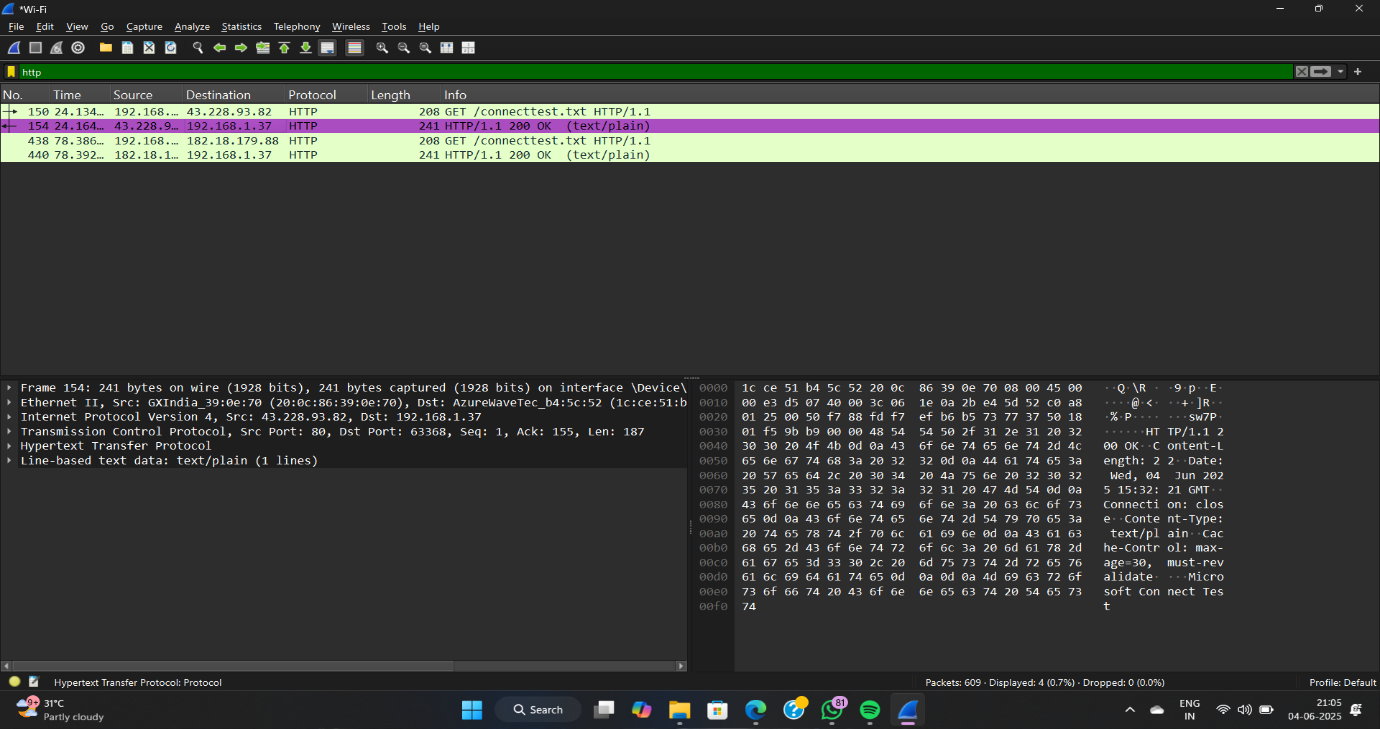
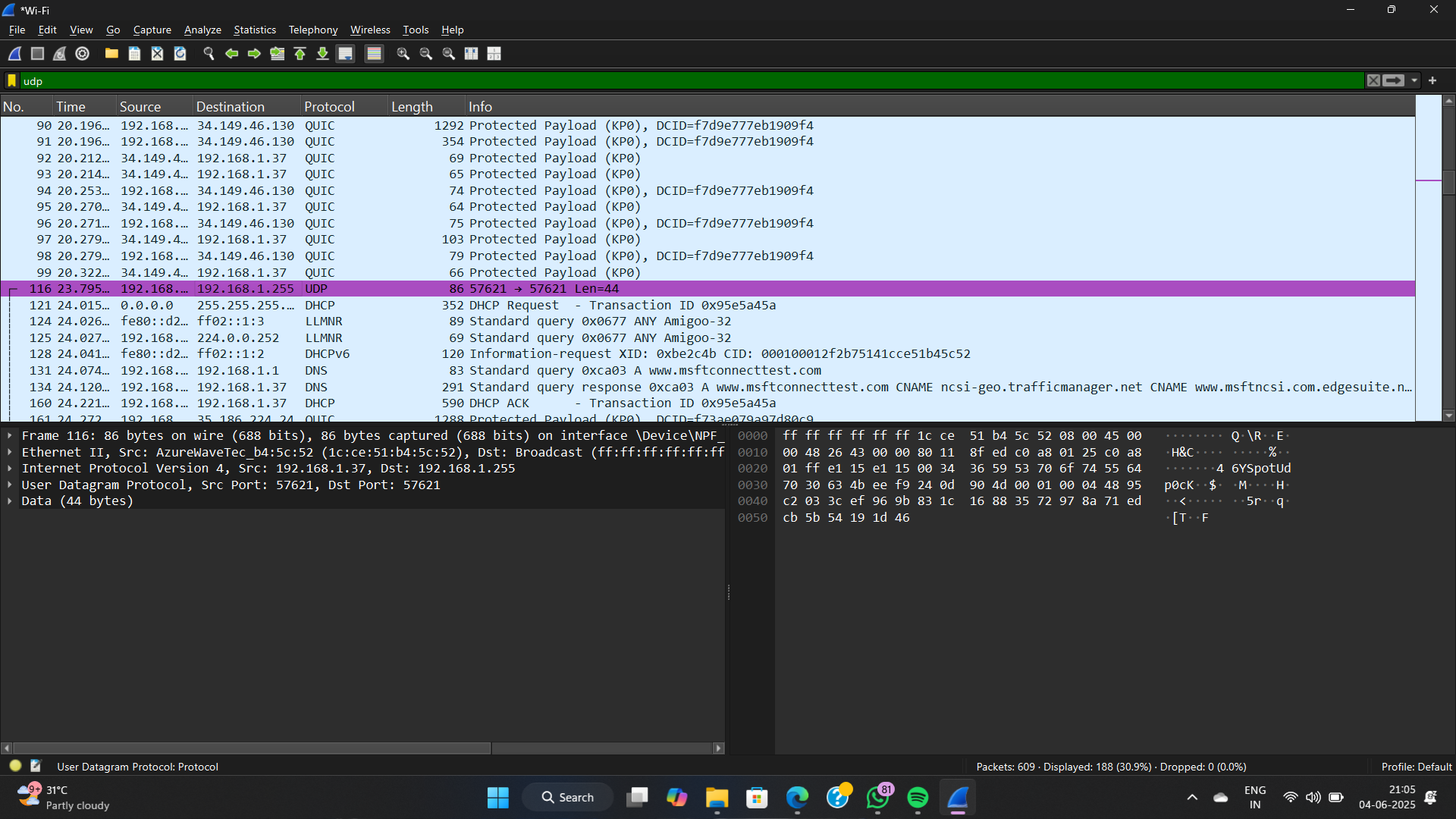
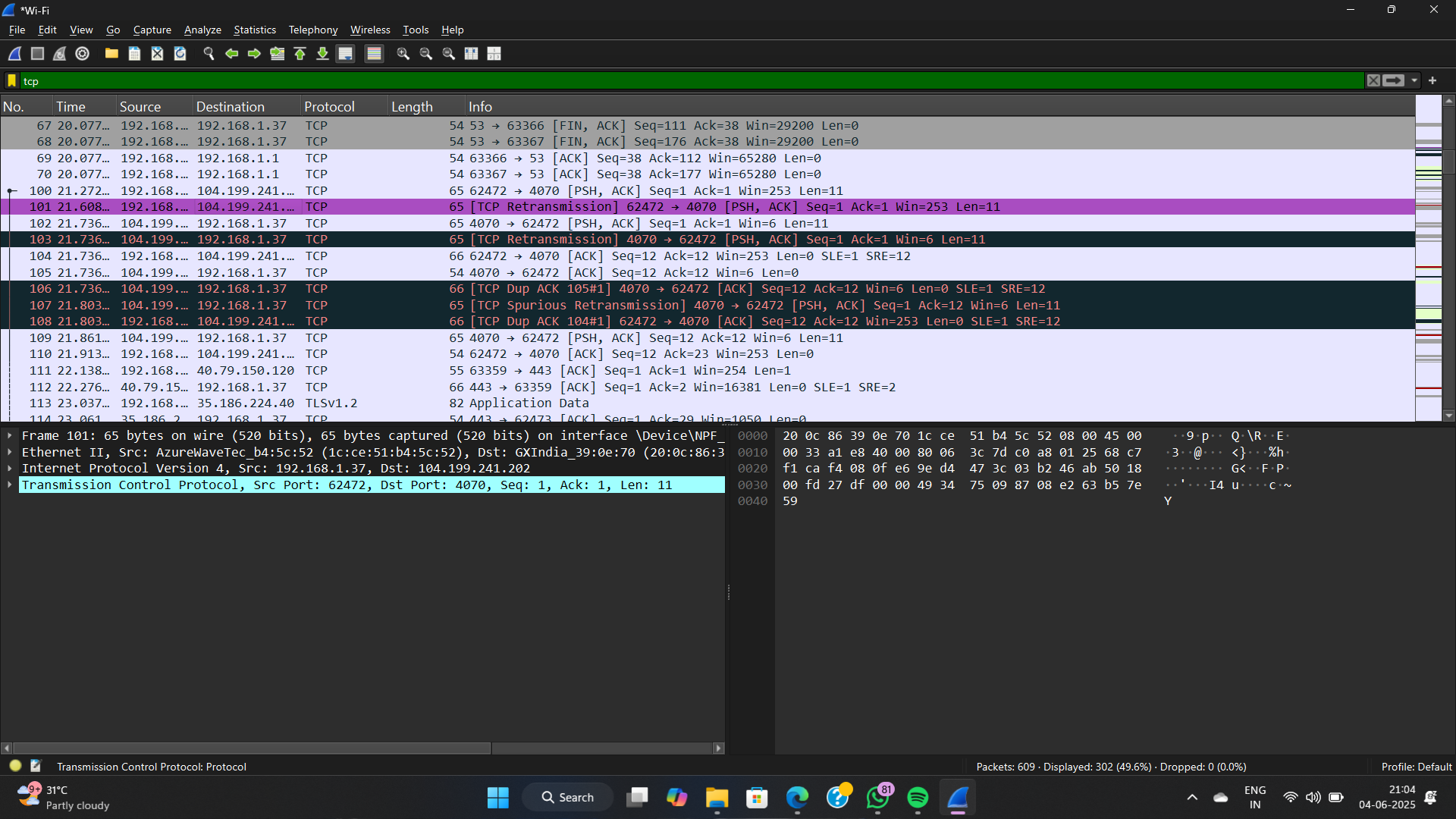
**TASK-5**

**Capture and Analyze Network Traffic Using Wireshark**

* **HTTP Packet Capturing**

****

* **UDP Packet Capturing**
* **TCP Packet Capturing**

****

**Protocol Scanning Report**

**Captured Using** : Wireshark  
**Date** : 04 June 2025  
**Location** : Local Network Capture on Interface Wi-Fi  
**Source System IP**: 192.168.1.37  
**Operating System**: Windows 11

**1. HTTP Protocol Analysis**

**Key Observations:**

* **Request Type**: GET
* **File Accessed**: /connecttest.txt
* **Host**: 43.228.93.82
* **HTTP Response**: HTTP/1.1 200 OK
* **Content Type**: text/plain
* **Response Data**: Microsoft Connect Test

**Technical Summary:**

| **Parameter** | **Value** |
| --- | --- |
| Source IP | 192.168.1.37 |
| Destination IP | 43.228.93.82 |
| Source Port | Dynamic (e.g., 63368) |
| Destination Port | 80 (HTTP) |
| Method | GET |
| Response Length | 241 bytes |
| Content-Length Header | 22 |

The HTTP traffic indicates an automatic connectivity test by the operating system to verify internet access, commonly seen in captive portal detection.

**2. UDP Protocol Analysis**

**Key Observations:**

* **Source IP**: 192.168.1.37
* **Destination IP**: 192.168.1.255 (Broadcast)
* **Source Port**: 57621
* **Destination Port**: 57621
* **Length**: 86 bytes
* **Payload Size**: 44 bytes

This is a UDP broadcast packet likely related to **local service discovery** or **connectivity testing** (possibly related to Windows network awareness).

**Interpretation:**

Broadcasted UDP traffic from a local client intended to discover available services or broadcast network information. It includes a DHCP and DNS query to www.msftconnecttest.com.

**3. TCP Protocol Analysis**

**Key Observations:**

* **Multiple TCP segments captured** including retransmissions and acknowledgments.
* **Notable communication** between:
  + Source: 192.168.1.37
  + Destination: 104.199.241.202 (Google Cloud-hosted server)
  + Ports: Source (62472), Destination (4070)
* **Sequence Analysis**:
  + Several [PSH, ACK], [ACK], and [TCP Dup ACK] packets.
  + Indications of packet loss or delays (retransmissions).
  + TLS traffic noted in further communication (TLSv1.2), suggesting an encrypted connection following TCP handshake.

**Technical Summary:**

| **Parameter** | **Value** |
| --- | --- |
| Protocol | TCP |
| Issues Detected | Retransmissions, Dup ACKs |
| Session Type | Possibly TLS handshake |
| Target IP | 104.199.241.202 |
| Dest Port | 4070 |

**Interpretation:**

The TCP traffic is consistent with application-level communication attempting to establish or maintain a secure session. The presence of retransmissions indicates either packet loss or delay in the network path.

**Conclusion**

The protocol scanning activity shows routine network behavior from a Windows 11 system:

* **HTTP**: Connectivity checks to Microsoft's test URL.
* **UDP**: Broadcast for service discovery and DHCP operations.
* **TCP**: Secure communication sessions with retransmissions, likely due to unstable connectivity or network congestion.

Report by : **Guthula Dharma Sai Ram**

Date : **04/06/2025**