BOOK CHAPTER | What's in that Packet

Packet Analysis for Network Forensics

Asiedu Francis
Digital Forensics and Cyber Security Graduate Programme
Department of Information Systems & Innovations
Ghana Institute of Management & Public Administration
Greenhill, Accra, Ghana
E-mail: faseidu22@gmail.com
Phone: +233249398982

ABSTRACT

If the packet characteristics acquired are sufficiently detailed, packet analysis is a common forensic approach in network forensics that can replay the whole network traffic for a specified time period. This can be used to find evidence of illicit online activity such as data breaches, unauthorized website access, malware infection, and infiltration attempts, as well as to reproduce image files, documents, email attachments, and other material sent over the network. This paper covers a comprehensive assessment of the usage of packet analysis, including deep packet inspection, in network forensics, as well as a discussion of AI-powered packet analysis methodologies with sophisticated network traffic classification and pattern recognition.

Keywords: Cybersecurity; Network Security; Traffic Analysis; Deep Inspection; Intrusion Detection; Network Forensics

BOOK Chapter | Research Nexus in IT, Law, Cyber Security & Forensics. Open Access. Distributed Free

Citation: Asiedu Francis (2022): Packet Analysis for Network Forensics
SMART-IEEE-Creative Research Publications Book Chapter Series on Research Nexus in IT, Law, Cyber Security & Forensics.
Pp 91-98 www.isteams.net/ITlawbookchapter2022. dx.doi.org/10.22624/AIMS/CRP-BK3-P15

1. INTRODUCTION

It is no longer possible to evaluate commercial and government activities without the Internet. Many businesses and government agencies can now offer their services online, making them more convenient for users thanks to the increasing rise of the Internet and its technologies. Cyberattacks on people and businesses, however, are growing more widespread as a result of this increase. This includes collecting valuable data from stolen networks or shutting down victims' servers. Most applications, particularly those considered critical (e.g., Internet Banking), are inadmissible if their assets are compromised or if they are forced off for an extended length of time.

Early detection and mitigation measures are needed not only when a system is attacked but also to minimize damage and restore normal operations as rapidly as possible. To achieve this early detection, advanced network tools and analysis, in conjunction with qualified experts in the cybersecurity field, can be deployed. Rodriguez and colleagues (2017). One approach to investigating network assaults is Deep Packet Inspection (DPI). This method requires a thorough examination of the fields contained in packets that transit across the network under inquiry. It allows for the detection of network traffic anomalies as well as other critical information used in incident response, such as the IP address involved, the nature, timing, and length of the assault, as well as other information that assists security specialists in incident mitigation. Network forensics is used to find and collect evidence against attacks that could be linked to a crime, such as the theft of confidential information. Although this is not always the case, gathering and reviewing evidence as if it were going to be used in court is crucial. It's vital to observe Chain of Custody (CoC) regulations while dealing with incident response and cyberattack mitigation.

There are still certain limitations, such as the requirement for a specific technique to convert pcap data to csv so that it may be indexed and studied. Another current drawback is the lack of a data pipeline, which prevents packet payload processing in real time. Because not all network data is admissible in court, the types of digital evidence that is acceptable are thoroughly explained. In view of their potential use in network forensics, the features of both hardware appliances and packet analyzer software are examined.

1.2 The Study's Background

Data transmission protocols, or strategies for recognizing and establishing connections, as well as data transmission formatting requirements and norms, make communication between network devices easier. Network data can be analyzed and network traffic can be separated by type using purpose-built software. (Sikos, 2020a). Packet analyzers designed exclusively for packet analysis are known as packet analyzers (packet sniffers, sometimes network analyzers). These software programs intercept and log network traffic passing over a digital network or a segment of a network via packet capture. Decoding the raw data and visually analyzing the information by showing many fields can then be done on the captured packets (Rodrigues et al., 2017). Setting a capable wired network interface controller (NIC) or wireless network interface controller (WNIC) into promiscuous mode allows all incoming network traffic to be sent to the central processing unit (CPU), rather than just those frames the controller is specifically designed to accept.

Examining network packets helps with the collection and reporting of network data as well as the debugging of client-server communications. Network packet capture files contain a wealth of data about online user activity that can be useful in network forensics, such as visited websites and time spent on them, successful and unsuccessful login attempts, credentials, illicit file downloads, intellectual property misappropriation, and so on. Packet files can include a wide range of data, and they can also be retrieved in different formats, such as individual frames and client-server interactions. Packet streams, sessions, and flows In network forensics, packet analysis can be used to collect evidence for digital activity investigations, detect hazardous network traffic and behavior, such as intrusion attempts and network misuse, and identify man-in-the-middle attacks and malware such as ransomware (Ari et al., 2019).

2. RELATED LITERATURE

A brief survey of packet analysis fundamentals in the literature illustrates why. A packet network is made up of a web of wires that connects "routers," which are specialized computers. A digital source must first break down its stream of data into small bits before sending it via a packet network ("packets"). The packets are then forwarded to the nearest router one by one. This router controls how a packet is sent to its intended destination. As a result, each data packet may be routed through a different set of routers and lines to reach its destination. This is beneficial because it distributes traffic around the network and enables more efficient network resource utilization.

In addition, the average packet travel time is lowered. However, this efficiency comes at a price. The network may deliver packets out of order, drop packets, or deliver the same packet many times if the load becomes too large. These variables cause mayhem with real-time data streams. When audio packets go missing, when audio is sent out of order, the quality suffers significantly. Because Picture Tel's encoding only transmits updates, missing packets are possibly worse with video. One failed packet invalidates all following updates. (Sikos, 2020a). (Rodrigues and colleagues, 2017).

3. PACKET PROCESSING AND NETWORK PACKETS

Using purpose-built network carvers or packet analyzers that support file export from packet capture, files traversing a network can be reconstructed from network packet streams (network carving) (Sikos, 2020b). Packet sniffing is a technique for intercepting data packets. Specifically, packets traveling over a communication network as well as re-transmitted packets with modified TCP properties (Pilli et al., 2010). This technique can be used to reconstruct data transferred over a network or even as an anti-forensic technique.

Deep packet inspection (DPI)

Deep packet inspection (DPI) is a type of packet analysis that looks at the content of the packet as well as the header data. DPI can be used to detect data streams and identify non-business traffic that has to be filtered or controlled in businesses, such as social media use.
Artificial intelligence-assisted packet analysis: Formal knowledge representation in the form of ontologies is used in network forensics to automate the processing of network packet sequences (Sikos, 2020a). Ontologies that are purpose-built, such as the Ontology for Packet-Centric Networks, when identifying malicious traffic using Snort, (Sikos, 2020a) used machine learning and a plugin to lower the likelihood of false positives.

By decoding packet data and identifying network packets, this plugin optimizes and offloads packet processing. Hardware acceleration and offloading for network packet processing is provided by application-specific integrated circuits (ASICs), field programmable gate arrays (FPGAs), and graphics processing units (GPUs). Most IPv4 and IPv6 traffic, as well as IPsec VPN encryption, CAPWAP communication, and multicast traffic, can be offloaded via the FortiASIC NP6 from FortiGate. Rodriguez and colleagues (2017)

The Charles Web Debugging Proxy.

Karl Von created Web Debugging proxy44 is an HTTP proxy, HTTP monitor and reverse proxy that visualizes all HTTP and SSL/HTTPS communication between a PC and the internet.

Eric Lawrence created Fidddler45, a free web debugging proxy that can log HTTP. The network data can be filtered to hide sessions, highlight important traffic, bookmark breakpoints and so on. A session inspector widget in the software can display the contents of a recorded web session including status, headers, caching, cookies URLS, protocols, compression types, redirects and so on. WebScarab52 is an integrated penetration testing tool for online applications that is simple to use. It is capable of packet analysis. These, however are limited in scope. Using the HTTP and HTTPS technologies to communicate

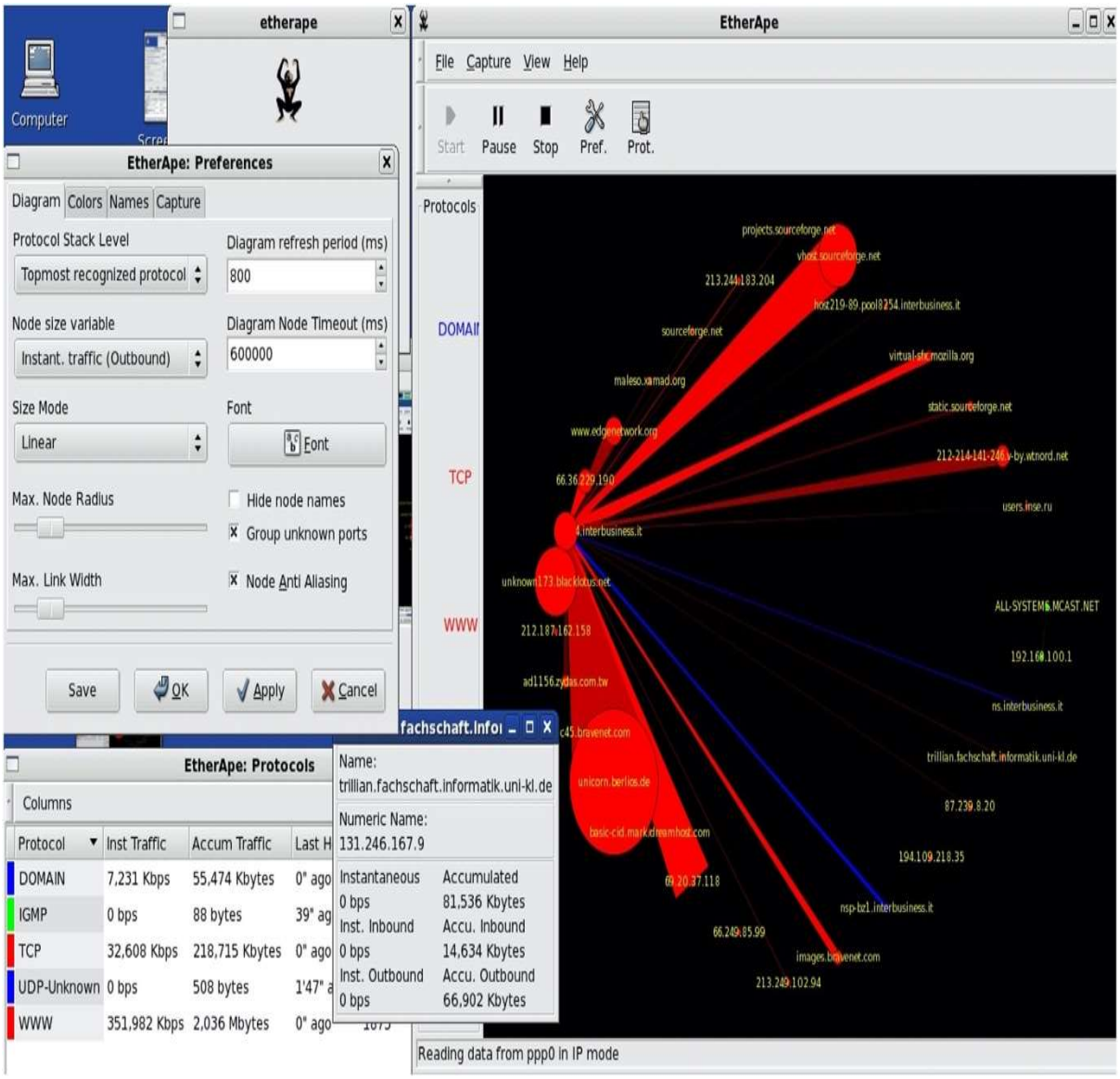

Fig 1: The Charles Web Debugging proxy.
Source : L.F. Sikos / Forensic Science International: Digital Investigation 32 (2020) 200892.(Sikos, 2020a)

Data Packets As Digital Evidence

Network forensics is primarily reliant on network packet capture, analysis, and backtracking (Asrodia, Pallavi, and Patel, 2012). Network packets are live network evidence sources that are integrated with data from remote network services. Depending on the online content, network packets have a defined, non-zero acquisition window within which evidence can be inspected or obtained. On the one hand, others contend that using packets as evidence can be problematic if they are falsified (Rodrigues et al., 2017). The ultimate forensic evidence is network packets, which can be used to enhance firewall logs and network monitoring tools. 2012 (Asrodia, Pallavi, and Patel)

Packet capture files can be used to extract potential forensic evidence from network data using the Highly Extensible Network Packet Analysis (HENPA) framework (Steinberger & Horn, 2022). Both directly and indirectly, data extracted from network packets might be used as evidence. For example, some of the information in the packets (Sikos, 2020a) (Pilli et al., 2010) The sender and receiver IP addresses, port numbers, and other metadata, as well as the transferred data, can be used as direct evidence (Asrodia, Pallavi, and Patel, 2012).

Packet Analyzer Software:

There are purpose-built packet analyzer and network tools that provide features for packet capture and analysis among the packet analyzer software packages(Asrodia, Pallavi and Patel, 2012). Intrusion detection software, proxies, vulnerability assessment tools, network scanners and network monitoring tools are example of network tools. Gerald Combs created Ethereal a free and open-source packet analyzer, in 1998. (Steinberger & Horn, 2022)Wireshark was renamed in 2006. Wireshark has grown in popularity as one of the most popular graphical packet capture and protocol analysis tools, (Sikos, 2020a)a user-friendly interface for packet analysing.

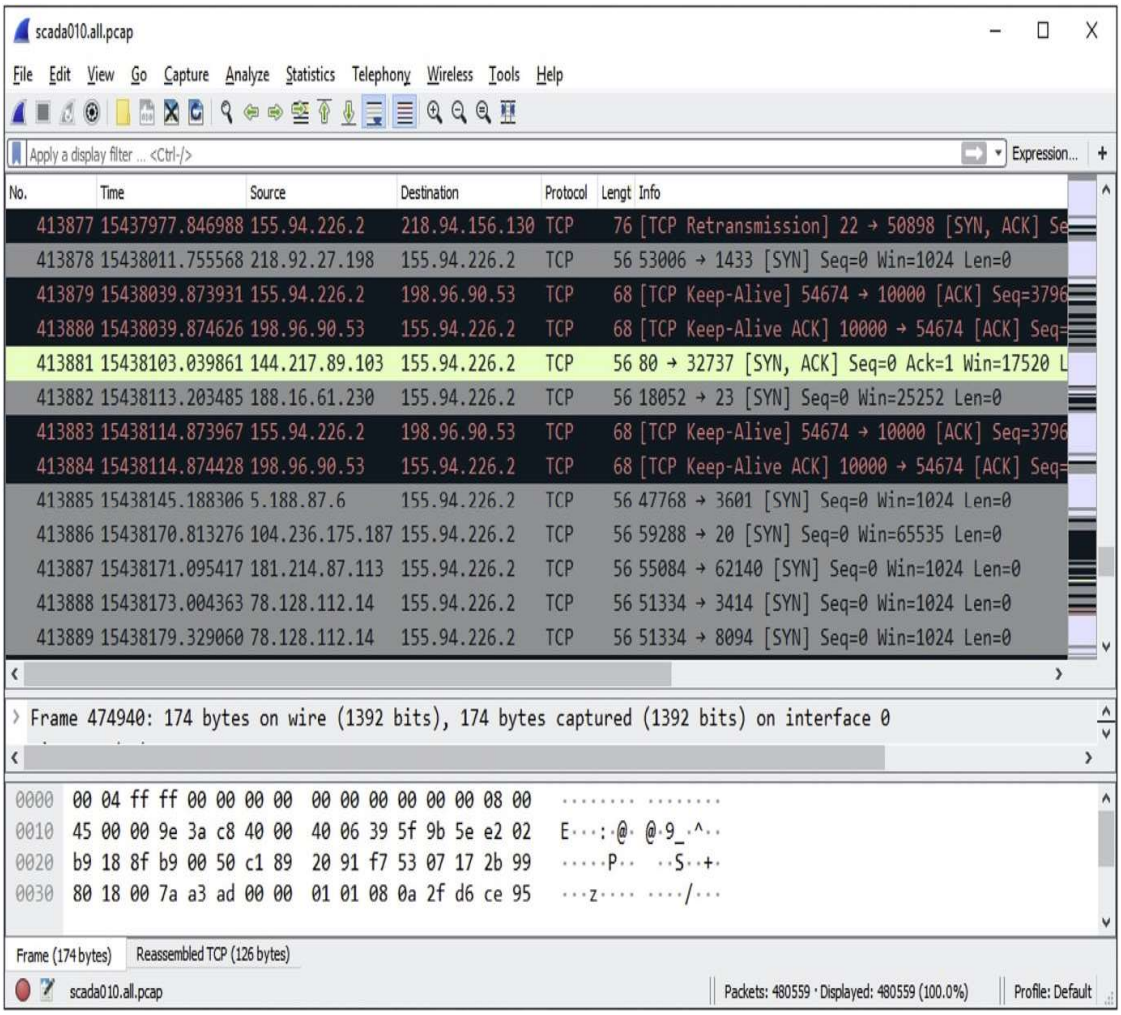

Fig 2: A Typical Packet Analyzer Interface
Source: L.F. Sikos / Forensic Science International: Digital Investigation 32 (2020) 200892

This GUI contains a customized packet browser that may display up to three windows at once, including a packet list, packet information and packet bytes for the presently select packet.(Sikos, 2020b)

4. CONCLUSION

In network forensics, analyzing network packets is critical for gathering data and serving evidence admissible in court, as well as gaining a comprehensive picture of online user actions at a certain point in time. Although some may doubt the accuracy of information retrieved or reconstituted from packet data, network packets supplement other data sources such as corporate firewall logs or CCTV footage, and in many cases, they are the only source of information about what happened during an online activity and who was involved. Because network forensics makes use of packet analysis (Steinberger & Horn, 2022), (Sikos, 2020a).

5. IMPLICATIONS OF CYBER SAFETY IN AFRICA

The position in Africa regarding cybercrime and electronic evidence legislation is not adequate, since only about 20% of countries have the essential legal framework in place. On the plus side, many states are undergoing changes, which is good. Data protection laws are rapidly being introduced in African countries, typically in conjunction with cybercrime legislation. Individual rights are further protected as a result of this. Not only are Mauritius, Morocco, and Senegal Parties to the Convention or have been invited to join the Budapest Convention on Cyber Crime, but have also requested membership in the Council of Europe's Data Protection Convention 108. 2014 African Union Convention on Cyber Security and Personal Data Protection includes an important chapter on personal data protection. The greatest hindrance to an efficient criminal justice response to cybercrime and other offences utilizing electronic evidence, not only in Africa but in other nations throughout the world, is limited capacity of law enforcement, prosecutors, and the court.

6. RECOMMENDATION FOR POLICY AND PRACTICES

Cyber-attack can be done through an IP intersect on any device and any location. ISP providers play a vital part in cybercrime investigation, there would need to be a unique standardizing policy in terms of IP address distribution and domain registrations. as well as approved legal operation standardisation between countries and ISP providers. On the part of African countries, there is a need to develop a realistic risk plan that is accompanied by appropriate laws and cybersecurity policies, as well as a good recovery plan that is responsible for monitoring and tracking current cyber theft trends. How to distribute IP addresses and register domains according to the Internet Corporation for Assigned Names and Numbers. Policy can be made through government agency responsible cybersecurity. example .GH will be registered with the majority of Ghanaian businesses in order for the country to become more well-known in the world of domain registration and enable the track of IP address and domain registration easily.

7. FUTURE PROJECT DIRECTION

Packet analysis of Internet of Things (IoT) networks is becoming increasingly important in the battle against cybercrime and mass surveillance. For example, IoT packet analysis can help detect distributed denial-of-service (DDoS) assaults and the botnet development process. As cloud-based services become more widespread, there is a greater demand for packet capturing and analysis in cloud environments than in network segment packet capture files. The government and financial sectors; cyber defense and security applications; cloud-managed services; VoIP services; and other industries use cloud storage and cloud computing services, which come with additional problems beyond the source and destination IPs, protocols, and port numbers. Amazon, for example, has offered VPC traffic mirroring, which allows for large-scale acquisition and inspection of AWS network data. This research will continue to improve the architecture to enable real-time payload analysis, including automatic data translation and a pipeline between Honeynet and Logstash for indexing data as it is created. Kafka, Hadoop, Solr, and other big data technologies are expected to assist with this. In the same way, establishing various depths of packet inspection devices and focusing analysis on the lower layers of the TCP/IP model may offer fascinating information that may be utilized to compare and correlate the results reported here and uncover more problematic trends.

REFERENCES

1. Asrodia, Pallavi and Patel, H. (2012). Analysis of Various Packet Sniffing Tools for Network Monitoring and Analysis. *International Journal of Electrical, Electronics and Computer Engineering*, *1*(1), 55–58.
2. Cho, C. Y., Lee, S. Y., Tan, C. P., & Tan, Y. T. (2006). Network forensics on packet fingerprints. *IFIP International Federation for Information Processing*, *201*, 401–412. https://doi.org/10.1007/0-387-33406-8_34
3. Devi, A. (2017). *Cyber Crime and Cyber Security*. 160–171. https://doi.org/10.4018/978-1-5225-2154-9.ch011
4. Pilli, E. S., Joshi, R. C., & Niyogi, R. (2010). A Generic Framework for Network Forensics. *International Journal of Computer Applications*, *1*(11), 1–6. https://doi.org/10.5120/251-408
5. Sikos, L. F. (2020a). Packet analysis for network forensics: A comprehensive survey. *Forensic Science International: Digital Investigation*, *32*, 200892. https://doi.org/10.1016/j.fsidi.2019.200892
6. 6.Sikos, L. F. (2020b). Packet analysis for network forensics: A comprehensive survey. *Forensic Science International: Digital Investigation*, *32*. https://doi.org/10.1016/j.fsidi.2019.200892
7. 7.Steinberger, M., & Horn, M. (2022). Robust filtered Smith predictors for networked control systems with packet-based data transmission. *Journal of Process Control*, *111*, 86–96. https://doi.org/10.1016/j.jprocont.2022.01.008
8. 8.Asrodia, Pallavi and Patel, H. (2012). Analysis of Various Packet Sniffing Tools for Network Monitoring and Analysis. *International Journal of Electrical, Electronics and Computer Engineering*, *1*(1), 55–58.
9. 9.Cho, C. Y., Lee, S. Y., Tan, C. P., & Tan, Y. T. (2006). Network forensics on packet fingerprints. *IFIP International Federation for Information Processing*, *201*, 401–412. https://doi.org/10.1007/0-387-33406-8_34
10. 10.Devi, A. (2017). *Cyber Crime and Cyber Security*. 160–171. https://doi.org/10.4018/978-1-5225-2154-9.ch011
11. 11.Pilli, E. S., Joshi, R. C., & Niyogi, R. (2010). A Generic Framework for Network Forensics. *International Journal of Computer Applications*, *1*(11), 1–6. https://doi.org/10.5120/251-408
12. 12.Sikos, L. F. (2020a). Packet analysis for network forensics: A comprehensive survey. *Forensic Science International: Digital Investigation*, *32*, 200892. https://doi.org/10.1016/j.fsidi.2019.200892
13. 13.Sikos, L. F. (2020b). Packet analysis for network forensics: A comprehensive survey. *Forensic Science International: Digital Investigation*, *32*. https://doi.org/10.1016/j.fsidi.2019.200892
14. 14.Steinberger, M., & Horn, M. (2022). Robust filtered Smith predictors for networked control systems with packet-based data transmission. *Journal of Process Control*, *111*, 86–96. https://doi.org/10.1016/j.jprocont.2022.01.008