

Packet Analysis for Cyber Attack Detection

**Dr. Harish Joshi^{1*}, Ashok Bawge², Uzma Kausar³, Shaik Riyan⁴,
Prathik Kulkarni⁵, Raheem Ali⁶**

¹HOD & Associate Professor, Guru Nanak Dev Engineering College, Bidar-585403, India

^{2,3}Assistant Professor, Guru Nanak Dev Engineering College, Bidar-585403, India

^{4,5,6}Student, Guru Nanak Dev Engineering College, Bidar-585403, India

***Corresponding Author**

E-Mail Id:- hodicb@gndecb.ac.in

ABSTRACT

Real-time network data collection is crucial for identifying security risks such as outdated software and open ports. Network forensics uses packet analysis to monitor traffic, detect threats, trace intrusions, and recover digital content. This study evaluates the integrity of home networks using Wireshark, capturing traffic across devices. Wireshark provides both basic statistics and advanced tools for analyzing network performance.

Keywords:- Wireshark, Packet Analysis, TCP, Network Traffic, Network Monitoring

INTRODUCTION

With the rise of internet accessibility, digital communication depends heavily on packet-based data transfer. These packets carry both data and control information across networks.

However, attackers can exploit this system using packet sniffers to intercept sensitive data like passwords. Sniffers operate in two modes: active (detectable) and passive (undetectable), with tools like Wireshark falling under the latter. Packet capture (pcap) tools collect data across multiple network layers, aiding in protocol analysis and forensic investigations.

Key Aspects:

- Capturing and retaining network packets
- Traffic analysis using Wireshark
- Extracting information for security assessment.

BACKGROUND

Protocols govern how devices communicate over networks. Packet capture tools log raw data for analysis, helping identify traffic types and security threats. As packets travel between devices, they pass through multiple intermediaries, with NICs using physical addresses for delivery. Systems in promiscuous mode can monitor all traffic within their network segment, revealing detailed network activity.

DATA DESCRIPTION

A shared access point connected five devices two laptops and three mobile phones to the network. The access point was assigned a static IP address, understanding of the system's configuration.



Figure 1: Network Topology.

Fig.1:- Protocol Types.

Figure 1 categorizes various network protocols, illustrating their roles in data transmission and communication.

Domain Name System (DNS)

The Domain Name System (DNS) facilitates network connectivity by identifying machines that are reachable via a local network or the Internet. Each domain name is linked to a

corresponding IP address, enabling name resolution that directs queries to the appropriate reachable host.

Figure 3 illustrates the connection between hosts, detailing packet timing, direction, port numbers, and comments associated with each captured interaction.

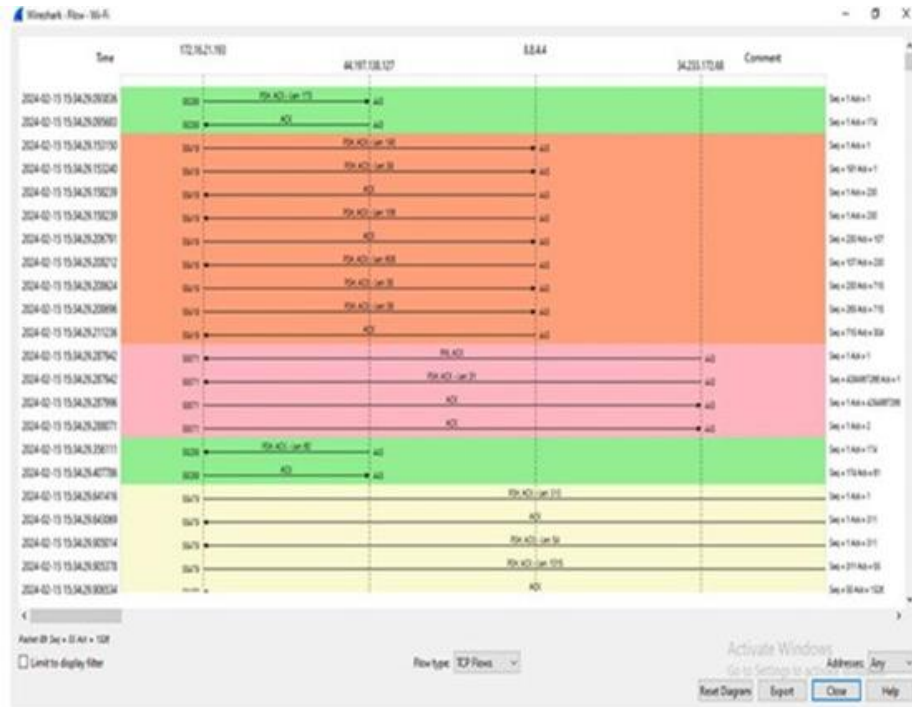


Fig.2:-Flow Graph

A range of filters can be applied within the Flow Graph window, including ICMP (Internet Control Message Protocol) flows, ICMPv6 flows, UIM flows, and TCP flows. These controls enhance packet analysis by allowing users to refine traffic data based on specific protocols.

Flow graphs are instrumental in identifying port numbers and IP addresses, enabling the detection of unusual traffic patterns and potential network anomalies.

An example of a capture filter can be seen in Figure 4.



Fig.3:-Capture Filters

Figure 5 illustrates the process of data filtering, demonstrating how specific parameters can be applied to refine captured network traffic.

By using filtering techniques, users can isolate relevant packet data, improving efficiency in network analysis and troubleshooting.

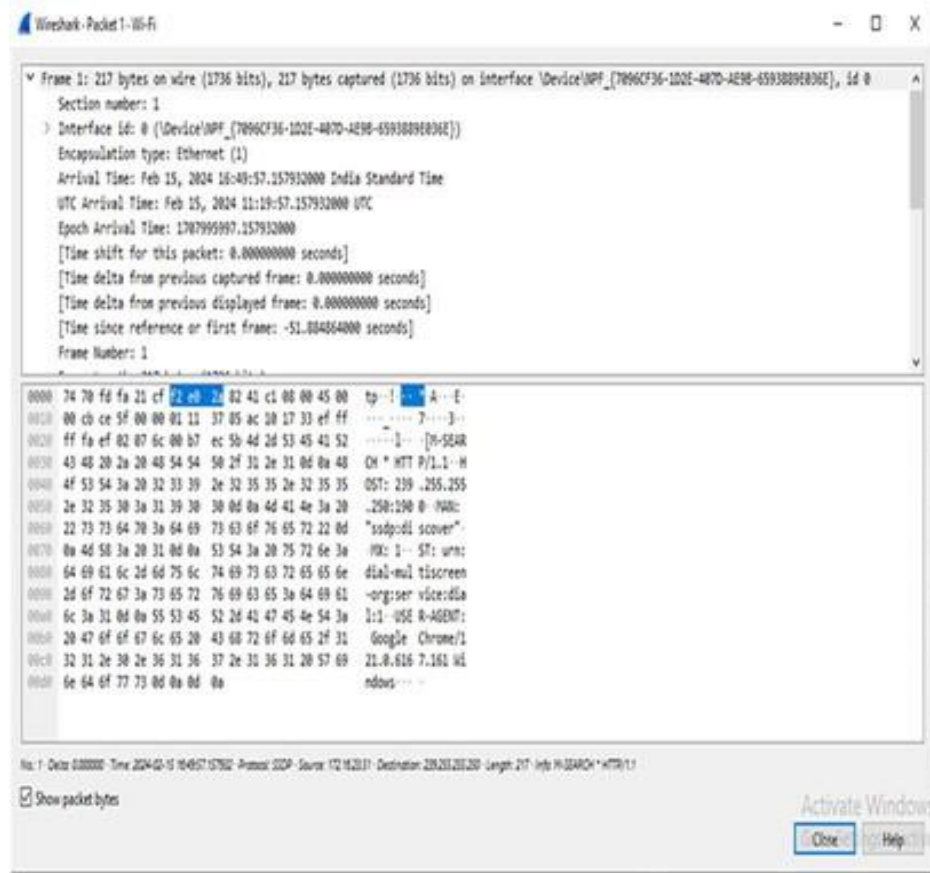


Fig.4:- Data Filtering

Figure 4 illustrates the process of filtering data, demonstrating how specific criteria can be applied to refine network traffic analysis. Figure 5: Destination and Port Address

Figure 5 presents the destination and port address, offering insights into how packets are directed based on their assigned network endpoints.

Topic / Item	Count	Average	Min Val	Max Val	Rate (pps)	Percent	Burst Rate	Burst Start
Destinations and Ports 1000					2.9834	100%	0.3402	276.561
Ether II	34				0.0079	0.26%	0.1000	50.389
UDP	1				0.0002	0.04%	0.0100	50.389
53	1				0.0002	100.00%	0.0100	50.389
TCP	33				0.0077	97.36%	0.1000	50.389
443	33				0.0077	100.00%	0.1000	50.389
Ether II	82				0.0191	0.64%	0.0800	20.012
TCP	82				0.0191	100.00%	0.0800	20.012
443	82				0.0191	100.00%	0.0800	20.012
74.125.24.188	7				0.0016	0.05%	0.0100	10.001
TCP	7				0.0016	100.00%	0.0100	10.001
443	7				0.0016	100.00%	0.0100	10.001
64.233.175.84	34				0.0079	0.26%	0.1800	86.547
TCP	34				0.0079	100.00%	0.1800	86.547
443	34				0.0079	100.00%	0.1800	86.547
54.165.33.80	3				0.0007	0.02%	0.0100	17.090
TCP	3				0.0007	100.00%	0.0100	17.090
443	3				0.0007	100.00%	0.0100	17.090
52.84.12.38	3				0.0007	0.02%	-	-
TCP	3				0.0007	100.00%	-	-
443	3				0.0007	100.00%	-	-
52.84.12.48	3				0.0007	0.02%	-	-
TCP	3				0.0007	100.00%	-	-
443	3				0.0007	100.00%	-	-
52.204.134	1				0.0002	0.01%	-	-
TCP	1				0.0002	100.00%	-	-
443	1				0.0002	100.00%	-	-
52.204.196.248	119				0.0077	0.62%	0.1000	236.481
TCP	119				0.0077	100.00%	0.1000	236.481
443	119				0.0077	100.00%	0.1000	236.481
52.123.160.105	12				0.0028	0.09%	0.0100	5.532
TCP	12				0.0028	100.00%	0.0100	5.532
443	12				0.0028	100.00%	0.0100	5.532

Fig.5: Capture Filters

Capture filters allow users to selectively filter network traffic during packet capture, enabling more precise data collection.

Figure 5 presents various capture filter options, which help refine packet selection based on specific protocols, addresses, or connection attributes. These filters enhance efficiency by reducing unnecessary packet capture and focusing on relevant network traffic for analysis.

CONCLUSION

This paper presents case studies in packet analysis, emphasizing the significance of packet analyzers particularly Wireshark in network forensics. Traditional security methods often fail to detect all cyber threats, especially emerging attacks, without comprehensive network packet analysis.

While antivirus software remains a preferred security solution among home and enterprise users, many rely on signature-based detection, which has notable limitations.

Historically, packet analyzers were proprietary and expensive, but open-source solutions like Wireshark now provide detailed packet data, making them highly effective tools. However, despite its powerful features, Wireshark is not an intrusion detection system. Instead, network security professionals can leverage Wireshark's capabilities to identify unusual network behavior and potential security threats.

This paper demonstrates how Wireshark aids in detecting security risks and attacks targeting networked systems.

Here's a refined paraphrase of your references section:

REFERENCES

1. Alfawareh, H. M. (n.d.). *A deeper look into network traffic analysis using Wireshark*. Academia.edu, 1, 4–7. Available online.
2. Kaur, G. (2019). Investigating network traffic using packet sniffing tool – Wireshark. *Journal of Emerging*

- Technologies and Innovative Research*, 6(1), 181–186. Available online.
3. M., S. A., A. S., & R. K. (2023). Exploring Wireshark for network traffic analysis. *International Journal of Multidisciplinary Research*, 5(6), 1–12. <https://doi.org/10.36948/ijfmr.2023.v05i06.8876>.
 4. Saxena, A., & Sharma, S. K. (2017). Analysis of network traffic using packet sniffing tool: Wireshark. *International Journal of Advanced Research*, 3(6), 804–808. Available online.
 5. Shandilya, R., Ganguli, C., Izonin, I., & Nagar, P. A. K. (2023). Cyber attack evaluation dataset for deep packet inspection and analysis. *Data in Brief*, 46, 108771. <https://doi.org/10.1016/j.dib.2022.108771>.
 6. Sikos, L. F. (2020). Packet analysis for network forensics: A comprehensive survey. *Forensic Science International: Digital Investigation*, 32, 200892. <https://doi.org/10.1016/j.fsidi.2019.200892>.
 7. Soepeno, B. (n.d.). *Wireshark: [Title incomplete]*. [Additional publication details missing].
 8. Tuli, R. (2023). Analyzing network performance parameters using Wireshark. *International Journal of Network Security and Its Applications*, 15(1), 1–13. <https://doi.org/10.5121/ijnsa.2023.15101>