MA3105

Computer Networks

Assignment-6

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, identify various network protocols, and interpret packet-level details. The analysis was performed on traffic generated by visiting two secure websites (https://example.com, https://wikipedia.org) and executing a ping command to 8.8.8.8

Key findings and Protocol Activity

Most Active Protocols

Analysis of the captured traffic (capture.pcap) via the Protocol Hierarchy statistics revealed the following distribution of activity:

Protocol	Percent Packets	Packets	Percent Bytes	Bytes	Bits/s	End Packets	End Bytes	End Bits/s	PDUs
Frame	100.0	1209	100.0	447395	24 k	0	0	0	1209
Ethernet	100.0	1209	3.8	16926	932	0	0	0	1209
Internet Protocol Version 4	100.0	1209	5.4	24180	1332	0	0	0	1209
User Datagram Protocol	68.3	826	1.5	6608	364	0	0	0	826
QUIC IETF	42.7	516	39.7	177638	9789	516	173087	9539	532
Domain Name System	0.4	5	0.0	162	8	5	162	8	5
Data	25.2	305	19.0	85079	4688	305	85079	4688	305
Transmission Control Protocol	31.3	379	1.7	7700	424	300	6120	337	379
Transport Layer Security	5.3	64	28.2	126088	6948	64	126088	6948	64
Data	1.2	15	0.0	15	0	15	15	0	15
Internet Control Message Protocol	0.3	4	0.0	160	8	4	160	8	4

Insights

The statistics show a high volume of traffic, with **1209 total packets** captured. The data reveals that the network activity is highly dominated by modern, secure internet communication and transport protocols.

1. Dominance of User Datagram Protocol (UDP)

- **UDP is the primary transport protocol, accounting for 68.3% of packets**. This is significantly higher than TCP's 31.3%.

- **QUIC (Quick UDP Internet Connections) is the main contributor to UDP traffic (42.7% of all packets)**. QUIC is a newer transport layer protocol developed by Google, often used for secure connections to services like Google Search, YouTube, and Chrome. Its high percentage suggests heavy usage of modern web services.
- **DNS (Domain Name System) is minimal (0.4% of packets)**. This indicates that most name lookups were resolved quickly, or the capture duration was short relative to the total traffic flow.

2. Significant Secure Web Traffic

- **Transmission Control Protocol (TCP) accounts for 31.3% of packets**.
- Within TCP, **Transport Layer Security (TLS) accounts for 5.3% of all packets**. Since TLS runs over TCP and is used for HTTPS, this confirms that a portion of the secure web browsing activity was conducted using the traditional HTTPS over TCP stack.
- **The combined presence of QUIC and TLS/TCP highlights that virtually all web traffic was secured (encrypted)**, which is standard for modern web activity (HTTPS).

3. Minimal ICMP Activity

- **Internet Control Message Protocol (ICMP) accounts for a very small percentage (0.3% of packets)**. This traffic likely corresponds to the single ping 8.8.8.8 command run during the capture, confirming that no prolonged or excessive ICMP activity occurred.

Detailed Packet Analysis Summary

The following table summarizes key layer details from a selected packet for each protocol family:

Protocol	Source IP	Destination IP	TTL	Packet Length	Flags
ICMP	192.170.4.46	8.8.8.8	128	74 bytes	Echo (ping) request (8)
HTTP (as TCP 443)	192.170.4.46	172.202.64.254	128	54 bytes	[FIN, ACK]
DNS	192.170.4.46	8.8.8.8	128	70 bytes	Standard query

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 the domain name to an IP address. For

instance, a query for wikipedia.org was sent to the local DNS server (192.168.1.1 in the example).

- **Web Traffic is Encrypted:** All connections to https:// websites initiated **TCP** connections on port **443**. This highlights that the **HTTP** protocol is encapsulated and encrypted by the **TLS** layer, preventing network observers from viewing the actual data or URI content without the corresponding decryption keys.
- **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 small, 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 (web browsing and pinging).

Observation: There were several **TCP Retransmission** and **Duplicate ACK** packets observed within the TCP/TLS sessions. While sometimes indicating a problem, in this case, they are likely minor network jitter or drops common in Wi-Fi networks and are not considered malicious or unusual for a typical web browsing session.

Conclusion

The assignment successfully demonstrated the use of Wireshark for network analysis. The captured data provided tangible examples of **DNS** resolution (UDP), simple **ICMP** connectivity, and the dominant role of **TCP** and **TLS** in securing modern web traffic. The exercise in applying custom filters, such as ip.src == 192.170.4.46, proved effective in isolating specific, critical communication flows for further analysis.