NFSU JOURNAL OF CYBER SECURITY & DIGITAL FORENSICS

NFSU – Journal of Cyber Security and Digital Forensics
Volume –3, Issue – 2, December 2024
E – ISSN – 2583-7559

A COMPARATIVE STUDY OF OPEN SOURCE AND ANTI-FORENSICS TOOLS AND TECHNIQUES

Sejal P Tembhare

School of Forensic Sciences
National Forensic Sciences University
Gandhinagar, India

Aswin Pramod

School of Forensic Sciences
National Forensic Sciences University
Gandhinagar, India

Dr. Krishna Modi

School of Forensic Sciences
National Forensic Sciences University
Gandhinagar, India

Dr. Kapil Shukla

School of Forensic Sciences
National Forensic Sciences University
Gandhinagar, India

Abstract - This research assesses the disc imaging, file recovery, artefact analysis, and network monitoring capabilities of open-source forensic tools. Through a detailed assessment, the study finds that while the open-source tools are efficient and possess a wide variety of features, they have limitations in resource efficiency and anti-forensic technique detection. Anti-forensic techniques show a lot of potential in hindering forensic inquiries, creating difficulties in data retrieval and evidential consistency. There is a need for continuous development in forensic technology, especially in improved detection algorithms. By identifying the strengths and weaknesses of existing open-source tools, this study contributes to enhance the effectiveness of forensic investigations against evolving cyber threats.

Keywords - Open-source forensic tools, anti-forensic techniques, trail obfuscation, data wiping, data hiding.

I. INTRODUCTION

The rapid increase of digital data in recent times requires powerful tools to identify, preserve, analyze and present digital evidence. Open source tools such as FTK imager, Autopsy, OSForensics, ProDiscover Basic, Wireshark and Shodan help investigators locate and examine digital evidence with greater accuracy. Being open-source softwares, these tools are cost-effective and versatile. They also enjoy the support of a dedicated community that works constantly to update them in order to deal with new and evolving threats. Despite this, several challenges arise due to the use of anti-forensic techniques and attacks of forensic technologies. This results in a constant rivalry of forensic and anti-forensic techniques. For better investigation and results, proper knowledge regarding the capabilities, advantages and disadvantages of the tool are required.

II. PROBLEM STATEMENT

Open-source forensic tools attempt to detect and preserve digital evidence, while the anti-forensic techniques are being updated to pose more challenges towards the investigation efforts. This study aims to examine the impact of open-source tools and anti-forensic techniques by comparing their effectiveness, reliability, and usability.

III. RESEARCH OBJECTIVE

The primary objectives of this research are:
1. To analyze the strengths and drawbacks of specific open-source forensic tools.
2. To assess the effectiveness of different anti-forensic methods in evading detection and analysis.
3. To assess the impact of the tools and techniques on the outcome of the digital investigation.
4. To determine the necessary improvements in forensic strategies.

IV. LITERATURE REVIEW

Digital evidences are highly significant in criminal cases; some of the challenges encountered during analysis, examining browser history, emails, and message logs can impact timely investigations and ultimately affect the delivery of justice . The use of virtual machines for testing and disaster recovery has also increased, acknowledging their potential in facilitating cybercrimes, making it essential to analyze both host and guest machines as culprits may attempt to conceal evidence within these systems. Additionally, tools like FTK and Autopsy are important in recovering data from lost or corrupt virtual machines.[1][2]

A number of studies concentrate on anti-forensics, which make evidence recovery difficult in investigations. Research has been done to categorize anti-forensic tools, create taxonomies, and highlight data-wiping standards and the role of metadata in forensic analysis[3][4] Anti-forensic tools used by cybercriminals impede investigations, although forensic methods can sometimes recover important data[5] The anti-forensics methods can be briefly divided into evidence destruction, hiding, source elimination and counterfeiting these make the use of forensic tools difficult hence require further research[6] Encryption and steganography are other challenges faced by forensic tools[7] Hash collisions, MACE time manipulation, file erasure, metadata alteration, log manipulation, and trail masking make forensic analysis difficult[8] Sophisticated memory-hiding techniques further mask malicious processes, calling for enhanced detection techniques[9][10] Research emphasizes AI-based countermeasures, anti-anti-forensic (AAF) software, and law reforms to increase forensic precision. Despite investigators' awareness, continued research is essential to counteract emerging anti-forensic methods.[11][12][13]

Numerous studies investigate the efficiency, reliability and the legal scope of open-source and commercial computer forensic software. A study compared Sleuth Kit, EnCase, and FTK, and found that although all of them generated equal results, their innate functionality differed—EnCase and FTK provided high-level search options and intuitive interfaces, while Sleuth Kit was reliable but less user-friendly[14] Open-source tools possess legal validity based on the fact that transparency and correctness correlate well with standard legal metrics, making them more acceptable in judicial proceedings[15] Research into forensic software in investigations of cybercrimes evaluated both the advantages and disadvantages of proprietary and open-source solutions to enable forensic experts to make the best choices. Further, studies on software quality using open and closed-source models uncovered no indication that open source is of lower quality but observed that competition influences both the quality and innovation of open as well as closed-source tools.[16][17]

A digital forensics survey informs of an increase in cybercrimes and the challenges that come with it. Anti-forensic methods make investigation difficult by concealing evidence, with detection mechanisms needing to be updated. As techniques, Bayesian networks and entropy analysis provide precision but are time-consuming[18][19] Web surfing forensics indicate that private and portable browsers leave footprints in RAM and logs even when data is attempted to be removed[20] Remote forensics can help counter cyberattacks[21] Research into the reliability of forensic tools indicates that none of the tools reviewed could successfully identify all anti-forensic techniques, highlighting the need for improved digital evidence handling[22] Private browsing research discovers that artifacts are still recoverable, with Chrome Portable leaving more traces than Opera and Firefox, revealing the limitations of private browsing security[23]

The development of digital anti-forensics using novel steganographic techniques such as Highlight of Exploiting Modification Direction (HoEMD) and Adaptive Exploiting Modification Direction (AdEMD) indicate better results compared to Peak Signal to Noise Ratios (PSNR)[24] More research and innovation in the field of Internet of Things(Iot) is required. Developments in the field should include better training for investigators, automated evidence detection tools, counter anti-forensics techniques, etc.[25]

V. TABLE 1: TOOLS AND METHODOLOGIES EMPLOYED IN PRIOR RESEARCH

Paper Name	Tools Used	Results
Javed et al., 2022	FTK, Encase, OSForensics, Autopsy, Redline, Belkasoft, Magnet Axiom, Network Miner, LogRythm, Plixer, Nmap, Cognitech, InstaForensics	FTK was best for OS, file system, web, and email forensics. Belkasoft excelled in memory forensics. Network Miner and LogRythm were best for network analysis. Cognitech and InstaForensics were superior for multimedia analysis.
Rasool & Jalil, 2020	Phrozen Browser Forensic, MyLastSearch, Chrome Cache View, Internet Evidence Finder, Web Historian	These tools help extract browsing history, cookies, and search queries. Phrozen Browser Forensic is useful for keyword searches, while MyLastSearch retrieves queries

		from search engines.
Gul & Kugu, 2017	Data Pooling, File Signature Manipulation, Hash Collisions, Restricted Filenames, Non-Standard RAID Configurations	Techniques hinder forensic investigations by hiding, destroying, or falsifying evidence. Countermeasures include fuzzy hashing, forensic triage, and specialized RAID recovery.
Conlan et al., 2016	308 anti-forensic tools (encryption, data destruction, data hiding)	Proposed a taxonomy for anti-forensic methods, emphasizing the need for standardization and comprehensive forensic countermeasures.
Abdullahi et al., 2023	Encryption, Data Hiding, File Signature Manipulation, Virtual Machines, Memory Manipulation	Criminals use anti-forensics to erase digital traces, making investigations difficult. Stronger forensic countermeasures are needed.
Riaz & Tahir, 2018	FTK Imager, Magnet Axiom, Autopsy, VMware Workstation	Discussed forensic challenges with virtual machines, noting that snapshots and reversion techniques erase forensic evidence.
Park et al., 2017	Signature-Based Anti-Forensic Detection, Windows Registry Analysis, File System Analysis	Proposed a signature-based detection method to identify anti-forensic traces in forensic triage investigations.
Lovanshi & Bansal, 2019	ProDiscover, Cyber Check Suite, FTK Analyzer, Recuva, EaseUS, Win-Lift, Belkasoft, Volatility, NMAP, Wireshark, Ettercap, Nessus	Compared tools based on performance and efficiency. Found EnCase costly but reliable, FTK effective but time-consuming, and Wireshark useful for live network analysis.
Sun et al., 2011	HoEMD, AdEMD, PVD, LSB, Steganalysis methods	Introduced a new steganographic technique (HoEMD and AdEMD) that improves message concealment while minimizing detection risk.
Harris, 2006	Various anti-forensic techniques categorized (data hiding, artifact wiping, trail obfuscation, evidence counterfeiting)	Proposed a framework for categorizing and countering anti-forensic methods, highlighting the need for standardization.
Bhat et al., 2020	EnCase, FTK, The Sleuth Kit (TSK), OSForensics	Evaluated forensic tools against anti-forensic attacks and found them vulnerable to file system manipulations, raising concerns over forensic reliability.
Pajek & Pimenidis, 2009	Log wiping, time-stamp manipulation, hash collision, steganography, encryption, data hiding	Found that forensic software struggles to detect well-executed anti-forensic techniques, raising questions about evidence reliability in court.
Ambhire, 2012	EnCase, FTK, ProDiscover, Autopsy, Wireshark, Volatility, The Sleuth Kit (TSK)	Discussed strengths and limitations of each tool, noting that ProDiscover is good for corporate investigations,

		Wireshark can be used for network forensics, and Volatility for memory analysis.
Carrier, 2009	The Sleuth Kit (TSK), Autopsy, Wireshark, Volatility, GRR, CAINE	Argued that open-source tools can better meet legal admissibility standards due to transparency, though they may lack vendor support.
Olvecky & Gabriska, 2018	Eraser, KillDisk, DBan, HDDErase, MHDD, Disk Wipe	Evaluated different data wiping standards, including DoD 5220.22M, Gutmann 35-pass, and Schneier method. Found that SSDs retain some recoverable data even after multiple wipe passes.
Majed et al., 2020	Eraser, Free Wipe Wizard, File Shredder, Registry Cleaner, Timestomp, Defiler's Toolkit	Identified various anti-forensic techniques such as metadata manipulation, registry wiping, log manipulation, and encryption to mislead forensic investigations.
Maheswari & Shobana, 2021	EnCase, FTK, X-Ways, Mandiant RedLine, Autopsy, Bluepipe, Oxygen Forensics, DCFLDD	Compared remote forensic tools and techniques, highlighting the need for forensic investigations over encrypted internet connections. Found remote forensic tools effective but facing legal and privacy challenges.
Palutke et al., 2020	Rekall, Volatility, Rootkits, Malware, Page Table Entries, Memory Area Structures	Introduced three novel memory subversion techniques for Windows and Linux that manipulate memory structures to prevent forensic tools from detecting malicious code. Developed two Rekall plugins for detection.
Yaacoub et al., 2022	IoT forensic frameworks, network forensics, evidence-preserving techniques	Explored digital forensics for IoT, highlighting vulnerabilities in evidence collection and the role of anti-forensics in cyberattacks.
De Beer et al., 2015	Data hiding, timestamp manipulation, encryption, forensic evasion techniques	Examined challenges forensic practitioners face due to anti-forensic tools, emphasizing their increasing sophistication.
Yaacoub et al., 2021	Digital and anti-forensic tools for malware, cloud, mobile, network forensics	Reviewed forensic and anti-forensic challenges, proposing AI-based countermeasures.
Ohana & Shashidhar, 2013	FTK, EnCase, RAM analysis, browser cache analysis	Investigated forensic recoverability of browsing data from private and portable browsers, finding residual artifacts even after session deletion.
Arias et al., 2024	DFIR tools, forensic data wiping, anti-forensic strategies	Systematically reviewed anti-forensic techniques and their impact on digital investigations.
Raghunathan et al., 2005	Open Source Tools: Autopsy, The Sleuth Kit	Open-source tools offer greater transparency, peer validation,

	(TSK), GRR Closed Source Tools: EnCase, FTK, Magnet Axiom	and legal admissibility due to their open nature, though they may lack vendor support. Closed-source tools provide better user-friendliness, comprehensive support, and advanced features, but their closed architecture limits external review.

VI. METHODOLOGY

Three anti-forensic techniques, data wiping, timestamp manipulation, steganography were examined. The methods were chosen based on their relevance in digital forensics. Three open-source anti-forensic tools were selected for each technique based on their accessibility and prevalance. To maintain validity and integrity of the experiment, the techniques were executed in an isolated virtual machine environement. This ensured the reliability of the findings.

The experimental procedure encompassed a sequential execution of the following stages:

1. Establishment of the virtual machine
2. Implementation of anti-forensic techniques within the virtual environment
3. Acquisition of a forensic image from the virtual machine

For the experimental setup, a virtual machine was established with the following specifications:
Memory: 2 GB
Processors: 2
Hard Disk (NVMe): 60 GB
Operating System: Windows 10

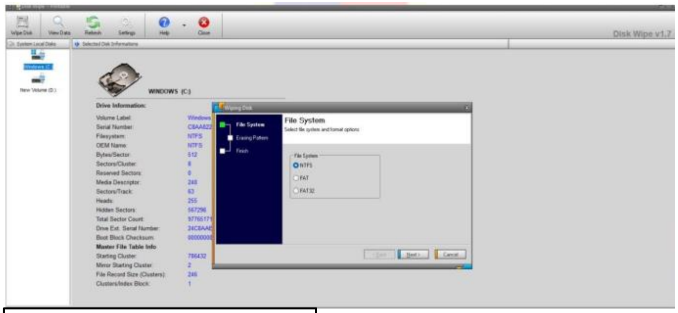
The virtual machine was cloned for each anti-forensic technique to ensure consistency and control.

A. Implementation 1 (Anti-forensic)

1. Experiment 1.1: Data Wiping

- *DISK WIPE*

The DiskWipe tool was installed in one of the virtual machines. A new E: drive was created and a sample dataset was added. The Disk Wipe tool was then employed using Peter Gutmann method. It performs 35 passes to ensure comprehensive data erasure. After the wiping process, the entire data was erased and reformatted using the NTFS file system.



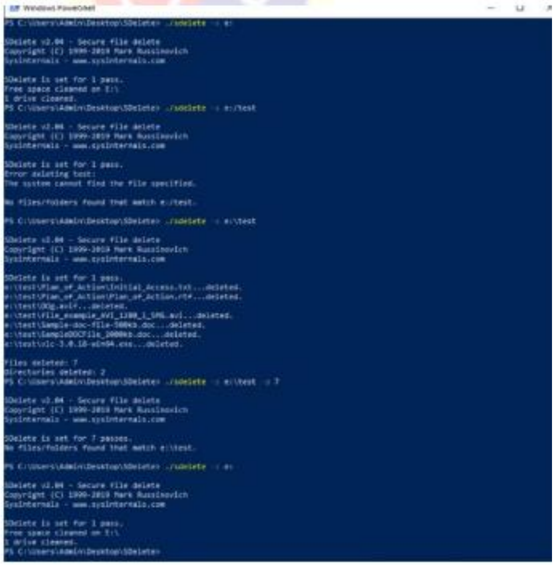
Drive Information:
Volume Label: Windows
Serial Number: C8AA822
Filesystem: NTFS
OEM Name: NTFS
Bytes/Sector: 512
Sectors/Cluster: 8
Reserved Sectors: 0
Media Descriptor: 248
Sectors/Track: 63
Heads: 255
Hidden Sectors: 567296
Total Sector Count: 97765171
Drive Ext. Serial Number: 24C8AAE
Boot Block Checksum: 00000000
Master File Table Info
Starting Cluster: 786432
Mirror Starting Cluster: 2
File Record Size (Clusters): 246
Clusters/Index Block: 1

File System
Select file system and format options
File System
● NTFS
○ FAT
○ FAT32

Fig 1: DiskWipe tool

- *SDELETE*

In another virtual machine, SDelete was installed and the same sample set of data was added to the E: drive. Afterwards, the disk was wiped using SDelete . SDelete operates within the PowerShell environment.



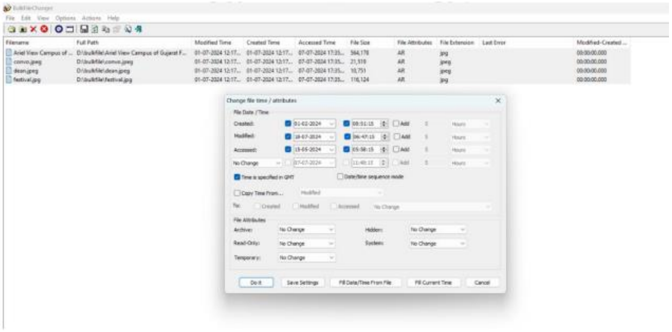
```
PS C:\Users\Admin\Desktop\SDelete> ./sdelete -z e:

SDelete v2.04 - Secure file delete
Copyright (C) 1999-2019 Mark Russinovich
Sysinternals - www.sysinternals.com

SDelete is set for 1 pass.
Free space cleaned on E:\
1 drive cleaned.
PS C:\Users\Admin\Desktop\SDelete> ./sdelete -s e:/test

SDelete v2.04 - Secure file delete
Copyright (C) 1999-2019 Mark Russinovich
Sysinternals - www.sysinternals.com

SDelete is set for 1 pass.
Error deleting test:
The system cannot find the file specified.

No files/folders found that match e:/test.

PS C:\Users\Admin\Desktop\SDelete> ./sdelete -s e:\test

SDelete v2.04 - Secure file delete
Copyright (C) 1999-2019 Mark Russinovich
Sysinternals - www.sysinternals.com

SDelete is set for 1 pass.
e:\test\Plan_of_Action\Initial_Access.txt...deleted.
e:\test\Plan_of_Action\Plan_of_Action.rtf...deleted.
e:\test\DOg.avif...deleted.
e:\test\file_example_AVI_1280_1_5MG.avi...deleted.
e:\test\Sample-doc-file-500kb.doc...deleted.
e:\test\SampleDOCFile_2000kb.doc...deleted.
e:\test\vlc-3.0.18-win64.exe...deleted.

Files deleted: 7
Directories deleted: 2
PS C:\Users\Admin\Desktop\SDelete> ./sdelete -s e:\test -p 7

SDelete v2.04 - Secure file delete
Copyright (C) 1999-2019 Mark Russinovich
Sysinternals - www.sysinternals.com

SDelete is set for 7 passes.
No files/folders found that match e:\test.

PS C:\Users\Admin\Desktop\SDelete> ./sdelete -z e:

SDelete v2.04 - Secure file delete
Copyright (C) 1999-2019 Mark Russinovich
Sysinternals - www.sysinternals.com

SDelete is set for 1 pass.
Free space cleaned on E:\
1 drive cleaned.
PS C:\Users\Admin\Desktop\SDelete>
```

Fig 2: sdelete

2. Experiment 1.2: Timestamp Changes

a) BULKFILECHANGER

A file was added in the BulkFileChanger tool, and modifications were applied to its created, modified and accessed timestamps.



BulkFileChanger

Filename	Full Path	Modified Time	Created Time	Accessed Time	File Size	File Attributes	File Extension	Last Error	Modified-Created ...
Ariel View Campus of ...	D:\bulkfile\Ariel View Campus of Gujarat F...	01-07-2024 12:17...	01-07-2024 12:17...	07-07-2024 17:35...	564,178	AR	jpg		00:00:00.000
convo.jpeg	D:\bulkfile\convo.jpeg	01-07-2024 12:17...	01-07-2024 12:17...	07-07-2024 17:35...	21,518	AR	jpeg		00:00:00.000
dean.jpeg	D:\bulkfile\dean.jpeg	01-07-2024 12:17...	01-07-2024 12:17...	07-07-2024 17:35...	10,751	AR	jpeg		00:00:00.000
festival.jpg	D:\bulkfile\festival.jpg	01-07-2024 12:17...	01-07-2024 12:17...	07-07-2024 17:35...	116,124	AR	jpg		00:00:00.000

Change file time / attributes

File Date / Time
- Created: ☑ 01-02-2024 ☑ 08:51:15 □ Add
- Modified: ☑ 18-07-2024 ☑ 06:47:15 □ Add
- Accessed: ☑ 15-05-2024 ☑ 05:58:15 □ Add
- No Change □ 07-07-2024 □ 11:48:15 □ Add

☑ Time is specified in GMT □ Date/time sequence mode

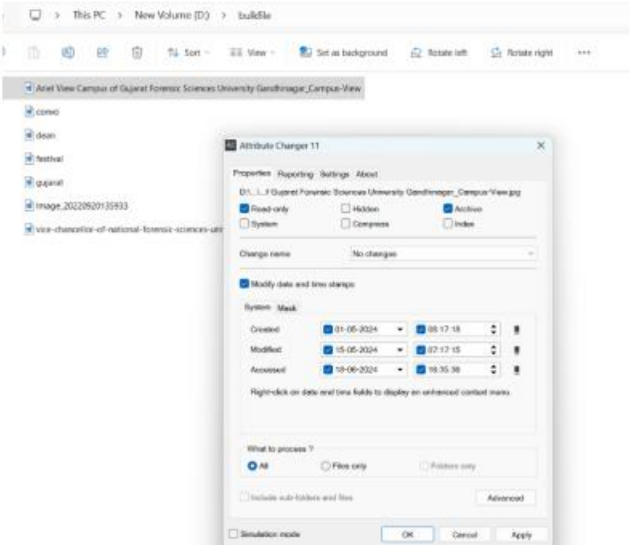
□ Copy Time From... Modified

File Attributes
- Archive: No Change
- Hidden: No Change
- Read-Only: No Change
- System: No Change
- Temporary: No Change

Fig 3: Bulk File Changer

b) ATTRIBUTE CHANGER

Another file was opened with Attribute Changer and MAC time was edited.



This PC › New Volume (D:) › bulkfile

Attribute Changer 11

Properties Reporting Settings About

D:\...\...f Gujarat Forensic Sciences University Gandhinagar_Campus-View.jpg

☑ Read-only □ Hidden ☑ Archive
□ System □ Compress □ Index

Change name: No changes

☑ Modify date and time stamps

System Mask
- Created ☑ 01-05-2024 ☑ 08:17:18
- Modified ☑ 15-05-2024 ☑ 07:17:15
- Accessed ☑ 18-06-2024 ☑ 18:35:38

Right-click on date and time fields to display an enhanced context menu

What to process ?
● All ○ Files only □ Folders only

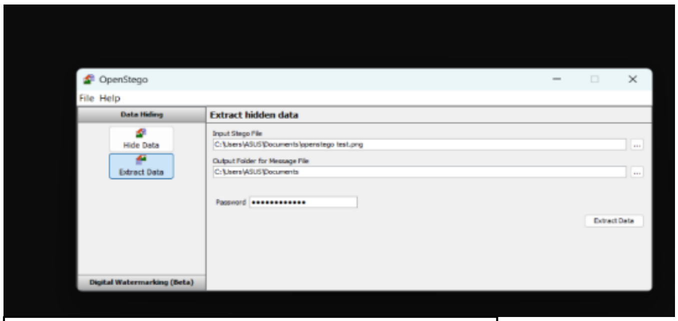
□ Include sub-folders and files

□ Simulation mode

Fig 4: Attribute Changer

3. *Experiment 1.3: Steganography*

The experiment involved the utilization of OpenStego, an open-source steganographic tool. A text file was generated and hidden in a JPEG image. An encryption was applied to the hidden message using the password, "forensic@123"



OpenStego

Extract hidden data

Input Stego File: C:\Users\ASUS\Documents\openstego test.png

Output Folder for Message File: C:\Users\ASUS\Documents

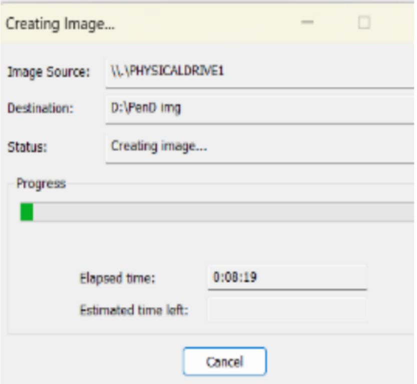
Password: ●●●●●●●●●●●●●

Fig 5: OpenStego

B. Implementation -2 (Open source tools)

1. Experiment 2.1: FTK Imager

FTK Imager is an effective and flexible tool used for forensic imaging and analysis.



Creating Image...

Image Source: \\.\PHYSICALDRIVE1

Destination: D:\PenD img

Status: Creating image...

Progress

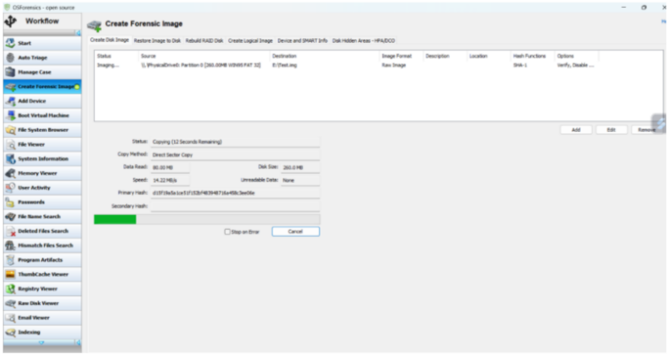
Elapsed time: 0:08:19

Estimated time left:

Fig 6: Creating Image in FTK Imager

2. Experiment 2.2: OSForensics

OSForensics, while not being fully open-source, incorporates open-source components and libraries, fostering customization and community contributions.



Create Forensic Image

Create Disk Image | Restore Image to Disk | Rebuild RAID Disk | Create Logical Image | Device and SMART Info | Disk Hidden Areas - HPA/DCO

Status	Source	Destination	Image Format	Description	Location	Hash Functions	Options
Imaging...	\\.\PhysicalDrive0: Partition 0 [260.00MB WIN95 FAT 32]	E:\Test.img	Raw Image			SHA-1	Verify, Disable ...

Status: Copying (12 Seconds Remaining)

Copy Method: Direct Sector Copy

Data Read: 80.00 MB Disk Size: 260.0 MB

Speed: 14.22 MB/s Unreadable Data: None

Primary Hash: d15f19a5a1ce51f152bf483948716a458c3ee06e

Secondary Hash:

□ Stop on Error

Fig 7: Creating Image in OSForensics

3. Experiment 2.3: Wireshar

Wireshark is an industry standard tool for packet analysis, designed to analyse network traffic in real time. It can capture and read packet data, thus playing a crucial role in various network-related projects. Wireshark is one of the most effective and reliable open-source options for packet analysis.s

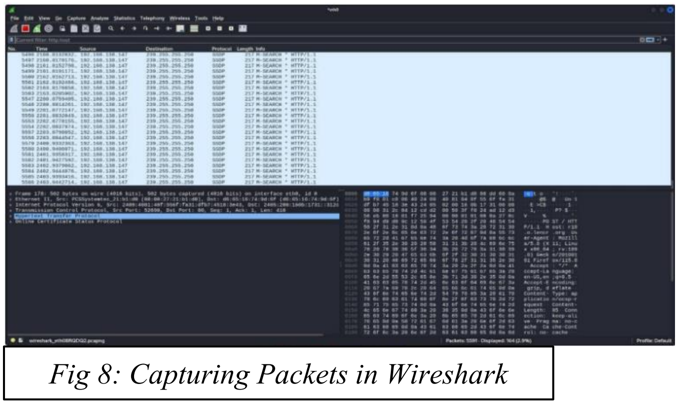
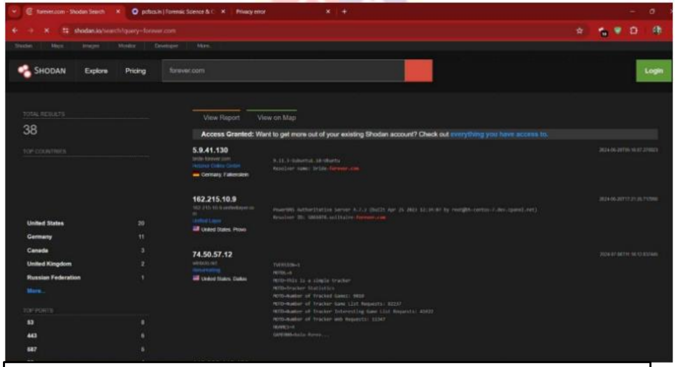


Fig 8: Capturing Packets in Wireshark

4. Experiment 2.4: Shodan

Shodan is a specialized search engine for identifying specific internet-connected devices. By leveraging various search parameters, it enables users to locate cameras, routers, servers and IoT devices. These features make Shodan a valuable tool for Reconnaissance and vulnerability assessment.



TOTAL RESULTS
38

TOP COUNTRIES

United States	20
Germany	11
Canada	3
United Kingdom	2
Russian Federation	1

More...

TOP PORTS

53	8
443	6
687	6

Access Granted: Want to get more out of your existing Shodan account? Check out everything you have access to.

5.9.41.130
Germany, Falkenstein

162.215.10.9
United States, Provo

74.50.57.12
United States, Dallas

Fig 9: Analyzing website's IP using Shodan

Results

Anti-forensic attacks were performed using techniques like data erasure, steganography and timestamp modification. Analysis of various open-source tools revealed that none of the analyzed tools were able to detect, flag or recover the data manipulated using the anti-forensic methods. The tools lacked dedicated features or tabs for identifying anti-forensic activities, despite detecting potential anomalies. The research highlights the need for further developments in forensic technologies to detect anti-forensic alterations.

Tools	Prodiscover Basic	Autopsy	Wireshark	Shodan
Imaging		✓		
Hashing	✓			
Recovery	✓	✓		
Acquire		✓		
Packet Sniffing			✓	
Packet Spoofing			✓	
Open Port				✓
Seizer	✓	✓		
Protocol			✓	✓

VII. CONCLUSION

The comparative analysis of open-source forensic tools have revealed varying capabilities in the tools used in imaging, data recovery, network analysis and reconnaissance.

Anti-forensic techniques pose challenges to the tools in the form of steganography, data wiping and time stamp manipulation. Despite these, open-source tools with machine learning integration and AI driven analysis would offer better solutions for detecting and mitigating the impact of anti-forensic tactics.

A collaborative effort among researchers, forensic practitioners and policy makers would be crucial in developing methodologies and tools to preserve the integrity of digital evidence in legal proceedings against the emerging cyber threats.

VIII. REFERENCES

[1] Ambhire, V. R., & Meshram, B. B. (2012). Digital Forensic Tools. 2(3), 392–398. www.iosrjen.org392|Page

[2] Riaz, H., & Tahir, M. A. (2018). Analysis of VMware virtual machine in forensics and anti-forensics paradigm. IEEE Xplore, 1–6. https://doi.org/10.1109/isdfs.2018.8355375

[3] Conlan, K., Baggili, I., & Breitinger, F. (2016). Anti-forensics: Furthering digital forensic science through a new extended, granular taxonomy. DFRWS 2016 USA - Proceedings of the 16th Annual USA Digital Forensics Research Conference, S66–S75. https://doi.org/10.1016/j.diin.2016.04.006

[4] Ölvecký, M., & Gabriška, D. (2018). Wiping Techniques and Anti-Forensics Methods. SISY 2018 - IEEE 16th International Symposium on Intelligent Systems and Informatics, Proceedings, 127–131. https://doi.org/10.1109/SISY.2018.8524756

[5] Abdullahi, Z. H. (2023). An Overview of Anti-forensic Techniques and their Impact on Digital Forensic Analysis. https://www.researchgate.net/publication/368365338

[6] Harris, R. (2006). Arriving at an anti-forensics consensus: Examining how to define and control the anti-forensics problem. Digital Investigation, 3(SUPPL.), 44–49. https://doi.org/10.1016/j.diin.2006.06.005

[7] P., & Pimenidis, E. (2009). Computer anti-forensics methods and their impact on computer forensic investigation. In Communications in computer and information science (pp. 145–155). https://doi.org/10.1007/978-3-642-04062-7_16

[8] Gül, M., & Kugu, E. (2017, October 30). A survey on anti-forensics techniques. IDAP 2017 - International Artificial Intelligence and Data Processing Symposium. https://doi.org/10.1109/IDAP.2017.8090341

[9] Majed, H., Noura, H. N., & Chehab, A. (2020). Overview of Digital Forensics and Anti-Forensics Techniques. IEEE Xplore, 1–5. https://doi.org/10.1109/isdfs49300.2020.9116399

[10] Palutke, R., Block, F., Reichenberger, P., & Stripeika, D. (2020). Hiding Process Memory Via Anti-Forensic Techniques. Forensic Science International: Digital Investigation, 33. https://doi.org/10.1016/j.fsidi.2020.301012

[11] González Arias, R., Bermejo Higuera, J., Rainer Granados, J. J., Bermejo Higuera, J. R., & Sicilia Montalvo, J. A. (2024). Systematic Review: Anti-Forensic Computer Techniques. In Applied Sciences (Switzerland) (Vol. 14, Issue 12). Multidisciplinary Digital Publishing Institute (MDPI). https://doi.org/10.3390/app14125302

[12] Yaacoub, J. A., Noura, H. N., Salman, O., & Chehab, A. (2021). Digital Forensics vs. Anti-Digital Forensics: Techniques, Limitations and Recommendations. https://www.semanticscholar.org/paper/Digital-Forensics-vs.-Anti-Digital-Forensics%3A-and-Yaacoub-Noura/e9cef52300cbf88d2e1ff5eb7717df883c06a140

[13] De Beer, R., Stander, A., & Van Belle, J. (2015). Anti-Forensics: A practitioner perspective. https://www.semanticscholar.org/paper/Anti-Forensics%3A-A-Practitioner-Perspective-Beer-Stander/0f2c9ed130ca154c73a1b775c96c2e62631e4564

[14] Manson, D., Carlin, A., Ramos, S., Gyger, A., Kaufman, M., & Treichelt, J. (2007). Is the open way a better way? Digital forensics using open source tools. Research Gate. https://doi.org/10.1109/hicss.2007.301

[15] Carrier, B. D. (2009). Open Source Digital Forensics Tools The Legal Argument 1. ResearchGate. https://www.researchgate.net/publication/240899558_Open_Source_Digital_Forensics_Tools_The_Legal_Argument_1

[16] Lovanshi, M., & Bansal, P. (2019). Comparative Study of Digital Forensic Tools. In Data, Engineering and Applications: Volume 2 (Vol. 2, pp. 195–204). Springer Singapore. https://doi.org/10.1007/978-981-13-6351-1_15

[17] Raghunathan, S., Prasad, A., Mishra, B. K., & Chang, H. (2005). Open source versus closed source: Software quality in monopoly and competitive markets. IEEE Transactions on Systems, Man, and Cybernetics Part A:Systems and Humans, 35(6), 903–918. https://doi.org/10.1109/TSMCA.2005.853493

[18] Javed, A. R., Ahmed, W., Alazab, M., Jalil, Z., Kifayat, K., & Gadekallu, T. R. (2022). A Comprehensive Survey on Computer Forensics: State-of-the-Art, Tools, Techniques, Challenges, and Future Directions. IEEE Access, 10, 11065–11089. https://doi.org/10.1109/ACCESS.2022.3142508 list. (n.d.).

[19] Park, K., Park, J.-M., Kim, E., Cheon, C., & James, J. (2017). Anti-Forensic Trace Detection in Digital Forensic Triage Investigations. Journal of Digital Forensics, Security and Law. https://doi.org/10.15394/jdfsl.2017.1421

[20] Rasool, A., & Jalil, Z. (2020). A Review of Web Browser Forensic Analysis Tools and Techniques. Researchpedia Journal of Computing, 1(1), 15–21. https://doi.org/10.1111/RpJC.2020.DOI

[21] Maheswari, K. U., & Shobana, G. (2021). The state of the art tools and techniques for remote digital forensic investigations. 2021 3rd International Conference on Signal Processing and Communication, ICPSC 2021, 464–468. https://doi.org/10.1109/ICSPC51351.2021.9451718

[22] Bhat, W. A., AlZahrani, A., & Wani, M. A. (2021). Can computer forensic tools be trusted in digital investigations? Science and Justice, 61(2), 198–203. https://doi.org/10.1016/j.scijus.2020.10.002

[23] Ohana, D. J., & Shashidhar, N. (2013). Do private and portable web browsers leave incriminating evidence?: a forensic analysis of residual artifacts from private and portable web browsing sessions. http://jis.eurasipjournals.com/content/2013/1/

[24] Sun, H. M., Weng, C. Y., Lee, C. F., & Yang, C. H. (2011). Anti-forensics with steganographic data embedding in digital images. IEEE Journal on Selected Areas in Communications, 29(7), 1392–1403. https://doi.org/10.1109/JSAC.2011.110806

[25] Yaacoub, J. P. A., Noura, H. N., Salman, O., & Chehab, A. (2022). Advanced digital forensics and anti-digital forensics for IoT systems: Techniques, limitations and recommendations. In Internet of Things (Netherlands) (Vol. 19). Elsevier B.V. https://doi.org/10.1016/j.iot.2022.100544