A Review Study on Anti-Forensic Techniques and Their Detection in Digital Forensics

Chinthakindhi Bhanu Prakash[1*]
[*1]*B.Sc. (Hons) Digital Forensic Science, Malla Reddy University, Hyderabad, India.*
ch.bhanuprakash1357@gmail.com

Abstract:

Digital forensic methodologies and tools have become a crucial part for investigation of cybercrimes. Digital forensics experts usually follow a common workflow and use known methodologies and tools while investigating a case. Attackers and cybercriminals are aware of which methodologies are used in an investigation and how digital forensic tools work, as a consequence, they started to find and implement a new methodology which is called Anti-Forensics where attackers try to tamper the digital forensic investigation process by manipulating evidence to hide or conceal their tracks of malicious activities. They make it difficult or almost impossible for investigators to uncover the digital evidence which aim to mislead the investigation process. Therefore, implementing effective countermeasures is essential to identify the anti-forensics tools or techniques and stop these attackers. This review study focuses on comprehensive analysis of commonly used anti forensic tools and techniques and their detection and countermeasures used in digital forensic investigations. This paper classifies various anti-forensic methods into evidence hiding, evidence destruction, evidence manipulation furthermore it examines different detection methods including timeline reconstruction, file system analysis and machine learning based techniques. By reviewing recent research articles and works, this study highlights the efficiency and limitations of present detection mechanisms this paper also highlights challenges faced by investigators such as encryption, handling volatile data and dependency on tools.

Keywords: Anti-Forensics, Digital Forensics, Cybercrimes, Evading techniques

D. R. Reddy et al. (eds.), *Proceedings of the First International Conference on Advances in Forensics and Cyber Technologies (ICFACT 2025)*, Advances in Computer Science Research 127,
https://doi.org/10.2991/978-94-6239-610-4_20

1. Introduction:

Digital forensics plays an important role as the use of digital devices has become widespread today. digital forensics is a field which involves the collection, preservation, and analysis of digital evidence for investigation purposes and presenting them in the court, digital Forensics is “The use of scientifically derived and proven methods toward the preservation, collection, validation, identification, analysis, interpretation, documentation, and presentation of digital evidence, these digital evidence holds significant importance in investigative procedures and is processed through electronic means derived from digital sources to facilitate or further the reconstruction of events found to be criminal, or helping to anticipate unauthorized actions shown to be disruptive to planned operations”. A forensic investigator handles the digital evidence in cyberspace is crucial for identifying the perpetrator, the precise timing of events, and their occurrence. The aim of digital forensics is to preserve evidence relevant to an investigation in its original form to use it in a court of law. For the evidence to be admissible in court of law, forensics investigators must follow strict procedures when collecting and analyzing the evidence. each case maintains set protocols for evidence collection, acquisition, examination, and reporting while maintaining a chain of custody and preserving evidence integrity. (Beeb & Clark, 2005; Casey 2011)

However in order to avoid detection or identification of digital evidences, cyber criminals are using various anti-forensic methods to destroy or tamper or erase or manipulating digital evidences using various anti-forensic tools and techniques for example a cybercriminal might use encryption to protect the data or they might use tools to hide the data or to destroy the evidences related to the case their objective is to mislead the forensic investigator or to delay the investigation process. (Garfinkel 2007; Gujar et. al., 2023)

Forensic investigators are constantly searching for the new methods to increase effectiveness in their investigations. Forensic investigators are utilizing new technological advances. However, criminals who commit cybercrimes are also 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 details related to crime.

2. Anti-forensic techniques:

Anti-forensic techniques are primarily classified based on their method of disrupting evidence collection and analysis methods, Dr. Marcus Rogers classification is the one of the most widely accepted classification, in this classification Rogers divided anti forensic techniques into different types which includes data hiding, artifact wiping, trail obfuscation, attacks against forensic tools, some classifications expand by including physical destruction . (Garfinkel 2007; Colan et. al., 2016)

Anti-forensic techniques are classified into four primary categories this includes:

2.1.Data hiding: Data hiding is an anti-forensic technique used by attackers to conceal the digital evidences so that digital evidence cannot be discovered or analyzed by investigator. Instead of deleting evidence criminals hide data in locations where investigators are less likely to look or places where detection is technically difficult.

Types of data hiding techniques

- **File system data hiding**: this technique hides data within the structure of a file system or it is a method in which data is stored in unused disk area so it is not visible to normal users such as

  Slack space hiding: the unused space in the file system is known as slack space which is not visible to normal users, attackers use this slack space to store or hide the data

  Hidden Partitions: these hidden partitions type of disk partitions that are not listed in the standard partition tables, attackers use these hidden partitions space to hide the evidences

  In order to hide data in these locations, criminals use tools like Slacker to hide data. (Garfinkel et. al., 2007; Gobel et. al., & Baier et. al.,2018)
- **Memory data hiding:** This technique uses file less malware and memory injection techniques to hide data in the volatile memory, in this technique it can only hide data in RAM (Random Access Memory) meaning that data only exists when system is powered on

  in this method data is stored in stack or heap memory of running processes. (Ligh et. al.,2014; Rutkowska, 2006)

- **Network-based hiding:** In this Network based data hiding user hides the digital evidences by manipulating the network protocols or by embedding data in traffic using encryption or by using steganography making it difficult for investigators to trace them. Attackers use techniques like

  Covert channels: In this method to hide the evidences the data is embedded to the unused fields of the network protocols.

  Packet crafting: This method involves in modifying the packet headers and time to transmit data.(Zander et. al., 2007; johnson et. al., 2001)
- **Encryption:** This the process of converting the plain text (readable data) into a cipher text (unreadable format) using cryptographic keys, so that it can prevent investigators for accessing the data and even if the data is found It cannot be read without the key. In order to achieve these users, use tools like VeraCrypt (VeraCrypt is an open-source disk encryption tool used to encrypt virtual disk, partitions or it encrypts entire drive) BitLocker. (Gujar et al, 2023; Garfinkel, 2007)
- **Rootkits:** A Rootkit is a malicious software that gives the user hidden access (administrator access) and it cannot be easily detected because in hides in the deeper layers of operating system. Rootkit can conceal malicious software and file. (Rutkowska 2006; Garfinkel, 2007)

2.2.Artifact Wiping: Artifact wiping is the destruction method used by criminals. in this artifact wiping user deliberately erases or deletes the digital evidences from the storage device, it goes beyond standard deletion were standard deletion only deletes file pointers, wiping involves in overwriting the actual data making it unreadable. Some of the common artifact wiping methods and tools includes

- **File wiping:** File wiping is the process of deleting (overwriting the) individual files from the operating system. To do so, criminals use tools like Secure Erase, DBAN, Eraser, and CCleaner for file wiping. File wiping tools overwrite the data with unwanted or meaningless information such as overwrite the multiple times with random patterns and numbers, this makes original data irretrievable. (Mutawa et, al., 2012 Hosgor, 2012)
- **Metadata wiping:** Metadata is the data about the data, which can provide information such as author info, creation, timestamps, and can provide crucial insights about the data. The main objective of erasing metadata is to hide file-related history tools used to for metadata wiping includes Exif tool, MAT2(metadata anonymization toolkit), and DigiKam. Tools are used for metadata wiping.(Mutawa et. al., 2012; Garfinkel 2007)

- **Generic data wiping:** Generic data wiping is the process of permanently deleting the data from the storage device, including free space. It is done by overwriting (using single pass, multiple pass) all the storage sectors with new data patterns. Generic data wiping technique can also be done using in built operating system functions.
- **Registry wiping:** These registry entries store all the information related to system activities, which can be used by investigators to identify malicious activity or actions performed. To avoid being detected, criminals use registry wiping. Registry wiping is the process of deleting or manipulating the registry entries using different tools and methods, such as using custom scripts. And tools like Fcleaner, Sdelete. (Casey, 2011 Ligh et. al., 2014)

2.3.Trail obfuscation: Trail obfuscation is the process of replacing/altering/modifying the existing sensitive information with information that looks real but has no use. These are deliberate actions made to conceal digital traces or to manipulate digital traces left by the user, which include timestamps, deleting logs, using proxies/VPNs/Tor, and creating fake artefacts. To make the investigation more difficult and time consuming, the main motive is to reduce the risk of being detected & can be done by using altered signatures. To achieve this attacker uses techniques like timeline manipulation, file header manipulation, and tools like transmogrify from Metasploit. accomplish this, the attacker uses techniques such as log cleaning, timeline manipulation, file header manipulation, and tools like timestamp and transmogrify from Metasploit. (Garfinkel, 2007; Colan et. al., 2016)

2.4. Attacks against forensic tools: Attackers deliberately try to target the tools and methodologies instead of hiding the digital evidence. Their main objective is to detect, mislead or disable forensic tools or to disrupt the investigative procedures, making examination and analysis unreliable or incomplete. These attacks directly impact the analysis process.

Use attacks like Denial-of-service attack (Dos), Compression bombs,

- **Compression Bombs:** While analyzing the data forensic tools will also analyze compressed files such as Zip files during analysis of the file system, this compression bombs are compressed files which contain large amount of data which cannot be handles by the forensic tools once they are extracted making forensic tool unstable (unable to handle the huge amount of data) resulting in crash of forensic tool.

- **Denial of service attack (Dos):** Denial of service is another attack type against forensic tools. By draining resources like the RAM (random access memory) and CPU required by the tools, an attacker can be required by the tools, an attacker can disrupt the analysis process. (Surakanthi et. al., 2025, Garfinkel 2007)

2.5. Physical destruction: This method completely obliterates the digital evidence. Physical destruction involves dismantling or destroying the evidence or making the evidence unusable for the examination and analysis process.

3. Detection of anti-forensic techniques:

3.1 Detection of Hidden data: Detection of hidden data is an important task in digital forensics because sometimes instead of deleting the data cyber criminals conceal the data in different locations to avoid being detected and avoid suspicion by forensic tools. The attacker uses evidence hiding methods such as file system manipulation, steganography, and encryption. The motive of hiding data detection is to identify irregularities that indicate the existence of hidden data present in the system. A digital forensic investigator uses various methods and forensic tools to detect this hidden data.

- **File system Meta data Analysis:** Attackers usually hide the evidence in the file system by manipulating the file system attributes like unused disk areas, hidden flags, or alternate data streams. In this investigator analyze allocation table, file metadata, and data structures, to detect the presence of suspicious activity or irregularities between file size and actual file disk usage. (Casey, 2011, Ligh et. al.,2014)
- **Steganalysis:** Steganalysis is the process of detecting the hidden information embedded in images, videos and audio files. Cybercriminals often manipulate the insignificant bits to store data without visibly manipulating the file. Digital forensic investigator uses detection techniques to analyze noise patterns, statistical irregularities, pixel value distribution or abnormal histogram patterns, which often indicate the presence of steganographic content. (Johnson et. al., 2001, Garfinkel 2007)
- **Slack space and Unallocated space Analysis:** Analysis of slack apace and unallocated space is done to detect hidden data because these locations can used by cybercriminals for hiding sensitive information or data without creating a visible file. To detect such hidden data forensic investigator scans these spaces to recover the hidden data or

residual data fragments. Detection of any suspicious patterns in these spaces may indicate the presence of concealed information.

- **Detection of Network Based Hiding:** Attackers use covert channels to transfer data by embedding data to packets and packet crafting methods to manipulate header details to transmit data to detect these, investigator use methods such as

  Deep packet inspection: In this investigator examines the exact payloads to find hidden or encrypted content.

  Steganalysis of network traffic: This method is used for identifying hidden data embedded in the packet headers or in payloads

- **Detection of rootkits:** Rootkit is a malicious software which is used to hide data or malicious software in deep levels of operating system

  Behavioral analysis: investigator looks for abnormal patterns such as unauthorized privilege escalation; this conforms usage of tool which may not be seen normally.

  Memory analysis: This memory analysis method is used to detect concealed process drivers, that cannot be seen in standard system listings.

  (Ligh, et. al., 2014; Rutkowska, 2006)

3.2 Detection of Artifact wiping: Artifact wiping is a destruction method used by attacker to completely erase the digital evidences from the storage device, in order to achieve this attacker, use different methods to detect these, investigator use various tools to identify them

- **Detection of File wiping:**

  Master File Table (MFT): records information related to the all the file data even after file wiping by analyzing this MFT, investigator can get information related to the deleted files such as filename, size, timestamps. Investigators can use these records to prove the existence of the file.

  Data carving: In this method digital forensic investigator uses forensic tools to scan unallocated disk spaces to recover fragments of file or partial data from device even after wiping attempts

- **Detection of metadata wiping:**

  Timeline Reconstruction: By using tools like KAPE or Timeline Explorer investigator can reconstruct the activity timelines from different sources such as registry, MFT, Logs, to identify suspicious gaps or inconsistencies to identify metadata wiping.

  Nanosecond precision analysis: In this detection technique digital forensic investigator searches for irregular or abnormal nanosecond values which indicates use

of automated anti-forensic techniques or tools like Metasploit timestamp to detect metadata wiping

Few other detection techniques include USN journal analysis, SI (standard information) vs FN (File Name) attributes comparison to detect metadata wiping.(Garfinkel, 2007, Hosgor 2012)

- **Generic data wiping:** Generic data wiping is the process of permanently deleting the data from the storage device even after that it leaves small traces even after overwriting attempts, that can be used for investigative process.

  Registry Key Analysis: Windows registry stores all the system entry details including information related to the wiping tools, execution history, and even deleted registry entries can be recovered from registry hives, analysis of these registry entries can provide crucial insights about the evidence.

  Entropy and Overwrite Pattern analysis: wiping tools produce a characteristic entropy patterns and byte sequence by analyzing the sector level entropy it will reveal whether data was normally deleted or randomly overwritten.

3.3 Detection of Registry wiping: Registry wiping is the process of deleting or manipulating the registry entries using different tools, in order to detect registry wiping Investigator uses specific methods to recover the registry data

Registry transaction logs: Windows creates a registry transaction logs files for each registry hive to maintain data integrity and it also provides backup of registry files, when attackers overwrite the data these registry transaction logs would still contains the original data which can be used by investigator to prove facts.

Deleted registry recovery: unlike file system deletion, deleted registry keys always leave recoverable remnants by using tools like registry explorer investigator can recover the deleted keys including complete data before deletion.

3.4 Detection of trail obfuscation:

Log tampering detection: Cybercriminals usually overwrite the system logs to conceal the system logs to conceal their actions Nonetheless, the forensic investigators have the capability of identifying tampering by various independent sources of logs.

Baseline Comparison: A baseline of behavioral patterns of normal system activity is created by forensic analysts. Any sharp breaks in the records or lack of anticipated records signify interference. As an illustration, normal business hours ought to reflect certain trends of user log-in/log-out activities. Lack of such anticipated entries is questionable.

Hash Verification: windows operating systems calculate the hash of files to identify a change in files. In case the event logs files have been modified, the hash values will be different to the previously recorded baselines. Such tools as File Integrity Monitoring (FIM) solutions are used to monitor such changes.

4 Detection of attacks against forensic tools:

Attackers deliberately try to target the tools, and methodologies instead of hiding the digital evidences, they use tool or methods such as DOS, compression bombs, to detect and protect against these attacks' investigators use various methods such as

File structure analysis: To avoid attacks on forensic tools investigator scans file structure to find any unusual file structures or compression patterns; by identifying them investigator can prevent attacks on forensic tools.

Resource Monitoring During Extraction*:* investigator uses behavioral analysis tool which flags abnormal usage of CPU and Memory consumption during extraction, if data that is being extracted is original usage CPU and memory is normal but if usage of CPU and memory is higher than the normal it indicates presence of compression bombs because compression bombs require high usage of CPU and Memory.

5. Challenges and Limitations:

- **Tools and techniques limitations:** As the use of technology is increasing, cyber criminals are also using advanced tools that cannot be countered using current forensic tools for example, some analysis methods can produce false positives. This can interrupt investigation process or mislead the case Forensic tools cannot crack or bypass advanced encryption methods. These limitation shows the current limitations of forensic tools.
- **Large volume of data:** Analysis of digital evidence in the current time is a very time-consuming process because existence of large volumes of data, these large data sets analysis process is time consuming and makes it harder to find the evidence in the large data sets.
- **Evolution of anti-forensic tools:** Cybercriminals are continuously developing new anti forensic tools which are more advanced than the currently available forensic tools all of them designed to avoid being detected or to mislead investigation process.

- **Lack of standardization:** There is no universal standard for the digital forensic investigation process, tools, and anti-forensic countermeasure methods. This kind of lack of standardization leads to irregularities in the investigative process or specialized tools to detect anti-forensic techniques.
- **Use of Encryption:** Nowadays almost everyone is using advanced encryption methods to protect their data, encryption like tools VeraCrypt, BitLocker etc. to encrypt their data, without decryption keys or vulnerabilities it cannot be cracked or bypassed using any tool or method. (Gujar et, al., 2023; Surakanthi et, al., 2025)

6. Comparative Review of Existing Literature:

The review of existing states about the Anti-forensic techniques and their impact on the digital forensic investigative process and 8 gaps and future directions

- Detection and Mitigation of Anti-Forensic (Hosgor,2012). this research investigated file system data hiding, network-based hiding, encryption, steganography, artifact wiping, and other attacks against forensic tools, and their detection techniques to identify them. this research emphasized that while many anti-forensic techniques could be detected but evidence recovery is still remained challenging or impossible in most cases.
- Anti-forensic Techniques and its impact on Digital Forensics (Gurjar, Naik, Sardhara, 2023) This paper focuses on understandings of anti-forensic techniques and proposes countermeasures for those anti-forensic techniques. This paper highlights 60% of encrypted data cases remain unprosecuted due to decryption. The study highlights that forensic investigators must maintain awareness of emerging techniques and develop new strategies.
- Countering Anti-forensic tactics in cybercrime investigations: A systematic Review (Surakanthi, Goundar, Dwight, 2025) This research identifies critical gaps in literature, it states about that while existing anti-forensic techniques are widely classified into artifact wiping, data hiding, train obfuscation, attacks on forensic tools explains how these attacks disrupt the specific investigative process.it also evaluated the effectiveness of different techniques, artifact wiping is rated high severity, trail obfuscation as medium and tools attacks as medium to high. Key findings revealed the limitations in current forensic tools.

this review strongly recommends transitioning from reactive forensic methods to proactive approaches including real-time monitoring, SEIM and Block chain integrated intrusion detected systems for enhanced evidence integrity preservation.

7. Future directions:

- The field of digital forensic is advancing well but there still need for countering anti forensic techniques. One of the major issues that need to be addressed is lack of automated detection techniques and tools that are capable of countering specific advanced anti-forensic tools and techniques and almost all existing digital forensic approaches are signature based and reactive making them less effective against advanced and customized anti-forensic tools and techniques.
- Another important gap is there is a need of standard forensic methodologies to evaluate the effective ness of anti-forensic detection tools and standardization of forensic procedures for emerging domains such as IOT (internet of things), serverless architectures.
- Furthermore, one of the important gaps lies in countering anti-forensic techniques is integration of artificial intelligence and machine learning in forensic tools. Future research should focus on implementing standard forensic methodologies in increase the effectiveness of anti-forensic detection tools and techniques. And also, use of AI and Machine learning in forensic framework which can effective in countering anti-forensic tools and techniques.
- Future research in anti-forensic should focus on developing proactive, adaptive forensic methodologies. And it should prioritize the design of forensic tools that are resilient to anti-forensic exploitation.

8. Conclusion:

The review study focuses on anti-forensic techniques and their detection within domain of digital forensics. As cybercrimes are increasing rapidly attackers are using anti-forensic tools to evade detection and mislead investigation. At the same it also includes detection techniques used to counter ani-forensic tools their effectiveness in recovering data even after multiple attempts of erasing the digital evidences and challenges faced by digital forensic investigators during the investigation process and limitations of

current Forensic tools and techniques. This review paper highlights the need for advancements in forensic tools and implementing the universal standard for digital forensic investigative process, introducing new adaptive strategies, integration of AI and Machine learning technologies to counter anti-forensic forensic threats this ensures the reliability and integrity of digital evidence in the cybercrime investigations.

Acknowledgement:

We would like to express our sincere gratitude to **Mr. Vinod Kaaparthi**, Department of Digital Forensic Science, Malla Reddy University, for his valuable guidance, constructive suggestions, and continuous support throughout the course of this research. His academic expertise and feedback significantly contributed to the direction, methodology, and overall quality of the study. We also acknowledge the academic environment and resources provided by Malla Reddy University, which facilitated the successful completion of this work.

References:

1. Garfinkel, S. L. (2007, March 8–9). Anti-forensics techniques, detection and countermeasures. In Proceedings of the 2nd International Conference on I-Warfare and Security (ICIW). Naval Postgraduate School, Monterey, CA, United States. https://hdl.handle.net/10945/44248
2. Conlan, K., Baggili, I., & Breitinger, F. (2016). Anti-forensics: Furthering digital forensic science through a new extended, granular taxonomy. Digital Investigation, 18(Supplement), S66–S75. https://doi.org/10.1016/j.diin.2016.04.006
3. Detection and mitigation of anti-forensics. (2012). *International Journal of Computer Science and Information Security (IJCSIS)*, 10(3), 21–27. Zenodo. https://zenodo.org
4. Al Mutawa, N., Baggili, I., & Marrington, A. (2012). Detection and mitigation of anti-forensics. International Journal of Computer Science and Information Security (IJCSIS), 10(2), 1–8.
5. Behl, A., & Behl, K. (2012). Detection and mitigation of anti-forensics. International Journal of Computer Science and Information Security (IJCSIS), 10(5), 25–31.

6. Garfinkel, S. L. (2007). *Anti-forensics: Techniques, detection and countermeasures* [Conference paper]. International Conference on Information Warfare and Security (ICIW). http://www.simson.net/ref/2007/ICIW.pdf
7. Zdzichowski, P., Sadlon, M., Väisänen, T. U., Botas Munoz, A., & Filipczak, K. (2015). *Anti-forensic study*. NATO Cooperative Cyber Defence Cent Göbel, T., & Baier, H. (2018). Anti-forensic capacity and detection rating of hidden data in the Ext4 filesystem. In G. Peterson & S. Shenoi (Eds.), Advances in digital forensics XIV (pp. 87–110). Springer. https://doi.org/10.1007/978-3-319-99277-8_6re of Excellence. https://www.ccdcoe.org
8. Gurjar, S., Naik, D., & Sardhara, A. (2023). Anti-forensic techniques and its impact on digital forensic. International Research Journal of Engineering and Technology, 10(4), 1669–1674. https://www.irjet.net
9. Jacob, J., & Sandhya, R. (2023). A study of anti-forensic techniques and their mitigation strategies. International Journal for Scientific Research & Technology (IJSART), 9(2), 101–106. https://www.ijsart.com
10. Beebe, N. L., & Clark, J. G. (2005). A hierarchical, objectives-based framework for the digital investigations process. Digital Investigation, 2(2), 147–167. https://doi.org/10.1016/j.diin.2005.04.005
11. Johnson, N. F., Duric, Z., & Jajodia, S. (2001). Information hiding: Steganography and watermarking—Attacks and countermeasures. Springer. https://doi.org/10.1007/978-1-4615-1699-4
12. Garfinkel, S. L. (2010). Digital forensics research: The next 10 years. Digital Investigation, 7(S), S64–S73. https://doi.org/10.1016/j.diin.2010.05.009
13. Rutkowska, J. (2006). Rootkits: Subverting the Windows kernel. Black Hat Briefings.
14. Zander, S., Armitage, G., & Branch, P. (2007). A survey of covert channels and countermeasures in computer network protocols. IEEE Communications Surveys & Tutorials, 9(3), 44–57. https://doi.org/10.1109/COMST.2007.4317620
15. Casey, E. (2011). Digital evidence and computer crime: Forensic science, computers and the Internet (3rd ed.). Academic Press.
16. Ligh, M. H., Case, A., Levy, J., & Walters, A. (2014). The art of memory forensics. Wiley.

learning for network intrusion detection. IEEE Symposium on Security and Privacy, 305–316. https://doi.org/10.1109/SP.2010.25

18. Al-Dhaqm, A., Razak, S. A., Othman, S. H., & Ali, A. (2025). Countering anti-forensic tactics in cybercrime investigations: A systematic literature review. International Journal of Information Security. https://doi.org/10.1007/s10207-025-01131-y

19. The role of digital forensics in modern investigations. (n.d.). *Diverse Daily*. https://diversedaily.com/the-role-of-digital-forensics-in-modern-investigations/

20. Ofori, A. Y., & Akoto, D. (2020). Digital forensics investigation jurisprudence: Issues of admissibility of digital evidence. *Forensic & Legal Investigation Sciences, 6*, Article 045. https://www.heraldopenaccess.us/openaccess/digital-forensics-investigation-jurisprudence-issues-of-admissibility-of-digital-evidence

21. Ofori, A. Y., & Akoto, D. (2020). Digital forensics investigation jurisprudence: Issues of admissibility of digital evidence. *Forensic & Legal Investigation Sciences, 6*, Article.https://forensicfield.blog/uncovering-digital-crime-the-crucial-role-of-forensic-services-in-modern-security/