Group Project:
Forensic tools for computers and networks

Academic Year & Quarter: 2022 Spring for Professor: L. Slusky

Class: CIS 4370 Security Risk Management

___

Group: 1

___

Student: Vanessa Munoz

Abstract

Technology is advancing every day, and forensic tools for computers and networking is no different. However, with such powerful tools available, it does raise some questions in regard to its cyber security and how well a company or business should be if they decide to employ the technology. And accuracy, how reliable the technology is within their work organization, and whether it can be trusted to make the right decisions. In addition, the terminology of "computer forensics" is essential for all cyber security users. As an outcome, forensic tools for computers and networking are now available for everyone. As computers and mobile devices become more technologically advanced, new security methods will become highly beneficial to the security area.

Modern Technology can be described as a window into both our lives and the lives of criminals. There was a distinction between the virtual and physical worlds in this metaphor. As technology advances, this division is no longer an issue. Technology is inextricably linked to our daily life, always present and active. As technology evolves and advances worldwide, our paper presents the basic concepts of "Forensic tools for computer and networking." It will address the terminology on Forensic tools, explain the different experiences using forensic tools for computers and networking, and represent the significant impacts that forensic tools have made in history.

Principles of Forensic Tools

Terminology of Forensic Tools

There are many different definitions of forensic tools for computers and networking. According to the book called Digital Evidence and Computer Crime: Forensic Science, Computers, and the internet, "The term computer forensic usually refers to the forensic examination of computer components and their contents such as hard drives, compact disks, and printers. However, the term is sometimes used more loosely to describe the forensic examination of all forms of digital evidence (Casey E., 2011). The term "computer forensics" has been used by the information security community to represent a wide range of operations that have less to do with collecting data but more to do with protecting computer systems. The terminology of computer forensics has split into various subdisciplines, such as malware and mobile device forensics.

Digital Forensics

As forensic tools improve throughout many years, the phrase "digital forensics" has come to refer to the entire field. Digital forensics has many different meanings in technology. And it is a branch of forensic science, it also deals with rescuing, investigating, evaluating, and analyzing data stored on computers. Throughout many years, digital forensics has become increasingly essential in cases where electronic devices have been utilized to commit a crime in recent years. Digital forensic investigations began with a focus on criminal acts with computers. Still, the discipline has since extended to cover a variety of devices where digitally stored information can be modified and utilized for various criminal acts. In this article called New Improvement In Digital Forensic Standard Operating Procedure, "Executing evidence collection in digital forensic investigation is completely different compared to other evidence collection such as blood, tool mark, and fibers (Brill & Pollitt, 2006). In both law enforcement and business, digital forensic investigations are increasingly widespread. Also, with the rapid advancement of technology, investigators can now utilize a variety of different ways to determine the underlying cause of a crime. Digital forensics is a collection of tasks, steps, or sub-processes that are carried out during an investigation. As a result, a digital forensic method must be adaptable enough to accept various technologies.

Accuracy of Forensic Tools

A principle of forensic tools that is crucial is accuracy. In an article titled Public beliefs about the accuracy and importance of forensic evidence in the United States, "Recent advances in forensic science, especially the use of DNA technology, have revealed that faulty forensic analyses may have contributed to miscarriages of justice" (Jacob K., Shichun L., Maria C., 2020). In this article, the researcher discovered that respondents feel forensics is far from ideal, with accuracy ratings ranging from 55% for voice analysis to 83% for DNA analysis, with the majority of procedures falling between 65 and 75% accurate. However, many people still believe that forensic evidence is vital for any criminal case. As fictional shows start portraying forensic science to look very realistic, most of the United States do not believe they are flawless or even close to the perfect portrayal of forensic science techniques. With different forensic tools still improving, it is still ideal for everyone to explore these tools today.

Methods of Forensic Tools

The Methodology of Forensic Tools

Cybercrime is a type of crime and it also occurs in the virtual world. The method of detecting such crimes is known as digital forensics. Digital forensic tools development is tremendously popular in the digital world. As researchers use mobile forensic tools, data should not be altered once it is captured, as this is the only way to recover evidence in its original state. The main aspect of forensic tools is that after a file or data is recovered, it'll preserve the file's original content and see if the extracted information has been altered. In the case of cybercrime, forensic tools strive to defend against identity theft and money laundering while also keeping privacy and prohibiting unwanted access to personal and confidential information. As technology advances and there is more non-reporting of cybercrime, it isn't easy to catch cybercriminals. According to an article called Layered Framework for Mobile Forensics Analysis, "Lack of technical knowledge of handling tools may lead to damage of crucial evidence while lack of standard legislation imposes legal challenges. Extracting and preserving evidence present on mobile devices in a proper manner is also important. Noting down each and every step and activity performed while carrying out the forensic process is essential, therefore documentation is necessary" (Goel M. & Kumar V., 2019). As cybercrime increases rapidly, examiners need to use forensic tools and thoroughly understand how they work. One device that everyone uses is a mobile phone. There's a lot of information on mobile phones where criminals have hacked call records, messages sent and received, and internet history. For Android phones, Autopsy, and MOBILedit are helpful applications, whereas, for iOS phones, iBackup Extractor and iPhone Analyzer are also useful. However, one instrument is defective to finish the research process correctly. As a result, investigators employ a variety of tools in coordination to complete the forensic procedure. Cybercriminals can now be blocked on our laptops and computers with many useful applications. However, cybercriminals can still hack our mobile devices. It is helpful to research the best applications for our mobile devices that'll block cybercriminals from reaching our private information.

Digital Forensic Investigation

Digital forensics is critical for effective punishment to digital criminals who use various digital devices, including computers, networks, mobile phones, and storage devices. Within a court of law, lawyers would use digital forensic evidence to retrieve proof within their cases.

As a result, many necessary procedures must be considered in order to conduct an effective digital forensic inquiry. According to this article called Mapping Process of Digital Forensic Investigation Framework, "Digital investigation is a process to answer questions about digital states and events. In contrast, a digital forensics investigation is a special case of a digital investigation where the procedures and techniques that are used will allow the results to be entered into a court of law" (Siti S., Robiah Y., Shahrin S., 2008). The digital crime scene, according to them, is a virtual environment generated by software and hardware in which digital proof of a crime or incident exists. This framework divides the process into five categories, each containing 17 phases. Readiness phases, physical crime scene investigation phases, digital crime scene investigation phases, and review phases are the different grouping phases. Studying the different phases has led to developing a framework to find faster forensic examinations. This article has also defined critical activities in the collection process, such as collecting images of effected computers collecting logs of intermediate devices. The collection logs primarily process records on the internet and data from intrusion detection systems, firewalls, and other similar devices. As an outcome, a few essential procedures must be considered in order to conduct an effective forensic inquiry. There are hundreds of digital forensics investigative methodologies established all over the world in the field of digital forensics. Each organization develops its own procedures, with some focusing on technological issues like data collecting and analysis. As technology changes over time, most organizations have to deal with many different technologies used within their workspace. With technology transforming over time, many organizations have started using digital forensics and private securities to keep confidential work information out of reach from cybercriminals. With newer procedures used in the workspace, every organization can now store valuable information on their work laptop and computer.

Analysis of Forensic Tools

In order to prevent loss or destruction to the evidence collected, proper procedure must be followed during the forensic process; otherwise, the evidence will be useless. The steps of a forensic process are identification, acquisition, examination, analysis, and finally, reporting. These procedures often involve the use of forensic tools in a secure environment. In fact, the device used to conduct forensic analysis can be considered one. The Kali Linux virtual machine is an ideal system for information security, as it is natively equipped with all sorts of tools (and can be upgraded with additional [ones]" (Moric, Redzepagic, J., & Gatti, F., 2021). Experts should be familiar with whatever tools are used and be able to apply their knowledge to a forensic case.

The first step in a typical forensic analysis is identifying an incident and preparing to collect data, known as precollection. Forensic experts prepare to collect data after the identification process, where the system affected is noted, and records are made. An essential tool for any forensic investigation is a write blocker, a device that ensures the integrity of the evidence by permitting read-only access. If a physical write blocker is not available, software that performs the same task should be used.

Acquisition of the evidence from the affected systems can begin once the proper equipment and tools have been gathered and set up. This process aims to collect all data without damaging the evidence in the process. If the system is currently running, the technician should create an image of the computer to capture the computer's activity at the time. Capturing working memory like RAM is extremely important as it stores data on currently running processes, open files, and network connections. However, as it is volatile data, the memory must be captured as soon as possible before it is lost. A tool for capturing random access memory is 7-RAM capture, which extracts data to be analyzed by other tools. A tool for network connection is Xplico, which can glean information from active network connections captured by the image by analyzing network and internet captures. Multipurpose tools like Volatility are also alternatives. A forensic expert can use Browser history capturer by Foxton to analyze browsing history.

While collecting the data using the write blocker tool, the investigator must maintain the integrity of the evidence. To determine that, devices are used to create cryptographic hashes. It is a "type of mathematical function that creates a unique, fixed-size mathematical value from an arbitrary set of input values" (Moric, Redzepagic, J., & Gatti, F., 2021). The investigator will use a hash tool to generate a unique hash number when collecting evidence. Investigators can compare the hash number generated initially with a new one generated from the same file to ensure that the integrity of the evidence wasn't changed. Furthermore, the hash value can also be used to identify and sort through the evidence. Various hash programs available are the Message-Digest series, Secure hash algorithm series, WHIRLPOOL, and Hashdeep. While all these programs perform the same essential functions, particular programs specialize in specific functions, such as unpacking binary files. Once the integrity of the evidence has been confirmed, the forensic process can continue to the analysis phase.

As implied by the name, the analysis phase is analyzing the recovered data for helpful information. Several popular tools are available with common features that can perform forensic analysis; three standard tools are The Sleuth Kit, the Autopsy, and Encase.

One standard tool called The Sleuth Kit is used to analyze disk images and recover deleted information. It should find all files, including deleted or hidden ones, and display metadata. Another tool is The Autopsy which also runs The Sleuth Kit. Like other tools, it offers hash filtering and file system analysis. Finally, Encase, offered by Guidance Software, offers broad functions like the other tools and includes data recovery. The final step of the forensic process is reporting the information found. While there is no specific tool for this process step, tools like Encase offer reporting functions that create forensic reports.

Usability of Network Forensic Tools

The goal of network forensics is to capture, record, and analyze events in a network that may have been involved in an incident. Special tools are used to monitor network performance and detect potential issues, such as internal or external attacks. Special tools can also be used to track events and packets within a network, which is crucial for any computer network incident. While web forensic tools are beneficial in investigations, users must be familiar with the tools in order to use them to their fullest potential. In the article "Exploring user requirements of network forensic tools" by Kousik Barik, Saptarshi Das, Karabi Konar, Bipasha Chakrabarti Banik, and Archita Banerjee sought to gauge the knowledge local Indian cybersecurity experts had on these tools. To do this, they held a survey, asking about the respondent's familiarity with concepts and topics related to network forensics and gauging their opinion on these tools.

Their survey found that those interviewed agreed that finding and using the right tool for a particular forensic investigation is one of the most critical parts of the forensic process in general. The respondents interviewed favored using command-line programs as they believed that they offered greater flexibility and control than a graphical user interface. They noted a lack of support with some of the tools, especially if it was open source. As part of the survey, they compared five different forensic tools and six common capabilities. Then they presented their respondents with three case studies and presented them with tools to complete them. The surveyors found that respondents were familiar with the tools shown. The authors of the study concluded that respondents favored the flexibility of programs run with a command line. Nevertheless, they recognized that graphical-based interfaces are more user-friendly. However, the respondents suggested some features that they would like to see for open-source forensic tools, such as more accessible user feedback, better documentation, and better performance.

Future of Network Forensic Tools

As technology advances, so can the crimes that can occur involving them. As a result, the techniques and tools needed to adapt to the new situations, outlined in an article called "Digital Forensics Subdomains: The State of the Art and Future Directions". Network attacks have become more frequent and sophisticated, necessitating the development of the field of network security. There has been significant development in this field such as the development of a model that automatically detects and logs suspicious incidents or the development of a "'Forensics-as-a-Service" model which "offers an authorized environment subjects that can use to remotely control the forensics process" (Al-Dhaqm) allowing the cloud provider to handle data acquisition and data analysis. Another program offers the capability for rapid response to a possible incident by establishing a cooperative system.

Despite all these programs, the authors of the paper noted that many of these tools are designed to collect data instead of addressing the entire forensic process. While this does not make them not useful, it means that agencies available end up serving redundant purposes and rely on the actual analysis being done by people instead of being done or assisted by the available tools.

Conclusion

To summarize, there are many different kinds of forensic tools used today. For example, Digital Forensic tools are used within the court of law. Digital forensics refers to the forensic examination of computers involved in an incident but has expanded to broadly refer to the explanation of digital evidence. Experts rely on various digital forensic tools to conduct digital forensic investigations after an incident. Forensic tools play different critical roles throughout the steps of the digital forensic process, such as preventing the accidental tampering of evidence by the investigators themselves to analyze the data from affected systems. The different methods used in a forensic process are identification, acquisition, examination, analysis, and reporting. Understanding the fundamental strategies about forensic tools will be vital in the future for developing counter-action plans to maintain security and protection from cyberattacks.

In terms of the research gathered, to improve cybersecurity for all technology users and improve the Universities Information System research on cybersecurity. In our research, we will also discuss the importance of digital forensics. As a result, in order to perform an excellent forensic investigation, a few fundamental techniques must be considered. In the discipline of digital forensics, there are hundreds of investigative digital forensics approaches in use all around the world. These forensics tools should be easy and straightforward for professionals to use the full capability of devices. As technology evolves, most businesses are forced to cope with a variety of technologies in their workplace. As cyber threats continue to change, the tools needed to detect and take apart their attacks also need to adapt. Each company develops its own techniques, with some concentrating on technological challenges such as data collection and analysis.

References

Al-Dhaqm, Ikuesan, R. A., Kebande, V. R., Razak, S. A., Grispos, G., Choo, K.-K. R., Al-Rimy, B. A. S., & Alsewari, A. A. (2021). Digital Forensics Subdomains: The State of the Art and Future Directions. IEEE Access, 9, 152476–152502. https://doi.org/10.1109/ACCESS.2021.3124262

Barik, Das, S., Konar, K., Chakrabarti Banik, B., & Banerjee, A. (2021). Exploring user requirements of network forensic tools. Global Transitions Proceedings, 2(2), 350–354. https://doi.org/10.1016/j.gltp.2021.08.043

Casey, E. (2011). *Digital evidence and computer crime: Forensic science, computers, and the internet*. Academic press.

Goel, M., & Kumar, V. (2019, March). Layered framework for mobile forensics analysis. In *Proceedings of 2nd international conference on advanced computing and software engineering (icacse)*.

Ghazinour, K., Vakharia, D. M., Kannaji, K. C., & Satyakumar, R. (2017, September). A study on digital forensic tools. In *2017 IEEE international conference on power, control, signals and instrumentation engineering (ICPCSI)* (pp. 3136-3142). IEEE.

Kaplan, J., Ling, S., & Cuellar, M. (2020). Public beliefs about the accuracy and importance of forensic evidence in the United States. *Science & Justice*, *60*(3), 263-272.
Moric, Redzepagic, J., & Gatti, F. (2021). ENTERPRISE TOOLS FOR DATA FORENSICS. *Annals of DAAAM & Proceedings*, 98–. https://doi.org/10.2507/32nd.daaam.proceedings.014

Parveen, Khan, Z. H., & Ahmad, S. N. (2020). Classification and evaluation of digital forensic tools. Telkomnika, 18(6), 3096–3106. https://doi.org/10.12928/TELKOMNIKA.v18i6.15295

Perumal, S., & Md Norwawi, N. (2011). New improvement in digital forensic Standard Operating Procedure (SOP).

Selamat, S. R., Yusof, R., & Sahib, S. (2008). Mapping process of digital forensic investigation framework. *International Journal of Computer Science and Network Security*, *8*(10), 163-169.