MA3105 Computer Networks

Assignment-6: Network Traffic Analysis Report

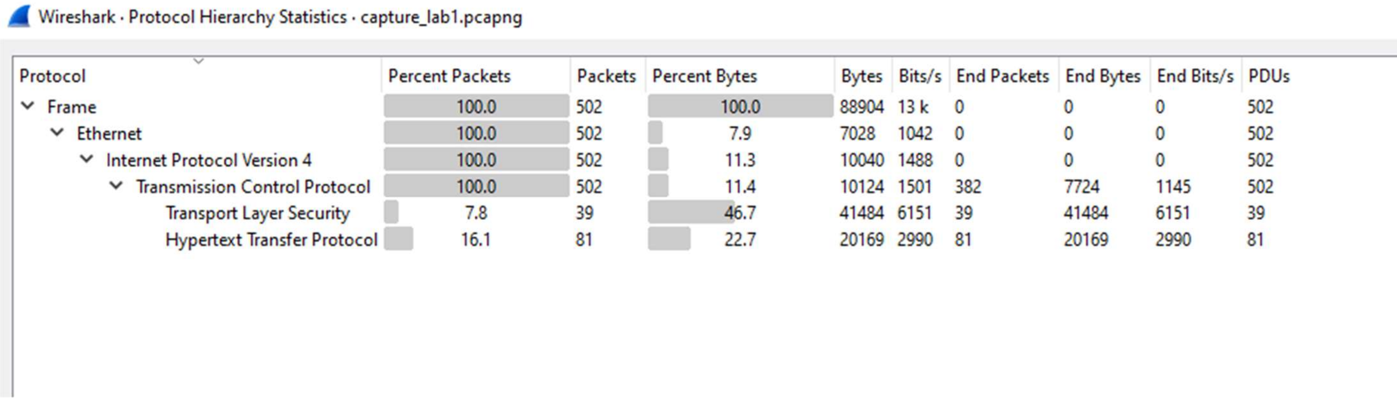
Introduction and Objective

This report summarizes the findings from the network traffic analysis conducted using **Wireshark**, as outlined in the Computer Networks Lab assignment. The objective was to capture and analyze live network traffic to identify various network protocols and interpret packet-level details. The analysis was performed on traffic generated by visiting secure websites and executing a `ping` command to `8.8.8.8`.

Key Findings and Protocol Activity

Most Active Protocols

Analysis of the captured traffic (`capture_lab1.pcapng`) via the Protocol Hierarchy statistics revealed the following distribution of activity:



Wireshark · Protocol Hierarchy Statistics · capture_lab1.pcapng

Protocol	Percent Packets	Packets	Percent Bytes	Bytes	Bits/s	End Packets	End Bytes	End Bits/s	PDUs
Frame	100.0	502	100.0	88904	13 k	0	0	0	502
Ethernet	100.0	502	7.9	7028	1042	0	0	0	502
Internet Protocol Version 4	100.0	502	11.3	10040	1488	0	0	0	502
Transmission Control Protocol	100.0	502	11.4	10124	1501	382	7724	1145	502
Transport Layer Security	7.8	39	46.7	41484	6151	39	41484	6151	39
Hypertext Transfer Protocol	16.1	81	22.7	20169	2990	81	20169	2990	81

Insights

The statistics show a total of **502 packets** captured. The data reveals that the network activity was dominated by the TCP/IP suite, which is standard for modern web communication.

1. **Dominance of Transmission Control Protocol (TCP)**

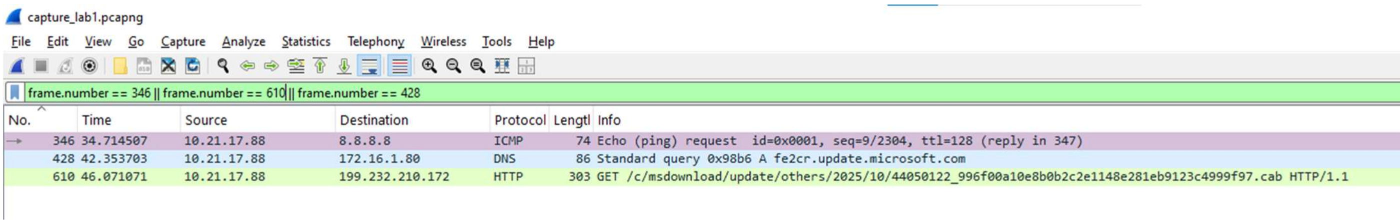
   1.
   - TCP is the primary transport protocol in this capture, accounting for **100% of the packets** at the transport layer. This indicates that the web browsing activity primarily utilized the traditional HTTPS-over-TCP stack rather than newer protocols like QUIC.

2. **Significant Secure and Unsecured Web Traffic**
   - **Transport Layer Security (TLS)** accounts for **7.8% of packets** but a substantial **46.7% of the total bytes**. This confirms that a significant portion of the web browsing was encrypted (HTTPS), involving larger packet payloads for secure data exchange.

  - **Hypertext Transfer Protocol (HTTP)** accounts for **16.1% of packets**, indicating that there was also unencrypted web communication, likely for fetching updates or other system services.
3. **Minimal ICMP and DNS Activity in Hierarchy**
   - While present in the full capture (as seen in later analysis), protocols like **ICMP** and **DNS** do not appear as major contributors in the protocol hierarchy statistics. This is expected, as they typically involve a small number of packets for initial lookups or connectivity checks compared to the continuous stream of data packets in a web session.

Detailed Packet Analysis Summary

The following table summarizes key layer details from a selected packet for each protocol family, based on the provided screenshots.


capture_lab1.pcapng
File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help

frame.number == 346 || frame.number == 610 || frame.number == 428

No.	Time	Source	Destination	Protocol	Lengtl	Info
→ 346	34.714507	10.21.17.88	8.8.8.8	ICMP	74	Echo (ping) request id=0x0001, seq=9/2304, ttl=128 (reply in 347)
428	42.353703	10.21.17.88	172.16.1.80	DNS	86	Standard query 0x98b6 A fe2cr.update.microsoft.com
610	46.071071	10.21.17.88	199.232.210.172	HTTP	303	GET /c/msdownload/update/others/2025/10/44050122_996f00a10e8b0b2c2e1148e281eb9123c4999f97.cab HTTP/1.1

Traffic Analysis and Insights

Key Network Communication Insights

The capture provided clear insights into typical network communication flows:

- **DNS Precedes Web Traffic**: The communication sequence for visiting a website first involves a DNS query (using UDP) to resolve a domain name (like `fe2cr.update.microsoft.com`) to an IP address.
- **Web Traffic is Both Encrypted and Unencrypted**: Connections to secure websites initiated TCP handshakes on port 443, encapsulating data within the TLS layer. Simultaneously, standard HTTP traffic on port 80 was observed, likely for system updates.
- **ICMP for Connectivity**: The `ping 8.8.8.8` command exclusively utilized the ICMP protocol to send Echo Request messages and receive Echo Reply messages, confirming network layer connectivity.

Suspicious or Unusual Traffic

Based on the controlled nature of the capture, **no genuinely suspicious or malicious activity was observed**. All traffic was a direct result of the activities specified in the assignment.

- **Observation**: Several **TCP Retransmission** and **Duplicate ACK** packets were observed within the TCP/TLS sessions. While sometimes indicating a network problem, in this case, they are likely due to minor network jitter or packet drops common in Wi-Fi networks and are not considered malicious.

Conclusion

The assignment successfully demonstrated the use of Wireshark for network analysis. The captured data provided tangible examples of DNS resolution, simple ICMP connectivity checks, and the dominant role of TCP and TLS in securing modern web traffic. The exercise in applying custom filters, such as `ip.src == 10.21.17.88`, proved effective in isolating specific communication flows for further analysis.