Wireshark: An Effective Tool for Network Analysis

Method · September 2023

DOI: 10.13140/RG.2.2.34444.69769

1 author:

Ryufath Soepeno
Sampoerna University
17 PUBLICATIONS **7** CITATIONS

SEE PROFILE

Wireshark: An Effective Tool for Network Analysis

Submitted for the course:

CYBV - Introductory Methods of Network Analysis

September 2023

Ryufath Alief Adhyaksa Putera Soepeno (23792097)

Information Systems

Faculty of Engineering & Technology

Sampoerna University

&

Applied Computing

College of Applied Science & Technology

University of Arizona

Wireshark: An Effective Tool for Network Analysis

Wireshark, a prominent network analysis software, serves as the digital detective of the virtual realm. It captures and dissects data packets in real-time, offering unparalleled precision and thoroughness. During four weeks of network analysis using Wireshark, it meticulously unveils the layers of each protocol, yielding a valuable repository of knowledge about data packet behavior. In today's digital landscape, Wireshark is an indispensable tool for investigators and analysts exploring the intricacies of internet-based activities.

Wireshark plays a vital role in network security analysis, providing insights into internet communication, network infrastructure, and edge devices. For internet communication, Wireshark allows analysts to monitor and scrutinize data traffic, identifying issues like network abuse, malicious connections, and performance degradation (Kumar & Yadav, 2016). It achieves this by capturing real-time network traffic data and displaying packet-level details and patterns. In the realm of network infrastructure, Wireshark's data capture capabilities ensure comprehensive traffic visibility, aiding in the detection of security threats and anomalous activities. This complete view of traffic patterns empowers network administrators to proactively address vulnerabilities and safeguard data integrity. Moreover, Wireshark assists in troubleshooting and optimizing data transmission by pinpointing bottlenecks and identifying problematic packets, ensuring smooth data flow (Tuli, 2023).

Exploring Non-Wireshark Packet Sniffing Tools

TCPdump is a widely used packet sniffer that allows network administrators and security professionals to capture and analyze network traffic in real-time. Piyush and Anorag Goyal (2017) infer that TCPdump plays a critical role in network security analysis by enabling the monitoring and detection of suspicious or malicious activities within a network. By examining

the contents of captured packets, TCPdump can help in pinpointing the source and nature of a network threat, aiding in incident response and forensic investigations. Moreover, TCPdump's ability to save captured packets for later analysis is valuable for historical data retrieval and long-term threat assessment. It can be instrumental in identifying suspicious or malicious activity, such as unusual traffic patterns, unauthorized access attempts, or potential security breaches. TCPdump helps identify anomalies, such as unusual traffic patterns, potential security breaches, or unauthorized access attempts, which are crucial for early threat detection and response

NetFlow, a technology developed by Cisco, offers a high-level overview of network traffic by summarizing packet data into flow records. This makes it particularly valuable for monitoring and analyzing network traffic at scale, providing detailed information about network flows, including source and destination IP addresses, port numbers, and data volume. NetFlow aids in understanding communication patterns within a network, identifying traffic anomalies, and detecting potential security threats like distributed denial-of-service (DDoS) attacks or data exfiltration attempts (Islam et al, 2023). Furthermore, it provides detailed flow-level data that significantly contributes to network security analysis by offering insights into traffic patterns, facilitating the identification of abnormal behavior, and assisting security professionals in mitigating various cyber threats, including insider threats. Additionally, NetFlow data can be aggregated for capacity planning, optimizing network performance, and enforcing security policies.

Wireshark offers features like live packet capture, display filters, and protocol decoders, making it a preferred choice for network administrators and analysts over TCPdump, a command-line packet sniffer. While Netflow provides valuable insights into network traffic

trends and bandwidth utilization, it lacks the detailed packet-level analysis found in Wireshark and TCPdump, crucial for troubleshooting network issues. Wireshark remains the go-to tool for network professionals seeking in-depth insights into network traffic, solidifying its status as the top choice for precise and comprehensive packet-level analysis in networking.

HTTP in Networking

HTTP (Hypertext Transfer Protocol) is the foundation for data communication on the World Wide Web and is a fundamental protocol in the realm of computer networking and the internet. HTTP defines the rules and conventions for how web servers and web clients or browsers should interact with each other to request and transmit web resources, such as HTML documents, images, videos, and more (Bressoud & White, 2020). It operates within the application layer of the Internet Protocol Suite, which is a stack of networking protocols used to facilitate communication between devices on the internet. HTTP is a stateless protocol, meaning that each request-response cycle is independent, and the server doesn't retain information about past interactions. HTTP requests are issued by clients to retrieve resources from web servers, while HTTP responses contain the requested data and status information, such as success or error codes.

HTTP is often referred to as an application layer protocol because it operates at the highest layer of the Internet Protocol Suite, which is the application layer. This layer focuses on the communication between software applications rather than the technical details of data transmission over the network. HTTP, in this context, is responsible for defining how web browsers and web servers should interact and exchange data and abstracts the complexities of lower-level networking protocols like TCP/IP and provides a user-friendly interface for requesting and delivering web content (Pohl et al., 2018). HTTP's simplicity and ease of use

have contributed significantly to the growth of the World Wide Web, making it accessible to billions of users worldwide.

C-I-A Triad

The C-I-A triad, which stands for Confidentiality, Integrity, and Availability, is a fundamental concept in network security and information assurance. These three principles are at the core of any comprehensive security framework. Confidentiality ensures that data is kept private and only accessible to authorized individuals or systems. This means that sensitive information should not be disclosed to unauthorized parties. Integrity guarantees the accuracy and trustworthiness of data. It ensures that data remains unaltered during transmission or storage, preventing unauthorized modifications or tampering. Finally, Availability ensures that data and network resources are accessible when needed. It involves maintaining the reliability and uptime of systems to ensure that authorized users can access data and services when required.

Protocols play a crucial role in ensuring compliance with the C-I-A triad. A protocol is a set of rules and conventions that govern communication between devices and systems in a network. To comply with the C-I-A triad, a protocol must incorporate specific security measures. For Confidentiality, protocols should include encryption mechanisms to protect data from unauthorized access. Integrity can be ensured through features like checksums and digital signatures, which detect any unauthorized changes in data during transmission. Availability is often maintained through redundancy and failover mechanisms, which ensure that network services remain accessible even in the face of hardware or software failures.

In applicable terms, consider the HTTPS protocol used for secure web communication. HTTPS employs encryption to ensure that data exchanged between a web server and a client remains confidential and inaccessible to eavesdroppers, therefore confidentiality. HTTPS also

uses digital certificates to verify the authenticity of the server, preventing man-in-the-middle attacks, while also operating over the reliable TCP protocol and includes error-checking mechanisms to ensure data accuracy, therefore integrity. Lastly, web servers are designed with load balancing and redundancy to maintain service availability, even under heavy traffic or server failures, therefore availability. Thus, HTTPS exemplifies how a protocol can align with the C-I-A triad principles to enhance network security (Covert et al., 2020).

Wireshark's Packet Sniffing Power for HTTP

Wireshark is a powerful network protocol analyzer that allows users to capture, inspect, and analyze network traffic and is a valuable tool for understanding and troubleshooting network communication. When it comes to HTTP, Wireshark can capture and dissect HTTP packets, providing detailed information about the HTTP requests and responses exchanged between clients and servers. This includes details like the HTTP method (GET, POST, etc.), headers, status codes, payload, and more. Wireshark's ability to analyze HTTP traffic is particularly useful for diagnosing network issues, and security threats, and optimizing web applications. It can reveal insights into the timing and efficiency of web requests, helping network administrators and developers pinpoint bottlenecks and errors (Kumar & Yadav, 2016).

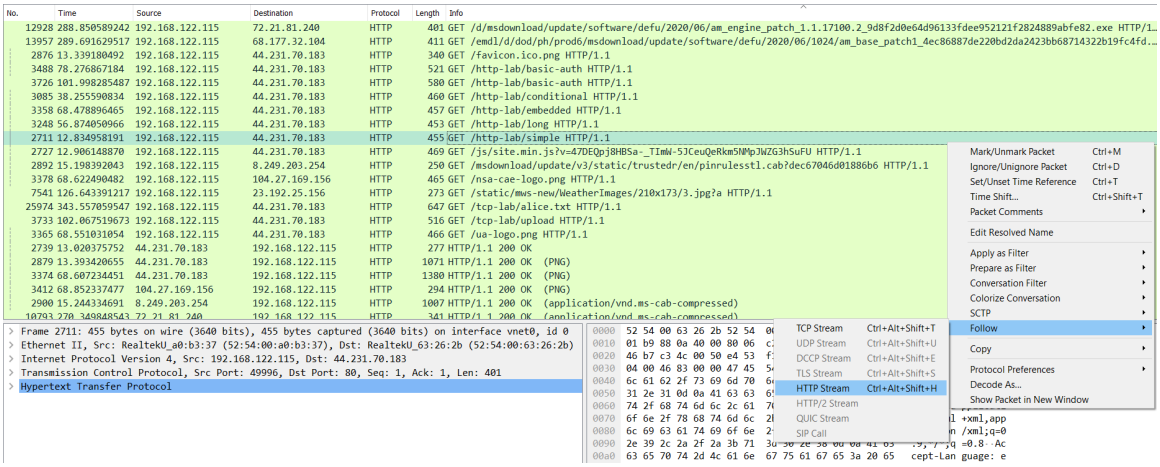

Figure 1: *Method to follow and observe an HTTP stream*

Begin by accessing the info bar to locate the specific HTTP session for "http-lab/simple HTTP 1.1." Then, employ the context click (or right-click) option to initiate the process of tracking and examining the complete HTTP stream associated with this session in the Wireshark capture. This action will provide a detailed view of the HTTP protocol, allowing for the analysis of the various HTTP requests and responses exchanged during this communication, thereby aiding in the understanding of the intricacies of the HTTP 1.1 protocol implementation.

When delving into the analysis of an HTTP stream within Wireshark to ascertain its alignment with the C-I-A triad principles, attention should be directed towards specific facets of the communication. Firstly, it is essential to identify whether any sensitive information, such as login credentials or personal data, is transmitted without encryption (HTTP instead of HTTPS), as this can potentially signify a breach of confidentiality. Secondly, one must be vigilant for signs of data tampering or unauthorized alterations within the stream, as the presence of inconsistencies or modified content might imply a deficiency in data integrity. Lastly, the examination of the stream should extend to the identification of service disruptions or indications of denial of service, such as the occurrence of frequent connection resets or unexpected spikes in network traffic, as these irregularities may hint at potential availability issues.

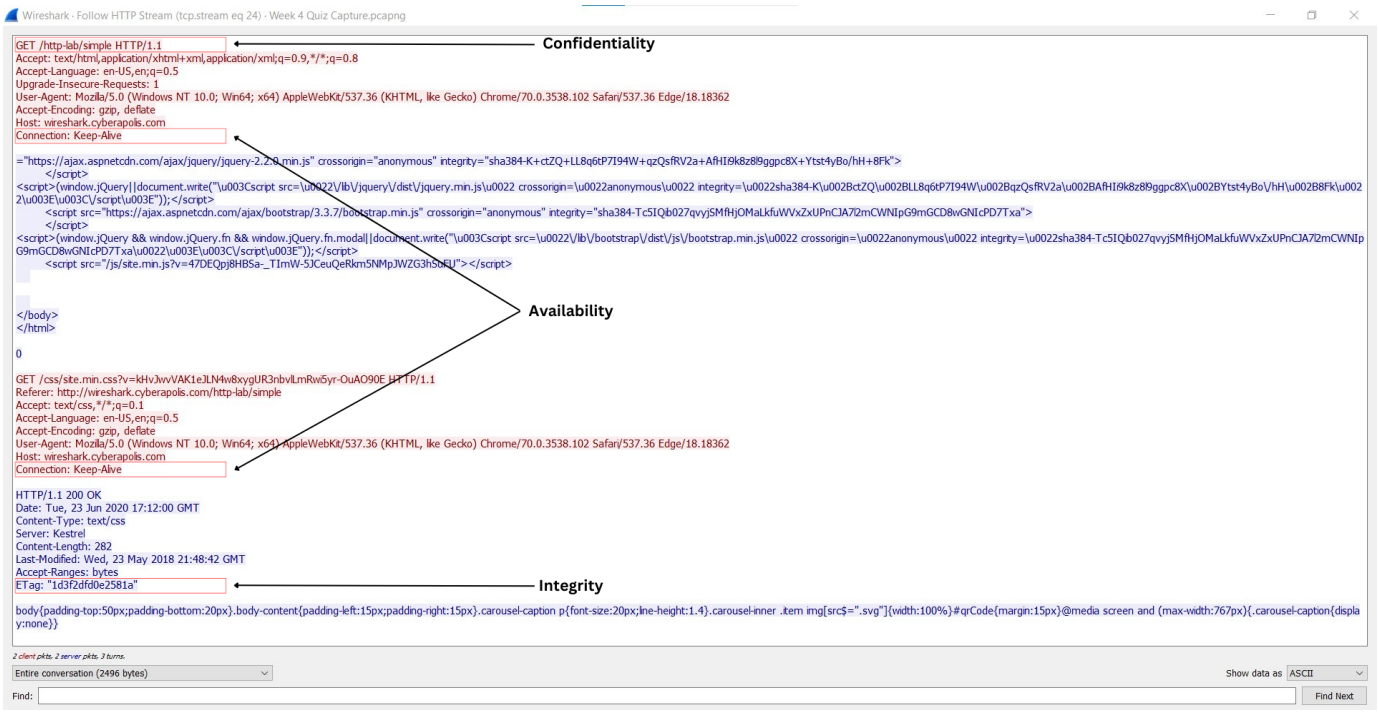

Figure 2: *HTTP stream analysis of "http-lab/simple HTTP 1.1.*"

For "http-lab/simple HTTP 1.1." case shown in figure 2, the presented HTTP stream demonstrates a strong consistency to the C-I-A triad, which includes the concepts of Confidentiality, Integrity, and Availability. To begin, it maintains Confidentiality by using HTTPS (Hypertext Transfer Protocol Secure) for communication, as demonstrated by the "GET /http-lab/simple HTTP/1.1" request: The 's' in HTTPS indicates that data transfer between the client and server is encrypted and secure, protecting against unwanted access and ensuring the confidentiality of sent information. The stream also highlights Integrity through the utilization of an "ETag" header in the HTTP response ("HTTP/1.1 200 OK"): This ETag facilitates the validation of resource integrity and if the content remains unaltered since the last request (as indicated by the ETag), the server can respond with a "Not Modified" status, ensuring that data remains uncorrupted during transit. Lastly, the stream maintains Availability by including the "Connection: Keep-Alive" header, indicating the intention to involve a persistent connection

between the client and server: This approach reduces the overhead of establishing new connections for subsequent requests, thus enhancing the availability of the web service by ensuring efficient and responsive communication.

For capturing and analyzing network traffic, particularly HTTP packets, Wireshark is indispensable. By examining HTTP streams, it assists in identifying network problems and security threats while upholding the C-I-A triad principles and demonstrating strong confidentiality, integrity, and availability in the case of "http-lab/simple HTTP 1.1."

DDOS: A Look at Relevant DNS Vulnerability

In today's ever-evolving landscape of cybersecurity threats, one recurring concern is the vulnerability associated with Domain Name System (DNS) attacks. DNS serves as the internet's address book, translating human-readable domain names into IP addresses. Despite its fundamental role, DNS remains susceptible to various forms of exploitation (Lyu et al., 2021). DDoS attacks, once considered relatively primitive, have reemerged as a potent threat, especially for businesses and enterprises.

A pertinent case is highlighted by respectively *Washington Post* cybersecurity newsletter writer and cyber security & technology policy Researcher, Tim Starks and David DiMolfetta (2023) regarding the incident involving Microsoft's Outlook email service outage that serves as a stark reminder of their capacity for harm. While DDoS attacks don't usually entail data theft, they can nonetheless do a great deal of harm by flooding their targets with phony traffic and disrupting services. Concurrently, cybersecurity professionals are aware that attacks using DDoS are changing, getting more complex, and focusing on a wider range of targets. Concerns have been raised by this change since attackers are now using DDoS assaults as part of larger

campaigns, and certain organizations, such as Killnet and Anonymous Sudan, are escalating the increase in attacks.

Financial institutions in Europe have seen a significant increase in DDoS assaults as a result of this. Loss of production and possible extortion are only two examples of the severe economic consequences. Attackers will occasionally threaten to carry out DDoS attacks if ransoms are not paid. Recent measures by the Justice Department show a rising effort to counter these dangers, along with those of organizations like the Cybersecurity and Infrastructure Security Agency. Concerns about DDoS assaults are growing, emphasizing the need for enterprises to strengthen their defenses against this expanding threat. Additionally, the article mentions a trend towards more sophisticated DDoS attacks on DNS, the very backbone of the internet, signaling the importance of fortifying this critical infrastructure against cyber threats.

Wireshark as Diagnosis Tool for DNS Vulnerabilities

In a business setting, tools like Wireshark can be invaluable for diagnosing and mitigating potential vulnerabilities, particularly in the context of evolving cyber threats like DDoS attacks. With the help of the sophisticated network protocol analyzer Wireshark, analysts may examine and deconstruct network traffic in real time. Wireshark can give crucial information about the nature of DDoS assaults, assisting analysts in recognizing trends, source IPs, and the particular methodologies being used. Wireshark, for this instance, may be used by analysts to record and examine traffic during a suspected DDoS assault, demonstrating the flurry of requests that are directed at a certain service or server (Fidele et al., 2020). Understanding the attack's features and possible effects on the business may need this knowledge.

Furthermore, Wireshark's capabilities extend beyond passive monitoring: It allows analysts to configure alerts and triggers that automatically find anomalous traffic patterns

suggestive of DDoS attacks (Yaacoub et al., 2023). This proactive strategy is crucial for quick reaction and mitigation in a commercial setting. Following the identification of the attack, mitigating measures can be implemented, such as rerouting traffic through a DDoS protection provider or putting firewall rules in place to restrict malicious traffic. Enterprises may utilize the data gathered by Wireshark for post-attack research and forensics to better understand the attack pathways, flaws, and vulnerabilities in their network architecture, enabling enterprises to keep control over their network security in today's interconnected and fragile digital ecosystem, where cyber-attacks may strike at several points and assists businesses in preventing attacks, securing their vital online assets, and offering real-time insight into network traffic and quick response to any weaknesses.

Conclusion

Wireshark stands as a crucial tool in network analysis, providing deep insights into data packet behavior and aiding in network security analysis as it empowers investigators and analysts in uncovering the intricacies of internet-based activities. While alternatives like TCPdump and NetFlow have their merits, Wireshark's packet-level analysis remains unparalleled for troubleshooting and comprehensive inspection. Wireshark's application in dissecting HTTP streams aligns with the C-I-A triad principles, enhancing network security by ensuring confidentiality, integrity, and availability; and in the evolving landscape of cybersecurity, Wireshark's role as a diagnostic tool for vulnerabilities, such as DDoS attacks on DNS, is indispensable for proactive monitoring, quick response, and post-attack analysis, contributing to the overall resilience of modern enterprises and nevertheless cybersecurity.

References

Bressoud, T., & White, D. (2020). The HyperText Transfer Protocol. In *Introduction to Data Systems*. https://doi.org/10.1007/978-3-030-54371-6_20

Covert, Q., Steinhagen, D., Francis, M., & Streff, K. (2020). Towards a triad for data privacy. *Proceedings of the . . . Annual Hawaii International Conference on System Sciences*. https://doi.org/10.24251/hicss.2020.535

Fidele, K. A., Suryono, S., & Syafei, W. A. (2020). Denial of Service (DoS) attack identification and analyse using sniffing technique in the network environment. *E3S Web of Conferences*, *202*, 15003. https://doi.org/10.1051/e3sconf/202020215003

Goyal, P., & Goyal, A. (2017). Comparative study of two most popular packet sniffing tools-Tcpdump and Wireshark. *Institute of Electrical and Electronics Engineers (IEEE)*. https://doi.org/10.1109/cicn.2017.8319360

Islam, R., Patamsetti, V. V., Gadhi, A., Gondu, R. M., Bandaru, C. M., Kesani, S. C., & Abiona, O. (2023). Design and analysis of a network traffic analysis tool: NetFlow Analyzer. *Int'l J. of Communications, Network and System Sciences*, *16*(02), 21–29. https://doi.org/10.4236/ijcns.2023.162002

Kumar, A., & Yadav, J. B. (2016). Comparison: Wireshark on different parameters. *International Journal of Engineering and Computer Science*. https://doi.org/10.18535/ijecs/v5i3.33

Lyu, M., Gharakheili, H. H., Russell, C., & Sivaraman, V. (2021). Hierarchical Anomaly-Based detection of distributed DNS attacks on enterprise networks. *IEEE Transactions on Network and Service Management*, *18*(1), 1031–1048. https://doi.org/10.1109/tnsm.2021.3050091

Pohl, M., Kubela, J., Bosse, S., & Turowski, K. (2018). Performance Evaluation of Application Layer Protocols for the Internet-of-Things. *2018 Sixth International Conference on Enterprise Systems (ES)*. https://doi.org/10.1109/es.2018.00035

Starks, T., & DiMolfetta, D. (2023, June 27). The lowly DDoS attack is showing signs of being anything but. *Washington Post*. https://www.washingtonpost.com/politics/2023/06/27/lowly-ddos-attack-is-showing-signs-being-anything/

Tuli, R. (2023). Analyzing Network performance parameters using wireshark. *International Journal of Network Security & Its Applications (IJNSA)*, *5*(1), 1–2. https://doi.org/10.5121/ijnsa.2023.15101

Yaacoub, J. A., Noura, H., Salman, O., & Chehab, A. (2023). Ethical hacking for IoT: Security issues, challenges, solutions and recommendations. *Internet of Things and Cyber-physical Systems*, *3*, 280–308. https://doi.org/10.1016/j.iotcps.2023.04.002