

HW2

1)

List 3 different protocols that appear in the protocol column in the unfiltered packet-listing window.

UDP: For especially time-sensitive transfers like video playing or DNS lookups, the User Datagram Protocol, or UDP, is a communication protocol that is used throughout the Internet. It speeds up communications by not formally establishing a connection before data is transferred.

DNS protocol: The Internet's phone book is the Domain Name System (DNS). Humans use domain names like espn.com or nytimes.com to access content online. Through Internet Protocol (IP) addresses, web browsers may communicate. For browsers to load Internet resources, DNS converts domain names to IP addresses. Each Internet-connected device has a distinct IP address that other computers can use to find the device. DNS servers take the place of the necessity for people to remember IP addresses like 192.168.1.1 (in IPv4) or more complicated modern alphanumeric IP addresses like 2400:cb00:2048:1::c629:d7a2 (in IPv6).

QUIC: QUIC (Quick UDP Internet Connections, pronounced quick) is an experimental transport layer network protocol designed by Google. The overall goal is to reduce latency compared to that of TCP. Think of QUIC as being like TCP+TLS+HTTP/2 implemented on UDP.

Here is the screenshot:

No.	Time	Source	Destination	Protocol	Length	Info
250.	488.225578	142.251.42.234	172.17.42.10	UDP	126	443 → 50078 Len=0
251.	488.225579	142.251.42.234	172.17.42.10	UDP	71	443 → 50078 Len=25
252.	488.227285	172.17.42.10	142.251.42.234	UDP	75	50078 → 443 Len=33
253.	488.248353	172.17.42.10	8.8.8.8	DNS	70	Standard query 0xa7d9 A dns.google
254.	488.248434	172.17.42.10	8.8.8.8	DNS	70	Standard query 0xa7da HTTPS dns.google
255.	488.248875	8.8.8.8	172.17.42.10	DNS	102	Standard query response 0xa7d9 A dns.google A 8.8.4.4 A 8.8.8.8
256.	488.249359	8.8.8.8	172.17.42.10	DNS	150	Standard query response 0xa7da HTTPS dns.google SOA ns1.zdns.google
257.	488.249968	172.17.42.10	8.8.4.4	QUIC	1292	Initial, DCID=ea5a13786a4f4, PKN: 1, PADDING, PING, PING, PADDING, CRYPTO, CRYPTO, CRYPTO, CRYPTO
258.	488.258187	172.17.42.10	8.8.4.4	QUIC	117	0-RTT, DCID=ea5a13786a4f4
259.	488.258378	172.17.42.10	8.8.4.4	QUIC	288	0-RTT, DCID=ea5a13786a4f4
260.	488.258416	172.17.42.10	8.8.4.4	QUIC	256	0-RTT, DCID=ea5a13786a4f4
261.	488.253453	172.17.42.10	172.17.41.227	MNRS	392	Standard query response 0x0000 PTR Ralph's MacBook Pro_companion-Link_tcp.local SRV, cache flush
262.	488.262789	8.8.4.4	172.17.42.10	QUIC	1292	Protected Payload (KPB)
263.	488.262790	8.8.4.4	172.17.42.10	QUIC	830	Protected Payload (KPB)
264.	488.262791	8.8.4.4	172.17.42.10	QUIC	183	Protected Payload (KPB)
265.	488.262791	8.8.4.4	172.17.42.10	QUIC	71	Protected Payload (KPB)
266.	488.263120	172.17.42.10	8.8.4.4	QUIC	120	Handshake, DCID=ea5a13786a4f4
267.	488.263149	172.17.42.10	8.8.4.4	QUIC	75	Protected Payload (KPB), DCID=ea5a13786a4f4
268.	488.266296	8.8.4.4	172.17.42.10	QUIC	71	Protected Payload (KPB)
269.	488.266296	8.8.4.4	172.17.42.10	QUIC	839	Protected Payload (KPB)
270.	488.266297	8.8.4.4	172.17.42.10	QUIC	68	Protected Payload (KPB)

> Frame 26052: 86 bytes on wire (688 bits), 86 bytes captured (688 bits) on interface en0,
 > Ethernet II, Src: 08:c5:85:51:fa:00 (08:c5:85:51:fa:00), Dst: Apple-49:8a:59 (3c:86:30:4
 > Internet Protocol Version 6, Src: fe80::146e:56d7:ce17:a914, Dst: fe80::164:bb82:9ffd:942
 > Internet Control Message Protocol v6

0000 3c 06 30 49 8a 59 0a c5 05 51 fa 00 86 dd 60 00 <0I Y...Q...
 0010 00 00 00 20 3a ff fe 08 00 00 00 00 00 00 24 0e:.....
 0020 56 d7 ce 17 a9 14 fe 80 00 00 00 00 00 00 00 64 V.....d
 0030 bb 82 9f fd 09 42 87 00 c5 4b 00 00 00 00 fe 80B...K.....
 0040 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00d.....B
 0050 0a c5 05 51 fa 00Q...

wireshark_Wi-FiCXBUT.pcapng Packets: 26054 · Displayed: 26054 (100.0%) · Dropped: 0 (0.0%) Profile: Default

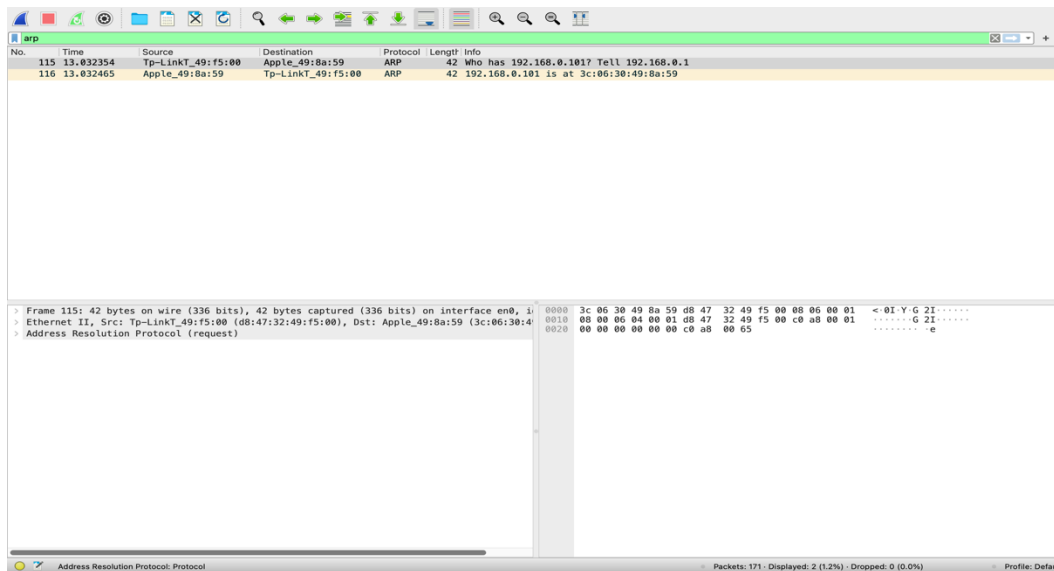
2)

ARP protocol: **Address Resolution Protocol (ARP)** is a procedure for mapping a dynamic IP address to a permanent physical machine address in a local area network (LAN). The physical machine address is also known as a media access control (MAC) address.

How do you find out ARP packets by using Wireshark?

First, I observe the traffic captured in the top Wireshark packet list pane. Look for traffic with ARP listed as the protocol. To view only ARP traffic, I type arp (lower case) in the Filter box and press Enter.

Here is the screenshot:



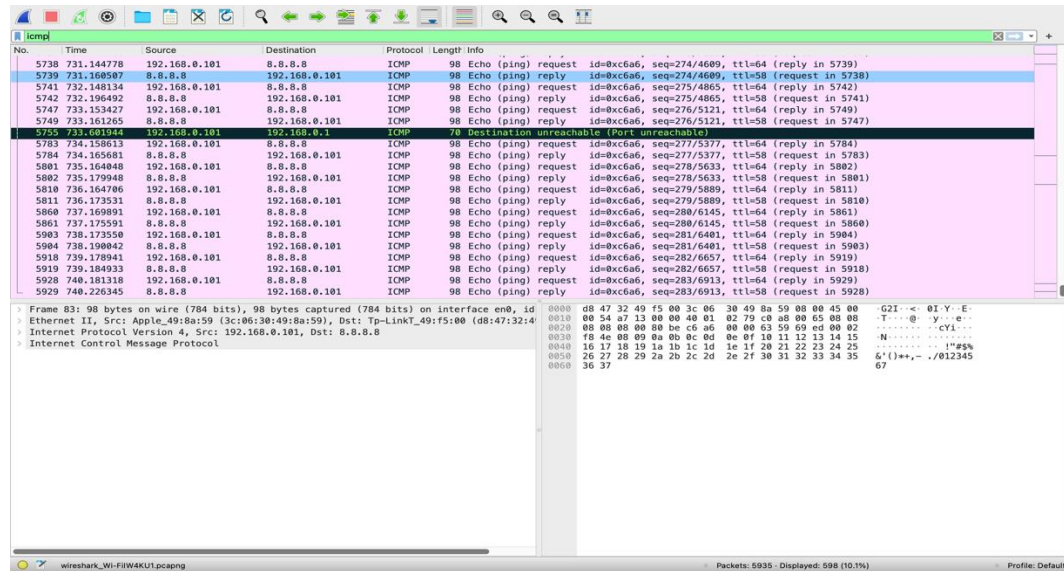
3)

ICMP protocol: **The Internet Control Message Protocol (ICMP)** is a network layer protocol used by network devices to diagnose network communication issues. ICMP is mainly used to determine whether data is reaching its intended destination in a timely manner or not. Commonly, the ICMP protocol is used on network devices, such as routers. ICMP is crucial for error reporting and testing, but it can also be used in distributed denial-of-service (DDoS) attacks.

How do you find out ICMP packets by using Wireshark?

- I use the ping tool to get ICMP requests and replies.
- I open the terminal on Mac.
- Run Wireshark
- Run the below command:
ping 8.8.8.8

Here is the screenshot:



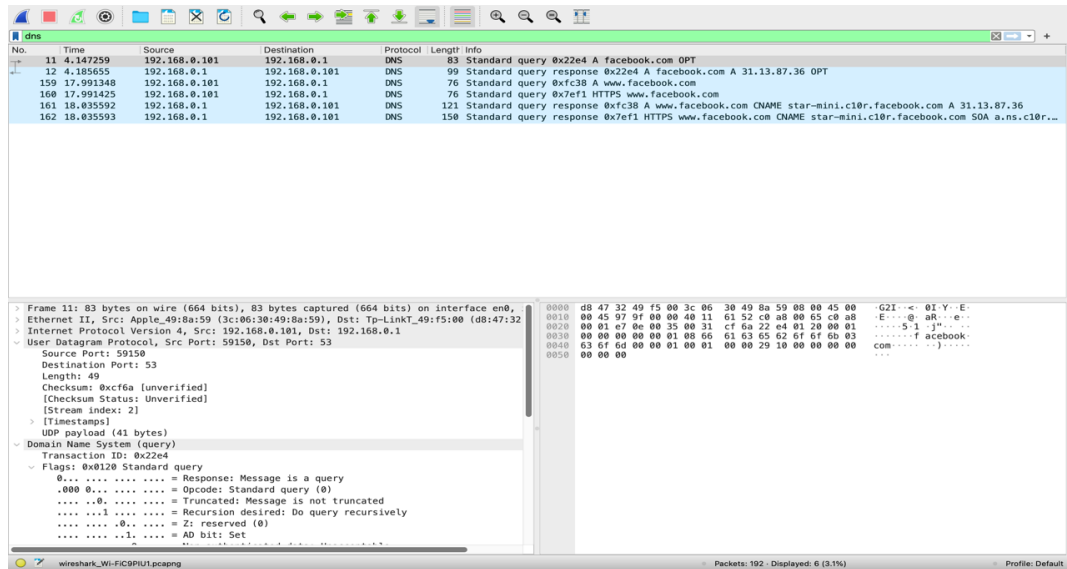
4)

DNS protocol: The Internet's phone book is the Domain Name System (DNS). Humans use domain names like `espn.com` or `nytimes.com` to access content online. Through Internet Protocol (IP) addresses, web browsers may communicate. For browsers to load Internet resources, DNS converts domain names to IP addresses. Each Internet-connected device has a distinct IP address that other computers can use to find the device. DNS servers take the place of the necessity for people to remember IP addresses like `192.168.1.1` (in IPv4) or more complicated modern alphanumeric IP addresses like `2400:cb00:2048:1::c629:d7a2` (in IPv6).

How do you find out DNS packets by using Wireshark?

- I use the `dig` tool to get DNS requests and replies.
- I open the terminal on Mac.
- Run Wireshark.
- Run the below command:
`dig facebook.com`

Here is the screenshot:



5)

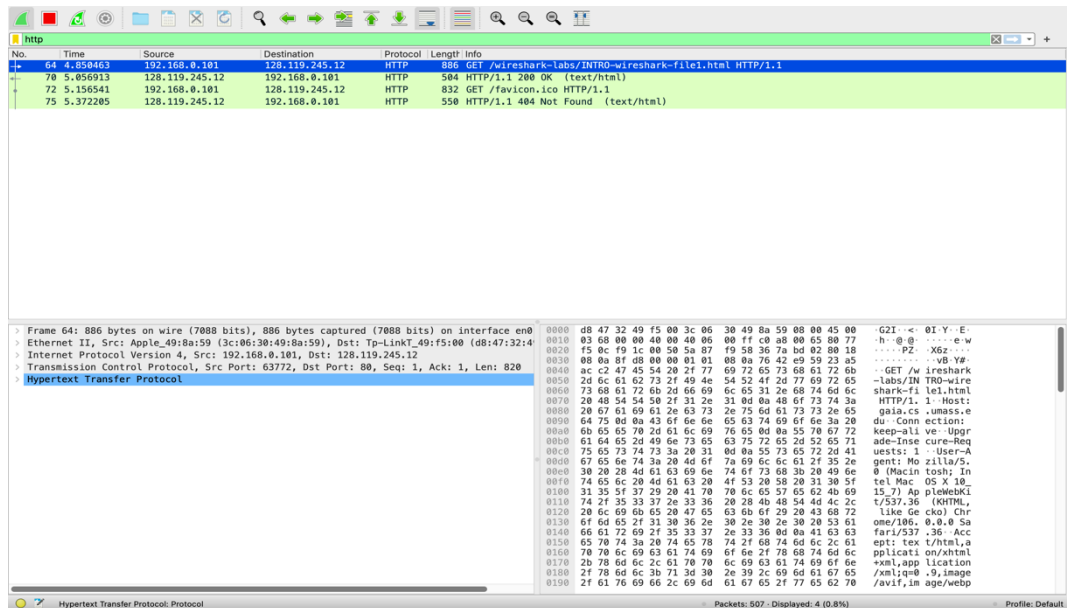
While Wireshark is running, I enter the URL:

<http://gaia.cs.umass.edu/wireshark-labs/INTRO-wireshark-file1.html>.

HTTP packets exchanges in Wireshark:

Before diving into HTTP, it's important to note that TCP and port 80 are used as transport layer protocols for HTTP. Let's examine what occurs on the network when we enter that URL into the browser and press Enter.

Here is the screenshot :



6)

The time it takes when the HTTP GET message was sent until the HTTP OK reply was received is:

5.056913 - 4.850463=0.20645

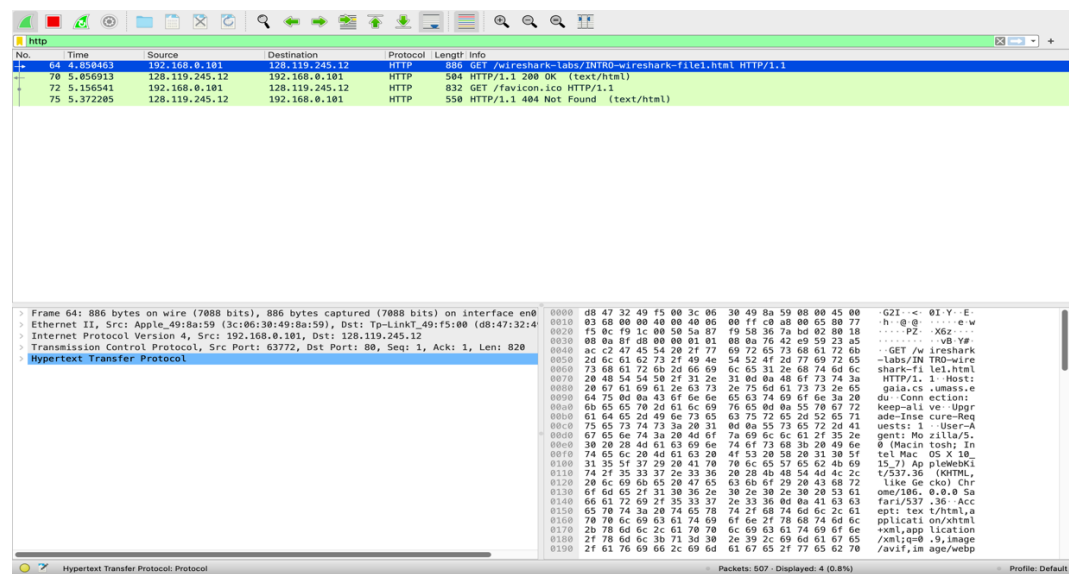
HTTP GET:

1.Request Method: GET ==> The packet is a HTTP GET.

2. Request URL: /wireshark-labs/INTRO-wireshark-file1.html==> The client is asking for file INTRO-wireshark-file1.html present under /wireshark-labs

3.Request version: HTTP/1.1 ==> It's HTTP version 1.1

Here is the screenshot.



HTTP OK:

After TCP data [content of INTRO-wireshark-file1.html] is sent successfully HTTP OK is sent to the client and here are the important fields in the packet.

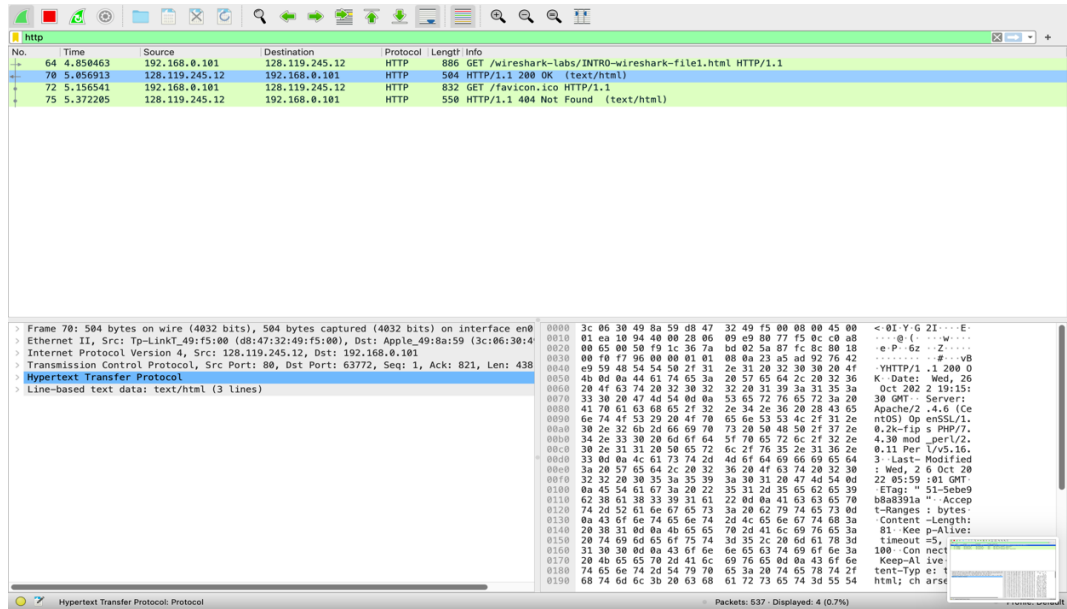
1. Response Version: HTTP/1.1 ==> Here server also in HTTP version 1.1

2. Status Code: 200 ==> Status code sent by the server.

3. Response Phrase: OK ==> Response phrase sent by the server.

So from 1 and 2, we get 200 OK which means the request [HTTP GET] has succeeded.

Here is the screenshot

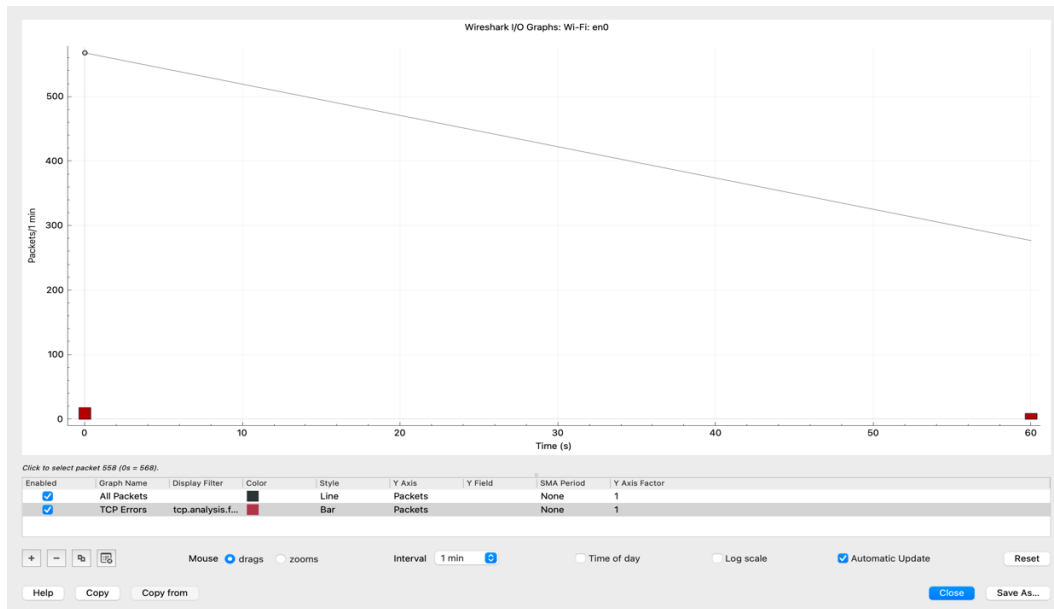


7)

I start the Wireshark by selecting the network we want to analyze. Then I go into the Wireshark and click on Statistics→ I/O Graph menu. This will then bring up Wireshark’s “I/O Graph” window. I set up the interval per minute.

The screenshot below of the I/O Graph window displays the graph of the captured network packets that are highly configurable. This graph displays all the traffic present in a capture file which is measured in packets(bytes/bits) per minute. By default, the x-axis represents the time in seconds and the y-axis represents the number of packets per tick.

Here is the screenshot:



8)

TLS protocol: The most popular protocol for implementing cryptography on the web is Transport Layer Security (TLS). TLS uses several cryptographic techniques to offer safe network communication.

makes sure that data transported between client and server apps is encrypted with secure algorithms and cannot be viewed by third parties by enabling client and server programs to support TLS. TLS is now supported by the most recent versions of all major web browsers, and default TLS support is becoming more and more common on web browsers.

9)

Wireshark is a packet analyzer. Packets are captured, filtered, and analyzed using it. Because the remote hosts are not connected to the same network, Wireshark does not show their actual Mac address. If the remote host is connected to the same network, it is also considered a local host.

10)

There are capture filters and display filters in Wireshark. Only copies of packets that match the filter are retained by capture filters. When you've finished recording everything and need to cut through the background noise to evaluate packets or flows, you can use display filters.

