

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

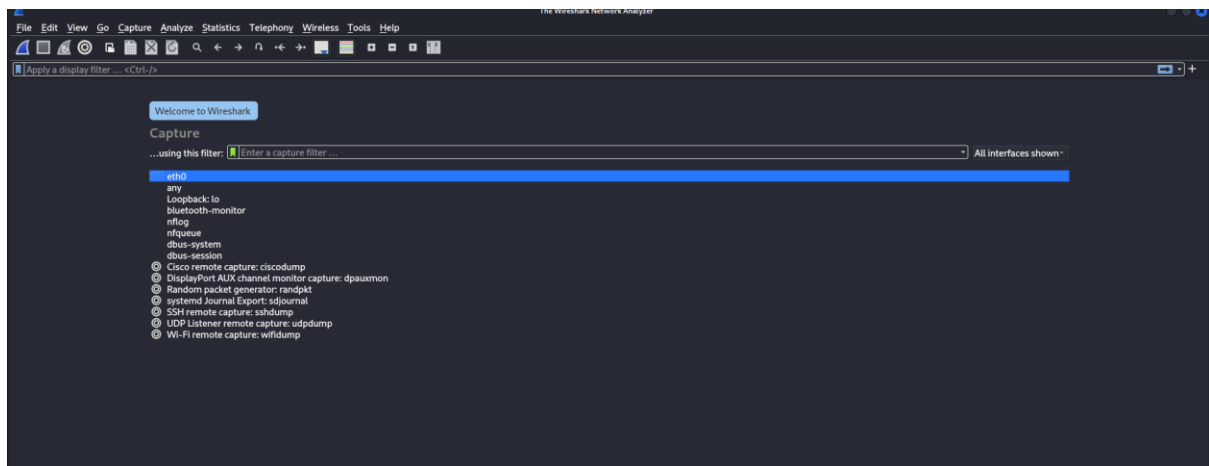
1. Launch Wireshark from Start Menu or Desktop shortcut
2. Wireshark main interface will appear

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

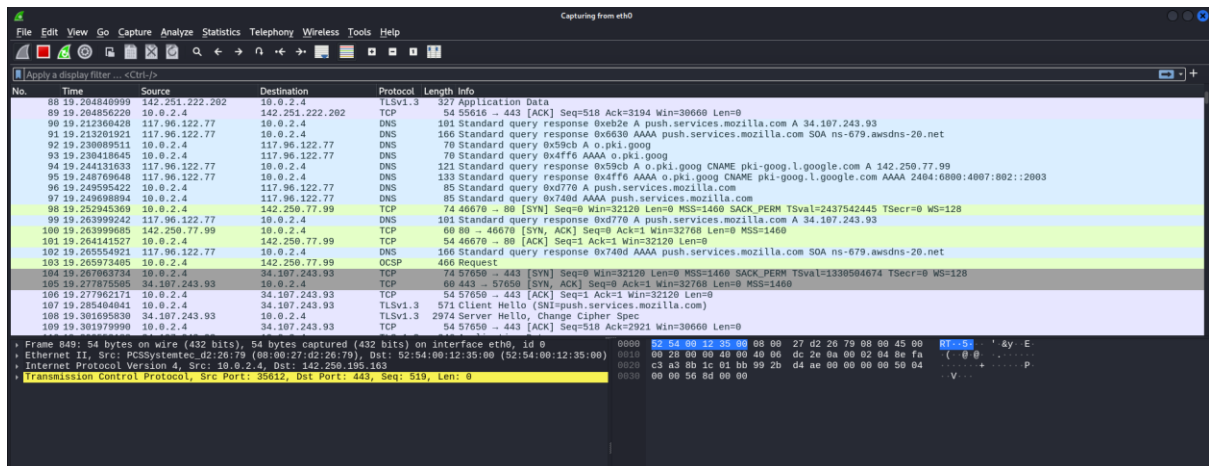
Method 1: Web Browsing Traffic

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

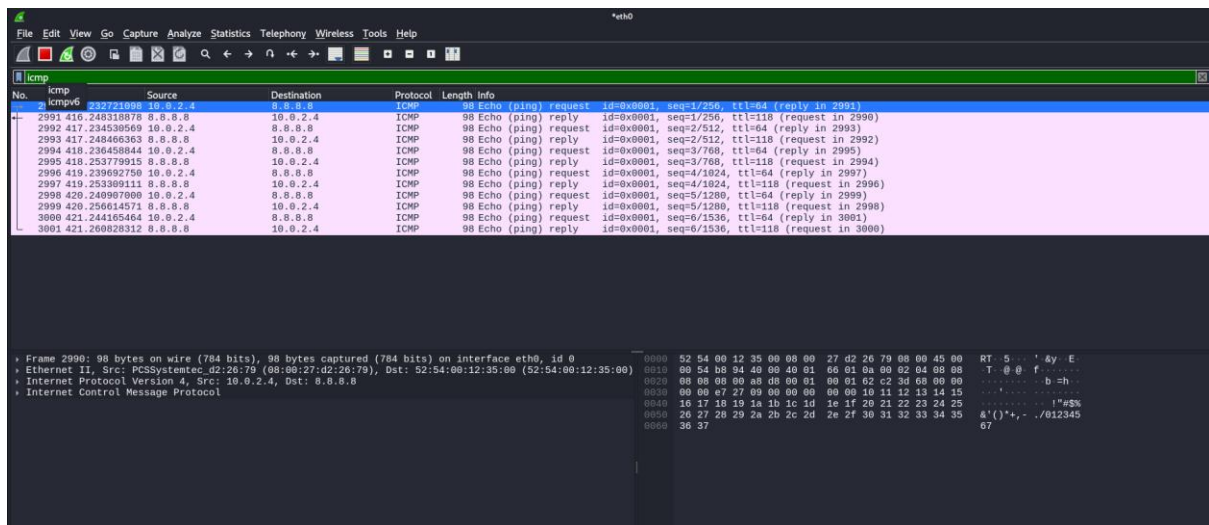
Step 2: Generate ICMP Traffic

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

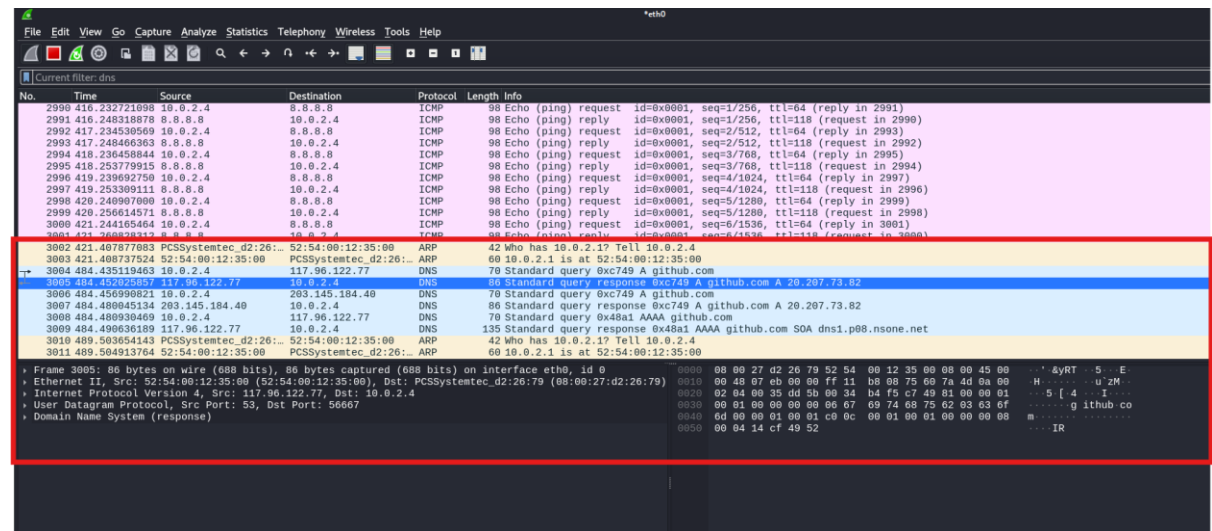
nslookup facebook.com

nslookup github.com

Screenshot Placeholder:

```
(kali@myserver)-[~/Downloads]
$ nslookup github.com
;; Got recursion not available from 117.96.122.77, trying next server
Server:                203.145.184.40
Address:                203.145.184.40#53

Non-authoritative answer:
Name:   github.com
Address: 20.207.73.82
```



Part 4: Stopping Capture and Initial Analysis

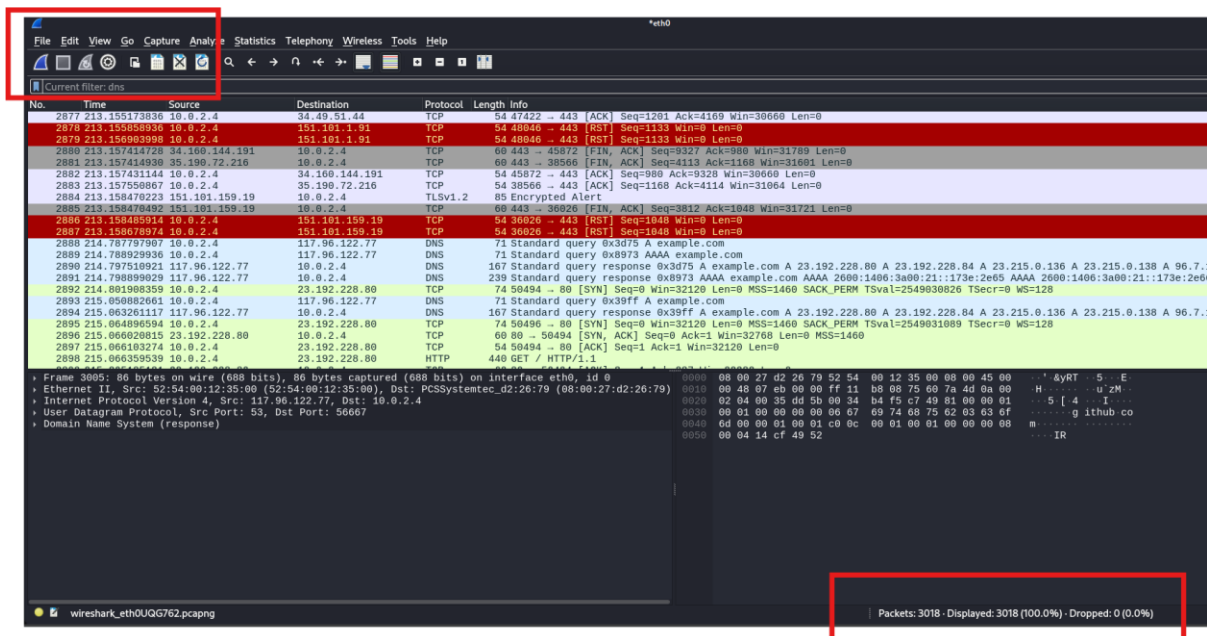
Stopping the Capture

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

*eth0						
File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help						
Current filter: dns						
No.	Time	Source	Destination	Protocol	Length	Info
1	0.000000000	PCSSystemtec_d2:26:...	Broadcast	ARP	42	Who has 10.0.2.1? Tell 10.0.2.4
2	0.000673987	52:54:00:12:35:00	PCSSystemtec_d2:26:...	ARP	60	10.0.2.1 is at 52:54:00:12:35:00
2351	57.119683643	PCSSystemtec_d2:26:...	PCSSystemtec_a6:d4:...	ARP	42	Who has 10.0.2.3? Tell 10.0.2.4
2352	57.120208016	PCSSystemtec_a6:d4:...	PCSSystemtec_d2:26:...	ARP	60	10.0.2.3 is at 08:00:27:a6:d4:ce
2636	130.592416461	PCSSystemtec_d2:26:...	52:54:00:12:35:00	ARP	42	Who has 10.0.2.1? Tell 10.0.2.4
2637	130.593121684	52:54:00:12:35:00	PCSSystemtec_d2:26:...	ARP	60	10.0.2.1 is at 52:54:00:12:35:00
2926	261.152556712	PCSSystemtec_d2:26:...	52:54:00:12:35:00	ARP	42	Who has 10.0.2.1? Tell 10.0.2.4
2927	261.152999172	52:54:00:12:35:00	PCSSystemtec_d2:26:...	ARP	60	10.0.2.1 is at 52:54:00:12:35:00
2965	320.032008493	PCSSystemtec_d2:26:...	52:54:00:12:35:00	ARP	42	Who has 10.0.2.1? Tell 10.0.2.4
2966	320.032555133	52:54:00:12:35:00	PCSSystemtec_d2:26:...	ARP	60	10.0.2.1 is at 52:54:00:12:35:00
2984	349.215806730	PCSSystemtec_d2:26:...	52:54:00:12:35:00	ARP	42	Who has 10.0.2.1? Tell 10.0.2.4
2985	349.216589251	52:54:00:12:35:00	PCSSystemtec_d2:26:...	ARP	60	10.0.2.1 is at 52:54:00:12:35:00
2988	357.250361694	PCSSystemtec_d2:26:...	PCSSystemtec_a6:d4:...	ARP	42	Who has 10.0.2.3? Tell 10.0.2.4
2989	357.282721134	PCSSystemtec_a6:d4:...	PCSSystemtec_d2:26:...	ARP	60	10.0.2.3 is at 08:00:27:a6:d4:ce
3002	421.407877083	PCSSystemtec_d2:26:...	52:54:00:12:35:00	ARP	42	Who has 10.0.2.1? Tell 10.0.2.4
3003	421.408737524	52:54:00:12:35:00	PCSSystemtec_d2:26:...	ARP	60	10.0.2.1 is at 52:54:00:12:35:00
3010	489.503654143	PCSSystemtec_d2:26:...	52:54:00:12:35:00	ARP	42	Who has 10.0.2.1? Tell 10.0.2.4
3011	489.504913764	52:54:00:12:35:00	PCSSystemtec_d2:26:...	ARP	60	10.0.2.1 is at 52:54:00:12:35:00
3015	626.207802780	PCSSystemtec_d2:26:...	52:54:00:12:35:00	ARP	42	Who has 10.0.2.1? Tell 10.0.2.4
3016	626.209759544	52:54:00:12:35:00	PCSSystemtec_d2:26:...	ARP	60	10.0.2.1 is at 52:54:00:12:35:00
2341	51.949307525	10.0.2.4	10.0.2.3	DHCP	328	DHCP Request - Transaction ID 0x228fde57
2342	51.960705203	10.0.2.3	10.0.2.4	DHCP	590	DHCP ACK - Transaction ID 0x228fde57
2986	351.9500085463	10.0.2.4	10.0.2.3	DHCP	328	DHCP Request - Transaction ID 0x298e3450
2987	351.969050390	10.0.2.3	10.0.2.4	DHCP	590	DHCP ACK - Transaction ID 0x298e3450
3017	651.950672984	10.0.2.4	10.0.2.3	DHCP	328	DHCP Request - Transaction ID 0x4ee5581f
3018	651.971499452	10.0.2.3	10.0.2.4	DHCP	590	DHCP ACK - Transaction ID 0x4ee5581f
3	0.000685618	10.0.2.4	117.96.122.77	DNS	80	Standard query 0x31da A myserver.example.com
4	5.002667610	10.0.2.4	203.145.184.40	DNS	80	Standard query 0x31da A myserver.example.com
5	5.264534199	203.145.184.40	10.0.2.4	DNS	136	Standard query response 0x31da No such name A myserver.example.com SOA ns.icann.org
6	5.265284001	10.0.2.4	117.96.122.77	DNS	68	Standard query 0x2b46 A myserver
7	10.272244355	10.0.2.4	203.145.184.40	DNS	68	Standard query 0x2b46 A myserver
8	10.323256448	203.145.184.40	10.0.2.4	DNS	143	Standard query response 0x2b46 No such name A myserver SOA a.root-servers.net
9	10.351349578	10.0.2.4	117.96.122.77	DNS	80	Standard query 0xef4c A myserver.example.com
10	10.360872362	117.96.122.77	10.0.2.4	DNS	136	Standard query response 0xef4c No such name A myserver.example.com SOA ns.icann.org
11	10.361596653	10.0.2.4	117.96.122.77	DNS	68	Standard query 0xa24f A myserver
12	10.372691705	117.96.122.77	10.0.2.4	DNS	143	Standard query response 0xa24f No such name A myserver SOA a.root-servers.net
13	15.143298302	10.0.2.4	117.96.122.77	DNS	88	Standard query 0xh623 A contile.services.mozilla.com

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

*eth0						
File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help						
http						
No.	Time	Source	Destination	Protocol	Length	Info
375	23.252611452	10.0.2.4	142.250.66.14	HTTP	388	GET / HTTP/1.1
377	23.300760325	142.250.66.14	10.0.2.4	HTTP	1019	HTTP/1.1 301 Moved Permanently (text/html)
2404	67.766747104	10.0.2.4	23.192.228.80	HTTP	389	GET / HTTP/1.1
2412	68.032873676	23.192.228.80	10.0.2.4	HTTP	1031	HTTP/1.1 200 OK (text/html)
2420	68.240672808	10.0.2.4	23.192.228.80	HTTP	340	GET /favicon.ico HTTP/1.1
2424	68.523442846	23.192.228.80	10.0.2.4	HTTP	242	HTTP/1.1 404 Not Found (text/html)
2898	215.066359539	10.0.2.4	23.192.228.80	HTTP	440	GET / HTTP/1.1
2902	215.402071716	23.192.228.80	10.0.2.4	HTTP	1032	HTTP/1.1 200 OK (text/html)
32	16.417513125	10.0.2.4	23.15.37.18	OCSP	470	Request
33	16.436159091	23.15.37.18	10.0.2.4	OCSP	943	Response
57	16.745858898	10.0.2.4	23.15.37.18	OCSP	470	Request
59	16.760698280	23.15.37.18	10.0.2.4	OCSP	943	Response
103	19.265973405	10.0.2.4	142.250.77.99	OCSP	466	Request
112	19.325206719	142.250.77.99	10.0.2.4	OCSP	563	Response
121	19.365944776	10.0.2.4	23.15.37.18	OCSP	470	Request
128	19.383540087	23.15.37.18	10.0.2.4	OCSP	943	Response
297	20.372856291	10.0.2.4	23.15.37.18	OCSP	470	Request
298	20.391245402	23.15.37.18	10.0.2.4	OCSP	943	Response

No.	Time	Source	Destination	Protocol	Length	Info
375	23.252611452	10.0.2.4	142.250.66.14	HTTP	388	GET / HTTP/1.1
377	23.300760325	142.250.66.14	10.0.2.4	HTTP	1019	HTTP/1.1 301 Moved Permanently (text/html)
2494	67.766747104	10.0.2.4	23.192.228.80	HTTP	389	GET / HTTP/1.1
2495	68.322038370	23.192.228.80	10.0.2.4	HTTP	1031	HTTP/1.1 200 OK (text/html)
2420	68.240672808	10.0.2.4	23.192.228.80	HTTP	340	GET /favicon.ico HTTP/1.1
2421	68.533453846	23.192.228.80	10.0.2.4	HTTP	242	HTTP/1.1 404 Not Found (text/html)
Frame 2412: 1631 bytes on wire (8248 bits), 1631 bytes captured (8248 bits) on interface eth0, id 6 Ethernet II, Src: 52:54:00:12:35:00 (52:54:00:12:35:00), Dst: PCSystemtec_d2:26:79 (00:00:27:d2:26:79) Internet Protocol Version 4, Src: 23.192.228.80, Dst: 10.0.2.4 Transmission Control Protocol, Src Port: 80, Dst Port: 40690, Seq: 1, Ack: 336, Len: 977 Hypertext Transfer Protocol HTTP/1.1 200 OK\r\n Accept-Ranges: bytes\r\n Content-Type: text/html\r\n Etag: "84238dfc8092e5d9c0dac8ef93371a07:1736799800.121134"\r\n Last-Modified: Mon, 13 Jan 2025 20:11:20 GMT\r\n Vary: Accept-Encoding\r\n Content-Encoding: gzip\r\n Content-Length: 648\r\n [Content length: 648] Cache-Control: max-age=486\r\n Date: Mon, 02 Jun 2025 15:19:32 GMT\r\n Connection: keep-alive\r\n \r\n [HTTP response 1/1] [Time since request: 0.266126572 seconds] [Request in frame: 2404] [Request URI: http://example.com/] Content-encoded entity body (gzip): 648 bytes -> 1256 bytes File Data: 1256 bytes Line-based text data: text/html (46 lines)						

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

*eth0									
File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help									

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

- Clear previous filter
- Type: icmp
- Press Enter to apply the filter

No.	Time	Source	Destination	Protocol	Length	Info
2990	416.232721098	10.0.2.4	8.8.8.8	ICMP	98	Echo (ping) request id=0x0001, seq=1/256, ttl=64 (reply in 2991)
2991	416.248318878	8.8.8.8	10.0.2.4	ICMP	98	Echo (ping) reply id=0x0001, seq=1/256, ttl=118 (request in 2990)
2992	417.234530569	10.0.2.4	8.8.8.8	ICMP	98	Echo (ping) request id=0x0001, seq=2/512, ttl=64 (reply in 2993)
2993	417.248466363	8.8.8.8	10.0.2.4	ICMP	98	Echo (ping) reply id=0x0001, seq=2/512, ttl=118 (request in 2992)
2994	418.236458844	10.0.2.4	8.8.8.8	ICMP	98	Echo (ping) request id=0x0001, seq=3/768, ttl=64 (reply in 2995)
2995	418.253779915	8.8.8.8	10.0.2.4	ICMP	98	Echo (ping) reply id=0x0001, seq=3/768, ttl=118 (request in 2994)
2996	419.239692750	10.0.2.4	8.8.8.8	ICMP	98	Echo (ping) request id=0x0001, seq=4/1024, ttl=64 (reply in 2997)
2997	419.253309111	8.8.8.8	10.0.2.4	ICMP	98	Echo (ping) reply id=0x0001, seq=4/1024, ttl=118 (request in 2996)
2998	420.240987000	10.0.2.4	8.8.8.8	ICMP	98	Echo (ping) request id=0x0001, seq=5/1280, ttl=64 (reply in 2999)
2999	420.256614571	8.8.8.8	10.0.2.4	ICMP	98	Echo (ping) reply id=0x0001, seq=5/1280, ttl=118 (request in 2998)
3000	421.244165464	10.0.2.4	8.8.8.8	ICMP	98	Echo (ping) request id=0x0001, seq=6/1536, ttl=64 (reply in 3001)
3001	421.260828312	8.8.8.8	10.0.2.4	ICMP	98	Echo (ping) reply id=0x0001, seq=6/1536, ttl=118 (request in 3000)

ICMP Analysis:

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

Filter 4: TCP Traffic

Step 4: Apply TCP Filter

- Clear previous filter
- Type: tcp
- Press Enter to apply the filter

No.	Time	Source	Destination	Protocol	Length	Info
2141	45.338496683	10.0.2.4	34.149.100.209	TCP	54	55410 → 443 [ACK] Seq=6440 Ack=493603 Win=65535 Len=0
2142	45.339543454	10.0.2.4	34.149.100.209	TCP	54	55410 → 443 [ACK] Seq=6440 Ack=497983 Win=65535 Len=0
2146	45.331575977	10.0.2.4	34.149.100.209	TCP	54	55410 → 443 [ACK] Seq=6440 Ack=508003 Win=65535 Len=0
2149	45.332755952	10.0.2.4	34.149.100.209	TCP	54	55410 → 443 [ACK] Seq=6440 Ack=503823 Win=65535 Len=0
2150	45.332829491	10.0.2.4	34.149.100.209	TCP	54	55410 → 443 [ACK] Seq=6440 Ack=508203 Win=65535 Len=0
2151	45.333354798	34.149.100.209	10.0.2.4	TCP	602	443 → 55410 [PSH, ACK] Seq=508203 Ack=6440 Win=32376 Len=548 [TCP segment of a reassembled PDU]
2153	45.334031726	10.0.2.4	34.149.100.209	TCP	54	55410 → 443 [ACK] Seq=6440 Ack=510211 Win=65535 Len=0
2156	45.334537193	10.0.2.4	34.149.100.209	TCP	54	55410 → 443 [ACK] Seq=6440 Ack=514591 Win=65535 Len=0
2159	45.335580759	10.0.2.4	34.149.100.209	TCP	54	55410 → 443 [ACK] Seq=6440 Ack=517271 Win=65535 Len=0
2162	45.336709560	10.0.2.4	34.149.100.209	TCP	54	55410 → 443 [ACK] Seq=6440 Ack=521555 Win=65535 Len=0
2165	45.337245044	10.0.2.4	34.149.100.209	TCP	54	55410 → 443 [ACK] Seq=6440 Ack=524475 Win=65535 Len=0
2169	45.338460307	10.0.2.4	34.149.100.209	TCP	54	55410 → 443 [ACK] Seq=6440 Ack=527395 Win=65535 Len=0
2171	45.338839841	10.0.2.4	34.149.100.209	TCP	54	55410 → 443 [ACK] Seq=6440 Ack=531775 Win=65535 Len=0
2175	45.340445492	10.0.2.4	34.149.100.209	TCP	54	55410 → 443 [ACK] Seq=6440 Ack=534215 Win=65535 Len=0
2176	45.340595177	10.0.2.4	34.149.100.209	TCP	54	55410 → 443 [ACK] Seq=6440 Ack=538595 Win=65535 Len=0
2180	45.341620939	10.0.2.4	34.149.100.209	TCP	54	55410 → 443 [ACK] Seq=6440 Ack=541515 Win=65535 Len=0
2183	45.342372501	10.0.2.4	34.149.100.209	TCP	54	55410 → 443 [ACK] Seq=6440 Ack=544435 Win=65535 Len=0
2186	45.343066753	10.0.2.4	34.149.100.209	TCP	54	55410 → 443 [ACK] Seq=6440 Ack=547355 Win=65535 Len=0
2187	45.343871611	10.0.2.4	142.250.77.99	TCP	54	[TCP Keep-Alive] 52530 → 80 [ACK] Seq=412 Ack=569 Win=31624 Len=0
2189	45.344078047	142.250.77.99	10.0.2.4	TCP	60	[TCP Keep-Alive ACK] 80 → 52530 [ACK] Seq=509 Ack=413 Win=32356 Len=0
2191	45.344189266	10.0.2.4	34.149.100.209	TCP	54	55410 → 443 [ACK] Seq=6440 Ack=550275 Win=65535 Len=0
2192	45.344284176	10.0.2.4	34.149.100.209	TCP	54	55410 → 443 [ACK] Seq=6440 Ack=553195 Win=65535 Len=0
2195	45.345394826	10.0.2.4	34.149.100.209	TCP	54	55410 → 443 [ACK] Seq=6440 Ack=556855 Win=65535 Len=0
2198	45.346252561	10.0.2.4	34.149.100.209	TCP	54	55410 → 443 [ACK] Seq=6440 Ack=562695 Win=65535 Len=0
2202	45.346684528	10.0.2.4	34.149.100.209	TCP	54	55410 → 443 [ACK] Seq=6440 Ack=565615 Win=65535 Len=0

Frame 2983: 54 bytes on wire (432 bits), 54 bytes captured (432 bits) on interface eth0, id 0
 Ethernet II, Src: PCSystemtec_d2:26:79 (08:00:27:d2:26:79), Dst: 52:54:00:12:35:00 (52:54:00:12:35:00)
 Internet Protocol Version 4, Src: 10.0.2.4, Dst: 35.244.181.201
 Transmission Control Protocol, Src Port: 53689, Dst Port: 443, Seq: 1555, Ack: 6124, Len: 0

Transmission Control Protocol: Protocol
 Packets: 3018 · Displayed: 1905 (63.1%) · Dropped: 0 (0.0%)

No.	Time	Source	Destination	Protocol	Length	Info
75	16.944240882	34.36.137.203	10.0.2.4	TCP	60	443 → 57870 [CK] Seq=3915 Ack=1003 Win=31766 Len=0
80	19.159291971	10.0.2.4	142.251.222.202	TCP	74	55616 → 443 [YN] 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 [YN, 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 [CK] Seq=1 Ack=1 Win=32120 Len=0
87	19.204348210	10.0.2.4	142.251.222.202	TCP	54	55616 → 443 [CK] Seq=518 Ack=2921 Win=38660 Len=0
89	19.204856220	10.0.2.4	142.251.222.202	TCP	54	55616 → 443 [CK] Seq=518 Ack=3194 Win=38660 Len=0
98	19.252945369	10.0.2.4	142.250.77.99	TCP	74	46670 → 80 [SN] 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 [SN, 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 [CK] Seq=1 Ack=1 Win=32120 Len=0
104	19.267063734	10.0.2.4	34.107.243.93	TCP	74	57656 → 443 [YN] Seq=0 Win=32120 Len=0 MSS=1460 SACK_PERM TSval=1330584674 TSecr=0 WS=128
105	19.277875585	34.107.243.93	10.0.2.4	TCP	60	443 → 57656 [YN, ACK] Seq=0 Ack=1 Win=32768 Len=0 MSS=1460
106	19.277902171	10.0.2.4	34.107.243.93	TCP	54	57656 → 443 [CK] Seq=1 Ack=1 Win=32120 Len=0
109	19.301979990	10.0.2.4	34.107.243.93	TCP	54	57656 → 443 [CK] Seq=518 Ack=2921 Win=38660 Len=0
111	19.302507771	10.0.2.4	34.107.243.93	TCP	54	57656 → 443 [CK] Seq=518 Ack=3119 Win=38660 Len=0
113	19.325230709	10.0.2.4	142.250.77.99	TCP	54	45076 → 80 [CK] Seq=433 Ack=510 Win=31024 Len=0
118	19.360529930	10.0.2.4	23.15.37.18	TCP	74	42474 → 80 [SN] Seq=0 Win=32120 Len=0 MSS=1460 SACK_PERM TSval=1289996890 TSecr=0 WS=128
119	19.365526230	23.15.37.18	10.0.2.4	TCP	60	80 → 42474 [SN, ACK] Seq=0 Ack=1 Win=32768 Len=0 MSS=1460
120	19.365621840	10.0.2.4	23.15.37.18	TCP	54	42474 → 80 [CK] Seq=1 Ack=1 Win=32120 Len=0
124	19.378105046	142.251.222.202	10.0.2.4	TCP	60	443 → 55616 [CK] Seq=3194 Ack=752 Win=32017 Len=0
127	19.381102631	10.0.2.4	142.251.222.202	TCP	54	55616 → 443 [CK] Seq=1303 Ack=3008 Win=30660 Len=0
129	19.383570790	10.0.2.4	23.15.37.18	TCP	54	42474 → 80 [CK] Seq=417 Ack=890 Win=31231 Len=0
134	19.429302580	10.0.2.4	142.251.222.202	TCP	54	55616 → 443 [CK] Seq=1394 Ack=5299 Win=30660 Len=0
135	19.429371355	10.0.2.4	142.251.222.202	TCP	54	55616 → 443 [CK] Seq=1394 Ack=8219 Win=30660 Len=0
136	19.430397010	10.0.2.4	142.251.222.202	TCP	54	55616 → 443 [CK] Seq=1394 Ack=11231 Win=30660 Len=0
141	19.431312000	10.0.2.4	142.251.222.202	TCP	54	55616 → 443 [CK] 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

No.	Time	Source	Destination	Protocol	Length	Info
50	16.687548884	34.160.144.191	10.0.2.4	TLSv1.2	2974	Server Hello, Certificate
52	16.688889158	34.160.144.191	10.0.2.4	TLSv1.2	197	Server Key Exchange, Server Hello Done
54	16.692604326	10.0.2.4	34.160.144.191	TLSv1.2	147	Client Key Exchange, Change Cipher Spec, Encrypted Handshake Message
56	16.704004564	34.160.144.191	10.0.2.4	TLSv1.2	418	New Session Ticket, Change Cipher Spec, Encrypted Handshake Message, Application Data
63	16.843321967	10.0.2.4	34.160.144.191	TLSv1.2	231	Application Data
64	16.847432379	10.0.2.4	34.160.144.191	TLSv1.2	301	Application Data
66	16.848474748	10.0.2.4	34.160.144.191	TLSv1.2	92	Application Data
67	16.853997621	34.160.144.191	10.0.2.4	TLSv1.2	92	Application Data
69	16.865274792	34.160.144.191	10.0.2.4	TLSv1.2	4434	Application Data, Application Data, Application Data
71	16.865717216	34.160.144.191	10.0.2.4	TLSv1.2	1482	Application Data, Application Data, Application Data
73	16.867143168	10.0.2.4	34.160.144.191	TLSv1.2	100	Application Data
284	19.859366336	10.0.2.4	34.149.100.209	TLSv1.2	272	Client Hello (SNI=firefox.settings.services.mozilla.com)
286	19.889307387	34.149.100.209	10.0.2.4	TLSv1.2	1466	Server Hello
288	19.881771534	34.149.100.209	10.0.2.4	TLSv1.2	1514	Certificate
290	19.882311373	34.149.100.209	10.0.2.4	TLSv1.2	308	Server Key Exchange, Server Hello Done
292	19.907464382	10.0.2.4	34.149.100.209	TLSv1.2	147	Client Key Exchange, Change Cipher Spec, Encrypted Handshake Message
293	19.921170133	34.149.100.209	10.0.2.4	TLSv1.2	418	New Session Ticket, Change Cipher Spec, Encrypted Handshake Message, Application Data
300	20.602046610	10.0.2.4	34.149.100.209	TLSv1.2	231	Application Data
301	20.602366994	10.0.2.4	34.149.100.209	TLSv1.2	303	Application Data
302	20.602583556	10.0.2.4	34.149.100.209	TLSv1.2	92	Application Data
304	20.610508040	34.149.100.209	10.0.2.4	TLSv1.2	92	Application Data
306	20.621735767	34.149.100.209	10.0.2.4	TLSv1.2	696	Application Data, Application Data, Application Data
308	20.628509821	10.0.2.4	34.149.100.209	TLSv1.2	100	Application Data
311	20.911692297	10.0.2.4	34.149.100.209	TLSv1.2	193	Application Data
312	20.924128089	34.149.100.209	10.0.2.4	TLSv1.2	161	Application Data

Frame 310, 1514 bytes on wire (12112 bits), 1514 bytes captured (12112 bits) on interface eth0, id 0

Ethernet II, Src: 52:54:00:12:35:00 (52:54:00:12:35:00), Dst: PCSsystemec_d2:26:79 (08:00:27:d2:26:79)

Internet Protocol Version 4, Src: 34.149.100.209, Dst: 10.0.2.4

Transmission Control Protocol, Src Port: 443, Dst Port: 55410, Seq: 4278, Ack: 961, Len: 1460

Transport Layer Security

0000 00 00 27 d2 26 79 52 54 00 12 35 00 00 00 45 00 ...&yRT 5 E

0010 05 dc 00 fc 09 00 ff 06 21 b6 22 95 64 d1 0a 00 ...! " d

0020 02 04 01 bb d8 72 00 00 2b d5 c6 c2 fb 2f 50 18 ...r + /P

0030 7c 40 f6 1e 00 00 17 03 03 05 7f 00 00 00 00 00 ... dv V7U

0040 00 00 07 e7 0a 64 76 ac 5f a0 50 37 55 00 b5 1d ...9 s P c

0050 96 f6 9f 92 39 cc 5f a2 20 b4 73 b7 50 1b 63 81

TLS Analysis:

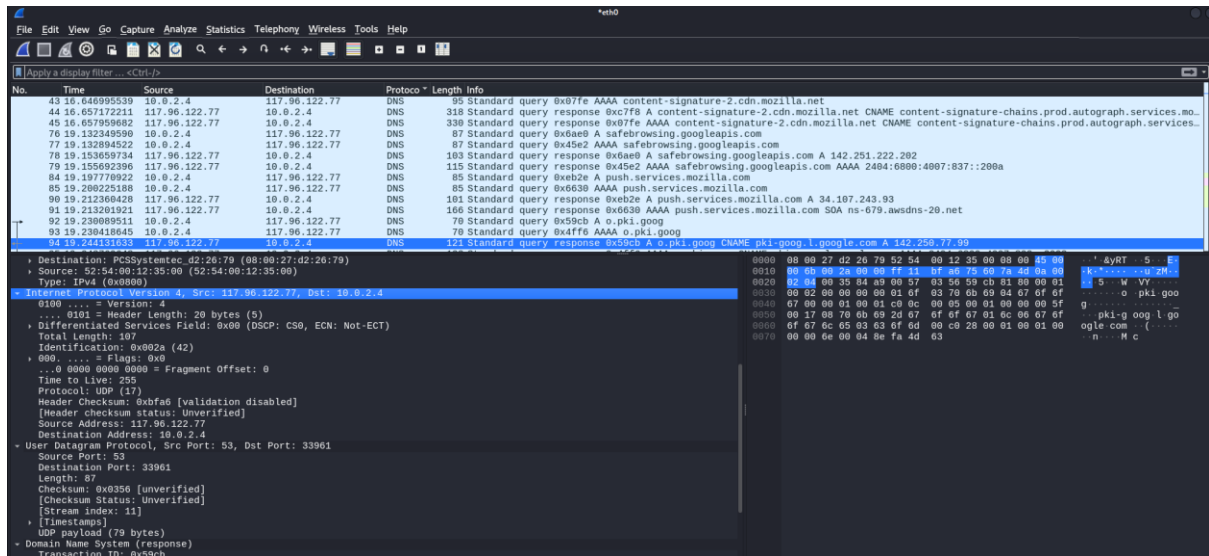
- TLS Handshake Elements:
 - Client Hello
 - Server Hello
 - Certificate exchanges
 - Encrypted application data

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

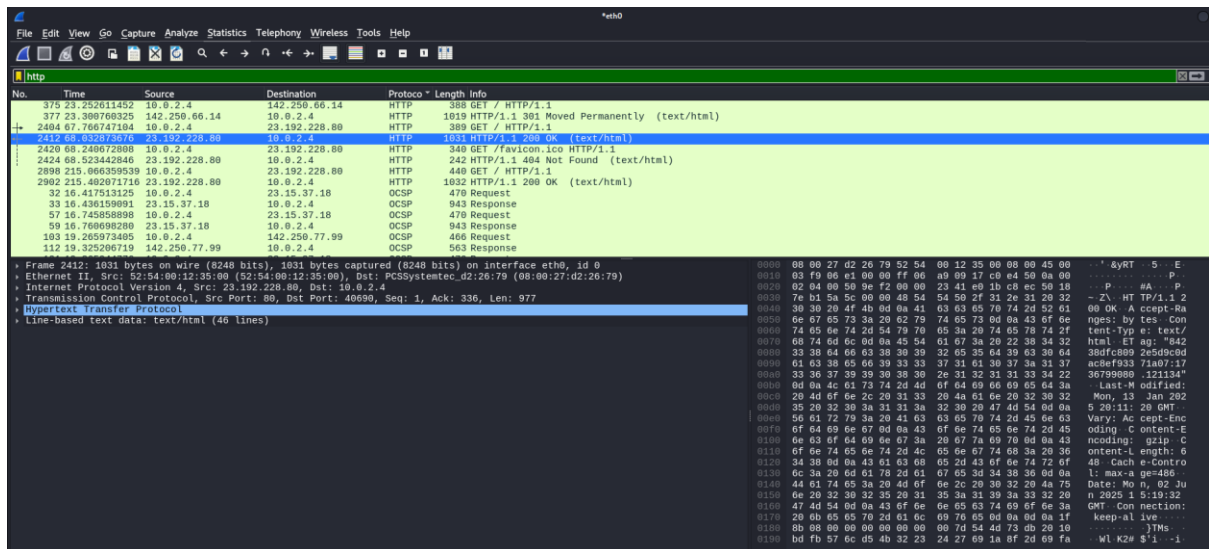


Protocol Stack Analysis

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