Detecting and Mitigating Anti-Forensic Techniques: A Comprehensive Framework for Digital Investigators

Nadia Asim*
School of Computer Science and Engineering
University of Westminster,
W1W 6UW London, UK
nadiaasim340@gmail.com

Jude Osamor*
School of Computing & Creative Technologies
University of the West of England,
BS16 1QY Bristol, UK
Jude.osamor@ieee.org

Funminiyi Olajide
School of Computer Science and Engineering
University of Westminster,
W1W 6UW London, UK
F.Olajide@westminster.ac.uk

Njideka Okeke
Senior Finance Manager
Modern Work and Security
Microsoft,
Washington, USA
njideka.okeke@gmail.com

Celestine Iwendi
School of Creative Technologies
University of Bolton,
Deane Road, Bolton, BL3 5AB
C.Iwendi@bolton.ac.uk

***Abstract*— The main goal of anti-forensics tools and techniques are to "frustrate" not only the investigators but also the forensic tools used such as Sleuth Kit. Anti-forensics is quite exactly the opposite of Cyber Forensics. These tools affect an investigation negatively making it harder to reach a conclusion. Anti-forensic methods include operations such as deliberate deletion of data by means of overwriting it with new data by using anti-forensic tools, safely wiping out data that cannot be restored ever, altering the file properties to avoid being identified in timeline analysis and many other such methods. [1] While tools such as Autopsy, X-Ways, FTK, EnCase present the ability to detect some anti-forensic techniques if not all, these are not particularly dedicated for anti-forensic technique detection. To summarize, general forensic tools as mentioned above, perform several functions on the data source, of which anti-forensic is just one aspect. Though there exist tools like Timestomp Detector that are made for detecting altered file timestamps. Again, it is specific to only one feature and not many of the anti-forensic techniques. This dissertation aims to develop a dedicated framework that can help detect a few anti-forensic techniques based on user input. This will be integrated within a website format in order to make it easy for the users. This type of prototype could be very useful for investigators working on cases. Instead of going through the entire disk image, that could potentially take hours, investigators could separate any suspicious files and use this detection framework to identify if any of the files have been altered or managed using the anti-forensic techniques.**

***Index Terms*— Anti-Forensic, Cyber Forensic, Detection Techniques.**

INTRODUCTION

Cybercriminals are constantly growing in number, finding new loopholes amidst ever-evolving technology. These 'loopholes' help them avoid getting caught. They use a variety of strategies referred to as 'anti-forensic techniques to thwart off digital investigations and hide illegal activities. The attackers are getting smarter with the methods they employ to avoid detection and continue with their exploitation of systems that have been compromised. This comes with the need to meet the strongly growing field of forensics which again is essential to handle the increasing complexity of cyber threats. Methods such as data hiding, encryption etc., help attackers make it difficult for law enforcement to complete their process of identifying, collecting and analyzing digital evidence that could prove of value in court to prosecute the criminals. [2]A conference paper published in 2014 quite simply highlighted the fact that most of the crimes taking place in today's world involve digital devices which have made law enforcement officials pay equal attention to digital evidence just as eyewitnesses. While investigators take proper steps to ensure the digital evidence from devices is recovered intact, the criminals, on the other hand, take even stricter measures to conceal or destroy any evidence trail which in turn makes the investigation even harder. [3]

In an era where digital evidence is considered to be one of the most crucial pieces of evidence in solving a case and reaching the possibility of conviction, the rise on anti-forensic techniques stands as a serious threat in way of forensic investigations. Cybercriminals are constantly utilizing advanced methods to alter, erase or hide any digital traces, making it a huge difficulty for the investigating officials to reach the truth. Inspired by a desire to provide an improved tool for DF professionals, the proposed dissertation aims to contribute to further enhancement of the field of forensics. The tool will be able to analyze user inputs and study for any anti-forensic techniques within the file. The results will be presented to the user which would alert them of any malicious content existing in the file.

Through this design, the goal is to leave an impact on the field of cyber and forensics which can possibly pave the road for more enhanced tools and broader effort to ensure security in the digital world.

In recent years, anti-forensic techniques have picked up quite the pace, leaving investigators baffled seeing the ever-evolving tactics being employed by criminals. This has made it tougher for investigations to reach accurate conclusions which at times might also lead to wrong convictions. For detecting such techniques, the tools present in the market are very scarce. The research has addressed this issue and has provided a solution where a tool is built focusing on identifying four such tactics. This is on a prototype stage, as a start to build something much enhanced in the future. The web app is designed in a simple manner so that it doesn't require much learning time. All this combined in one powerful tool could contribute hugely towards the department of legal enforcement, police and other related entities.

This research follows an exploratory design approach which is ideal for delving into the under-explored domain of anti-forensic tactics. Since the research is experimental in nature, it permits flexibility and adaptability, which is vital when studying the various existing and evolving techniques that hackers use to evade DF investigations. The objective was to identify current trends, build a deeper understanding of these techniques and eventually come up with a framework that digital / law enforcement officials could use. Applied research methodology was employed for building of the prototype, since the core of this methodology is focused on solving more actual problems and development of tools as a solution to the problem. [4]. The research initiated with a thorough assessment of the literature, in order to identify prevalent anti-forensic approaches and any existing tools that detect such techniques. This was followed by the development of a system aimed at enhancing detecting abilities of forensic investigators. The next step was where the framework was converted into a web application which offered a useful tool for determining specific anti-forensic methods depending on user input. The results will then be presented to the user in a report file. The inputs could be easily customized to ensure the effectiveness of the detection framework.

I. PROBLEM STATEMENT AND OBJECTIVES

Law enforcement agencies and digital forensic investigators face major issues with the widespread implementation of advanced anti-forensic tactics. Some of the methods among many involve log and time manipulation, encryption and wiping of data and so on. These are gradually becoming easier to use, giving efficient results. A 2023 report from the CISA (Cybersecurity and Infrastructure Security Agency) stated that anti-forensic methods are currently being used in more than 60% of major cyberattacks, making it severely problematic to trace back to the source of attacks or retrieve essential evidence. [5]

Impact: It acts as a hinderance for forensic investigators amidst an ongoing investigation which can lead to inconclusive results. Consequently, the conviction rates of cybercriminals will drop and on the other side of the scale the investment in not only restoring the damages caused by these criminals, but also implementing preventive measures to avoid such situations, will see a drastic rise [6] [17].

Attackers use such techniques to stay within the system without being caught. Their prolonged stay also means them being able to roam within the network and get access to confidential details. If stolen, it would result in fraud, monetary losses, possible ransom ask and even identity theft. This event kickstarts a whole chain of downfall with damage to the company's reputation leading to sale decline and lost trust [6].

Competitive companies trying to be on top in their fields also at times employ such techniques through which they could steal valuable trade-related information and any other secrets that could be advantageous to them.

OBJECTIVES:

- Design and execute a strong framework that has the ability to detect the four mentioned anti-forensic techniques (steganography, data wiping and encryption, timestomping), based on the user given input such as a file path.
- Integrate the framework into a flask-based website to convert it into a web-based tool to ensure easy access and use by authorized officials.
- Secure the framework with a set username and password login structure so that it is not accessible to everyone.
- Conduct testing of the built framework using a variety of inputs to evaluate its accuracy in identifying tampered files.
- Customize input files in order to ensure all techniques involved are detected.
- Present the results to the users in a pdf report format.
- To offer appropriate strategies for mitigation.
-

II. LITERATURE REVIEW

A conference paper stated the opinions on anti-forensics being divided into 2. People who debate that AF techniques can act as a shield for a good person from an evil government and people who oppose AF techniques as that can disallow a good government from looking into an evil person.[2]

1. Data Hiding: There are a variety of ways in which data can be hidden. Steganography being the most common from the 1990's. Stego tools/software's are present for all computer devices, this allows users to hide information within any type of file such as a document, video, images, .exe, and even audio files. These files act as carrier files which carry this hidden information to their destination. Other regular methods that do not use any software can also be utilized, such as hiding your data under an image or a table in regular documents. Other ways to confuse investigators and hide data would involve tricks like using file names which uses letters similar to English alphabet but are not English, the file then seems like a normal file but may actually hide data. Modifying a files path by making it longer, which makes it difficult for the system to manage and detect the file. A main server, if not well secured, the criminal could easily hide data in someone else's user space. [7]

2. Data Wiping: Various tools for erasing data are present such as Eraser, BC Wipe etc. These tools destroy data within the given files by carrying out overwriting multiple times that makes original data recovery close to impossible. Software like Secure Clean and Evidence Eliminator completely remove cache files, different browser's history, slack space and even few OS files. There are numerous tutorials that address specifically which files should be removed to hinder forensic analysis. [8]. Forensic examiners are faced with a more challenging analysis when criminals use data wiping tools, nonetheless these tools are not flawless. The majority of the programs leave noticeable evidence of their wiping and many of them are not as effective as they usually claim to be, frequently leaving behind traces of the exact items they claim to have removed. [9]

3. Obfuscation of Trail: Cybercriminals try their best to lead the investigators in the wrong direction by leaving out misleading or fake clues or at times just bring them to a 'dead end' by completely hiding their tracks. Time stamp and log file manipulation, erasing or altering system events and server log files or even regular files are some examples. Any discrepancies with these point to a probable trail obfuscation. There are several anonymous email services that ensure the identity of sender remains untraceable using tricks like fake headers, open SMTP proxies and so on. [10]

4. Data Encryption: Although encryption is frequently used to safeguard data from unauthorized access, cybercriminals have begun using this to hinder forensic examinations. This tactic renders data unreadable without the use of decryption, but it does not conceal the data. Encryption software is publicly available for use, which criminals make use of to perform encryption on data or disks, this makes the data close to impossible to read without the accurate decryption keys. Computer criminals typically use two common forms of encryption: disk encryption: encryption of complete storage device, requiring a decryption key and file encryption: converts contents of the file into ciphertext that can solely be accessed through decryption with the right key. VeraCrypt and other such programs support both of these encryption types. Cybercriminals are obligated by the Regulation of Investigatory Powers Act of 2000 in the UK, to grant access to all the data they may have that could be relevant to a forensic inquiry. Due to data that cannot be accessed, approximately 60% of cases which involve encrypted data are never prosecuted. [11]

5. Attack on Forensic Tools: The forensic process consists of six essential steps: identification of evidence, preservation of evidence, gathering the evidence, examination and analyzing of digital evidence and finally presentation of evidence in court. It took several years to establish ground rules on what could be acceptable evidence in court, and which could not be. The Daubert test was established in 1993, which is a procedure that helps courts determine the admissibility of evidence [12]. When anti-forensic techniques attack the process and forensic tools, the reliability of evidence comes in question, which then might become useless in court. There have been attacks carried out effectively on tools such as SleuthKit, FTK, EnCase etc. Various programs have been presented for several years that manipulate NTFS file tables, FAT directory and file signatures. DOS has also been popularly used to attack forensic tools in a way that exhausts crucial resources such as the CPU and RAM which are vital for the tools, a criminal can delay the investigation. [10] [7]

Few techniques that could potentially be applied for DoS attacks against DF tools include ZIP bombs (commonly known as zip of death), is a harmful file that is designed in such a way that when any program or system attempts to read it, the entire system will crash. These bombs are often implemented to deactivate any antivirus software present within the system so that traditional viruses could easily get into the device. These could also be used to carry out an attack on forensic tools. [13]

III. DEVELOPED SYSTEMS

The widely used Metasploit Framework, a pen testing tool, developed by H.D Moore and his team in 2003, later saw the integration of the Anti-Forensic tool with the Framework, expanding its capabilities.. This specific tool was developed by Bishop Fox, a multinational enterprise that focuses on computer and network security. The Metasploit Anti-Forensics Project (by Bishop Fox) includes several AF tools such as Timestomp, Slacker (hides data in file system) and Sam Juicer, all which contribute to altering or hiding data and ensuring no traces are left behind [14]. Additionally, there are several other tools focused on specific anti-forensic techniques. These include wbStego, OmniHide, PRO, DBAN and Universal Shield, which specialize in data wiping, steganography (data hiding), modification or encryption.

COMPARISION: The tool developed in this research offers a web-integrated, user-friendly solution specifically tailored for investigative purposes. Its goal is to extend the practical applications of the concepts outlined above by addressing key anti-forensic techniques comprehensively. The framework targets four main anti-forensic techniques – encryption, wiping, steganography and timestomping, making sure of an absolute analysis and precise detection on a user-provided input. Unlike existing tools that often specialize in one or two techniques, this solution integrates the detection and analysis of multiple methods within a unified framework. This integrated approach simplifies the investigative process and ensures more thorough and precise detection. This framework is also then converted into a web-based tool with a safe and secure login system that lets users only use already provided login credentials instead of signing up, this reduces the chances of unauthorized users entering the system.

IV. METHODOLOGY

Data Collection: Owing to the investigative nature of the study, the primary sources of data collection range from academic journals, conference papers to technical documents from prominent cyber firms in the industry. Crucial repositories such as IEEE, Google Scholar and Xplore were made use of to access appropriate publications. These sources shed light on latest AF techniques as well as the weaknesses of currently available forensic tools. As the goal was to build a theoretical and practical knowledge of anti-forensic techniques rather than empirically validate them through surveys or inquiries, there were no participants involved for data collection. Instead, an **applied research methodology** was adopted to facilitate the understanding and development of a robust framework. It was essential to study the logic behind these techniques to make sure that when the program runs, it accurately picks the anti-forensic technique within the given file input. Additionally, online videos demonstrating the creation of basic tools related to this topic were reviewed to gather data for backend design considerations.

Data Analysis: To determine the largely prevalent and difficult AF tactics for digital forensics, data that was gathered from papers and publishes were studied. The foundation of AF detection framework was built using a categorization system, that incorporated popular techniques, leveraging insights gained from the analyzed data. The exploratory research approach helped pinpoint gaps in current forensic tools, providing valuable insights to address these deficiencies in the proposed framework prototype. Following the applied research technique, the data collected on development of the framework was analyzed which aided in precisely identifying the software tools and packages that would be required for successful implementation. The data also helped in understanding the structure and logic behind the working of the techniques and how it looks through the input file.

Framework Development: The framework was developed in a step-by-step manner, actively incorporating any findings from the research conducted previously. The procedure comprised identifying particular AF techniques such as steganography, data wiping, data encryption and timestomping. Every technique was examined to learn about its features and how these techniques may be detected using appropriate forensic approaches. **Python** was chosen as the primary programming language for framework development due to its extensive library support. Key libraries included **Flask** (for web integration), **EWF** (for reading formats like E01 files), and others to ensure seamless functionality of all components. This framework was then included within a web tool for a more user-friendly experience. For the purpose of front-end development, HTML (designing), JavaScript (logic) and CSS (styling) were used. Flask served as the web framework on which the tool was developed and integrated into the website. This will allow the user to easily check the required files for any alterations.

As a part of the development process, test scenarios and test input files were created to validate the framework's performance and reliability. These tests ensured the framework's capability to accurately identify tampered files, demonstrating its efficacy and robustness in real-world applications.

V. SYSTEM ARCHITECTURE

Several components together form a fully functional system. It is an essential part of any technology-driven development since it establishes system parameters, modules, data flow and user system interaction. [21] To understand the architecture and working of the prototype, it is vital to understand the functionality of each module separately.

User Interface:

Once the prototype functionality is completed, the next crucial part is to ensure the tool is built in a way that is easy to navigate by the user and still looks presentable with no overcrowding. Here the popularly used flask framework is being utilized. It is a lightweight web-based framework specially designed for python, allowing developers to quickly integrate their system into a web app. This website was developed with appropriate styling, and it lets users upload files and view results in one click. Since different techniques are being checked which may involve different file types, the backend was designed to support different types of extensions specifically in case of encrypted files.

File Input:

A textbox that takes the file path given by the user, with no character limit. The 'Analyze' button below it validates the file path and sets it up for processing to look for any AF techniques present within it.

Anti-forensic detection engine:

This tool utilizes detection algorithms that run on the backend and work on the users input. There are four main modules:

Steganography Detector: Takes in the input and works through to look for any hidden data within the file.

Data Wiping Analyzer: Checks if the file has any overwritten data which points to the fact that information has been erased and made it unrecoverable.

Timestomping Identifier: Detects if the file's accessed, modified or created date has been tampered with by using specific algorithms.

Encryption Detector: Checks for file extensions and headers which could potentially point towards encryption.

Pdf Generator:

This generates the results in a pdf format which includes the file path, and all possible techniques detected within the file input. It also gets downloaded and saved on the user's device.

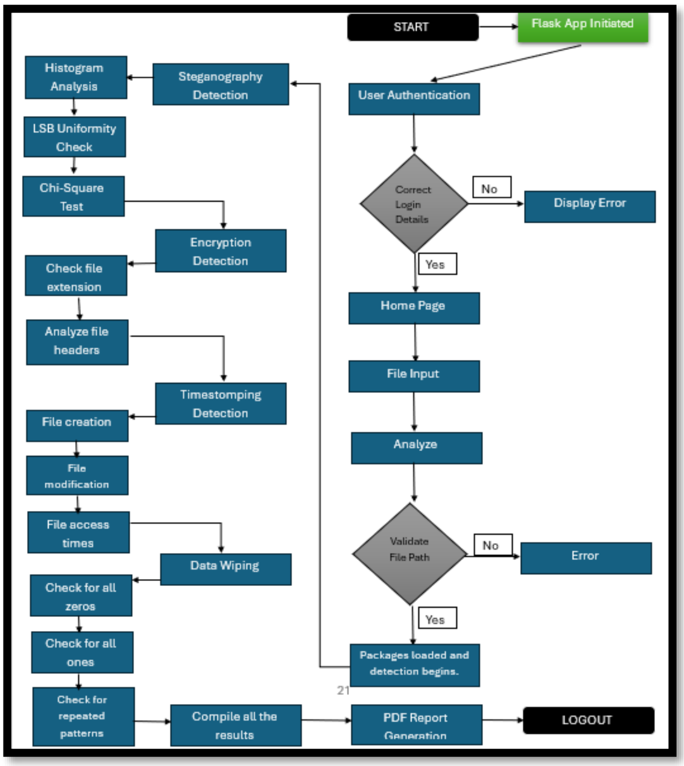


Figure 1: Flow of the tool

VI. RESULTS

Assuming the login details are verified, the home page is displayed. This space allows the user to enter the file path they want to analyze for detecting anti-forensic techniques. The user must click on 'Analyze' to initialize the file processing.

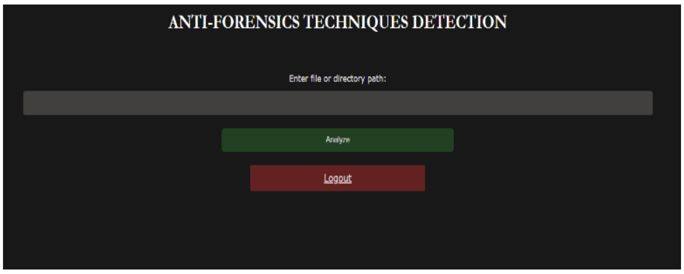
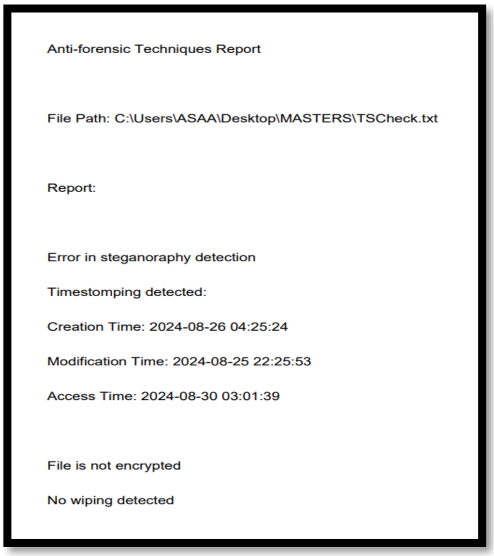

ANTI-FORENSICS TECHNIQUES DETECTION
Enter file or directory path:
Analyze
Logout

Figure 2: Homepage

Sample Input Files were created using some online resources such as **Bulk File Changer** (Timestomping), **OpenStego** (Steganography), **Hex Editor** (Data Wiping) and **Hat.Sh** (Encryption).

Here the file path of a timestamp modified file has been given and the Figure 3 below accurately displays the timings and identifies time stomping. It shows that there have been alterations in the timestamps since creation time is greater than the modification time. It tests false for all other functions.

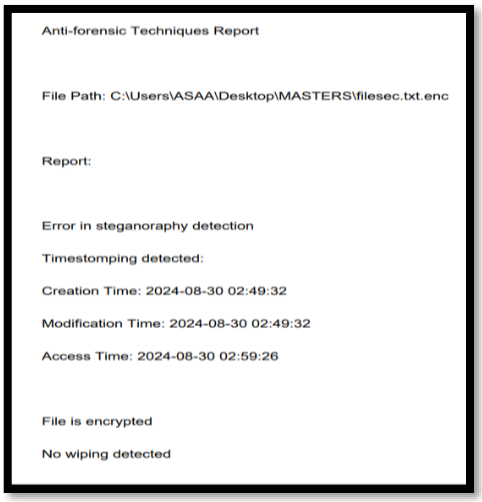


```
Anti-forensic Techniques Report

File Path: C:\Users\ASAA\Desktop\MASTERS\TSCheck.txt

Report:

Error in steganoraphy detection
Timestomping detected:
Creation Time: 2024-08-26 04:25:24
Modification Time: 2024-08-25 22:25:53
Access Time: 2024-08-30 03:01:39

File is not encrypted
No wiping detected
```

Figure 3: Output Report

An essential point to keep in mind is that the timestomping feature is quite sensitive when it comes to picking up anomalies in timestamps of the files. This will be spoken about in a later section.

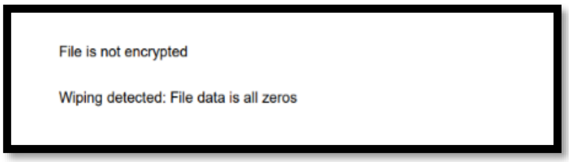
For an encrypted file path, the function inspects the file for headers and file extensions, based on which it takes a decision. Here, the result says, 'file is encrypted'. Here since the access and modification times are quite close, it detects positive for timestomping.



```
Anti-forensic Techniques Report

File Path: C:\Users\ASAA\Desktop\MASTERS\filesec.txt.enc

Report:

Error in steganoraphy detection
Timestomping detected:
Creation Time: 2024-08-30 02:49:32
Modification Time: 2024-08-30 02:49:32
Access Time: 2024-08-30 02:59:26

File is encrypted
No wiping detected
```

Figure 4: Output Report (2)

It is important to notice that the wiping function goes through four checks: empty file, all zeroes, all ones and random patterns. The below output is for that of file with zeroes.



```
File is not encrypted

Wiping detected: File data is all zeros
```

Figure 5: Output Report (3)

The below present table presents the overview of results which were demonstrated by the tool.

Table 1: Results

Feature	Description	Outcome/Result
Steganography Detection	Uses histogram analysis, LSB uniformity check, and chi-square test to detect hidden data.	Couldn't accurately present results of hidden data in the pdf, instead showed in terminal.
Encryption Detection	Detects encrypted files through file extensions and byte pattern/header analysis.	Accurately flags encrypted files with specific extensions or distinct patterns in the file headers.
Timestomping Detection	Compares file creation, modification, and access times for discrepancies or future timestamps.	Flags suspicious timestamps effectively when they deviate significantly from expected norms.
Data Wiping Detection	Analyzes files for zeroes, ones, repeated patterns, or high entropy to detect overwritten data.	Accurately identifies wiped files based on these patterns, though more extensive testing might be required.
PDF Report Generation	Generates a PDF report summarizing detected anti-forensic techniques for user input.	Successfully creates a readable and downloadable report format for easy interpretation by investigators.
Accuracy	Evaluating the detection accuracy across implemented techniques.	High accuracy for the four main techniques tested, with occasional false positives/negatives.
Performance	Speed and resource efficiency of the framework during execution.	Efficient for small to medium datasets but may slow down when scaling larger datasets or more complex inputs.
Usability	Ease of use for investigators via a web-based interface.	User-friendly interface allows file upload and results retrieval with minimal effort.
Limitations	Challenges identified in testing and functionality.	Limited to detecting only four AF techniques with steganography error; requires updates for evolving techniques and broader applicability. Need to lessen false positives/negatives.

VII. PERFORMANCE ANALYSIS

Table 2: Performance Stats in comparison to other tools

Parameter	**Existing Tools**	**Proposed Tool**	**Advantages of Proposed Tool**
Primary Focus	Forensic tools like FTK, Autopsy, EnCase focus on data recovery and analysis of file systems.	Focused on detecting anti-forensic (AF) techniques (encryption, wiping, steganography, timestomping).	Tailored detection of AF techniques not addressed comprehensively by other tools.
Detection Methods	Signature-based detection of tampered files (FTK, Autopsy).	Implements multiple detection algorithms for each AF technique (e.g., histogram analysis, entropy checks).	Reduces reliance on signature matching, minimizing false negatives.
Coverage	Existing tools like ADS Spy or Timestomp Detector target individual techniques.	Unified framework covering multiple AF techniques in one tool.	Simplifies investigation by providing a consolidated approach.
Limitations	Tools may fail to detect advanced or evolving AF techniques.	Currently limited to four AF techniques; prototype stage.	Opportunities for scalability and inclusion of advanced algorithms or AI/ML.
False Positives/Negatives	High, due to reliance on signature-based detection.	Minimized by employing algorithmic checks for logical inconsistencies.	Improves accuracy by reducing reliance on pre-defined signatures.
Customization	Restricted by default configurations.	Easily customizable for investigators, allowing flexibility to add features based on case-specific needs.	Tailored to evolving investigation requirements without dependence on external software updates.
Security Features	Standard authentication systems.	Secure login system with pre-assigned credentials (Flask framework).	Reduces unauthorized access and ensures compliance with privacy regulations.

VIII. LIMITATIONS

The tool being a prototype, does lack in a few spaces and has potential of improvement. It is vital to give preference to these limitations first while enhancing the system.

- After the files are analyzed, it is important for the results to be displayed within a PDF format generated report. This works effectively for all techniques except for steganography which displays the results within the terminal. This could be an issue since the user can't access the terminal, they might not be able to visibly see the results.
- The tool is limited to a few specific techniques, within those techniques the method checks are also limited, which can hinder the tool's performance.
- Timestomping detection is a sensitive feature that picks up the slightest modifications which could also be a limitation of the tool as it could confuse the users. In modern Windows systems, the access time of a file can be updated even if a user just reads the file metadata or checks the properties. This might also confuse the function.
- Within data wiping feature, the result for file of all ones reads as 'repeated patterns' instead of 'all ones'. It is due to the fact that hex editors, when producing file of all ones, tend to add invisible space/data or alter some metadata that doesn't fit the condition to check for all ones. Hence it reads as 'repeated patterns'.

IX. SECURITY CONCERNS OF THE TOOL

Evasion Tactics: It is highly possible that attackers may come up with more newer techniques of anti-forensics, which may help them avoid detection by the tool. Therefore, it is important that the tool is constantly being updated with changing times.

False Positives: It may incorrectly raise the flag on a file where some legitimate activity might have occurred, this could lead to false positives.

False Negatives: Since it works on identifying four main AF techniques, it may fail to identify other techniques, leading to false negatives.[16]

Scalability: A huge challenge would be scaling the tool to adapt and identify various anti-forensic techniques present, along with it, processing several file extensions.

Data Compliance: Because sensitive data is involved in this situation, any protected data, if exposed, can cause compliance issues.

Several attacks can be carried out on digital forensic tools and process through altered logs, images, videos, emails and even pdfs. Few techniques that could potentially be applied for DoS attacks against DF tools include ZIP bombs (commonly known as zip of death), is a harmful file that is designed in such a way that when any program or system attempts to read it, the entire system will crash. These bombs are often implemented to deactivate any antivirus software present within the system so that traditional viruses could easily get into the device. These could also be used to carry out an attack on forensic tools.[16]

X. RECCOMENDATION

S.H Saeed and others mention in their paper the sphere of digital forensics saw rise in research on two major topics, which were attacks on computer security and online frauds. Several forensic techniques exist which concentrate on legitimacy of digital artifact by examining it to avoid spreading of online forgery. On the opposite side, anti-forensic techniques have a negative effect on the authenticity of evidence related to an investigation. AF is used to manipulate and alter or delete any traces of anti-forensic being used within the file or artifact which could also be the evidence. This prevents investigators from retrieving evidence in a reliable manner or even discovering any other evidence.[20] This makes it all the more essential to ensure that a tool like this is built and implemented.

This tool has areas for improvement that for now have been left unexplored due to resource, funding and time constraint. There are several features that could be added on to utilize the potential of the tool to its maximum. Some of them could be the following:

a. The tool could be expanded in regard to the number of anti-forensic techniques being implemented. The prototype has used four techniques, other such existing techniques could be hard-coded and integrated into this tool.
b. The limitations could be worked upon such as editing the timestomping feature and setting it with a more stricter parameter in order to reduce false positives.
c. A database could be integrated into the tool that saves data for future use and ease of access.
d. The features such as steganography, data wiping, encryption could be developed in a way that within the results, the file contents are also revealed.
e. Integration with AI/ML could also prove to be a benefit in terms of reading the contents of file and pointing out exactly where the techniques have been used.
f. SIEM system, if incorporated within the tool, can provide investigators with real time monitoring and alerts which can enable a quicker response.[22]

XI. CONCLUSION

The emergence of anti-forensic methods presents a serious obstacle to digital forensic enquiries, making it more difficult to unearth the truth about cybercrimes. Since fraudsters are using these strategies more frequently to avoid detection, our study emphasises the critical need for specialised technologies that can identify and counteract them. The suggested framework is an important step towards improving the skills of digital investigators since it identifies important anti-forensic techniques like steganography, data wiping, encryption, and timestomping. By incorporating this architecture into an intuitive web tool, we enable forensic experts and law enforcement to quickly examine questionable files, increasing the precision and effectiveness of their investigations. Continuous development and modification of forensic tools will be necessary as cyber threats continue to change in order to guarantee that justice is served and integrity of evidence is preserved.

XII. REFERENCES

[1] S. Garfinkel, "Calhoun: The NPS Institutional Archive Faculty and Researcher Publications Faculty and Researcher Publications," 2007. Accessed: Jun. 30, 2024. [Online]. Available: https://core.ac.uk/download/pdf/36736409.pdf

[2] Z. H. Abdullahi , N. Sagarwal, and M. Soni, "An Overview of Anti-forensic Techniques and their Impact on Digital Forensic Analysis," in *4th International Online Multidisciplinary Research Conference*, Hyderabad, India: Osmania University Centre for International Program, Oct. 2020.

[3] Gurpal Singh Chhabra, "Anti-Forensics Techniques: An Analytical Review," *ResearchGate*, Aug. 07, 2014. https://www.researchgate.net/publication/275155942_Anti-Forensics_Techniques_An_Analytical_Review

[4] A. research, "What is Applied Research? Definition, Types,

Examples | Appinio Blog," *www.appinio.com*. https://www.appinio.com/en/blog/market-research/applied-research (accessed Aug. 12, 2024).

[5] M. Fabro, L. Perch, and E. Cornelius, "Creating Cyber Forensics Plans for Control Systems," 2008. Available: https://www.cisa.gov/sites/default/files/recommend_practices/Forensics_RP.pdf

[6] B. Sartin, "ANTI-Forensics – distorting the evidence," *Computer Fraud & Security*, vol. 2006, no. 5, pp. 4–6, May 2006, doi: https://doi.org/10.1016/s1361-3723(06)70354-2.

[7] G. Kessler, "Anti-Forensics and the Digital Investigator ," in *Australian Digital Forensics Conference*, Edith Cowan University, Dec. 2007. Accessed: Aug. 11, 2024. [Online]. Available: https://ro.ecu.edu.au/cgi/viewcontent.cgi?article=1000&context=adf

[8] Miroslav Ölvecký and Darja Gabriska, "Wiping Techniques and Anti-Forensics Methods," *ResearchGate*, Sep. 2018. https://www.researchgate.net/publication/328834436_Wiping_Techniques_and_Anti-Forensics_Methods (accessed Aug. 11, 2024).

[9] M. Geiger, "Counter-Forensic Tools: Analysis and Data Recovery." Accessed: Aug. 11, 2024. [Online]. Available: https://www.first.org/conference/2006/papers/geiger-matthew-papers.pdf

[10] E. Caglar Hosgor, "(PDF) Detection and Mitigation of Anti-Forensics," *ResearchGate,* Dec. 12, 2020. https://www.researchgate.net/publication/349312895_Detection_and_Mitigation_of_Anti-Forensics (accessed Aug. 11, 2024).

[11] S. Gurjar, D. Naik, and A. Sardhara, "Anti-Forensic Techniques and Its Impact on Digital Forensic," Apr. 2023. Available: https://www.irjet.net/archives/V10/i4/IRJET-V10I4251.pdf

[12] "Daubert Standard: Definition & Implications | StudySmarter," *StudySmarter UK,* 2019. https://www.studysmarter.co.uk/explanations/psychology/forensic-psychology/daubert-standard/#:~:text=The%20Daubert%20Standard%20refers%20to (accessed Aug. 14, 2024).

[13] P. Zdzichowski, M. Sadlon, T. Uolevi, V. Alvaro, B. Munoz, and K. Filipczak, "Tallinn 2015 Anti-Forensic Study," 2015. Available: https://ccdcoe.org/uploads/2018/10/AF_with-intro.pdf

[14] "Metasploit Anti-Forensics Project," *Bishop Fox Resources*, Sep. 06, 2013. https://resources.bishopfox.com/resources/tools/other-free-tools/mafia/ (accessed Aug. 20, 2024).

[15] T. Panhalkar, "Anti-Forensics Tools," *Infosavvy Security and IT Management Training*, Jul. 22, 2020. https://info-savvy.com/anti-forensics-tools/

[16] S, R. (2023). *What do you mean by False Positive and False Negative?* [online] Medium. Available at: https://ogre51.medium.com/what-do-you-mean-by-false-positive-and-false-negative-39a459d47aac.

[17] Yaacoub, J.-P.A., Noura, H.N., Salman, O. and Chehab, A. (2021). *Digital Forensics vs. Anti-Digital Forensics: Techniques, Limitations and Recommendations*. [online] arXiv.org. doi:https://doi.org/10.48550/arXiv.2103.17028.

[18] V. Horton, "Anti-Forensics: What it is, Examples and How to Defend Against it," IT Governance Blog En, May30, 2024. https://www.itgovernance.eu/blog/en/anti-forensics-what-it-is-examples-and-how-to-defend-against-it

[19] K. Holmes, "Understanding the Impact of Anti-Forensics Techniques,"www.ftitechnology.com. https://www.ftitechnology.com/resources/blog/understanding-the-impact-of-anti-forensics-techniques

[20] S. H. Saeed, H. L. Arash, and A. A. Ghorbani, "A survey and research challenges of anti-forensics: Evaluation of game-theoretic models in simulation of forensic agents' behaviour," *Forensic Science International: Digital Investigation*, vol. 35, p. 301024, Dec. 2020, doi: https://doi.org/10.1016/j.fsidi.2020.301024.

[21] C. Raroque, "What is a Systems Architecture: Startup's Strategic Guide," *Aloa.co*, Jul. 15, 2024. https://aloa.co/blog/systems-architecture#:~:text=Systems%20architecture%20is%20the%20foundation (accessed Aug. 16, 2024).

[22] Temple, K. (2024). *Integrating AI and Machine Learning into SIEM Systems* |. [online] Securetrust.io. Available at: https://securetrust.io/blog/integrating-ai-and-machine-learning-into-siem-systems/.