. UEFI replaced the more vulnerable BIOS chips, and the TPM chip

hosts a core set of cryptographic features, including the secure storage of critical system cryptographic keys. Both chips allow any OS vendor to better maintain the integrity of their OS, and other applications, such as data storage encryption, during and after boot.

b. Apple macOS:

Apple adopted an early version of UEFI with far less protection known as EFI 1.0, but hasn't adopted the more secure, later, versions of UEFI. Instead, Apple has created many proprietary features with some of the same, but not identical, protections. Because Apple has not released detailed information on its proprietary protections, it is difficult to get more specifics on Apple's pre-boot and boot protections to see how well they compare. However, several boot-up protections can be enabled on the Mac, specifically to prevent access to the data on a Mac's hard drive if it falls into the wrong hands. The standard user account password provides rudimentary protection against access on a properly booted Mac, but does nothing against someone with access to the equipment and with knowledge of Target Disk Mode.To prevent unauthorized access, startup disks can be encrypted using FileVault 2, and the Mac can be set to prevent booting to external devices via firmware passwords. FileVault 2 encrypts the entire drive using the AES-XTS mode of AES with 128-bit blocks and a 256-bit key, and it prevents anyone who does not have an unlock-enabled account from seeing disk contents whatsoever.The new iMac Pro released in late 2017 features an Apple-designed T2 chipset. This chipset consolidates a bunch of hardware subsystems into one chipset, but also introduces some interesting security features that will be adopted on other Macs, eventually.

c. Memory protections

Microsoft Windows 10: Microsoft has done much security work in memory protections, usually to prevent initial exploits, zero days, and privilege escalations. Most are gathered under the Windows Defender Exploit Guard, and many came from a previous exploit protection add-on called Enhanced Mitigation Experience Toolkit (EMET).Data Execution Protection (DEP) has been around since Windows XP. DEP attempts to prevent malicious buffer overflows, where a malware program attempts to place executable code in a data area, and then trick the OS into executing it. DEP prevents the OS from executing anything in areas marked as data.Microsoft Windows Vista introduced many new security features, including Address Space Layout Randomization (ASLR), Structured Exception Handling Overwrite Protection (SEHOP), and Protected Processes. ASLR places common, critical, system executables in different places in memory between each boot. This makes it significantly harder for malicious programs that attempt to manipulate and modify these components to find them.SEHOP attempts to stop malicious, rogue, error handling from being installed and executed when an execution error is found. These security features and other preventative technologies morphed into what Microsoft now calls Control Flow Guard. It is enabled on every Microsoft program and is available in programming tools such as Microsoft Visual Studio 15.EMET also arrived in Vista, as an add-in to help prevent 0day attacks. It contained memory protections, digital certificate handling improvements (like certificate pinning), early warnings, and improved reporting to both the OS admin and Microsoft so they could identify the technical specifics of different new attacks. EMET expanded to over 15 separate mitigations, and its proven protection became so recommended that Microsoft built it into Windows 10 with the Creators Update release (as Windows Defender Exploit Guard).Apple macOS: Macs have an XD (execute disable) feature built into Intel's processors that prevents memory used for data and memory used for executable instructions from accessing each other. This is a common attack used by malware to compromise a system, but the XD creates a barrier of sorts.Also built into every Mac is the macOS kernel's use of ASLR, which makes it more difficult for attackers to pinpoint application vulnerabilities by randomly arranging the values of target addresses. Basically, with ASLR enabled, a hacker is more likely to crash the app they're trying to exploit than gain access to do anything malicious.

d. Logon/authentication

Windows 10: Once an OS boots up, the most important security feature it can have is in limiting who has allowed, authorized access to it. This is controlled by a logon authentication security feature and might include passwords, biometrics, digital certificates, and other multi-factor devices, such as smartcards and USB authentication tokens. It has also become especially important to protect logon credentials after the authorized party has logged on, temporarily or permanently, whether stored in memory or on disk, to stop various credential theft and re-use attacks. Windows 10 has strong support for broad password policies, and for biometric, multi-factor, and digital certificate authentication. Microsoft's newest and most secure logon feature is known as Windows Hello. It supports face and fingerprint recognition, which allows for quick and easy signors, but behind the scenes uses secure digital certificate technology. Users can still use a password or a shorter PIN, although each of these can only be enabled as an option after setting up more traditional authentication methods (such as password). Windows Hello also works with enabled applications, such as

Dropbox and multiple password managers.Microsoft, worried about the theft of credentials in memory, created Virtualization Based Security (VBS), where logon credentials are secured in a hardware-based, virtualized subset of the operating system that is nearly impervious to malicious attacks. You may hear VBS also referred to as Virtual Secure Mode (VSM).Using the VBS core, they created Windows Defender Credential Guard and Device Guard. Credential Guard protects multiple types of logon credentials including NTLM, Kerberos, and other non-web, domain-based credentials stored in Microsoft Windows' Credential Manager. Credential Guard defeats many of the most critical and popular password attacks. Credential Guard requires 64-bit version of Windows, UEFI, TPM (recommended, not required), Secure Boot, and an Intel or AMD processors with the appropriate virtualization extensions.

6. CONCLUSION

As Apple's market share rises, Mac OS X platform will become target for malware attackers. The proliferation of Mac malware demanded the Mac OS X incident response and Mac malware analysis skills. Collection of relevant volatile information is very much necessary in handling the security incident. In some cases one can determine if a system is compromised based on the volatile data alone. Mac as X forensicsis an important but relatively unexplored area of research. This paper has discussed procedures for recovering evidence from allocated space, unallocated space, slack space and virtual memory, as well as Mac as X default email, web browser and instant messaging applications, and command line input Our study analysis to provides simple access to Spotlight metadata maintained by the operating system, yielding efficient file content search and exposing metadata such as digital camera make and model.

7. REFERENCE

1. Dr. DigvijaysinhRathod ," MAC OSX FORENSICS" International Journal of Advanced Research in Computer Engineering & Technology (IJARCET) Volume 6, Issue 8, August 2017, ISSN: 2278 – 1323.
2. ShiluDollybenNarendrabhai , CHANDRESH PAREKH," Digital Forensic Analysis For Mac OS X" 2019 JETIR April 2019, Volume 6, Issue 4 www.jetir.org (ISSN-2349-5162).
3. Philip Craiger, PhD, Paul K. Burke," Mac Forensics: Mac OS X and the HFS+ File System"
4. ChrisChao-ChunCheng,ChenShi,NeilZhenqiangGong,andYongGuan, "EviHunter:Identifying Digital Evidenceinthe Permanent Storage of Android Devicesvia Static Analysi"CCS'18, October 15-19, 2018, Toronto, ON, Canada.
5. Du, X., Le-Khac, N.A., Scanlon, M., 2017. Evaluation of digital forensic process modelswith respect to digital forensics as a service. In: Proceedings of the 16th European Conference on Cyber Warfare and Security (ECCWS 2017). ACPI, Dublin,Ireland, pp. 573e581.
6. Du, X., Ledwith, P., Scanlon, M., 2018. Deduplicated disk image evidence acquisitionand forensically-sound reconstruction. In: Proceedings of the 17th IEEE International Conference on Trust, Security and Privacy in Computing and Communications (TrustCom-18). IEEE, New York, USA, pp. 1674e1679.
7. Donnelly, Derrick. Presentation on Mac OS X Forensics. O'Reilly Mac OS X Conference, October 2004. http://conferences.oreillynet.com/cs/macosx2004/view/e_sess/5556
8. Hawkins, Peter. Macintosh Forensic Analysis Using OS X. SANS Institute, 2002. http://www.sans.org/reading_room/whitepapers/apple/
9. Apple. Audit XNU source code, 2010.
10. Apple. BSM XNU source code, 2010.
11. Apple. OS X: Mac OS Extended format (HFS Plus) volume and file limits. Apple Technical White Paper, page 33, 2010.
12. Apple. ASL Library, 2011.
13. Apple. OS X Security. Apple Technical White Paper, page 13, 2012.
14. Apple. Audit.log, Basic Security Module (BSM) file format, 2013.