AMITY UNIVERSITY DUBAI

Cyber Forensics

HOME ASSIGNMENT

STUDENT NAME- Jaden Ade
AUD- 15697

PROGRAMME- BSc (IT)
SEM- 5
TEACHER- Dr. Vinod Shukla

Index

Search and Seizures of E-Evidence & Policies Monitoring Systems

Introduction

Cyberforensics is a branch of forensic science that focuses on retrieving, gathering, and analyzing forensic evidence of materials found in electronic devices in relation with cybercrimes. Because of the extensive use of the internet and advancements in technology, cyberattacks are increasing. Cyber forensics is also used to gather electronic data and conduct an analysis that enables it to be utilized as admissible evidence in court when harmful evidence is found in a device or on a network. Additionally, it is employed to retrieve lost data from a system. The information gathered is used to prosecute a criminal.

Attacks by malware on electronic devices as well as crimes against the internet have become more frequent. Computer evidence is being used in criminal prosecutions, accounting for about 85% of all cases now. Digital forensics currently lacks a set of security features comparable to those for computer security, which lists confidentiality, integrity, and availability as its three main criteria. If computer forensics attributes have not yet been specified, there is no documented mechanism to characterize an IT system's forensics capabilities or to formally compare systems. Because of this, it is unknown how to set up forensics' capacity enforcement procedures. Future benefits from improved forensics specification methodologies may be possible. One of the key benefits of having clearly stated forensics criteria is the ability to create solutions to suit these demands. A further benefit of developing a standardized, accurate, and repeatable procedure for constructing digital forensics features is the potential to specify additional generic forensics characteristics. Given their widespread acceptance, characteristics of digital data capturing systems would aid enforcement, program implementers, and system administrators in understanding forensics requirements and the limitations of systems in meeting those requirements. Digital evidence, whose volume is expanding and presents various handling and administration difficulties due to its complexity, is becoming a more vital component of all investigations. Digital evidence can help a case in one of two ways: directly using information from various sources, including CCTV cameras or mobile phones, in a normal criminal case. When digital proof is essential because the crime was committed online, such as in a virus attack or a cyber-fraud, direct involvement in a cyber-crime is necessary. A forensics policy mechanism can be used to define a system's forensics capacity, and it has a number of benefits. One benefit is the enormous corpus of security policy research that can be leveraged to address the digital forensics issue. The ability to determine a system's ability to conform to a forensics policy is another advantage. The system's forensics capabilities might also be formalized by formalizing the policy, which would also more accurately specify the skills required to adhere to the policy. The International Narcotics Control Board

has frequently cautioned against committing crimes online since it is so easy to do so (cybercrime). There are few resources required to access and use the internet. There are fewer threats to the criminal's personal safety and lower chances of getting caught because cybercrimes are difficult to investigate and prosecute. Digital evidence has become much more widely used in recent years. Prosecutors have been given access by courts to emails, digital images, word documents, spreadsheets, instant messaging, internet browsers, electronic door keys for hotels, ATM receipts, and schedules for global positioning system devices. The fact is that because new rules have not developed swiftly enough, contemporary realities have not been sufficiently handled. To accommodate the receipt of digital evidence, the rules currently in place for physical and conventional investigations are employed.

Literature Review

The Electronic Transaction Act of 2015 defines electronic evidence as "data or information preserved in binary form, electronic devices, or recovered from some electronic devices of a probative nature that may be submitted as evidence."(The Electronic Transaction Act,2015). Electronic evidence is any digital information saved on computers, networks, or other electronic devices and allowed as testimony in court. (Mason,2017). Electronic evidence includes audio, emails, movies, spreadsheets, and other data that can be accessed from any computer equipment and used as evidence in criminal proceedings (ParioCommunication,2020). From a range of devices, such as CDs, printers, scanners, laptops, mobile phones, etc., electronic evidence can be recovered. Electronic evidence is invisible because it is immaterial. It is kept on digital storage devices in binary code (ones and zeros) and it can only be retrieved using sophisticated forensic equipment. Therefore, in relation to human abilities and the human eye, advanced instruments and technologies must be utilized to extract electronic evidence (Mehta, 2012). It is volatile, therefore if the proper safety measures are not taken when searching for and seizing it, it could easily be destroyed or unintentionally tempered. When the proper steps are taken, computer forensics or digital forensics is produced. Some academics, however, use these phrases to refer to the employment of hardware tools for the extraction and analysis of complex data that has been stored or processed by computer networks or systems, such as when a targeted device is connected to a processing device (Mason,2007). A forensic tool is a special tool or piece of software developed especially to assist forensic investigators in carrying out their duties when handling electronic evidence, such as gathering evidence from dubious computers and analyzing data from electronic devices, according to the Cybercrime Act of 2015 (The Cyber Crimes Act,2015). The Act acknowledges that electronic evidence does not have the same legal standing as physical evidence. Electronic evidence cannot be handled, as contrast to physical evidence, which may be examined or seen. As a result, the Act mandates the use of specialized instruments throughout the "digital/computer forensics" phase of computer crime investigation. Computers automatically keep track of every activity they perform. Digital forensics experts employ computers' ability to log and store information about each activity that is occurring, including who did it, how, and when, to find these traces (SANS Institute, 2013). Instances of theft, industrial espionage, hacker breaches, child exploitation, improper Web use, and facilitation for e-Discovery can all involve the use of digital forensics. Collection, preservation, analysis, and visualization

are the four main stages of the digital forensic process (Kessler,2010). On the other hand, research has been done to improve each of these domains. There are still several factors that hinder the analytical step. These components include a lack of standards, accreditation, and human bias and inaccuracy. This has had a detrimental effect on forensic analysts' credibility in court cases (Ademu, Preston, & Imafidon, 2011). Maintaining evidence integrity is the process of ensuring that the evidence is in the same state as when it was obtained. A person can demonstrate the consistency of the evidence by demonstrating that nothing has changed since the suspects took it. To maintain the integrity of the original evidence, digital forensic investigators employ a variety of techniques, such as Bit image copies and the use of cryptographic hashes. Using a mix of conventional and cutting-edge methods, investigators recover computer records, information documents, communication logs, system logs, network logs, and associated data as evidence. In order to complete the assignment and gather evidence, it may later be essential to apply electronic investigative procedures or processes. Initial phases of an investigation may include conducting undercover operations with suspects or employing interviewing techniques. Data extraction from dubious systems or devices, data requests from third parties like IIS and host firms, and - where necessary - interference with electronic communications are all possible approaches (United Nations, 2013). The connections and interactions between independent and dependent variables are explained using a conceptual framework. The legal system and knowledge are two independent variables in the framework, while the validity of the evidence and the admissibility of electronic evidence are two dependent variables. This framework also includes the search and seizure procedures as an intervening variable that affects the dependent variables. Sremack (2007) asserts that since lawyers evaluate the overall significance and reliability of the evidence, they are the primary driving force behind digital forensics. The search and seizure processes in the lifespan of electronic evidence are a series of steps taken to achieve a certain objective. Digital evidence must be true, correct, complete, and persuasive to the judge to be admitted in court. A dependent variable is whether electronic evidence is admitted into evidence.

What then makes up a forensics policy that deals with forensic readiness for a specific system? The steps outlined below make it easier to create a forensics policy that considers the requirements for forensic ready:

- Identify the valuable digital assets.

- Run a risk analysis to see if these assets are vulnerable to harm or loss.

- Get rid of any assets that are not worth the trouble of filing charges.

- Determine the pertinent data, gathering, and storage needs for these assets.

- The forensic policy should define digital assets, forensic events, data gathering, and storage.

- Ensure that the forensics policy is effectively enforced.

Recent Examples

Digital forensics is a method used in criminal investigations. To do this, digital evidence must be gathered from a variety of infrastructures, resources, and gadgets, including PCs, mobile devices, hard drives, and cloud storage platforms.

Here are a few well-known situations where the use of digital forensics was necessary.

Network data reveals theft of trade secrets

Engineer Xiaolang Zhang was employed at Apple's section for autonomous vehicles. He had worked for the company for two and a half years when he declared he would be leaving to take care of his mother in China. He disclosed to his management that he would be working for a Chinese maker of electric vehicles. Following the discussion, the management voiced doubt. Company security opened an investigation. After searching Zhang's two work phones and laptop, the analysis of his network activities concerned them the most. The network data showed that Zhang's activity peaked in the days leading up to his resignation, reaching a two-year high. It entails "targeted downloading enormous pages of material" from the few databases to which he had substantial access. Zhang confessed to stealing business secrets when questioned. Zhang was accused of stealing trade secrets after the FBI was given the case.

Wearable sensors

In 2015, Connie Dabate perished there. Her husband Richard summarized the day's events by claiming he came home after hearing an alarm, per his arrest warrant. Richard alleges a thief entered his home, imprisoned him, and tortured him. He claimed that when Connie came back from the gym, the intruder shot and killed her. Police confirmed through Connie's Fitbit that she was at home when Richard claimed she was at the gym. Connie stopped moving one minute before the home alarm sounded, according to Fitbit data.

Issues & Challenges

In order to identify, collect, preserve, validate, analyze, interpret, and present digital evidence gathered from electronic sources to aid in the restoration of actions that have been ruled to be unlawful, digital forensics uses processes which have been developed and validated by science. These computer forensics research methodologies, however, run across some major obstacles when it comes to practical implementation.

Technology advances alongside criminal behavior and criminals. In the field of digital forensics, this process is referred to as an anti-forensic technique and is very difficult to execute. Digital forensic

specialists employ forensic tools to gather small pieces of information against criminals, while criminals use them to hide, alter, or remove any evidence of their crimes.

- Encryption: By keeping the information hidden from a user or other person who is not permitted, it is successfully employed to ensure the privacy of information. Unfortunately, criminals can utilize it to cover up their misdeeds.
- Covert Channel: An attacker can avoid intrusion detection systems and hide data on a network by using a protocol known as a covert channel. It was used by the attacker to hide his connection to the compromised machine.
- Absence of guidelines and standards: There are no established guidelines for the gathering and acquisition of digital evidence. The forensic labs and investigating agencies are developing their own set of rules. As a result, the potential of digital evidence has been destroyed.
- Volume and Replication: Integrity, confidentiality, and accessibility of electronic documents can all be easily jeopardized. Data can cross physical boundaries thanks to a vast network that is made possible by wide-area networks and the internet. The volume of data has increased due to the accessibility and ease of communication afforded by electronic documents, making it harder to locate the original and pertinent data.

Future Scope

The volume barrier will continue to be the main challenge soon as we get used to managing terabytes of digital evidence daily. Even if hardware efficiency and computing power are still increasing, there will be more digital evidence available in the future. The necessity to go from the domain of creating tools to extract all data to the region where the evidence is correlated to wrap up an inquiry has been recognised by researchers. Correlations in this data have a great deal of potential, despite the exponential growth in the variety of digital devices. Recognizing this connection across many digital forms of evidence and automatically associating such evidence pieces would be one method to address the volume issue. There may be fewer issues that need individual study because of this. This approach may also facilitate automatic corroboration, an important aspect of forensic investigation. This approach has resulted in satisfactory results despite the specialized and individualized applications from the past. If we are to address the challenges, we need a specific national law that covers everyone who engages in, deals with, or provides any resources, tools, or software used in a digital forensic inquiry. In addition to the awareness and training programs, the investigation businesses must conduct for its computer forensics investigators so that they are aware of modern innovations, the companies that produced the tools for digital forensics must also provide sufficient instruction booklets that contain a great summary, advantages, and disadvantages surrounding the instruments. There are not any established requirements or credentials that the court should recognize as proof of one's expertise in electronic evidence inquiry as of now. As a result, it has been misconstrued that an IT expert can also be a digital forensic expert, which could result in evidence being presented by a specialist who is unqualified to do so and evidence being kept without the required chain of custody.

Conclusion

The practice of diverse tools and techniques, as well as their varied ways of operation, create many difficulties to both legal and technical professionals in the field of cyber forensics because it is such a vast one. Rapid technological change, big data, the use of anti-forensic techniques by criminals, the use of free online tools for investigation, and a lack of appropriate guidelines for the collection, acquisition, and presentation of electronic evidence are some common problems that indicate the need for new legislation, changes to the existing code, and patched technologies.

During cybercrime investigations, investigators are looking for evidence other than pieces of computer equipment. Instead, they can be used to indicate ownership, knowledge, or possession of electronic evidence and can take the form of metadata data, electronic artifacts, and electronic communications. Cybercrime can be committed in a different setting than traditional crimes can, so during investigations, detectives will need to follow consistent and well-defined search and seizure protocols.

References

Taylor, C., Endicott-Popovsky, B., & Frincke, D. A. (2007, June 12). *Specifying Digital Forensics: A forensics policy approach*. Digital Investigation.

Sabika Tasneem & Sidra Jabeen. (n.d.). *How to overcome major problems in handling digital evidence?*

Mason, S. (2017). A Convention on Electronic Evidence.

ParioCommunication. (2020, January). Search and Seizure of Digital Evidence in Criminal Proceedings.

Mehta, S. (2012). Cyber forensic and Admissibility of Digital Evidence.

Mason, S. (2007). Electronic Evidence: Disclosure, Discovery & Admissibility. 2nd Edition. London: LexisNexis Butterworth.

Kessler, G. C. (2010). Judges' Awareness, Understanding, andApplication of Digital Evidence.

Ademu,, I. O., Preston, D. S., & Imafidon, C. O. (2011). A New Approach of Digital Forensic Model for Digital Forensic Investigation. International Journal of Advanced Computer Science and Applications, 4.

SANS Institute. (2013). Digital Forensic Fundamental and Evidence Acquisition.

Sremack, J. C. (2007). The Gap between Theory and Practice in Digital Forensics. Conference on Digital Forensics, Security and Law, (p. 10). Washington.

EclipseForensics. (2021, July 31). *3 famous cases solved through digital forensics*.

Kasper, Agnes, and Eneli Laurits. "Challenges in collecting digital evidence: a legal perspective." The future of law and eTechnologies. Springer, Cham, 2016. 195-233.

Raghavan, S. Digital forensic research: current state of the art. CSIT 1, 91–114 (2013).

Vacca, J. R. (2002). Computer Forensics: Computer Crime Scene Investigation. Elsevier Science.