International Journal for Multidisciplinary Research (IJFMR)
E-ISSN: 2582-2160 ● Website: www.ijfmr.com ● Email: editor@ijfmr.com

Comprehensive Study of Network Forensic

Rashmi R. More[1], Mrs. Dipalee Divakar Rane[2]

[1]PG Student D.Y. Patil college of engineering, Akurdi, Pune, Maharashtra, India
[2]Assistant Professor D.Y. Patil college of engineering, Akurdi, Pune, Maharashtra, India

Abstract
Today, as the cybercrimes are increasing rapidly, there is necessity to find the root cause of the loopholes that are left while taking care of cyber security. So, the evidences are searched to find the source of the cyber-attack. This can be done by detecting networks and network components used by criminals which comes under network forensic. Network forensic is a domain of computer forensic which studies internal and external network to find out important artifacts for investigators to discover the origin of the cyber-attack. The proposed survey focuses on overview of network forensic domain having different network forensic methods, methodology along with the analysis of network forensic tools (NFTs). The proposed survey also concentrates on the comparison of NFTs like Network Miner, Xplico, LogRhythm, NIKSUN, Nmap, etc. based on their features, compatibility with platforms, whether they are open source or commercial, etc. Finally, this paper concludes with the basic purpose and features of every tool and its usability.

Keywords: Network forensics, Network forensic tools, Cyber attack

1.Introduction

Nowadays, world is moving towards digitalization making our life more efficient, more productive, more filled with social connectivity but there is also a darker side of these advantages in the form of cybercrimes. The criminals also have new ways of cyber-attacks. These cybercrimes are frequently happening all over the world. The recent example is cyber-attack on email system under 'gov.lk' domain which affects on multiple Sri Lankan government institute. This attack came out to the light on 26th August,2023 and lasted for almost 2 weeks This results in substantial data loss and disruption of communication. The another example is the cyberattack on AIIMS (All India Institute of Medical Science) done on November 23, 2022.The AIIMS server went offline for about two weeks. It had affected daily services like appointments, registration, discharge, scheduled surgeries etc. Attackers had demanded lots of money to restore services. It had influenced the online services of AIIMS. It had corrupted all the files stored on main and backup servers in hospitals. It had turned into a big loss. These both attacks were ransomware attacks. Ransomware is any software that encrypts corrupted files. Cyberattacks affect not only financial but also social, personal, and medical information. Even though cyber-attacks are very harmful, we can recover loss as soon as possible as attacker could left some artifacts in device storage or any other location. This can help investigator to find the source of the attack. To do this task, network forensic helps investigators. It is the branch of computer forensics. Computer forensic is the field of technology that uses investigative techniques to identify and store evidences from computer devices.Computer forensic information can be plucked from software, databases, the web, or email, as well as from memory cards, smart cards, dongles, biometric scanners, GPS systems, etc. Computer forensic is closely related to human behavior. Behavioral Evidence Analysis(BEA) of computer forensic helps to understand psychology of criminal at a particular situation.[1]

This can provide the assistance to the investigator in his perusal.

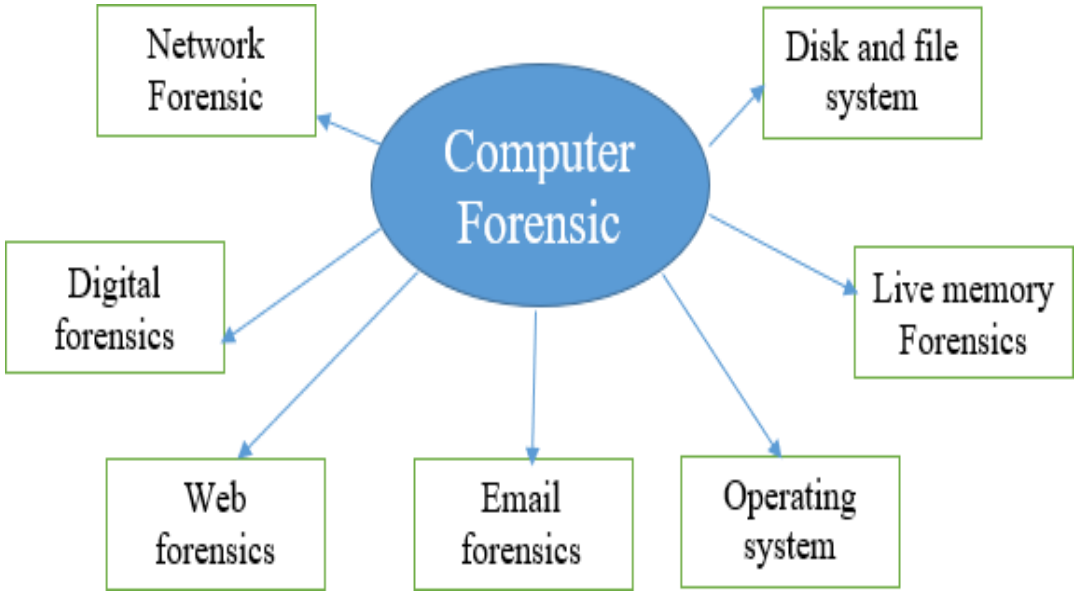

Fig.1 Domains of computer forensic

There are different branches of computerforensic. 1) Operating system forensics 2) Disc and file system forensics 3) Live memory forensics 4) Web forensics 5) Email forensics 6) Network forensics 7) Multimedia forensics and others, as shown in Fig.1

This papermainly focuses on network forensics along with its process, method, methodology and tools used for investigation followed by comparative analysis of some network forensic tool. Basically, network forensic deals with monitoring and analysis of network traffic. Network forensic is an investigation process conducted when any criminal attack is detected on a network. The purpose of network forensic is to find the source of an attack through analyzing network which is dynamic and volatile [1][2]. Furthermore, it is also concerned with determining nature of attack and storing data forensically sound way to present them in court of law. There are two aspects of forensics evidences, first is real time i.e. live forensics and second is after the event i.e. dead forensics.[16] Forensics activities include the capture and note-making of events and further analysis of them to reach the source.

2. Related Work

Authors	Proposed Work
Abdul R.J. et.[1]	They proposed detailed description of computer forensic with all its domains along with the Feature Scoring Model (FSM) for good tool detection. They elaborated functionalities of NFTs. They performed analysis of different tools of all domains based on their characteristics.
Suleman K. et.[2]	They proposed C-NFM i.e Network Forensics Method which finds root cause of network attack through network packet, logs events and

	applications.
Syed Rizvi et[3]	They proffered the use of artificial intelligence in network forensics with the help of machine learning, deep learning or ensemble learning. They also explained network forensic process model.
Fahad M.G. et[4]	They proposed network forensic process with its architecture. Also gave comparative analysis of some network forensics tools.
Damir et.[5]	They offered comparative analysis of various NFTs on different operating system
Jiao[6]	He proposed fuzzy decision tree reasoning method for NF.

3.Analysis Of Network Forensic

A. Network forensic methods

The main aim of network forensic is to prepare plan before any type of attack performed on network. So, Syed Rizvi, Mark Scanlon and other stated that there are two methods of capturing data for fulfilling this aim.

1. Catch it as you can- This approach has continuous monitoring of traffic It is proactive approach which tries to catch or save everything that is the reason it requires large storage space [1]. Wireshark, TCPDump are the examples of it.[7]
2. Stop, look and listen- This spontaneous approach is usedafter attack. It find out network traffic communication atthe time of attack [1].

NFM is classified into five categories:1) Intrusion detection 2) Traceback 3) Distributive and 4) attack graphs [2]5) fuzzydecision tree reasoning method[6].

1. Intrusion detection system provides protection to thenetwork infrastructure by detecting anomalies investigate anomalies by pattern matching, attack time, packetinspection etc[2].
2. Traceback is a method used after attack. It gives reply ofits sequential steps again for investigating effectiveness of attack to reach to its origin.
3. Distributive method gives analysis of malicious traffic indistributed location of network.
4. Attack graph method visualizes attack paths in network. It reduces investigation time.
5. Fuzzy decision tree reasoning method first collect information of relevant targets then establish analysis diagram with finding accurate attack target and then formulate intrusion plan from collected information[6].

B. Network Forensic process

Network forensic is a process with specific model.

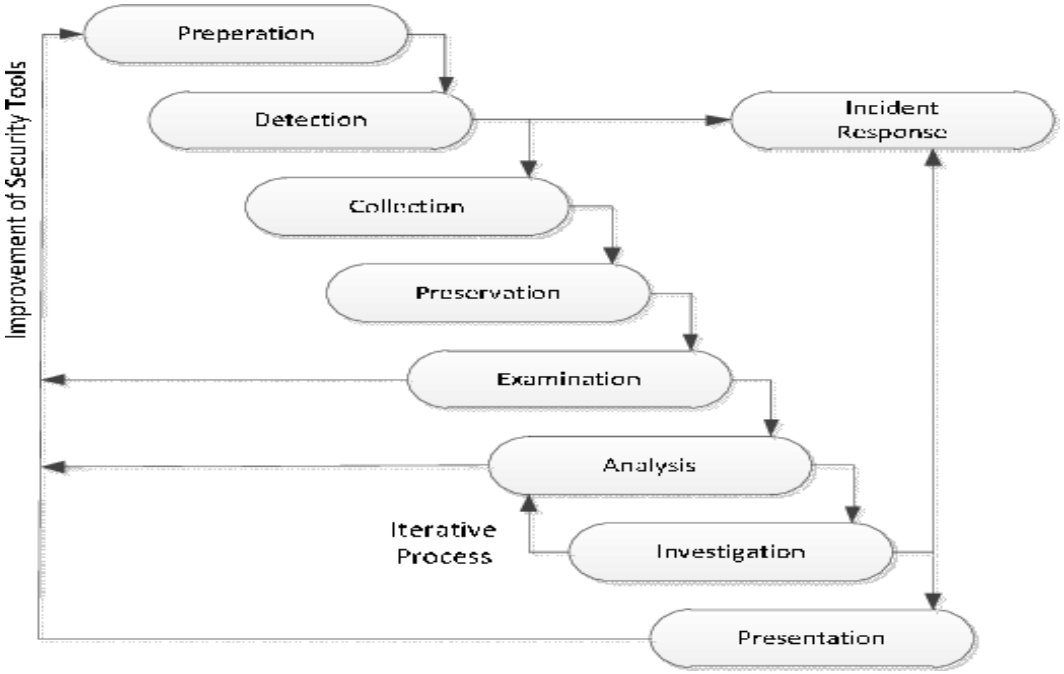

Fig 1.2 Network forensic process (adapted from [3])

Network forensic process is composed of 8 stages. First one should be prepared for recovery of losses in cyber-attack. Then the next stage is detection of attack based on evidences collected after the attack. The evidences collected are preserved for further examination Then these are analyzed and investigated to reach out towards the culprit. Once the culprit is found, the proofs are presented in systematic manner. The analysis and investigation stages are in loop i.e.as many as evidences are collected ,they are investigated and analyzed[2].

C. Network forensic methodology

Sirajuddin, Saima and others in their paper proposed OSCAR methodology for the network of forensics. InOSCAR, O means Obtaining Information, S means Strategizing, C means Collecting evidence. A means Analyzing evidences, and R means Reporting. Obtaining information is concerned with gaining information about the incident happened. It involves collection of all needful data about the attack. Strategizing involves making blueprints of a detailed plan of how the investigation will move forward. Collecting evidences includes collecting evidences from the device of victim and components associated with network along with prioritization of evidences. Analyzing involves documentation of evidences for further analysis of it. Reporting is the most vital part of network forensic because it will show the results of all this investigation. The report should be clear and understandable by any non-technical person [15].

D. Network Forensic Tools

NFTs examine network, collect information about network traffic or data, help to analyze the situation and support in finding evidences from incident used in the court of law[4].There are different NFTs available which differ in their functionalities like netflow, OS fingerprints, port scanner, banner grabber, whether it

is open source or not, threat analysis ,how it recovers data ,extraction ofcredentials, whether it can encrypt traffic or not, log collection, remote analysis, and others [1].

Following is the explanation of functionalities of NFTs:

NetFlow: When a tool supports netflow, it can find out source and destination addresses, protocols, conversations,and packet captures. Also, it may assist in discovering protocol-specific characteristics like RTP stat, response time, TCP retransmission, etc.

OS Fingerprints: When a tool supports OS fingerprints, it can relate to OS-related statistics.

Port scanner: It allows to search the system for open ports.

Banner Grabber: It discovers what services and their versions are running on the system.

Threat analysis: It may detect impact of threat on the system.

Recover data: The tool recovers significant data like files, emails, and VoIP's.

Extract user credentials and encrypted data: This tool can extract critical information and encrypted data in different situations.

Log collection: This tool keeps a history of all operations performed during communication.[1]

The tool selection process is not only based on its features but also depends upon the compatibility of the platform, what type of license it has, and whether it is open source or commercial. There are number of network forensic tools available. But we are going to shed light on some of them shown in fig.1.3

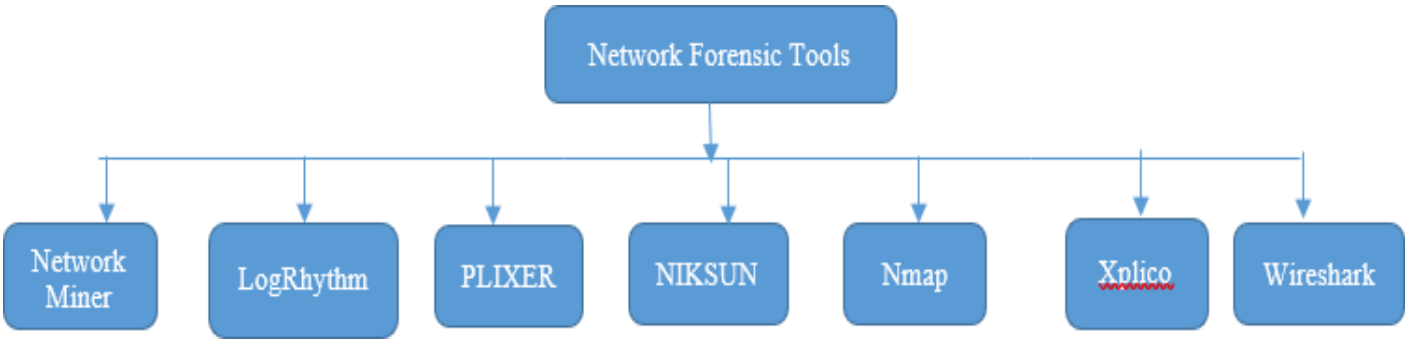

Fig.2 Network forensic tools

1. **Network miner**: Network miner is an open-source network forensic tool that extracts artifacts like files, images, emails, and passwords from PCAP (Packet Capture) files captured from the network. A PCAP file is a file that contains packet data from a network. The PCAP file is used to analyze the network characteristics, control network traffic and determine network status. It supports all of the above- mentioned features except the banner grabber. It can also be used to capture live network traffic by monitoring a network. It can also analyze pre-captured data through network traffic in an offline manner. It is specially designed to run on Windows but can also be run on Linux, Mac OS,and Free BSD. It is available in free and professionalversions. It also contains host inventory, where each IP in the PCAP file is maintained. Network Miner supports passive network monitoring. i.e., it doesn't communicate with the network. It works in a modest way. It can analyze protocols like HTTP, FTP, SMTP, DNS, and SSL/TLS. It can determine the geographical location of an IP address based on geoIP location [5][7].
2. **LogRhythm**: LogRhythm NDR is a product of LogRhythm that monitors networks in real time

with an ML-driven threat detection response and a built-in MITREATT&CK engine. It is an open-source tool. It supports all features except banner grabbers like network miners.[8]

3. **PLIXER**: With PLIXER, we can gain critical data and contents to predict network performance issues, plan capacity, and ensure an excellent user experience with confidence. It is a commercial tool that supports all the above functions except OS fingerprints and banner grabber [17][1].

4. **NIKSUN**: NIKSUN delivers real-time, forensics-based cyber security and network monitoring solutions to secure captious infrastructure, refine service delivery, and curtail compliance risks. Based on the world's most scalable and modular technology, Alpine, NIKSUN is revolutionizing the network monitoring industry. It is an open-source tool with OS fingerprints, port scanners, threat and remote analysis, and log collection features[12].

5. **Nmap (Network Mapper):** Nmap is open source and supported with Windows, Linux, solaris and Mac OS with all features included in the above tool. But it cannot extract user credentials. Nmap is a free and open- source utility for network discovery and security auditing.It is also useful for tasks such as network inventory, managing service upgrade schedules, and monitoring host or service uptime. Nmap uses raw IP packets in novel ways to determine what hosts are available on the network, what services those hosts are offering, what operating systems they are running, what type of packet filters or firewalls are in use, and lots of other characteristics. Nmap can run on all major operating systems but is mostly used on Windows, Linux, and Mac OS[9].

6. **XPLico**: XPLico is open source tool and supported with Linux OS tools. It is a network forensics analysis tool, which reconstructs the contents of acquisitions performed with a packet sniffer. It allows concurrent access by multiple users. It can only recover data. e.g. XPLico is able to extract all email carried by POP and SMTP. Xplico reconstructs audio, video, images, pdf, and several other text files from a network.[10] It can collect application data, information from database/files using SQLite or MYSQL. It Support online and offline analysis of packet capture along with live steaming of traffic. It support many protocols ARP, PPP, VLAN, IPV4, IPV6, SNOOP, TCP, IRC, HTTP, SMTP, FTP, SIP, HTTP[4].

7. **Wireshark**: Wireshark is an open-source GUI based application software packet analyzer, which is used for education, analysis, software development, communication protocol development, and networktroubleshooting. It is used to track the packets so that each oneis filtered to meet our specific needs. It is generally called as**a** sniffer, network protocol analyzer, and network analyzer. It is used by network security engineers to examine securityproblems. Wireshark can capture live network data and create PCAP file for passive analysis. It has decoding protocol feature. It also allows to view captured packets. It can save ,filter and store packet data for later use[11][15].

Uses of NFTs

Tool	When to use
Network Miner	1.When you want to use easy tool 2.When you want to detect operating system, sessions, host names in passive ways
Xplico	1.When you want to capture internet data from application 2.When you want to classify the protocol
Nmap	1.When you want network exploration, host discovery and security auditing

Wireshark	1.When you want to troubleshoot network performance issues 2.When you want to trace network connection 3.When you want to identify bursts of traffic
LogRhythm NDR	1.When you want easy threat detection

Comparative Analysis

Features	Tool						
	Network Miner	*LogRhythm*	*PLIXER*	*NIKSUN*	*Nmap*	*Xplico*	*Wireshark*
NetFlow	Yes	Yes	Yes	Yes	Yes	Yes	Yes
OS Fingerprints	Yes	Yes	No	Yes	Yes	No	No
Banner Grabber	No	No	No	No	Yes	No	No
Threat analysis	Yes	Yes	Yes	Yes	Yes	No	No
Recover data	Yes	Yes	Yes	No	Yes	Yes	No
Extract data and credentials	Yes	Yes	Yes	No	No	No	No
Log Collection	Yes	Yes	Yes	Yes	Yes	No	Yes
Remote analysis	Yes	Yes	Yes	Yes	Yes	No	No
Open source/ Commercial	Open Source	Open Source	Commercial	Open Source	Open Source	Open Source	Open Source
Supported OS	Windows, Linux, MAC OS, FreeBSD				Windows, Linux, Solaris, Mac OS	Linux	Windows, Linux

4. Conclusion

This paper has successfully called out the fundamental information about Network Forensic including Network Forensic methods, process, methodology and tools. The main focus of the paper is on understanding and analysis of various Network Forensic Tools (NFT's) such as Network miner, Log Rhythm, PLIXER etc. including their functionalities. Further, the paper throws light on an important part in network forensic for defining criteria to select the most appropriate tool in a given scenario. This will help the investigators to shortlist the right set of tools while investigating a cyber-attack. This paper has also given a detailed comparison of all the NFTs based on various parameters such as NetFlow, OS Fingerprints, threat analysis and log collection etc. Finally, we conclude that each of the NFTs has its own pros and cons. However, selection of the most appropriate NFT based on the situation and various parameters defined in the paper, will be the savior for the investigators during their investigation and help identify the defaulters.

5. References

1. Abdul R.J., Waqas A. Mamoun A., Zunera J. Kashif K., Thippa R.G." Comprehensive Survey on Computer Forensics: State-of-the-Art, Tools, Techniques, Challenges, and Future Directions" IEEEAccess , vol 10,pp.1- 4,14-15, 31 Jan 2022
2. Suleman K., Abdullah G., eta "Towards an Applicability of Current Network Forensics for Cloud Networks: A SWOT Analysis" IEEEAccess, Vol 4,pp.4-9 2016
3. Syed Rizvi, Mark Scanlon "Application of Artificial Intelligence to Network Forensics: Survey, Challenges and Future Directions" IEEEAccess vol.10, pp. 2.21oct 2022
4. Fahad M. G., Abrahim A .eta "Comparative Analysis of Network Forensic Tools and Network Forensics Processes" IEEE(ICSCEE2021)
5. Damir d., Ivan M., Goran S." Comparative Analysis of Network Forensic Tools on Different Operating Systems" MIPRO 2021,oct 2021
6. Jiao Ye "fuzzy decision tree reasoning method for network forensics analysis"2022World Automation Congress(WAC),11-15oct 2022
7. https://thesecmaster.com/how-to-analyse-a-pcap-file-using-network-miner-a-network-forensic-analysis-tool-nfat
8. https://logrhythm.com/products/features
9. https://nmap.org/
10. https://labs.ece.uw.edu/nsl/students/alomair/LB- Arabic/general/forensic-tools/xplico.html
11. https://www.wireshark.org /
12. https://www.niksun.com/netdetector.php
13. L. F. Sikos, ``Packet analysis for network forensics: A comprehensive survey , "Forensic Sci. Int., Digit. Invest., vol. 32, Mar. 2020
14. H. Arshad, A. Jantan, G. K. Hoon, and I. O. Abiodun, ``Formal knowledge model for online social network forensics," Computer. Security., vol. 89, Feb. 2020
15. Sirajuddin Qureshi, Saima T. eta" Network Forensics: A Comprehensive Review of tools and Techniques",IJACSAVol.12,No.5,May 2021
16. Ray Hunt, "New Developments in Network Forensics :Tools and Technique",IEEE,2012
17. https://www.plixer.com/
18. Kazuki Hashimoto,"Development of intellectual network forensic system LIFT against targeted

attacks", Fourth International Conference on Cyber Security, Cyber Warfare, and Digital Forensic,2015
19. Gulshan Shrivastava "Network Forensics: Methodical Literature Review", IEEE,2016
20. S. Pawar, C. Bhusari, and S. Vaz, ``Survey on digital forensics investigation and their evidences," Int. J. Adv. Res. Sci., Commun.Technol., vol. 10,2020