Wireshark Network Traffic Capture and Analysis Report

Soumil Gupta

Task 05

Capture live network packets using Wireshark and identify basic protocols and traffic types to develop hands-on packet analysis skills and protocol awareness.

Part 1: Installing Wireshark

Download and Installation

Step 1: Download Wireshark

1. Visit the official Wireshark website: https://www.wireshark.org/
2. Click on "Download" section
3. Select the appropriate version for your operating system
4. Download the installer (.exe file for Windows)

Step 2: Installation Process

1. Run the downloaded installer as Administrator
2. Follow the installation wizard
3. Accept the license agreement
4. Choose installation components (keep default selections)
5. Install WinPcap/Npcap when prompted (required for packet capture)
6. Complete the installation

Step 3: First Launch

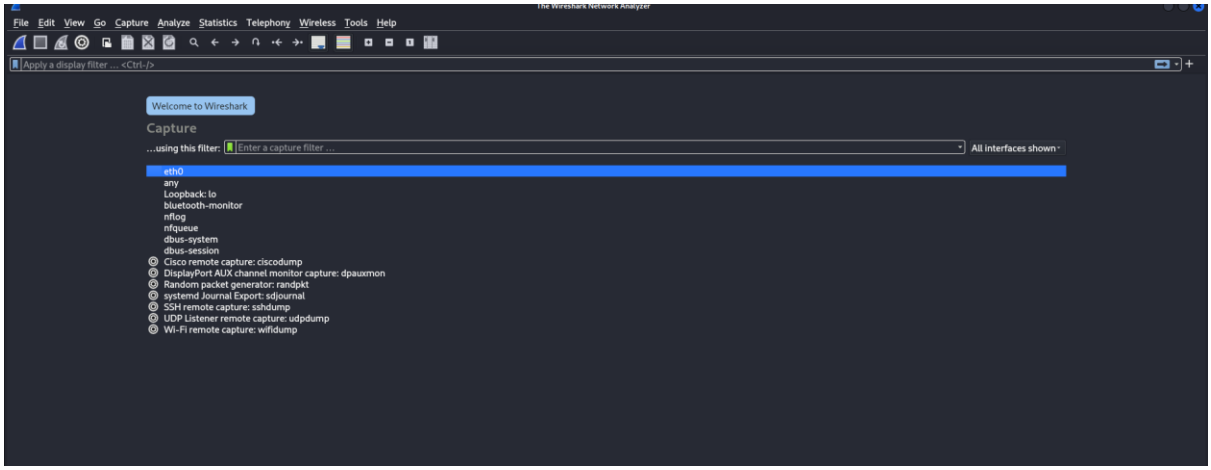
1. Launch Wireshark from Start Menu or Desktop shortcut
2. Wireshark main interface will appear

Part 2: Starting Network Capture

Identifying Network Interface

Step 1: Select Network Interface

1. In Wireshark main window, view available network interfaces
2. Identify your active network interface (usually shows traffic activity)
3. Look for interfaces with IP addresses and active traffic graphs



Step 2: Start Packet Capture

1. Double-click on your active network interface, OR
2. Select the interface and click the "Start capturing packets" button (shark fin icon)
3. Packet capture will begin immediately

Part 3: Generating Network Traffic

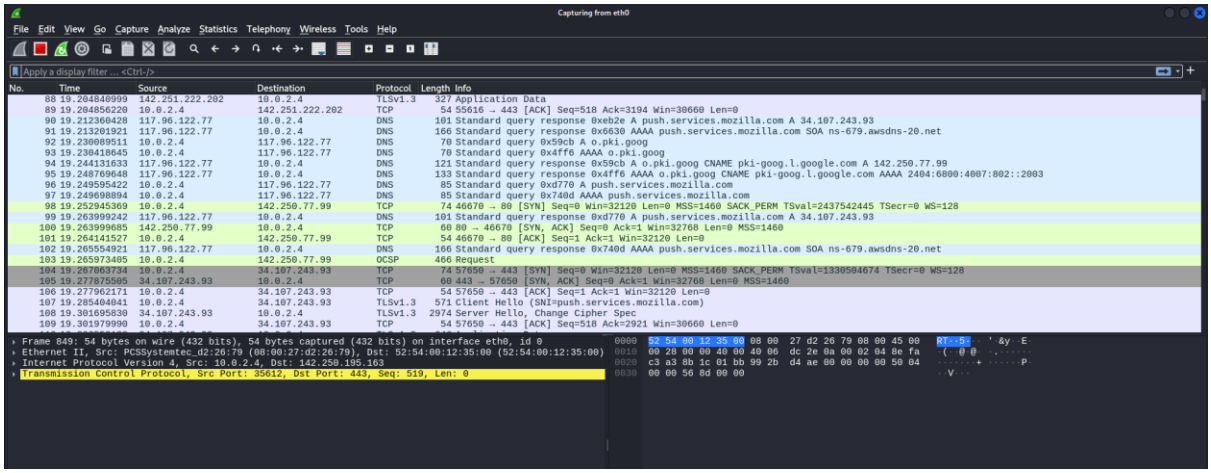
Method 1: Web Browsing Traffic

Step 1: Generate HTTP/HTTPS Traffic

1. Open a web browser
2. Visit several websites (e.g., http://example.com, https://google.com)
3. Navigate through different pages
4. Observe packets appearing in Wireshark

Websites Visited:

- http://example.com (for HTTP traffic)
- https://www.google.com (for HTTPS traffic)
- https://www.github.com (for additional HTTPS traffic)



Method 2: Ping Commands

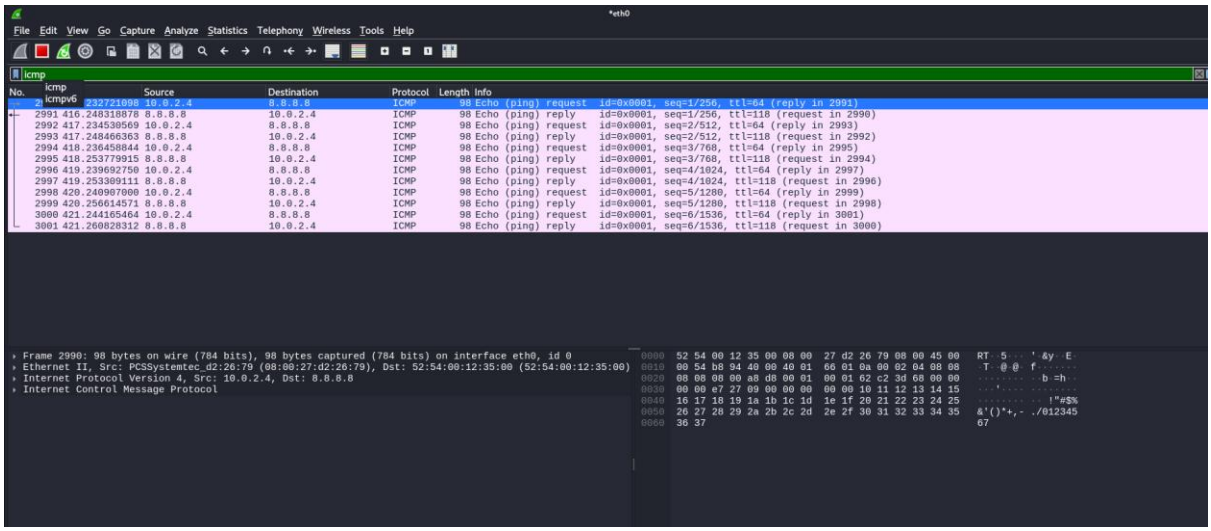
Step 2: Generate ICMP Traffic

1. Open Command Prompt
2. Execute ping commands to generate ICMP traffic:

ping google.com

ping 8.8.8.8

ping -t 1.1.1.1



Method 3: DNS Lookups

Step 3: Generate DNS Traffic

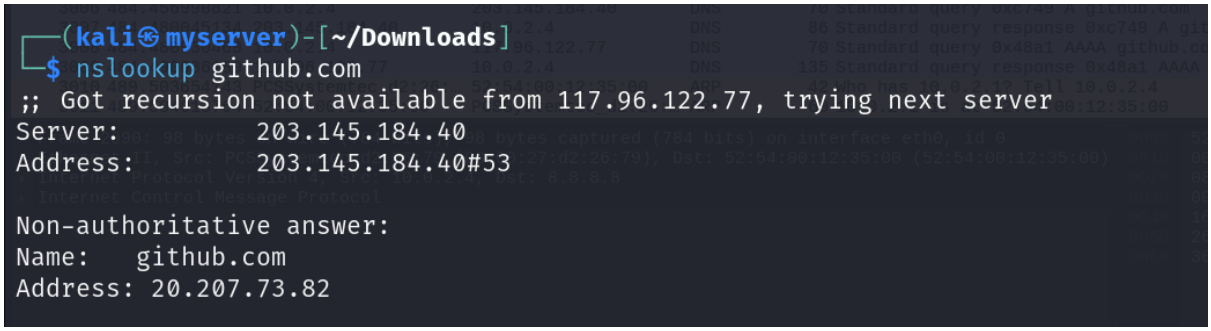
1. Use nslookup commands to generate DNS queries:

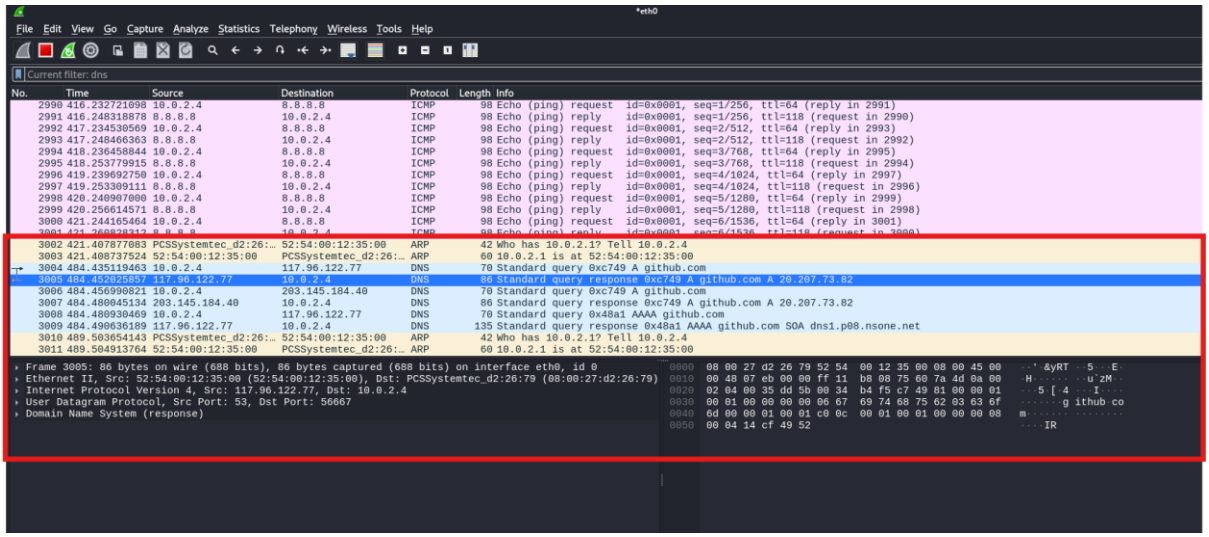
nslookup google.com

nslookup facebook.com

nslookup github.com

Screenshot Placeholder:





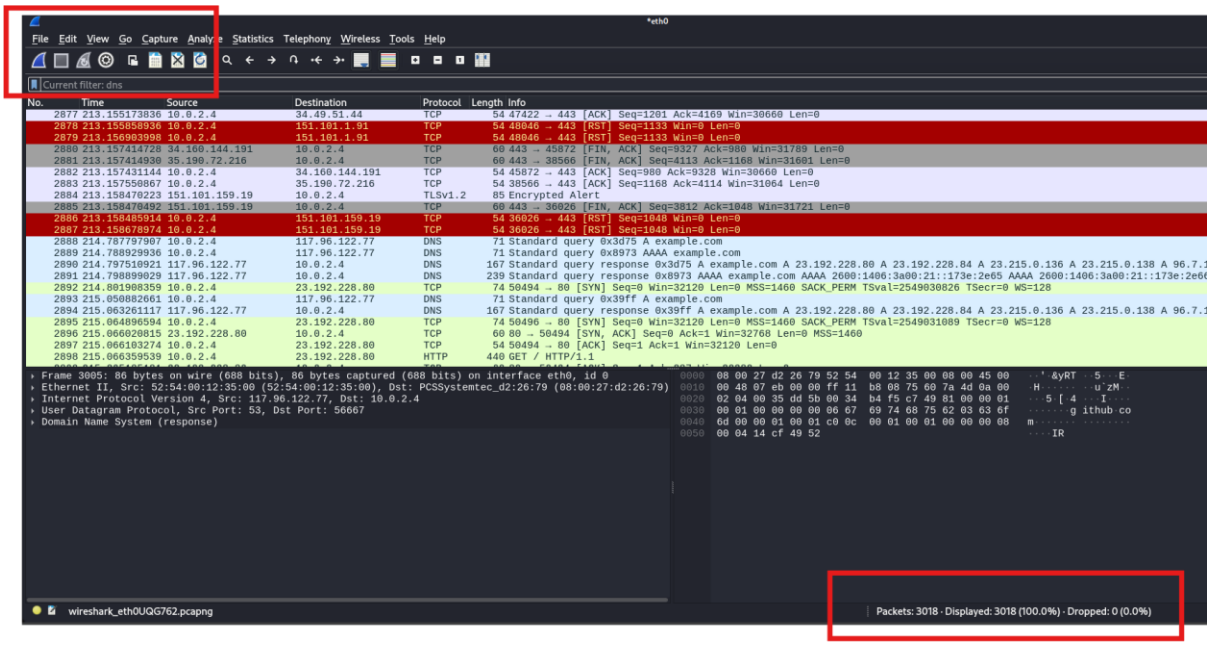
Part 4: Stopping Capture and Initial Analysis

Stopping the Capture

Step 1: Stop Packet Capture

1. Click the red "Stop" button in Wireshark toolbar
2. Capture will stop and all packets will be displayed

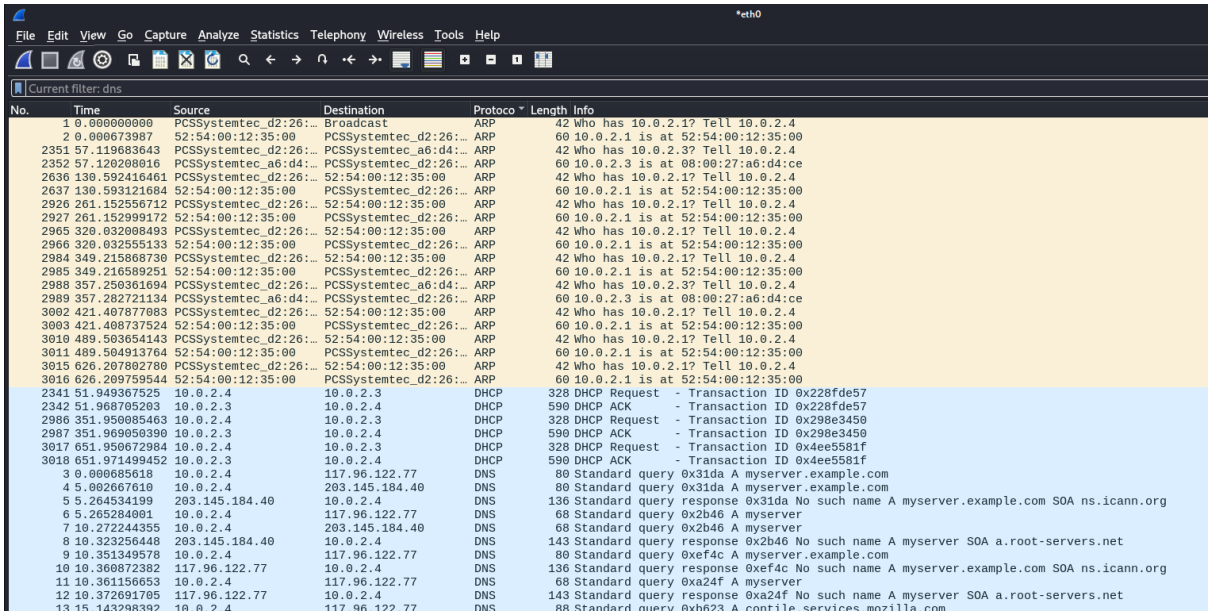
Capture Duration: Approximately 60 seconds
Total Packets Captured: 3018



Initial Packet Overview

Step 2: Review Captured Traffic

1. Observe the packet list in the main window
2. Note the variety of protocols shown in the "Protocol" column
3. Review source and destination IP addresses

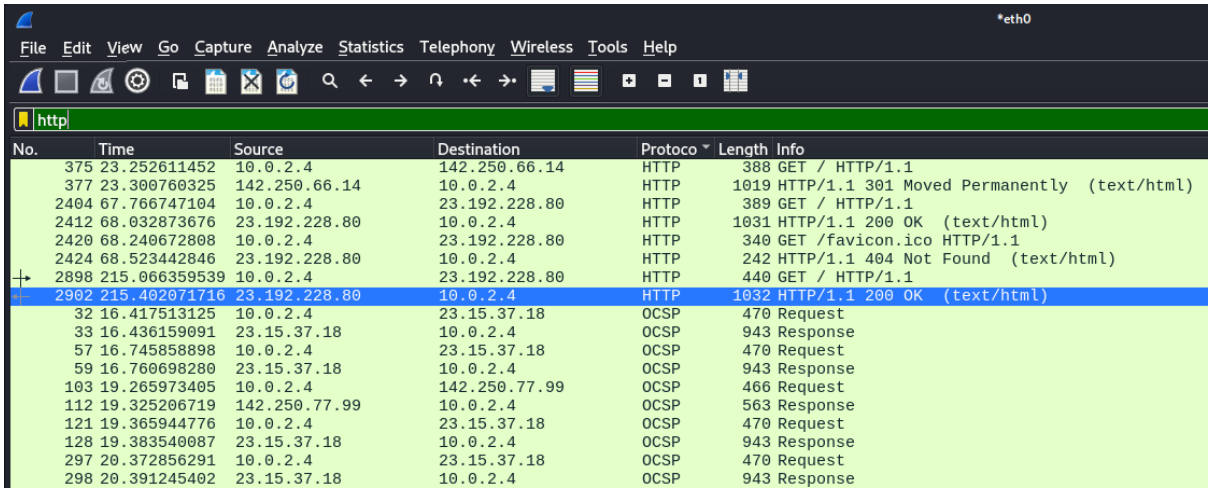


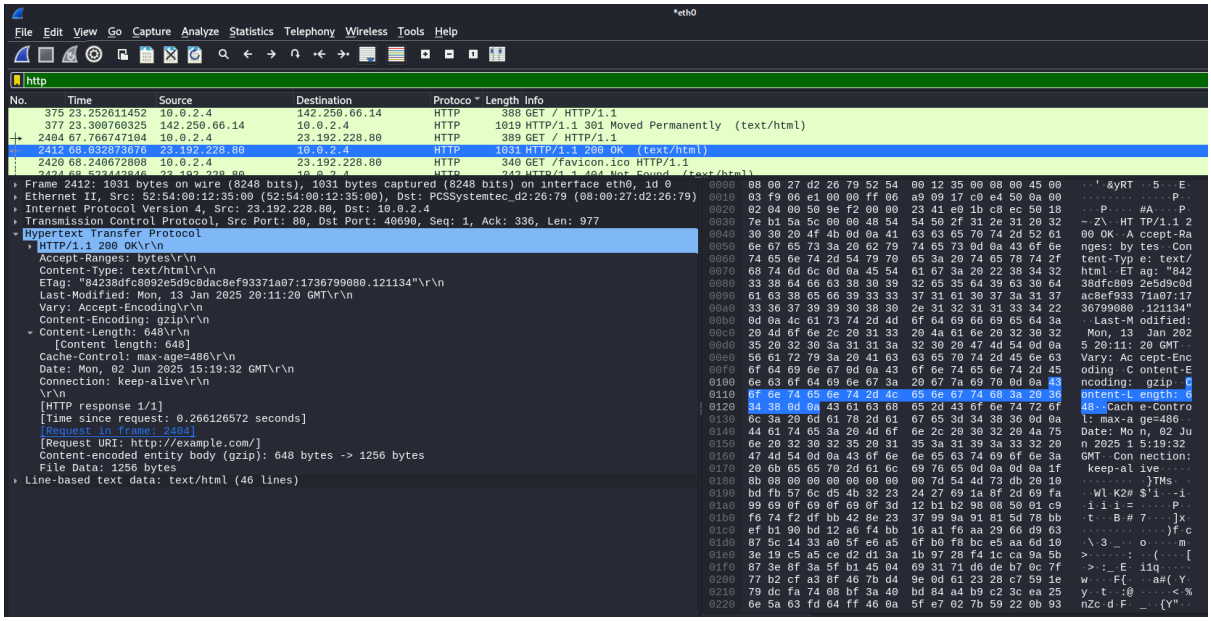
Part 5: Protocol Filtering and Analysis

Filter 1: HTTP Traffic

Step 1: Apply HTTP Filter

1. In the filter bar, type: http
2. Press Enter to apply the filter
3. Analyse HTTP requests and responses





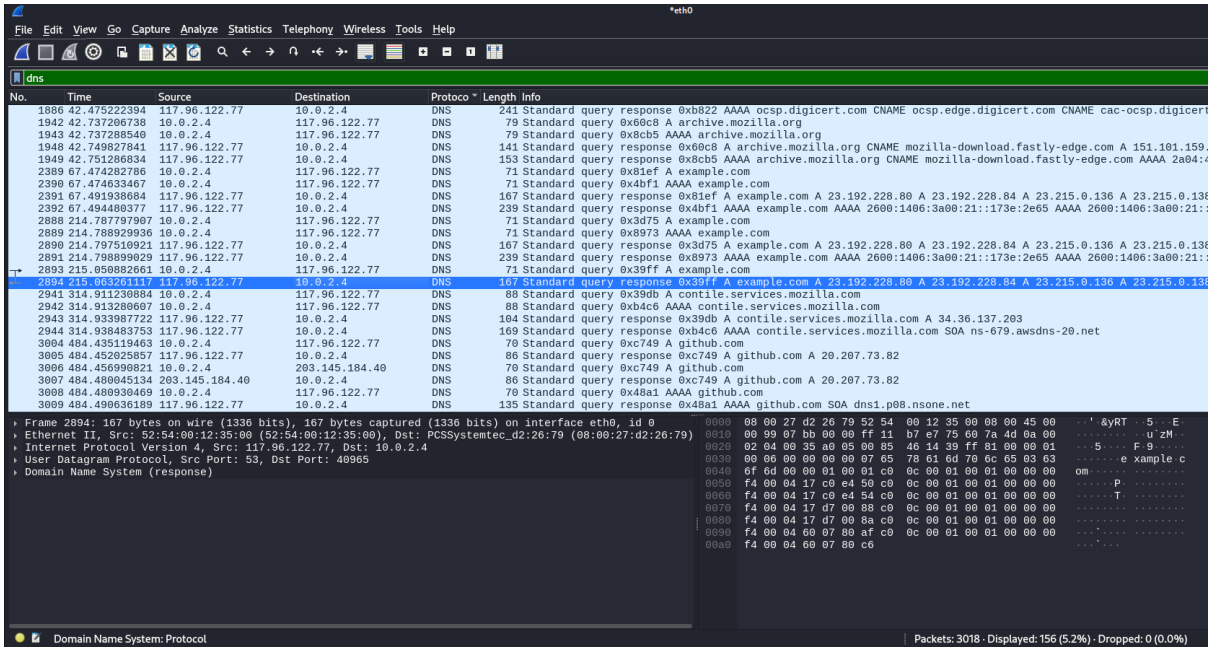
HTTP Analysis:

- HTTP Requests Observed:
  - GET requests to various websites
  - User-Agent strings
  - Host headers
- HTTP Responses Observed:
  - Status codes (200 here)
  - Content-Type headers
  - Server response headers

Filter 2: DNS Traffic

Step 2: Apply DNS Filter

1. Clear previous filter
2. Type: dns
3. Press Enter to apply the filter



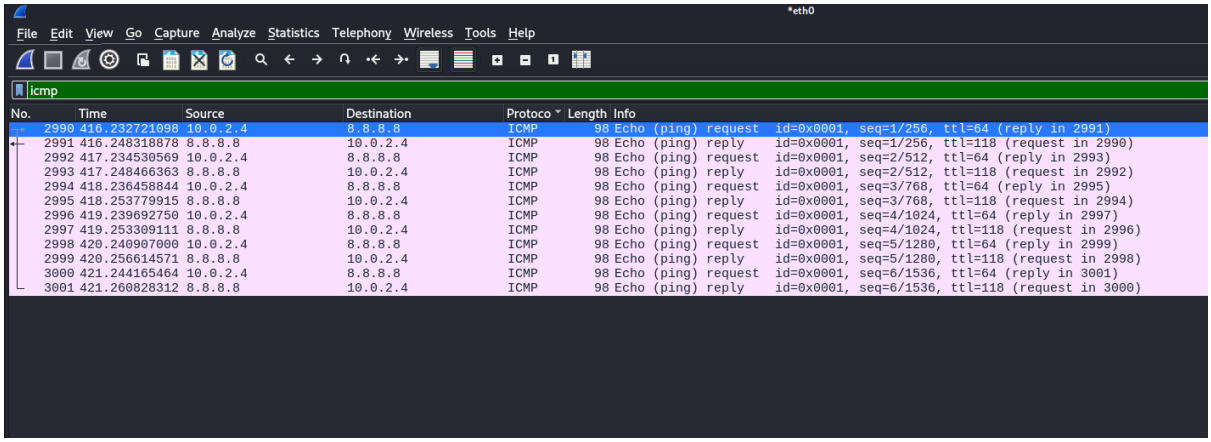
DNS Analysis:

- Query Types Observed:
  - A records (IPv4 addresses)
  - AAAA records (IPv6 addresses)
  - CNAME records (canonical names)
- DNS Servers Contacted:
  - Dns1.p08.nsone.net
  - Ns-679.awsdns-20.net

Filter 3: ICMP Traffic

Step 3: Apply ICMP Filter

1. Clear previous filter
2. Type: icmp
3. Press Enter to apply the filter



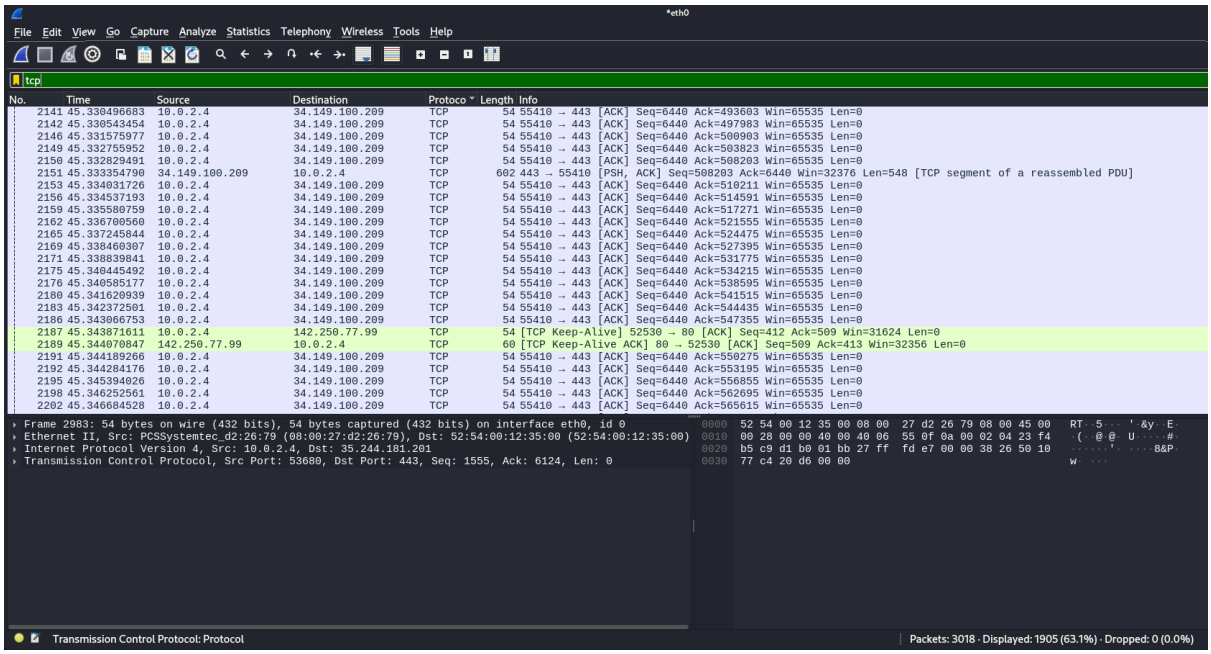
ICMP Analysis:

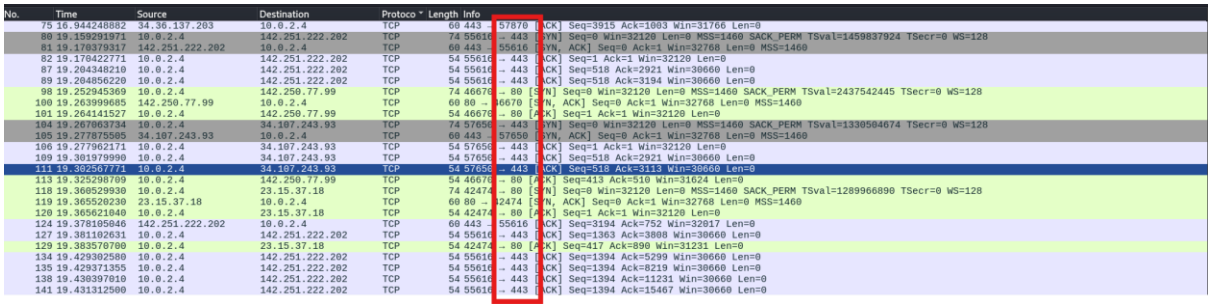
- ICMP Types Observed:
    - Echo Request (Type 8)
    - Echo Reply (Type 0)

Filter 4: TCP Traffic

Step 4: Apply TCP Filter

1. Clear previous filter
2. Type: tcp
3. Press Enter to apply the filter





No.	Time	Source	Destination	Protocol	Length	Info
75	16.944248882	34.36.137.203	10.0.2.4	TCP	60	443 → 57870 [ACK] Seq=3915 Ack=1003 Win=31766 Len=0
80	19.159291971	10.0.2.4	142.251.222.202	TCP	74	55616 → 443 [SYN] Seq=0 Win=32120 Len=0 MSS=1460 SACK_PERM TSval=1459837924 TSecr=0 WS=128
81	19.170379317	142.251.222.202	10.0.2.4	TCP	60	443 → 55616 [SYN, ACK] Seq=0 Ack=1 Win=32768 Len=0 MSS=1460
82	19.170422771	10.0.2.4	142.251.222.202	TCP	54	55616 → 443 [ACK] Seq=1 Ack=1 Win=32120 Len=0
87	19.204348210	10.0.2.4	142.251.222.202	TCP	54	55616 → 443 [ACK] Seq=518 Ack=2921 Win=30660 Len=0
89	19.204856220	10.0.2.4	142.251.222.202	TCP	54	55616 → 443 [ACK] Seq=518 Ack=3194 Win=30660 Len=0
98	19.252945369	10.0.2.4	142.250.77.99	TCP	74	46670 → 80 [SYN] Seq=0 Win=32120 Len=0 MSS=1460 SACK_PERM TSval=2437542445 TSecr=0 WS=128
100	19.263999685	142.250.77.99	10.0.2.4	TCP	60	80 → 46670 [SYN, ACK] Seq=0 Ack=1 Win=32768 Len=0 MSS=1460
101	19.264141527	10.0.2.4	142.250.77.99	TCP	54	46670 → 80 [ACK] Seq=1 Ack=1 Win=32120 Len=0
104	19.267063734	10.0.2.4	34.107.243.93	TCP	74	57650 → 443 [SYN] Seq=0 Win=32120 Len=0 MSS=1460 SACK_PERM TSval=1330504674 TSecr=0 WS=128
105	19.277875505	34.107.243.93	10.0.2.4	TCP	60	443 → 57650 [SYN, ACK] Seq=0 Ack=1 Win=32768 Len=0 MSS=1460
106	19.277962171	10.0.2.4	34.107.243.93	TCP	54	57650 → 443 [ACK] Seq=1 Ack=1 Win=32120 Len=0
109	19.301979990	10.0.2.4	34.107.243.93	TCP	54	57650 → 443 [ACK] Seq=518 Ack=2921 Win=30660 Len=0
111	19.302567771	10.0.2.4	34.107.243.93	TCP	54	57650 → 443 [ACK] Seq=518 Ack=3113 Win=30660 Len=0
113	19.325298709	10.0.2.4	142.250.77.99	TCP	54	46670 → 80 [ACK] Seq=413 Ack=510 Win=31624 Len=0
118	19.360529930	10.0.2.4	23.15.37.18	TCP	74	42474 → 80 [SYN] Seq=0 Win=32120 Len=0 MSS=1460 SACK_PERM TSval=1289966890 TSecr=0 WS=128
119	19.365520230	23.15.37.18	10.0.2.4	TCP	60	80 → 42474 [SYN, ACK] Seq=0 Ack=1 Win=32768 Len=0 MSS=1460
120	19.365621040	10.0.2.4	23.15.37.18	TCP	54	42474 → 80 [ACK] Seq=1 Ack=1 Win=32120 Len=0
124	19.378105046	142.251.222.202	10.0.2.4	TCP	60	443 → 55616 [ACK] Seq=3194 Ack=752 Win=32017 Len=0
127	19.381102631	10.0.2.4	142.251.222.202	TCP	54	55616 → 443 [ACK] Seq=1363 Ack=3808 Win=30660 Len=0
129	19.383570700	10.0.2.4	23.15.37.18	TCP	54	42474 → 80 [ACK] Seq=417 Ack=890 Win=31231 Len=0
134	19.429302580	10.0.2.4	142.251.222.202	TCP	54	55616 → 443 [ACK] Seq=1394 Ack=5299 Win=30660 Len=0
135	19.429371355	10.0.2.4	142.251.222.202	TCP	54	55616 → 443 [ACK] Seq=1394 Ack=8219 Win=30660 Len=0
138	19.430397010	10.0.2.4	142.251.222.202	TCP	54	55616 → 443 [ACK] Seq=1394 Ack=11231 Win=30660 Len=0
141	19.431312500	10.0.2.4	142.251.222.202	TCP	54	55616 → 443 [ACK] Seq=1394 Ack=15467 Win=30660 Len=0

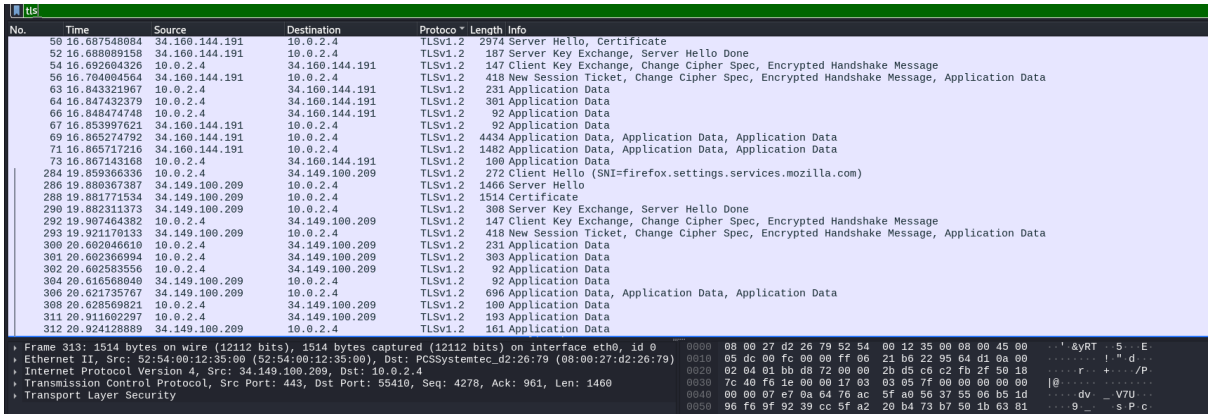
TCP Analysis:

- TCP Flags Observed:
    - SYN (connection initiation)
    - ACK (acknowledgment)
    - FIN (connection termination)
    - RST (connection reset)
- Port Numbers:
    - Port 80 (HTTP)
    - Port 443 (HTTPS)
    - Port 55616

Filter 5: HTTPS/TLS Traffic

Step 5: Apply TLS Filter

1. Clear previous filter
2. Type: tls
3. Press Enter to apply the filter



TLS Analysis:

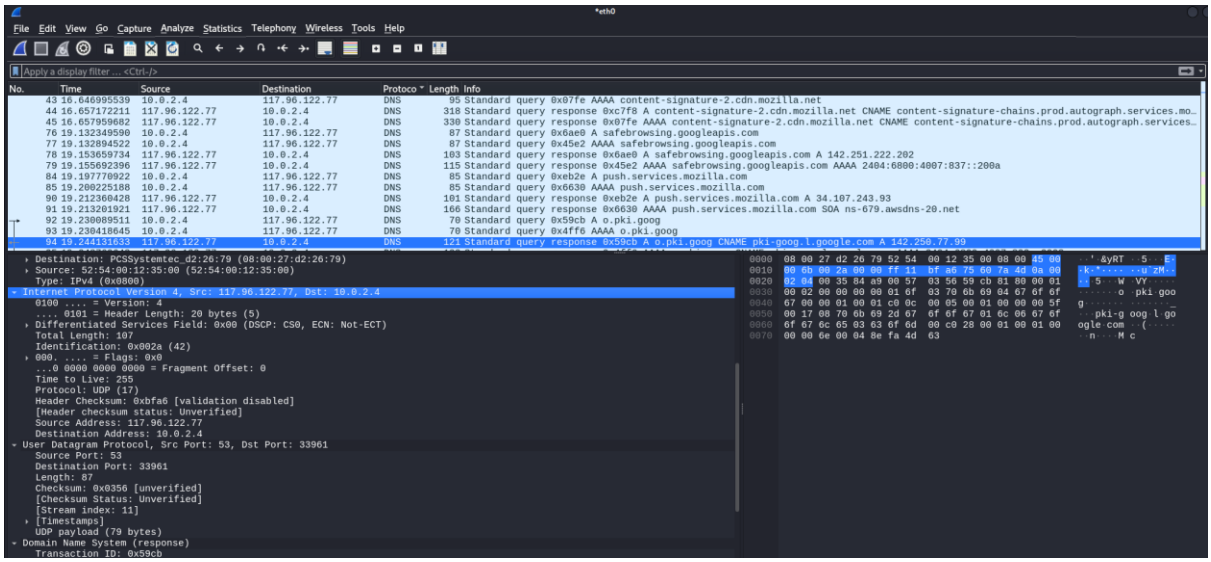
- TLS Handshake Elements:
    - Client Hello
    - Server Hello
    - Certificate exchanges
    - Encrypted application data

Part 6: Detailed Packet Analysis

Analysing Individual Packets

Step 1: Select a Packet for Detailed Analysis

1. Click on any interesting packet in the packet list
2. Observe the packet details in the middle pane
3. Review the hex dump in the bottom pane

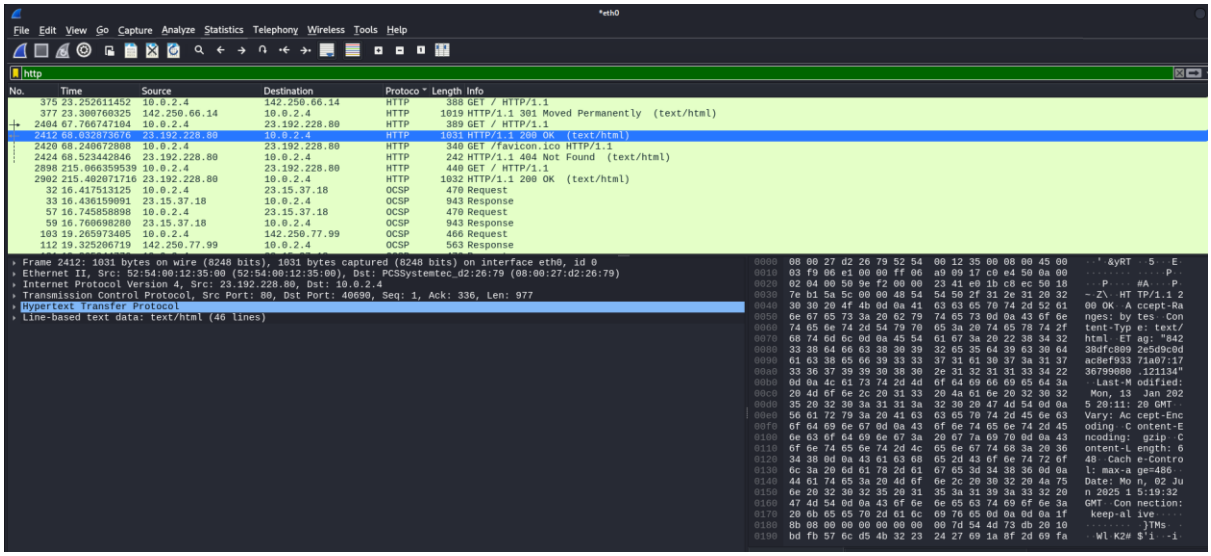


Protocol Stack Analysis

Example Packet Analysis:

Packet #2412: HTTP GET Request

- Frame: Physical layer information
- Ethernet II: Data link layer (MAC addresses)
- Internet Protocol Version 4: Network layer (IP addresses)
- Transmission Control Protocol: Transport layer (ports, flags)
- Hypertext Transfer Protocol: Application layer (HTTP headers)



Part 7: Exporting Capture File

Saving the Packet Capture

Step 1: Save Capture File

1. Go to File → Save As
2. Choose location and filename
3. Ensure file type is "Wireshark/tcpdump/... - pcap"
4. Click Save

File Details:

- Filename: network_capture_task5
- File Size: 2.1MB
- Number of Packets: 3018
- Capture Duration: 621 seconds

Part 8: Protocol Identification Summary

Protocols Identified in Capture

Protocol	Layer	Port/Type	Purpose
HTTP	Application (Layer 7)	80	Web browsing
HTTPS/TLS	Application (Layer 7)	443	Secure web browsing
DNS	Application (Layer 7)	53	Domain name resolution
TCP	Transport (Layer 4)	Various	Reliable data transmission
UDP	Transport (Layer 4)	Various	Fast data transmission
ICMP	Network (Layer 3)	N/A	Network diagnostics (ping)
IPv4	Network (Layer 3)	N/A	Internet addressing
Ethernet	Data Link (Layer 2)	N/A	Local network framing

Additional Protocols (if observed):

- ARP (Address Resolution Protocol)
- DHCP (Dynamic Host Configuration Protocol)
- NTP (Network Time Protocol)
- SSDP (Simple Service Discovery Protocol)

Part 9: Traffic Pattern Analysis

Communication Flows Observed

HTTP Communication Flow:

1. DNS query to resolve domain name
2. TCP three-way handshake (SYN, SYN-ACK, ACK)
3. HTTP GET request
4. HTTP response with content
5. TCP connection termination

Network Statistics

Step 1: View Protocol Hierarchy

1. Go to Statistics → Protocol Hierarchy
2. Analyse protocol distribution

Step 2: View Conversations

1. Go to Statistics → Conversations
2. Review top talkers by protocol

Part 10: Summary

Major Observations

1. Protocol Diversity:
    - Successfully captured and identified multiple network protocols
    - Observed both encrypted and unencrypted traffic
    - Witnessed complete communication flows
2. Traffic Patterns:
    - Web browsing generates multiple protocol types (DNS, TCP, HTTP/HTTPS)
    - Each web request involves several packet exchanges
    - Background system traffic also captured (DHCP, ARP, etc.)
3. Packet Structure:
    - Each packet contains multiple protocol layers
    - Headers provide essential routing and control information
    - Payload contains actual application data

Protocol Layer Understanding

Physical to Application Layer Traffic:

- Layer 2 (Data Link): Ethernet frames with MAC addresses
- Layer 3 (Network): IP packets with source/destination addresses
- Layer 4 (Transport): TCP/UDP segments with port information
- Layer 7 (Application): HTTP, DNS, and other application protocols