# **NETWORK PACKET ANALYSIS**

# **USING**

# **WIRESHARK**

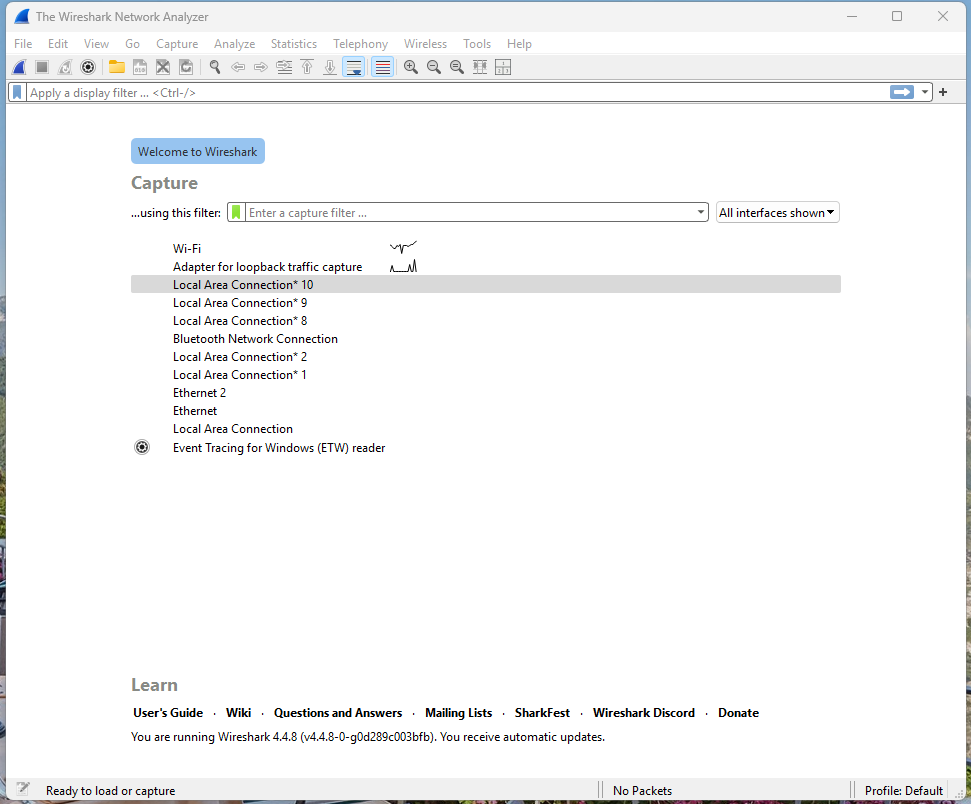
PREPARED BY : LOVEPREET SINGH

BTECH 7TH SEMSTER

TOPIC - NETWORK SECURITY ANALYSIS

# **SETUP**

* **Capture Interface** : WiFi (en0)
* **No of packets Captured :** 15545
* **File Name :** Network\_packets.png

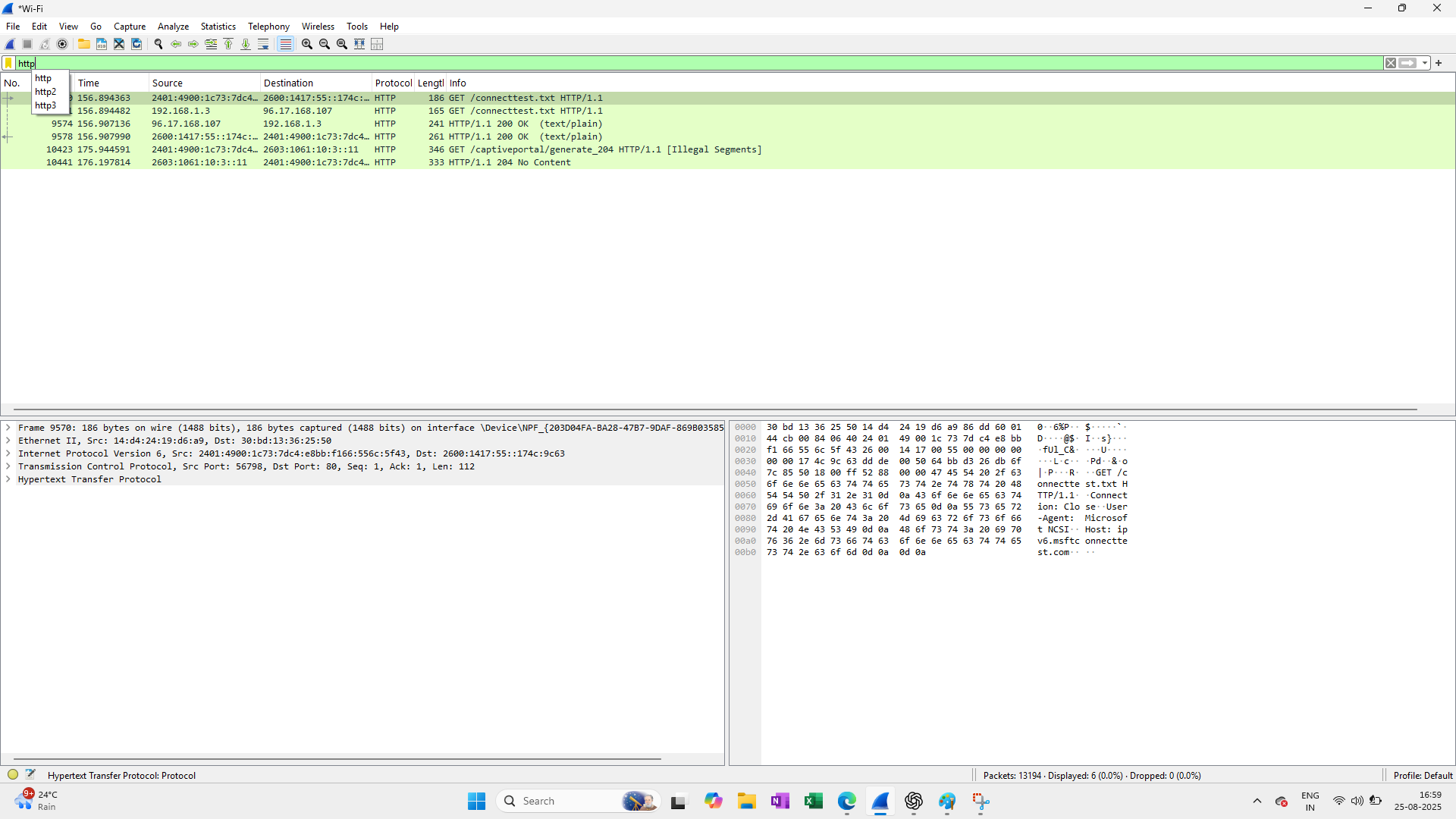
\

# **FINDINGS**

## 🔹 **HTTP Filters**

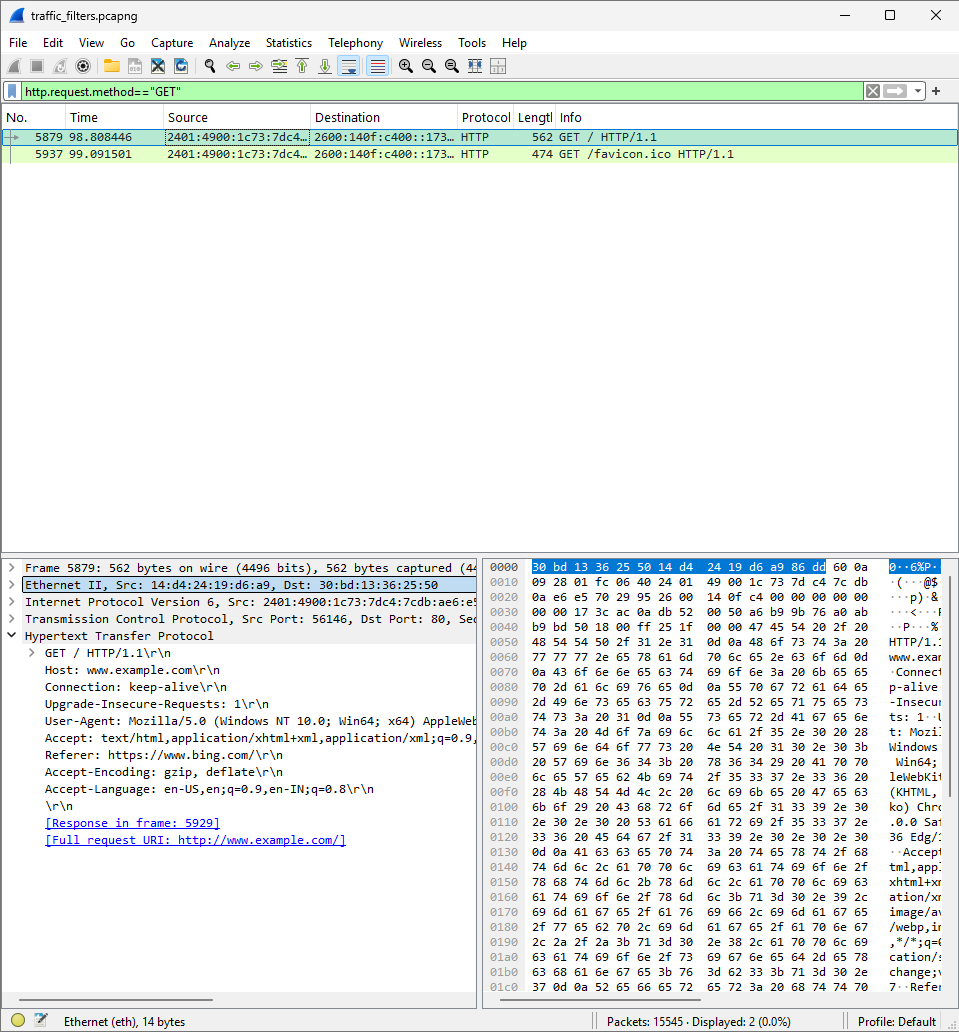
1. **Filter Used:** http

* **Observation:** Captures all HTTP traffic (requests and responses).
* **Security Risk:** HTTP is unencrypted; attackers can sniff usernames, passwords, and data.
* **Recommendation:** Replace HTTP with HTTPS; block plaintext HTTP if possible.



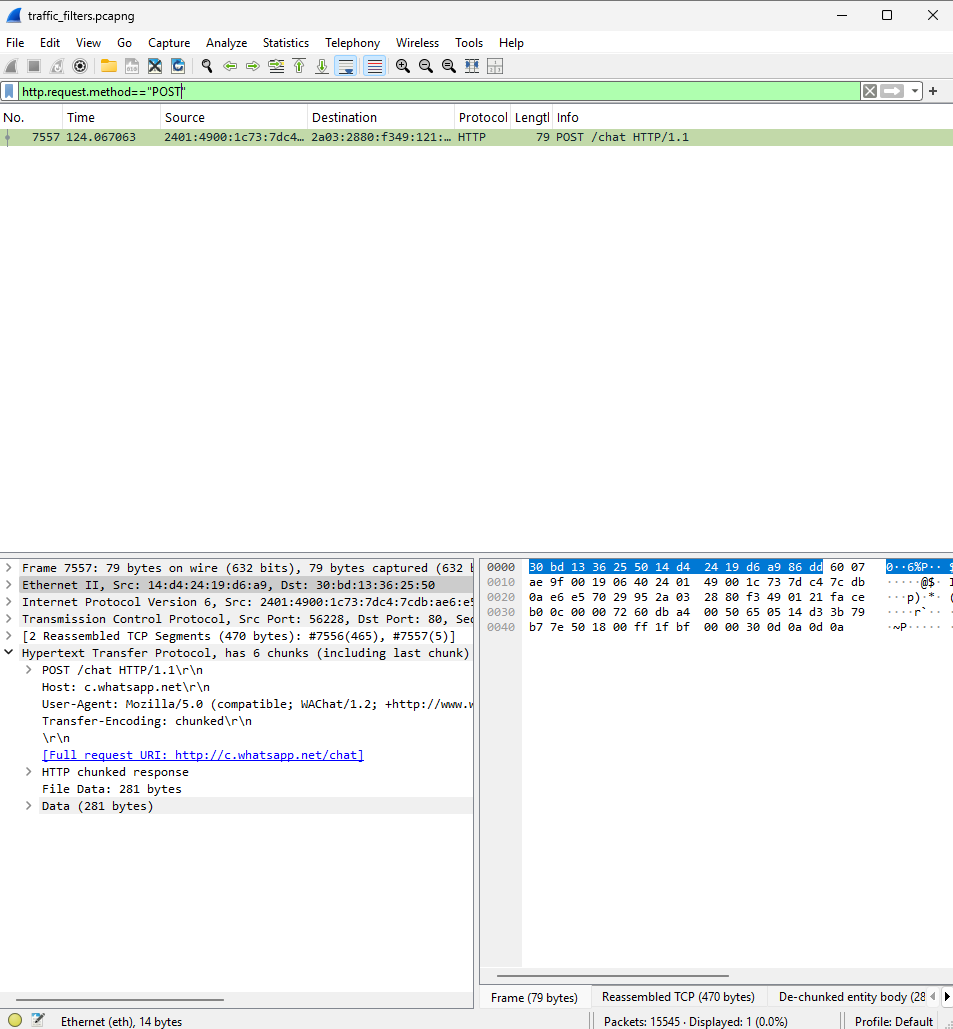
1. **Filter Used:** http.request.method == "GET"

* **Observation:** Shows all GET requests (retrieving resources).
* **Security Risk:** Sensitive information may be leaked in URL query strings (e.g., tokens, session IDs).
* **Recommendation:** Avoid sending sensitive data in GET requests; enforce POST with encryption.

****

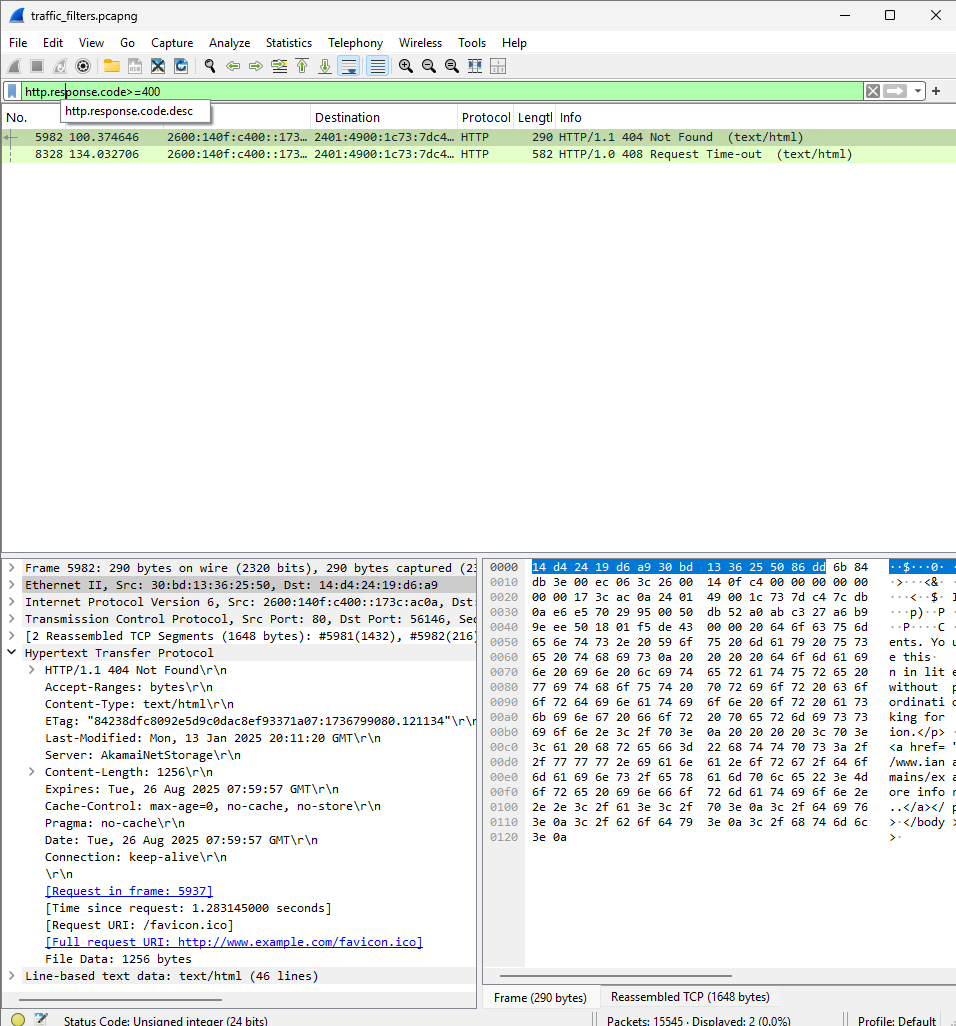
1. **Filter Used:** http.request.method == "POST"

* **Observation:** Captures POST requests (data submissions).
* **Security Risk:** If unencrypted, sensitive form data (credentials, personal data) may be exposed.
* **Recommendation:** Ensure POST requests are always sent via HTTPS.



1. **Filter Used:** http.response.code >= 400

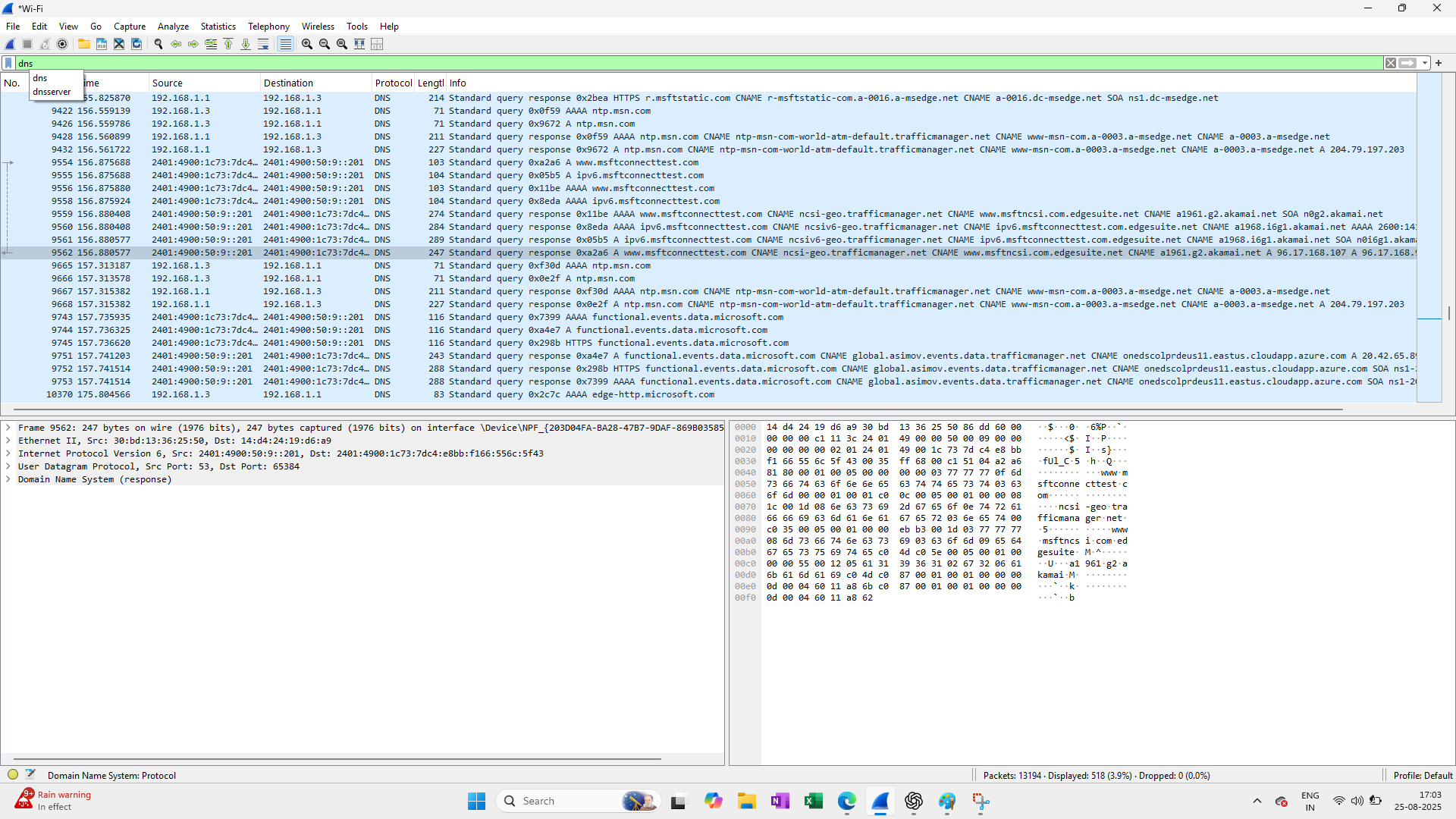
* **Observation:** Identifies error responses (client and server errors).
* **Security Risk:** Frequent 500-series errors may expose server misconfigurations; 404 scans could indicate reconnaissance attempts.
* **Recommendation:** Monitor error patterns and harden servers against scans.



**🔹 DNS Filters**

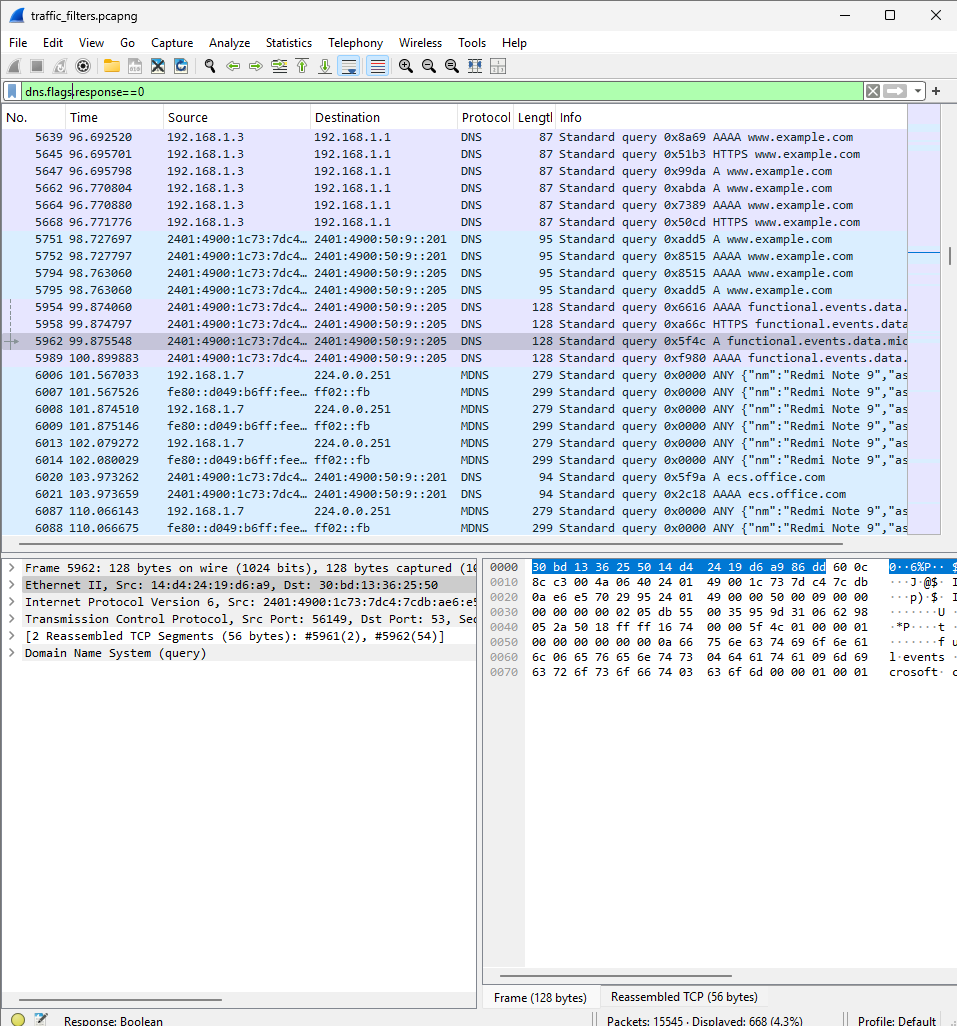
**1) Filter Used:** dns

* **Observation:** Captures all DNS queries and responses.
* **Security Risk:** Attackers can perform DNS tunneling or track domains being queried.
* **Recommendation:** Enable DNSSEC or encrypted DNS (DoH/DoT).



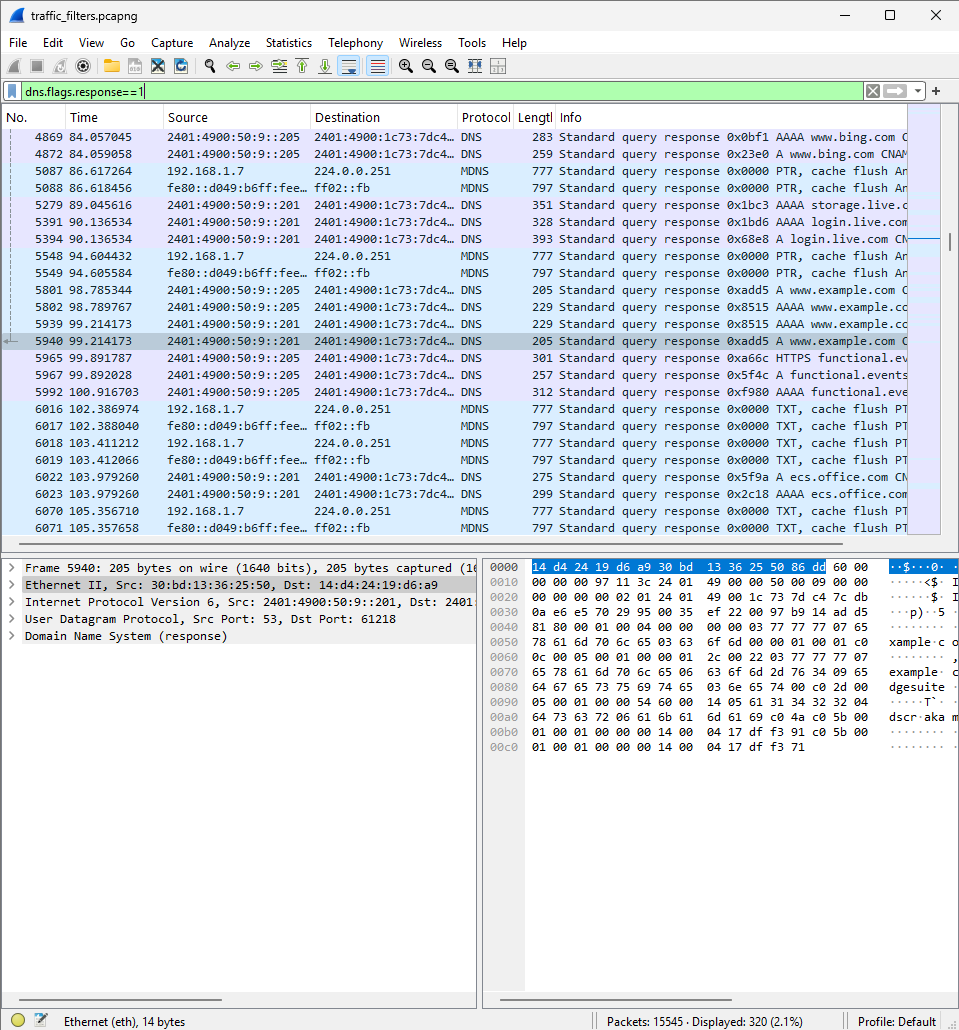
**2) Filter Used:** dns.flags.response == 0

* **Observation:** Shows DNS queries.
* **Security Risk:** High query volume may indicate malware beaconing to C2 domains.
* **Recommendation:** Monitor unusual query spikes and block suspicious domains.



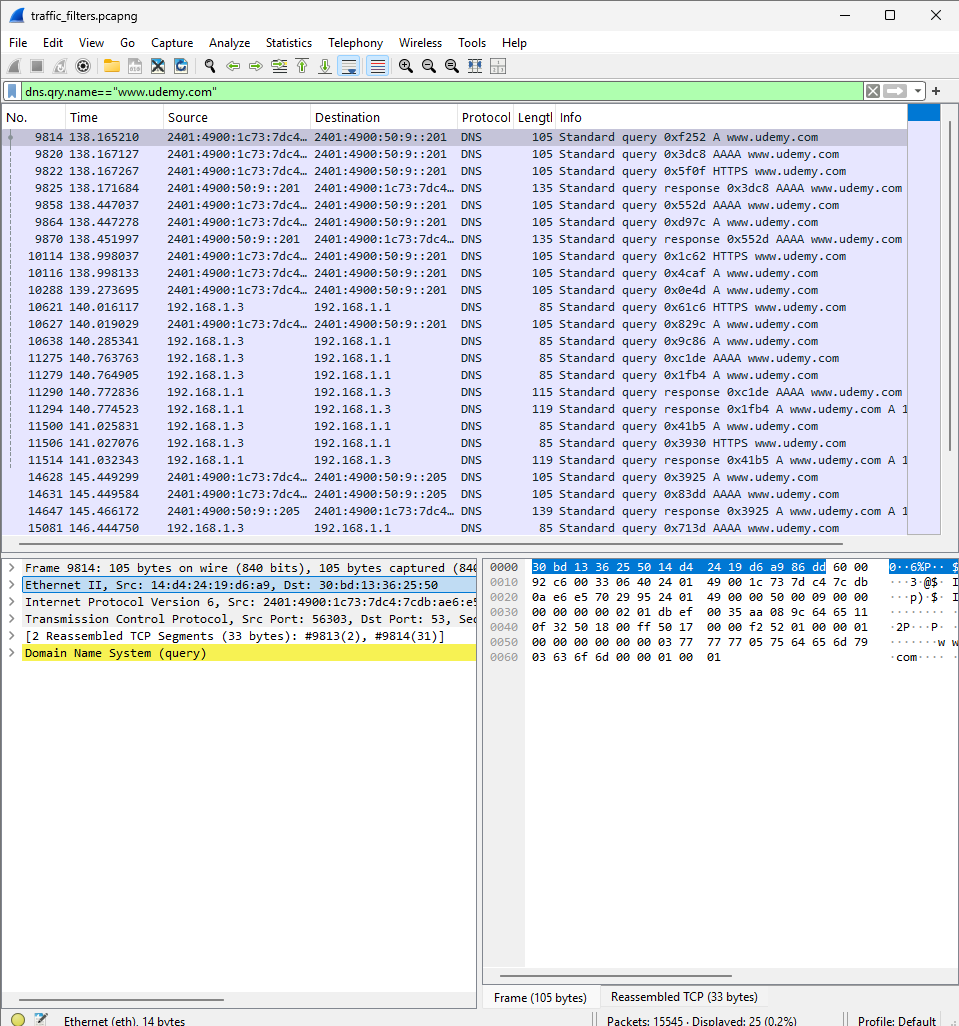
**3) Filter Used:** dns.flags.response == 1

* **Observation:** Shows DNS responses.
* **Security Risk:** Malicious responses can redirect users to fake IPs (DNS spoofing).
* **Recommendation:** Use DNSSEC and trusted resolvers.

****

**4)Filter Used:** dns.qry.name == "www.example.com"

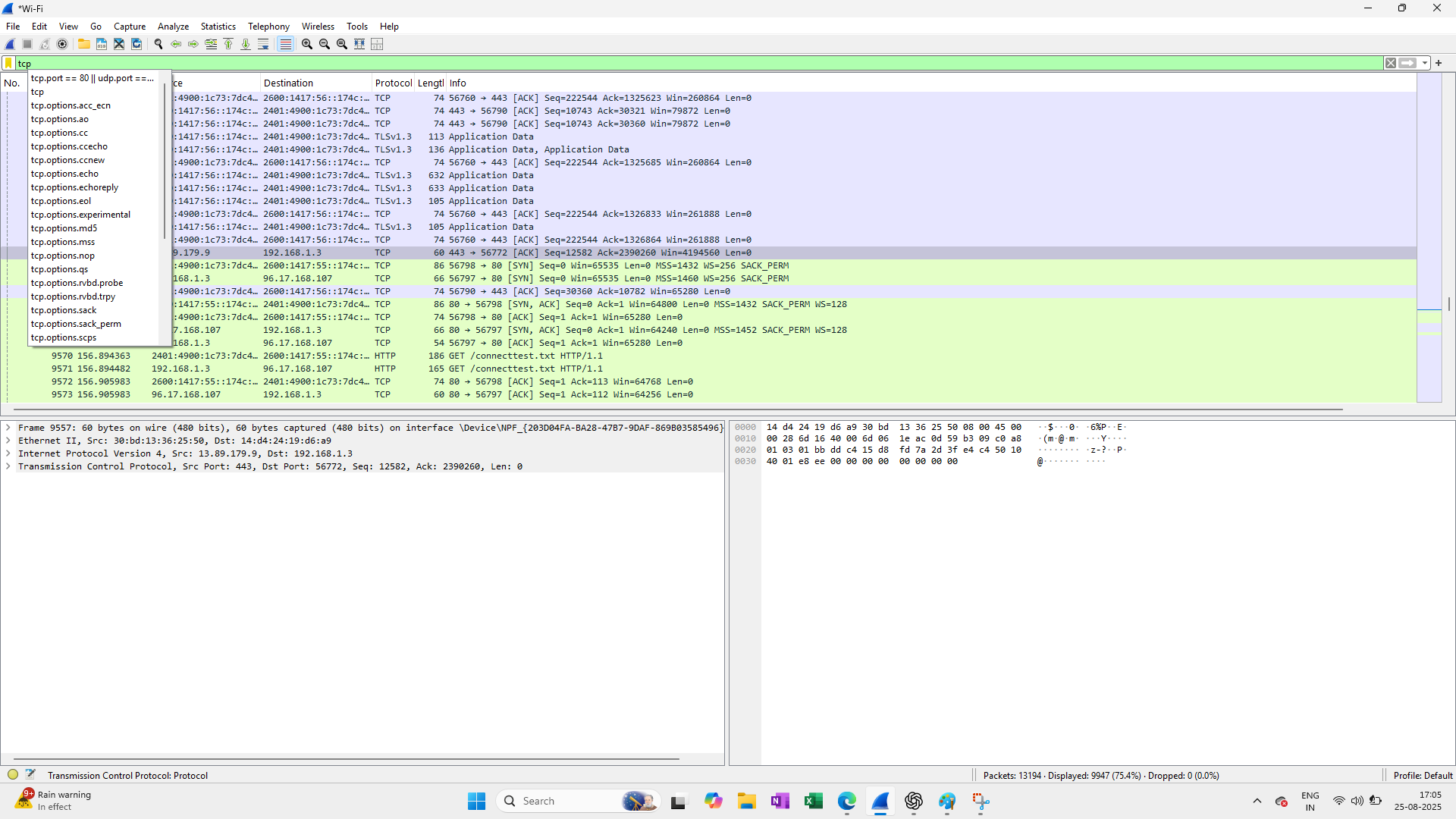
* **Observation:** Filters queries for a specific domain.
* **Security Risk:** Could reveal targeted reconnaissance on particular domains.
* **Recommendation:** Monitor sensitive domains frequently queried inside the network.



**🔹 TCP Filters**

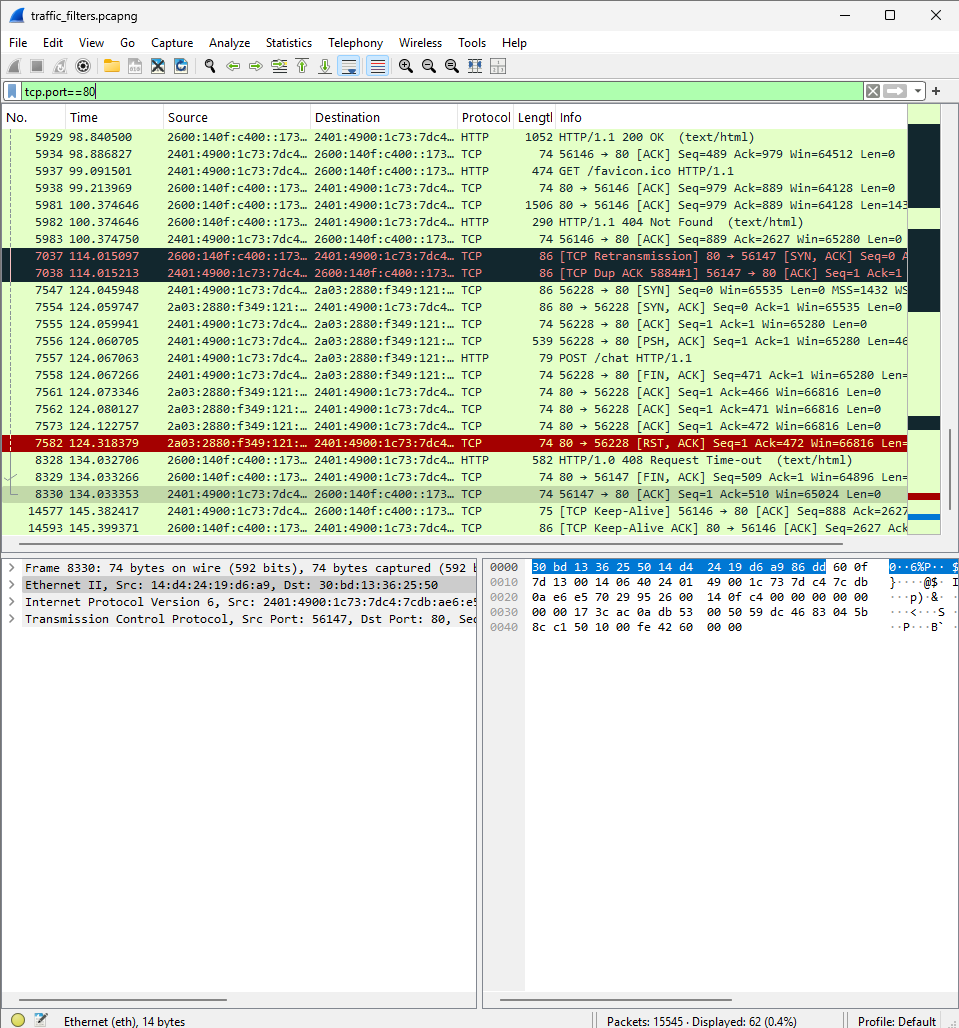
**Filter Used:** tcp

* **Observation:** Captures all TCP traffic.
* **Security Risk:** High traffic volume could hide scans, brute-force attempts, or data exfiltration.
* **Recommendation:** Baseline normal TCP traffic; alert on anomalies.



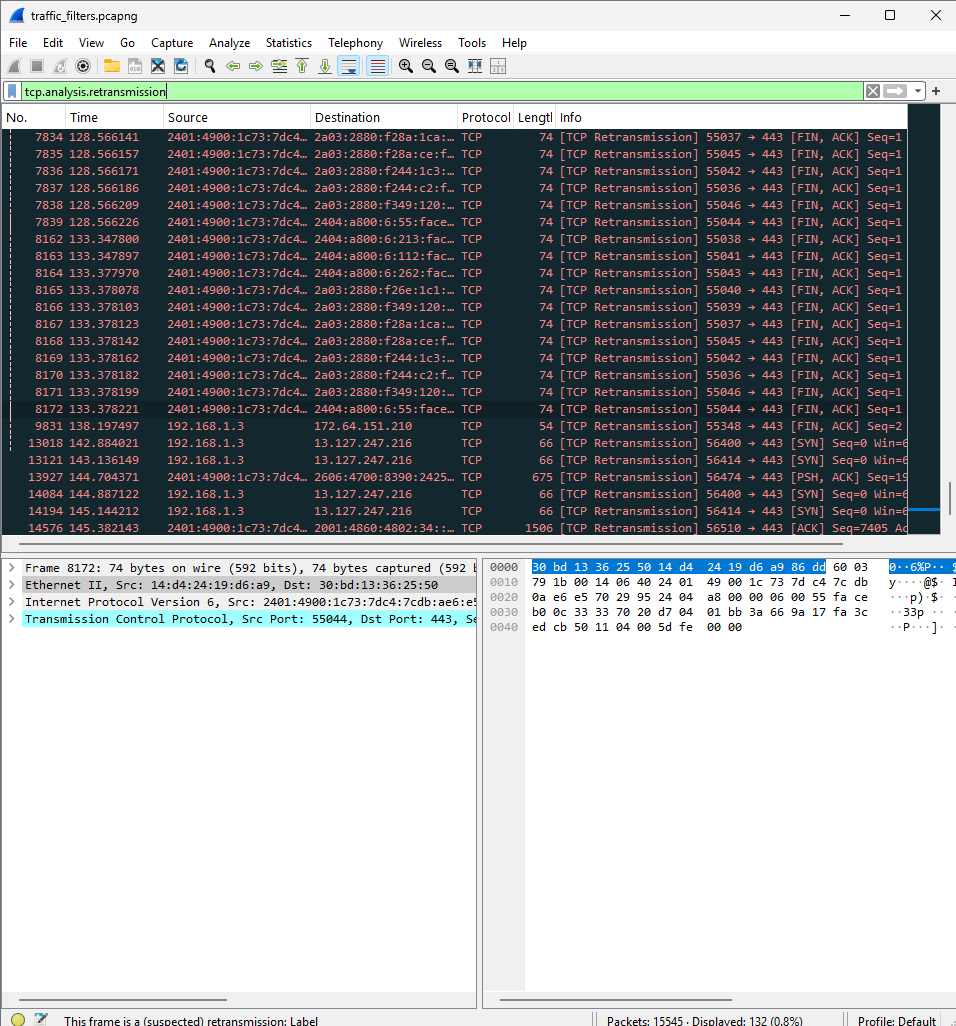
**Filter Used:** tcp.port == 80

* **Observation:** Captures traffic on port 80 (HTTP).
* **Security Risk:** Plaintext communication vulnerable to sniffing or man-in-the-middle attacks.
* **Recommendation:** Redirect all port 80 traffic to HTTPS (443).

****

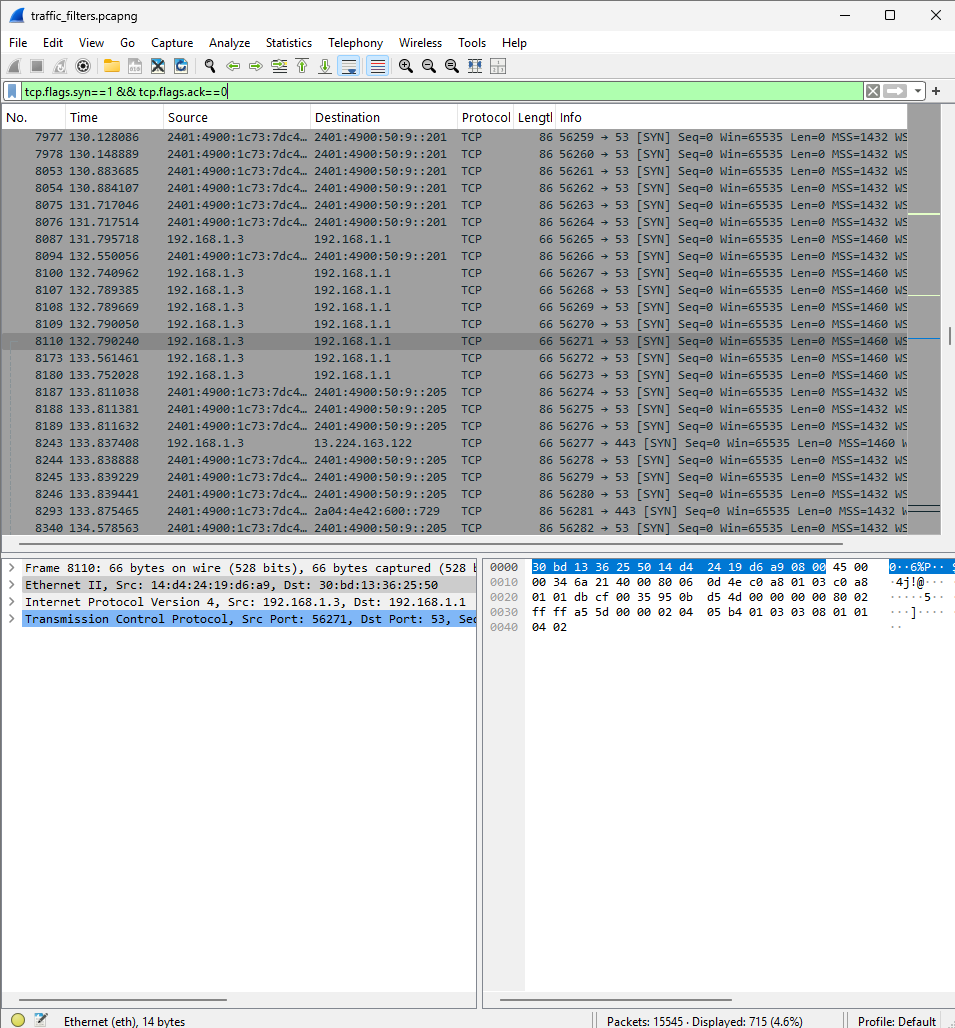
**Filter Used:** tcp.analysis.retransmission

* **Observation:** Identifies TCP retransmissions (potential packet loss or congestion).
* **Security Risk:** May indicate DoS attacks, poor network quality, or misconfigured devices.
* **Recommendation:** Investigate high retransmission rates; optimize routing/firewall rules.

****

**Filter Used:** tcp.flags.syn == 1 && tcp.flags.ack == 0

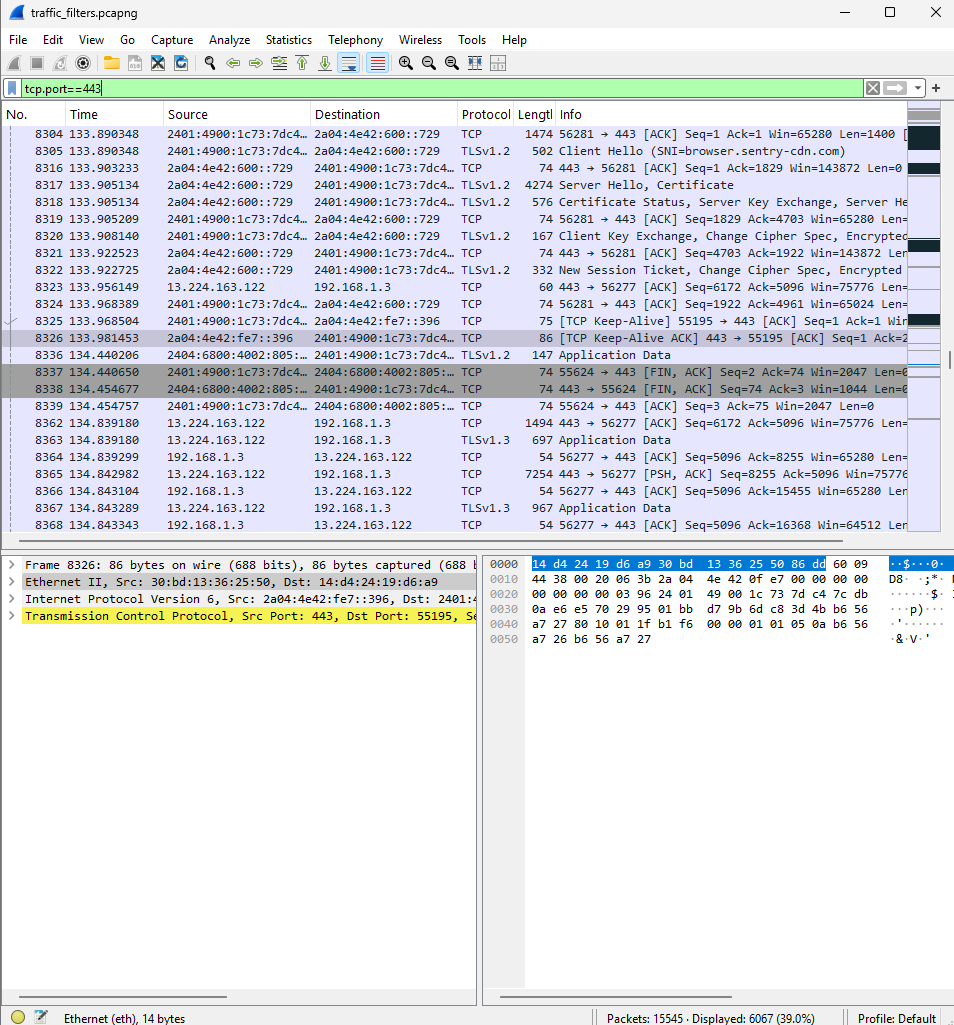
* **Observation:** Captures initial SYN packets (connection attempts).
* **Security Risk:** A high volume of SYN packets may indicate SYN flood (DoS attack).
* **Recommendation:** Deploy SYN cookies and monitor for abnormal SYN patterns.



**🔹 TLS/HTTPS Filters**

**Filter Used:** tcp.port == 443

* **Observation:** Captures HTTPS traffic.
* **Security Risk:** Content is encrypted, but metadata (IP, SNI, timing) can still leak info.
* **Recommendation:** Inspect TLS metadata; ensure modern cipher suites.

****

**Filter Used:** ssl.handshake

* **Observation:** Captures TLS handshake messages (certificates, key exchange).
* **Security Risk:** Weak ciphers or expired certificates weaken encryption.
* **Recommendation:** Enforce TLS 1.2+ and disable weak ciphers.

