A Study of Anti Forensic Techniques And Their Mitigation Strategies

Justin Jacob[1], Dr. Sandhya R[2]
[1]Dept of CSE
[2]Dept of CA
[1, 2]SNGCE, Kerala, India

Abstract- *The field of digital forensics is facing an increasing challenge due to the rise of anti-forensic techniques that are being used to tamper with digital evidence. This paper presents a comprehensive review of anti-forensic techniques (AFTs) used to hide or destroy digital evidence in digital crime investigations. AFTs can be classified into several types, including data hiding, data destruction, encryption, steganography, file system and memory manipulation, and network and cloud-based AFTs. Each type of AFT has multiple subcategories that can be used to evade detection or prevent recovery of digital evidence. This paper describes the various types and subcategories of AFTs and provides technical details on their implementation and detection. The paper also discusses several mitigation strategies for each type of AFT, including network monitoring and analysis, cloud service monitoring, data backup and recovery, access control and encryption, and file integrity monitoring. The information provided in this paper can be used by digital forensic investigators to better understand AFTs and improve their ability to detect and recover digital evidence in digital crime investigations.. This review provides a valuable resource for digital forensics practitioners and researchers who are interested in understanding the various techniques used to tamper with digital evidence and how to detect and analyze them.*

Keywords- digital forensics, anti-forensic techniques, file system manipulation, software manipulation, hardware manipulation, tampering, digital evidence, investigation,

I. INTRODUCTION

Digital forensics is the process of collecting, preserving, analyzing, and presenting electronic data in a way that is admissible in a court of law. As the use of digital devices and technology continues to increase in our daily lives, so does the potential for criminal activity involving these devices. Therefore, the need for digital forensics has become essential in modern law enforcement and legal proceedings. The integrity and authenticity of digital evidence are of utmost importance in this field, which has led to the development of various techniques and tools for collecting and analyzing digital data. However, with the rise of technology, criminals are becoming increasingly adept at using anti-forensic techniques to manipulate digital evidence and avoid detection. This paper aims to review the different anti-forensic techniques used for tampering with digital evidence, their impact on digital forensics investigations, and the current state of detection and analysis methods used to address these challenges.

Computer forensics is a process of collecting, analyzing, and preserving digital data from electronic devices to be used as evidence in legal proceedings. The process of computer forensics typically involves the following steps:

- Identification: The first step in computer forensics is to identify the digital devices and data that may be relevant to a particular case. This could include computers, smartphones, servers, or any other electronic devices that may contain relevant data.
- Collection: Once the relevant devices and data have been identified, the data is collected in a way that preserves its integrity and chain of custody. This can involve making a forensic copy of the data, which is an exact replica of the original data that can be used for analysis.
- Analysis: The collected data is then analyzed to identify relevant information, such as deleted files, hidden data, and network activity. This analysis can be done manually or with the use of specialized software tools.
- Presentation: Finally, the results of the analysis are presented in a report that can be used as evidence in legal proceedings. The report should clearly state the methods used to collect and analyze the data, as well as any conclusions drawn from the analysis.

Overall, computer forensics is a highly technical and specialized field that requires a deep understanding of digital devices and data. The process of computer forensics is designed to ensure that the integrity and authenticity of digital evidence is maintained throughout the investigation, making it admissible in a court of law.

II. ANTI FORENSICS

Anti-forensics refers to the techniques and strategies used to undermine or circumvent digital forensics investigations. Anti-forensic techniques can be used to hide, modify, or destroy digital evidence, making it difficult or impossible for investigators to collect or analyze the evidence. In the context of digital forensics, anti-forensic techniques can include file system manipulation, encryption, steganography, and data wiping. These techniques can be used by criminals to cover their tracks and avoid detection, making it more difficult for investigators to obtain evidence and prosecute offenders. The study of anti-forensics is an important area of research in digital forensics, as it is essential for investigators to understand these techniques in order to identify and counteract them. [1]

The general categories for anti-forensics techniques presented in [2]:

- Hiding, Obfuscation and Data Encryption,
- Deletion or Data Destruction,
- Data Falsification,
- Analysis Prevention,
- Obstruction of Traces Collection,
- Tools Subversion.

These AFTs can be used in combination to evade detection and hide evidence of criminal activity.

III. ANTI FORENSIC TECHNIQUES

The findings of the study, which were presented in [3], revealed that there are numerous anti-forensic tools (AFT) available, numbering in the hundreds.

A. Data Hiding

Data hiding is an anti-forensic technique used to conceal sensitive data within another file or in an unused portion of a disk. This technique is used to hide data in a way that makes it difficult to detect and recover.[4] There are several types and subcategories of data hiding that can be used for this purpose:

- File System Data Hiding: This technique involves hiding data by altering file system metadata to conceal the presence or location of a file. This technique can be achieved by changing the file attributes, manipulating the directory entries, or modifying the file allocation table.
- Alternate Data Stream (ADS) Hiding: This technique involves hiding data by attaching it to a legitimate file as an alternate data stream. ADS is a feature of NTFS file systems that allows multiple data streams to be associated with a single file. This feature can be exploited to hide data within a legitimate file without altering the file size or contents.
- Steganography: This technique involves hiding data within an image, audio, or video file by altering the least significant bit of each pixel or sample. This technique is used to conceal the data within the file, making it difficult to detect and recover.
- Unused Partition Data Hiding: This technique involves hiding data within an unused portion of a disk. This unused portion can be a deleted partition, free space, or slack space. The data is hidden in such a way that it does not affect the file system and remains undetected.
- Cryptography: This technique involves encrypting data using a cryptographic algorithm to make it unreadable without the correct key. The encrypted data can be hidden in a legitimate file or sent over the network without raising suspicion.

To mitigate the effects of data hiding, digital forensic investigators can use the following tools and techniques:

- Use file system analysis tools: Digital forensic investigators can use specialized file system analysis tools such as EnCase, FTK, or Autopsy to detect and recover hidden data. These tools can analyze file system metadata and detect inconsistencies in file attributes, directory entries, and file allocation tables that may indicate the presence of hidden data.
- Use file integrity checkers: Investigators can use file integrity checkers such as Tripwire or AIDE to monitor changes to file system metadata and detect any unauthorized changes that may indicate the presence of hidden data.
- Use alternate data stream scanners: Investigators can use alternate data stream scanners such as LADS or ADS Spy to detect the presence of alternate data streams that may contain hidden data.
- Use steganography detection tools: Investigators can use steganography detection tools such as Steg Detect or Out Guess to detect the presence of steganographic data hidden within image, audio, or video files.
- Use disk imaging tools: Investigators can use disk imaging tools like the FTK Imager or utilities like dd to create a forensic copy of a disk or partition. This copy can be analyzed using file system analysis tools

or other forensic tools to detect and recover hidden data.
- Use cryptographic analysis tools: Investigators can use cryptographic analysis tools such as OpenSSL or Cryptool to analyze encrypted data and recover the keys needed to decrypt it.

B. Data Destruction

Data destruction is an anti-forensic technique used to permanently erase data from storage devices to prevent it from being recovered.[5] There are several types and subcategories of data destruction that can be used for this purpose:

- Physical destruction: This technique involves physically destroying the storage device using techniques such as shredding, degaussing, or melting. This technique ensures that the data cannot be recovered, but it destroys the device and makes it unusable.
- Overwriting: This technique involves overwriting the existing data on the storage device with new data to make it unreadable. This can be done using software tools that write random data over the existing data, making it impossible to recover the original data.
- Secure Erase: This technique involves using specialized software or firmware to erase the data on the storage device in a secure manner. This technique is designed to prevent recovery of data by overwriting it multiple times with random data or using other secure erase algorithms.
- Crypto Shredding: This technique involves encrypting the data on the storage device using strong encryption algorithms and then deleting the encryption key. This makes the data unreadable and effectively destroys it.

To mitigate the effects of data destruction, digital forensic investigators can use the following tools and techniques::

- Use write-blocking devices: Digital forensic investigators can use write-blocking devices such as hardware write-blockers or software write-blockers to prevent any further changes to the storage device, ensuring that the existing data remains intact.
- Use forensic imaging tools: Investigators can use forensic imaging tools like the FTK Imager or utilities like dd to to create a forensic copy of the storage device before attempting to recover any data. This ensures that the original data is preserved and can be analyzed using forensic tools.
- Use data recovery tools: Investigators can use specialized data recovery tools such as Recuva, PhotoRec, or TestDisk to recover deleted or overwritten data from the storage device. These tools can recover data that has not been completely overwritten or destroyed.
- Use backup and recovery procedures: Organizations can implement backup and recovery procedures to ensure that critical data is backed up regularly and can be restored in the event of data loss or destruction.

By using these tools and techniques, digital forensic investigators can effectively mitigate the effects of data destruction and recover data that may have been thought to be permanently lost.

C. Encryption

Encryption is an anti-forensic technique used to protect data from unauthorized access by converting it into a form that cannot be read without the appropriate decryption key. Encryption can be used to hide data on storage devices, network traffic, or communication channels.[6] There are several types and subcategories of encryption that can be used for this purpose:

- Symmetric Encryption: This technique uses a single key to encrypt and decrypt data. The same key is used for both encryption and decryption, and both the sender and receiver must have access to the key to encrypt and decrypt the data.
- Asymmetric Encryption: This technique uses a pair of keys, one for encryption and one for decryption. The public key can be freely distributed to anyone, while the private key is kept secret by the owner. This technique is often used for secure communication and digital signatures.

To mitigate the effects of encryption, digital forensic investigators can use the following tools and techniques:

- Use key recovery tools: Digital forensic investigators can use specialized tools such as Elcomsoft or Passware to recover encryption keys from storage devices or memory dumps. These tools can recover both symmetric and asymmetric encryption keys, allowing investigators to decrypt the encrypted data.
- Use known plaintext attacks: Investigators can use known plaintext attacks to recover the encryption key

by analyzing the encrypted data and comparing it to known plaintext. This technique can be effective if the attacker has access to a significant amount of plaintext data.

- Use brute-force attacks: Brute-force attacks involve trying all possible combinations of keys until the correct one is found. This technique can be effective against weak encryption, but it can be time-consuming and resource-intensive.
- Use side-channel attacks: Side-channel attacks exploit weaknesses in the physical implementation of encryption algorithms, such as power consumption or electromagnetic radiation, to recover encryption keys. This technique requires specialized equipment and expertise

By using these tools and techniques, digital forensic investigators can effectively mitigate the effects of encryption and recover data that may have been thought to be inaccessible. However, it is important to note that encryption is a powerful tool for protecting sensitive data and should be used appropriately to ensure the confidentiality and integrity of the data.

D. Steganography

Steganography is a technique used to hide data within other data, such as text within an image or audio file.[6] There are several types and subcategories of steganography, including:

- Image Steganography: This technique involves hiding data within an image file. The data can be hidden within the pixel values of the image or within the metadata of the file.
- Audio Steganography: This technique involves hiding data within an audio file. The data can be hidden within the audio signal itself or within the metadata of the file.
- Video Steganography: This technique involves hiding data within a video file. The data can be hidden within the video frames or within the metadata of the file.

To mitigate the effects of steganography, digital forensic investigators can use the following techniques:

- Use specialized steganalysis tools: These tools can analyze image, audio, and video files for signs of data hiding, such as changes in file size or anomalies in the pixel values of an image.
- Use visual inspection: Investigators can visually inspect images and videos for signs of data hiding, such as patterns or anomalies in the image.
- Use statistical analysis: Investigators can use statistical analysis to detect changes in the data distribution of an image or audio file, which may indicate data hiding.

E. File system and memory manipulation

File system and memory manipulation are anti-forensic techniques used to modify or delete data on storage devices or in memory.[8,9] There are several types and subcategories of file system and memory manipulation, including:

- File Deletion: This technique involves deleting files from a storage device. This can be done using specialized software or by physically destroying the storage device.
- File Hiding: This technique involves hiding files on a storage device by modifying file attributes or hiding them in unallocated space.
- Memory Scrubbing: This technique involves modifying or erasing data in memory to remove evidence of malicious activity.

To mitigate the effects of file system and memory manipulation, digital forensic investigators can use the following techniques:

- Use specialized recovery tools: These tools can recover deleted files or files that have been hidden on a storage device.
- Use memory analysis: Investigators can analyze the memory of a system to detect signs of memory scrubbing or other malicious activity.
- Use write-blocking tools: These tools can prevent data from being modified on a storage device, preserving the integrity of the data for forensic analysis.

F. Network and cloud-based AFTs

Network and cloud-based AFTs are techniques used to hide or destroy digital evidence in network or cloud environments. These AFTs can be classified into several types and subcategories:

- Network-based AFTs: This type of AFT involves the manipulation of network traffic to evade detection or interception. Examples of network-based AFTs

include network tunneling, traffic shaping, and packet fragmentation.[10]

- Cloud-based AFTs: This type of AFT involves hiding or deleting data stored in cloud services to prevent its discovery. Examples of cloud-based AFTs include cloud wiping, data obfuscation, and virtual machine-based AFTs.[11]

To mitigate the effects of network and cloud-based AFTs, digital forensic investigators can use several techniques, including:

- Network monitoring and analysis: By monitoring and analyzing network traffic, investigators can detect unusual or suspicious network behavior and identify potential AFTs.
- Cloud service monitoring: By monitoring cloud services, investigators can detect unusual activity, such as data deletion or modification, and take appropriate action.[12]
- Data backup and recovery: By regularly backing up data and storing it in secure locations, investigators can prevent data loss due to AFTs.
- Access control and encryption: By implementing access control and encryption measures, investigators can limit the damage caused by AFTs and prevent unauthorized access to sensitive data.

G. Time stamp manipulation

Time stamp manipulation is an AFT that involves altering the metadata of files or system logs to misrepresent the time of an event. This can be done to make it difficult for investigators to determine the sequence of events in a digital crime.[13] Time stamp manipulation can be categorized into several subcategories, including file creation, file modification, and system logs.

To mitigate the effects of time stamp manipulation, investigators can use several techniques, including:

- Network time synchronization: By synchronizing the clocks of all network devices, investigators can detect time discrepancies and identify potential time stamp manipulation.
- Analysis of multiple data sources: By analyzing multiple sources of data, such as system logs and network traffic, investigators can detect inconsistencies in time stamps and identify potential time stamp manipulation.
- Use of trusted time sources: By using trusted time sources, such as a time server, investigators can ensure the accuracy and reliability of time stamps.

H. Anti-logging

Anti-logging is an AFT that involves preventing or deleting logs of digital activity to hide evidence of a digital crime. This can be done by disabling or deleting log files, modifying system settings, or using specialized software to conceal activity. Anti-logging can be categorized into several subcategories, including event log deletion, process monitoring, and rootkit-based AFTs.

To mitigate the effects of anti-logging, investigators can use several techniques, including:

- File integrity monitoring: By monitoring file changes and system logs, investigators can detect unauthorized modifications and identify potential anti-logging activity.
- Use of anti-rootkit tools: By using specialized tools to detect and remove rootkits, investigators can prevent rootkit-based anti-logging AFTs.
- Implementation of security policies: By implementing security policies that require the retention of logs and restrict access to system settings, investigators can prevent anti-logging activity.

IV. CONCLUSION

In conclusion, anti-forensics techniques pose a significant challenge to digital forensics investigations. Attackers are continuously developing new tools and techniques to make the examination of digital evidence harder. This paper has provided an overview of the various categories and subcategories of anti-forensics techniques, including hiding, obfuscation, encryption, deletion, data falsification, analysis prevention, and obstruction of traces collection. It is crucial to apply security policies targeting data backups and logs and to stay up to date with the latest countermeasures to mitigate the effectiveness of anti-forensics techniques. By studying the traces of an anti-forensics attack, investigators can detect that such techniques have been used on the examined system, which might reduce the time of the investigation. Overall, digital forensics experts must continuously improve their knowledge of anti-forensics techniques to stay ahead of attackers and maintain the credibility of digital evidence in legal proceedings.

It is impractical to thoroughly investigate every potential instance of anti-forensics in each case. The decision to search for anti-forensic techniques should be based on the suspect's profile, such as whether they are a technical or regular user. Though this paper discusses individual anti - forensic techniques and their challenges, if any of these are combined and used, it will definitely raise a greater challenge to the investigators in this field of digital forensics, which may be an extension of this paper.

REFERENCES

[1] K. Hausknecht and S. Gruičić, "Anti-computer forensics," 2017 40th International Convention on Information and Communication Technology, Electronics and Microelectronics (MIPRO), Opatija, Croatia, 2017, pp. 1233-1240, doi: 10.23919/MIPRO.2017.7973612.

[2] M. Gul, & E. Kugu (2017). A survey on anti-forensics techniques. 1-6. 10.1109/IDAP.2017.8090341.

[3] K. Conlan & I. Baggili, & F. Breitinger, (2016). Anti-forensics: Furthering digital forensic science through a new extended, granular taxonomy. Digital Investigation. 18. 10.1016/j.diin.2016.04.006.

[4] A. Jain and G. S. Chhabra, "Anti-forensics techniques: An analytical review," 2014 Seventh International Conference on Contemporary Computing (IC3), Noida, India, 2014, pp. 412-418, doi: 10.1109/IC3.2014.6897209.

[5] M. Ölvecký and D. Gabriška, "Wiping Techniques and Anti-Forensics Methods," 2018 IEEE 16th International Symposium on Intelligent Systems and Informatics (SISY), Subotica, Serbia, 2018, pp. 000127-000132, doi: 10.1109/SISY.2018.8524756.

[6] S. S. Lee, K. -Y. Chang, D. Lee and D. Hong, "A New Anti-Forensic Tool Based on a Simple Data Encryption Scheme," Future Generation Communication and Networking (FGCN 2007), Jeju, Korea (South), 2007, pp. 114-118, doi: 10.1109/FGCN.2007.21.

[7] H. -M. Sun, C. -Y. Weng, C. -F. Lee and C. -H. Yang, "Anti-Forensics with Steganographic Data Embedding in Digital Images," in IEEE Journal on Selected Areas in Communications, vol. 29, no. 7, pp. 1392-1403, August 2011, doi: 10.1109/JSAC.2011.110806.

[8] H. Majed, H. N. Noura and A. Chehab, "Overview of Digital Forensics and Anti-Forensics Techniques," 2020 8th International Symposium on Digital Forensics and Security (ISDFS), Beirut, Lebanon, 2020, pp. 1-5, doi: 10.1109/ISDFS49300.2020.9116399.

[9] Ahn, Na Young & University), Dong. (2022). Security of IoT Device: Perspective Forensic Anti-Forensic Issues on Invalid Area of NAND Flash Memory. IEEE Access. 10. 10.1109/ACCESS.2022.3190957.

[10] A. Odebade, T. Welsh, S. Mthunzi and E. Benkhelifa, "Mitigating anti-forensics in the Cloud via resource-based privacy preserving activity attribution," 2017 Fourth International Conference on Software Defined Systems (SDS), Valencia, Spain, 2017, pp. 143-149, doi: 10.1109/SDS.2017.7939155.

[11] S. Ahmed and M. Y. A. Raja, "Tackling cloud security issues and forensics model," 7th International Symposium on High-capacity Optical Networks and Enabling Technologies, Cairo, Egypt, 2010, pp. 190-195, doi: 10.1109/HONET.2010.5715771.

[12] D. -i. Jang, G. -J. Ahn, H. Hwang and K. Kim, "Understanding Anti-forensic Techniques with Timestamp Manipulation (Invited Paper)," 2016 IEEE 17th International Conference on Information Reuse and Integration (IRI), Pittsburgh, PA, USA, 2016, pp. 609-614, doi: 10.1109/IRI.2016.94.