Exploring Free Computer Forensics Applications for Digital Investigations

Wilson Alicea Cortés
Master in Computer Science
Advisor: Alfredo Cruz, Ph.D.
Polytechnic University of Puerto Rico
Graduate Project EXPO, October 2024

Abstract *— In the realm of digital investigations, the utilization of effective forensic tools is paramount for the analysis and recovery of crucial data. This paper, 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. The applications examined include Ophcrack v.3.8.0, designed for password recovery through rainbow tables; Autopsy v.4.21.0, a powerful digital forensics platform for analyzing hard drives and smartphones; Bulk Extractor v.1.6.0, which excels in extracting useful information from disk images; FTK Imager v.4.7.1, known for its capability to create forensic images of data; Magnet RAM Capture v.1.20, a tool for capturing volatile memory; and Network Miner v.2.9.0, which aids in the analysis of network traffic. This paper 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.*

Key Terms *– Community Support, Cross-Tool Compatibility, Data Integrity and Preservation, Resource Limitations.*

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.

Figure 1
Free Computer Forensics Apps Logos

This paper focuses on six notable free computer forensics applications as shown in Figure 1: Ophcrack v3.8.0, Autopsy v4.21.0, Bulk Extractor v1.6.0, FTK Imager v4.7.1, Magnet RAM Capture v1.20, and Network Miner v2.9.0. Each of these tools offers unique functionalities that cater to different aspects of forensic investigations. For instance, Ophcrack is renowned for its password recovery capabilities, utilizing rainbow tables to efficiently crack Windows passwords. Autopsy serves as a comprehensive digital forensics platform, providing a user-friendly interface for analyzing hard drives and mobile devices.

Bulk Extractor stands out for its ability to extract useful information from disk images without the need for file system parsing, making it invaluable for data recovery tasks. FTK Imager is widely used for creating forensic images of storage devices, ensuring the integrity of evidence during investigations. Magnet RAM Capture specializes in capturing volatile memory from live systems, which is critical for understanding the state of a system at a specific moment. Lastly, Network Miner is a powerful tool for network forensics, capable of analyzing captured network traffic to reconstruct sessions and extract files.

The objective of this paper is to evaluate these applications in terms of their effectiveness, usability, and performance in real-world forensic scenarios. By providing detailed tutorials and analyses, this project aims to contribute to the understanding of how these free tools can be leveraged in digital forensic investigations, ultimately enhancing the capabilities of practitioners in the field. As the landscape of cybercrime continues to evolve, the development and utilization of accessible forensic tools will play a pivotal role in combating digital threats and ensuring justice.

PROBLEM STATEMENT

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 paper aims to fill this gap by evaluating six free tools, providing a detailed analysis of their strengths and weaknesses. However, the use of tools such as these presents several challenges that can impact the effectiveness and reliability of forensic investigations.

- *Data Integrity and Preservation*: One of the primary concerns in digital forensics is ensuring that the original evidence remains unaltered during the imaging and analysis process. Tools like FTK Imager are designed to create disk images without modifying the original data. However, there are instances where imaging can inadvertently alter data, particularly in volatile memory scenarios, which can compromise the integrity of the evidence.
- *Complexity of Analysis*: While tools like Autopsy provide a user-friendly graphical interface for analyzing file system artifacts and recovering deleted files, the sheer volume of data that needs to be processed can overwhelm investigators. The challenge lies in efficiently sifting through large datasets to identify relevant evidence, which can be time-consuming and requires a high level of expertise.
- *Cross-Tool Compatibility*: Different forensic tools often have varying capabilities and formats for data output. For instance, while Bulk Extractor excels at extracting specific data types from disk images, integrating its findings with those from Network Miner or Magnet RAM can be cumbersome. This lack of interoperability can hinder a comprehensive analysis and slow down the investigative process.
- *Resource Limitations*: Many forensic tools, including Ophcrack for password recovery, may require significant computational resources to operate effectively. In environments with limited hardware capabilities, the performance of these tools can be severely impacted, leading to delays in investigations.
- *Training and Expertise*: The effectiveness of these tools is heavily dependent on the skill level of the forensic investigator. As new features and updates are introduced, continuous training is necessary to keep up with the evolving landscape of digital forensics. This requirement can pose a barrier for organizations with limited training budgets or resources.

In summary, while tools like these are invaluable in the field of digital forensics, challenges related to data integrity, analysis complexity, tool compatibility, resource limitations, and the need for ongoing training must be addressed to enhance the effectiveness of forensic investigations.

PROJECT GOALS

The primary goal is to provide a detailed evaluation of six free computer forensics applications, offering a structured tutorial that demonstrates their functionalities, use cases, and comparative advantages. The tutorial will also

highlight any potential limitations or barriers to their adoption. By providing a thorough comparative analysis, the research aims to aid forensic professionals in selecting the appropriate tools for their specific investigative needs.

RESEARCH QUESTIONS

The questions below will guide me through in the development for each free computer forensics apps tutorials.

1. What are the key features and functionalities of the selected free computer forensics applications?
2. How do these tools compare to commercial alternatives in terms of usability and effectiveness?
3. What challenges do users face when employing these free tools for digital investigations?
4. How can practitioners maximize the utility of these applications in their forensic workflows?
5. What are the best practices for using these tools in forensic investigations?

RELEVANCE AND SIGNIFICANCE

This paper is relevant as it addresses the critical need for accessible digital forensics tools in an era of rising cybercrime. By providing a comprehensive analysis of free software options, the project aims to empower practitioners, enhance investigative workflows, and promote best practices in digital forensics. This paper is significant as it provides valuable insights for forensic investigators, helping them choose the most appropriate tools for their needs. It also contributes to the academic field by filling a gap in the literature regarding the comparative analysis of free forensic tools.

METHODOLOGY & DESIGN

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.

Selection Criteria

The selection of these applications was based on the following criteria:

- *Functionality*: Each app must provide essential features for digital forensics, such as data recovery, analysis, or evidence collection.
- *User Accessibility*: The tools should be free and open-source or have a free version available for educational purposes.
- *Community Support*: Preference was given to tools with active user communities and documentation to facilitate learning and troubleshooting.

Installation and Setup

- *Ophcrack*: This tool was installed on a Windows environment to test its ability to recover passwords [1] from Windows systems as shown in Figure 2. The installation process involved downloading the ISO file and creating a bootable USB drive [2], [3], [4].

Figure 2
Ophcrack Live CD

- *Autopsy*: Installed on a Windows system, Autopsy serves as a graphical interface for The Sleuth Kit as in Figure 3. The setup required installing dependencies and configuring the database [5].

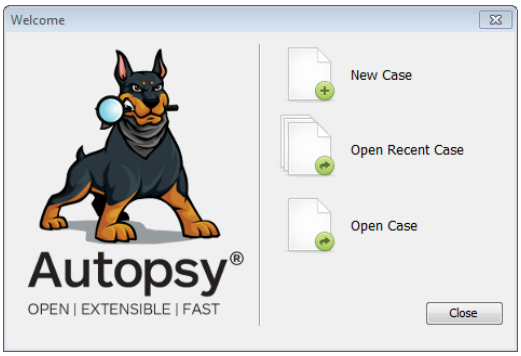

Figure 3
Autopsy Opening Splash Screen

- *Bulk Extractor*: Set up on a Windows machine [6], allowing for the extraction of useful information from disk images and files [7].
- *FTK Imager*: Installed on a Windows machine [8] as in Figure 4. Used to create forensic images of drives and analyze file systems [9].

Figure 4
FTK Imager Installer

- *Magnet RAM Capture*: This application was installed to capture volatile memory from a live system, requiring administrative privileges for proper functionality [10].
- *Network Miner*: Set up on a networked environment, it was used to analyze captured network traffic for forensic evidence [11].

Testing Scenarios

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

- *Ophcrack*: Tested on a sample Windows system with known passwords as shown in Figure 5 to assess its recovery capabilities [1].
- *Autopsy*: Used to analyze a disk image containing various file types, focusing on file recovery and timeline analysis [5]. Autopsy User Interface Layout components are a Tree Viewer (Green), Result Viewer (Blue), Content Viewer (Red), Keyword Search (upper right corner), Status Area (Purple) as shown in Figure 6.

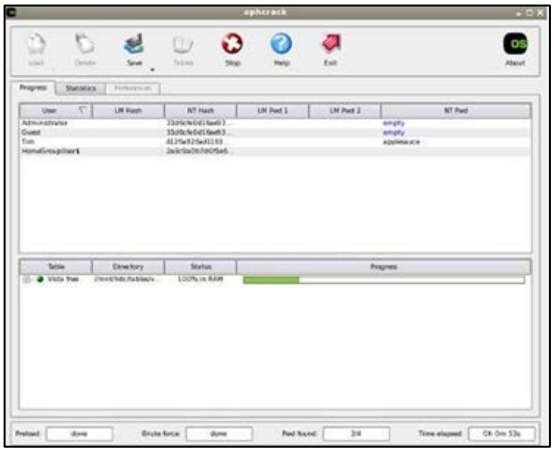

Figure 5
Ophcrack Password Recovery

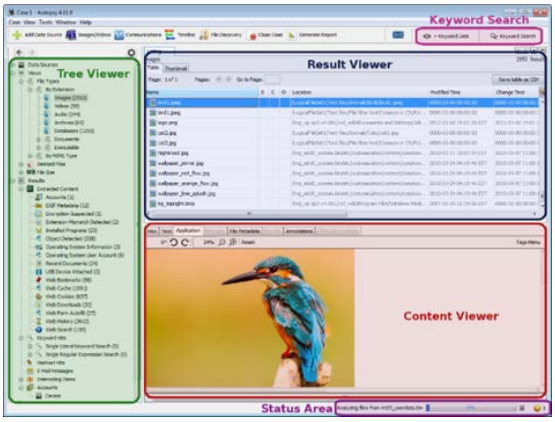

Figure 6
Autopsy User Interface Layout

- *Bulk Extractor*: Applied to a disk image to extract email addresses, URLs, and other artifacts, measuring its efficiency in data extraction [6]. Progress Window updates as bulk extractor is running, providing status information during the run and after the run is complete as shown in Figure 7.

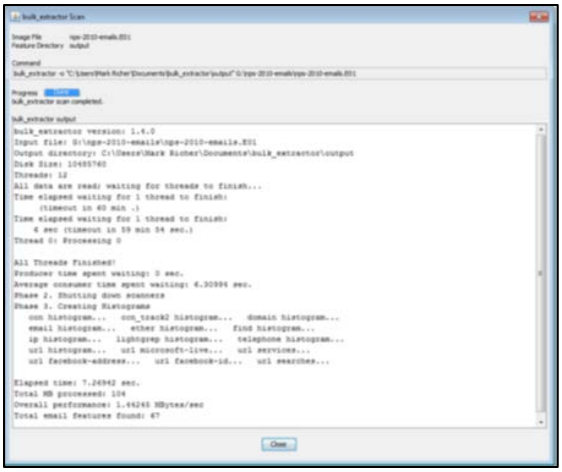

Figure 7
Bulk Extractor Progress Window

- *FTK Imager*: Utilized to create a forensic image of a USB drive and verify the integrity of the image using hash values [9]. FTK Imager Evidence User Interface could have deleted as well as overwritten data like in Figure 8.

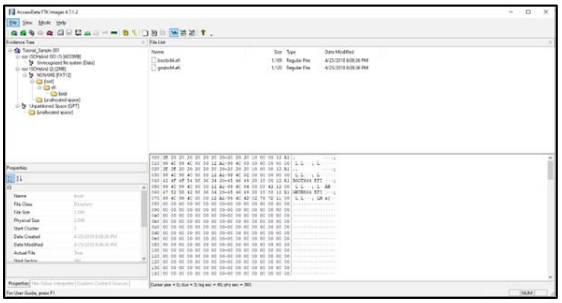

Figure 8
FTK Imager Evidence User Interface

- *Magnet RAM Capture*: Conducted a live capture of RAM (Fig. 9) from a Windows machine to analyze running processes and network connections [10]. A progress bar will provide the investigator with the status of the collection like in Figure 9.

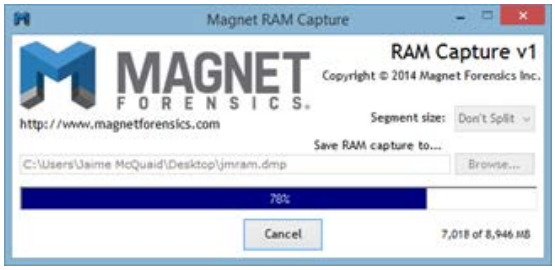

Figure 9
RAM Capture Progress

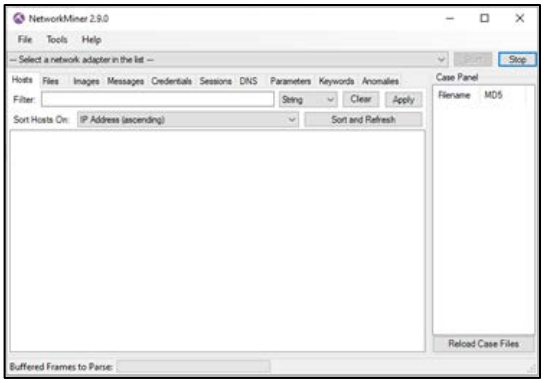

Figure 10
Network Miner User Interface

- *Network Miner*: Analyzed a pcap file to extract files and credentials transmitted over the network, assessing its ability to reconstruct sessions [11]. The User Interface is user-friendly and designed for ease navigation as shown in Figure 10.

Analysis and Evaluation

After conducting the tests, the results were analyzed based on:

- *Effectiveness*: How well each tool performed its intended function.
- *User Experience*: The ease of use and intuitiveness of the interface.
- *Performance*: Speed and resource consumption during operation.
- *Documentation and Support*: Availability of user guides, tutorials, and community forums for troubleshooting.

This methodology provides a structured approach to evaluating the selected computer forensics applications. By focusing on installation, testing, and analysis, we can effectively assess the capabilities and usability of each tool in real-world forensic scenarios. This evaluation will contribute to understanding the strengths and weaknesses of free computer forensics applications, aiding users in selecting the right tools for their needs.

RESULTS

I will explain part by part the results of the completion of this paper and how it relates to the

research questions that were explained in that section. These are the results for all the apps overall:

1. *Ophcrack v.3.8.0* - Key features include password cracking, Live CD/USB support, user-friendly interface and automatic detection. When comparing to commercial alternatives, several factors are notable like usability and effectiveness. Users may encounter several challenges like limited password types, rainbow table limitations and learning curve. To maximize the utility of Ophcrack in forensic workflows, practitioners can combine with other tools, regular updates and document processes. When using Ophcrack in forensic investigations, practitioners should adhere to the following best practices like preserve evidence integrity, use appropriate rainbow tables and keep detailed records.
2. *Autopsy v.4.21.0* - Key functionalities include user-friendly interface, modular architecture, data analysis tools and case management. When comparing to commercial alternatives, several aspects stand out like usability and effectiveness. Users may encounter several challenges like learning curve, limited support and integration with others tools. To maximize the utility of Autopsy in forensic workflows, practitioners can utilize plugins, regular training and collaborative use. When using Autopsy in forensic investigations, practitioners should follow these best practices like preserve evidence integrity, document findings and stay informed.
3. *Bulk Extractor v.1.6.0* - Key features include data extraction, non-intrusive analysis and automated processing. When comparing to commercial alternatives, several factors come into play usability and effectiveness. Users of free tools often encounter several challenges like learning curve, limited support and integration issues. To maximize the utility of Bulk Extractor in forensic workflows, practitioners can combine tools, automate processes and regular training. When using Bulk Extractor in forensic investigations, practitioners should adhere to the following best practices like maintain data integrity, document processes and stay updated.
4. *FTK Imager v.4.7.1* – Its key features include forensically sound imaging, data preview, support for multiple formats, file carving and hashing capabilities. When comparing FTK Imager to commercial alternatives, several factors emerge like usability and effectiveness. Users of FTK Imager may encounter several challenges like limited advanced features, learning curve and integration issues. To maximize the utility of FTK Imager in forensic workflows, practitioners can combine with other tools, regular training and document processes. When using FTK Imager in forensic investigations, practitioners should adhere to the following best practices like preserve evidence integrity, use hashing and keep detailed records.
5. *Magnet RAM v1.20* - Its key features include memory imaging, live capture, user-friendly interface and integration with other tools. When comparing Magnet RAM Capture to commercial alternatives, several aspects are noteworthy like usability and effectiveness. Users of Magnet RAM Capture may encounter several challenges like limited advanced features, learning curve and integration issues. To maximize the utility of Magnet RAM Capture in forensic workflows, practitioners can combine with other tools, regular training and document processes. When using Magnet RAM Capture in forensic investigations, practitioners should adhere to the following best practices: Preserve evidence integrity, use hashing and keep detailed records.
6. *NetworkMiner v.2.9.0* - Key features include traffic analysis, file extraction, session reconstruction, protocol analysis and user-friendly interface. When comparing NetworkMiner to commercial alternatives, several factors come into play like usability and effectiveness. Users of NetworkMiner may encounter several challenges like limited advanced features, learning curve and

integration issues. To maximize the utility of NetworkMiner in forensic workflows, practitioners can combine with other tools, regular training and document processes. When using NetworkMiner in forensic investigations, practitioners should adhere to the following best practices like preserve evidence integrity, use hashing and keep detailed records.

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.

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.

REFERENCES

[1] C. Tissieres. (2024). *ophcrack Howto* [Online]. Available: https://sourceforge.net/p/ophcrack/wiki/ophcrack%20Howto/. [Accessed: October 20, 2024].

[2] A. 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. [Accessed: October 20, 2024].

[3] Blog Page. (2024, October). *Rufus – Creating bootable USB drives* [Online]. Available: https://kb.filewave.com/books/filewave-general-info/page/rufus-creating-bootable-usb-drives. [Accessed: October 20, 2024].

[4] Forum Page. (2008, March). *ImgBurn Guides CD/DVD/BD Burning Guides* [Online]. Available: https://forum.imgburn.com/forum/4-guides/. [Accessed: October 20, 2024].

[5] The Sleuth Kit. (2024, Feb. 6). *Autopsy User Documentation 4.21.0*. *Autopsy User Guide* [Online]. Available: https://sleuthkit.org/autopsy/docs/user-docs/4.21.0/index.html. [Accessed: October 20, 2024].

[6] J. R. Bradley & S. L. Garfield. (2015, March 23). *Bulk Extractor 1.4 User Manual* [Online]. Available: http://digitalcorpora.org/downloads/bulk_extractor/BEUsersManual.pdf. [Accessed: October 20, 2024].

[7] B. Allen (2014, June 19). *Bulk Extractor* [Online]. Available: https://github.com/simsong/bulk_extractor/wiki/Installing-bulk_extractorhttp. [Accessed: October 20, 2024].

[8] Access Data. (2021, September 10). *Imager User Guide* [Online]. Available: https://d1kpmuwb7gvu1i.cloudfront.net/Imager/4_7_1/FTKImager_UserGuide.pdf. [Accessed: October 20, 2024].

[9] GeeksforGeeks. (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/. [Accessed: October 20, 2024].

[10] Magnet Forensics. (2015, February 2). *Acquiring Memory with Magnet RAM Capture* [Online]. Available: https://www.magnetforensics.com/blog/acquiring-memory-with-magnet-ram-capture/. [Accessed: October 20, 2024].

[11] E. 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. [Accessed: October 20, 2024].