Exploring Free Computer Forensics Applications for Digital Investigations

Author: Wilson Alicea
Advisor: Alfredo Cruz, PhD
Electrical and Computer Engineering and Computer Science Department

Abstract

In the realm of digital investigations, the utilization of effective forensic tools is paramount for the analysis and recovery of crucial data. This report, titled "Exploring Free Computer Forensics Applications for Digital Investigations," provides a comprehensive overview of six prominent free applications that serve as invaluable resources for forensic practitioners. This report includes tutorials that guide users through the functionalities and applications of each tool, highlighting their unique features, ease of use, and effectiveness in various forensic scenarios. By providing insights into these free resources, the report aims to empower investigators and enhance their skill sets in conducting thorough digital investigations, ultimately contributing to the advancement of the field of computer forensics.

Introduction

In an era marked by the rapid advancement of technology and the increasing prevalence of cybercrime, the field of digital forensics has become essential for law enforcement, corporate security, and personal data protection. Digital forensics involves the recovery, analysis, and presentation of data from digital devices, which can be crucial in legal proceedings and investigations. As cyber threats evolve, so does the need for effective forensic tools that can assist investigators in uncovering digital evidence. These applications will remain a cornerstone of cybersecurity and digital forensics, helping to address the challenges posed by cybercrime.

Background

Computer forensics tools are developed to retrieve, inspect, and analyze data stored on electronic devices such as computers, smartphones, and tablets. They enable forensic investigators to understand what happened during an incident by examining digital artifacts, recovering deleted files, and analyzing user activity. These tools can handle various tasks, including Data Recovery, Timeline Analysis, Keyword Search and Web Artifacts Extraction. The landscape of computer forensics applications includes a variety of tools, each with its unique capabilities. Some tools focus on specific tasks, such as Disk Imaging, Network Forensics and Memory Analysis. The rise of cyber threats has made computer forensics applications increasingly vital in cybersecurity. They help organizations respond to incidents, comply with legal requirements, and protect sensitive information. By utilizing these tools, forensic investigators can provide critical evidence in legal cases, support incident response efforts, and enhance overall security posture.

Problem

In the field of computer forensics, professionals often rely on a variety of specialized applications to gather, analyze, and preserve digital evidence. Despite the availability of free digital forensics tools, there is limited understanding of their effectiveness and usability in real-world scenarios. Many practitioners may be unaware of these resources or how to utilize them effectively. This gap in knowledge can hinder the ability to conduct thorough investigations, particularly for those without the budget for premium forensics software. This project aims to fill this gap by creating a tutorial and evaluating six free computer forensics tools, providing a detailed analysis of their strengths and weaknesses.

Methodology

A tutorial of six free computer forensics apps was developed that will mainly help students entering PUPR Cyber Security program, understand the academic aspects of cybersecurity specially in computer forensics and understand the academic aspects of it and instruct them through resources to guide them to acquire new skills and knowledge for professional development in cybersecurity in the field of computer forensics. The selection of these applications was based on the following criteria: *Functionality*, *User Accessibility* and *Community Support*. Their logos are shown in Figure 1.

Figure 1
Free Computer Forensics Apps Logos

The six free computer forensics apps are *Ophcrack* [1] (see Figure 2), *Autopsy* [2], *Bulk Extractor* [3], *FTK Imager* [4], [5] (see Figure 3), *Magnet RAM Capture* [6], *Network Miner* [7] were installed and setup in a windows computer to test their functionality.

Figure 2
Ophcrack LiveCD Setup

Figure 3
FTK Image Install

Each application was subjected to specific testing scenarios to evaluate its effectiveness:

- *Ophcrack*: Tested on a sample Windows system with known passwords to assess its recovery capabilities [1].
- *Autopsy*: Analyzed a disk image containing various file types, focusing on file recovery and timeline analysis [2] (see Figure 4).
- *Bulk Extractor*: Applied to a disk image to extract email addresses, URLs, and other artifacts, measuring its efficiency [3].
- *FTK Imager*: Utilized to create a forensic image of a USB drive and verify the integrity of the image using hash values [5].
- *Magnet RAM Capture*: Conducted a live capture of the physical memory (RAM) from a Windows machine for recovery and analysis of valuable data only found in memory [6] (see Figure 5).
- *Network Miner*: Analyzed a pcap file to extract files and credentials transmitted over the network [7].

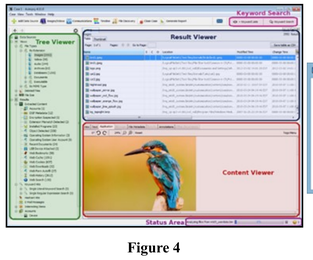

Figure 4
Autopsy User Interface

Figure 5
Magnet RAM Live Capture

Results and Discussion

These are the results for all the apps overall:

- When comparing to commercial alternatives, several factors are notable like usability and effectiveness.
- Practitioners should adhere to the following best practices like maintain data integrity, keep detailed records, document processes, use hashing and stay updated.
- To maximize these apps in forensic workflows, practitioners can combine with other tools, utilize plugins, regular updates, collaborative use and document processes.

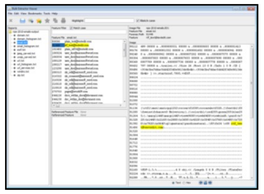

Figure 6
Bulk Extractor Progress Window

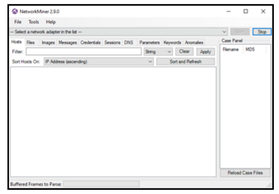

Figure 7
Network Miner User Interface

These are the specific results for all apps:

1) *Ophcrack v.3.8.0*:

- Key features include password cracking, Live CD/USB support, user-friendly interface and automatic detection.
- Users may encounter several challenges like limited password types, rainbow table limitations and learning curve.

2) *Autopsy v.4.21.0*:

- Key features include user-friendly interface, modular architecture, data analysis tools and case management.
- Users may encounter several challenges like learning curve, limited support and integration with others tools.

3) *Bulk Extractor v.1.6.0 (see Figure 6)*:

- Key features include data extraction, non-intrusive analysis and automated processing.
- Users of free tools often encounter several challenges like learning curve, limited support and integration issues.

4) *FTK Imager v.4.7.1*:

- Key features include forensically sound imaging, data preview, support for multiple formats, file carving and hashing capabilities.
- Users of FTK Imager may encounter several challenges like limited advanced features, learning curve and integration issues.

5) *Magnet RAM v1.20*:

- Key features include memory imaging, live capture, user-friendly interface and integration with other tools.
- Users of Magnet RAM Capture may encounter several challenges like limited advanced features, learning curve and integration issues.

6) *NetworkMiner v.2.9.0 (see Figure 7)*:

- Key features include traffic analysis, file extraction, session reconstruction, protocol analysis and user-friendly interface.
- Users of NetworkMiner may encounter several challenges like limited advanced features, learning curve and integration issues.

Conclusion

Leveraging the capabilities of these free computer forensics applications not only empowers investigators to uncover critical evidence but also promotes a greater understanding of digital forensics as a discipline. As cyber threats continue to evolve, staying informed about available tools and their functionalities will be essential for achieving successful outcomes in forensic investigations. I encourage users to explore these applications further, experiment with their features, and contribute to the growing body of knowledge within the digital forensics community.

Future Work

The completion of this paper meets the initial objectives and also have the space to implement future projects. Adding more content sections on each tutorial is one of the future implementations that will make these tutorials more advanced and specific in some areas of each free computer forensics apps covered in this paper. Also adding more than the six free apps for computer forensics used on this paper will also add more values to this project. There are hundreds of free apps for computer forensics out there and some are open-source apps that the community keeps adding more tools to them.

Acknowledgements

Thanks to my advisor Dr. Alfredo Cruz for the guidance , patience and advise.

References

[1] April Ashley (2023, December 20). “How to use ophcrack to Reset Password on Windows 10 in 2024” [Online]. Available: https://itoolab.com/windows-password/ophcrack-windows-10/?srsltid=AfmBOopjhVhpXZGwSSlx339-s69D5_M0zZ7DuxpADV64cWcMG7OIrXeb

[2] “Autopsy User Documentation 4.21.0. Autopsy User Guide” [Online]. Available: https://sleuthkit.org/autopsy/docs/user-docs/4.21.0/index.html

[3] Jessica R. Bradley, Simson L. Garfield (2015, March 23). “Bulk Extractor 1.4 User Manual.” [Online Document]. Available: http://digitalcorpora.org/downloads/bulk_extractor/BEUsersManual.pdf

[4] Access Data (2021, September 10). “Imager User Guide.” [Online Document]. Available: https://d1kpmuwb7gvu1i.cloudfront.net/Imager/4_7_1/FTKImager_UserGuide.pdf

[5] Blog Page (2022, September 5). “How to Create a Forensic Image with FTK Imager.” [Online] Available: https://www.geeksforgeeks.org/how-to-create-a-forensic-image-with-ftk-imager/

[6] Blog Page (2015, February 2). “Acquiring Memory with Magnet RAM Capture.” [Online]. Available: https://www.magnetforensics.com/blog/acquiring-memory-with-magnet-ram-capture/

[7] Erik Hjelmvik (2018, February 26). “Examining Malware Redirects with NetworkMiner Professional.” [Online] Available: https://www.netresec.com/?page=Blog&month=2018-02&post=Examining-Malware-Redirects-with-NetworkMiner-Professional