

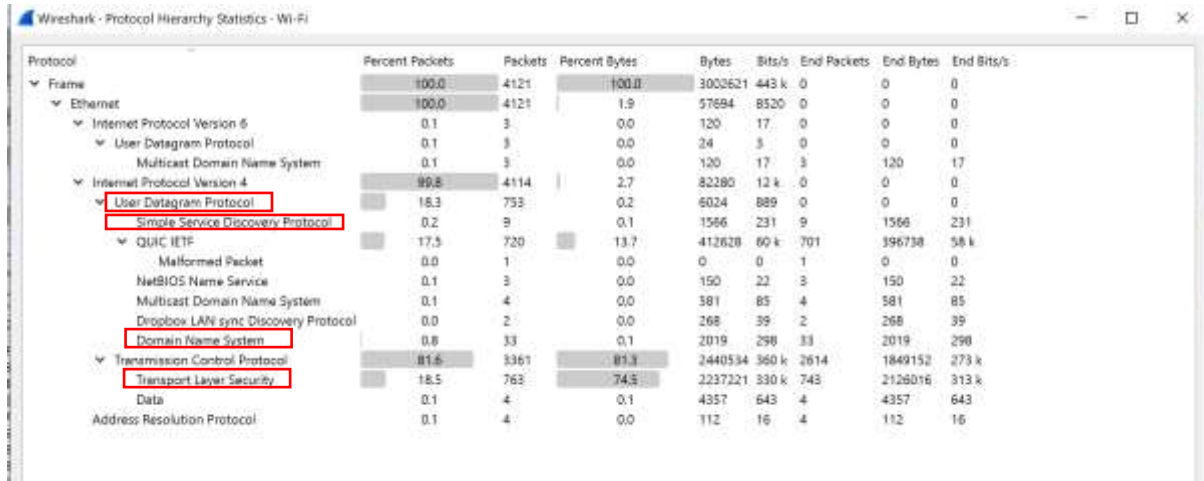
# گزارش آزمایش دوم

روژینا کاشفی-۹۸۳۱۱۱۸

## • لایه بندی پروتکل ها

(سوال ۱)

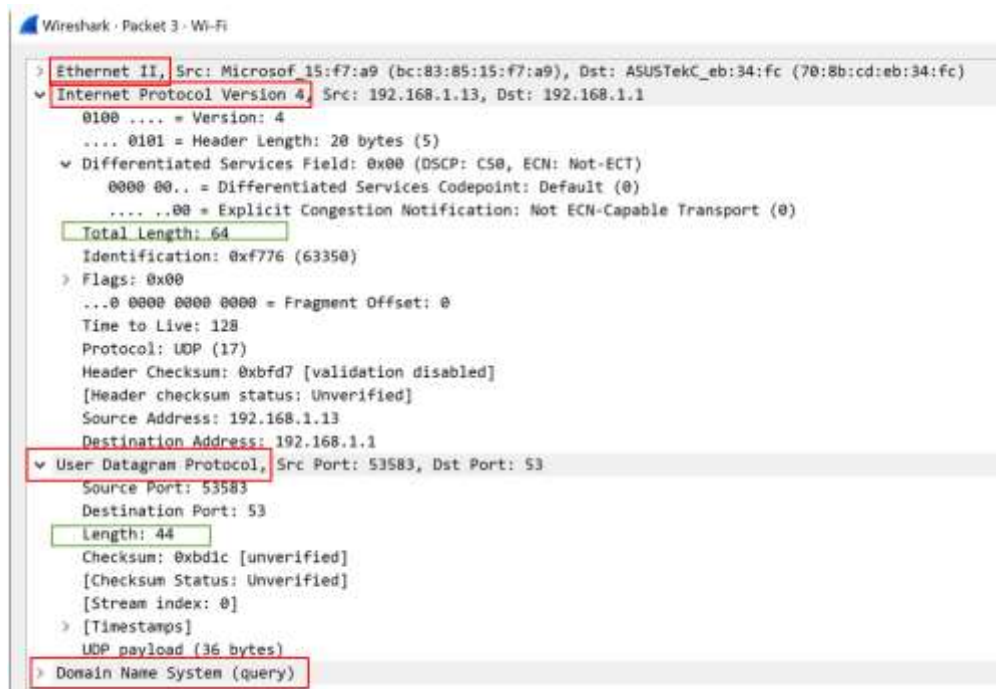
انواع متفاوتی از پروتکل ها با میزان استفاده شدنشان در جدول زیر مشاهده میکنیم.



Protocol	Percent Packets	Packets	Percent Bytes	Bytes	Bits/s	End Packets	End Bytes	End Bits/s
Frame	100.0	4121	100.0	3002621	443 k	0	0	0
Ethernet	100.0	4121	1.9	57694	8520	0	0	0
Internet Protocol Version 6	0.1	3	0.0	120	17	0	0	0
User Datagram Protocol	0.1	3	0.0	24	3	0	0	0
Multicast Domain Name System	0.1	3	0.0	120	17	3	120	17
Internet Protocol Version 4	99.8	4114	2.7	82280	12 k	0	0	0
User Datagram Protocol	18.3	753	0.2	6024	889	0	0	0
Simple Service Discovery Protocol	0.2	9	0.1	1566	231	9	1566	231
QUIC IETF	17.3	720	13.7	412628	60 k	701	396738	58 k
Malformed Packet	0.0	1	0.0	0	0	1	0	0
NetBIOS Name Service	0.1	3	0.0	150	22	3	150	22
Multicast Domain Name System	0.1	4	0.0	381	85	4	381	85
Dropbox LAN sync Discovery Protocol	0.0	2	0.0	268	39	2	268	39
Domain Name System	0.8	33	0.1	2019	298	33	2019	298
Transmission Control Protocol	81.6	3361	81.3	2440534	360 k	2614	1849152	273 k
Transport Layer Security	18.5	763	74.5	2237221	330 k	743	2126016	313 k
Data	0.1	4	0.1	4357	643	4	4357	643
Address Resolution Protocol	0.1	4	0.0	112	16	4	112	16

(سوال ۲)

مشاهده میکنیم در لایه application از dns و در لایه transport از udp استفاده میشود و در لایه network از ipv4 و در لایه datalink از ethernet II استفاده میشود. ترتیب قرارگیری بدین صورت است که ابتدا بیتهای لایه بالاتر قرار میگیرد و مشاهده میکنیم در این پکت اندازه فریم لایه دوم برابر با ۴۴ و در لایه سوم برابر با ۶۴ است.



Ethernet II, Src: Microsoft 15:f7:a9 (bc:83:85:15:f7:a9), Dst: ASUSTekC_eb:34:fc (70:8b:cd:eb:34:fc)
Internet Protocol Version 4, Src: 192.168.1.13, Dst: 192.168.1.1
0100 .... = Version: 4
.... 0101 = Header Length: 20 bytes (5)
Differentiated Services Field: 0x00 (DSCP: CS0, ECN: Not-ECT)
0000 00.. = Differentiated Services Codepoint: Default (0)
.... ..00 = Explicit Congestion Notification: Not ECN-Capable Transport (0)
Total Length: 64
Identification: 0xf776 (63350)
Flags: 0x00
...0 0000 0000 0000 = Fragment Offset: 0
Time to Live: 128
Protocol: UDP (17)
Header Checksum: 0xbfd7 [validation disabled]
[Header checksum status: Unverified]
Source Address: 192.168.1.13
Destination Address: 192.168.1.1
User Datagram Protocol, Src Port: 53583, Dst Port: 53
Source Port: 53583
Destination Port: 53
Length: 44
Checksum: 0xbd1c [unverified]
[Checksum Status: Unverified]
[Stream index: 0]
[Timestamps]
UDP payload (36 bytes)
Domain Name System (query)

سوال ۳)

بله بسته های ARP لایه های نام برده شده را ندارند.

47.3.972326	ASUSTekC_eb:34:fc	Broadcast	ARP	42 Who has 192.168.1.6? Tell 192.168.1.1
> Frame 47: 42 bytes on wire (336 bits), 42 bytes captured (336 bits) on interface \Device\NPF_{C9A896A3-CC72-4D4D-B15F-79996F809C77}, id 0 > Ethernet II, Src: ASUSTekC_eb:34:fc (78:8b:cd:eb:34:fc), Dst: Broadcast {ff:ff:ff:ff:ff:ff} > Address Resolution Protocol (request)				

سوال ۴)

مشاهده میکنیم checksum برابر با 0xbb74 است.

No.	Time	Source	Destination	Protocol	Length	Info
65	3.746123	212.16.77.100	192.168.1.13	TLSv1.0	986	Application Data
66	3.745012	192.168.1.13	212.16.77.100	TLSv1.0	85	Application Data
67	3.777008	212.16.77.100	192.168.1.13	TCP	54	65616 → 58976 [ACK] Seq=3818 Ack=1298 Win=65536 Len=0
68	4.410079	212.16.77.100	192.168.1.13	TCP	1986	443 → 58976 [ACK] Seq=3818 Ack=1298 Win=65536 Len=1452 [TCP segment of a reassembled PDU]
69	4.410079	212.16.77.100	192.168.1.13	TCP	1986	443 → 58976 [PSH, ACK] Seq=3818 Ack=1298 Win=65536 Len=1252 [TCP segment of a reassembled PDU]
70	4.410148	192.168.1.13	212.16.77.100	TCP	54	58976 → 443 [ACK] Seq=1399 Ack=3818 Win=12288 Len=0
71	4.410179	212.16.77.100	192.168.1.13	TLSv1.0	1427	Application Data
72	4.410179	212.16.77.100	192.168.1.13	TCP	1986	443 → 58976 [ACK] Seq=3818 Ack=1298 Win=65536 Len=1452 [TCP segment of a reassembled PDU]
73	4.410416	192.168.1.13	212.16.77.100	TCP	54	58976 → 443 [ACK] Seq=1399 Ack=3818 Win=12288 Len=0
74	4.410416	212.16.77.100	192.168.1.13	TCP	1986	443 → 58976 [PSH, ACK] Seq=3818 Ack=1298 Win=65536 Len=1252 [TCP segment of a reassembled PDU]
75	4.410416	212.16.77.100	192.168.1.13	TCP	1986	443 → 58976 [ACK] Seq=3818 Ack=1298 Win=65536 Len=1452 [TCP segment of a reassembled PDU]

Wireshark Packet 75 - 804B	
0100 .... = Version: 4 .... 0101 = Header Length: 20 bytes (5) Differentiated Services Field: 0x00 (DSCP: CS0, ECN: Not-ECT) Total Length: 169 Identification: 0x188a Flags: 0x00 ... 0 0000 0000 = Fragment Offset: 0 Time to Live: 64 Protocol: TCP (6) Header Checksum: 0xbb74 [validation disabled] [Header checksum status: Unverified] Source Address: 212.16.77.100 Destination Address: 192.168.1.13 Transmission Control Protocol, Src Port: 443, Dst Port: 58976, Seq: 3818, Ack: 1298, Len: 1452	

سوال ۵)

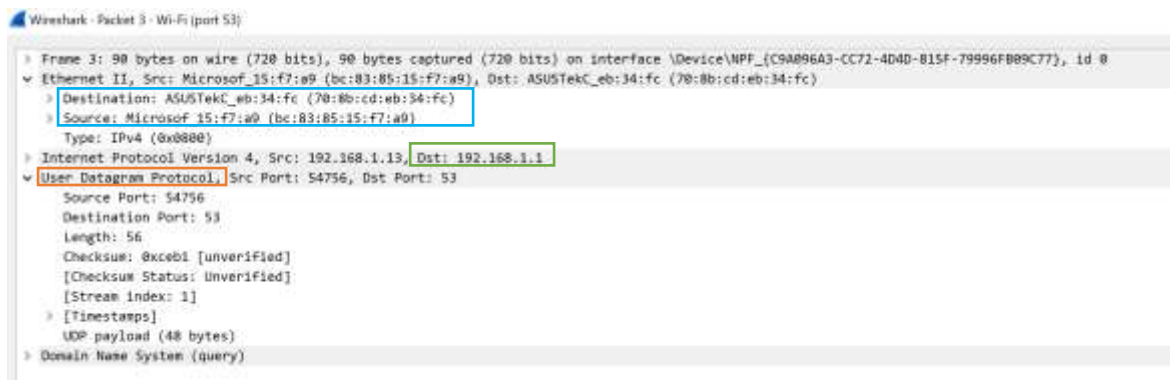
برای udp مشاهده میکنیم که پورت مبدا برابر ۵۳۴۰۸ و مقصد برابر ۱۵۶۰۰ است و check sum برابر 0xf827 است.  
پورت مبدا نشان دهنده پورت شروع کننده اتصال و پورت مقصد همان DNS است و به برنامه های در حال اجرا میدهند.

> Ethernet II, Src: 66:64:4a:03:39:d4 (66:64:4a:03:39:d4), Dst: Microsof_15:f7:a9 (bc:83:85:15:f7:a9)	
> Internet Protocol Version 4, Src: 192.168.1.5, Dst: 239.255.255.250 0100 .... = Version: 4 .... 0101 = Header Length: 20 bytes (5) > Differentiated Services Field: 0x00 (DSCP: CS0, ECN: Not-ECT) 0000 00.. = Differentiated Services Codepoint: Default (0) .... ..00 = Explicit Congestion Notification: Not ECN-Capable Transport (0) Total Length: 63 Identification: 0xf05f (61535) > Flags: 0x40, Don't fragment ...0 0000 0000 0000 = Fragment Offset: 0 Time to Live: 64 Protocol: UDP (17) Header Checksum: 0x98a6 [validation disabled] [Header checksum status: Unverified] Source Address: 192.168.1.5 Destination Address: 239.255.255.250	
> User Datagram Protocol, Src Port: 53408, Dst Port: 15600 Source Port: 53408 Destination Port: 15600 Length: 43 Checksum: 0xf827 [unverified] [Checksum Status: Unverified] [Stream index: 12] > [Timestamps] UDP payload (35 bytes)	
> Data (35 bytes)	

## • کار با فیلترکننده بسته ها

سوال (۶)

پروتکل لایه transport مورد استفاده udp است و ادرس ip مقصد برابر است با 192.168.1.1 و سرایند لایه دوم در شکل با کادر ای قابل مشاهده است.



سوال (۷)

ادرس های مشاهده شده در قسمت قبل

No.	Time	Source	Destination	Protocol	Length	Info
1	0.000000	192.168.1.13	192.168.1.1	DNS	70	Standard query 0x5ec A google.com
2	0.026858	192.168.1.1	192.168.1.13	DNS	86	Standard query response 0x5ec A google.com A 142.250.185.46
3	11.038516	192.168.1.13	192.168.1.1	DNS	90	Standard query 0x426a A relay-a16ffdc7.net.anydesk.com
4	11.066981	192.168.1.1	192.168.1.13	DNS	106	Standard query response 0x426a A relay-a16ffdc7.net.anydesk.com A 51.80.42.234

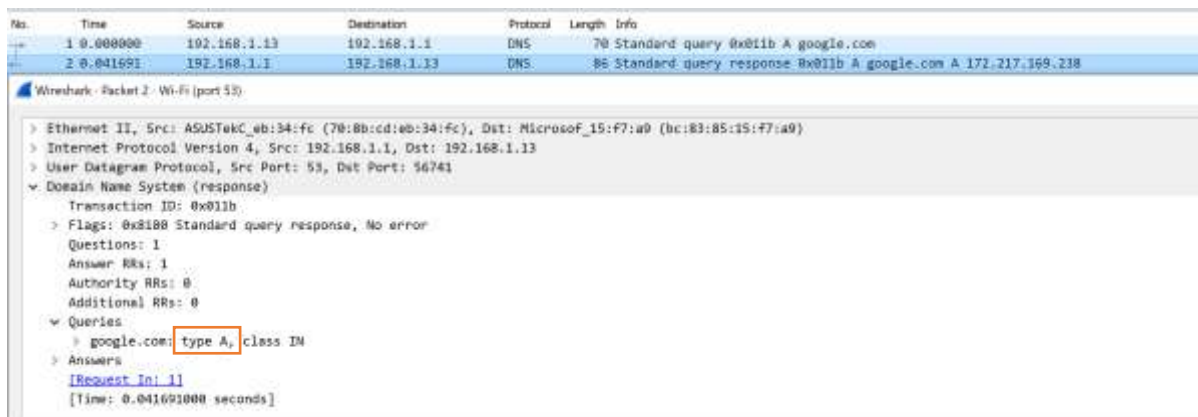
ادرس های مشاهده شده پس از اجرای ipconfig /all

No.	Time	Source	Destination	Protocol	Length	Info
1	0.000000	192.168.1.13	192.168.1.1	DNS	72	Standard query 0xdfad A oenatuor.com
2	0.155123	192.168.1.13	192.168.1.1	DNS	72	Standard query 0xdfad A oenatuor.com
3	0.280170	192.168.1.1	192.168.1.13	DNS	88	Standard query response 0xdfad A oenatuor.com A 139.45.197.253
4	0.288170	192.168.1.1	192.168.1.13	DNS	88	Standard query response 0xdfad A oenatuor.com A 139.45.197.253

مشاهده میکنیم میتوانیم همان ادرس ها را در دو قسمت مشاهده کنیم که ادرس دستگاه خودمان و گیت خروجی است.

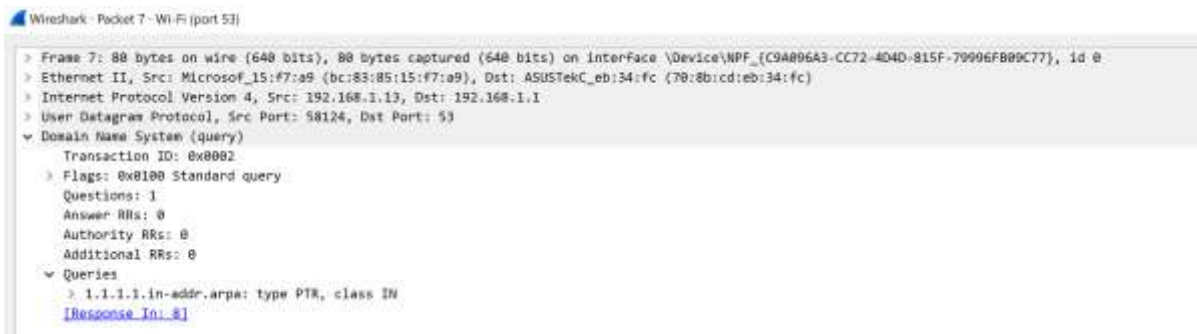
سوال (۸)

مشاهده می کنیم که نوع بسته انتخابی A است و این تایپ یک nameserver را به ip متناظرش تبدیل میکند



سوال ۹)

مشاهده میکنیم از نوع PTR است و عملکردی دقیقاً عکس تایپ A دارد و یک ip را به یک nameserver تبدیل میکند.



سوال ۱۰)

Cname که برای نام مستعار نام میزبان به میزبانی دیگر باشد.

Mx که یک سرور ایمیل برای دامنه به منظور مسیریابی ایمیل های خروجی به سرور ایمیل مشخص میکند.

NS که مشخص میکند یم منطقه Dns به یک سرور معتبر واگذار شده و ادرس سرور را ارائه میدهد.

• کار با filter display

سوال ۱۱)

تمامی بسته هایی که دران چه در مبدا چه در مقصد ip مورد نظر یافت شده نشان داده میشود و همچنین پرتوک ICMP نشان داده میشود.

A screenshot of the Wireshark interface showing a packet capture on interface \Device\NPF\_{C9A896A3-CC72-4D4D-815F-70996FB09C77}. The selected packet is an ICMP Echo (ping) request from 192.168.1.13 to 192.168.1.1. The packet details pane shows: Type: Echo (ping) request, ID: 0x0000, Seq: 6485/21785, TTL: 1 (no response found). The packet bytes pane shows the raw data. The packet list pane shows a list of 20 packets, all of which are ICMP Echo (ping) requests or responses between 192.168.1.13 and 192.168.1.1. The packet details pane for the selected packet shows: Type: Echo (ping) request, ID: 0x0000, Seq: 6485/21785, TTL: 1 (no response found). The packet bytes pane shows the raw data. The packet list pane shows a list of 20 packets, all of which are ICMP Echo (ping) requests or responses between 192.168.1.13 and 192.168.1.1.

سوال ۱۲)

تایپ برابر با ping request است و مقدار TTL برابر ۱ است.





### سوال ۱۳)

در دستور traceroute داده ها از مبدأ به مقصد مشخصی حرکت میکنند و اینکار را با عمل هاپ با استفاده از دستگاههای مسیریاب و سویچ انجام میدهند.

کار TTL محدود کردن مدت زمان یک داده در یک شبکه استن و زمانی که بسته در مسیر مورد نظر حرکت میکند یک مقدار ازش کم میشود.

### سوال ۱۴)

مشاهده میکنیم پرتوکل های TCP و زیرمجموعه انها را به عنوان خروجی میدهد زیرا عدد ۶ به معنای TCP است.

No.	Time	Source	Destination	Protocol	Length	Info
0	0.293426	192.168.1.13	20.189.173.2	TCP	54	59230 → 443 [SYN, ACK] Seq=5175 Win=65535 Len=0 MSS=1460 win=0 SACK_PERM=2
5	0.298177	192.168.1.13	20.189.173.2	TCP	54	59230 → 443 [ACK] Seq=5 Ack=5 Win=342184 Len=0
6	0.298177	192.168.1.13	20.189.173.2	TLSv1.2	283	Client Hello
7	0.573428	20.189.173.2	192.168.1.13	TCP	596	443 → 59230 [ACK] Seq=1 Ack=230 Win=52512 Len=1052 [TCP segment of a reassembled PDU]
8	0.573408	192.168.1.13	20.189.173.2	TCP	54	59230 → 443 [ACK] Seq=230 Ack=1053 Win=262184 Len=0
9	0.574210	20.189.173.2	192.168.1.13	TCP	596	443 → 59230 [ACK] Seq=1453 Ack=230 Win=52512 Len=1052 [TCP segment of a reassembled PDU]
10	0.574277	192.168.1.13	20.189.173.2	TCP	54	59230 → 443 [ACK] Seq=230 Ack=1005 Win=262184 Len=0
11	0.574728	20.189.173.2	192.168.1.13	TCP	470	[TCP Previous segment now captured] 443 → 59230 [PSH, ACK] Seq=5880 Ack=230 Win=52512 Len=416 [TCP segment of a reassembled PDU]
12	0.574776	192.168.1.13	20.189.173.2	TCP	46	[TCP Dup ACK 1001] 59230 → 443 [ACK] Seq=230 Ack=5884 Win=262184 Len=0 SILENCE=0 ECN=0
13	0.580728	20.189.173.2	192.168.1.13	TCP	596	[TCP Out-Of-Order] 443 → 59230 [ACK] Seq=2905 Ack=230 Win=52512 Len=1052 [TCP segment of a reassembled PDU]
14	0.580788	192.168.1.13	20.189.173.2	TCP	46	59230 → 443 [ACK] Seq=230 Ack=4357 Win=262184 Len=0 SILENCE=0 SRTT=6221
15	0.584328	20.189.173.2	192.168.1.13	TCP	596	[TCP Out-Of-Order] 443 → 59230 [ACK] Seq=4357 Ack=230 Win=52512 Len=1052
16	0.584403	192.168.1.13	20.189.173.2	TCP	54	59230 → 443 [ACK] Seq=230 Ack=6225 Win=262184 Len=0
17	0.604011	192.168.1.13	20.189.173.2	TLSv1.2	212	Client Key Exchange, Change Cipher Spec, Encrypted Handshake Message
18	0.608329	20.189.173.2	192.168.1.13	TLSv1.2	105	Change Cipher Spec, Encrypted Handshake Message
19	0.608306	192.168.1.13	20.189.173.2	TCP	54	59230 → 443 [ACK] Seq=188 Ack=6276 Win=261888 Len=0
20	0.609665	192.168.1.13	20.189.173.2	TLSv1.2	1048	Application Data
21	1.455521	192.168.1.13	20.189.173.2	TCP	1056	[TCP Retransmission] 59230 → 443 [PSH, ACK] Seq=588 Ack=6376 Win=525888 Len=1014
22	1.730641	20.189.173.2	192.168.1.13	TLSv1.2	536	Application Data
23	1.730713	192.168.1.13	20.189.173.2	TCP	54	59230 → 443 [ACK] Seq=1482 Ack=6758 Win=361376 Len=0