International Research Journal of Engineering and Technology (IRJET) e-ISSN: 2395-0056
Volume: 10 Issue: 04 | Apr 2023 www.irjet.net p-ISSN: 2395-0072

Anti-Forensic Techniques and Its Impact on Digital Forensic

Satvik Gurjar[1], Dhaval Naik[2], Aarti Sardhara[3]

[1]LY B. Tech Computer Engineering, Science & Technology, Vishwakarma University, Pune, India - 411048
[2]LY B. Tech Computer Engineering, Science & Technology, Vishwakarma University, Pune, India - 411048
[3]Assistant Professor, Dept. of Computer Engineering, Vishwakarma University, Pune, India – 411048

Abstract - *This research paper focuses on anti-forensic techniques, which are used to evade or defeat digital forensics investigations. With the proliferation of digital devices, forensic investigations have become an essential tool for law enforcement agencies and security professionals. However, criminals and attackers are also using advanced techniques to hide their activities and make it difficult for investigators to trace their actions. Anti-forensics is a set of techniques used to cover up digital traces, confuse forensic investigators, and thwart the discovery of digital evidence. This paper provides an overview of the most common anti-forensic techniques used by attackers and cybercriminals, such as file wiping, data hiding, steganography, encryption, and obfuscation. We discuss the technical aspects of these techniques, their effectiveness, and the countermeasures that can be taken to detect and mitigate them. The research findings highlight the need for the development of new forensic tools and techniques that can effectively counter anti-forensic methods, which are becoming increasingly sophisticated and challenging to detect. The paper concludes by identifying the areas of future research in anti-forensics and their implications for digital investigations and cybercrime.*

Key Words: **Anti-forensic, Encryption, Steganography, obfuscation, Cybercrimes.**

1.INTRODUCTION

In today's world, digital evidence holds significant importance in investigative procedures and is processed through electronic means. The Locard principle states that a transfer occurs between the perpetrator and the crime scene, and this principle applies to digital evidence, which is stored on hard disks and memory as logs and other components that depict activities. The use of digital evidence in cyberspace is crucial for identifying the perpetrator, the precise timing of events, and their occurrence. Digital forensic investigators gather all relevant pieces of evidence into a cohesive report that outlines the nature and progression of a specific action.

However, various methods of anti-forensic activities exist, which can impede the investigative process at any given stage. Although some of these techniques have legitimate purposes, most are used to obstruct digital forensics. For example, encryption is used to protect organizational assets, while digital watermarking is applied to prevent copyright infringement. But if attackers and criminals use these techniques against digital forensics, they could prevent investigators from accessing essential data. The effectiveness of anti-forensic techniques is still largely unknown due to minimal practical research in this field.

Therefore, the primary objective of this research paper is to identify prevalent digital anti-forensic methods and assess them using forensic software. The goal is to determine whether computer anti-forensic activities can impede the investigation process and hinder the discovery of real evidence that could be presented as admissible in a legal proceeding.

2.MOTIVATION AND OBJECTIVE

The motivation for this research stems from the growing need to counter the use of anti-forensic techniques by attackers and cybercriminals, which makes it increasingly challenging for digital investigators to collect evidence and solve crimes. As these techniques evolve, it is crucial to develop countermeasures and improve investigation methodologies to detect and mitigate anti-forensic methods. The paper also aims to raise awareness of the need for innovative research and development in this field to develop new forensic tools and techniques.

2. RELATED WORK

The aforementioned research paper utilized several mechanisms to obtain the most appropriate sources for review. Initially, authoritative sources from government agencies, including the judiciary and technology standard-creating organizations, were selected. The objectivity and clarity of the sources were assessed to ascertain the credibility of the reviewed papers. Additionally, the reputation of the authors and the journal publication area were considered.

As previously stated, digital forensics is an emerging field that is rapidly expanding due to an increase in computer-related crimes and their complexity. Law enforcement agencies are primarily focused on resolving cases related to the misuse of digital technology. In most search-and-seizure situations, mobile phones are usually seized, as every crime has some form of association with computer forensics. Various studies and scholars contend that cybercriminals utilize anti-forensic techniques to obscure

their activities, making it difficult for forensic investigators to detect them. The lack of adequate theoretical investigations in digital forensics is mainly attributed to anti-forensics, in contrast to more conventional research methods.

To ensure the admissibility of electronic evidence in court, forensic experts must adhere strictly to procedures in the retrieval and investigation of digital systems. During the forensic examination process, multiple vulnerabilities may impede the retrieval of essential evidence necessary to support prosecution. Research has indicated that cybercriminals are employing anti-forensic techniques to disrupt the forensic process and hinder the recovery of electronic evidence.

2. ANTI FORENSIC TECHNIQUES

Forensic investigators are constantly exploring and adopting new methods to increase the efficiency and reliability of their investigations. Forensic investigators are utilizing new technological advances. However, criminals who commit cybercrimes are equally using advanced technology to employ intricate methods to obscure forensic investigation. These techniques are known as anti-forensic strategies, and they are aimed at hiding relevant forensic data that could be used by investigators to uncover the crime.

Data hiding is a distinctive anti-forensic strategy that is used to conceal any pertinent forensic data that may be used by investigators. Three common techniques are used in data hiding, which are encryption, steganography, and trail obfuscation. Research has shown that obfuscation and encryption are commonly used by computer criminals to prevent identification and collection of forensic data by investigators while allowing access to themselves.

This paper aims to explore some techniques used in data hiding.

4.1. ENCRYPTION

Encryption is a technique that is commonly used to protect data from unauthorized access, but it has also been adopted by computer criminals to impede forensic investigation. This strategy does not hide the presence of data from investigators, but it makes the data unreadable without decryption. With the availability of public encryption programs, criminals can easily encrypt data or disks using modern encryption algorithms that make the data nearly impossible to read without the correct decryption keys. There are two types of encryptions that are commonly used by computer criminals: file-based encryption, which turns file content into ciphertext that can only be read through decryption with the correct key, and disk encryption, which encrypts the entire storage partition containing the data, making access to the disk require a decryption key. VeraCrypt and Cipher Shed are encryption tools that allow for both types of encryptions. In the UK's Regulation of Investigatory Powers Act of 2000, computer crime offenders are required to provide access to any data in their possession that might be useful in forensic investigation. However, around 60% of cases involving encrypted data are unprosecuted due to the data's inaccessibility. The Open Rights Group also agrees with these statistics and states that only three out of nineteen cases involving a refusal to provide decryption keys between 2011 and 2013 were successfully prosecuted. Criminals may try to counter these regulations by providing access to a small amount of data while keeping the most incriminating data hidden.

4.2. STEGANOGRAPHY

Steganography is a technique that involves the concealment of data within other non-secret data to make it difficult for forensic investigators to detect. This technique is commonly used by computer criminals as an anti-forensic strategy to subvert the identification and extraction of forensic data. Steganography involves the embedding of hidden information within digital media such as images, videos, and audio files. This can be achieved by altering the least significant bits (LSB) of the digital media to contain the hidden data without noticeably changing the original data. The use of steganography in anti-forensic techniques has made it difficult for investigators to detect and extract hidden data as it is often well hidden and hard to distinguish from the original data. Some examples of steganography tools that can be used by computer criminals to conceal data include OpenStego, StegHide, and SilentEye.

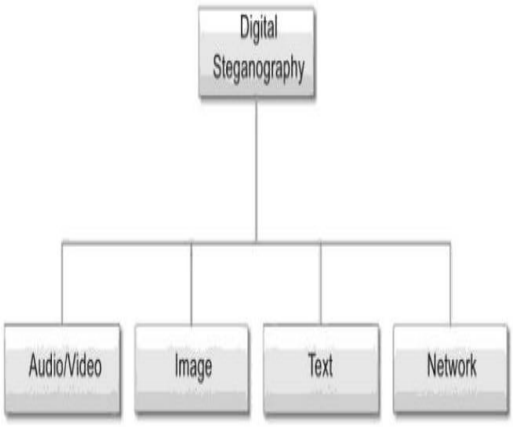

FIG 4.1: DIGITAL STEGANOGRAPHY

4.3. TRIAL OBFUSCATION

Trial obfuscation is an anti-forensic technique that involves modifying the code of a software program to

make it difficult for forensic investigators to analyze and understand it. This technique is commonly used by software developers to protect their intellectual property or by computer criminals to make their malicious software harder to detect and analyze. The primary goal of trial obfuscation is to prevent forensic investigators from reverse engineering the code to understand its functions and to find vulnerabilities or backdoors. By obfuscating the code, investigators may struggle to identify the intended functions of the code or to differentiate between benign and malicious behavior. Techniques used in trial obfuscation may include altering variable and function names, inserting extraneous code, adding bogus control flows, and using code encryption. Popular tools for trial obfuscation include ProGuard, Dotfuscator, and Jscrambler. While trial obfuscation can be a useful tool for protecting intellectual property, it also presents a significant challenge for forensic investigators trying to understand the nature and scope of computer crimes.

One common technique used in trial obfuscation is the creation of multiple fake accounts that are used to conduct illegal activities. These accounts are often registered under false names, and the information provided is intentionally misleading. This makes it difficult for investigators to identify the actual person behind the account and trace their activities. Another method of trial obfuscation is the use of misleading information. This can involve the creation of fake documents or the alteration of existing documents to hide important information. By altering or falsifying documents, criminals can create a false narrative that misleads investigators and makes it difficult to determine the truth. Hidden pathways are also a common tactic used in trial obfuscation. Criminals can create hidden pathways within networks or systems that allow them to conduct illegal activities without being detected. These pathways can be designed to appear as legitimate traffic, making them difficult to identify and trace.

In addition to above techniques, trial obfuscation can also involve the use of encryption and steganography to hide data and make it difficult for investigators to extract evidence. Overall, trial obfuscation is a powerful anti-forensic technique that can hide digital evidence and impede investigations. To combat this, investigators must be vigilant and use a variety of tools and techniques to identify and extract evidence. This may involve the use of specialized software and hardware, as well as a thorough understanding of digital forensic procedures and techniques.

4.4. ONION ROUTING

Onion routing is a technique used to enhance the privacy and security of internet communications. It is commonly used in anti-forensic techniques to prevent investigators from tracing the origin and destination of network traffic. Onion routing involves the use of multiple layers of encryption to protect the communication and the identity of the sender and recipient. The traffic is encrypted and then sent through a series of randomly selected servers, which decrypt each layer of the traffic, before forwarding it to the next server. Each server only knows the previous and next server in the chain, making it difficult to trace the origin and destination of the traffic. Onion routing is often used by criminals to communicate with each other without being detected by law enforcement agencies. The most popular onion routing network is Tor (The Onion Router), which is a free and open-source software used to enable anonymous communication on the internet. Tor has been used for various purposes, including bypassing internet censorship, accessing the dark web, and conducting illegal activities.

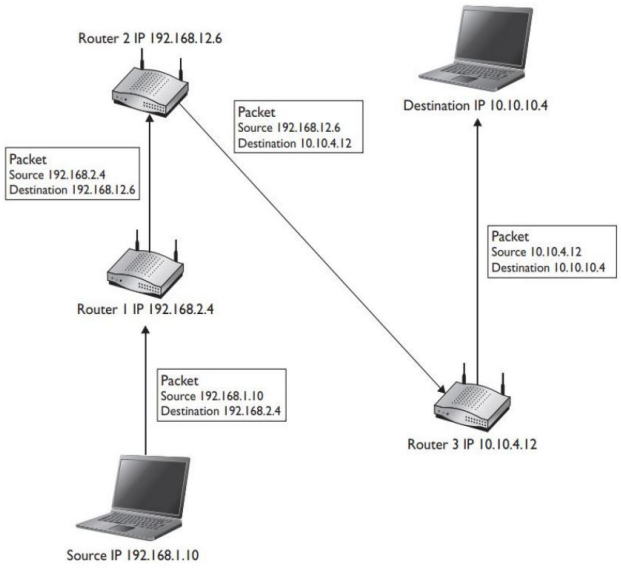

FIG 4.2: ONION ROUTING

4.4. SPOOFING

Spoofing is a technique commonly used by computer criminals to disguise their identity and evade forensic investigations. It involves the manipulation of data to appear as if it is coming from a different source than the actual sender. This can be achieved by falsifying IP addresses, MAC addresses, email addresses, and phone numbers.

One of the most common forms of spoofing is IP spoofing, which involves the modification of the source IP address of a packet to hide the sender's true identity. This technique is used by attackers to launch distributed denial-of-service (DDoS) attacks, send spam emails, and conduct phishing attacks.

Spoofing is also used in anti-forensic techniques, where criminals seek to cover their tracks and evade detection. By spoofing their identity, criminals can make it difficult

for forensic investigators to trace the origin of an attack or track down the real culprit. This can be achieved by spoofing the IP address of a device used in the attack, or by using a VPN or Tor network to conceal their true identity. In addition, spoofing can also be used in phishing attacks, where criminals create fake websites or emails that appear to be legitimate to trick users into revealing sensitive information. By spoofing the email address or URL of a legitimate organization, attackers can deceive users into thinking that they are interacting with a trusted entity.

Overall, spoofing is a powerful tool that can be used for both malicious and anti-forensic purposes. As such, it is important for organizations to implement strong security measures to detect and prevent spoofing attacks, and for forensic investigators to be vigilant in identifying and tracing the true source of attacks.

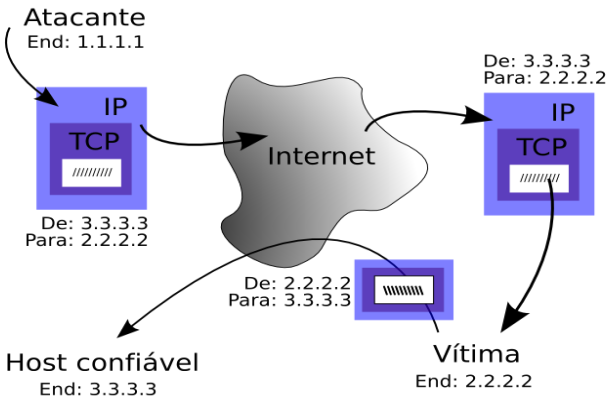

FIG 4.2: IP SPOOFING

4.4. CHANGING METADATA

Metadata is data that describes other data, such as information about the creation, modification, and access to a file. Changing metadata is a technique used by computer criminals to manipulate digital evidence, making it difficult for forensic investigators to accurately analyze and interpret the data. By changing metadata, criminals can obscure the original source, time and location of the file, and other important information that could be used as evidence against them.

There are several ways in which metadata can be changed, such as modifying the file properties, editing the document properties, and manipulating the Exif data in images. This can be done using various tools and software, some of which are freely available on the internet.

Changing metadata is often used as an anti-forensic technique in cases such as intellectual property theft, cyberstalking, and online fraud. In these cases, criminals aim to conceal their identity, location, and activities, making it difficult for investigators to trace the source of the crime. However, changing metadata is not foolproof and can be detected by forensic investigators using specialized software and techniques. Therefore, it is important for investigators to be aware of this technique and take measures to ensure the integrity of the digital evidence.

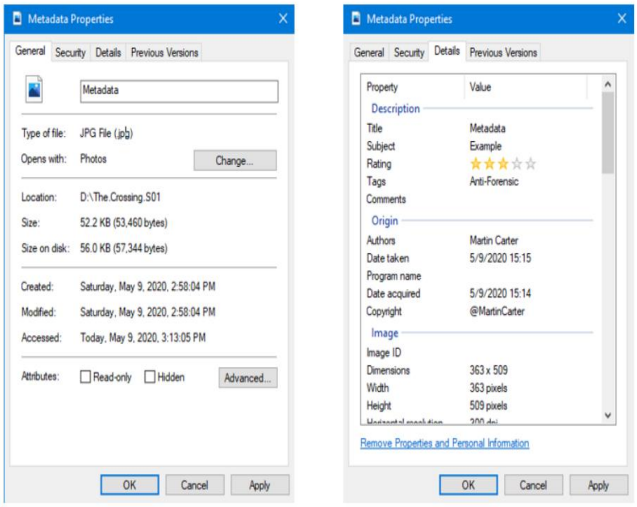

FIG 4.3: FILE METADATA

5. ANTI-FORENSIC TOOLS

There are various anti-forensic tools that can be used by attackers to cover their tracks and make it difficult for forensic investigators to identify and extract digital evidence. Here are some examples:

- CCleaner: CCleaner is a popular tool that can be used to clean up digital traces on a system. It can be used to delete temporary files, browser history, cookies, and other digital artifacts that can be used to track user activity.
- BleachBit: BleachBit is another tool that can be used to erase digital traces on a system. It can delete temporary files, logs, browser history, and other files that can be used to track user activity.
- VeraCrypt: VeraCrypt is a tool that can be used to encrypt data on a system. It can create encrypted volumes and partitions that can only be accessed with the correct password or key. This can prevent forensic investigators from accessing sensitive data.
- Tor Browser: Tor Browser is a web browser that can be used to browse the internet anonymously. It uses onion routing to hide the user's IP address and encrypt traffic, making it difficult for forensic investigators to identify the user's online activity.

- OpenStego: OpenStego is a steganography tool that can be used to hide data within digital images. It can be used to conceal sensitive data and make it difficult for forensic investigators to identify and extract the hidden data.

- Anti-Forensic Toolkit (AFT): AFT is a collection of anti-forensic tools that can be used to cover tracks and hide evidence. It includes tools for cleaning up digital traces, encrypting data, and manipulating file metadata.

While these tools can be used to cover tracks and make it difficult for forensic investigators to identify and extract digital evidence, there are countermeasures that can be used to detect and mitigate these techniques. For example, digital forensic investigators can use memory forensics to identify running processes and detect the use of anti-forensic tools. They can also use file carving techniques to recover deleted or hidden files, and analyze file metadata to identify signs of manipulation. Overall, it is important for forensic investigators to stay up to date with the latest anti-forensic techniques and tools in order to effectively detect and mitigate them.

6. COUNTERMEASURES FOR ANTI-FORENSIC TECHNIQUES.

As the use of anti-forensic techniques by cybercriminals continues to increase, it is important for forensic investigators to have a range of countermeasures to mitigate their impact. Below are some effective strategies for countering anti-forensic techniques:

- Real-Time Monitoring: Real-time monitoring of networks, systems, and endpoints is one of the most effective ways of detecting anti-forensic techniques. It enables forensic investigators to detect any unusual activity and behavior, including hidden network traffic, unusual access patterns, and other activities that could be indicative of anti-forensic behavior.

- Implementing Forensic Controls: Forensic controls such as audit logs, event logs, and system backups can help forensic investigators to recover data that has been tampered with. These controls enable investigators to analyze and identify suspicious activities and take appropriate measures to prevent data loss or theft.

- Digital Forensic Tools: There are several digital forensic tools available that can be used to counter anti-forensic techniques. These tools are designed to recover deleted or hidden data, detect steganography, and analyze encrypted data. Some popular forensic tools include EnCase, FTK, and Autopsy.

- Metadata Analysis: Analyzing metadata can be an effective countermeasure to anti-forensic techniques. Forensic investigators can analyze metadata to determine when a file was created, accessed, or modified, and who created or modified it. This information can help investigators to identify potential tampering or data hiding.

- Network Segmentation: IT can be used to separate critical systems and data from other parts of the network. This can prevent cybercriminals from accessing and tampering with critical data and systems, making it more difficult for them to use anti-forensic techniques.

- Training and Awareness: Educating users on the risks of anti-forensic techniques and how to prevent them can be an effective countermeasure. This can help to reduce the likelihood of employees inadvertently engaging in anti-forensic behavior.

7. CONCLUSION

The implementation of various anti-forensic techniques and tools remains largely limited to the academic and research communities, although there have been instances of technically proficient cybercriminals utilizing specific tools. Due to the limited resources of law enforcement agencies, it is reasonable to speculate that attackers who employ anti-forensic technology are less likely to be caught compared to those who do not use such technology. Anti-forensic technology is designed to impede investigations, and as a result, organizations may consider banning their use and even possession. However, with high-quality anti-forensic technology increasingly being incorporated into consumer operating systems to promote data privacy objectives, such bans may prove ineffective. In the field of computer forensics, investigators have traditionally relied on information inadvertently left behind by other programs. However, organizations may soon need to explicitly identify the information they want to preserve as part of their standard operations and devise strategies to maintain this information in a forensically sound manner.

8. FUTURE WORK

Future research should focus on developing more effective anti-forensic detection and mitigation techniques to counteract the increasing use of anti-forensic technology by cybercriminals. Staying abreast of the rapidly evolving landscape of digitization requires continuous and progressive professional development. Joining professional associations and networking with peers can be beneficial in tackling computer crimes by providing a platform for exchanging ideas and best practices.

Researchers seeking to enhance their results should consider conducting in-depth analyses of individual anti-forensic tools, as well as specific anti-forensic strategies to gain a better understanding of their underlying implementation mechanisms. organization can establish scalable in-house policies that streamline forensic investigations, especially considering that forensic analysis tools can be expensive. Collaborative efforts among organizations to pool resources for mutual interests may also be a viable option.

REFERENCES

[1] H. Jahankhani and E. Beqiri, Handbook of Electronic Security and Digital Forensics (Google eBook), vol. 2. 2010.

[2] K. Conlan, I. Baggili, and F. Breitinger, "Anti-forensics: Furthering digital forensic science through a new extended, granular taxonomy," Digit. Investig., vol. 18, no. December 2015, pp. S66–S75, 2016.

[3] I. Baggili, A. BaAbdallah, D. Al-Safi, and A. Marrington, "Research trends in digital forensic science: An empirical analysis of published research," Digit. Forensics Cyber Crime, pp. 144–157, 2012.

[4] S. Garfinkel, "Anti-Forensics : Techniques , Detection and Countermeasures," 2nd Int. Conf. Inf. Warf. Secur., pp. 77–84, 2007.

[5] B. Shirani, "Anti-forensics," High Technol. Crime Investig. Assoc., 2002.

[6] C. S. J. Peron and M. Legary, "Digital anti-forensics: emerging trends in data transformation techniques," Proc. 2005 E-Crime Comput. Evid. , 2005.

[7] M. Geiger, "Evaluating commercial counter-forensic tools," Proc. 5th Annu. Digit. Forensic …, pp. 1–12, 2005.

[8] R. Harris, "Arriving at an anti-forensics consensus: Examining how to define and control the anti-forensics problem," Digit. Investig., vol. 3, no. SUPPL., pp. 44–49, 2006.