Digital Forensics and Anti-Forensics Techniques

Dr. J. Savitha [1], M. Nisanth[2], K. Monishkumar [3], S. Suriyadhanush[4], J.Benito Sam Kumar[5]
[1]*Professor, Dr. N. G. P. Arts and Science College*
[2,3,4,5]*Student, Dr. N.G. P. Arts and Science College*

***Abstract*—The importance of digital forensics in any investigation where data is involved following a security breach cannot be overstated. Data may be personal, commercial, or confidential. The purpose of digital forensic analysis is to legally obtain and evaluate the data being examined. Conversely, anti-forensics techniques are designed to conceal, manipulate, or erase the data or to challenge the credibility of the evidence obtained. This paper provides an overview of current anti-forensics methods, the techniques employed, and the available countermeasures.**

***Index Terms*— Digital forensics, anti-forensics, forensics techniques.**

I. INTRODUCTION

We are living in a digital age, where nearly everything depends on digital information. Technology is pervasive in many domains, and digital data is everywhere. Individuals, companies, and governments use digital data in all aspects of their lives. The growth in this domain has been accompanied by the growth in digital forensics, for a variety of reasons, including cybercrimes and terrorism, where digital data may provide valuable information. However, digital forensics tools also serve as a warning sign for hackers, threat actors, and privacy-conscious parties, as they seek to develop antiforensics tools to protect the ability of forensic tools (FT) to retrieve valuable and pertinent information. Computer forensics tools, also known as Computer Forensics (CF) and Mobile Forensics (MFT), are used by the forensic examiner to collect information from the device, create a physical copy of the information to be analyzed, and to obtain reliable evidence that is legally admissible in court.

II. DISCUSSION

The use of Anti-Forensics Techniques (AFT) encompasses a wide range of types and techniques; an extensive survey of the available tools was conducted to illustrate the categorizations and sub-categories of AFT. The results of the study revealed that there are numerous types of AFT available. AFT is classified into multiple categories based on the purpose of use and the type of attacks conducted.

A. Artifact wiping

When you delete a file or a folder from your storage device, your actual data remains on your storage device until you overwrite it with new data. The term “artifact” or “secure” wiping is used to describe an AF technique that is designed to erase and destroy all data on your storage device. You can apply artifact wiping or secure wiping to files, entire disks, or a partition. Some of the tools that can be used to perform artifact wiping include:

- Eraser
- External Examiner
- Free Wipe Wizard
- File Shredder
- Registry Cleaner

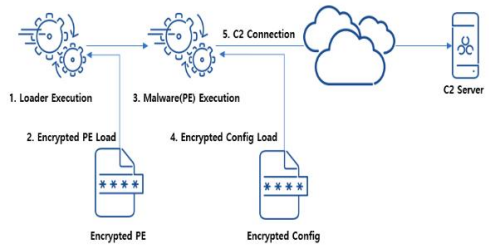


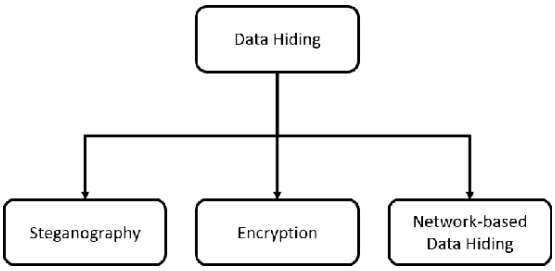
Figure 1. Artifact wiping

- Wiping is a process used to get rid of data on a specific disk or partition by wiping all the sectors on it.
- The process of disk degaussing involves placing an electronic storage device under a magnetic field in order to completely remove and erase any data previously stored on the device.

- The registry is what Microsoft Windows uses to store all the settings and info for the operating system and apps. Forensics examiners often find useful stuff in the registry during their investigations, which is why registry wipers try to get rid of it forever.
- Metadata manipulation is the process by which operating systems and software tools create metadata for each file created and saved on a storage device. Metadata is also known as information about information. Metadata varies depending on the file type but typically includes the creation date, modification date, last accessed date, last modified date, and information about the author. Metadata manipulation is used to manipulate and change metadata to redirect the forensic examiner's attention to the wrong places. Metadata is very sensitive information and is essential for creating a timeline of events.

B. Data Hiding

This technique is employed to locate the presence of data on the storage device, thus making it difficult or impossible for forensic examiners to assess and analyze digital evidence. The data hiding taxonomy is divided into three categories: steganography (or data concealment), data control, manipulation of the file system, manipulation of hard drives, and network data hiding.



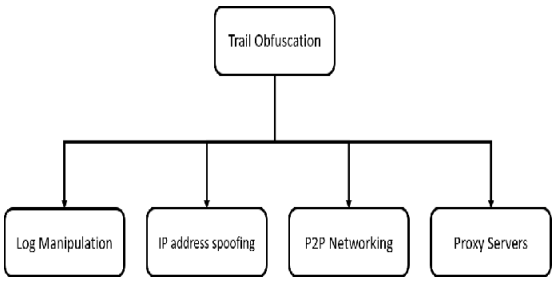
- Steganography: is the art of hiding a covert message within a regular message, but not the fact that two parties are communicating with each other . The secret message might be embedded in multiple types of files such as pdf, video, audio, images, and text.
- Data Encryption is a way of keeping your data safe from hackers. It can be used to encrypt a single file, a database, an email, or even an entire disk. There are a few different encryption algorithms that can be used to do this.

What is Network-Based Data Hiding?

Network-based data hiding is the same as data encryption, but it's done on the fly rather than at rest. Network-based data hiding has been used by many different platforms to protect privacy, such as end to end encryption . Regular Internet users can use VPN services to get around geographical restrictions if they're worried about privacy. Recently, attackers have been using network based data hiding or encryption to encrypt communications with bots or zombies, as well as to transfer data from attacked machines securely.

C. Trail obfuscation

Trace obfuscation, also referred to as evidence counterfeiting, is a technique employed to deceive and disorient an investigation. This can be accomplished in a variety of ways.



Log manipulation is when someone takes control of the logs stored on the machine they're trying to hack and uses them to manipulate the investigation and give false info. Usually, these logs are stored on the machine you're trying to hack, but if someone gets access to those logs, they can use them to take control of the investigation.

III. What is P2P Networking?

P2P networking is a way of sharing data that doesn't rely on a central server or host. Instead, data is shared among nodes that connect to the network very quickly. Each node that is connected to the network has a small amount of the file that needs to be shared, and each device that requests the file can provide it to the person who requests it. The transmitted data may be illegal or violate copyright law.

IV. LIMITATIONS & COUNTERMEASURES

A. Artifact wiping

Artifact wiping is one of the biggest threats to digital forensics investigations, and the only way to protect yourself from this type of attack is to back up your data as often as you can to either a network attached storage (NAS) or the cloud. Depending on how much data you're storing, the more often you back up, the less of an impact it'll have. Unfortunately, these solutions come with some drawbacks, like storage and resource usage if you're using a NAS, plus they can be expensive and take up a lot of bandwidth when you're using the cloud.

B. Data Hiding

The issue of Data Hiding is of paramount importance in the forensic field. Forensics examiners employ a variety of software tools to identify concealed data on the inspected equipment. The following is a compilation of the software used for the various types of data hiding.

- Forensics examiners may attempt to decrypt the data by memory dumping if the system is accessible while it is running. However, if the system is not accessible, forensic examiners must resort to brute force password attacks or dictionary attacks to decrypt the data. These type of attacks are both resource and time consuming, depending on the encryption type and the complexity of the password. Additionally, forensic examiners may also take advantage of an existing encryption algorithm weakness to decrypt the data, however, using modern encryption ciphers will make it difficult or impossible for forensic examiners to retrieve the data without the key.
- Companies may limit the use of Virtual Private Networks (VPNs) on the firewall, thus preventing employees from utilizing VPNs to transmit confidential information. At the level of Internet Service Providers (ISPs), privacy restrictions may impede the use of VPNs. However, since VPNs are encrypted and their primary purpose is to provide connectivity, ISP's cannot terminate service. The national Internet Gateway in each country may be able to decrypt symmetric traffic for security purposes, as in the case of Turkey, as the country possesses a root certificate for such decryption. However, this method is not effective when dealing with symmetric or end to end encryption.

C. Trail obfuscation

Typically, events, logs, and Netflow generated by routers are securely stored on secure Syslog machines, which are not susceptible to compromise. Endpoint software then transmits the logs, events, and Netflow from the machines to secure machines, where the log is subsequently correlated and analyzed. If logs are stored on another machine, forensic examiners can access them, even if the attacker has wiped them from the attacked machine. Logs from proxy servers are also necessary to monitor user activity. Netflow provides data about each packet, and with proper analysis, forensic examiners may be able to detect if peer-to-peer (P2P) communication has taken place on the network. Detecting IP spoofing originating from external sources is essential, and avoiding IP spoofing necessitates regulations and enforcement from interested parties, such as RIPE, to ensure that Internet service providers never permit spoofing sources.

V. CONCLUSION

This paper is about how different types of Anti-forensics attack and techniques work, and what challenges forensics examiners might face in the digital forensics field. It also looks at countermeasures against these types of attacks, taking into account their limits. Basically, attackers are constantly improving the effectiveness of AFTs, and they're coming up with new tools and techniques to make it harder for forensics examiners to do their job. It would be great if people, companies, and governments would follow and enforce security policies that focus on data backups and log backups. Encryption is tricky in any investigation because it's hard to decrypt without super-computing, and it's measured by a work function to show how powerful the algorithm is. Data hiding techniques are also tricky because they hide the detection of secret messages, especially when combined with encryption. Finally, looking at the traces of AFTs on a system could help forensics examiners figure out if these techniques have been used on the system they're looking at, which could help reduce the time of the investigation.

VI. REFERENCES

[1] M. K. Rogers and K. Seigfried, "The future of computer forensics: a needs analysis survey," Computers & Security, vol. 23, no. 1, pp. 12–16, 2004.

[2] M. Al Fahdi, N. L. Clarke, and S. M. Furnell, "Challenges to digital forensics: A survey of researchers & practitioners attitudes and opinions," in 2013 Information Security for South Africa, pp. 1–8, IEEE, 2013.

[3] M. Gül and E. Kugu, "A survey on anti-forensics techniques," in 2017 International Artificial Intelligence and Data Processing Symposium (IDAP), pp. 1–6, IEEE, 2017.

[4] K. Conlan, I. Baggili, and F. Breitinger, "Anti-forensics: Furthering digital forensic science through a new extended, granular taxonomy," Digital investigation, vol. 18, pp. S66–S75, 2016.

[5] K. Conlan, I. Baggili, and F. Breitinger, "Anti-forensics: Furthering digital forensic science through a new extended, granular taxonomy," Digital Investigation, vol. 18, 08 2016.

[6] H.-M. Sun, C.-Y. Weng, C.-F. Lee, and C.-H. Yang, "Anti-forensics with steganographic data embedding in digital images," IEEE Journal on selected areas in Communications, vol. 29, no. 7, pp. 1392–1403, 2011.

[7] G. C. Kessler, "An overview of steganography for the computer forensics examiner," Forensic science communications, vol. 6, no. 3, pp. 1–27, 2004.

[8] A. Aminnezhad, A. Dehghantanha, and M. T. Abdullah, "A survey on privacy issues in digital forensics," International Journal of CyberSecurity and Digital Forensics, vol. 1, no. 4, pp. 311–324, 2012.