Network Forensics: A Comprehensive Review of Tools and Techniques

Sirajuddin Qureshi[1], Saima Tunio[2], Faheem Akhtar[3], Ahsan Wajahat[4], Ahsan Nazir[5], Faheem Ullah[6]
Faculty of Information Technology,
Beijing University of Technology, Beijing 100124, China.[1,2,4,5,6]
Department of Computer Science, Sukkur IBA University, Pakistan[3]

***Abstract*—With the evolution and popularity of computer networks, a tremendous amount of devices are increasingly being added to the global internet connectivity. Additionally, more sophisticated tools, methodologies, and techniques are being used to enhance global internet connectivity. It is also worth mentioning that individuals, enterprises, and corporate organizations are quickly appreciating the need for computer networking. However, the popularity of computer and mobile networking brings various drawbacks mostly associated with security and data breaches. Each day, cyber-related criminals explore and devise complicated means of infiltrating and exploiting individual and corporate networks' security. This means cyber or network forensic investigators must be equipped with the necessary mechanisms of identifying the nature of security vulnerabilities and the ability to identify and apprehend the respective cyber-related offenders correctly. Therefore, this research's primary focus is to provide a comprehensive analysis of the concept of network forensic investigation and describing the methodologies and tools employed in network forensic investigations by emphasizing on the study and analysis of the OSCAR methodology. Finally, this research provides an evaluative analysis of the relevant literature review in a network forensics investigation.**

Keywords*—*Network forensics; Tshark; Dumpcap; Wireshark; OSCAR; network security

I. Introduction

The evolution of computer networks and the internet has created many opportunities for the perpetration of cyber-related crimes. Numerous computing devices are connected to a complex mesh of computer networks all over the globe. Cyber attackers are continuously adapting complicated strategies to perpetuate cyber-related crimes. The nature and the type of crimes are costly to the affected victims [1]. In some instances, the committed cybercrimes not only cause significant financial losses but might also render the affected organization inoperable. Thus, it is essential to have a mechanism of performing necessary investigation and audit to establish the course and the perpetrators of the associated cybercrimes. In the context of cyber-criminal investigations, the mechanism is referred to as network forensics.

Network forensics is a digital forensic process that involves the investigation, Analysis, and monitoring of computer networks to discover essential information that helps in the apprehension of cybercriminals [2]. Network forensics also helps in gathering necessary and legal information, evidence, and traces of intrusion detection. In essence, network forensics helps a cyber-forensic investigator monitor network traffic and identify any malicious content within network traffic. Network forensics is data-centric, and thus it is not primarily restricted to the Analysis of network traffic. Instead, it is also associated with related concepts, notably mobile forensics, memory forensics, and host-based forensics [1].

Primarily recent Internet technology advances drive the evolution of network security and its associated forensic processes and related toolsets. When more facets of our everyday lives move to electronic networks and databases where they are vulnerable to illegal activity, there is a growing need for advanced analytical resources. Some widely mentioned explanations for the use of network forensics are based on

- Analysis of computer systems belonging to victims or authorities.
- Collection of facts for use in court; Recovery of lost data in the event of software and hardware failure.
- Analysis for a computer system after a break-in.
- Collection of information about how the computer systems function for debugging purposes, optimization of their computer systems The list only scratches the surface of what network forensics can do in the sense of risk management and data recovery;

The following example illustrates the critical role that this technology can play in an investigation process. The companies usually use different items when it comes to network security. Such devices typically approach protection from two main perspectives; detection and monitoring, in other words. Types of items for protection include firewalls and systems for access controls. Likewise, the intrusion detection systems and anti-virus software are examples of detection products. Although the used products foil several attacks, novel attacks often bypass protection products without being detected. Investigating the attacks in these cases is a challenging job. Serious attackers are, in many cases, skilled at removing evidence. Consequently, firewall logs and intrusion detection warnings that miss such attacks entirely or may prove insufficient for a thorough investigation, mainly when the goal is to apprehend the attacker.

Network forensics has been suggested in information security literature to incorporate investigative capabilities in existing networks. This refers to a dedicated research infrastructure that enables network packets and events to be captured and evaluated for research purposes. Complementation of the above Network Security optimization is performed. The forensic network is of significant importance to companies worldwide. On the one hand, it helps learn the specifics of recent threats, ensuring that potential attacks are thwarted. Furthermore, network forensics is essential to investigate the abuses of insiders that constitute the second most costly model of corporate assault. Lastly, law enforcement refers to network forensics for cases in which a device or digital machine is either the object of a crime or used to carry a criminal offense.

Network forensics is a complex phenomenon that needs the utilization of a variety of tools and methodologies. It is thus essential to have a good understanding of how these tools and techniques can aid in the process of network forensics and the discovery of malicious activity and intrusion attempts. This paper aims to provide a comprehensive description of network forensics' concept to understand the tools and methodologies used. Emphasis is based on giving a vivid portrait of the OSCAR methodology as used in network forensics. An analysis and review of critical related works that illustrate the practical implementation of the network forensics concept are extensively discussed.

II. Related Work

The field of network forensics attracts diverse interests that ultimately have led to the publication of various research works aimed at bridging the knowledge gap within the topic domain. In particular, much of the related works in the field of network forensics is related to security. It is essential to note that any network provided that is connected to the internet is prone to a variety of cyber-attacks. The attacks are generally designed in such a way that they exploit ay vulnerabilities within the network. A forensic investigator is thus tasked with the responsibility of coming up with essential strategies to perform a comprehensive network forensic process to identify potential cases of network intrusion [3]. In addition to the fact that the legislature has borne some of the cost of crime prevention, company secrets are compelled to utilise the most dynamic security measures available to secure their essential information [4].The advent of information and communication technologies has ushered in a new era of human existence known as the information society. As the most well-known product of this community, cyberspace has provided people with enormous opportunity to search for and store large volumes of data. This has not only improved the visibility of information, particularly scientific and economic conclusions, but it has also resulted in an increase in targeted cyber-attacks aiming at gaining unauthorised access to such sensitive data. Meanwhile, the concept of safeguarding trade secrets has taken on new significance as information with independent economic or competitive worth [5]. One of the numerous issues that trade secrets have produced as valuable and sensitive knowledge as a result of the expanding space of information and communication interchange is the widespread response of governments to the use of coercive instruments with powerful deterrent effects, such as Terry's case [6]. This research comprehensively discusses it as discussed in the related domain [7], [8], [9], [10], [11].

A. Network Security and Network Forensic

Apart from assisting in identifying and apprehending cyberterrorists and attackers, network forensics also plays a significant role in extending the security model within a network. As noted by Almulhem, network forensics helps network administrators to enhance the prevention and detection of network and cyber-related attacks. In essence, network forensics makes it possible to perform a comprehensive vulnerability analysis process to identify potential threats facing a network [12]. Almulhem adds that network forensics is more associated with a security model than a product or service aimed at enforcing security or network prevention. Instead, network or digital forensics emphasizes the design and implementation of methodologies, tools, and concepts that aim to enhance the process of forensic investigation [12].

Kilpatrick et al. suggest the implementation of SCADA (supervisory control and data acquisition systems that form a vital infrastructure for network forensics [13]. SCADA networks are essential for forensic investigations in that the underlying architecture makes it possible to analyze, monitor, and monitor network behavior [13]. In particular, the SCADA network forensics makes it possible to design and build robust SCADA networks. This is because traffic analysis is an essential constituent of the architecture of a SCADA network.

Network forensics also plays a significant role in the implementation of security mechanisms in the machine to machine networks (M2M) [14]. M2M networks utilize artificial intelligence and machine learning to improve the communication process. Network forensics is used to identify security issues in M2M networks by implementing two distinct modules; forensic and attack detection module. Further, a forensics strategy that uses anti-distributed honeypot is used to aid in detecting and preventing DDoS attacks [14].

To illustrate and reiterate the importance of network forensics investigations, it is paramount to review several case studies whereby the concept has been adequately implemented. Particularly, Kurniawan and Riadi [15] managed to explore and device a unique framework upon which it was made possible to utilize the concept of network forensics to analyze and identify the behavior of the notorious Cerber Ransomware. The approach is aimed explicitly at establishing an attempt to reconstruct the timestamp of an attack [15]. Focus is placed on the need to exact malware deemed to have infected a particular network host. The eventual results indicate that analysis of network forensics behavior can identify patterns of infections, exploits channels, and the ultimate payload associated with the Cerber Ransomware.

1) Network Security Forensic Mechanisms: A firewall within a network environment provides a network forensic investigator with a perfect opportunity to conduct a comprehensive analysis of all the previous network intrusion attempts. As noted by Messier, the majority of firewall systems are equipped with the ability to either implement the software capability in UNIX or Windows [16]. Consequently, a forensic network investigator can either analyze Syslog or Event Logs files to identify and analyze the nature of intrusion activities within and targeted towards a network. An analysis of firewall logs is also essential. It greatly assists in identifying the existing security vulnerabilities and eventually enables the security administrator to develop essential security enhancements.

Bensefia and Ghoualmi reiterate the importance of having a unique branch of network forensics primarily dedicated to analyzing firewall logs [17]. Firewall forensics is a dedicated effort aimed at analyzing firewall logs with the specific objective of gaining useful insights regarding the nature of attacks identified and blocked by the network firewall. While the contents of a firewall log file might be difficult to decode, it is noteworthy to provide essential information that will eventually help a cyber-forensics investigator apprehend a suspected cybercrime offender.

2) Honeypot Forensics: A honeypot is a specialized part of a computer or network system that is designed is such a way that it appears and seems to have critical and sensitive information. At the same time, in a real sense, it is mainly isolated from the main network. An elaborate illustration of how a honeypot device(s) is placed in a network is indicated in Fig. 1. It is worth noting that most of Honeypot's services are secret though it is difficult to assert their suspicious nature [18]. Honeypots are considered to be essential components that help to enhance the security of an organization [19]. Having a honey port within a network makes it possible for a forensic investigator to conduct a comprehensive analysis of all the possible network-related activities and logs carried throughout the honeypot device. Additionally, network forensic investigators are in a good position to perform a comparative analysis of the data obtained from the Honeypot with similar data extracted from other network devices. A network forensic investigator must perform a comprehensive analysis of the existing honeypots in a network whereby the interaction level can be categorized as low, medium, or high level.

Network forensics is restricted to the analysis of firewalls and honeypots systems, but instead, it is widely applicable among most popular network devices. IDS and IPS are perhaps some of the most common types of devices and systems that are commonly targeted by a network forensic investigator to obtain essential cyber forensic evidence that will culminate with the apprehension of a cyber-forensic offender [19]. Routers and switches also provide essential value in that it is possible to obtain essential intrusion information from MAC address tables, ports, and routing tables, among others. Web proxies, as well as, special types of servers such as DCHP, name, and application servers also provide a network forensic investigator with rich information aimed at obtaining crucial cyber forensics evidence [19].

III. Network Forensics

Network forensics is a scientific method used to discover and retrieve information with evidential value and is used to solve a cyber-crime or apprehend a cyber-criminal. The evidence is retrieved from network and computing devices such as hard disks, routers, switches, memory devices, wireless devices, and mobile devices. Table I provides additional information related to possible viewpoints based on potential areas where the forensic investigation could be performed. Network forensics differs from intrusion detection in that the gathered evidence should be admissible in a court of law and thus should satisfy both legal and technical requirements [20]. Consequently, for forensic evidence to be accepted in a court of law, it must be authentic, relevant, complete, reliable, and believable. It is also noteworthy that the tools and techniques used to perform network forensics should also meet a court of law's legal and technical requirements.

While intrusion detection helps strengthen and improve a computer network's security, network forensics is primarily associated with the need to identify the evidence related to a security breach. In most cases, network forensics helps to solve matters related to cyber-terrorism, child pornography, narcotics, homeland security, online fraud, and corporate espionage, among others [21]. Public police mostly use the evidence obtained from network forensics and private investigators working for individuals, businesses, law enforcement agencies, and even the military [20]. It is also essential to note that business organizations and the military might also use network forensics to ensure continuity and availability of core services. In this context, network forensics help to identify vulnerabilities in corporate networks that make it convenient to implement the necessary security enhancements.

The context of the discussion offered in the paper is to explore the investigative purposes of network forensics. The investigation process starts with identifying a malicious activity upon which the evidence is then collected and preserved. The forensic activity proceeds to examine and analyze the evidence to establish the source and the nature of the malicious activity. Finally, the evidence is reported and presented to the relevant stakeholders and eventually used to make the required decision. All the essential processes involved in network forensic investigation are strategically executed using OSCAR principles that are explained in the next section.

IV. Network Forensics Methodology (OSCAR)

To ensure that forensic evidence is both accurate and reproducible, the OSCAR methodology of Network Forensics Investigation is applied. OSCAR [22] is an acronym that stats for,

- O for Obtaining Information
- S for Strategizing
- C for Collecting Evidence
- A for Analyzing Evidence
- R for Reporting

Fig. 2 illustrates the flow chart model for the OSCAR methodology.

A. Obtaining Information

This stage is associated with obtaining information regarding the incident itself and the environment in which the event took place. It is essential to collect as much information about an event to know exactly what took place. Usually, it is advisable to collect information on the description of the incident, time, date, and how it was discovered [15]. Other entities related to the event include the systems, persons, and devices involved and the summary of actions taken after the incidence discovery. It is also essential to note details about the review of discussions made, any legal issues, and the identity of the incident manager. The environment helps the forensic investigator have a good understanding of the organization's response towards an incident and the stakeholders who should be involved in the investigation process [23]. It is thus vital to collect as much information related to the organization as

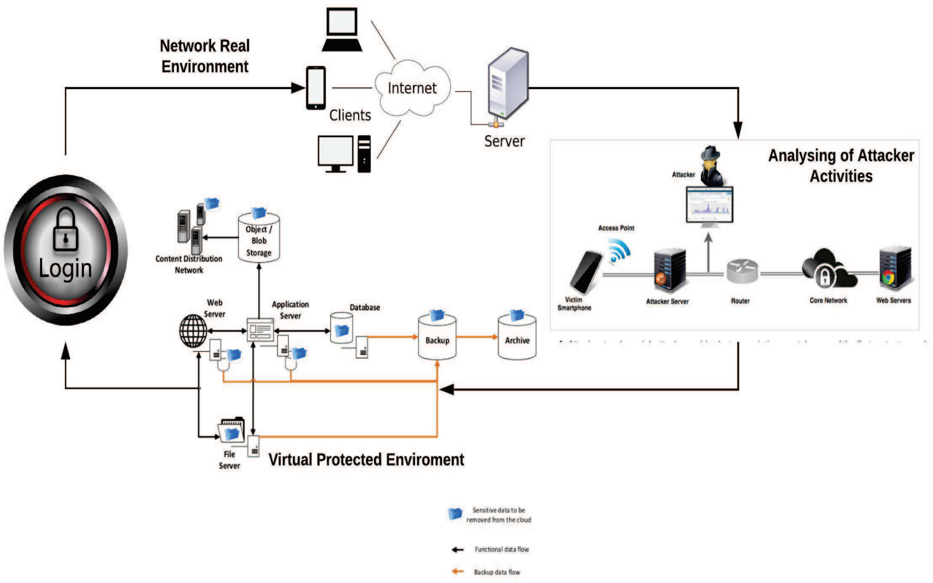

Fig. 1. Logical Placement of a Honeypot within a Network.

TABLE I. Presents Additional Information Related to Possible Viewpoints based on Possible Areas where Forensic Investigation Could be Performed

View Point	Nature of Forensics
Application	Internet browser, email, register files, application software, virus, worm, Trojans, and files (slack, erased, and swap)
System	UNIX, Windows, log system, and audit system
Hardware	PC, PDA, printer, router, switches, firewall, and IDS
Processing	Victim's, intermediate's, and attacker's side

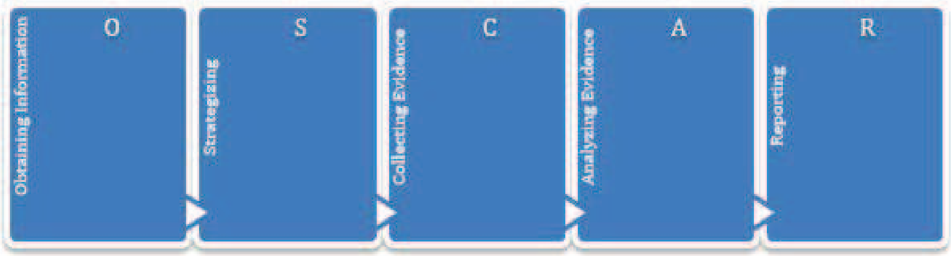

Fig. 2. Network Forensics Investigation Methodology (OSCAR).

possible. Relevant information includes the business model, any legal issues, available resources, communication systems, network topologies, and the procedures and processes used for incidence response management.

B. Strategy

Strategy requires the formulation of a detailed plan on how to carry out the investigation. Strategizing also details how evidence will be acquired [15]. This should be done using various criteria, mainly because pieces of evidence from different sources have varying levels of volatility. As indicated in Table II, the acquisition of proof should be based on several parameters such as source, the effort required, volatility, and the expected value. Evidence prioritization is vital because it helps the forensic to establish the priority of assigning personnel and resources required in network forensics. An important aspect worth noting is that each organization has different policies associated with data retention, access, and configurations [22]. Consequently, the evidence prioritization should be based on specific organizational policies. When formulating an evidence acquisition strategy, it is paramount to consider the following tips.

- Understand the goal of investigation and time frame
- List of your recourses
- Prioritize your evidence acquisition
- Estimate the value and cost of obtaining evidence
- Identify sources of evidence
- Plan to initial analysis
- Keep in mind that network forensics is a process that can be performed reiteratively

C. Collecting Evidence

The strategizing step requires the formulation of an acquisition plan and prioritization of evidence sources. Evidence used in network forensics can be obtained either from the end or intermediate devices [22]. In the former, the evidence can be gathered from the attacker's or the victim's devices, while in the latter, evidence can be obtained from third-party devices and networks. A summary of the probable sources of evidence is provided in Table III.

The next step is to collect evidence from the identified sources using the established priority. Consequently, three vital components must be considered, notably documentation capture, and store or transport.

Documentation: This means that all actions, including a list of all systems, files, and resources, should be carefully logged. It is also essential to maintain self-descriptive notes that make it easy to identify the collected evidence. The descriptive content should contain the date, time source, investigating officer, and the method used to acquire the evidence. Ensure that all devices accessed and all actions were taken during the gathering of evidence are kept to a careful log. Your notes must be kept appropriately and can be cited in court. If the case is not going to court, the notes will also be very helpful during the review. Make sure to document the date, time, source, acquisition process, investigator name(s), and custody chain.

Capturing: evidence involves ensuring that the data or network traffic packets, as well as logs, are written to a hard, CD, or removable hard drive. Network forensics tools such as Wireshark and tcpdump are used to capture data packets [15].

Store/Transport: implies that the evidence should be stored in a secure place to maintain the chain of custody. It is essential to keep updated and signed log containing the details of all the parties who have obtained access to the evidence. Care should also be exerted when handling and disposing of evidence to maintain its integrity, reliability, and admissibility before a court of law.

TABLE II. PRESENTS EXAMPLE OF PRIORITIZATION OF EVIDENCE THAT LIST POSSIBLE SOURCES OF PROOF IN THE CASES, THE PROBABLE VALUE, LIKELY EFFORT OF OBTAINING AND THE EXPECTED VOLATILITY. FOR EVERY INVESTIGATION THESE PRINCIPLES WERE SELECT DISTINCT

Source of Evidence	Likely value	Effort	Volatility	Priority
Web Proxy Cache	High	Low	Medium	1
Firewall logs	High	Medium	Low	2
ARP tables	Low	Low	High	3

In summary, the following tips are crucial during the process of evidence collection.

- Obtaining evidence as soon as possible.
- Make verifiable steganography copies of collected evidence.
- Use reliable and reputable tools
- Document everything, which helps you later.
- Keep secure your notes and hide the original under restricted custody and access.

D. Analyze

The strategizing step requires the formulation of an acquisition plan and prioritization of evidence sources. Evidence used in network forensics can be obtained either from the end or intermediate devices [22]. In the former, the evidence can be gathered from the attacker's or the victim's devices, while in the latter, evidence can be obtained from third-party devices and networks. A summary of the probable sources of evidence is provided in Table III.

The next step is to collect evidence from the identified sources using the established priority. Consequently, three vital components must be considered, notably documentation capture, and store or transport.

Documentation: This means that all actions, including a list of all systems, files, and resources, should be carefully logged. It is also essential to maintain self-descriptive notes that make it easy to identify the collected evidence. The descriptive content should contain the date, time source, investigating officer, and the method used to acquire the evidence. Ensure that all devices accessed and all actions were taken during the gathering of evidence are kept to a careful log. Your notes must be kept appropriately and can be cited in court. If the case is not going to court, the notes will also be very helpful during the review. Make sure to document the date, time, source, acquisition process, investigator name(s), and custody chain.

Capturing: evidence involves ensuring that the data or network traffic packets, as well as logs, are written to a hard, CD, or removable hard drive. Network forensics tools such as Wireshark and tcpdump are used to capture data packets [15].

Store/Transport: implies that the evidence should be stored in a secure place to maintain the chain of custody. It is essential to keep an updated and signed log containing the details of all the parties who have obtained access to the evidence. Care should also be exerted when handling and disposing of evidence to maintain its integrity, reliability, and admissibility before a court of law.

In summary, the following tips are crucial during the process of evidence collection.

E. Report

This is perhaps the most crucial aspect of forensic investigation primarily because it helps to convey the results to the concerned parties. Thus, it is vital to present the report in a manner that can be understood by a lay and non-technical

TABLE III. Provides Evidence used in Network Forensics that can be Obtained Either from the End or Intermediate Devices

Affiliation	Source
End side (attacker and/or victim side)	Operation system audit trail, system event log, application event log, alert log, recovered data, and swap files
Intermediate	Traffic data packets, firewall log, IDS log, router log, and access control log

TABLE IV. Tools & Devices Use for Various Testing Applications

Device/Tool	Usage	Software/OS Version	Company/Developed
Mac-Book Air	Create a test network, host proxies	macOS Siera (10.12.6)	Apple
iPad	Test device connected to test network	iOS 11.2.6	Apple
Charles Proxy	Capture/save live network traffic	4.2.5	Karl von Randow
Wireshark	Capture/save live network trafficv	2.6.0	Wireshark
Burp Suite	Capture live network traffic	1.7.33	PortSwigger Security
Windows Laptop	Network forensics of iOS apps	Windows 10	Windows
NetworkMiner	Analyze network traffic	2.3.1	NETRESEC Erik Hjelmvik

audience. Additionally, the report should be not only factual but also contains defensible details. The report's technical information and results should be explained thoroughly to aid in the decision-making process.

V. Network Forensic Tools

Network forensic tools help in network investigation to gather essential information about an intrusion activity. These tools are used to analyze network traffic to identify the nature and type of activities within the network over a specific duration [45]. The forensic tools are designed so that they are compatible with network hardware devices such as firewalls, thereby making it possible to collect and preserve network traffic.

Additionally, these tools are equipped with the ability to perform a quick analysis of network traffic. Network forensics tools can be categorized based on either host-based or network-wide-based. Additional categories include general-purpose tools, specific tasks tools, or libraries/framework tools [46]. A review of the most frequently used network forensic tools is summarized in Table IV. The following subsections discuss them comprehensively.

A. Wireshark

Wireshark is an open-source graphical user interface application software tool designed to capture, filter, and analyze network traffic. It is easy to use, and thus it is helpful in the analysis of network forensics data. Wireshark has more packet filtering capabilities, decoding protocol features, and packets detail markup language (PDML). In Wireshark, it is possible to view network packets as they are captured in real-time. Wireshark also shows the results of lost pockets due to CPU power [47]. Wireshark can be used as several instruments in one Anwendung. Program. You will use it to evaluate the structure of Network traffic checking for potential security flaws And assaults on health. This can detect other types of Encapsulation, isolation, and show of all fields in the Packet network. You have all those powerful capabilities. Do you think Wireshark's hard to know? For specific instances, Respect it, but you can quickly learn how to use it, the filters with the app, and how to use them Packets unique to the network. Filters in WireShark refer to Berkeley Packet Filters. That is simply a language for microprogramming Compiled against packets and executed at run time Taken off by software like tcpdump and Wireshark. Primarily, filters are used to separate a Quite small parcel set among a large number of Packets focused on search criteria. The filter is compiled to run as best Quality, significant when you are doing a quality Real-time grab. Filtering is for others WireShark's most essential features since it makes Achieving two purposes: selectively collecting the packets From the network, and to locate interested parties Packages [47][48] [49].

B. Tshark

Tshrak is a command-line tool used for data network protocol analysis. It helps to capture traffic from a live data network and read traffic information from saved packet data files. It can also print a decoded form of network packets to a quality output or writes the packet to a pcap file. For instance, tshark can capture data traffic on the network interface "eth1" filtering out all traffic from port 22 and sorting the results in the file "test1.pcap. # tshark I eth1 w test1.pcap" not port 22. Capture on eth1 235. Tshark is a packet capture application that can potent-sensing and explain pcap scrutiny functionality. It captures packet-data from an alive network or inspects packets from an earlier trapped file and decodes those packets' form into the standard output file. The default capture file format built into TShark is pcap. Weka consists of data pre-processing, classification, regression, clustering, correlation and visualization methods that are well-suited to the creation of new schemes [22] [50] [51].

C. Dumpcap

The dumpcap is a network traffic analysis tool, which is designed to capture data packets. It is a Wireshark distribution tool, which comes in command-line. The tool captures traffic from a live network and is equipped to write the output in a pcapng file format. Dumpcap has the added advantage of using fewer system resources, making it possible to boost the capture capabilities. Table V provides a summative analysis of popular tools used for network forensics [47].

D. Network Forensic Analysis Tools (NFATs)

Network Forensic Analysis Tools (aka NFATs) allow network investigators and system administrators to track networks and gather any anomalous or malicious traffic information. Such tools synergize with network infrastructure and network

TABLE V. MOST COMMONLY USED TOOLS TO SUPPORT VARIETY OF NETWORK FORENSIC INVESTIGATIONS

Tools	Open Sourece/ Proprietary software	Plateform	Website	Attributes
TCPDump Win dump [24], [25]	Open Source	Unix/Windows	www.tcpdump.org	F
Ngrep [26], [27]	Open Source	Unix	http ://ngrep.sourceforge.net	F
Wireshark [28] [29] [28]	Open Source	Unix/Windows	www.Wireshark.org	F
Driftnet [28]	Open Source	Unix/Windows	www.backtrack-linux. Org/backtrack-S-releue [Release 3, August 2012]	F F
NetworkMiner [30] [31]	Open Source /Prop	Windows	www.netresec.com/?page=NetworkMiner	F
Airmon-ng. Airodump-ng & Aireplay-ng. [32] [33]	Open Source	Unix	www.backtrack-linux. Org /backtrack-S-releue [Release 3, August 2012]	F L R C F L R C
Kismet [33]	Open Source	Unix/Windows	www.kismetwireless.net	F
NetStumbler [34]	Open Source	Windows	www.netstumbler.com	F
Xplico [35]	Open Source	Unix	http://packetstormsecuity.org/files/tags/forensics	F
DeepNines [35]	Proprietary	Unix	www.deepnines.com	F
Sleuth Kit [36]	Open Source	Unix	www.sleuthkit.org	F R C
Argus [33]	Open Source	Unix	www.qosient.com/argus	F L
Fenris [31]	Open Source	Unix	http://camtuf.coredump.cx/fenris/whatis.shtml	F
Flow-Tools [30]	Open Source	Unix	www.splintered.net/sw/flowtools	F L
EtherApe [31]	Open Source	Unix	http ://etherape.sourceforge.net	F
Honeyd [37] [38]	Open Source	Unix	www.citi.umich.edu/u/provos/honeyd	F
SNORT [24], [25]	Open Source	Unix/Windows	www.snort.org	F
Omnipeek/ /EtherPeek [37]	Proprietary	Windows	www.wildpackets.com	F L R
Savant [31]	Proprietary	Appliance /Windows	www.intrusion.com	F R
Forensic Log Analysis-GUI [31]	Open Source /Prop	Unix	http://sourceforge.net/projects/pyflag	L
Dragon IDS [39] [40]	Proprietary	Unix	www.enterasys.com	F R L C
Infinistream [40]	Proprietary	Appliance	www.netscout.com	F R C
RSA En Vision [31]	Proprietary	Appliance /Windows	www.emc.com/security/rsa-envision.html	F L R C A
NetDetector [41] [42]	Proprietary	Appliance	www.niksun.com	F R C A
NetIntercept [43]	Proprietary	Appliance	www.nikson.com/sandstom.php	F R C A
NetWitness [44]	Proprietary	Windows	www.netwitness.com [www.rsa.com]	F L R C A

appliances, such as firewalls and IDS, to make it possible to maintain long-term network traffic records. NFATs allow for rapid analyzes of patterns detected by network security tools.

VI. SYSTEM TYPES ARE USED TO GATHER DATA / TRAFFIC FROM THE NETWORK

Two types of Network traffic collecting data systems can be "stop, look and listen" or "catch-it-as-you-can."

"Catch-it-as-you-can": All packets are sent to the database through a traffic point where they are stored in. The analysis is then conducted on stored data. Data from the analysis is also stored in the database. The data saved can be preserved for future review. Nevertheless, it should be noted that this type of device demands a considerable storage capacity.

The "stop, look and listen" method is different from the "catch-it-as-you-can" approach because only data is stored in the database needed for analysis. The incoming traffic in memory is filtered and processed in real-time, meaning this device needs less storage and a much faster processor.

Since the two systems need ample storage space, it is necessary to weigh and address privacy issues with the "catch-it-as-you-can" system. This program also collects user data; however, ISPs are prohibited from receiving or revealing information without user permission.

VII. CHALLENGES RELATING TO NETWORK EVIDENCE

Network-based evidence faces specific challenges in many fields, including collection, storage, content, privacy, confiscation, and admissibility. Below we'll cover some of the significant issues Below.

Collection : Within a network environment, clear proof can be hard to locate. Networks include as many bits of data as possible; from wireless devices to web proxies to big log servers; which often makes it difficult to determine the proof's correct position. Even if you know where a specific piece of evidence exists, it can be difficult for political or technological purposes to access it.

Storage: Commonly, the network of computers can not use permanent or secondary data. As a result, the data they hold can be so fragile they won't survive a computer reset.

Content: Unlike files, management to contain all file contents and their metadata, network devices with the desired degree of granularity may or may not store information. Network computers also have minimal storage capacity, instead of full data records that have crossed the network, only selected transaction or data transfer metadata are typically retained.

Privacy: Legal problems related to personal privacy occur unique to computer network-based retrieval techniques, depending on the jurisdiction.

Sezure: Seizing a hard disk may disturb a person or an organization. Nonetheless, it is also possible to design and implement a replica of the original, so that critical operations can continue with minimal disruption. Seizing a networked device can be even more damaging. A whole part of the network can be downgraded indefinitely for more extreme situations. Investigators can, however, minimize the impact on computer network operations in such circumstances.

Admissibility: For criminal and civil cases, evidence-based on file systems is now widely acknowledged. So long as the evidence stored on the file system is legitimate collected, adequately interpreted, and relevant to the case, there are clear precedents for the processing and presenting the evidence in court. In comparison, network forensics is a modern approach to automated investigations. There are often contradictory or even non-existent legal precedents for accepting different kinds of facts based on the digital network. With time, digital network-based testimony becomes more prevalent, setting precedents for the case and standardizing them.

VIII. Conclusion

Network forensic investigation is an essential process that helps a cyber-forensics investigator to obtain, analyze, evaluate, categorize, and identify crucial evidence. It ultimately makes it possible to apprehend a cyber-criminal or any person suspected of committing a cyber-criminal offense. Consequently, it is paramount for a network forensic investigator to consider adopting and utilizing an efficient and robust forensic network investigation methodologies that ultimately help improve the investigation process. As intimated in this research, the OSCAR methodology provides a forensic investigator with essential tools and guidelines that determines the approach, methods, and strategies used to obtain, strategize, collect, analyze, and report the findings of a network forensics investigations. It is also paramount for the network forensic investigation process to follow and be executed using essential tools such as Wireshark, tshark, Burpe Suite, and tcpdump that tends to help in simplifying and improving the forensics investigation process. Future work: To developed a tool-kits that parse various network protocols commonly used in various sorts of different networks are required. And, because most data in networks is volatile, it may be necessary to preserve or document it selectively in advance to speed up the forensic process.

References

[1] M. Matsalu *et al.*, “Digitaalse ekspertiisi tööjõu pädevuse arendamine eesti kaitseliidu näitel,” Ph.D. dissertation, 2019.

[2] G. S. Chhabra and P. Singh, “Distributed network forensics framework: A systematic review,” *International Journal of Computer Applications*, vol. 119, no. 19, 2015.

[3] G. A. Pimenta Rodrigues, R. de Oliveira Albuquerque, F. E. Gomes de Deus, G. A. De Oliveira Júnior, L. J. García Villalba, T.-H. Kim *et al.*, “Cybersecurity and network forensics: Analysis of malicious traffic towards a honeynet with deep packet inspection,” *Applied Sciences*, vol. 7, no. 10, p. 1082, 2017.

[4] D. Chang, M. Ghosh, S. K. Sanadhya, M. Singh, and D. R. White, “Fbhash: A new similarity hashing scheme for digital forensics,” *Digital Investigation*, vol. 29, pp. S113–S123, 2019.

[5] L. Liebler, P. Schmitt, H. Baier, and F. Breitinger, “On efficiency of artifact lookup strategies in digital forensics,” *Digital Investigation*, vol. 28, pp. S116–S125, 2019.

[6] K. Karampidis, E. Kavallieratou, and G. Papadourakis, “A review of image steganalysis techniques for digital forensics,” *Journal of information security and applications*, vol. 40, pp. 217–235, 2018.

[7] F. Akhtar, J. Li, M. Azeem, S. Chen, H. Pan, Q. Wang, and J.-J. Yang, “Effective large for gestational age prediction using machine learning techniques with monitoring biochemical indicators,” *The Journal of Supercomputing*, pp. 1–19, 2019.

[8] J. Li, D. Zhou, W. Qiu, Y. Shi, J.-J. Yang, S. Chen, Q. Wang, and H. Pan, “Application of weighted gene co-expression network analysis for data from paired design,” *Scientific reports*, vol. 8, no. 1, pp. 1–8, 2018.

[9] F. Akhtar, J. Li, Y. Pei, A. Imran, A. Rajput, M. Azeem, and Q. Wang, “Diagnosis and prediction of large-for-gestational-age fetus using the stacked generalization method,” *Applied Sciences*, vol. 9, no. 20, p. 4317, 2019.

[10] A. Imran, J. Li, Y. Pei, J.-J. Yang, and Q. Wang, “Comparative analysis of vessel segmentation techniques in retinal images,” *IEEE Access*, vol. 7, pp. 114 862–114 887, 2019.

[11] J. Li, L. Liu, J. Sun, H. Mo, J.-J. Yang, S. Chen, H. Liu, Q. Wang, and H. Pan, “Comparison of different machine learning approaches to predict small for gestational age infants,” *IEEE Transactions on Big Data*, 2016.

[12] A. Almulhem, “Network forensics: Notions and challenges,” in *2009 IEEE International Symposium on Signal Processing and Information Technology (ISSPIT)*. IEEE, 2009, pp. 463–466.

[13] T. Kilpatrick, J. Gonzalez, R. Chandia, M. Papa, and S. Shenoi, “An architecture for scada network forensics,” in *IFIP International Conference on Digital Forensics*. Springer, 2006, pp. 273–285.

[14] K. Wang, M. Du, Y. Sun, A. Vinel, and Y. Zhang, “Attack detection and distributed forensics in machine-to-machine networks,” *IEEE Network*, vol. 30, no. 6, pp. 49–55, 2016.

[15] A. Kurniawan and I. Riadi, “Detection and analysis cerber ransomware based on network forensics behavior,” *International Journal of Network Security*, vol. 20, no. 5, pp. 836–843, 2018.

[16] R. Messier, *Network forensics*. John Wiley & Sons, 2017.

[17] H. Bensefia and N. Ghoualmi, “An intelligent system for decision making in firewall forensics,” in *International Conference on Digital Information and Communication Technology and Its Applications*. Springer, 2011, pp. 470–484.

[18] S. Krasser, G. Conti, J. Grizzard, J. Gribschaw, and H. Owen, “Real-time and forensic network data analysis using animated and coordinated visualization,” in *Proceedings from the Sixth Annual IEEE SMC Information Assurance Workshop*. IEEE, 2005, pp. 42–49.

[19] Q. Al-Mousa and Z. Al-Mousa, “Honeypots aiding network forensics: Challenges and notins,” *Journal of Communication*, vol. 8, no. 11, pp. 700–707, 2013.

[20] J. Llano Tejera, “Herramientas forenses para la respuesta a incidentes informáticos,” Ph.D. dissertation, Universidad Central” Marta Abreu” de Las Villas, 2014.

[21] W. Ren, “Modeling network forensics behavior,” *Journal of Digital Forensic Practice*, vol. 1, no. 1, pp. 57–65, 2006.

[22] S. Davidoff and J. Ham, *Network forensics: tracking hackers through cyberspace*. Prentice hall Upper Saddle River, 2012, vol. 2014.

[23] J. Buric and D. Delija, “Challenges in network forensics,” in *2015 38th International Convention on Information and Communication Technology, Electronics and Microelectronics (MIPRO)*. IEEE, 2015, pp. 1382–1386.

[24] P. Arlos and M. Fiedler, “A comparison of measurement accuracy for dag, tcpdump and windump,” *available online at Blekinge Institute of Technology (Sweden)¡ www. its. bth. se/staft/pca*, 2007.

[25] P. Goyal and A. Goyal, “Comparative study of two most popular packet sniffing tools-tcpdump and wireshark,” in *2017 9th International Conference on Computational Intelligence and Communication Networks (CICN)*. IEEE, 2017, pp. 77–81.

[26] D. Dittrich, “Dissecting distributed malware networks,” *Availabel from:¡ http://security. isu. edu/ppt/pdfppt/Core02. pdf*, 2002.

[27] J. R. Binkley and S. Singh, “An algorithm for anomaly-based botnet detection.” *SRUTI*, vol. 6, pp. 7–7, 2006.

[28] U. Banerjee, A. Vashishtha, and M. Saxena, “Evaluation of the capabilities of wireshark as a tool for intrusion detection,” *International Journal of computer applications*, vol. 6, no. 7, pp. 1–5, 2010.

[29] L. Chappell, "Wireshark 101: Essential skills for network analysis-wireshark solution series," *Laura Chappell University, USA*, 2017.

[30] R. Chowdhary, S. L. Tan, J. Zhang, S. Karnik, V. B. Bajic, and J. S. Liu, "Context-specific protein network miner–an online system for exploring context-specific protein interaction networks from the literature," *PLoS One*, vol. 7, no. 4, p. e34480, 2012.

[31] R. Umar, I. Riadi, and B. F. Muthohirin, "Live forensics of tools on android devices for email forensics," *Telkomnika*, vol. 17, no. 4, pp. 1803–1809, 2019.

[32] P. Čisar and S. M. Čisar, "Ethical hacking of wireless networks in kali linux environment," *Annals of the Faculty of Engineering Hunedoara*, vol. 16, no. 3, pp. 181–186, 2018.

[33] O. Barybin, E. Zaitseva, and V. Brazhnyi, "Testing the security esp32 internet of things devices," in *2019 IEEE International Scientific-Practical Conference Problems of Infocommunications, Science and Technology (PIC S&T)*. IEEE, 2019, pp. 143–146.

[34] S. Ekhator, "Evaluating kismet and netstumbler as network security tools & solutions." 2010.

[35] J.-N. Hilgert, M. Lambertz, and D. Plohmann, "Extending the sleuth kit and its underlying model for pooled storage file system forensic analysis," *Digital Investigation*, vol. 22, pp. S76–S85, 2017.

[36] J.-N. Hilgert, M. Lambertz, and S. Yang, "Forensic analysis of multiple device btrfs configurations using the sleuth kit," *Digital Investigation*, vol. 26, pp. S21–S29, 2018.

[37] N. Provos, "Honeyd-a virtual honeypot daemon," in *10th DFN-CERT Workshop, Hamburg, Germany*, vol. 2, 2003, p. 4.

[38] R. Chandran, S. Pakala *et al.*, "Simulating networks with honeyd," *online], Technical paper, Paladion Networks, December*, 2003.

[39] P. Kazienko and P. Dorosz, "Intrusion detection systems (ids) part 2-classification; methods; techniques," *WindowsSecurity. com*, 2004.

[40] J. Kipp *et al.*, "Using snort as an ids and network monitor in linux," *GIAC*, pp. 1–4, 2001.

[41] P. Lin, K. Ye, and C.-Z. Xu, "Netdetector: an anomaly detection platform for networked systems," in *2019 IEEE International Conference on Real-time Computing and Robotics (RCAR)*. IEEE, 2019, pp. 69–74.

[42] Y. R. Wang and A. Kanemura, "Designing lightweight feature descriptor networks with depthwise separable convolution," in *????????????? ? 34 ????? (2020)*. ?????? ??????, 2020, pp. 2K1ES204–2K1ES204.

[43] R. Joshi and E. S. Pilli, "Network forensic tools," in *Fundamentals of Network Forensics*. Springer, 2016, pp. 71–93.

[44] T. A. Moore, M. E. Longworth, B. Girardi, and D. Love, "Apparatus and method for network analysis," Dec. 15 2009, uS Patent 7,634,557.

[45] M. H. Mate and S. R. Kapse, "Network forensic tool–concept and architecture," in *2015 Fifth International Conference on Communication Systems and Network Technologies*. IEEE, 2015, pp. 711–713.

[46] A. Lazzez, "A survey about network forensics tools," *Int. J. Comput. Inf. Technol*, vol. 2, no. 1, 2013.

[47] R. Hunt and S. Zeadally, "Network forensics: an analysis of techniques, tools, and trends," *Computer*, vol. 45, no. 12, pp. 36–43, 2012.

[48] S. Wang, D. Xu, and S. Yan, "Analysis and application of wireshark in tcp/ip protocol teaching," in *2010 International Conference on E-Health Networking Digital Ecosystems and Technologies (EDT)*, vol. 2. IEEE, 2010, pp. 269–272.

[49] V. Ndatinya, Z. Xiao, V. R. Manepalli, K. Meng, and Y. Xiao, "Network forensics analysis using wireshark," *International Journal of Security and Networks*, vol. 10, no. 2, pp. 91–106, 2015.

[50] Y. Lee and Y. Lee, "Toward scalable internet traffic measurement and analysis with hadoop," *ACM SIGCOMM Computer Communication Review*, vol. 43, no. 1, pp. 5–13, 2012.

[51] R. Menon and O. G. MENON, "Mining of textual databases within the product development process," Ph.D. dissertation, 2004.