Summer 8-10-2024

Open-Source Forensics Tools are great tools for critical used machines

Erik Herrera
Stephen F. Austin State University, herrerae4@outlook.com

Open-Source Forensics Tools are great tools for critical used machines

Creative Commons License

Open-Source Forensics Tools are great tools for critical used machines

By

Erik Herrera

Presented to the Faculty of the Graduate School of
Stephen F. Austin State University
In Partial Fulfillment
of the Requirements

For the Degree of
Master of Science

STEPHEN F. AUSTIN STATE UNIVERSITY
August 2024

Open Source Tools are great tools for critical used machines

By

Erik Herrera

Approved:

_____
Christopher Ivancic, Ph.D., Thesis Director

_____
Brian Barngrover, Ph.D., Committee Member

_____
Jianjun Zheng, Ph.D., Committee Member

_____
Dipak Singh, Ph.D., Committee Member

_____
Dr. Forrest Lane, Ph.D.
Dean of Research and Graduate Studies

Abstract

Open-Source software exists on everything from operating systems to daily productivity applications. In digital forensics, a very popular tool that is used to learn on and expand is Autopsy. Autopsy is known in the digital world due to its potential and wide usage. It is in many built packages of software inside the open-source world of applications. It is built into premade operating systems that are involved in Digital Forensics and Penetration Testing. Prebuilt OS includes Kali Linux and Computer Aided Investigative Environment (CAINE).

In the application to defend Open-Source software being just as good as closed-source software, I will conduct an experiment with a disk image that was provided by the National Institute of Standards and Technology (NIST). The image provided was designated for Forensics Image Test purposes. There will be 3 virtual machines set up to show the capabilities of each tool to conduct digital investigation. Kali Linux and CAINE are Ubuntu based operating systems with several tools built in to perform digital forensics. The 3rd Virtual Machine will be Windows based with a fresh and new copy of Autopsy loaded. Utilizing the core application Autopsy, there will be evidence that will be gathered and analyzed. The functionality of the process to solve the digital case will be noted and will be compared to the closed source software. The functionalities of open-source and closed-source tools will be compared for similarities. After analyzing the similarities, the experiment proves that open-source forensic tools are just as effective and can be great tools for digital forensics.

Acknowledgements

I would like to give thanks to my professors that helped me succeed through my Graduate and Undergraduate studies. I would like to give special thanks to Dr. Ivancic and Dr. Zheng for motivating me to learn about the world of Cyber Security. Dr. Ivancic has been a great professor as well as supporting trying out new things related to the field. Also, Dr. Zheng, for being an amazing professor and pushing the class to learn the material as well as explore new margins with new applications related to cyber security. I would also like to give my thanks to Dr. David Cook, he was an amazing soul in the Computer Science department. I still remember the great stories he would share with the class and our friendly conversations in the office. He was a great inspiration to pursue Computer Science and explore the world of IT.

I would also like to give thanks to my family, my mother Olimpia, who would push me to persevere and keep on pushing through tough times and to my brother Daniel, for his tough love and recognition to keep a strong family together. These two individuals have heard my complaints and guided me through my undergrad and graduate school. As a team we shall start climbing the building ladder and keep on discovering new success without fear.

Contents

List of Figures

1. Introduction:

Critical Systems face a common issue that may expose any agency or organization to havoc. A critical system is a system that requires high reliability and maintain reliability. There are methods in which we can search for vulnerabilities and weaknesses. There are many tools that exist to serve the purpose of discovering vulnerabilities. These are called Forensic Tools. Forensic tools are used for different systems to find such artifacts. The systems in which we utilize may include Unix base system, Windows, and other base systems. A few examples of Critical Systems include server hosting a website, a control that may control an application or device, and a desktop computer. There is no such thing as a secure critical system. New methods of hacking and force penetration are created every day. It is the owner and user's discretion to maintain and attempt to keep their systems secure as best as possible. Many systems get compromised due to software vulnerabilities, outdated hardware, lack of safeties implemented, open access doors, etc.

A common topic that is brought up is which tools are preferred when it involves a critical system. Several questions arise from users. Forensic tools are based on open-source code and closed/proprietary code. Are open-source tools useful tools? Which tools are preferred when it comes to forensics tools. This leads us to exploring open-source paradigm in conducting digital forensics. Open-source tools means that the source code is open available for the public and is developed by the public. Closed source means that its originator is the only source in which view and modify source code. Open source may mean that many programs can be based on the same source code. Expandability is indefinite since this opens the possibility for any agency to create their own tools based on the open-source tools.

In the discussion of utilizing a forensic tool against a critical system, the usage of data forensics will be utilized on an investigated machine. The common practices will be performed to analyze a sample machine to discover the utility and suspicious activity.

Disk Image was provided by the NIST and may have been a real case in which forensics tools were utilized to defend or upon a case.

2. Objective:

2.1 Hypothesis

Open Source framework is reliable for use in a critical system.

2.2 Research Question:

- Are open-source forensics tools able to detect vulnerabilities on critical systems?
- Are they updated regularly in the field?
- What are a few examples of what a critical system may be?
- What do each forensic tool offer?

2.3 Objective

A virtual machine will be set up to run Ubuntu OS. Utilizing this operating system certain tools will be tested against Linux based Virtual Machine and a Windows Machine. This is to emulate both world scenarios in which a critical machine may be running on. Both open and closed source forensic tools will be used to see the compatibility between each operating system and to see which features they may pack with. For the closed source forensic tools that may not be used for free, research will be based on academic articles and documents to prove the usability of the tools.

3. Literature Review

On-scene open source article regards a few examples of open source tools and proves its effectiveness on testing environments.[1] The tools used for the comparison include TriageIR, TR3Secure, and Kludge. Each one of them has its advantages and drawbacks. Charts are given in which each tool supports including networking, registers, file systems support, and configuration. Also shows effectiveness with different windows operating systems. All these tools serve a purpose within the data forensics sector.

Open-Source forensics article gives great examples of how open-source forensics tools compare to closed source options.[2] Each tool gives a different outcome on error rate, support for the environment being tested, integrity, etc... Also, gives examples of how the test was conducted regarding the topic of why open-source forensics tools are widely accepted.

A comprehensive survey on computer forensics, is an article regarding the various categories that are involved in computer forensics.[3] This includes operating system forensics, file system forensics, live memory forensics, etc... The article provides a breakdown of tools that are used on real life cases; such as Autopsy Sleuthkit[10], Redline, Belkasoft evidence center, Encase, Prodiscover basic, Xways forensics, FTK[11], Magnet Axiom[12], etc... Some of these tools support specific operating system platforms and are opensource, freeware, or proprietary.

Using Open-Source tools to fulfil digital preservation requirement is an important article talking about how Open-Source Software (OSS) is a necessity to into digital preservation.[4] Additional research must be performed to enhance OSS. Open-Source software is the reason for increasing digital collections. The expansion of OSS allows for many to fulfill their own needs.

The Department of Defense heavily depends on open-source software. This contributes development towards any critical system that the government utilizes. The US

Government does much of its software development under Linux Operating System. [5] This article gives a brief history of the utilization of open-source software and the restrictions of how certain things are not used today. Overall, this article gives good details of the pros and cons of open source and how it contributed to the DOD, Department of Defense.

Article by Prasanthi relates to the increased need for digital forensics. Cyber security as a field is evolving. The need to investigate and analyze digital evidence increases as new ways to exploit and hide digital data are discovered. The article provides an overview of the various types of forensics that may be conducted.[6] This includes computer, mobile device, network, virtual forensics framework, open computer forensics architecture, x-ways and many other types of forensics. A list of tools that may be used for the kind of forensics was provided.

An international journal written for the government of India provides a great overview about how OSS, open-source software, and how many types contribute to different workflows.[7] This journal provides explanation towards operating system, tools, software for authentication, etc.… There is a functionality, their security flaws as well as their pros, as well as their operating system support. Also, licensing and regulation examples are provided. Overall, this article gives a few recommendations that may be beneficial to the Department of Defense on software contracting.

In similarity of open-source software and their implementation to digital forensics, Open-source tools are always being updated and used. The topic regarding open software is evolving and is being used to create closed source code. An example of this includes FTK Imager which is a free tool that is based on FTK Forensic Toolkit. Creativeness and ideas are developed everyday.[4] Both open and closed source code provide as good functionality from one another. One may be more convenient but the creativity in open-source allows others to build upon.

4. Justification

Tools that will be used to defend Open-Source tools will include utilizing Kali Linux, CAINE, and Autopsy. FTK Forensic Toolkit, and MAGNET Forensics will be utilized as the closed source tools. The reason why these tools were chosen was because they are commonly used. FTK Forensic Toolkit and MAGNET Forensics are both well known in the law enforcement world. All these tools will be used under Ubuntu Virtual Machine using Oracle VM Virtual Box. The hardware machine running these virtual machines will be hosted on a portable computer with a 13th gen Intel core i7 CPU and 16gb of memory. In the experiment, a forensics case provided by the NIST, National Institute of Standard and Technology, will be utilized to capture and review a sample case.

5. Experiment

5.1 Kali Linux

Kali Linux contains several programs that serve different features that correlate to Computer Forensics. This is a dedicated Debian based Operating System that contains tools for digital forensics as well as penetration testing. The reason why the open-source operating systems are included is because they contain multiple tools to serve the same purpose as the forensic toolkit. Both Kali and CAINE are open-source tools that are contained within a Linux operating system. The tools that will be utilized will include Autopsy which will be used to process disk images and view disk contents of a machine that is being analyzed. An additional piece of software that will be used includes disk image carvers to restore corrupted disk images, and files. The names of these programs includes Magicrescue, Scalpel, Scrounge-ntfs. Magicrescue is designed to scan a file and solve what the file type should be. Scalpel is designed to recover a file by analyzing header and footer of the file being analyzed. Scrounge-ntfs attempts to recover data from corrupted NTFS partitions. An NTFS partition is a Windows Operating System partition that is used in modern day. Also, there is Pdfid and Pdf-parser. These applications are used to analyze pdf files. Another program that is similar to Autopsy is Bulk-extractor. This program is designed to analyze disk images and files on a byte by byte basis. Kali Linux is an overall suite of tools as an operating system, similar to CAINE.

5.2 Computer Aided Investigated Environment (CAINE)

CAINE has similar programs compared to Kali Linux. CAINE was designed around computer forensics only. There are several tools that are used for several kinds of digital forensics. Similar tools that are includes from kali includes Autopsy and bulk

extractor but with a GUI. This operating system contains several more tools and is separated in categories. This includes Analysis, Database, Disks, Hash, Malware, Memory Forensics, Mobile Forensics, Network Forensics, Timeline, and OSINT (Open Source Intelligence). On the Analysis portion of CAINE, several programs are included in this section. Stegosuite for steganography, RegRipper for windows registry analysis, Afro for Apple Computers that may use APFS file system, Ophcrack for windows password cracking, and Photorec for data carving. For the Database section, we have programs to parse through sqlite and DB Browser for SQLite. In Disks section, several tools are include to repair, mount, and recover various file systems. Guymager, is a disk imager, Disk Image Mounter for dd, ewf, and aff disk images. XHFS to browse HFS file systems, SafeCopy to image disks, VHDIMount to mount virtual hard disk files. There are programs to verify file hash such as QuickHash. In the malware section, we have stegosuit for steganography which looks for malware inside files. PDF Scanner to analyze pdf files, PEFrame for static malware analysis, and VolDiff for memory malware analysis. For memory analysis, we have also Volatility which analyzes ram memory to see anything that may have been open and is still active in memory, as well as Memdump which copies your ram memory and stores it into a local file for analysis. Next section is Mobile forensics, here we have tools that can be used against blackberry mobile phones by using Blackberry scripts, ANDRILLER to analyze mobile phone,ILoot for icloud extraction, LibMobileDevice for running scripts on IOS based devices. For Network forensics, we have Wireshark to monitor network traffic going and receiving to machine, Remote File System Mounter to connect to a remote computer, and Netdiscovery to see what is connected to the local network. Inside the OSINT section, we have TheHarvester, this tool is used to gather emails, subdomains, and names that may be used to a given email. Infoaga for email analysis and Carbon 14 to view when a website was created. Last section is Timeline, here we have programs to give you a timeline of a machine in which files and programs were used and changes to a machine were done. The programs include NBTempo and Log2Timeline. There are many more applications provided with

this Operating System configuration, but they may be used for miscellaneous exploration of certain devices. Reviewing CAINE and KALI being similar in functionality and purpose, Autopsy is a common program that are contained in both.

5.3 Autopsy

Autopsy is included in both Kali and CAINE. The versions included in Kali and CAINE are older releases. Fresh install in any machine, a newer version is available for installation with more functionality. It can be installed natively into any machine, including Windows, Macintosh, and Linux based machines. Main reason why it will be included natively is because the standalone program functions similarly to FTK and Magnet. The program allows you to create a case assign and image file and process it. Upon processing the disk images or files, subsections are created to view computer as a timeline, separate data artifacts including Data Artifacts, items in recycle bin, computer users, and extract files to view their true nature. Autopsy creates a read only environment to review files, this leads to FTK Forensic tool kit which provides similar functionality.

5.4 FTK Forensic Toolkit

FTK Forensic Toolkit, FTK 8.0, is a powerful suite that is commonly used in Law Enforcement. This program is very well known for being used in the private sector. This program is different from the first 2 options that was explained because it is not an open-source program. This program come with a hefty fee of 3995 per year. In additional, a free version of the program is limited to their FTK Imager program. It provides a simple timeline on a disk image and has some processing power to dissect a computer disk and do certain digital forensics. It is a standalone Suite in which users are allowed to install application to their work machine and run all kinds of forensics at once. You can connect a machine, image a drive, and run a thorough analysis with a timeline being generated all at once. Many subsections are given to pinpoint items that may require attention and lead to an investigation. Categories are given to view multimedia files, emails, chats,

Operating System vulnerabilities and events that were performed. Also, there is a built-in Mobile Data section to view and investigate a mobile dev

5.5 Magnet Forensics

Magnet Axiom forensics is an alternative to FTK 8.0 that performs similar operations for digital forensics. There is ability to build your case file to analyze disk images, examine and recover what is necessary to meet a goal. Ther are options to select a specific platform such as a computer, mobile device, cloud, and even vehicle data. The program can analyze, create timelines, and trace events to make it easier to what is required to be investigated. For mobile devices, you can assign Android, iOS, Windows devices, digital cameras and will automate and build the necessary steps to pinpoint what may be necessary to conduct a search. An interesting feature is that you can save evidence and can be shared within your agency to continue operating an investigation without losing security and not compromising integrity. Exploring enhance features with Magnet Forensics, there are simpler programs that can do basic functionality. This leads to experimenting with Pancake Viewer.

5.6 Pancake Viewer

Pancake Viewer is an open-source tool that shares similarities to FTK Forensic Toolkit little brother application called FTK Imager. This program is compiled by python and several other python-based dependencies. The program allows the investigator to open image files or a logical drive. Upon opening a disk, it provides a tree view of the file structure and extracts files out to be analyzed. The tool supports various disk formats including Apple's hfs file system. The application is ran by dfvfs, Digital Forensics Virtual File System which provides the application a read only to the disks that are analyzed by the tool.

5.7 Reviewing case with Autopsy

To begin with a baseline of the experiment of the NIST provided disk image, the usage of Autopsy 4.21.0 will be used to provide a starting line into discovering the evidence to prove a case. The file being investigated is '2020JimmyWilson.E01'. Once the case is created, the case will be like the following.

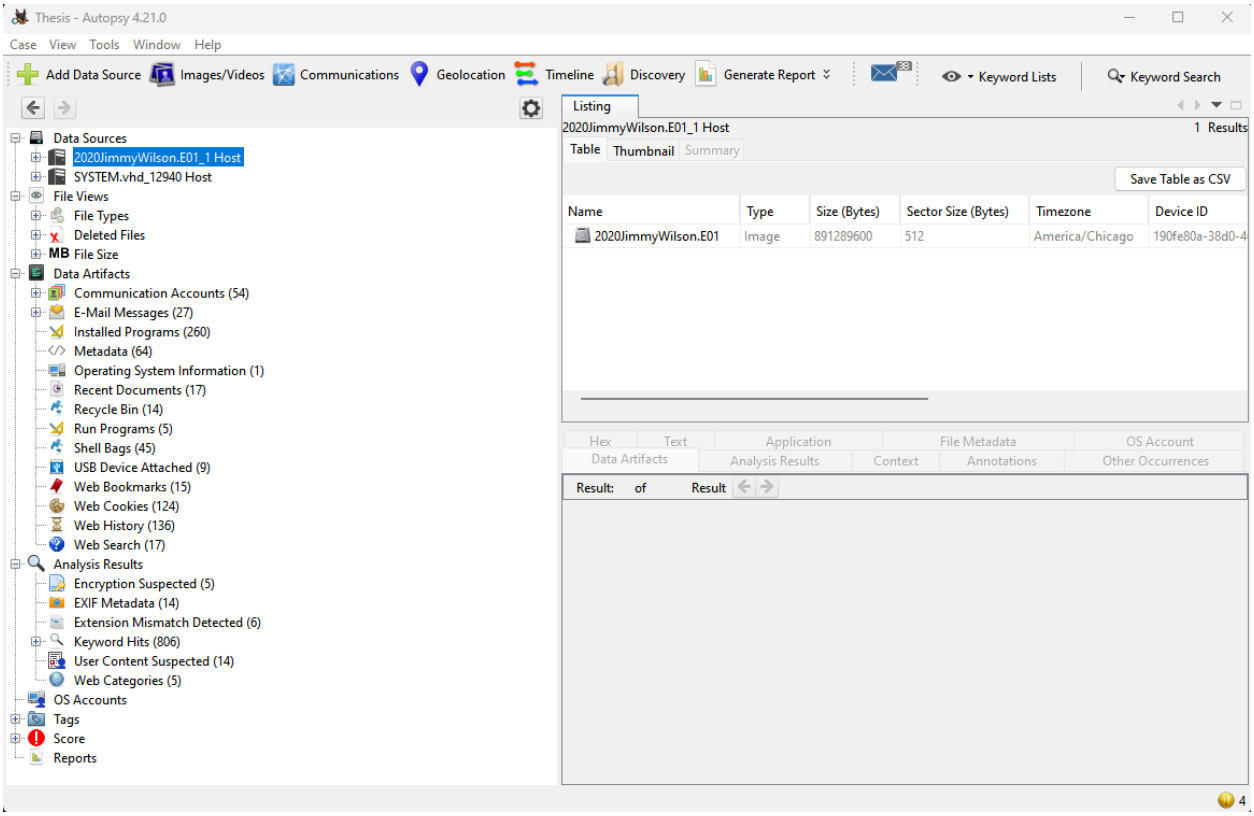


Figure 5.1: Autopsy Interface

There is no connection or cause towards what is being investigated, so the first plan is to see any suspicion. The initial step is to review any suspicious items which may be under the score tab on the left panel of the program. There will be a subsection named ‘Suspicious Items’. After viewing several files under that section, there is evidence of suspicious activity happening between one email user to another. Encryption in files seems to be evident.

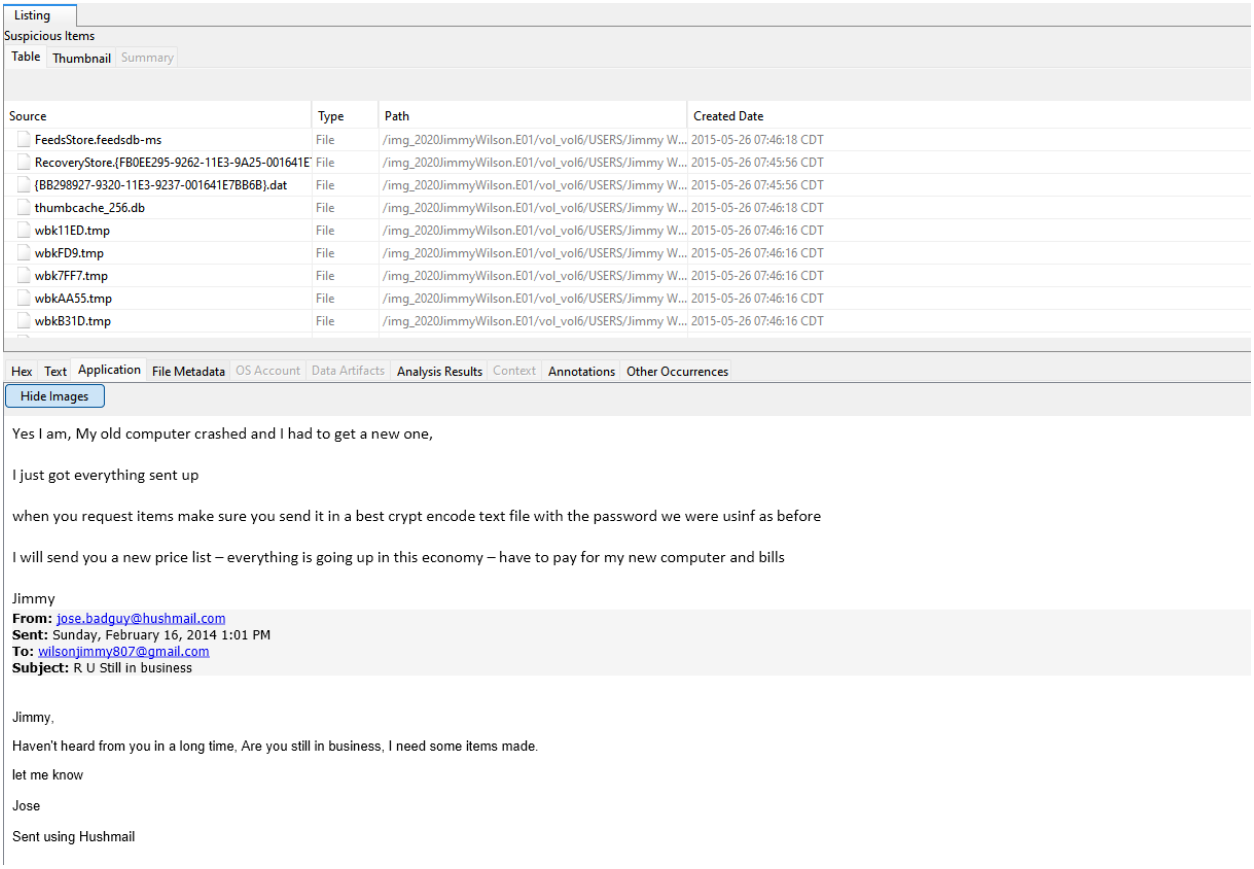


Figure 5.2: Autopsy Reading Suspicious Files

Since there is evidence happening via email, the email functionality of Autopsy can be used to see if there are any attachments or any additional clues coming from Jimmy Wilson. The email functionality is located under Data Artifacts/E-Mail Messages column on the left-hand panel. There are 27 emails found under this section. A few of the email is regarding some exchange and attached files. First email seem to have 4 attachments, 3 images and 1 unknown file. The files are exported to review. The image files seem weird as they are pictures of animals and the unknown file seems to be an encrypted file. Upon reviewing the encrypted file, there is evidence perhaps a 3rd party application was used to encrypt. BCTextEditor seems to be used.

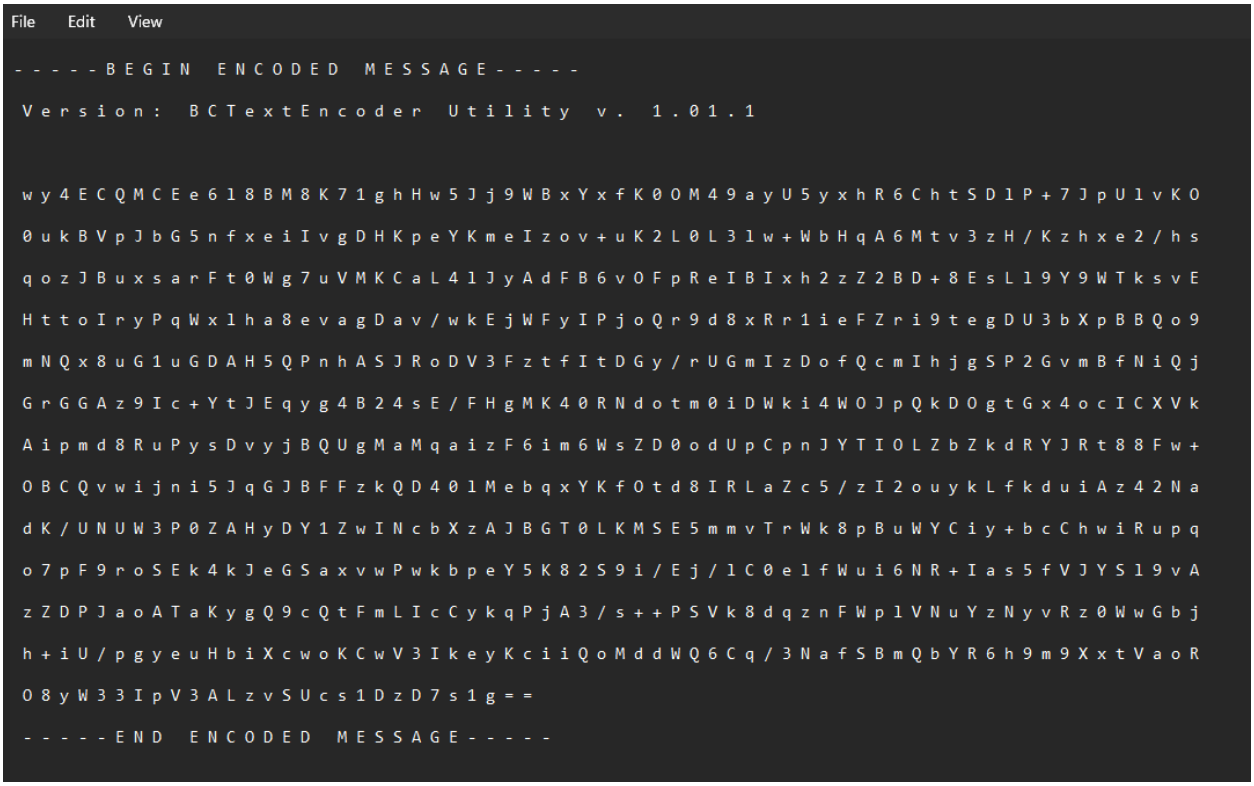


Figure 5.3: Encrypted Text File

Suspicion increases that evidence is being hidden inside encrypted files. After a few files have been exported, we have an idea of what files changes have been done prior to being encrypted. The program's timeline feature will come in handy to resolve what kind of transactions/interactions were performed through the found emails. After generating the time with Autopsy's timeline feature on the top portion of the program, there is evidence of original untouched files being present at a certain time.

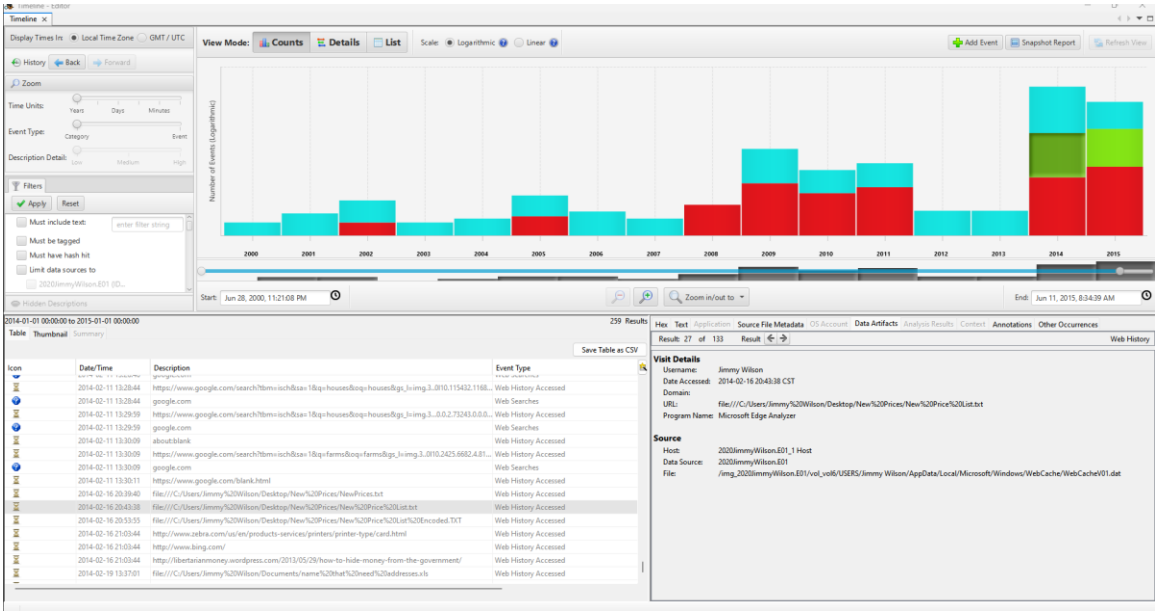


Figure 5.4: Autopsy Timeline

Tracing the files that were untouched, there will be a way to retrieve it to see the unencrypted file. After some searching of the files, a directory was found, and the given evidence gave a text file with pricing of what the email exchanges were speaking about. The untethered version of the text file is the following.

```
New Price List as of 01 FEBRUARY 2014

Credit Cards: $350.00

Drivers License: $250.00

ID Cards:  $250.00

Green Cards:  $300.00

Insurance Certifcates: $100.00
```

Figure 5.5: Unaltered Text File

After reviewing the text document, the user of the computer was performing some illegal activity related to credit card fraud, identification fraud, and falsifying documents. In addition to the obvious, the user was encrypting files. In addition to the timeline functionality of Autopsy, there is evidence the user installed TrueCrypt. This is a program to create an encrypted virtual drive on the installed machine. With the power of Autopsy, the drive can be seen.

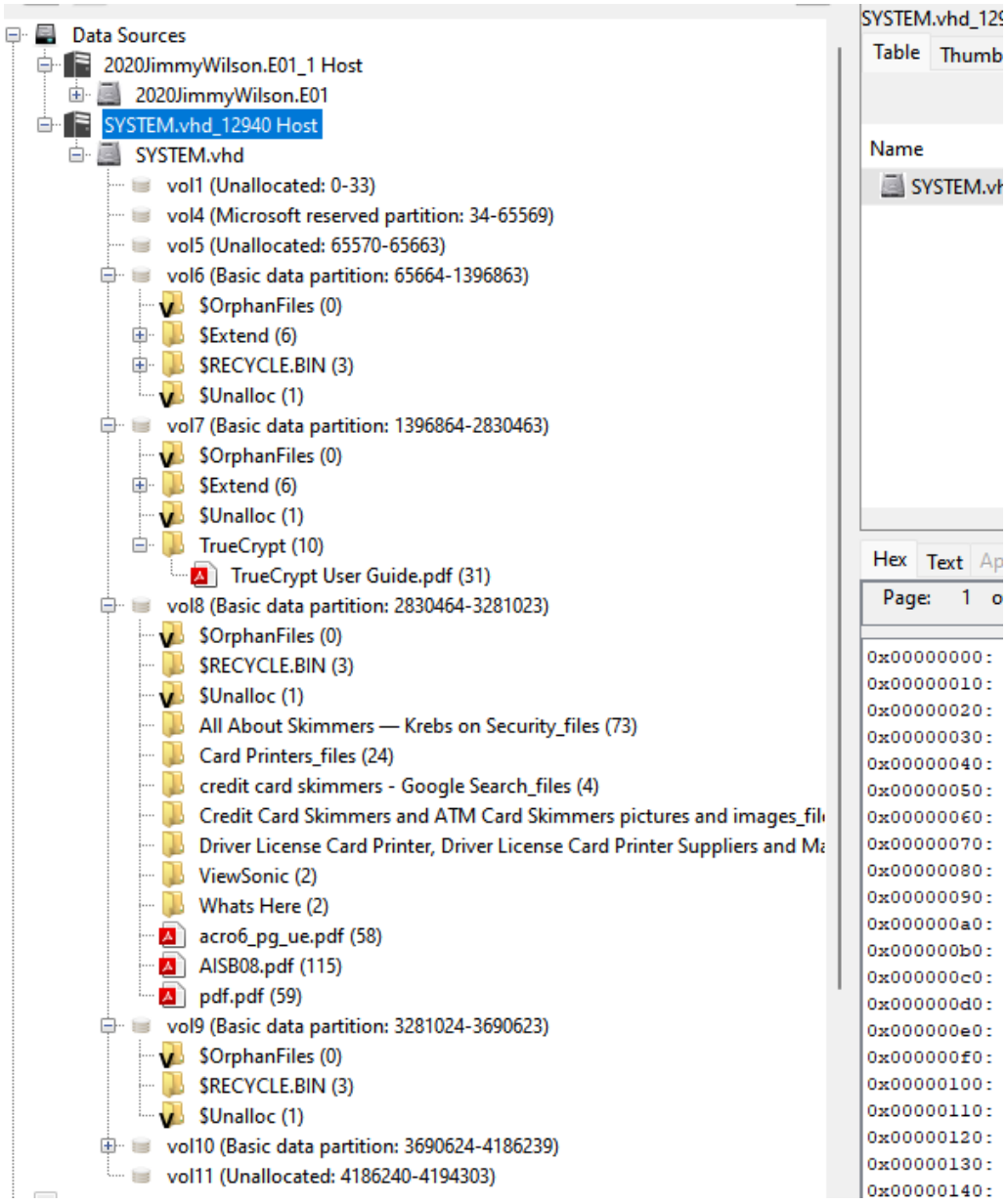


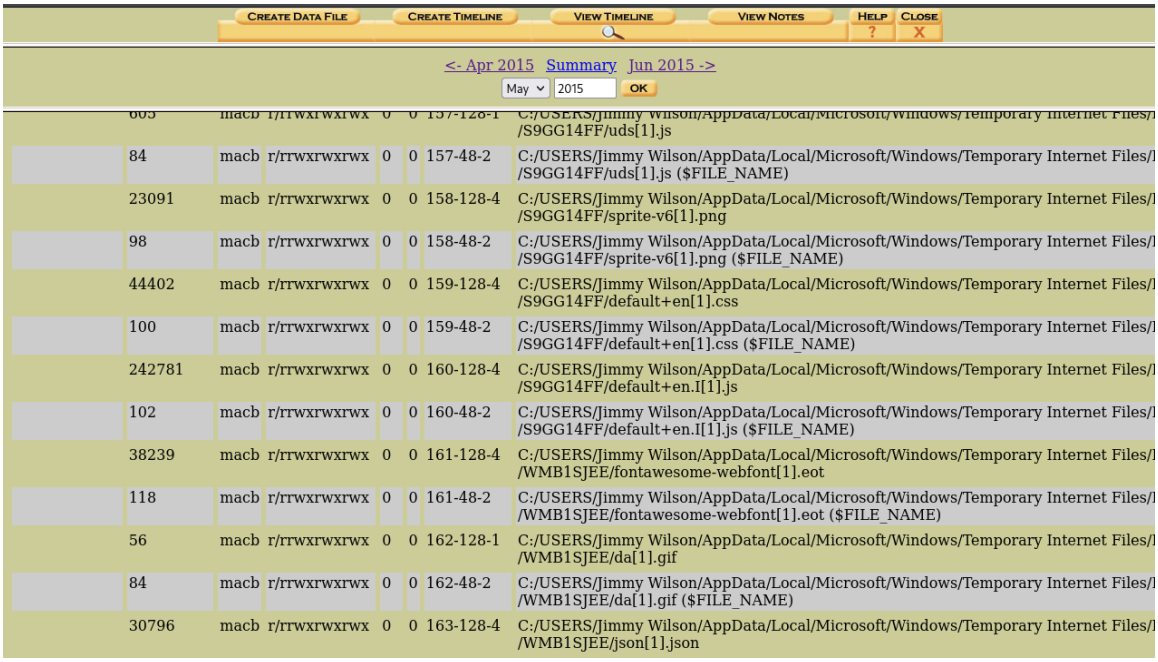
Figure 5.6: Hidden Encrypted Drive

The drive contains hidden files regarding card skimmers, printing driver licenses, and other files on hardware. Autopsy provides a lot of power in creating a case and file carving potential to see what may exist in a machine that may utilize for digital forensics. In the case provided by NIST, the image file of the machine being investigated, the user

was utilizing the machine for mischievous acts. This application was used on a Windows based Computer and performs similar to what Kali and CAINE have built into their applications.

5.8 Similarities between Autopsy, Caine, and Kali

The 3 are or includes Autopsy as the core forensic tool for data analysis. The difference between the current Autopsy installation as its own suite, is that it has an interactive Gui. Both Kali and CAINE have an older revision of the tool. The program is run through an internet browser. All the data that is shown is done via html output and forms of lists.



	84	macb	r/rrwxrwxrwx	0	0	157-48-2	C:/USERS/Jimmy Wilson/AppData/Local/Microsoft/Windows/Temporary Internet Files/I /S9GG14FF/uds[1].js ($FILE_NAME)
	23091	macb	r/rrwxrwxrwx	0	0	158-128-4	C:/USERS/Jimmy Wilson/AppData/Local/Microsoft/Windows/Temporary Internet Files/I /S9GG14FF/sprite-v6[1].png
	98	macb	r/rrwxrwxrwx	0	0	158-48-2	C:/USERS/Jimmy Wilson/AppData/Local/Microsoft/Windows/Temporary Internet Files/I /S9GG14FF/sprite-v6[1].png ($FILE_NAME)
	44402	macb	r/rrwxrwxrwx	0	0	159-128-4	C:/USERS/Jimmy Wilson/AppData/Local/Microsoft/Windows/Temporary Internet Files/I /S9GG14FF/default+en[1].css
	100	macb	r/rrwxrwxrwx	0	0	159-48-2	C:/USERS/Jimmy Wilson/AppData/Local/Microsoft/Windows/Temporary Internet Files/I /S9GG14FF/default+en[1].css ($FILE_NAME)
	242781	macb	r/rrwxrwxrwx	0	0	160-128-4	C:/USERS/Jimmy Wilson/AppData/Local/Microsoft/Windows/Temporary Internet Files/I /S9GG14FF/default+en.I[1].js
	102	macb	r/rrwxrwxrwx	0	0	160-48-2	C:/USERS/Jimmy Wilson/AppData/Local/Microsoft/Windows/Temporary Internet Files/I /S9GG14FF/default+en.I[1].js ($FILE_NAME)
	38239	macb	r/rrwxrwxrwx	0	0	161-128-4	C:/USERS/Jimmy Wilson/AppData/Local/Microsoft/Windows/Temporary Internet Files/I /WMB1SJEE/fontawesome-webfont[1].eot
	118	macb	r/rrwxrwxrwx	0	0	161-48-2	C:/USERS/Jimmy Wilson/AppData/Local/Microsoft/Windows/Temporary Internet Files/I /WMB1SJEE/fontawesome-webfont[1].eot ($FILE_NAME)
	56	macb	r/rrwxrwxrwx	0	0	162-128-1	C:/USERS/Jimmy Wilson/AppData/Local/Microsoft/Windows/Temporary Internet Files/I /WMB1SJEE/da[1].gif
	84	macb	r/rrwxrwxrwx	0	0	162-48-2	C:/USERS/Jimmy Wilson/AppData/Local/Microsoft/Windows/Temporary Internet Files/I /WMB1SJEE/da[1].gif ($FILE_NAME)
	30796	macb	r/rrwxrwxrwx	0	0	163-128-4	C:/USERS/Jimmy Wilson/AppData/Local/Microsoft/Windows/Temporary Internet Files/I /WMB1SJEE/json[1].json

Figure 5.7: Autopsy in Kali and CAINE

Seeing that Autopsy provides a timeline style output, the comparison to other software available provide similar functionality like FTK.

5.9 FTK 8.0

FTK is a very powerful tool that can replicate Autopsy functionality and much more. Similarities to Autopsy are available. On the left pane of the application, after

having a case created and disk image stored and loaded, you can see file artifacts as shown with Autopsy.

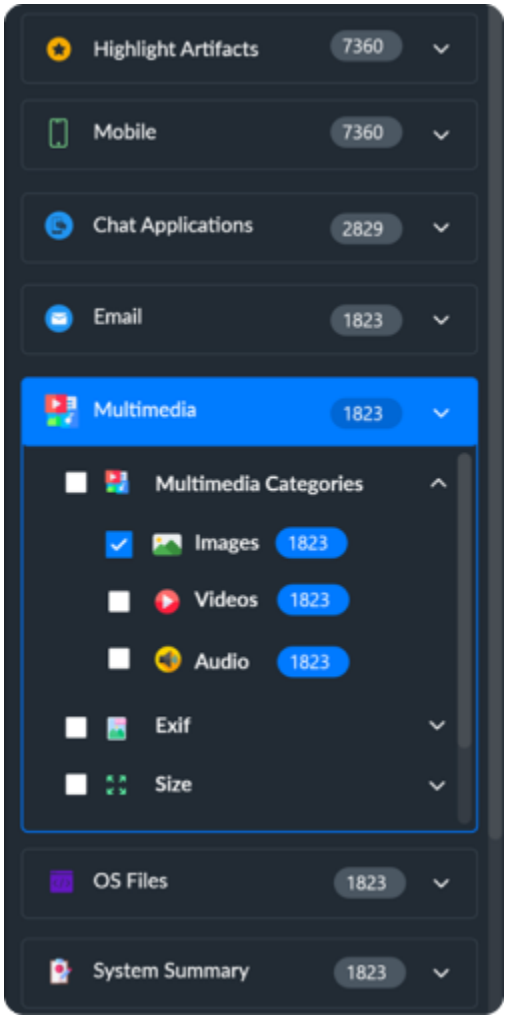


Figure 5.8: FTK 8.0 Data Artifacts options

In addition, the timeline feature is given. With the timeline, you can review file creation, deletion, location, etc.... There is ease of understanding file properties, but Autopsy provides it as best as it can without the price tag on its program. As the image is shown below, the structure and interface seem friendlier than what Autopsy was giving us, but that just affects convenience rather than overall functionality. This leads to

showing a similar program name Magnet, similar function, with slightly different interface.

Figure 5.9: FTK 8.0 Timeline

5.10 Magnet Axiom

Magnet's tools is similar to FTK but have a bit of a different was of interaction. The tool can analyze disk images as well as cloud storage, mobile phone, and other online based services. The functionality of filtering data artifacts still coexists as well as an interactive timeline to trace actions, logs, and files. The Data artifacts are sorted into sections as well. Rather than having an interactive feature of type of multimedia or file type it may be, it is filtered according to file extension and type.

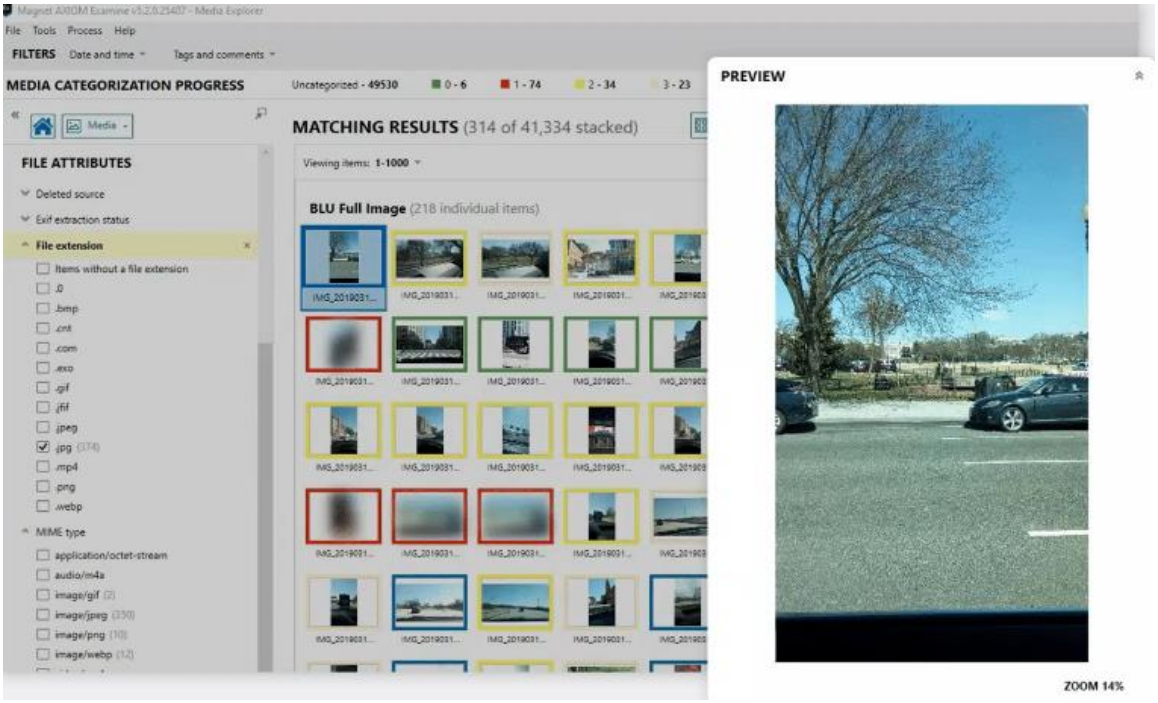


Figure 5.10: Magnet Axiom Data Artifacts

Magnet also provides a timeline system to pinpoint computer actions, file alternations, program installations as well as any artifacts that can be found within the investigated system. The timeline that Magnet provides is very similar to the one that Autopsy provides. The best part of the Magnet timeline is that it allows changes to the timeline according to what is being investigated. There are functions to create a timeline according to data artifacts and/or files and folders. In addition, the timeline can filter out

anything with just a search clause. This is convenient to find files fast as it will pinpoint all locations and does not require digging through the whole timeline to discover.

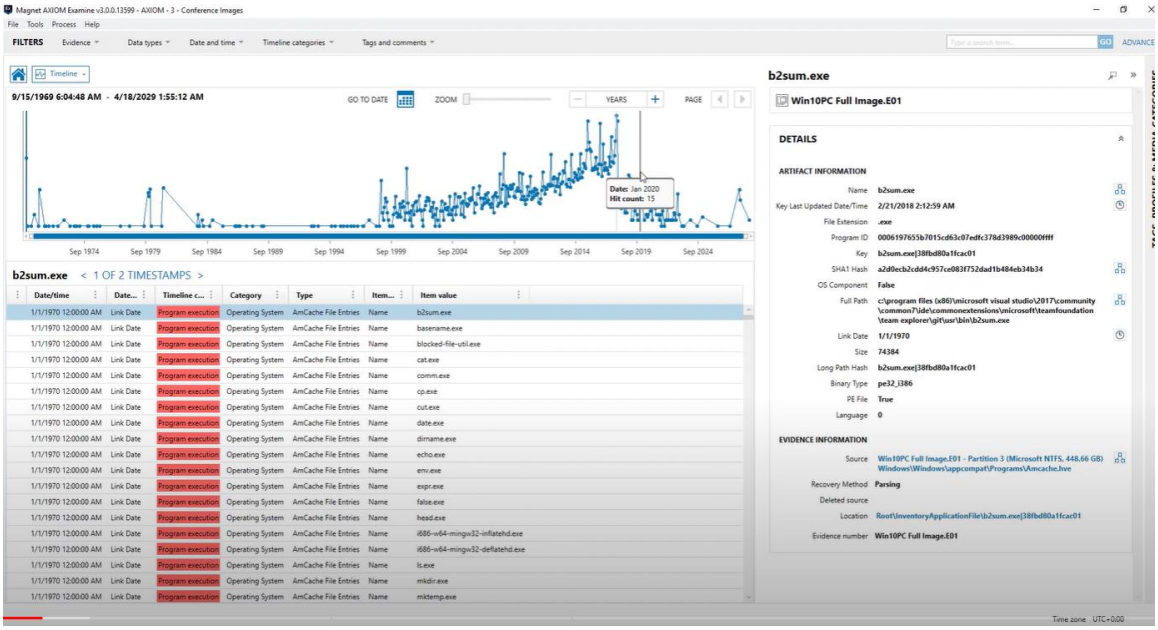


Figure 5.11: Magnet Axiom Timeline

After viewing these features enriched software, sometimes a simple explorer style application is useful. Pancake Viewer is file explorer version of Magnet Axiom with just simple functions.

5.11 Reviewing case with Pancake Viewer

Pancake Viewer is open using command prompt and the command, “Python pancakeViewerApp.py” and the following window opens.

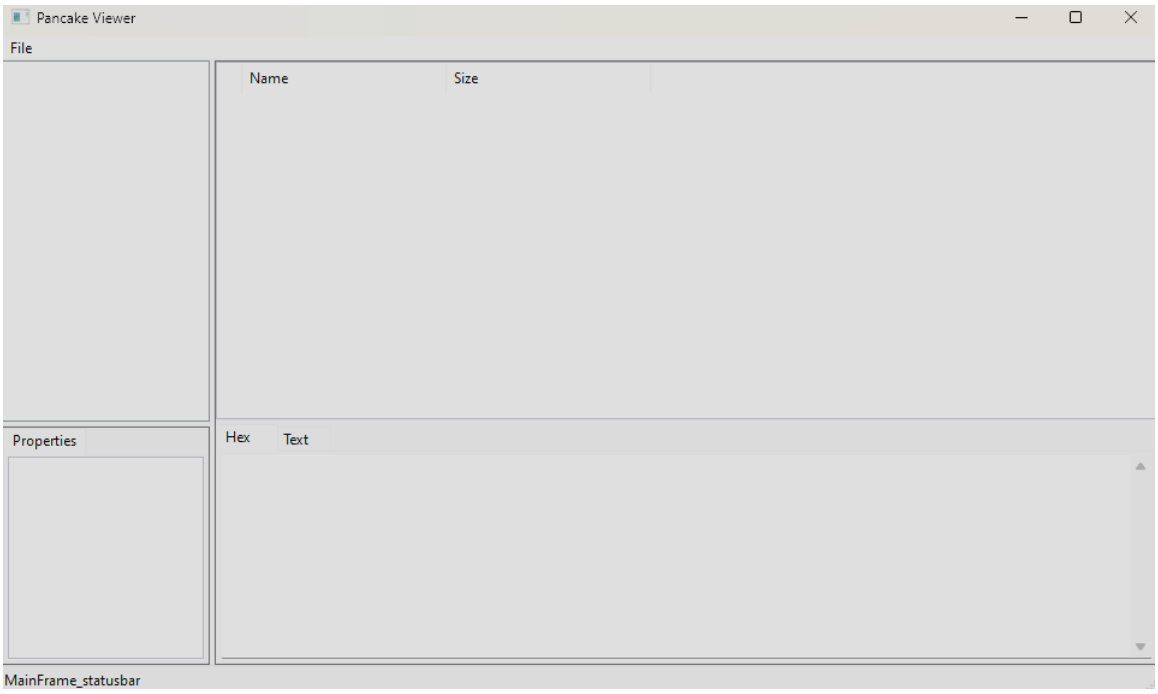


Figure 5.12: PancakeViewerApp

The case file will be open using the File tab on the upper left corner, and the open image option will be clicked. File explorer will open and the disk image file will be selected. The image file opens up and the disk image tree can be expanded by double clicking. After digging around the file system, evidence was found in the recycle bin, hidden in a folder. The files present is a non-encoded file as well as an encrypted file by BC TextEncoder.

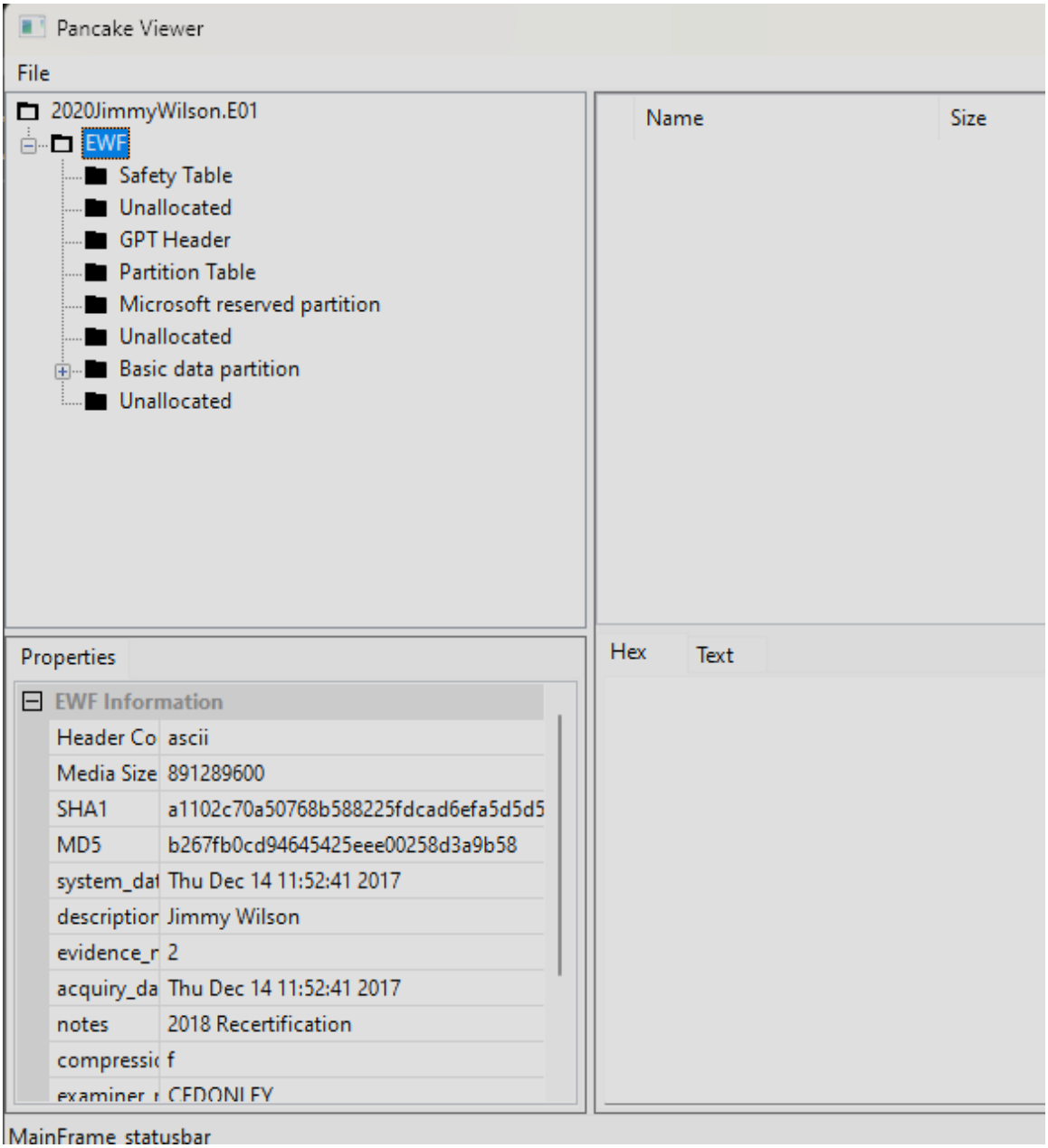


Figure 5.13: Pancake Viewer Disk Tree

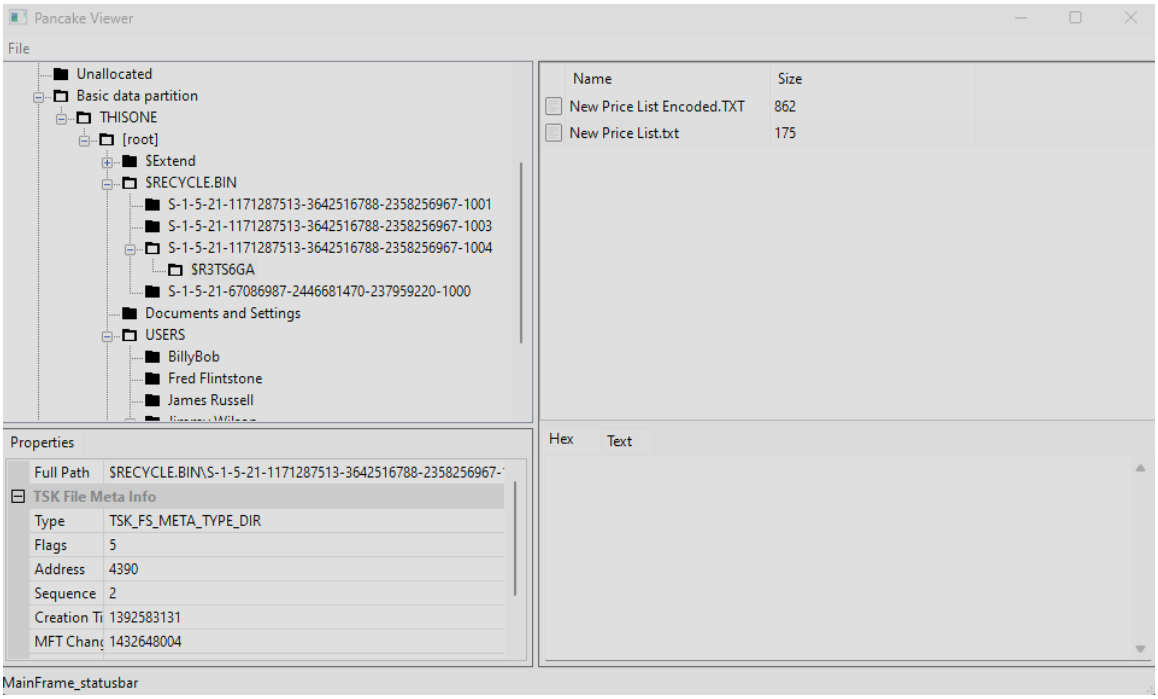


Figure 5.14: Pancake Viewer Recycle Bin

After reviewing this application, evidence was found of a pricelist for forged documents. The file was extracted and reviewed outside the application.

6. Analysis

With the facts that were given from the written sources, open-source forensic tools are a viable tool to be used with any critical machine. Most closed source tools have been based on the open tools but modified to serve a convenient close source tool.[4] Reviewing the capabilities of the popular tools for digital forensics, they really show their capabilities alongside with the open-source tools.[3] The usage of various tools is built in into a big suite to enhance functionality. Autopsy has expansion to grow with add on modules. Since Autopsy is open source, there are 3rd party sources that provide addons. Kali Linux and CAINE provide enhancements to functionality by providing external applications that may assist with specific functions. This includes opening pdf files and text files with either a text editor or pdf readers. The use of compiling the source code pancake reader, a lot was discovered with its capabilities as well as its dependencies that are required to make it work. As a unique application in which does not come as an installer, a lot was learned with understanding. Certain dependencies are updated almost bi monthly or sooner.

7. Conclusion

After analyzing Open-Source software with Closed-Source tools, they are both as effective to conduct most kinds of digital forensics. Depending on the case and usage of the tools, they provide various capabilities from file carving, to decrypting and recovering lost files. The major difference between open and closed source is the efficiency of keeping everything in one case file for modularity and convenience. Essentially a tool that is able to view an archived version of a complete physical disk image is satisfactory for most cases. Also, to be able to review it without affecting the integrity of its contents is a must. Insuring memory integrity of the host disk image ensures case to be unaltered.

After reviewing the content of each of the sources, we can conclude that in real case scenarios, enough evidence is contained with just the use of one open-source software. Autopsy provides enough features to take care of most cases and is completely free. There are premium features built into it and can be expanded at the discretion of the users or company. Also, Pancake Viewer provides basic functionality to review contents on both physical disk and archived disk images. It supports multiple platforms since it is python based and all its dependencies can be built within python ecosystem. Both Autopsy and Pancake Viewer can open disk image and provide a valid case with evidence of a user who is behind selling forged documents.

8. Bibliography

[1] S. Shiaeles, A. Chryssanthou, and V. Katos, “On-scene triage open source forensic tool chests: Are they effective?,” *Digital Investigation*, vol. 10, no. 2, pp. 99–115, Sep. 2013, doi: 10.1016/j.diin.2013.04.002.

[2] B. Carrier, “Open Source Digital Forensics Tools: The Legal Argument”.

[3] A. R. Javed, W. Ahmed, M. Alazab, Z. Jalil, K. Kifayat, and T. R. Gadekallu, “A Comprehensive Survey on Computer Forensics: State-of-the-Art, Tools, Techniques, Challenges, and Future Directions,” *IEEE Access*, vol. 10, pp. 11065–11089, 2022, doi: 10.1109/ACCESS.2022.3142508.

[4] M. Gengenbach *et al.*, “OSS4EVA: Using Open-Source Tools to Fulfill Digital Preservation Requirements,” *The Code4Lib Journal*, no. 34, Oct. 2016, Accessed: Jan. 05, 2023. [Online]. Available: https://journal.code4lib.org/articles/11940?utm_content=buffer0aaaa@utm_medium=social&utm_source=twitter.com&utm_campaign=buffer

[5] B. FitzGerald, P. L. Levin, and J. Parziale, “Open Source Software & the Department of Defense,” Center for a New American Security, 2016. Accessed: Mar. 14, 2023. [Online]. Available: https://www.jstor.org/stable/resrep06252

[6] B. V. Prasanthi, “Cyber Forensic Tools: A Review,” *International Journal of Engineering Trends and Technology*, vol. 41, pp. 266–271, Nov. 2016, doi: 10.14445/22315381/IJETT-V41P249.

[7] S. Mandecha, K. Raychaudhuri, M. George, and The Society of Digital Information and Wireless Communication, “A Comparative Study of the Performance of Open-

Source and Proprietary Disk Forensic Tools in Recovery of Anti-Forensically Doctored Data," *International journal of cyber-security and digital forensics*, vol. 8, no. 4, pp. 250–261, 2019, doi: 10.17781/P002624.

[8] *Kali Tools*, https://kali.org/tools

[9] CAINE, https://www.caine-live.net/

[10] Autopsy, https://www.autopsy.com/

[11] Exterro, https://www.exterro.com/ftk-8-0

[12] Magnet Forensics, https://www.magnetforensics.com/products/magnet-axiom/

[13] CFREDS, https://cfreds.nist.gov/

[14] GitHub, https://github.com

Vita

After exploring career paths at MacArthur High School, Houston, Texas, in 2014, Erik Herrera accepted admission at Stephen F. Austin State University at Nacogdoches, Texas. In between Summer terms, he attended Lonestar Community College. He received the degree of Bachelor of Arts from Stephen F. Austin State University in December 2018. After 3 years of employment, he entered the Graduate School of Stephen F. Austin State University, and received the degree of Master of Science in August of 2024. During the graduate program, he was working full time staff for Stephen F. Austin State University.

Permanent Address: 2129 Melissa Street
Houston, Texas 77039

Manuscript written in IEEE

This thesis was typed by Erik Herrera