PG LAB assignment 2a

1) Answer -

No.	Time	Source	Destination	Protocol	Length	Info
51	4.020132	Intel_5d:7c:30	Broadcast	ARP	42	Who has 172.20.10.1? Tell 172.20.10.3
54	4.131593	c2:b6:58:a7:58:64	Intel_5d:7c:30	ARP	42	172.20.10.1 is at c2:b6:58:a7:58:64
5091	80.478857	172.30.4.170	172.26.15.77	DNS	127	Standard query response 0x008c A accounts.youtube.com CNAME www3.l.google.com A 142.250.193.78
5092	80.478857	172.30.4.170	172.26.15.77	DNS	171	Standard query response 0x1247 HTTPS accounts.youtube.com CNAME www3.l.google.com SOA ns1.google.com
40	3.517942	152.195.38.76	172.20.10.3	OCSP	791	Response
90	5.361910	172.20.10.3	49.44.179.225	HTTP	208	GET /connecttest.txt HTTP/1.1
271	14.093191	2409:4055:2d0e:5ea3…	2409:4055:2d0e:5ea3…	ICMPv6	78	Neighbor Advertisement 2409:4055:2d0e:5ea3:dec:96b8:af70:8928 (rtr, sol)
515	16.593362	fe80::c0b6:58ff:fea…	fe80::7825:bed4:229…	ICMPv6	86	Neighbor Solicitation for fe80::7825:bed4:229c:43ab from c2:b6:58:a7:58:64
7677	143.256794	172.20.10.3	224.0.0.252	LLMNR	65	Standard query 0x0caa A https
7732	143.857704	fe80::7825:bed4:229…	ff02::1:3	LLMNR	85	Standard query 0xf87a A https
4276	105.158348	172.20.10.3	224.0.0.251	MDNS	500	Standard query response 0x0000 PTR, cache flush Yash.local PTR, cache flush Yash.local PTR, cache flush Yash.local PTR, cache f…
7625	142.832513	172.20.10.3	224.0.0.251	MDNS	71	Standard query 0x0000 A https.local, "QM" question
245	13.834428	2404:6800:4002:80c:…	2409:4055:2d0e:5ea3…	QUIC	1292	Initial, SCID=efd7666e73913039, PKN: 1, ACK, PADDING
246	13.834428	2404:6800:4002:80c:…	2409:4055:2d0e:5ea3…	QUIC	1292	Initial, SCID=efd7666e73913039, PKN: 2, CRYPTO, PADDING
3009	91.856461	172.20.10.3	239.255.255.250	SSDP	179	M-SEARCH * HTTP/1.1
3350	98.229961	172.20.10.3	239.255.255.250	SSDP	216	M-SEARCH * HTTP/1.1
242	9.422093	172.26.15.77	180.149.52.210	TCP	54	53377 → 443 [ACK] Seq=4664 Ack=29826 Win=262144 Len=0
243	9.424575	172.26.15.77	180.149.52.210	TLSv1.3	420	Application Data
339	9.663753	172.26.15.77	142.250.194.42	UDP	75	65237 → 443 Len=33
340	9.671091	142.250.194.42	172.26.15.77	UDP	361	443 → 65237 Len=319

The different protocols that I captured by applying the respective filter are:

1. ARP
2. DNS
3. HTTP
4. ICMPV6
5. LLMNR
6. MDNS
7. QUIC
8. SSDP
9. TCP
10. UDP

2) Answer -

*Wi-Fi

File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help

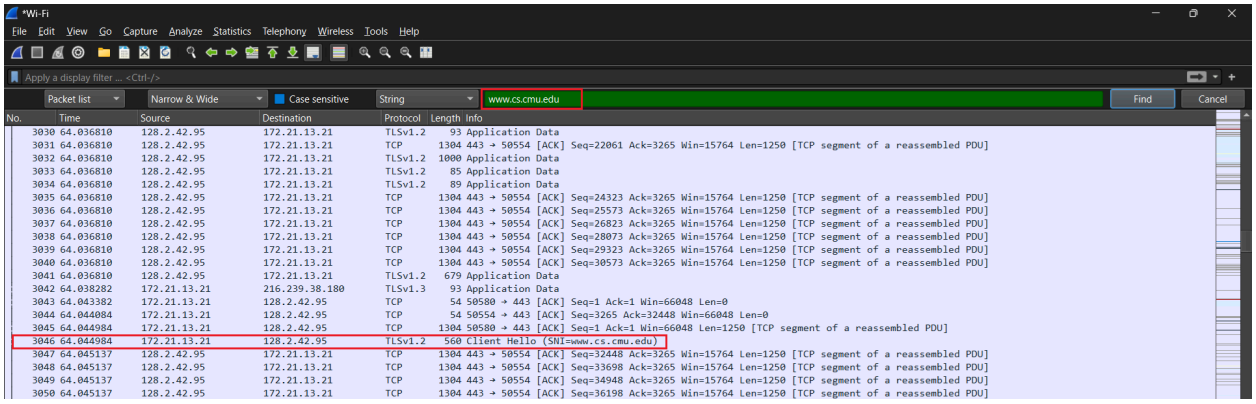
http

No.	Time	Source	Destination	Protocol	Length	Info
1476	36.999258	172.20.10.3	128.119.245.12	HTTP	535	GET /wireshark-labs/INTRO-wireshark-file1.html HTTP/1.1
1558	37.409949	128.119.245.12	172.20.10.3	HTTP	492	HTTP/1.1 200 OK (text/html)
1619	42.940230	2409:4055:2d0e:5ea3…	2a03:2880:f244:1c6:…	HTTP	79	POST /chat HTTP/1.1

Look at the highlighted box get request was sent at 36.999258 and HTTP ok reply was received at 37.409949. so the time difference between them is 0.410691 seconds

In the time column, look at the time of the GET request, which is at 36.999258 seconds after I started recording, and then look at the time column of ok HTTP, which is 37.409949, so the time difference between them is 0.410691 seconds.

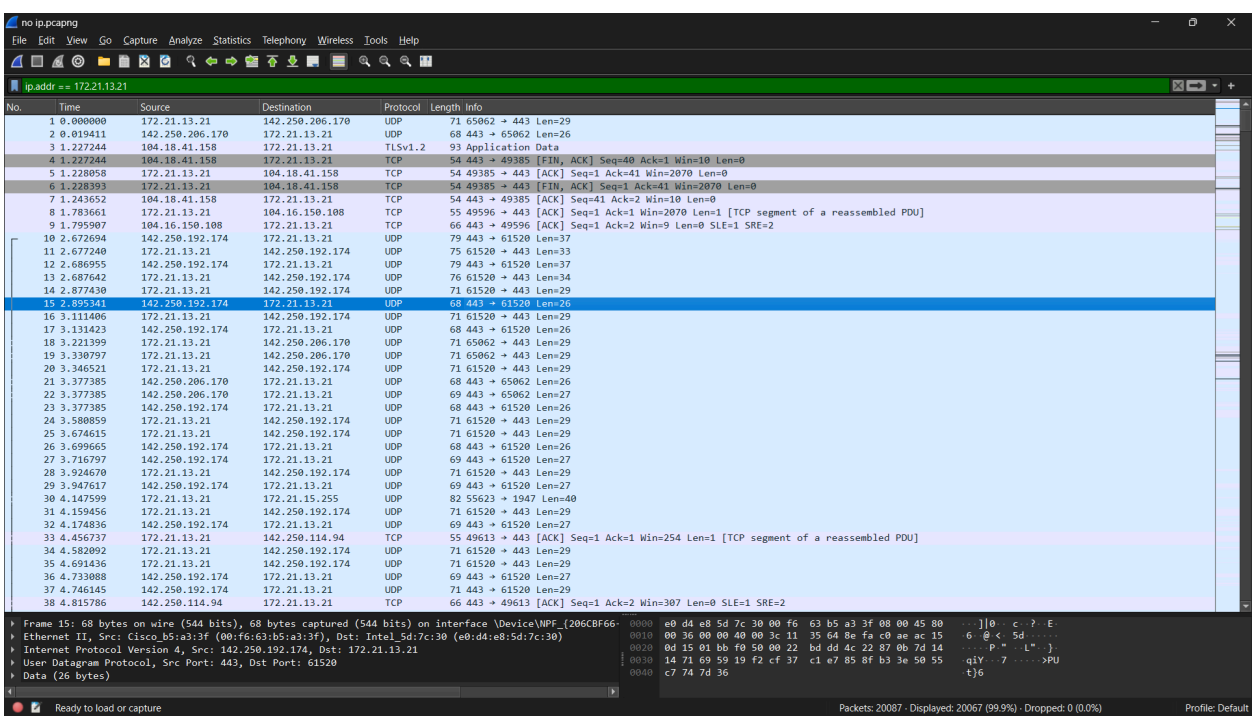
3) Answer -

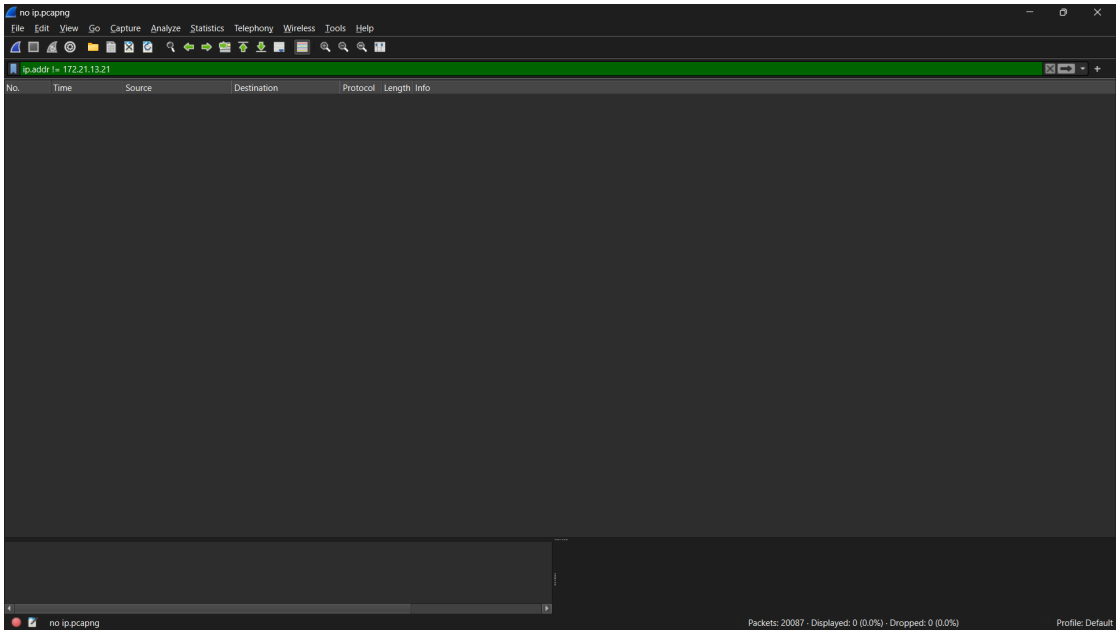


Look at the info column of the highlighted row. HTTP requests were not showing for www.cs.cmu.edu, so I used the “Ctrl + F” key to find the string “www.cs.cmu.edu” to find packets that contain this website name. In the destination column IP address of the website is mentioned, which is 128.2.42.95, and my network IP is in the source column, which is 172.21.13.21

4) Answer -

Wireshark captured 20087 packets. 20067 packets contain my IP address which I found out by using the filter ip.addr == 172.21.13.21, and at the bottom left corner, it shows the total number of packets after applying the filter(Displayed). 0 packets do not contain my IP. I used ip.addr != 172.21.13.21 this filter to see it.





5) Answer -

I set up a local FTP server on my Windows PC and tried to log in to the FTP server using a terminal while capturing packets on Wireshark(I selected an adapter for loopback traffic capture for capturing the packets since we have a local FTP server). I entered the username CS509-student, and the terminal asked me for a password I entered “IITRPR-cs509”, and I logged in. In Wireshark, I filtered the packets to show only ftp protocols, and there I saw the FTP protocol packet requesting the password and giving the response packet User logged in after I entered the password “IITRPR-cs509”, which concludes it is the correct password.