January - June 2023 Volume 32 Issue 1 PRINT ISSN: 2277-1867
ONLINE ISSN: 2277-8853

JOURNAL OF FORENSIC MEDICINE SCIENCE AND LAW

Official Publication of Medicolegal Association of Maharashtra

MULTISPECIALITY, MULTIDISCIPLINARY, NATIONAL
PEER REVIEWED, OPEN ACCESS, MLAM (SOCIETY) JOURNAL
Indexed with Scopus (Elsevier) & Index Copernicus (Poland)

Editorial Office Address
Department of Forensic Medicine & Toxicology, Third Floor, Library Building, Seth G S Medical College & KEM Hospital, Parel, Mumbai, Maharashtra, India. Pin-400 012. Email id: mlameditor@gmail.com Phone: 022-24107620 Mobile No. +91-9423016325.

JOURNAL OF FORENSIC MEDICINE SCIENCE AND LAW
(Official Publication of Medicolegal Association of Maharashtra)
Email.id: mlameditor@gmail.com

PRINT ISSN: 2277-1867
ONLINE ISSN: 2277-8853

Original Review Article

Anti-Forensics: Tool Against Cyber Forensics

Shyam Narayan Singh[a], Deepanshu Singh[a], Kapil Dev[b*], Atul Kumar Mittal[c], Ankit Srivastava[d]

[a] School Of Basic And Applied Sciences, Galgotias University, Greater Noida, Uttar Pradesh – 201301. [b]Deputy Director, Forensic Science Laboratory, Uttar Pradesh, Moradabad. 244001. [c]Director, Forensic Science Laboratory, Uttar Pradesh, Lucknow. 226006. [d] Associate Professor, Forensic Science, The West Bengal University of Juridical Sciences, Kolkata. 700098.

Article Info

Received on: 29.07.2022
Accepted on: 31.12.2022

Key words
Anti-forensics,
Digital Forensics,
Analysis Tools,
Cyber Crime,
Data erasing
and concealing.

Abstract

Introduction: Anti-forensics refers to a set of strategies and actions used by someone to obstruct a digital inquiry. **Objective:** The aim of this work is to organize the different anti-forensic tools, discussing their potential anti-forensic applications on a system, and provide a category data set that would be helpful to the digital forensic community. **Methodology:** This review paper examines a variety of Anti Forensic methods and procedures, including data concealing, system data erasing, and an attack against forensic technologies that aid in criminal investigations. With the increase in advancement of technology, it will increase cybercrime activities due to this the need of anti-forensic is compulsory for dealing with cybercriminals. **Result & Discussion:** Present backdrop provides important information about anti-forensics in cybercrime. Cybercriminals have recently improved their ability to decrypt forensics tools by practicing new skills. Investigators can recreate an intruder's activities and recover lost files thanks to the various forensic technologies. **Conclusion:** Cybercrime detectives and academics are becoming increasingly interested in Anti- forensic. The exchange of knowledge can be facilitated by a formal definition of anti-digital forensics and common terminology that is relevant to it and makes it possible for better mitigating measures. Any attempts to change, interrupt, negate, or otherwise interfere with forensic investigations that are supported by science are anti-forensics. They categorise anti-forensic mechanisms, tactics, and methods and assess their effectiveness.

1. Introduction

Digital forensic is useful in examination & analysis techniques to gather & preserve evidence from a suitable computing device in a form that is admissible in court. Despite being a relatively young scientific discipline, digital forensics has attracted a lot of attention during the past ten to fifteen years.[1] Digital cyber forensics' objective is to conduct a thorough examination while preserving a recorded chain of evidence to determine precisely what was discovered on that computing device. Examiners and analysts now regularly employ digital forensic techniques.

How to cite this article: Singh SN, Singh D, Dev K, Mittal AK, Srivastava A. Anti-Forensics: Tool Against Cyber Forensic. J For Med Sci Law 2023;32(1):68-73.

Corresponding author: Kapil Dev, Deputy Director & Head of Office, Forensic Science Laboratory, Uttar Pradesh, Moradabad. 244001. Email-ID: kapdevfsl@gmail.com (M): +91- 7017906504.

The enormous volume of data generated by contemporary computer systems, which have emerged as a key source of digital evidence, is what has drawn this attention.[1,2]The offender and the crime scene always exchange information, according to Locard's concept. The cyberspace-related Locard principle improves understanding of the interconnectedness of these types of evidence, their precise time frames of occurrence, and the most significant method to recognize offenders. Anti-forensic investigators dissect & compile all the information into a solo assertion that describes the nature & progression of a certain action.[2] Contrarily, anti-forensics is primarily focused on concealing or changing digital evidence to make it useless in legal proceedings, making it expensive and time-consuming to recover and examine. These concerns are present, along with others regarding the best forensic tools for anti-forensics work.[3]To put it briefly, anti-forensics compromises the usability and benefit of proof in procedures together with forensics for professionals. Anti-forensics actions can be carried out in a variety of ways, and once they are in place, they can have an impact on the course of an inquiry at any point.[2,4]

While most of the techniques are intended specifically to undermine digital forensics, some of these techniques have valid uses. For instance, digital watermarking prevents copyright infringement while encryption safeguards organizational assets.[4] Using such methods against computer forensics may prevent investigators from accessing crucial information.[5] Nevertheless, very little actual work has been done to evaluate the methodologies and essentially determine their suitability up to this point. The goal of this review is to recognize the most common digital AF procedures and examine them with forensic tools. The query of "whether computer anti-forensics can impede the investigation process and prevent real artifacts from being discovered and acceptable in the judicial process" is one of the main issues that needs to be taken care of.[6]

The review study used a variety of methods to find the best review sources. First, rely only on reliable sources from governmental organizations like the judicial system and organizations in charge of developing technical standards.[7] Due to computer-related crimes, digital forensics is an emerging and quickly expanding field.[5,7] Solving instances involving the abuse of digital technology has grown to be the enforcement agencies' main focus. According to several studies and academics, many criminals utilize anti-forensics strategies to conceal their actions so that forensic investigators won't catch them.[8] For instance, AF, as objected to the additional traditional research approaches on automated forensics, is mostly to blame for the dearth of sufficient hypothetical investigations. The forensic expert's retrieval and examination of a digital system must follow specific protocols for electronic evidence to be admissible in court.[9]

The main goal of anti-forensics is as follows:

- Avoid catching any evidence of nefarious conduct that has already occurred.
- Interfere with the acquisition of information by making it nearly unfeasible for the forensic investigator to find any proof that could be used against them.
- When an obstacle is placed in the way of the inquiry, the examiner must spend more time to conclude the case. The procedure is slowed down by anti-forensics, and dissatisfaction sets in. The exhaustion caused by this can make the digital forensic investigator consider giving up.[10]
- Doubting forensic reports or witnesses' testimony, so casting doubt on the admissibility of the evidence in the eyes of the jury or judge.
- Quickest attacks on the forensic examiner, such as finding and altering the examiner's network or bombing the same network which is being investigated, can be used to sabotage forensic tools by utilizing the same methods to target organizations within.

Digital forensics emerged as a new area of computer science in recent decades and has attracted a lot of interest. This is important to take into account because current computer systems store enormous amounts of data, which is effectively the best source of evidence when conducting an investigation.[11] Where the proof must be a comprehensive, dependable, accurate, experimentally lawful, and legally measured evaluation of this evidence reveals and recognizes its relevance.[6] Conlan outlined some of the limitations of a digital forensic inquiry as follows to provide more contexts:

a) Psyche: All forensic investigators employ a variety of techniques during the investigations.[3] Some procedure efficacy varies based on the investigator's intelligence, experience, and background, as well as factors like education and experience. To perform investigations in a way that is comfortable for them, many forensic investigators have built their techniques and procedure. These may have evolved through experience.[7]

b) Implementation of tools: Tools are a key component of forensic investigations. These, however, are vulnerable to compromise, which has an impact on the effectiveness and soundness of evidence results. For example, a forensics expert uses a limited set of techniques, which could hurt the conclusion of their inquiry, as in the case of memory forensics. The cost of purchasing commercial forensic equipment might be very high. The functionality of open-source tools could also be constrained, and they might require some add-ons that aren't always easy to come by.[6,7]

c) Logical/physical challenges: These include timetables and the issue of funding an inquiry, as well as the accessibility or insufficiency of implementing tools such as storage devices, write blocks, firewalls, etc.[7] The pace of technological advancement is faster than the speed of light, and forensics professionals must be adaptable and resilient to keep up.

Due to conflicting technological and regulatory I ssues, no. of difficulties is faced. For instance, encryption is frequently employed as a tactic to protect confidential papers.[11] At the same time, hackers employ encryption to thwart forensic investigations. The famous Apple Vs the FBI order is based on the San Bernardino case, in which the judiciary gave Apple orders to create a new program that would overcome the software security lock, allowing the government to unlock the phones and retrieve the data without going around the security measures. One of these demands was for Apple to digitally sign forensic software that would allow phones seized from suspects in the San Bernardino massacre to be unlocked.[12,13] The authorities asked for help from outside parties to unlock the phones after Apple refused to comply with their demands. The assumption that law enforcement agencies have the right to access these individual areas and details presents several legal issues regarding their eligibility for usual access to such data.[14]

In this study, just three anti-forensic methods will be investigated. These methods consist of:

- Masking of Data
- Encapsulation of Data
- Erasure of Data

The following instruments will be analyzed to gauge the effectiveness of forensic analytical tools:

- Autopsy
- Encase
- FTK Imager

Encase and Autopsy are two programs that can be used to analyze hidden processes and metadata, while FTK Imager can be used to create memory dumps and analyze email traces. While we conducted our investigation using free source software, commercial software is now available with improved reporting and analysis capabilities. As a result, our focus was strictly on the software's analysis of the results.[7,15,16]

2. Review of Literature and discussion

Defining anti-digital forensics:

As stated earlier, academicians and cybercriminal investigators are becoming increasingly interested in anti-digital forensics. Practitioners and scientists may be tempted to oppose anti-digital forensics with their definitions, based on their own experiences, which will differ, if there is no agreed-upon standard definition. Practitioners must be able to recognize the same anti-forensic activities that others have come across in the past, given the development of cybercrime and the abundance of software that can be used to obstruct forensic investigations. Better mitigation techniques can be implemented with the help of a defined definition of anti-digital forensics and a standardized vocabulary of terminology that is relevant to it. So, it would be good to start by highlighting how earlier research defined anti-digital forensics.[17]

Tackling the anti-digital forensics issue

It would be appropriate to become familiar with prior approaches that address the domain as a whole before addressing anti-digital forensics. Numerous works seek to define the subfield of anti-digital forensics and suggest potential solutions for the expanding issue. With the development of technology, forensic investigators are increasingly using new methods to carry out their investigations quickly, efficiently, and successfully.[18] Anti-forensic methods or procedures are those employed to undermine forensic investigation.[19] The recognition and unsheathing of forensic information that may be important to the examination come after the securement of the data source. Data concealment frequently employs the following three methods:

encryption, steganography, and trail obfuscation.[20] Masking and cipher are tools used by cyber criminals to thwart investigators' attempts to identify them and acquire forensic data while maintaining access to themselves.

Encryption, which is frequently used to safeguard data from unauthorized access, has been adopted by cybercriminals to thwart forensic investigations. The tactic is that the existence of the information is not concealed from the examiners, but its legibility is rendered unfeasible, barring additional decryption work.[21] File-based and disc encryption are the 2 types of encryptions that computer criminals most frequently use. File-based encryption converts the contents of the file into a ciphertext that can only be decrypted with the correct key to be read. Disk encryption encrypts the whole storage partition that houses the data, making it impossible to access the disc without a decryption key. Both forms of encryption are supported by encryption programs like Vera Crypt and Cipher Shed.[22]

Steganography

Steganography is a method for hiding data, messages, or files behind more obvious data, messages, or files. As an illustration, consider a subtle watermark tucked away inside a document. The method is applied to video/audio files, photos, and written materials.[23] Once the investigators catch wind of its use, it is quite straightforward to crack. FTK Imager is one example of a simple tool for deciphering ciphered texts. Second, the strategies are only applicable to extremely small amounts of data. Last, hiding a file inside another file changes its appearance, which the investigators may readily detect. Steganography can be used in conjunction with other encryption techniques, such as cryptography, to increase its effectiveness.

Trail obfuscation

The use of various tools and techniques to obfuscate the path of a computer crime is known as trail obfuscation. By altering the timestamps of the files, for instance, to provide a way for the investigators to look in the inappropriate periods, the goal of the present strategy is to deceive or redirect the investigator's line of inquiry away from the criminal’s traces. A culprit can successfully make a file pointless in a courtroom by using these kinds of technologies. A criminal can change a file header's metadata using Transmogrify to hide it. For instance, renaming an image's extension to (.doc) will cause the scanner used by a forensic investigator to leap the altered image because of its (.doc) extension. According to Perklin, a forensic inquiry can be hampered by trail obfuscation for around 15 hours. He suggests several masking methods; file locating, for instance, entails the formation of a record that loop, when followed, returns a monotonous fallacy. This new header contains the source and destination addresses of the following onion router in the network. The messages are encrypted to make sure they arrive at their destination anonymously. Reverse routing is the primary method used by forensic specialists to decrypt the message, which takes a lot of time.

Fake Spoofing is the process of hiding communication to access a structured organization without the necessary user privileges. Internet Protocol spoofing happens the moment an attacker conceals their true IP address by using many IP addresses to carry out malicious actions. When conducting a Distributed Denial of Service Attack, attackers mostly use IP spoofing (DDoS).[24] *Modifying the Metadata Data* that offers details on other data is referred to as metadata; other metadata can often be referred to as "data for a data." There are specific metadata 11 that are related to each file, such as the file's title. Metadata is crucial for learning more about a file because it is descriptive in nature. The type of the file, its size, the author, and the creation/modification date are further instances of metadata.[24]

Any time information is added to or modified in a file that information becomes the file's metadata. Metadata can be created manually or automatically; manually created metadata involves manually entering metadata items by a user; automatically created metadata involves an automated entry by software. Since a user has the freedom to insert any information, they think pertinent, manual production frequently results in more accurate results. Automated metadata is frequently restricted to a small number of components, including a file's size and its *Modification, Accessed, and Created* (MAC) dates, which display some metadata of an image file titled "Metadata."[25] Administrative data describes the Intellectual Property Rights (IPR) of a file and gives technical information about an asset, such as the author of the asset. The handbook advises using an automatic degausser to erase data from hard disc drives; the masquerader works by obliterating the central platters of the hard disc. However, the kind of wiping program, not the category of storage media, is what matters most when erasing data. A common procedure for permanently wiping data from storage devices to stop it from being recovered is called data sanitization. Many professionals in the forensic sector employ and investigate certain data-wiping standards that have generally been shown to be quite effective; few of these procedures constitute the following: [26,27]

- DoD 5220.22 M The US National Industrial Security Program is in charge of creating and maintaining this standard. It functions by overwriting particular data that is kept in a storage device. There are two basic variations of DoD 5220.22 M: a *3-phase* and a *7-phase* series of stages. Three steps make up the dexterity implementation. Writes a zero and checks the write, a one and checks the write, and a random character and checks the write.
- The US National Security Agency created and assisted NCSC-TG-025 The standard is implemented and functionally equivalent to DoD 5220.22 M, although it provides duplicate info.
- P-5239-26 NAVSO The US Navy helped to develop and promote this method. It is implemented like the AR 380-19, but it replaces specified characters with normal character complements and random personalities.
- Gutmann scored 35 passes. Peter Guttmann created this technique. The approach requires 35 passes of overwriting a random part and confirming, as the name would imply. This method is regarded as being outmoded, nevertheless, as storage device technology advances.

3. Conclusion and Future Prospects

The objective of the immense efforts was to gather and organize anti-forensic tools, specifying their potential anti-forensic uses on a system, and providing a category dataset that would be helpful to the AF community. The creation of an expanded taxonomy for the true AF anatomy was another objective, to capture all potential applications within the anti-forensics field. The category data set's scope could be expanded in future work to add more tools, of which there are a number of them. According to the findings, identifying information on anti-digital forensic tools and compiling it into a body of knowledge that is easily available has the potential to be useful and helpful to digital forensic ideologues. Last but not least, scientists working in computational linguistics may be interested in techniques to automate the classification of anti-forensic tools because this may potentially be done by analyzing tool information online and using machine learning. The developing issue of anti-digital forensics would be helped by a further study on this topic as well as in the field in general.

Contributor ship of Author: All authors equally contributed.

Conflict of interest: None to declare.

Source of funding: None to declare.

References:

1. Kessler GC, Carlton GH. Exploring myths in digital forensics. Int J Interdiscip Telecommun Netw. 2017; 9(4): 1–9.
2. Harris R. Arriving at an anti-forensics consensus: Examining how to define and control the anti-forensics problem. Digit Investig. 2006; 3:44-9.
3. Neralla S, Bhaskari L, Avadhani P. Combating anti-forensics aligned with e-mail forensics. Int J Comput Appl. 2013; (79): 16–9.
4. Cohen F. The science of digital forensics: Recovery of data from overwritten areas of magnetic media. Journal of Digital Forensics, Security and Law. 2012; (7)1: 7-20.
5. Berghel H. Hiding data, forensics, and anti-forensics. Communications of the ACM.2007 ;50(4):15-20.
6. Mothukur A R. Balla A. Taylor, D H, Teja Sirimalla S, Elleithy K. Investigation of countermeasures to anti-forensic methods, 2019 IEEE Long Island Systems, Applications, and Technology Conference (LISAT). 2019; 1–6.
7. Colan K. Baggili I. Breitinger F. Anti-forensics: Furthering digital forensic science through a new extended, granular taxonomy. Digit Investig. 2016; (18): 66–75.
8. Garfinkel S. Anti-forensics: Techniques, detection and countermeasures. In2nd International Conference on i-Warfare and Security 2007; 20087:77-84.
9. Jahankhani H, Beqiri E. Memory-Based antiforensic tools and techniques. International Journal of Information Security and Privacy (IJISP). 2008;2(2):1-3.
10. Qureshi MA, El-Alfy ES. Bibliography of digital image anti-forensics and anti-anti-forensics techniques. IET Image Processing. 2019;13(11):1811-23.
11. Berinato S. The rise of anti-forensics. 2007. [Cited 29october 2021] Available from:

https://www.csoonline.com/article/2122329/the-rise-of-anti-forensics.html.

12. Froomkin D. McLaughlin J. FBI vs. apple establishes a new phase of the crypto wars. 2016. [Cited 29 october 2021] Available from: https://theintercept.com/2016/02/26/ FBI-vs-apple-post-crypto-wars/
13. Pfefferkorn R. Apple vs the fbi: Where did it come from? What is it? Where is it going? (2016). [Cited 29october 2021] Available from: https: //cyberlaw.stanford.edu/files/blogs/Riana%20BIPLA %20talk%203-7-16.pdf
14. E. Hofverberg, "Government access to encrypted communications: Sweden," May 2016. [Cited 29october 2021] Available from: https://www.loc.gov/law/help/ encrypted-communications/sweden.php
15. "Hemlig dataavläsning justitieutskottets betänkande 2019/20: juu19.":Sveriges Riksdag. Secret data reading. [Cited 29october 2021] Available from: https://www.riksdagen.se/sv/dokument-lagar/arende/betankande/hemlig-dataavlasning_H701JuU19/html
16. Lee K. Hwang H. Kim K. Noh B. Robust bootstrapping memory analysis against anti-forensics. Digit Investig. 2016; 18.
17. Harris R. Arriving at an anti-forensics consensus: examining how to define and control the anti-forensics problem. Digit Investig. 2006; 3: 44e9.
18. Thuen C. Understanding counter-forensics to ensure a successful investigation. Department of Computer Science, University of Idaho, Moscow, Idaho (pdfs. semanticscholar. org/d5b6/b658d9178dbcdf33e095a53c45b4f7a43fc 8. pdf). 2007.
19. Pajek P, Pimenidis E. Computer anti-forensics methods and their impact on computer forensic investigation. In Global Security, Safety, and Sustainability: 5th International Conference, ICGS3 2009, London, UK, September 1-2, 2009. Proceedings 5 2009 (pp. 145-155). Springer Berlin Heidelberg.
20. Peron CS, Legacy M. Digital anti-forensics: emerging trends in data transformation techniques. 2005.
21. Rogers M. Anti-forensics: the coming wave in digital forensics. Retrieved September. 2006 Sep; 7:2008.
22. Smith A. Describing and categorizing disk-avoiding anti-forensics tools. J Digit Forensic Pract. 2007;1(4):309-13.
23. Types of metadata (plus examples uses for each). Jan 2020. [Online] [Cited 29 october 2021] Available from: Available: https://merlinone.com/types-of-metadata/
24. Easttom C. CCFP certified cyber forensics professional certification: exam guide. McGraw-Hill Education, 2015.
25. Home. National Security Agency/Central Security Service. [Cited 29 october 2021] Available from: https://www.nsa.gov/resources/everyone/ media-destruction/
26. Fisher T. 38 free programs to completely wipe data from hard drives in May 2020. [Cited 29 october 2021] Available from: https://www.lifewire.com/ free-data-destruction-software-programs-2626174
27. Author CCW, "8 effective algorithms to wipe and erase data permanently," Mar 2017. [Cited 29 october 2021] Available from: https://www.datanumen.com/blogs/ 8-effective-algorithms-wipe-erase-data-permanently/
28. Wei M, Grupp L, Spada FE, Swanson S. Reliably Erasing Data from {Flash-Based} Solid State Drives. In9th USENIX Conference on File and Storage Technologies (FAST 11) 2011; (04): 105–117.