INFOGAIN PUBLICATION

International Journal of Advanced Engineering, Management and Science (IJAEMS)
Peer-Reviewed Journal
ISSN: 2454-1311 | Vol-9, Issue-4; Apr, 2023
Journal Home Page: https://ijaems.com/
Article DOI: https://dx.doi.org/10.22161/ijaems.94.1

Evaluating Network Forensics Applying Advanced Tools

Abdullah Shah

engabdullah838@gmail.com

Received: 24 Feb 2023; Received in revised form: 18 Mar 2023; Accepted: 25 Mar 2023; Available online: 03 Apr 2023

Abstract— *Network forensics comes under the domain of digital forensics and deals with evidences left behind on the network after a cyber-attack. It is indication of the weakness that led to the crime and the possible cause. Network focused research comes up with many challenges which involves the collection, storage, content, privacy, confiscation and the admissibility. It is important and critical for any network forensic researcher or the investigator to consider adopting efficient forensic network investigation framework or the methodologies in order to improve investigation process. The main aim of this research contribution was to do a comprehensive analysis of concepts of networks forensics through extensive investigation and by analyzing various methodologies and associated tools which should be used in the network forensic investigations. Detailed and in depth analysis of concepts of network forensic investigation on a designed/conceived network architecture was carried out which was then followed by analyzing various methodologies and tools employed. An innovative framework for the investigation was designed which can be used by any forensic expert. The acquired data was analyzed by using information, strategizing and collecting evidence and by analyzing and reporting of the methodologies on the conceptualized network. Consequently, it led to the researcher to adopt and utilize a powerful and efficient forensic network methodology that will ultimately help in improving the investigation process and providing required tools/techniques along with the requisite guidelines that will determine the approach, methods, and strategies which are to be used for network forensic process to be followed and be executed with the use of relevant tools that will tend to help in the simplification and improvement of the forensics investigation process.*

Keywords— ***Forensic Science, Network Forensics, OSCAR.***

I. INTRODUCTION & BACKGROUND

In this section, the author presents introduction and the chosen topics background relating to Network Forensics and various concepts pertaining to it including the advanced tools being used to achieve this.

1.1. Introduction & Background

The Digital forensic and subsequently the network forensics stems from the forensic science with its evolution shown below;

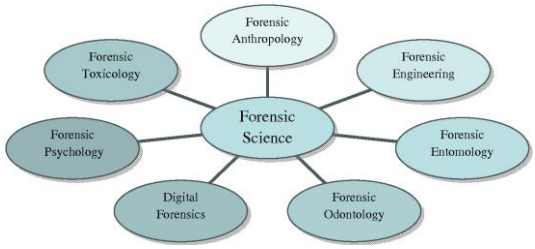

Fig.1.1: Forensic Science Branches

The forensic science has many sub-branches which are shown in the figure above and for each of them the advanced research is being carried out by the field researchers. Figure below shows in more detail how the forensic science has penetrated in every walk of life.

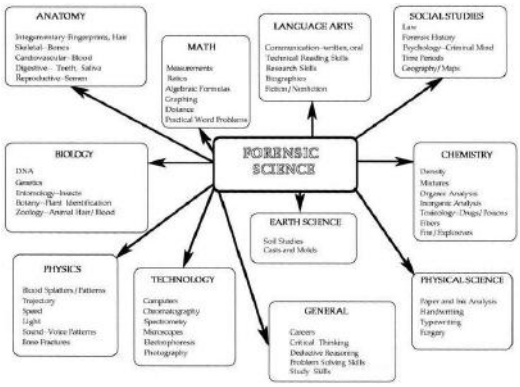

Fig.1.2: Forensic Science Penetration

Network forensics falls under the category of (DF) related to monitoring and analyzing computer network traffic for data collection purposes. Unlike DF, network forensic deals with dynamic information. It comes under the domain of DF and is related to the investigation of evidence left on the network following any cyber-attack. This forensic allowed the businesses to make it possible to enhance their security situation and apply the requisite corrections appropriately.

In fact, network forensics is a subset of the digital forensics itself is a branch of intelligence science - where jurists look for technologies or data that contain criminal evidence. Network forensics, surprisingly, refers to the investigation and analysis of all network traffic suspected of cybercrime i.e. proliferation of malicious software that steals data.

Law enforcement agencies use network forensics to analyze network traffic data collected from suspected criminal activities. Analysts will search for data that identifies human interactions, file fraud, and through use of keywords. By the use of network and digital forensics, the law enforcement agencies and the crime investigators can track communications and can easily set up time-based network events installed through a network controlled system.

In addition to criminal investigations, network forensics is often used to analyze network events in order to trace the origins of robberies and other security-related incidents. This includes looking at suspected network locations, collecting information about network features and resources & identifying incidents of unauthorized network access.

There exist 2 methods for full network forensics;

1. Catch as much as possible" method: Capturing network traffic for analysis requiring long process and maintenance.
2. Stop, watch and listen method: Based on analyzing each data packet which passes across network only what looks like suspicious and worthy of analysis data thus needing lots of processing power but can be achieved by less storage space.

Unlike DF, network forensics are much harder to perform as data transferred across the network and then lost; in CF data is usually stored on disk or solid state storage which makes them easy to access.

The applications of Digital Forensics are shown below;

Fig.1.3: Applications of Digital Forensics

The subsequent domains falling under them are shown in the figures below.

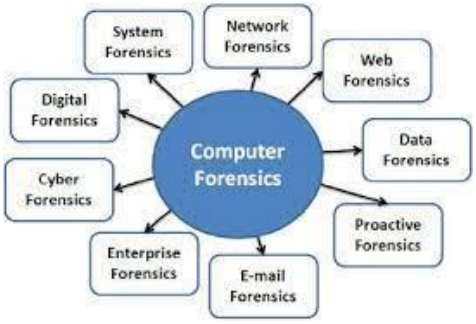

Fig.1.4: Computer Forensics

Fig.1.5: Mobile Forensics

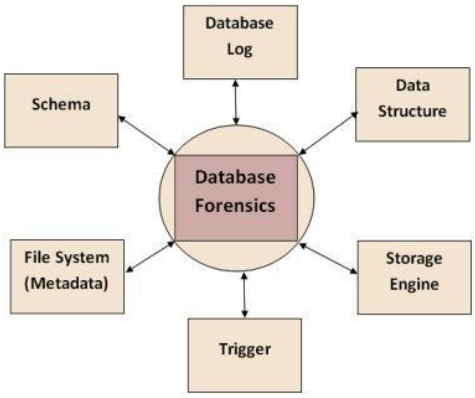

Fig.1.6: Database Forensics

Fig.1.6: Live Forensics

And finally the Network Forensics and its challenges, being the focus of this research contribution.

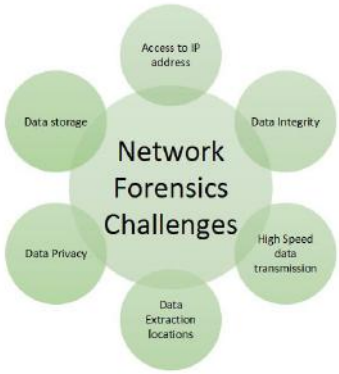

Fig.1.7: Network Forensics

Investigative process includes:

- I - Identification
- P - Preservation
- C - Collection
- E - Examination
- A - Analysis
- P - Presentation

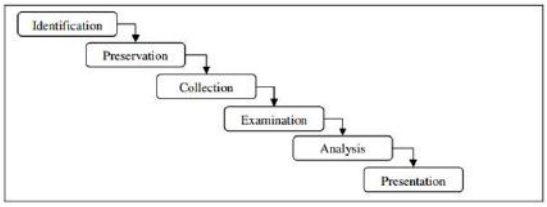

Fig.1.8: Network Forensics Investigative Process

Identifying attack patterns requires understanding of applications and network protocols.

- Protocols (on the web)
- FTP - File Transfer Protocols
- E-Mail (Protocols)
- Network (Protocols)

Application-Specific Digital Forensics Investigative Model is shown below;

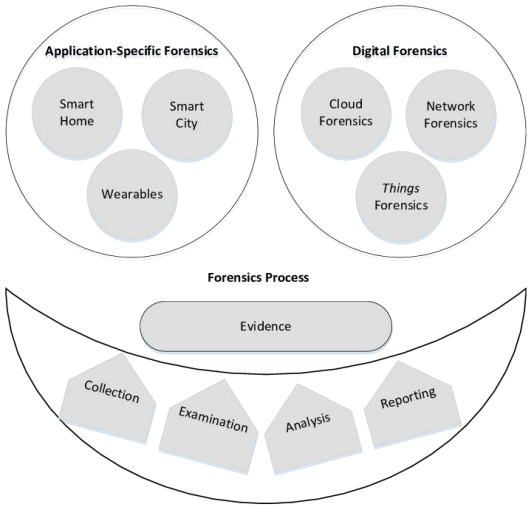

Fig.1.8: Digital Forensics Investigative Model

Network Forensics Tools include;

- Wireshark
- Tshark
- Dumpcap
- Network Forensic Analysis Tools

The requisite features are shown in the below figures.

Fig.1.9: Wireshark Features
(Source: https://www.wireshark.org/)

Fig.1.10: Tshark Features [25]

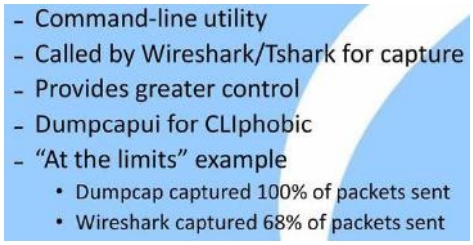

Fig.1.11: Dumpcap Features
(Source: https://docplayer.net/10961126-I3-maximizing-packet-capture-performance-andrew-brown.html)

Name	Platform	Description
Paraben Netanalysis	Windows	It interrogates the Web browser cache and history data with powerful searching, filtering, and evidence identification.
LogLogic's LX 2000	Windows	It is a log analysis tool. It ingests and processes all log files to secure, monitor and manage the IT environment. It dramatically reduces the time and cost required to uncover the information.
Webtracer	N/A	It determines the Owner of the website, the location of the server, the sender of an email, and other evidence of internet identity.
Spector CNE	Windows and Linux	It records everything the employees do online, including IM (Instant messengers), chats, sending and receiving e-mails, visiting websites, launching applications, downloading files, and typing keys.
dtSearch	Windows	It searches terabytes of text across a desktop, network, Internet or intranet sites. It consists of special forensic search options. It supports public and secure, static and dynamic web data.

Fig.1.12: Network Forensic Analysis Properitory Tools
(Source: https://www.researchgate.net/figure/Proprietary-tools-for-Network-Forensics_tbl6_315726562)

1.2. The Research Problem

Not adhering to digital forensics can lead to organizations loosing continuity and the availability of core services. Vulnerabilities can multiply in the networks making it vulnerable thus compromising security issues. This can lead to the collapse of all communication mechanisms because of network nodes failures and the whole setup can be compromised by the intruding hacker.

1.3. The Purpose of the Study

Penetration of brings many challenges associated with security and data breaches. Cyber attacker's come up with extremely complicated means of infiltrating networks' security. Hence the expert administrator monitoring the network activities should be fully equipped to identify the security vulnerabilities and can capture cyber related offenders. The main purpose of this research contribution is to come up with a standard and innovative framework which can help in analysis of concepts of networking forensic and the methodologies and associated tools which are to be used for network forensics. This is backed by detailed and exhaustive literature review.

1.4. Objectives

1. Detailed insight into the concept of network forensic investigation on conceptualized network.
2. Analyzing various methodologies-tools which can be used for network forensics.
3. Analyzing data using "obtain information, strategize, collect evidence, analyze and report" (OSCAR) methodology on the conceived network.
4. Designing of an innovative OSCAR Framework

1.5. The Research Questions

1. What are the concept of network forensic investigation and how are they analyzed on the network?
2. What are the best methodologies-tools?
3. How to apply methodology of obtaining information, strategizing, collecting evidence, analyzing and reporting data on a conceived network architecture design?
4. How to design an innovative OSCAR Framework?

1.6. Contribution to Knowledge (Academic)

Contribution of this research relates to providing an analysis which is based on the study of relevant literature. The knowledge helps the researchers to investigate processes which help in cyber-forensics by obtaining, analyzing, evaluating, categorizing, and identifying crucial evidences.

1.7. Statement of Significance (Practical Contribution)

The practical contribution relates to making it possible to apprehend a cyber-criminal. It is achieved through using effective forensic network investigation methodologies. The researched upon methodology will provide forensic specialist with essential tools that will determine the approach for obtaining, strategizing, collecting, analyzing and reporting the findings of a network forensics investigation. It will also identify the network forensic tools for forensics investigation processes.

II. Literature Review

Here, literature review and the gaps are identified in the light of the reviewed publications.

2.1. Literature Review

Nature and type of crime calls for affected victims help [1]. In some cases, Committed computer crime is not the only source of revenue losses but may make the affected organization inoperable. So, it is important to have a way of doing it the necessary research and auditing for the study once and for all associated computer criminals. Kumongo of cyber-criminal investigation, method referred to as network forensics. Network forensics is a process that involves computer research, analysis to find important information that helps in arrest of cybercriminals [2].

It is important to be careful that any provided network is connected to the internet accustomed to various cyber-attack. Attacks are common designed in way that they exploit weaknesses of anything in network. The investigator is therefore assigned a task the burden of coming up with strategies that are important to do network forensic process for diagnosis network entry conditions [3].

Idea of protecting trade secrets has been adopted with new significance as information with an independent economy or competitive value [5]. One of the many trade problems secrets produce important and sensitive information such as the result of increased information and communication space the exchange is a widespread response to government in the use of forcing steel with strong obstacles results, as in the case of Terry [6]. This is an in-depth study referenced at [7], [8], [9], [10], [11].

Almulhem added that network forensics are highly correlated with the security model. The network (digital forensics) emphasizes the design and implementation of methods, tools, and concepts aimed at improving forensic investigation process [12]. Kilpatrick et al. proposes the implementation of SCADA (monitoring control and constructive data acquisition programs an important infrastructure for network forensics [13]. It also plays a key role in implementation of machine-to-machine safety methods networks [14].

It is important to review several cases subjects where the concept has been used sufficiently. In particular, Kurniawan and Riadi [15] were able to test again use the unique framework from which it was obtained use the concept of network forensics analysis once point to the behavior of the infamous Cerber Ransomware. As noted by Messier and Bensefia and Ghoualmi, most fire protection systems have the ability to use software power in UNIX/Windows platforms [16] [17].

It is noteworthy that most Honeypot services are secretive [18]. Honey jars are considered important components which help to improve organizational safety [19]. Network forensics is different from access by the evidence gathered must be accepted in court as well hence satisfying technical/legal concerns [20].

While the acquisition of intervention helps in improving computer network security, network forensics are key corresponding to the need to identify related evidence security breach. Network forensics is helpful resolving issues related to online terrorism, child pornography, drugs, national security, cybercrime, and corporate intelligence, among others [21] [22] [23].

2.2. Literatures Gaps

There is a need to develop some tools that can parse varied network protocols in place or embedded in different networks. As most of the information carried on the networks is volatile, it is essential that it should be preserved in order to expedite the forensic process.

III. RESEARCH METHODOLOGY AND FRAMEWORK

This section deals with the research methodology and conceptualized framework of this research used by the researcher.

3.1. Research Methodology

After going through the detailed literature review, the research selected the base paper [24]. This research contribution is based on following a comprehensive process which will be executed by using OSCAR (obtain, strategize, collect, analyze and report) principles.

Fig. 3.1: OSCAR

The research will follow the following steps.

- Network Conceptualization
- Identification of Malicious Activities
- Identifying the Source of Activity
- Application of Tools
- Decision Making based on Data Analysis

The designed network will be analysed using the following tools.

- ***Wireshark***

Wireshark packet analyser: network troubleshooting, analysis, software and communications protocol development.

- ***Tshark***

TShark network protocol analyser: Captures packet data from a live network.

- ***Dumpcap***

Dumpcap is network traffic dump tool: Captures packet data from a live network & writes them to file.

- ***Network Forensic Analysis Tools (NFATs)***

NFATs help administrators monitor their environment for anomalous traffic, perform forensic analysis and get a clear picture of their environment.

The focus of this research contribution is cantered towards the need to find and look at the malware affecting network hosts. The analysis of the network behaviour can come up with infections, exploited channel, and the payload with ransomware. As we are focussed on the network forensics, hence, in order to move forward, the forensic mechanisms need to be looked at which fall under the following categories.

- Network Security Forensic Mechanisms
  - Embedding the Firewall forensics in the network.
- Honeypot Forensics
  - Network system designed is such to allure by depicting information as critical and sensitive.

A typical firewall forensics scenario is shown in the below figure. The firewall has to detect and mitigate the threat from the attacker using the IPs as identifiers.

A typical honeypot deployment is shown in the below figure. The honeypot is placed between the internet network and the firewall and the attacker instead of breaking the firewall is allured towards the honeypot considering it as the main network server. This saves the other network servers from being attacked and compromised.

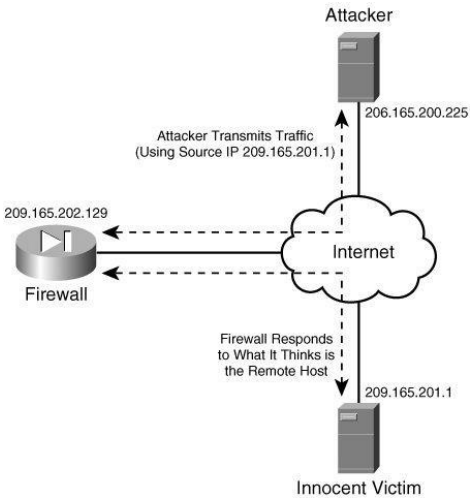

Fig.3.2: Firewall Forensics

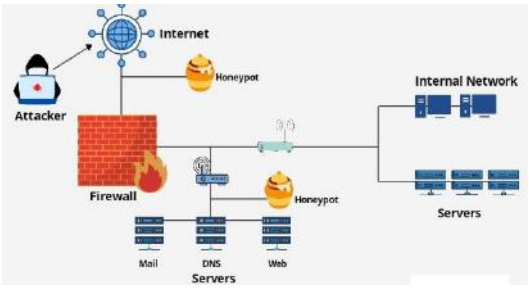

Fig.3.3: Honeypot Forensics (Placement in Network)

Exploring and investigating of network forensics will be done in this research work with identifying a malicious activity, evidence collections and its preservation. This will be followed by evidence reporting and making the decision based on the analysis. All the processes of network forensics will follow the following procedure of OSCAR principle as explained previously in this section. The evidence will be retrieved from the selected network and computing devices. The selected devices are shown in the table below.

Table 3.1: System Designed

S/NO	DESCRIPTION	TYPE OF FORENSICS
1	Application	Internet Browser, E-Mail, Registry, Software, Virus, Worm, Trojans and slack, erased, swap files
2	Deployed System	UNIX, Windows, Log and Audit System
3	Hardware	Personal Computer, Personal Digital Assistant, Printer, Router, Switches, Firewall, Intrusion Detection System
4	Processing	Type: Victim (Client), intermediate, and attacker (Hacker or the Threat Actor)

This will be followed by source of evidence, value, effort, volatility and priority of web proxy cache, firewall logging data and the address resolution protocol tables used for storing the information discovered. Address resolution protocol cache helps the attackers hide behind the fake IP address. Operations systems audit trail, system event logs, applications events logs, alerts logs, recovered data, and swap files of attacker/victim side will be analysed in addition to traffic data packets, firewall log, intrusion detection system log, router log, and access control log of the intermediate devices.

Below innovative conceptualized model is designed by the researcher.

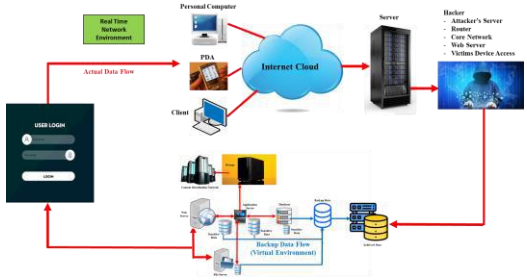

Fig.3.4: Conceptualized Model

In the above conceptualized network design, honeypot devices (sensitive data) is placed in a network for making it possible to carry out a detailed analysis of network activities and the logs being carried throughout the honeypot devices. Hence they are in a good position to help in finding out attacker's logs and activities. The attacker will attack the network and with honeypot devices strategically placed in the network, his attack activities will be logged.

IV. DATA ANALYSIS

The conceptualized network design is discussed in detail in the section after using various tools to capture the attacker's activities.

4.1. OSCAR Framework Design

OSCAR Design Steps are followed in this phase. Therese are summarized below for clarity.

- Obtaining Information
  - Information regarding the incident
  - Environment
  - Time/Date
  - Discovery
  - Systems involved
  - People involved
  - Devices involved
  - Actions executed after the discovery
  - Discussions record
  - Legal issues
  - Business model
  - Available resources
  - Communication system
  - Network topology
  - Procedures
  - Processes
  - Incidence response management

- Strategizing
  - Investigation goal
  - Investigation time frame
  - Investigation plan
  - Value/Cost of obtaining evidence
  - Evidence acquiring mechanisms
  - Proof acquisition
  - Source
  - Effort required
  - Volatility
  - Expected value
  - Evidence prioritization
  - Data retention policy
  - Access policy
  - Configurations policy
- Collecting Evidence
  - Obtaining evidence
  - Using reliable and reputable tools
  - Documenting
  - Capturing
  - Store/Transport
  - Security of information
- Analyzing Evidence
  - System files log
  - Resources log
  - Date, time and source of incident
  - Investigating officer profile
  - Methods used to acquire evidence
  - Devices accessed
  - Custody chain
  - Data/network traffic packets repository
  - Application of forensic tools
  - Storing/transport of log data
- Reporting
  - Technical information
  - Defensible details
  - Results

Based on the above identified parameters, a framework is established by the researcher as shown below.

Fig.4.1: Designed Framework

4.2. Selected Tools

The following tools were selected for the analysis of the conceptualized network along with their functionalities used.

- Wireshark
  - For capturing, filtering and analyzing network traffic
- Tshark
  - Data network protocol analyzer used for capturing and reading traffic data from live data network from packetized data files.
- Dumpcap
  - Network traffic analysis is done through the use of this tool which is designed to capture the data packets.
- Network Forensic Analysis Tools
  - Used for tracking networks and gathering malicious traffic information

4.3. Data Analysis

The conceptualized network is implemented using the tools outlined in the previous section. The below table outlines the setup details.

Table 4.1: Design Setup

S/NO	ATTRIBUTE	DETAILS
1	Source of Evidence	Web Proxy Cache, Firewall logs, Address Resolution Protocol Tables
2	Affiliation	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)
3	Device/Tool	
		Laptop-1 (Usage: Creating test network & host proxies)
		IPad (Usage: Test device connected to test network)
		Proxy (Usage: Capture/save live network traffic)
		Wireshark (Usage: Capture/save live network traffic)
		Burp Suite (Usage: Capture live network traffic)
		Laptop-2 (Usage: Network forensics of iOS apps)
		Network Miner (Usage: Analyze network traffic)

During the process of collection of network-based evidence, special care was done pertaining to the collection, storage, content, privacy, confiscation and admissibility. Test network was designed on laptop-1 in addition to the host proxies. The testing was done using IPad as the testing device. The proxy was used to capture the live network traffic. Capturing and saving of the network traffic was achieved through the usage of Wireshark tool and the burp suite. Burp

Suite is used to set up a proxy which allows to test web architecture by routing web traffic through it. Network forensics were collected from the applications on Laptop-2 while the analysis of the network traffic was done using the network miner. The below figures show the stepwise processes.

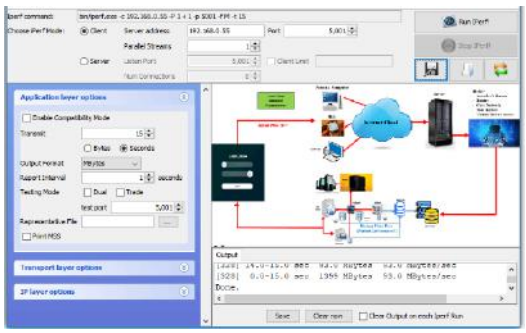

Fig.4.2: Test Network Design

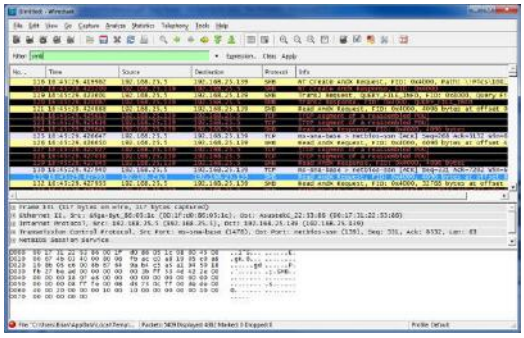

Fig.4.3: Capturing Traffic using Wireshark Tool

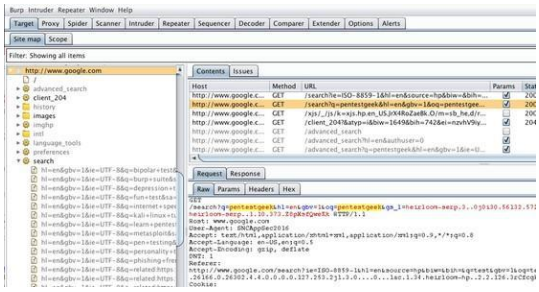

Fig.4.4: Penetration Testing with Burp Suite & Wireshark (Uncovering Vulnerabilities)

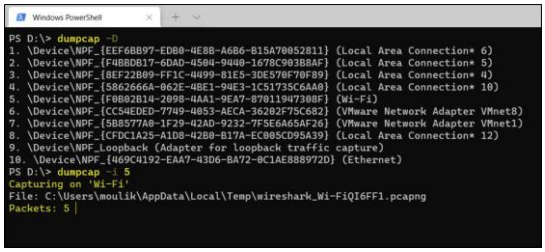

Fig.4.5: Dumpcap to Capture Data Packets

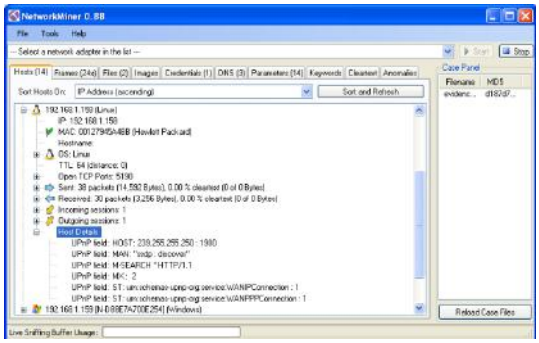

Fig.4.6: Network Miner for Analysis of Network Traffic

V. CONCLUSIONS AND FUTURE RECOMMENDATIONS

The section looks at the conclusions of the research and the future recommendations.

5.1. Conclusions

Following are the outcomes and conclusions of this research contribution.

- Detailed analysis of network forensic investigation on a conceptualized network.
- Methodologies/tools used were analysed and studied in depth.
- Analysed the data using "obtain information, strategize, collect evidence, analysing and reporting (OSCAR) methodologies on the conceived network.
- Designed an innovative OSCAR Framework which can be adopted in any network forensic analysis implementations.
- It was found that Network forensic science is extremely essential important and it helps a cyber-forensics investigator to;
  - O - Obtain
  - A - Analyse
  - E - Evaluate
  - C - Categorize
  - I - Identify crucial evidences
- Helps in apprehending cyber-criminals
- Network forensics investigator should adopt and utilize efficient forensic network investigation methodologies
- OSCAR methodology equips forensic investigator with critical tools and guidelines to develop;
  - Approach
  - Methods
  - Strategies
  - Strategizing
  - Collecting
  - Analysing
  - Report of findings
- Network forensics expert should use top of the line tools.

5.2. Future Recommendations

Following are the recommendations for future research work.

- Development tool kits which can analyse varied network protocols.
- Preserve and document data selectively in advance to speed up the forensic process.

REFERENCES

[1] M. Matsalu et al., “Digitaalse ekspertiisi t¨o¨oj˜ou p¨adevuse arendamine eestikaitseliidu n¨aitel,” 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 J´unior, L. J. Garc´ıa 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] Yousif, Dr. T., Dizay, Dr. S. K., & Anwer, Dr. R. N. A. (2021). Chronic Rhinosinusitis and Its Impact on Pregnancy. In International Journal of Chemistry, Mathematics and Physics (Vol. 5, Issue 4, pp. 1–6). AI Publications. https://doi.org/10.22161/ijcmp.5.4.1

[10] 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.

[11] 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.

[12] 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.

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

[14] 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.

[15] 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.

[16] 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.

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

[18] 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.

[19] S. Krasser, G. Conti, J. Grizzard, J. Gribschaw, and H. Owen, “Realtime 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.

[20] 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.

[21] J. Llano Tejera, “Herramientas forenses para la respuesta a incidents inform´aticos,” Ph.D. dissertation, Universidad Central” Marta Abreu” de Las Villas, 2014.

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

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

[24] Wazalwar, A. (2021). Growth Techniques of Ferroelectric Single Crystals. In International Journal of Chemistry, Mathematics and Physics (Vol. 5, Issue 3, pp. 01–03). AI Publications. https://doi.org/10.22161/ijcmp.5.3.1

[25] 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.

[26] Qureshi, Sirajuddin & Tunio, Saima & Akhtar, Faheem & Wajahat, Ahsan & Nazir, Ahsan. (2021). Network Forensics: A Comprehensive Review of Tools and Techniques. International Journal of Advanced Computer Science and Applications. 12. 2021. 10.14569/IJACSA.2021.01205103.

[27] Oracle (2019). Analyzing Network Traffic with TShark and Wireshark. Oracle Administering TCP/IP Networks, IPMP, and IP Tunnels in Oracle® Solaris 11.3