FILZA SAFDAR

TASK 2 REPORT:
Packet Analysis using Wireshark

Objective
To capture and analyze network traffic using Wireshark and understand basic network protocols.

Tool Used
- Wireshark (Packet Capture and Analysis Tool)
- Network Interface
- Active Interface: Wi-Fi

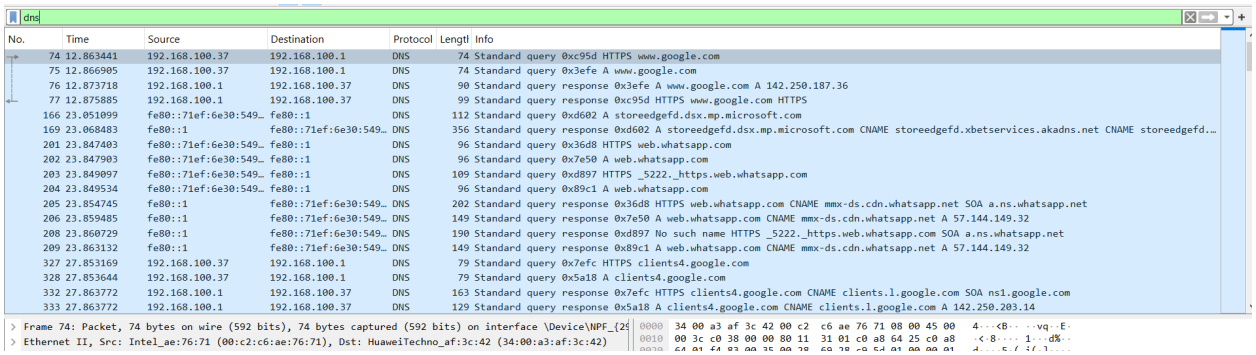
Procedure
Opened Wireshark and selected the active network interface.
Started packet capture.
Generated network traffic by browsing websites.
Stopped the capture after sufficient packets were collected.
Applied protocol filters to analyze traffic:
DNS filter
TCP filter
ARP filter
UDP filter
HTTP filter Inspected

TASK:02

FILZA SAFDAR

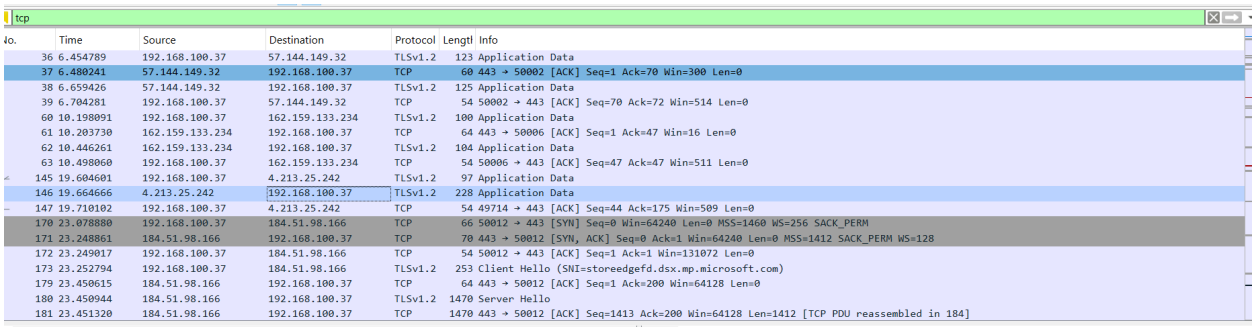
DNS Traffic Analysis

DNS packets were observed resolving domain names into IP addresses.
DNS communication used UDP port 53.
Source and destination IP addresses were visible in the packet details.
This confirms domain name resolution before communication begins.



TCP Traffic Analysis

TCP packets were observed ensuring reliable communication.
TCP uses a three-way handshake (SYN, SYN-ACK, ACK).
Source and destination ports were visible.
TCP ensures ordered and error-free data transmission

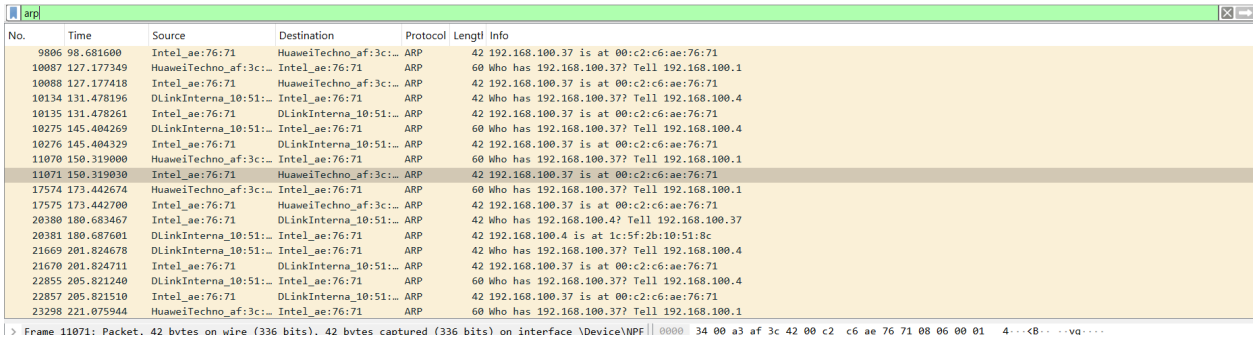


TASK:02

FILZA SAFDAR

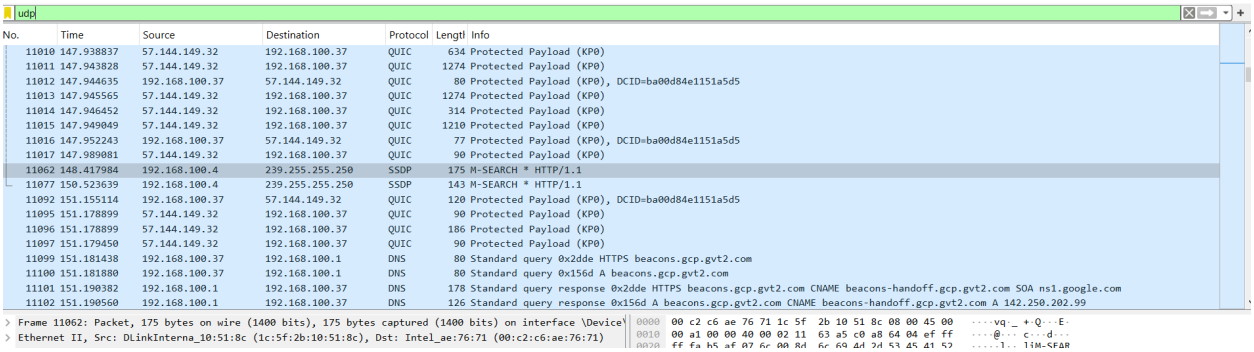
ARP Traffic Analysis

ARP packets were captured showing requests and replies.
ARP Request packets asked “Who has this IP address?”.
ARP Reply packets returned the corresponding MAC address.
This process enables devices to communicate within the same local network.



UDP Traffic Analysis

UDP packets were observed carrying lightweight traffic.
UDP does not establish a connection like TCP.
Source and destination ports were visible in packet details.
UDP is commonly used by DNS, streaming, and real-time applications.

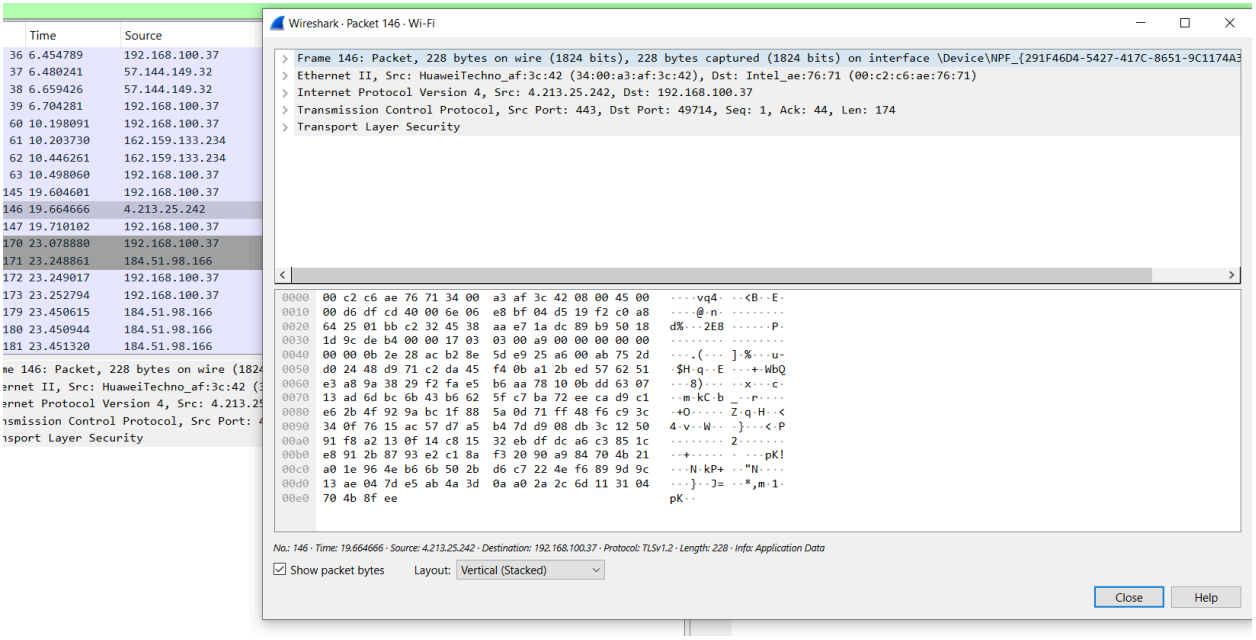


TASK:02

FILZA SAFDAR

Packet Detail Inspection

Individual packets were inspected to observe:
Source IP address
Destination IP address
Source and destination ports
Protocol type (TCP)
This helps understand how data flows between device



HTTPS Traffic Analysis

HTTPS traffic was observed during packet capture; however, the data payload was encrypted. Due to encryption, application-layer content was not readable. This demonstrates how HTTPS provides secure communication by protecting data confidentiality.

TASK:02

FILZA SAFDAR

PROTOCOLS

The following protocols were identified during packet capture:
Protocol
Purpose
DNS
Resolves domain names to IP addresses
ARP
Maps IP addresses to MAC addresses
TCP
Provides reliable, connection-oriented communication
UDP
Provides fast, connectionless communication
HTTPS
Ensures secure encrypted data transfer

TCP Three-Way Handshake

The TCP three-way handshake establishes a reliable connection between two devices.
Steps:
SYN – Client sends a synchronization request.
SYN-ACK – Server acknowledges and sends its own synchronization.
ACK – Client acknowledges, and the connection is established.
This process ensures both devices are ready to transmit data reliably.

Conclusion

The packet analysis demonstrated the functioning of multiple network protocols. ARP handled IP-to-MAC resolution within the local network, UDP enabled fast data transmission, DNS resolved domain names, and TCP ensured reliable communication. Wireshark proved effective for analyzing real network traffic.

GITHUB:https://github.com/filzasafdar8-netizen/CODEINTERN_TASKS

TASK:02