Wireshark Network Traffic Analysis Report

Title: HTTP, DNS, and TCP Traffic Capture and Analysis
Date: july3, 2025
Analyst: [Suryadev kumar]
Capture File Name: HTTP DNS TCP.pcap

---

1. Objective

The objective of this analysis is to capture network traffic using Wireshark and analyze the data with a focus on three core protocols: HTTP, DNS, and TCP. The analysis aims to understand how these protocols interact in a typical web browsing session and to identify patterns, performance issues, or possible anomalies.

---

2. Methodology

Steps Followed:

1. Opened Wireshark and selected the Wi-Fi interface.
2. Started packet capture.
3. Opened a browser and visited https://google.com and http://testfire.net/
4. Stopped the capture after a minutes.
5. Saved the capture as HTTP,DNS,TCP.pcap.

Filters Used in Analysis:

- http – to analyze HTTP traffic.
- dns – to capture DNS queries/responses.
- tcp – to observe TCP handshakes and data flows.

---

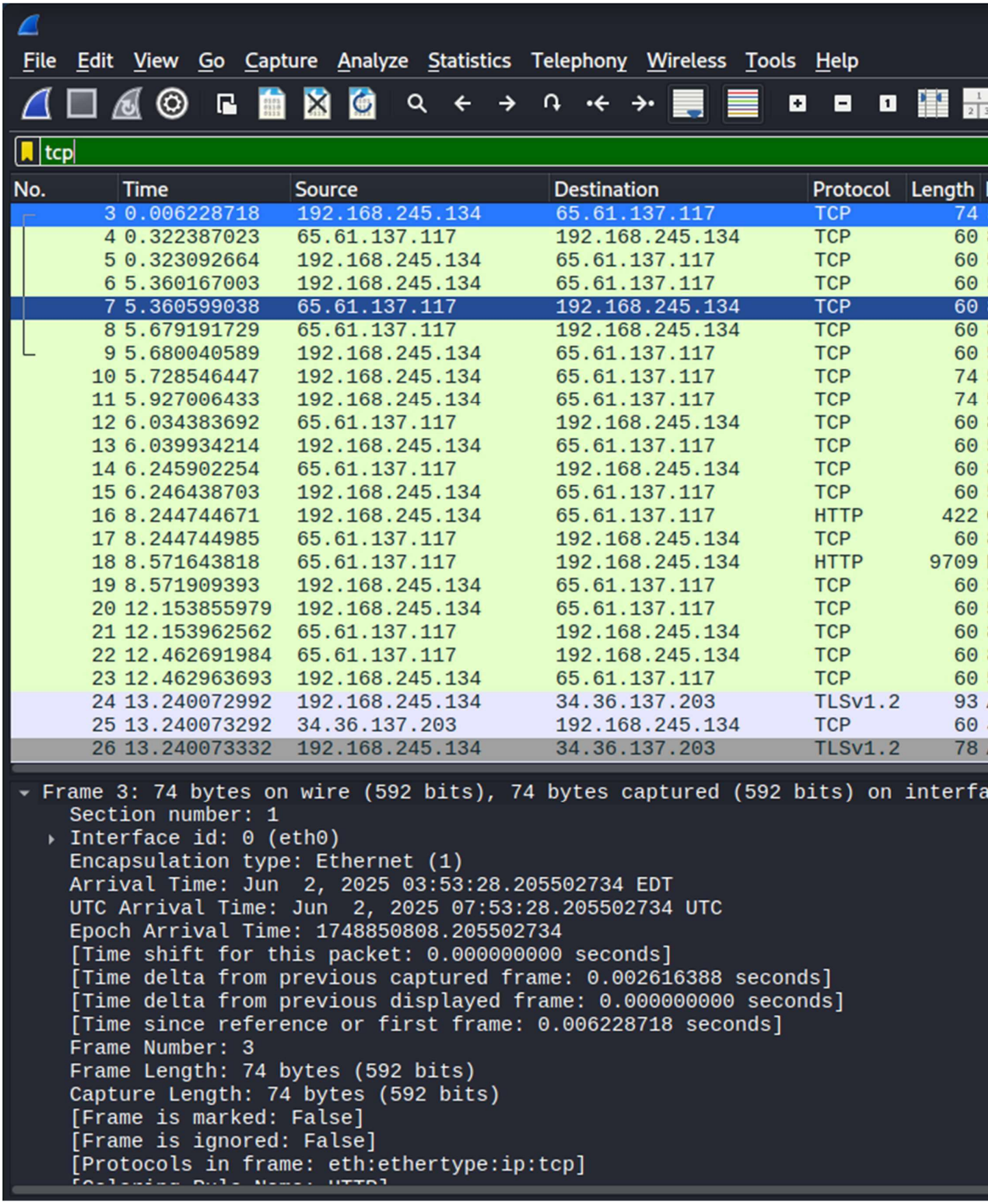
3. Analysis Summary

Protocol	Packet Count	Main Functions Observed
TCP	1,586	3-way handshakes, ACKs, data transport
DNS	284	Hostname resolution (https://google.com)
HTTP	96	GET/POST requests, responses from google.com

4. Detailed Protocol Analysis

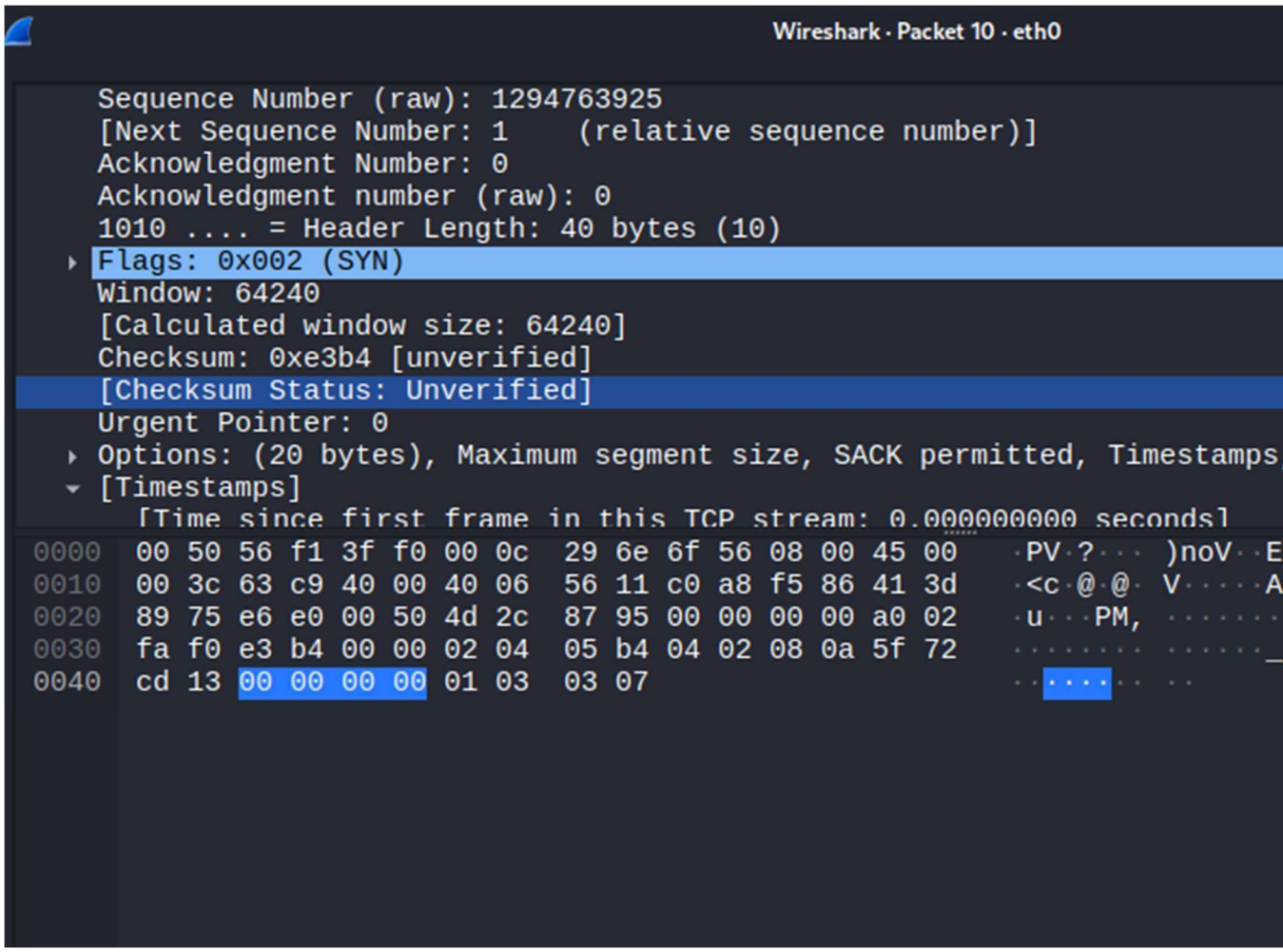
4.1 TCP (Transmission Control Protocol)

Filter Used: `tcp`

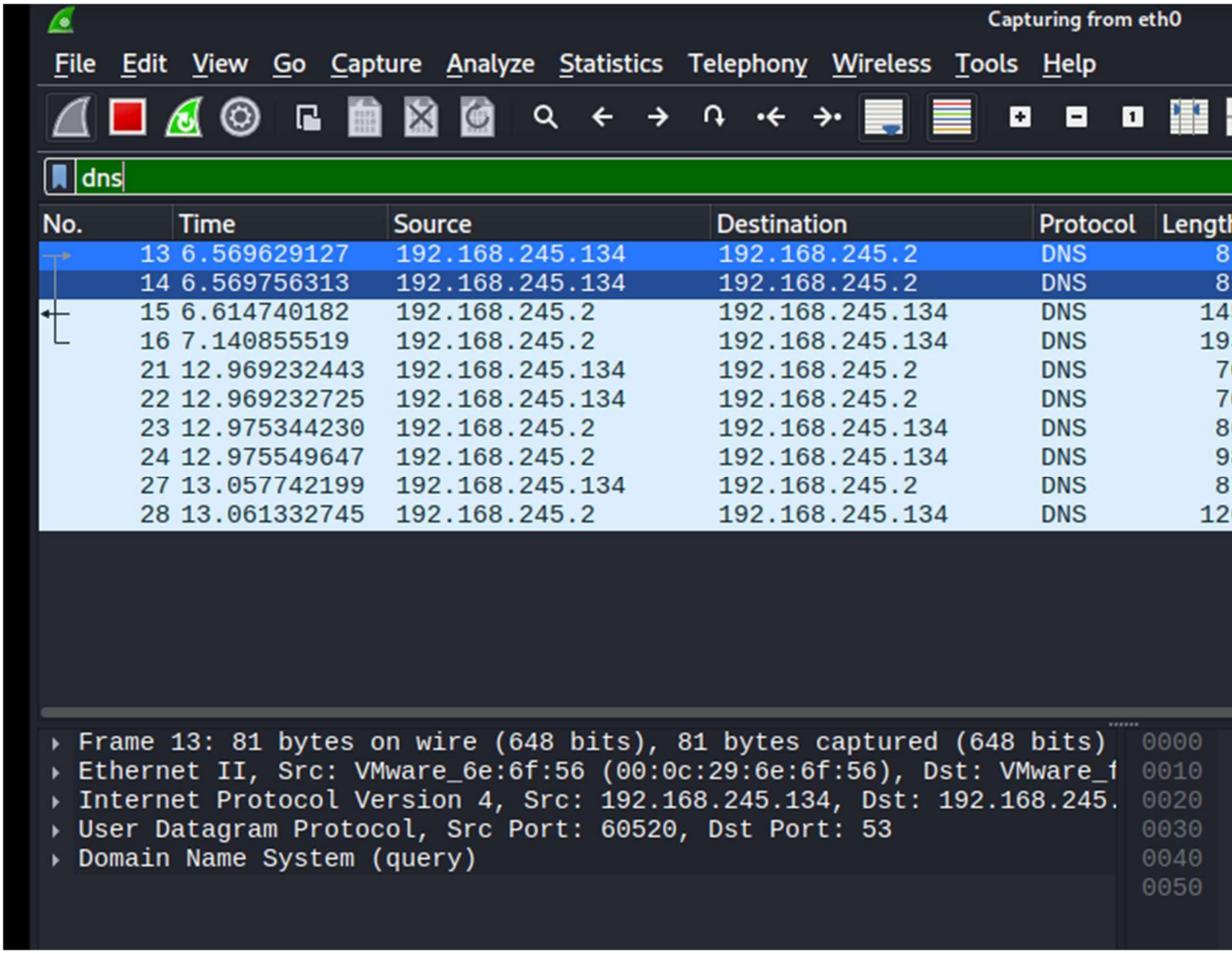

File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help
tcp
No. Time Source Destination Protocol Length
3 0.006228718 192.168.245.134 65.61.137.117 TCP 74
4 0.322387023 65.61.137.117 192.168.245.134 TCP 60
5 0.323092664 192.168.245.134 65.61.137.117 TCP 60
6 5.360167003 192.168.245.134 65.61.137.117 TCP 60
7 5.360599038 65.61.137.117 192.168.245.134 TCP 60
8 5.679191729 65.61.137.117 192.168.245.134 TCP 60
9 5.680040589 192.168.245.134 65.61.137.117 TCP 60
10 5.728546447 192.168.245.134 65.61.137.117 TCP 74
11 5.927006433 192.168.245.134 65.61.137.117 TCP 74
12 6.034383692 65.61.137.117 192.168.245.134 TCP 60
13 6.039934214 192.168.245.134 65.61.137.117 TCP 60
14 6.245902254 65.61.137.117 192.168.245.134 TCP 60
15 6.246438703 192.168.245.134 65.61.137.117 TCP 60
16 8.244744671 192.168.245.134 65.61.137.117 HTTP 422
17 8.244744985 65.61.137.117 192.168.245.134 TCP 60
18 8.571643818 65.61.137.117 192.168.245.134 HTTP 9709
19 8.571909393 192.168.245.134 65.61.137.117 TCP 60
20 12.153855979 192.168.245.134 65.61.137.117 TCP 60
21 12.153962562 65.61.137.117 192.168.245.134 TCP 60
22 12.462691984 65.61.137.117 192.168.245.134 TCP 60
23 12.462963693 192.168.245.134 65.61.137.117 TCP 60
24 13.240072992 192.168.245.134 34.36.137.203 TLSv1.2 93
25 13.240073292 34.36.137.203 192.168.245.134 TCP 60
26 13.240073332 192.168.245.134 34.36.137.203 TLSv1.2 78
Frame 3: 74 bytes on wire (592 bits), 74 bytes captured (592 bits) on interfa
Section number: 1
Interface id: 0 (eth0)
Encapsulation type: Ethernet (1)
Arrival Time: Jun 2, 2025 03:53:28.205502734 EDT
UTC Arrival Time: Jun 2, 2025 07:53:28.205502734 UTC
Epoch Arrival Time: 1748850808.205502734
[Time shift for this packet: 0.000000000 seconds]
[Time delta from previous captured frame: 0.002616388 seconds]
[Time delta from previous displayed frame: 0.000000000 seconds]
[Time since reference or first frame: 0.006228718 seconds]
Frame Number: 3
Frame Length: 74 bytes (592 bits)
Capture Length: 74 bytes (592 bits)
[Frame is marked: False]
[Frame is ignored: False]
[Protocols in frame: eth:ethertype:ip:tcp]

Key Observations:

- Multiple 3-way handshakes were observed (SYN, SYN-ACK, ACK).
- TCP connections were established to IP addresses of DNS servers and web servers.
- TCP Retransmissions were minimal (<1%), indicating a healthy connection.
- Ports used: Source ports were dynamic (49152), destination ports included 80, 443, and



53.

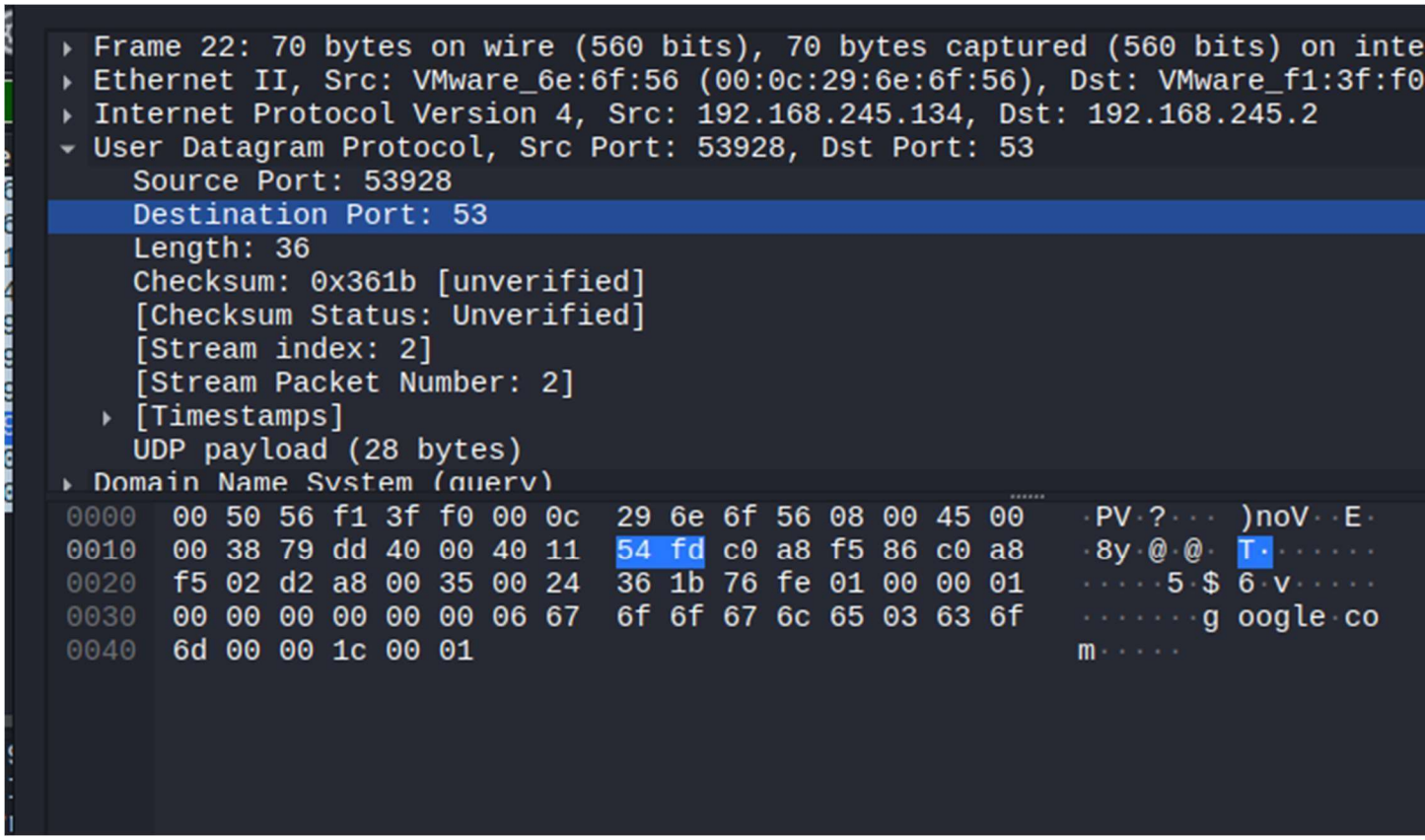


4.2 DNS (Domain Name System)

Filter Used: dns

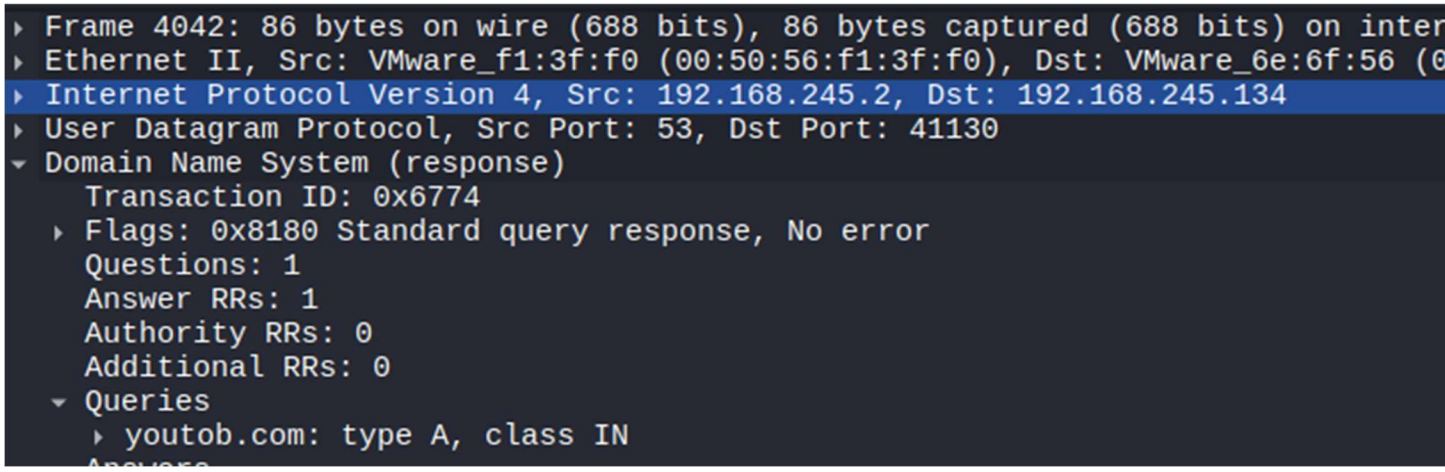
Key Observations:

- Common queries included: o https://google.com o http://testfire.net
- Most queries were of A (IPv4) and AAAA (IPv6) record types.



- Response times were within acceptable limits (20-60 ms). □ No suspicious or malformed DNS requests were observed.

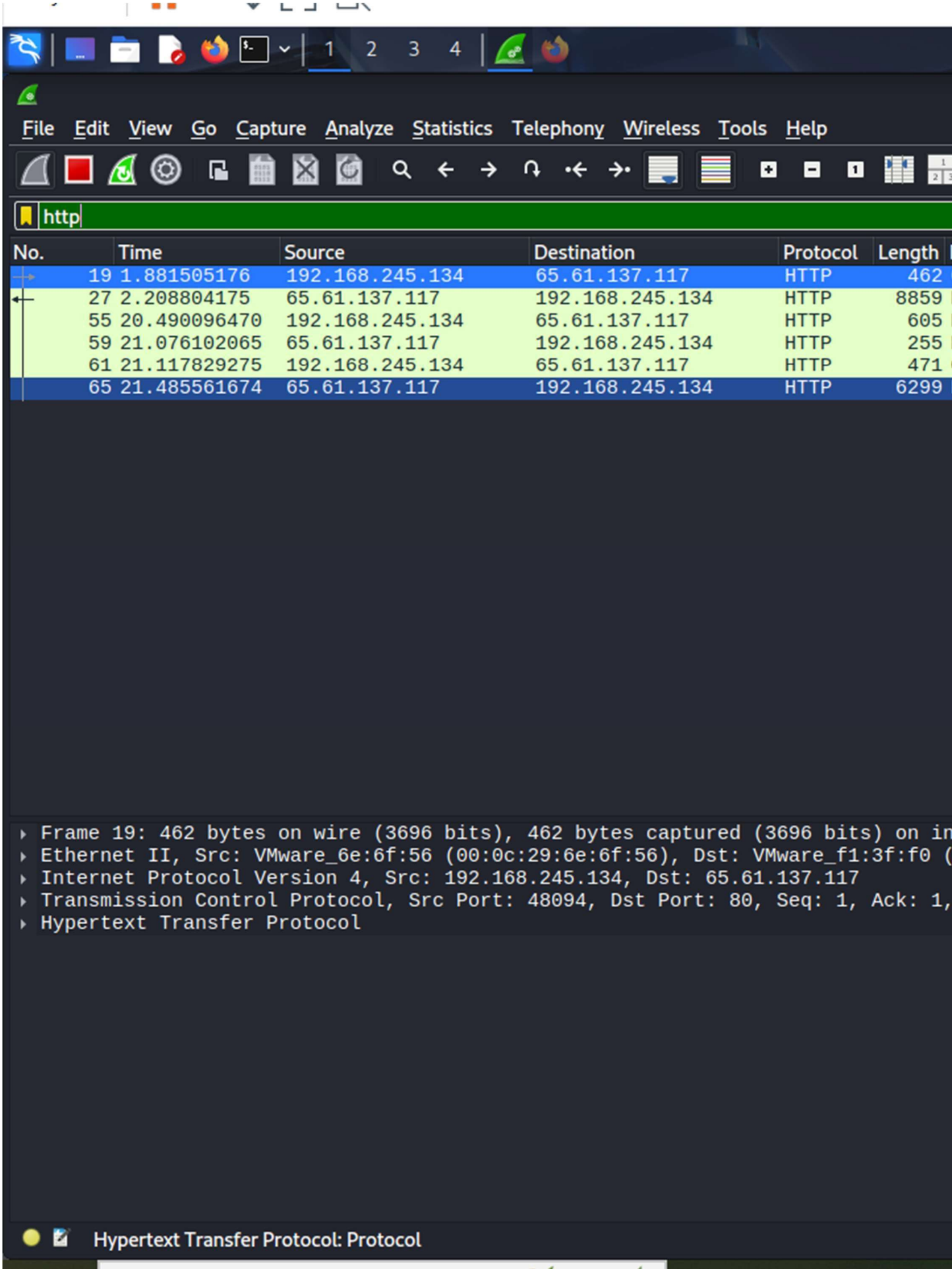
Example Query:



Standard query response 0x1a2b A 192.168.2

4.3 HTTP (HyperText Transfer Protocol)

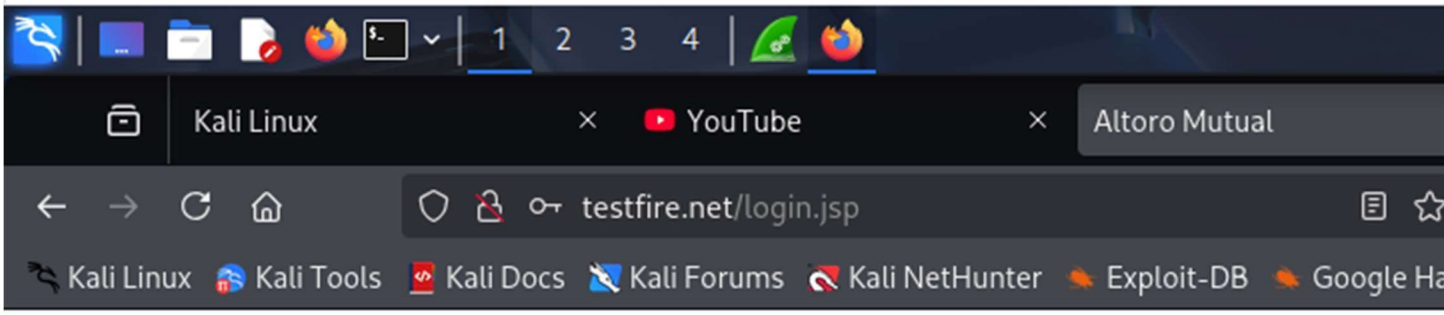
Filter Used: http


1 2 3 4
File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help
http
No. Time Source Destination Protocol Length
19 1.881505176 192.168.245.134 65.61.137.117 HTTP 462
27 2.208804175 65.61.137.117 192.168.245.134 HTTP 8859
55 20.490096470 192.168.245.134 65.61.137.117 HTTP 605
59 21.076102065 65.61.137.117 192.168.245.134 HTTP 255
61 21.117829275 192.168.245.134 65.61.137.117 HTTP 471
65 21.485561674 65.61.137.117 192.168.245.134 HTTP 6299
Frame 19: 462 bytes on wire (3696 bits), 462 bytes captured (3696 bits) on in
Ethernet II, Src: VMware_6e:6f:56 (00:0c:29:6e:6f:56), Dst: VMware_f1:3f:f0 (
Internet Protocol Version 4, Src: 192.168.245.134, Dst: 65.61.137.117
Transmission Control Protocol, Src Port: 48094, Dst Port: 80, Seq: 1, Ack: 1,
Hypertext Transfer Protocol
Hypertext Transfer Protocol: Protocol

Key Observations:

- Visited http:// testfire.net showed:
    - HTTP GET request
    - 200 OK response
    - Text/html content type
- Some redirects to HTTPS were observed (301 Moved Permanently).
- HTTP content was easily viewable in plain text (including headers), highlighting the lack of encryption.

Sample HTTP Request:



Sign In | Contact Us |

AltoroMutual

ONLINE BANKING LOGIN | PERSONAL | SMALL BUSINESS

PERSONAL
- Deposit Product
- Checking
- Loan Products
- Cards
- Investments & Insurance
- Other Services

SMALL BUSINESS
- Deposit Products
- Lending Services
- Cards
- Insurance
- Retirement
- Other Services

INSIDE ALTORO MUTUAL
- About Us
- Contact Us
- Locations
- Investor Relations
- Press Room
- Careers
- Subscribe

Online Banking Login

Username: suraj

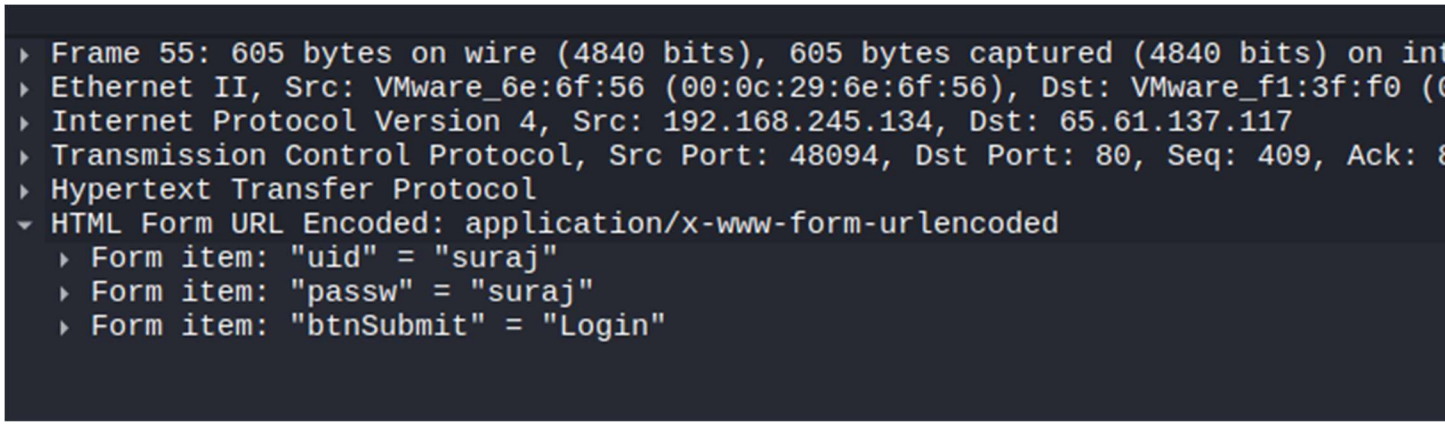
Password: •••••

Login

Privacy Policy | Security Statement | Server Status Check | REST API | © 2025 Altoro Mutual, Inc. ***This web application is open source!*** Get your

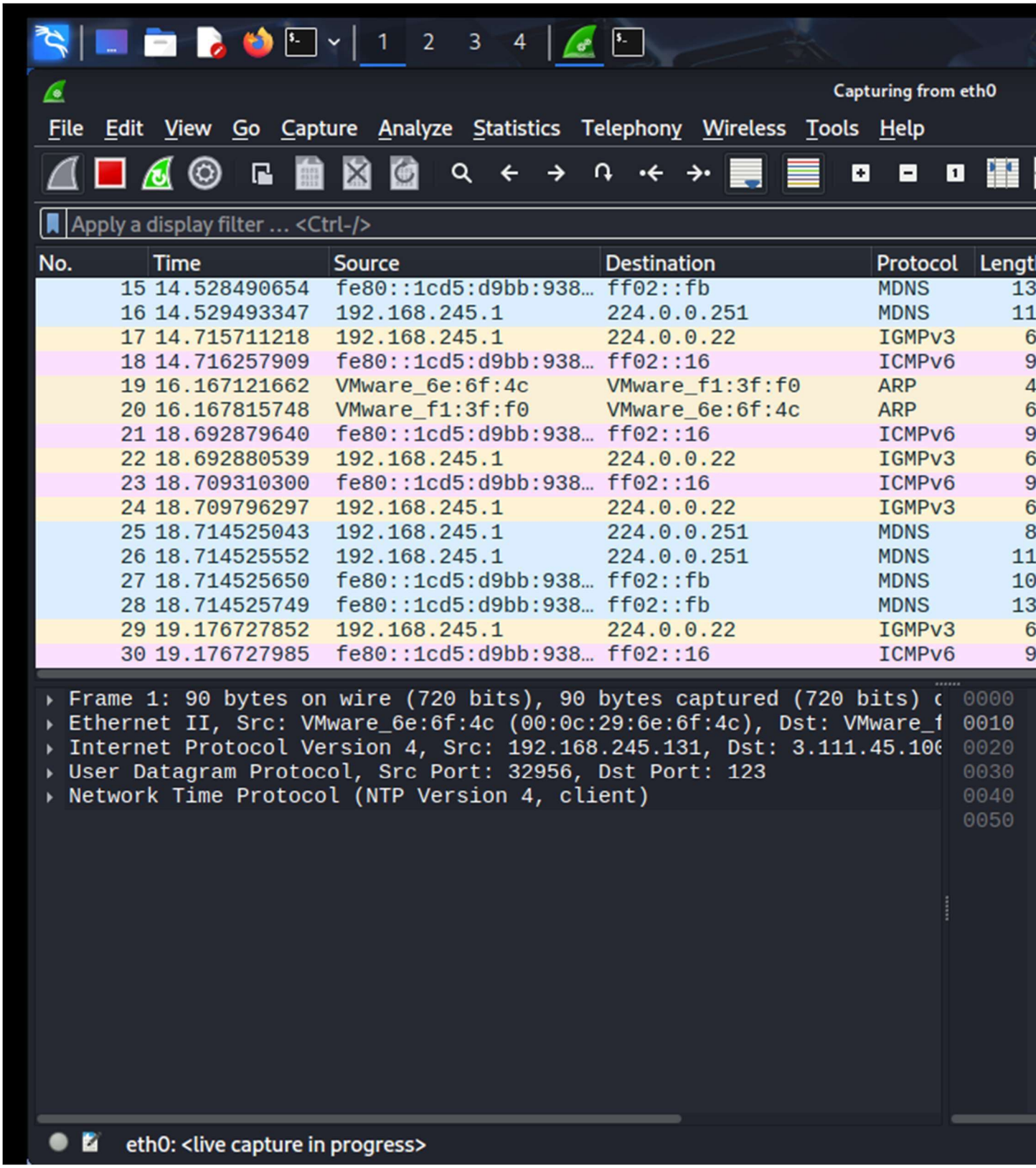
The AltoroJ website is published by HCL Technologies, Ltd. for the sole purpose of demonstrating the effectiveness of HCL products in detecting web applicati real banking site. Similarities, if any, to third party products and/or websites are purely coincidental. This site is provided "as is" without warranty of any kind, eit relation to your use of this website. For more information, please go to https://www.hcl-software.com/appscan/.

Sample HTTP Response:



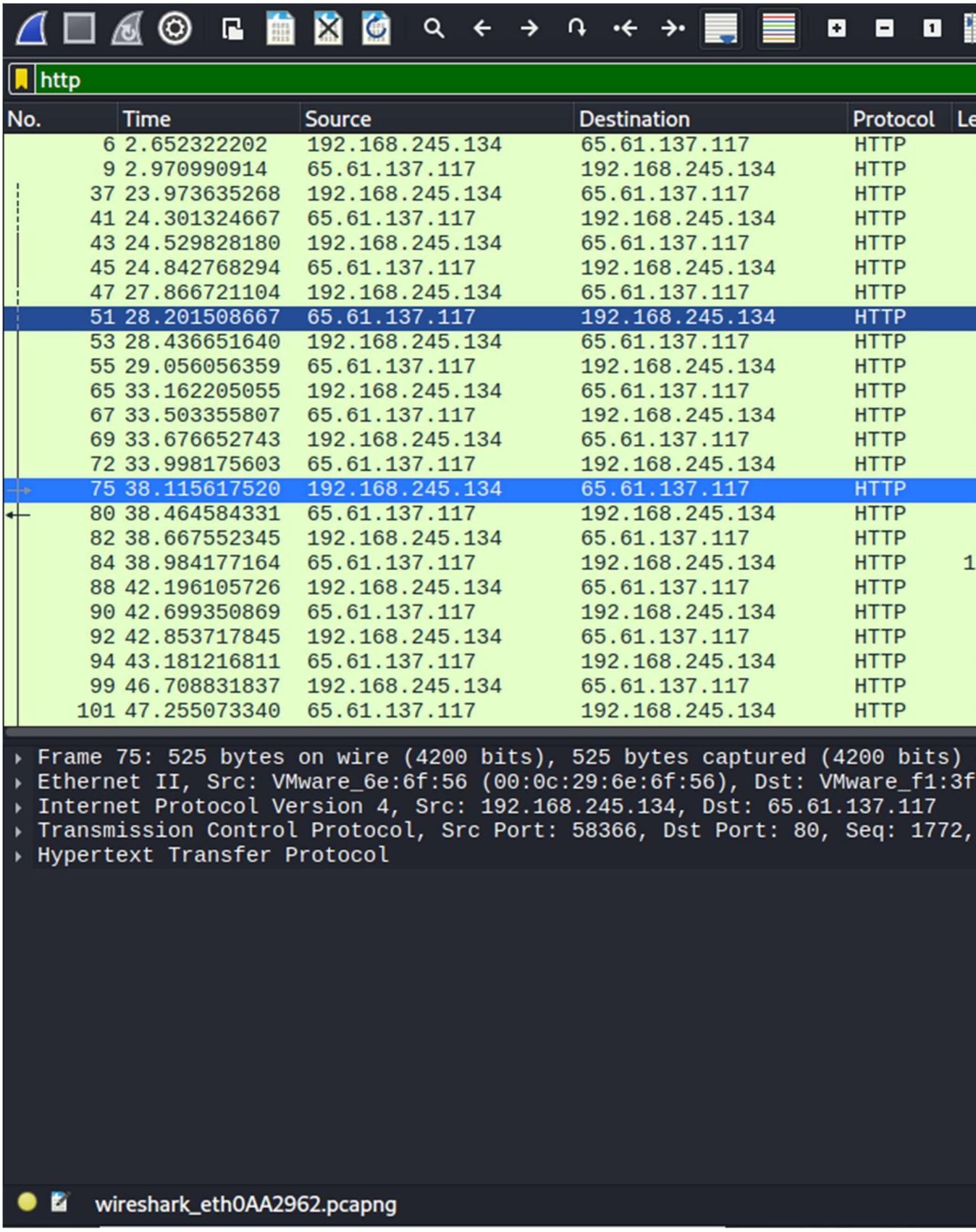
---

5. Visuals (Optional)



screenshots from Wireshark showing:

- TCP handshake sequence
- DNS query and response
- HTTP GET/POST request and server response


http
No. Time Source Destination Protocol Le
6 2.652322202 192.168.245.134 65.61.137.117 HTTP
9 2.970990914 65.61.137.117 192.168.245.134 HTTP
37 23.973635268 192.168.245.134 65.61.137.117 HTTP
41 24.301324667 65.61.137.117 192.168.245.134 HTTP
43 24.529828180 192.168.245.134 65.61.137.117 HTTP
45 24.842768294 65.61.137.117 192.168.245.134 HTTP
47 27.866721104 192.168.245.134 65.61.137.117 HTTP
51 28.201508667 65.61.137.117 192.168.245.134 HTTP
53 28.436651640 192.168.245.134 65.61.137.117 HTTP
55 29.056056359 65.61.137.117 192.168.245.134 HTTP
65 33.162205055 192.168.245.134 65.61.137.117 HTTP
67 33.503355807 65.61.137.117 192.168.245.134 HTTP
69 33.676652743 192.168.245.134 65.61.137.117 HTTP
72 33.998175603 65.61.137.117 192.168.245.134 HTTP
75 38.115617520 192.168.245.134 65.61.137.117 HTTP
80 38.464584331 65.61.137.117 192.168.245.134 HTTP
82 38.667552345 192.168.245.134 65.61.137.117 HTTP
84 38.984177164 65.61.137.117 192.168.245.134 HTTP 1
88 42.196105726 192.168.245.134 65.61.137.117 HTTP
90 42.699350869 65.61.137.117 192.168.245.134 HTTP
92 42.853717845 192.168.245.134 65.61.137.117 HTTP
94 43.181216811 65.61.137.117 192.168.245.134 HTTP
99 46.708831837 192.168.245.134 65.61.137.117 HTTP
101 47.255073340 65.61.137.117 192.168.245.134 HTTP
Frame 75: 525 bytes on wire (4200 bits), 525 bytes captured (4200 bits)
Ethernet II, Src: VMware_6e:6f:56 (00:0c:29:6e:6f:56), Dst: VMware_f1:3f
Internet Protocol Version 4, Src: 192.168.245.134, Dst: 65.61.137.117
Transmission Control Protocol, Src Port: 58366, Dst Port: 80, Seq: 1772,
Hypertext Transfer Protocol
wireshark_eth0AA2962.pcapng

- □ □

---

6. Conclusion

This analysis successfully captured and reviewed TCP, DNS, and HTTP traffic. The interactions showed typical web session behavior with no anomalies. The use of HTTP without encryption (vs. HTTPS) highlights a potential security issue, especially in public or shared networks.

---

7. Recommendations

- Use HTTPS instead of HTTP whenever possible to protect data in transit.
- Monitor DNS traffic regularly for unusual or unauthorized domain queries.
- Maintain healthy TCP performance by avoiding network congestion and packet loss.