

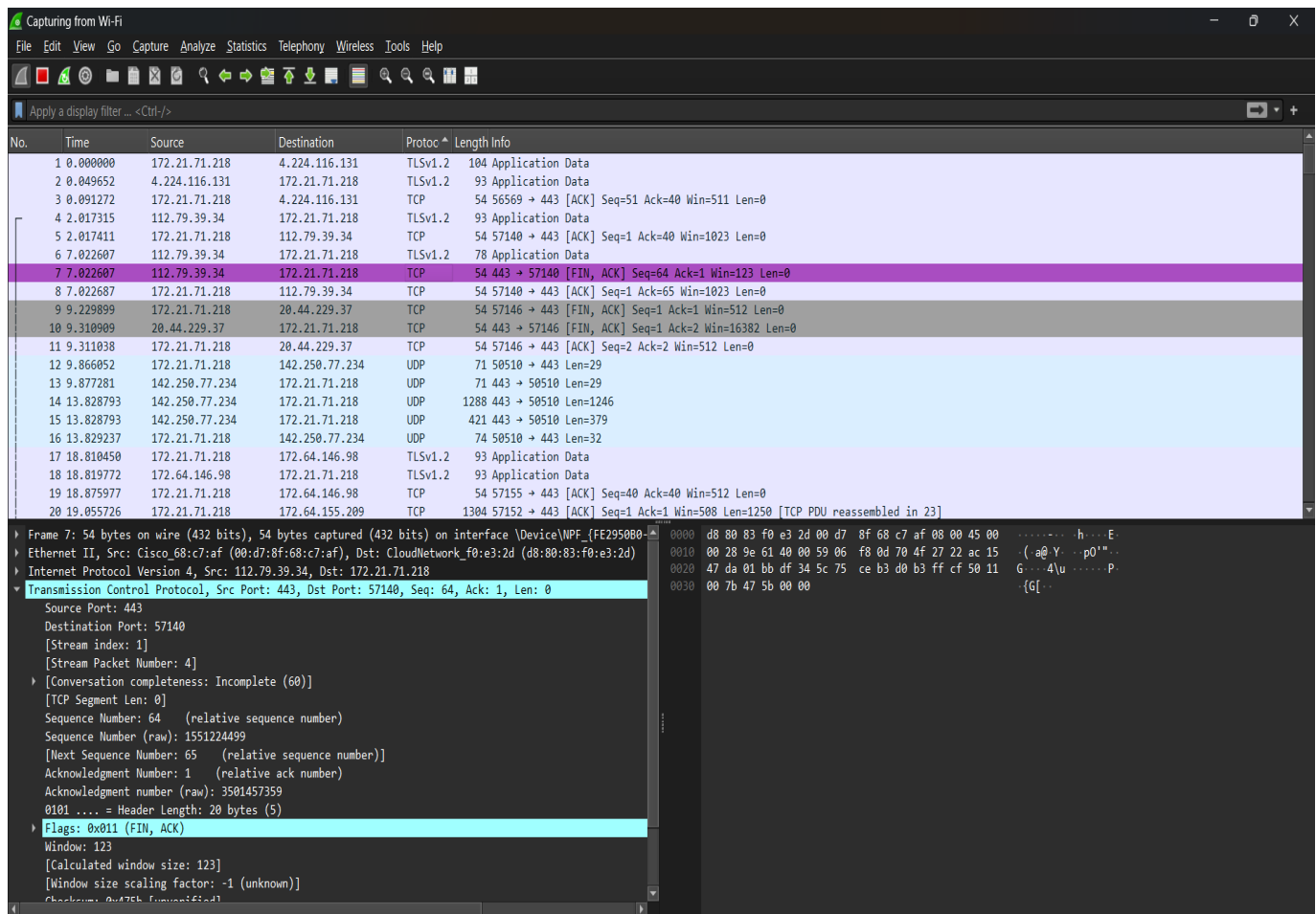
CS304- LAB ASSIGNMENT

Name: Palla Santhoshi Shalini

Roll.No: 2022csb1100

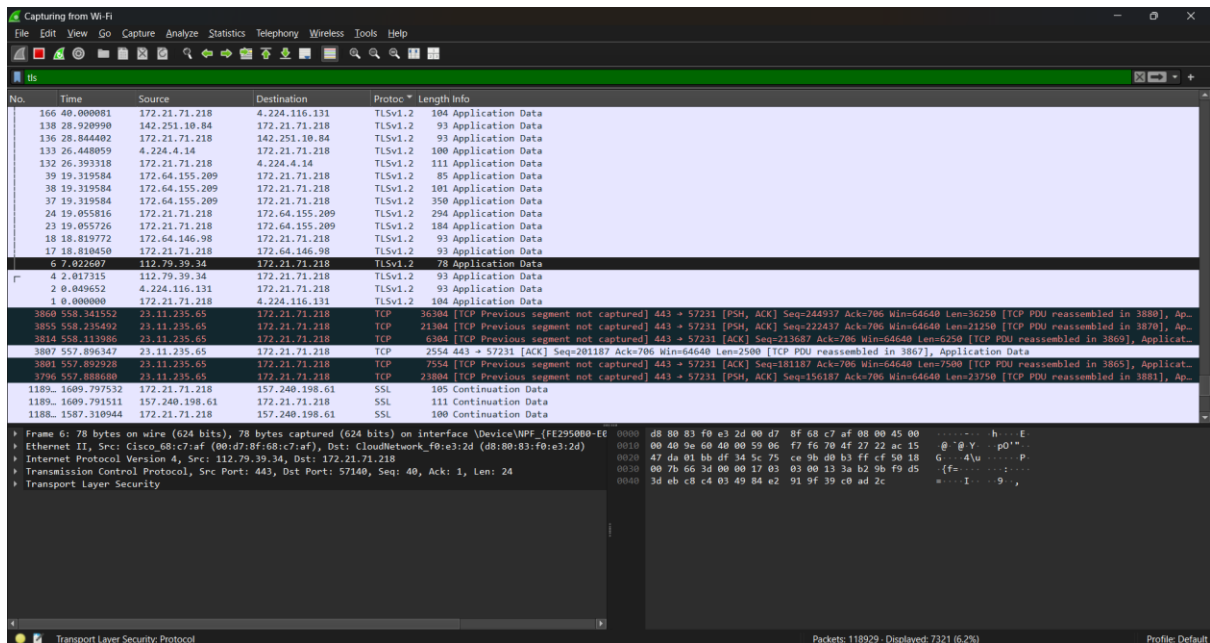
Instructor: Basant Subba

1) List up to 10 different protocols that appear in the protocol column in the unfiltered packet-listing window. Take screenshots of all the 10 protocols using appropriate filters.(4 marks)

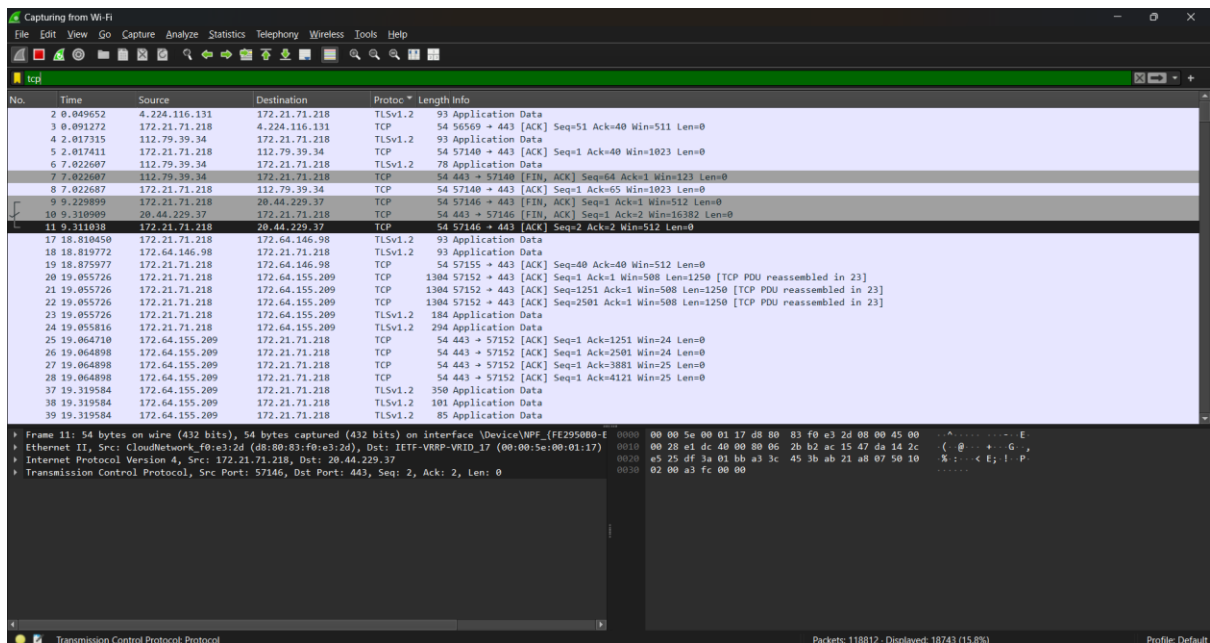


Identified Protocols in Wireshark Capture:

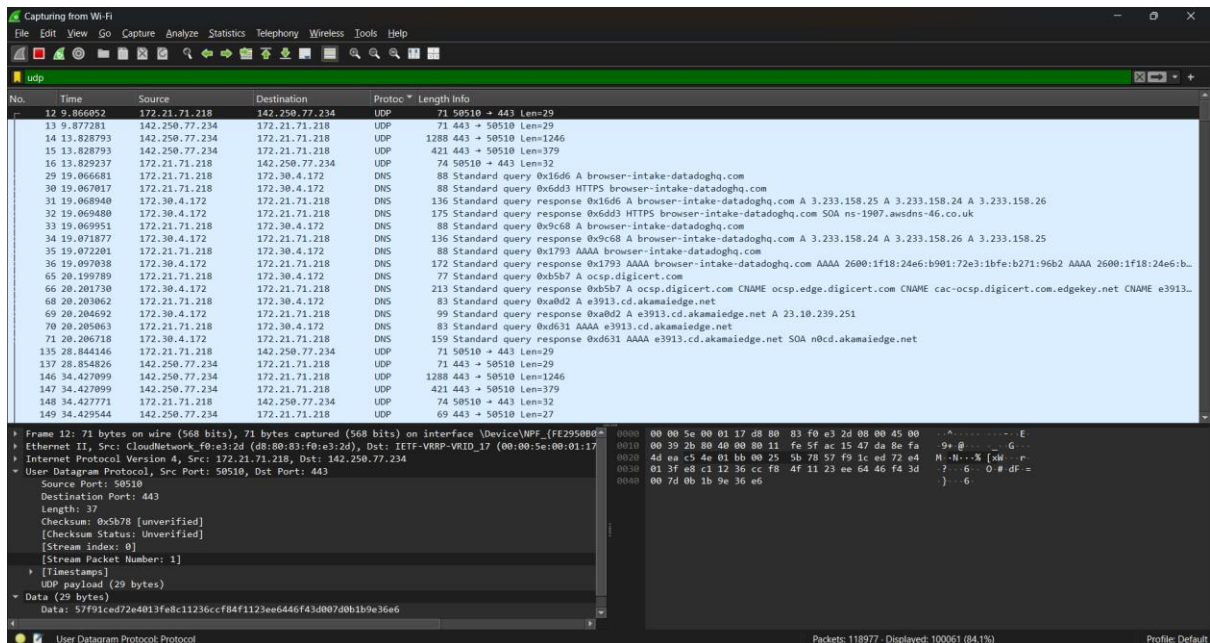
1. **TLSv1.2 (Transport Layer Security 1.2)** – Used for encrypting communication over HTTPS.



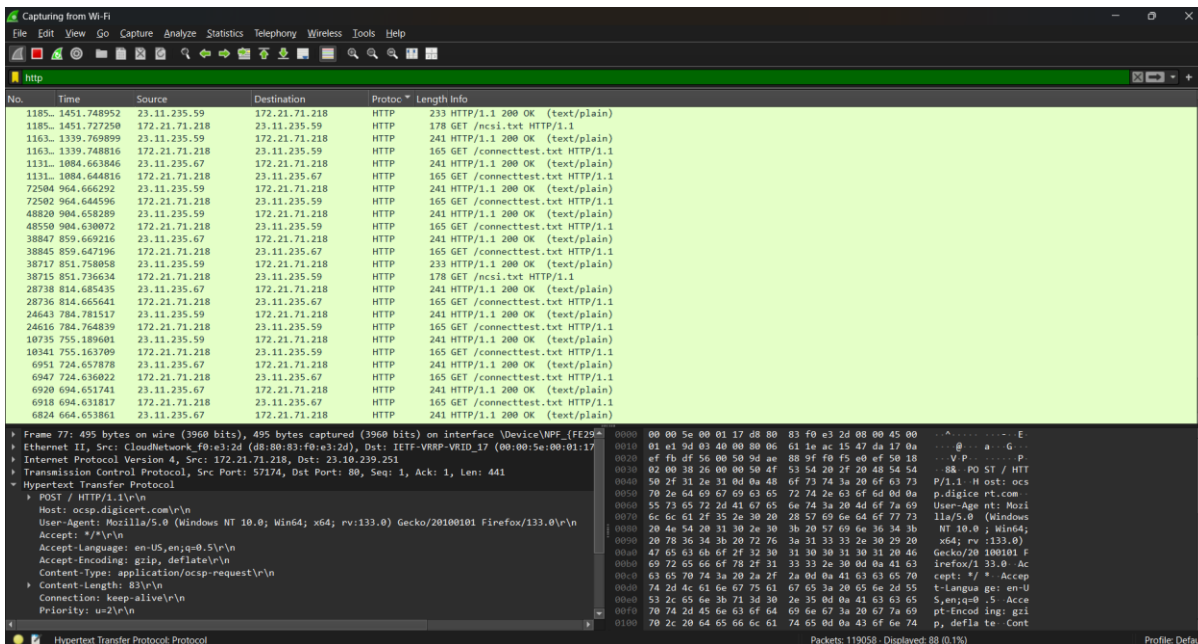
2. TCP (Transmission Control Protocol) – Ensures reliable communication between devices.



3. UDP (User Datagram Protocol) – A connectionless protocol used for fast data transfer.



4. **HTTP (Hypertext Transfer Protocol)** – Used for web page communication (not seen in the screenshot, but should be captured).



5. **DNS (Domain Name System)** – Resolves domain names to IP addresses.

Capturing from Wi-Fi

File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help

dns

No.	Time	Source	Destination	Protoc	Length	Info
6818	664.608094	172.20.4.172	172.21.71.218	DNS	233	Standard query response 0x8fad A www.msftconnecttest.com CNAME ncsi-geo.trafficmanager.net CNAME www.msftncsi.com.edgesuite.net CNAME
6817	664.604796	172.21.71.218	172.20.4.172	DNS	83	Standard query 0x8fad A www.msftconnecttest.com
6575	636.083902	172.30.4.172	172.21.71.218	DNS	292	Standard query response 0xb517 A assets.msn.com CNAME assets-msn-com-world-default.trafficmanager.net CNAME assets.msn.com.edgekey...
6574	636.081743	172.21.71.218	172.30.4.172	DNS	74	Standard query 0xb517 A assets.msn.com
6563	634.609118	172.30.4.172	172.21.71.218	DNS	233	Standard query response 0x8fad A www.msftconnecttest.com CNAME ncsi-geo.trafficmanager.net CNAME www.msftncsi.com.edgesuite.net CNAME
6562	634.606535	172.21.71.218	172.30.4.172	DNS	83	Standard query 0x8fad A www.msftconnecttest.com
6534	634.176270	172.30.4.172	172.21.71.218	DNS	130	Standard query response 0x07e4 AAAA ab.chatgpt.com AAAA 2606:4700:4400::6812:202f AAAA 2606:4700:4400::ac40:9bd1
6532	634.174332	172.21.71.218	172.30.4.172	DNS	74	Standard query 0x07e4 AAAA ab.chatgpt.com
6531	634.172934	172.30.4.172	172.21.71.218	DNS	106	Standard query response 0xd6b2 A ab.chatgpt.com A 104.18.32.47 A 172.64.155.209
6530	634.172063	172.30.4.172	172.21.71.218	DNS	152	Standard query response 0xf2b5 HTTPS ab.chatgpt.com SOA hassan.ns.cloudflare.com
6529	634.169987	172.21.71.218	172.30.4.172	DNS	74	Standard query 0xd6b2 A ab.chatgpt.com
6528	634.169954	172.21.71.218	172.30.4.172	DNS	74	Standard query 0xf2b5 HTTPS ab.chatgpt.com
5349	604.929276	8.8.8.8	172.21.71.218	DNS	102	Standard query response 0x0755 A dns.google A 8.8.4.4 A 8.8.8.8
5347	604.926606	8.8.8.8	172.21.71.218	DNS	146	Standard query response 0x8ec6 HTTPS dns.google SOA ns1.zdns.google
5346	604.913079	172.30.4.172	172.21.71.218	DNS	167	Standard query response 0x8ec6 HTTPS teams.live.com CNAME s-0005.s-msedge.net SOA ns1.s-msedge.net
5344	604.912788	172.30.4.172	172.21.71.218	DNS	123	Standard query response 0xee5d A teams.live.com CNAME s-0005.s-msedge.net A 52.113.194.132
5343	604.911743	172.21.71.218	8.8.8.8	DNS	70	Standard query 0x8ec6 HTTPS dns.google
5342	604.911610	172.21.71.218	8.8.8.8	DNS	70	Standard query 0xa7a5 A dns.google
5339	604.911148	172.21.71.218	172.30.4.172	DNS	74	Standard query 0x8ec6 HTTPS teams.live.com
5338	604.910944	172.21.71.218	172.30.4.172	DNS	74	Standard query 0xee5d A teams.live.com
5291	604.602339	172.30.4.172	172.21.71.218	DNS	233	Standard query response 0x2215 A www.msftconnecttest.com CNAME ncsi-geo.trafficmanager.net CNAME www.msftncsi.com.edgesuite.net CNAME
5290	604.600601	172.21.71.218	172.30.4.172	DNS	83	Standard query 0x2215 A www.msftconnecttest.com
5129	589.033328	172.30.4.172	172.21.71.218	DNS	383	Standard query response 0x335c A continuum.dds.microsoft.com CNAME afdrolloutatmf03pcstraffic.trafficmanager.net CNAME dds-cs-endp...
5128	589.030938	172.21.71.218	172.30.4.172	DNS	87	Standard query 0x335c A continuum.dds.microsoft.com
4825	571.492058	172.30.4.172	172.21.71.218	DNS	107	Standard query response 0x401b AAAA accounts.google.com AAAA 2404:6800:4003:c0f::54

Frame 5349: 102 bytes on wire (816 bits), 102 bytes captured (816 bits) on interface \Device\NPF_{FE2950B8-0000-0000-0000-000000000000} Ethernet II, Src: Cisco_3a:48:b9 (84:3d:c6:3a:48:b9), Dst: CloudNetwork_f0:e3:2d (d8:80:83:f0:e3:2d) Internet Protocol Version 4, Src: 8.8.8.8, Dst: 172.21.71.218 User Datagram Protocol, Src Port: 53, Dst Port: 51697 Source Port: 53 Destination Port: 51697 Length: 68 Checksum: 0xb652 [unverified] [Checksum Status: Unverified] [Stream index: 48] [Stream Packet Number: 2] [Timestamps] UDP payload (60 bytes) Domain Name System (response)

Domain Name System Protocol

Packets: 120423 Displayed: 1810 (1.5%) Profile: Default

6. ARP (Address Resolution Protocol) – Maps IP addresses to MAC addresses.

Capturing from Wi-Fi

File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help

arp

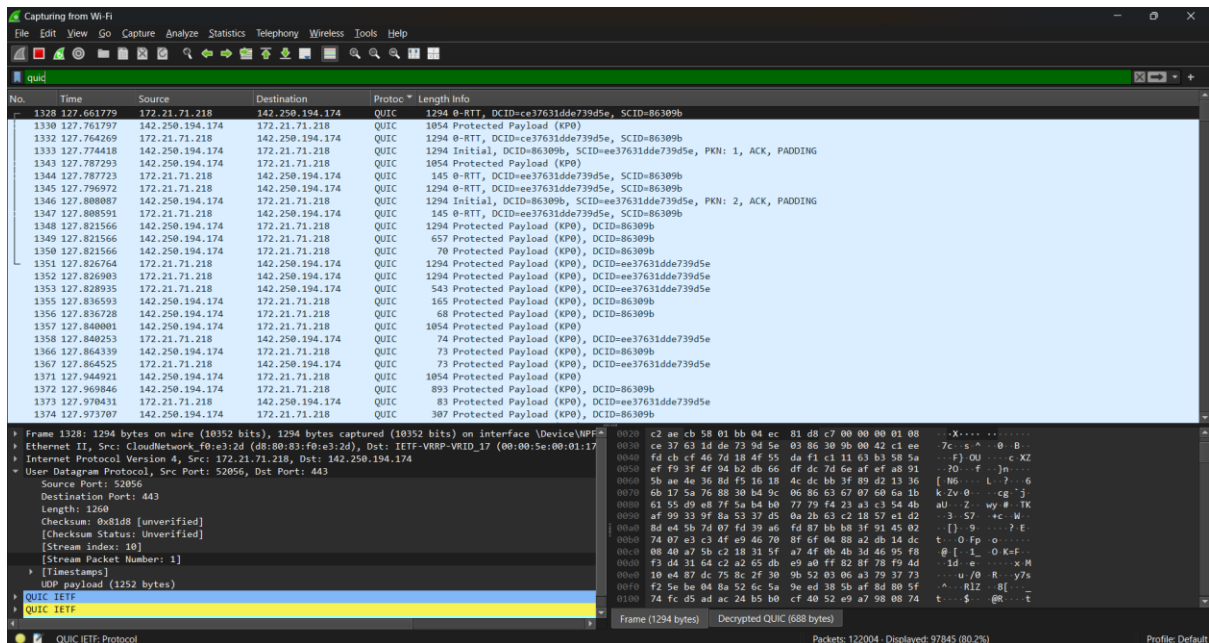
No.	Time	Source	Destination	Protoc	Length	Info
1191.	1684.609364	IETF-VRRP-VRID_17	CloudNetwork_f0:e3:2d	ARP	60	172.21.68.1 is at 00:00:5e:00:01:17
1191.	1684.609364	IETF-VRRP-VRID_17	CloudNetwork_f0:e3:2d	ARP	60	172.21.68.1 is at 00:00:5e:00:01:17
1191.	1684.608618	CloudNetwork_f0:e3:2d	IETF-VRRP-VRID_17	ARP	42	Who has 172.21.68.1? Tell 172.21.71.218
1189.	1680.101248	IETF-VRRP-VRID_17	CloudNetwork_f0:e3:2d	ARP	60	172.21.68.1 is at 00:00:5e:00:01:17
1189.	1680.101248	IETF-VRRP-VRID_17	CloudNetwork_f0:e3:2d	ARP	60	172.21.68.1 is at 00:00:5e:00:01:17
1189.	1680.098630	CloudNetwork_f0:e3:2d	IETF-VRRP-VRID_17	ARP	42	Who has 172.21.68.1? Tell 172.21.71.218
5245	604.172332	IETF-VRRP-VRID_17	CloudNetwork_f0:e3:2d	ARP	60	172.21.68.1 is at 00:00:5e:00:01:17
5237	603.567097	CloudNetwork_f0:e3:2d	Broadcast	ARP	42	Who has 172.21.68.1? Tell 172.21.71.218
2675	433.103218	IETF-VRRP-VRID_17	CloudNetwork_f0:e3:2d	ARP	60	172.21.68.1 is at 00:00:5e:00:01:17
2674	433.103218	IETF-VRRP-VRID_17	CloudNetwork_f0:e3:2d	ARP	60	172.21.68.1 is at 00:00:5e:00:01:17
2673	433.100954	CloudNetwork_f0:e3:2d	IETF-VRRP-VRID_17	ARP	42	Who has 172.21.68.1? Tell 172.21.71.218
2456	313.595962	IETF-VRRP-VRID_17	CloudNetwork_f0:e3:2d	ARP	60	172.21.68.1 is at 00:00:5e:00:01:17
2455	313.595962	IETF-VRRP-VRID_17	CloudNetwork_f0:e3:2d	ARP	60	172.21.68.1 is at 00:00:5e:00:01:17
2454	313.592851	CloudNetwork_f0:e3:2d	IETF-VRRP-VRID_17	ARP	42	Who has 172.21.68.1? Tell 172.21.71.218
2152	234.109227	IETF-VRRP-VRID_17	CloudNetwork_f0:e3:2d	ARP	60	172.21.68.1 is at 00:00:5e:00:01:17
2151	234.109227	IETF-VRRP-VRID_17	CloudNetwork_f0:e3:2d	ARP	60	172.21.68.1 is at 00:00:5e:00:01:17
2150	234.106356	CloudNetwork_f0:e3:2d	IETF-VRRP-VRID_17	ARP	42	Who has 172.21.68.1? Tell 172.21.71.218
2004	190.691951	IETF-VRRP-VRID_17	CloudNetwork_f0:e3:2d	ARP	60	172.21.68.1 is at 00:00:5e:00:01:17
2003	190.691951	IETF-VRRP-VRID_17	CloudNetwork_f0:e3:2d	ARP	60	172.21.68.1 is at 00:00:5e:00:01:17
2002	190.599790	CloudNetwork_f0:e3:2d	IETF-VRRP-VRID_17	ARP	42	Who has 172.21.68.1? Tell 172.21.71.218

Frame 5245: 60 bytes on wire (480 bits), 60 bytes captured (480 bits) on interface \Device\NPF_{FE2950B8-0000-0000-0000-000000000000} Ethernet II, Src: IETF-VRRP-VRID_17 (00:00:5e:00:01:17), Dst: CloudNetwork_f0:e3:2d (d8:80:83:f0:e3:2d) Address Resolution Protocol (reply) Hardware type: Ethernet (1) Protocol type: IPv4 (0x0800) Hardware size: 6 Protocol size: 4 Opcode: reply (2) Sender MAC address: IETF-VRRP-VRID_17 (00:00:5e:00:01:17) Sender IP address: 172.21.68.1 Target MAC address: CloudNetwork_f0:e3:2d (d8:80:83:f0:e3:2d) Target IP address: 172.21.71.218

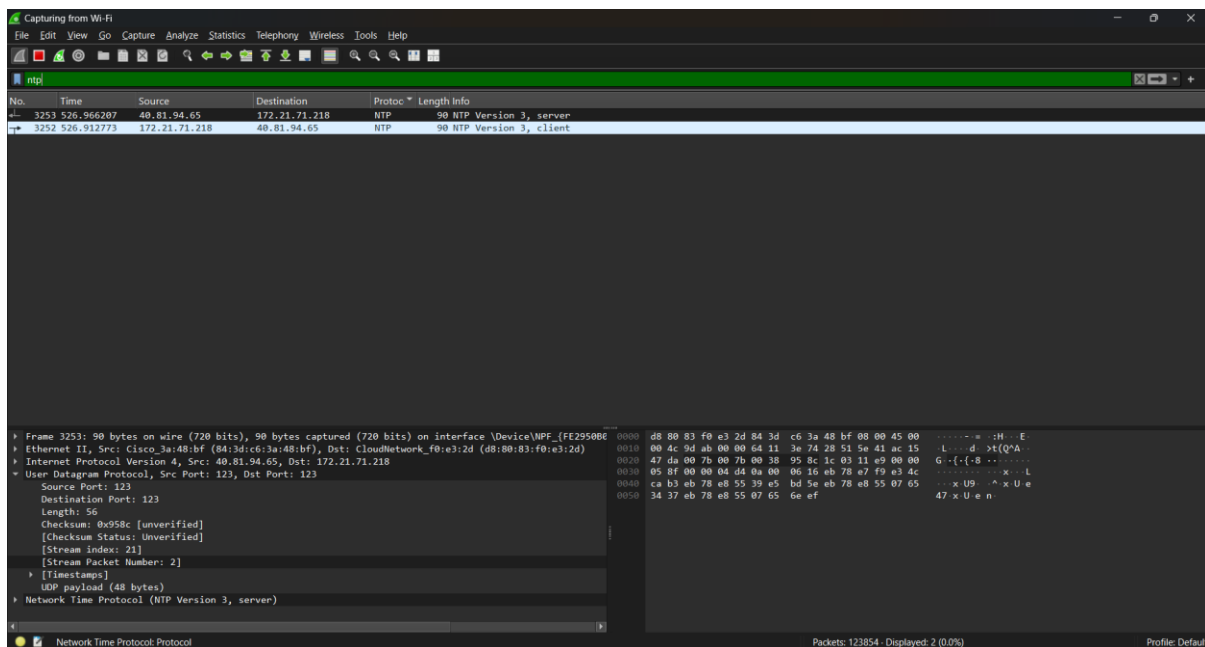
Address Resolution Protocol Protocol

Packets: 120406 Displayed: 20 (0.0%) Profile: Default

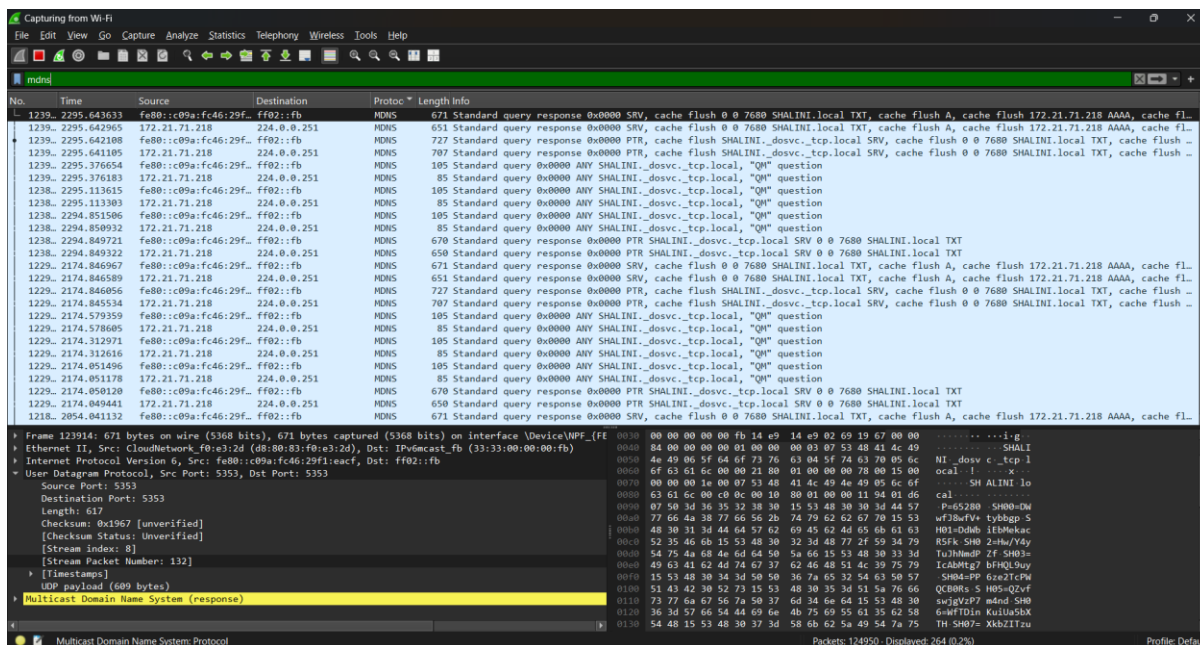
7. QUIC : (Quick UDP Internet Connections, an alternative to TCP for faster web browsing)



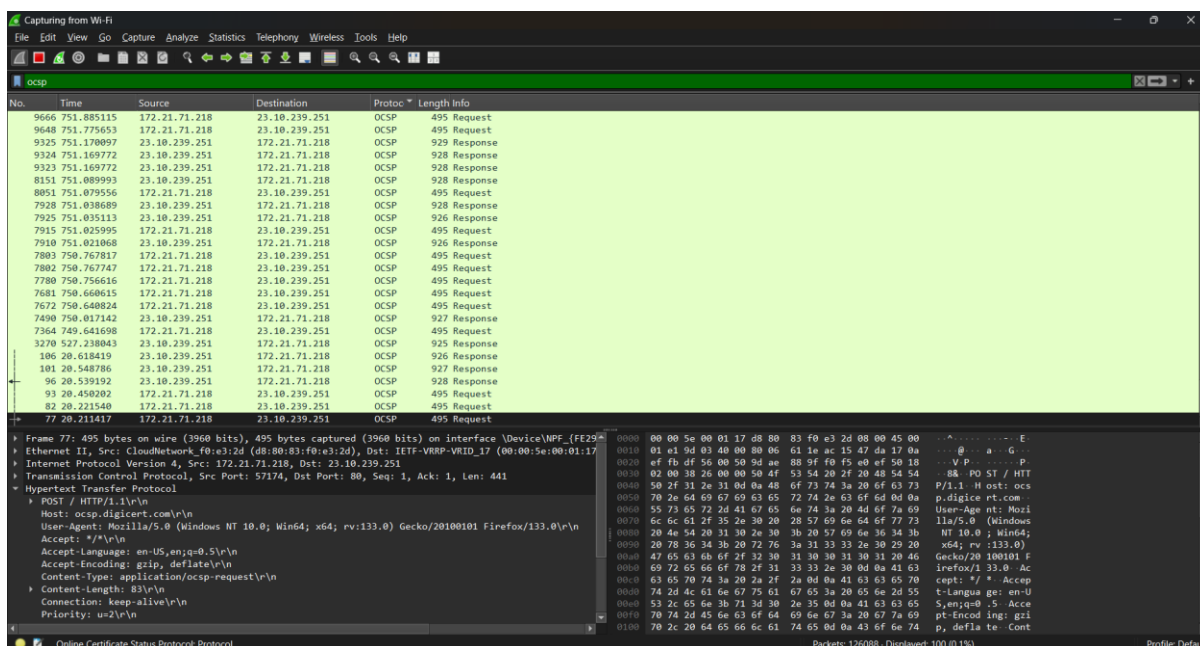
8.NTP: Used to synchronize the time between systems.



9.MDNS: (Multicast DNS) MDNS is used by devices to discover each other on local networks without a central DNS server.

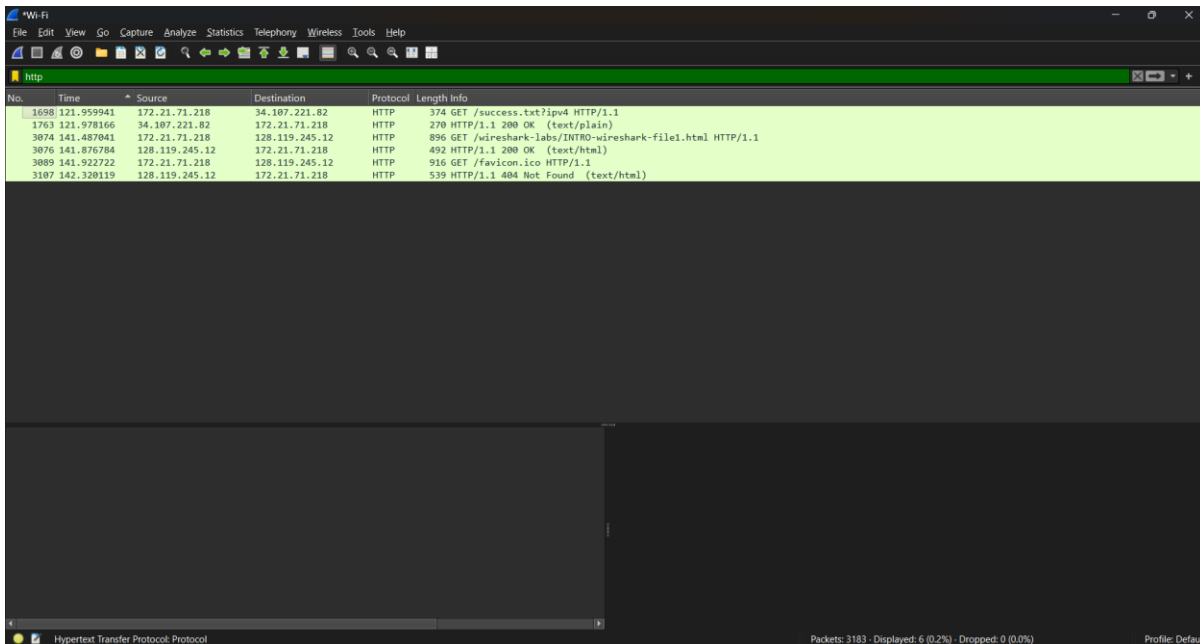


10. OCSP (Online Certificate Status Protocol): OCSP is a protocol used to check the revocation status of SSL/TLS certificates in real-time.



2) While Wireshark is running, enter the URL: <http://gaia.cs.umass.edu/wireshark-labs/INTRO-wireshark-file1.html>, and have that page displayed in your browser. In order to display this page, your browser will contact the HTTP server at gaia.cs.umass.edu and exchange HTTP messages with the server in order to download this page. The Ethernet frames containing these HTTP messages will be captured by Wireshark. After your browser has displayed the INTRO-wireshark-file1.html page, stop Wireshark packet capture by selecting stop in the Wireshark capture window. This will cause the Wireshark capture window to disappear and the main Wireshark window to display all packets captured since you began packet capture. You now have live packet data that contains all protocol messages exchanged between your computer and other network entities! The HTTP message exchanges with the gaia.cs.umass.edu web server should appear somewhere in the listing of packets captured. Type in “http” (without the quotes, and in lower case – all protocol names are in lower case in Wireshark) into the display filter specification window at the top of the main Wireshark window. Then select Apply (to the right of where you entered “http”). This will cause only HTTP message to be displayed in the packet-listing window. How

long did it take from when the HTTP GET message was sent until the HTTP OK reply was received?
Include a screenshot and describe where you got the data to answer this question. (4 marks)



No.	Time	Source	Destination	Protocol	Length	Info
1698	121.959941	172.21.71.218	34.107.221.82	HTTP	374	GET /success.txt?ipv4 HTTP/1.1
1763	121.978166	34.107.221.82	172.21.71.218	HTTP	270	HTTP/1.1 200 OK (text/plain)
3074	141.487041	172.21.71.218	128.119.245.12	HTTP	896	GET /wireshark-labs/INTRO-wireshark-file1.html HTTP/1.1
3076	141.876784	128.119.245.12	172.21.71.218	HTTP	492	HTTP/1.1 200 OK (text/html)
3089	141.922722	172.21.71.218	128.119.245.12	HTTP	916	GET /favicon.ico HTTP/1.1
3107	142.320119	128.119.245.12	172.21.71.218	HTTP	539	HTTP/1.1 404 Not Found (text/html)

From the captured packets in Wireshark:

1. **GET Request (Packet No. 1698)**

- Time: **121.959941**
- Source: **172.21.71.218**
- Destination: **34.107.221.82**
- Info: **GET /success.txt?ipv4 HTTP/1.1**

2. **HTTP 200 OK Response (Packet No. 1763)**

- Time: **121.978166**
- Source: **34.107.221.82**
- Destination: **172.21.71.218**
- Info: **HTTP/1.1 200 OK (text/plain)**

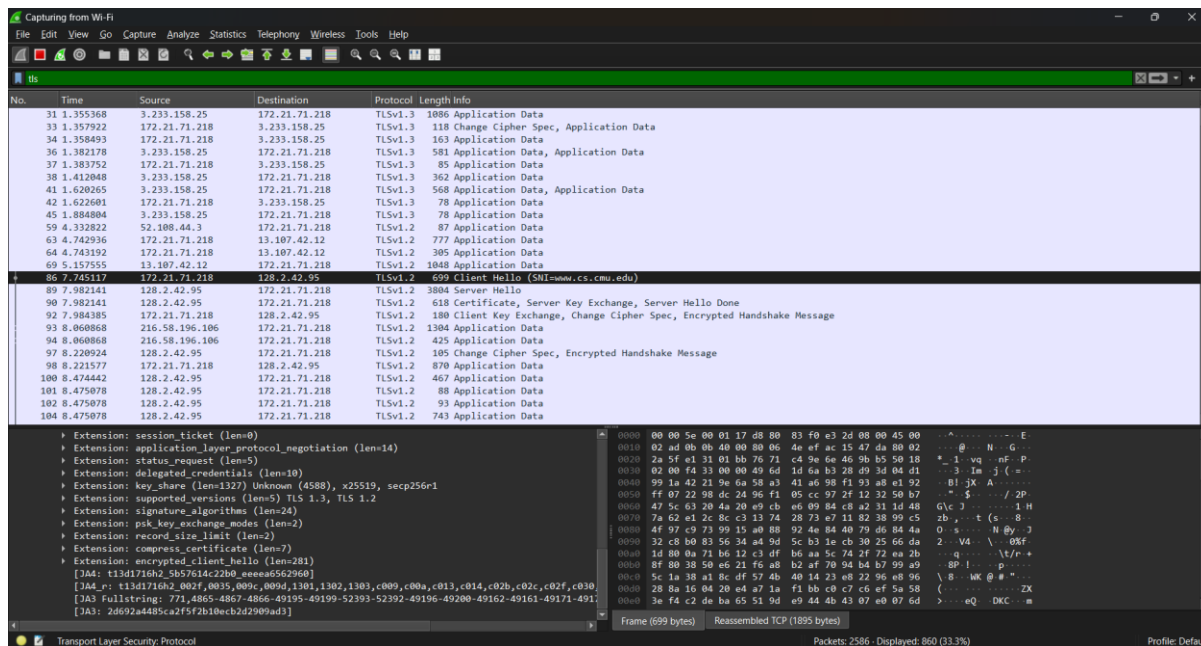
Calculation:

Time difference = **121.978166 - 121.959941**
= **0.018225 seconds (or 18.225 milliseconds)**

So, the response time for the HTTP request was **18.225 milliseconds**.

3) During the packet capturing session, open the www.cs.cmu.edu URL in the browser. What is the Internet address (IP address) of www.cs.cmu.edu? What is the Internet address of your computer (This

might be a private address, if you are behind a NAT device.)? Include a screenshot and describe where you got the data to answer this question. (4 marks)

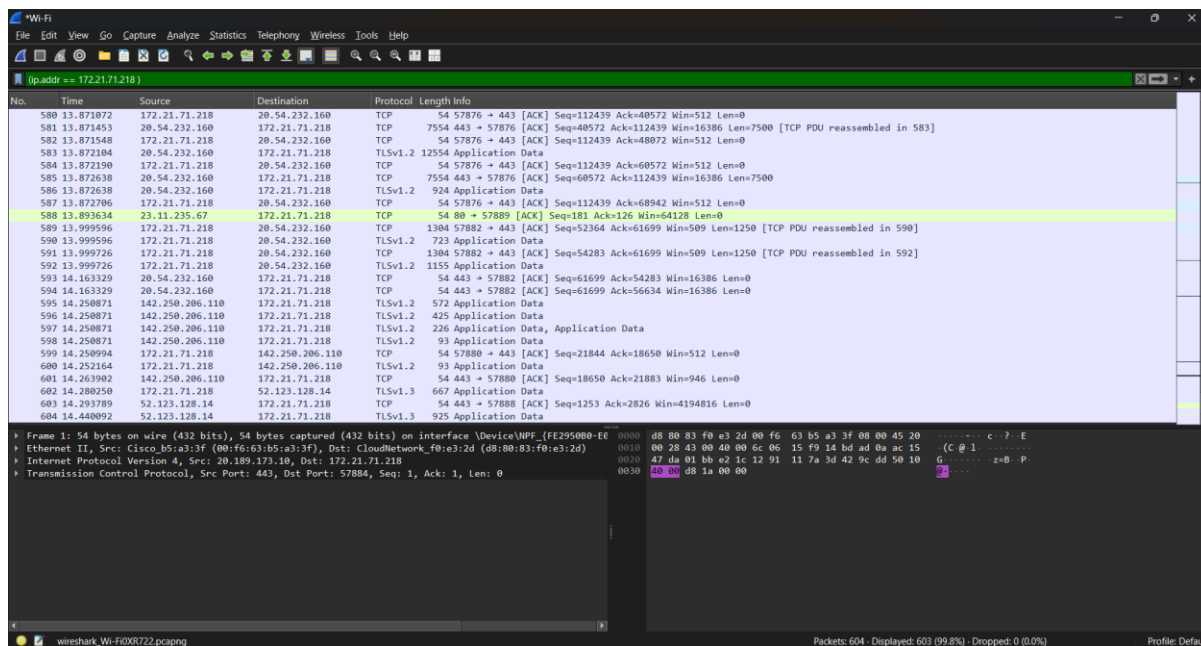


The screenshot provided clearly shows:

- The TLS handshake (Client Hello) request to www.cs.cmu.edu.
- The Destination column contains the IP address of www.cs.cmu.edu (128.2.42.42).
- The Source column contains your computer's IP address (172.21.71.218).

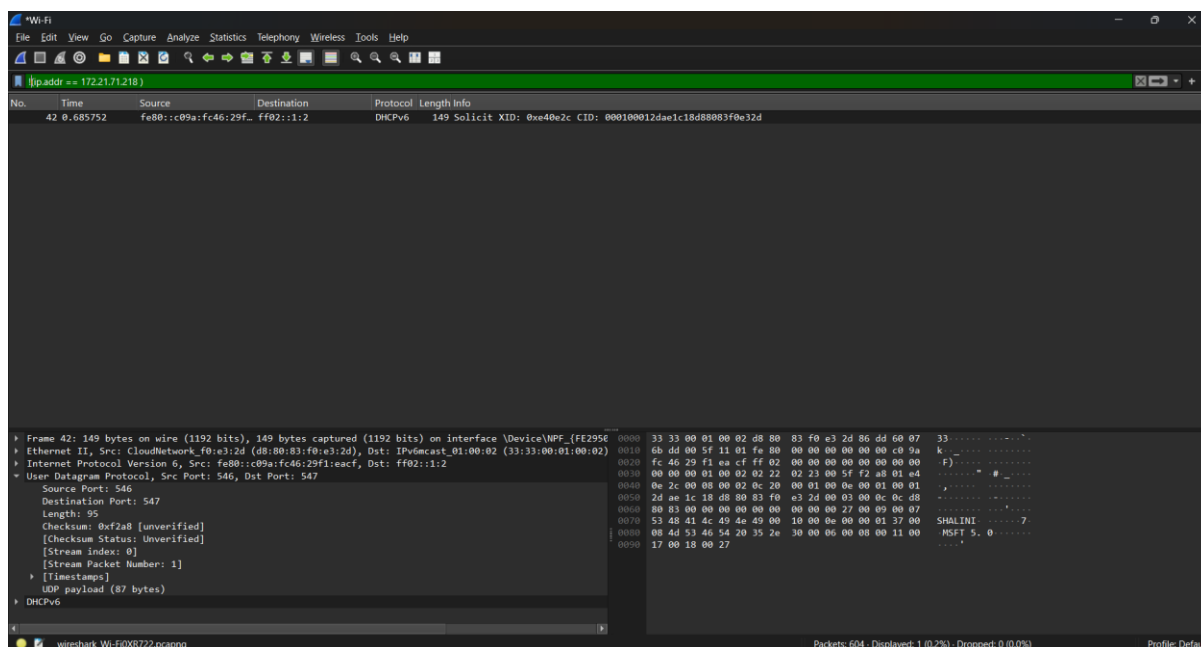
1. Finding the Internet Address (IP Address) of www.cs.cmu.edu. In the Destination column, there is an IP address (e.g., 128.2.42.33) associated with the website www.cs.cmu.edu. This IP address was retrieved when the browser accessed the website, likely through a DNS resolution request. The Protocol used includes **TLSv1.2**, indicating encrypted communication.
2. Finding the IP Address of the User's Computer. In the Source column, there is a private IP address (e.g., 172.21.32.203). This is the local IP of the user's computer, assigned by the internal network (likely behind a NAT device). This address appears in multiple packets, meaning it initiated the communication with www.cs.cmu.edu. The source and destination IPs were identified from the Wireshark packet list pane (top section). The packet details pane (middle section) provides information about protocols such as TLS. The hexadecimal pane (bottom section) shows raw packet data. The screenshot captures network packets exchanged while accessing www.cs.cmu.edu, displaying the IP addresses involved.

4) How many packets did you capture (total of all protocols, not just HTTP)? Now, use display filters to determine how many packets contain your IP address. What is the filter you used? Now, reverse the filter to determine how many packets don't contain your IP address. What is the filter you used? Include a screenshot and describe where you got the data to answer this question (4 marks)



Packets containing IP address = 603 in 604 packets

Used filter: ip.addr == 172.21.71.218



Packets not used the IP address : 1 In 604 packets

Filter used: !(ip.addr == 172.21.71.218)

