

به نام ایزد یکتا



دانشگاه صنعتی امیرکبیر
(پلی تکنیک تهران)



دانشکده مهندسی کامپیوتر

امایش دوم درس آزمایشگاه شبکه‌های کامپیوتری

گروه دوم

تهیه کننده: بردیا اردکانیان

۹۸۳۱۰۷۲

سوال اول) پروتکل‌هایی من جمله TCP, DNS, TLSv1, TLSv1.3, TLSv1.2, MDNS,...

No.	Time	Source	Destination	Protocol	Length	Info
9104	100.279243	192.168.1.106	216.58.209.142	TCP	66	2057 → 443 [SYN] Seq=0 Win=17520 Len=0 MSS=1460 WS=256 SACK_PERM=1
9105	100.285152	216.58.209.136	192.168.1.106	TCP	60	443 → 1915 [ACK] Seq=41 Ack=104 Win=273 Len=0
9106	100.301641	192.168.1.1	192.168.1.106	DNS	91	Standard query response 0x9105 A play.google.com A 216.58.209.142
9107	100.302108	192.168.1.106	192.168.1.1	DNS	75	Standard query 0x3df8 AAAA play.google.com
9108	100.302267	216.58.209.142	192.168.1.106	TCP	66	443 → 2055 [SYN, ACK] Seq=0 Ack=1 Win=65535 Len=0 MSS=1390 SACK_PERM=1 WS=256
9109	100.302312	192.168.1.106	216.58.209.142	TCP	54	2055 → 443 [ACK] Seq=1 Ack=1 Win=17408 Len=0
9110	100.304026	192.168.1.106	216.58.209.142	TLSv1	571	Client Hello
9111	100.326000	216.58.209.142	192.168.1.106	TCP	60	443 → 2054 [ACK] Seq=6091 Ack=2645 Win=72704 Len=0
9112	100.365453	216.58.209.142	192.168.1.106	TCP	66	443 → 2056 [SYN, ACK] Seq=0 Ack=1 Win=65535 Len=0 MSS=1390 SACK_PERM=1 WS=256
9113	100.365551	192.168.1.106	216.58.209.142	TCP	54	2056 → 443 [ACK] Seq=1 Ack=1 Win=17408 Len=0
9114	100.367371	192.168.1.106	216.58.209.142	TLSv1	571	Client Hello
9115	100.420034	216.58.209.136	192.168.1.106	TCP	66	[TCP Dup ACK 9105#1] 443 → 1915 [ACK] Seq=41 Ack=104 Win=273 Len=0 SLE=40 SRE=10

> Frame 1: 55 bytes on wire (440 bits), 55 bytes captured (440 bits) on interface \Device\NPF_{BF4ABADA-2C91-4476-AEFA-D0FB46D0C015}, id 0
 > Ethernet II, Src: AzureWav_1e:36:59 (80:c5:f2:1e:36:59), Dst: Tp-LinkT_f2:55:60 (18:a6:f7:f2:55:60)
 > Internet Protocol Version 4, Src: 192.168.1.106, Dst: 143.204.209.18
 > Transmission Control Protocol, Src Port: 1816, Dst Port: 443, Seq: 1, Ack: 1, Len: 1

عکس 1-1

سوال دوم)

در اینجا بسته شماره 4 را انتخاب کردیم و اطلاعات پروتکل‌های لایه‌های مختلف آن را مشاهده می‌کنیم:

در لایه Transport از TCP، در لایه Network از پروتکل IPv4، در لایه Link از پروتکل Ethernet II استفاده شده است (در این بسته، اطلاعات پروتکل لایه اپلیکیشن را مشاهده نمی‌کنیم). هر لایه اطلاعات دریافتی از لایه بالاتر را می‌گیرد و اطلاعات جدیدی به آن اضافه می‌کند (مثلاً لایه انتقال، مسیج را از لایه اپلیکیشن دریافت کرده و به سر آن بیت‌های جدیدی اضافه می‌کند و یک Segment را به لایه شبکه تحویل می‌دهد) همانطوری که در شکل 1-2 مشاهده می‌کنید اندازه فریم در این بسته 66 بایت است و اندازه بسته‌ی لایه 3 (Network) در شکل 2-2 مشخص شده است که 52 بایت می‌باشد.

Wireshark - Packet 41 - Wi-Fi	
> Frame 41: 66 bytes on wire (528 bits), 66 bytes captured (528 bits) on interface \Device\NPF_{BF4ABADA-2C91-4476-AEFA-D0FB46D0C015}, id 0 > Ethernet II, Src: Tp-LinkT_f2:55:60 (18:a6:f7:f2:55:60), Dst: AzureWav_1e:36:59 (80:c5:f2:1e:36:59) > Internet Protocol Version 4, Src: 134.0.216.227, Dst: 192.168.1.106 > Transmission Control Protocol, Src Port: 80, Dst Port: 1910, Seq: 1, Ack: 2, Len: 0	
0000 80 c5 f2 1e 36 59 18 a6 f7 f2 55 60 08 00 45 00 0010 00 34 b8 cb 40 00 34 06 6d 02 86 00 d8 e3 c0 a8 0020 01 6a 00 50 07 76 9d 43 a3 ab 35 ee 8a f6 80 10 0030 90 ed cc 77 00 00 01 01 05 0a 35 ee 8a f5 35 ee 0040 8a f6	----6V-- --U--E- -4-#4-m----- -3-P-V-C--S-----S...S...

شکل 1-2

```

> Ethernet II, Src: Tp-LinkT_f2:55:60 (18:a6:f7:f2:55:60), Dst: AzureWav_1e:36:59 (80:c5:f2:1e:36:59)
v Internet Protocol Version 4, Src: 134.0.216.227, Dst: 192.168.1.106
    0100 .... = Version: 4
    .... 0101 = Header Length: 20 bytes (5)
> Differentiated Services Field: 0x00 (DSCP: CS0, ECN: Not-ECT)
    Total Length: 52
    Identification: 0xb8cb (47307)
> Flags: 0x40, Don't fragment
    Fragment Offset: 0
    Time to Live: 52
    Protocol: TCP (6)
    Header Checksum: 0x6d02 [validation disabled]
    [Header checksum status: Unverified]

```

شکل 2-2

سوال سوم)

بسته‌ای که در سوال 2 مشاهده کردیم، لایه اپلیکیشن نداشت.

بسته‌ی زیر نیز ARP است و لایه اپلیکیشن و انتقال را ندارد.

No.	Time	Source	Destination	Protocol	Length	Info
1	0.000000	AzureWav_1e:36:59	Tp-LinkT_f2:55:60	ARP	42	Who has 192.168.1.1? Tell 192.168.1.106
2	0.446363	Tp-LinkT_f2:55:60	AzureWav_1e:36:59	ARP	60	192.168.1.1 is at 18:a6:f7:f2:55:60


```

> Frame 2: 60 bytes on wire (480 bits), 60 bytes captured (480 bits) on interface \Device\NPF_{BF4ABADA-2C91-4476-AEFA-D0FB46DBC015}, id 0
> Ethernet II, Src: Tp-LinkT_f2:55:60 (18:a6:f7:f2:55:60), Dst: AzureWav_1e:36:59 (80:c5:f2:1e:36:59)
> Address Resolution Protocol (reply)

```

شکل 1-3

در هردوی این بسته‌ها لایه فیزیکی و لایه لینک را داریم.

```
> Ethernet II, Src: AzureWav_1e:36:59 (80:c5:f2:1e:36:59), Dst: Tp-LinkT_f2:55:60 (18:a6:f7:f2:55:60)
✓ Internet Protocol Version 4, Src: 192.168.1.106, Dst: 23.58.222.26
    0100 .... = Version: 4
    .... 0101 = Header Length: 20 bytes (5)
    > Differentiated Services Field: 0x00 (DSCP: CS0, ECN: Not-ECT)
    Total Length: 41
    Identification: 0x3061 (12385)
    > Flags: 0x40, Don't fragment
    Fragment Offset: 0
    Time to Live: 128
    Protocol: TCP (6)
    Header Checksum: 0x1307 [validation disabled]
    [Header checksum status: Unverified]
    Source Address: 192.168.1.106
    Destination Address: 23.58.222.26
```

شکل 4-1

سوال پنجم)

در این بسته که از پروتکل tcp استفاده کرده است شماره پورت مبدا 443 و پورت مقصد 2012 می‌باشد. شماره پورت در مبدا نشان‌دهنده پردازنده است که داده را ارسال کرده است و در مقصد نشان‌دهنده پردازنده‌ایست که میبایست داده را دریافت کند و در اولین هدرهای tcp و udp گنجانده می‌شود.

No.	Time	Source	Destination	Protocol	Length	Info
49..65.705799	192.168.1.106	134.0.216.227	TCP	54	[TCP Retransmission] 1910 → 80 [FIN, ACK] Seq=2 Ack=1 Win=64 Len=0	
49..65.751262	192.168.1.106	134.0.216.227	TCP	54	[TCP Retransmission] 1911 → 80 [FIN, ACK] Seq=2 Ack=1 Win=64 Len=0	
49..65.769443	134.0.216.227	192.168.1.106	TCP	60	80 → 1910 [FIN, ACK] Seq=1 Ack=3 Win=237 Len=0	
49..65.769509	192.168.1.106	134.0.216.227	TCP	54	1910 → 80 [ACK] Seq=3 Ack=2 Win=64 Len=0	
49..65.808627	34.107.221.82	192.168.1.106	TCP	60	80 → 1793 [FIN, ACK] Seq=1 Ack=3 Win=265 Len=0	
49..65.808745	192.168.1.106	34.107.221.82	TCP	54	1793 → 80 [ACK] Seq=3 Ack=2 Win=66 Len=0	
49..65.816531	134.0.216.227	192.168.1.106	TCP	60	80 → 1911 [FIN, ACK] Seq=1 Ack=3 Win=237 Len=0	
49..65.816575	192.168.1.106	134.0.216.227	TCP	54	1911 → 80 [ACK] Seq=3 Ack=2 Win=64 Len=0	
49..65.905571	192.168.1.106	172.217.18.132	TCP	1444	[TCP Retransmission] 1939 → 443 [PSH, ACK] Seq=30611 Ack=727066 Win=122624 Len=1390	
50..65.915070	13.74.169.109	192.168.1.106	TLSv1.2	105	Change Cipher Spec, Encrypted Handshake Message	
50..65.915555	13.74.169.109	192.168.1.106	TLSv1.2	123	Application Data	
50..65.915628	192.168.1.106	13.74.169.109	TCP	54	2012 → 443 [ACK] Seq=392 Ack=3982 Win=17152 Len=0	

Transmission Control Protocol, Src Port: 443, Dst Port: 2012, Seq: 3913, Ack: 392, Len: 69

Source Port: 443

Destination Port: 2012

[Stream Index: 121]

[TCP Segment Len: 69]

Sequence Number: 3913 (relative sequence number)

Sequence Number (raw): 2184096663

[Next Sequence Number: 3982 (relative sequence number)]

Acknowledgment Number: 392 (relative ack number)

Acknowledgment number (raw): 3143234721

0101 ... = Header Length: 20 bytes (5)

> Flags: 0x018 (PSH, ACK)

Window: 2050

عکس 5-1

TCP Checksum: 0x0000ae4b

No.	Time	Source	Destination	Protocol	Length	Info
49..65.705799	192.168.1.106	134.0.216.227	TCP	54	[TCP Retransmission] 1910 → 80 [FIN, ACK] Seq=2 Ack=1 Win=64 Len=0	
49..65.751242	192.168.1.106	134.0.216.227	TCP	54	[TCP Retransmission] 1911 → 80 [FIN, ACK] Seq=2 Ack=1 Win=64 Len=0	
49..65.769443	134.0.216.227	192.168.1.106	TCP	60	80 → 1910 [FIN, ACK] Seq=1 Ack=3 Win=237 Len=0	
49..65.769509	192.168.1.106	134.0.216.227	TCP	54	1910 → 80 [ACK] Seq=3 Ack=2 Win=64 Len=0	
49..65.808627	34.107.221.82	192.168.1.106	TCP	60	80 → 1793 [FIN, ACK] Seq=1 Ack=3 Win=265 Len=0	
49..65.808745	192.168.1.106	34.107.221.82	TCP	54	1793 → 80 [ACK] Seq=3 Ack=2 Win=66 Len=0	
49..65.816531	134.0.216.227	192.168.1.106	TCP	60	80 → 1911 [FIN, ACK] Seq=1 Ack=3 Win=237 Len=0	
49..65.816575	192.168.1.106	134.0.216.227	TCP	54	1911 → 80 [ACK] Seq=3 Ack=2 Win=64 Len=0	
49..65.905571	192.168.1.106	172.217.18.132	TCP	1444	[TCP Retransmission] 1939 → 443 [PSH, ACK] Seq=30611 Ack=727066 Win=122624 Len=1390	
50..65.915070	13.74.169.109	192.168.1.106	TLSv1.2	105	Change Cipher Spec, Encrypted Handshake Message	
50..65.915555	13.74.169.109	192.168.1.106	TLSv1.2	123	Application Data	
50..65.915628	192.168.1.106	13.74.169.109	TCP	54	2012 → 443 [ACK] Seq=392 Ack=3982 Win=17152 Len=0	

Sequence Number (raw): 2184096663
[Next Sequence Number: 3982 (relative sequence number)]
Acknowledgment Number: 392 (relative ack number)
Acknowledgment number (raw): 3143234721
0101 = Header Length: 20 bytes (5)
> Flags: 0x018 (PSH, ACK)
Window: 2050
[calculated window size: 524800]
[window size scaling factor: 256]
Checksum: 0xae4b [unverified]
[Checksum Status: Unverified]
Urgent Pointer: 0
> [SEQ/ACK analysis]
[Timestamps]

```
0000 80 c5 f2 1e 36 59 18 a6 f7 f2 55 60 00 00 45 00 ...6V...U...E-
0010 00 6d 74 85 40 00 6d 06 20 3c 0d 4a a9 6d c0 a8 ..nt@m-<J-m-
0020 01 6a 01 bb 07 dc 82 2e ab 97 bb 59 f4 a1 50 18 .j.....Y..P-
0030 08 02 00 00 00 17 03 03 00 40 00 00 00 00 00 ..[.....@-....
0040 00 00 01 92 64 c8 1a 27 e0 c8 0a 56 b6 73 fb 88 ...d...V.s-
0050 83 4f 72 52 36 18 be 62 56 19 cd 53 4e 00 ad aa ..OrRG..bV..SH-
0060 8a 27 17 25 cd 8f 34 d9 d3 c2 2f 0e 8a 8d 3a b4 ..'%.4-./-:-
0070 5a 75 ec 86 cd 89 a0 0f 9c e3 5b Zu.....-[-
```

عكس 2-5

UDP checksum: 0x0000ef6b

47..62.877237	fe80::48a6:3d2f:981::	ff02::1:3	LLMNR	84	Standard query 0x6ce8 A shit
47..62.877580	192.168.1.106	224.0.0.252	LLMNR	64	Standard query 0x6ce8 A shit
47..62.878143	fe80::48a6:3d2f:981::	ff02::1:3	LLMNR	84	Standard query 0x81d1 AAAA shit
47..62.878425	192.168.1.106	224.0.0.252	LLMNR	64	Standard query 0x81d1 AAAA shit

> Frame 4799: 64 bytes on wire (512 bits), 64 bytes captured (512 bits) on interface \Device\NPF_{BF4ABADA-2C91-4476-AEFA-D0FB460BC015}, id 0
> Ethernet II, Src: AzureNv1e:36:59 (80:c5:f2:1e:36:59), Dst: IPv4mcast_fc (01:00:5e:00:00:fc)
> Internet Protocol Version 4, Src: 192.168.1.106, Dst: 224.0.0.252
v User Datagram Protocol, Src Port: 62847, Dst Port: 5355
Source Port: 62847
Destination Port: 5355
Length: 30
Checksum: 0xef6b [unverified]
[Checksum Status: Unverified]
[Stream index: 42]
> [Timestamps]
UDP payload (22 bytes)
> Link-local Multicast Name Resolution (query)

0000 01 00 5e 00 00 fc 80 c5 f2 1e 36 59 00 00 45 00 ...^.....6V...E-
0010 00 32 74 46 00 00 01 11 a2 66 c0 a8 01 6a e0 00 ..2tF.....f...j-
0020 00 fc f5 7f 14 eb 00 1e af 01 81 d1 00 00 00 01[.....s hit.....
0030 00 00 00 00 00 00 04 73 68 69 74 00 00 1c 00 01

عكس 3-5

بخش دوم

```
Pinging google.com [216.58.210.78] with 32 bytes of data:
Reply from 216.58.210.78: bytes=32 time=183ms TTL=111
Reply from 216.58.210.78: bytes=32 time=170ms TTL=111
Reply from 216.58.210.78: bytes=32 time=150ms TTL=111
Reply from 216.58.210.78: bytes=32 time=171ms TTL=111

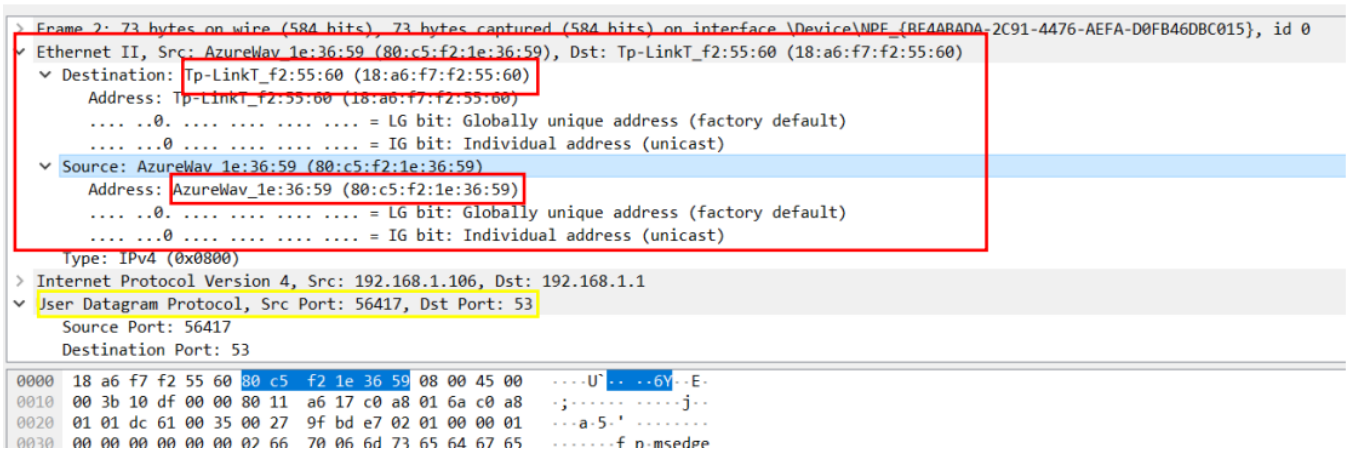
Ping statistics for 216.58.210.78:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
Approximate round trip times in milli-seconds:
    Minimum = 150ms, Maximum = 183ms, Average = 168ms

C:\Users\ASUS>nslookup 1.1.1.1
Server:    UnKnown
Address:   192.168.1.1

Name:      one.one.one.one
Address:   1.1.1.1
```

عکس 4-5

سوال ششم) یکی از بسته‌های ارسال شده را انتخاب کردیم. مبدا آن 192.168.1.106 می‌باشد. پروتکل لایه UDP می‌باشد که با کادر زرد مشخص شده است. آدرس IP مقصد نیز برابر 192.168.1.1 می‌باشد و از سرآیند لایه دوم، آدرس فیزیکی مبدا و مقصد را مشاهده می‌کنیم که در شکل با کادر قرمز مشخص شده است.



شکل 1-6

سوال هفتم) آدرس آییی مبدا و مقصد را می‌توانیم در بخش `ipconfig /all` مشاهده کنیم.

```
Wireless LAN adapter Wi-Fi:

Connection-specific DNS Suffix . . . : 
Description . . . . . : Realtek 8822BE Wireless LAN 802.11ac PCI-E NIC
Physical Address. . . . . : 80-C5-F2-1E-36-59
DHCP Enabled. . . . . : Yes
Autoconfiguration Enabled . . . . : Yes
Link-local IPv6 Address . . . . . : fe80::48a6:3d2f:981d:3372%26(Preferred)
IPv4 Address. . . . . : 192.168.1.106(Preferred)
Subnet Mask . . . . . : 255.255.255.0
Lease Obtained. . . . . : Thursday, April 8, 2021 9:41:59 PM
Lease Expires . . . . . : Sunday, April 11, 2021 9:41:59 PM
Default Gateway . . . . . : 192.168.1.1
DHCP Server . . . . . : 192.168.1.1
DHCPv6 IAID . . . . . : 209765874
DHCPv6 Client DUID. . . . . : 00-01-00-01-21-F4-F3-2A-2C-FD-A1-AC-52-7B
DNS Servers . . . . . : 192.168.1.1
NetBIOS over Tcpip. . . . . : Disabled

Ethernet adapter Bluetooth Network Connection:
```

عکس 7-1

سوال هشتم) محددات ران می‌کنیم و پینگ می‌گیریم تا فقط بسته‌های مربوط به پینگ را `capture` کنیم.

The image shows a Wireshark packet capture of network traffic. The top pane displays a list of packets with columns for No., Time, Source, Destination, Protocol, Length, and Info. The bottom pane shows the details of a selected DNS response packet (No. 6).

No.	Time	Source	Destination	Protocol	Length	Info
1	0.000000	192.168.1.106	208.67.222.222	DNS	108	Standard query 0xe484 A api.88c5aed2dae612309b9554e7d6a3a11b5b7a8e06.com
2	0.134337	208.67.222.222	192.168.1.106	DNS	140	Standard query response 0xe484 A api.88c5aed2dae612309b9554e7d6a3a11b5b7a8e06.com A 172.67.159.134 A 104.21.33.67
3	26.352273	192.168.1.106	192.168.1.1	DNS	70	Standard query 0xad9f A google.com
4	27.352678	192.168.1.106	192.168.1.1	DNS	70	Standard query 0xad9f A google.com
5	27.477944	192.168.1.1	192.168.1.106	DNS	86	Standard query response 0xad9f A google.com A 172.217.169.238
6	27.670109	192.168.1.1	192.168.1.106	DNS	86	Standard query response 0xad9f A google.com A 216.58.210.78

Domain Name System (response)
Transaction ID: 0xad9f
Flags: 0x8180 Standard query response, no error
Questions: 1
Answer RRs: 1
Authority RRs: 0
Additional RRs: 0
Queries
 google.com: type A, class IN
 Name: google.com
 [Name Length: 10]
 [Label Count: 2]
 Type: A (Host Address) (1)
 Class: IN (0x0001)
Answers

عکس 8-1

همانطور که می‌بینیم تایپ `A` یا `1` است. دکوردهای این تایپ ساده ترین دکوردهای `DNS` هستند و از آن‌ها برای اشاره یک دامنه با زیردامنه به یک آدرس `IP` استفاده می‌شود. به عبارتی این تایپ از دکورد برای ترجمه آدرس دامنه `google.com` به آدرس `IP` آن استفاده شده است.

سوال نهم) این بار تایپ query ما PTR است یا پوینتر است که برعکس دکوردهای تایپ 1، مشخص می کند که یک آدرس IP به چه دامنه ای اشاره می کند و بیشتر در DNS lookup از آن استفاده می شود.

No.	Time	Source	Destination	Protocol	Length	Info
1	0.000000	192.168.1.106	192.168.1.1	DNS	70	Standard query 0x712d A google.com
2	0.247236	192.168.1.1	192.168.1.106	DNS	86	Standard query response 0x712d A google.com A 172.217.169.238
3	11.000280	192.168.1.106	192.168.1.1	DNS	84	Standard query 0x0001 PTR 1.1.1.1.in-addr.arpa
4	11.887826	192.168.1.1	192.168.1.106	DNS	161	Standard query response 0x0001 No such name PTR 1.1.1.1.in-addr.arpa SOA prisoner.iana.org
5	11.889274	192.168.1.106	192.168.1.1	DNS	80	Standard query 0x0002 PTR 1.1.1.1.in-addr.arpa
6	12.007971	192.168.1.1	192.168.1.106	DNS	109	Standard query response 0x0002 PTR 1.1.1.1.in-addr.arpa PTR one.one.one.one


```

> Ethernet II, Src: AzureWav_1e:36:59 (80:c5:f2:1e:36:59), Dst: Tp-LinkT_f2:55:60 (18:a6:f7:f2:55:60)
> Internet Protocol Version 4, Src: 192.168.1.106, Dst: 192.168.1.1
> User Datagram Protocol, Src Port: 50531, Dst Port: 53
v Domain Name System (query)
  Transaction ID: 0x0002
  > Flags: 0x0100 Standard query
    Questions: 1
    Answer RRs: 0
    Authority RRs: 0
    Additional RRs: 0
  v Queries
    v 1.1.1.1.in-addr.arpa: type PTR, class IN
      Name: 1.1.1.1.in-addr.arpa
      [Name Length: 20]
      [Label Count: 6]
      Type: PTR (domain name PoinTeR) (12)
  
```

عکس 9-1

سوال دهم)

دکورد تایپ MX که در ارسال ایمیل از آن استفاده می شود.

دکورد تایپ LOC که نقطه جغرافیایی منسوب به یک دامنه را مشخص می کند.

دکورد تایپ APL که لیستی از رنج های آدرسی را مشخص می کند.

بخش سوم

No.	Time	Source	Destination	Protocol	Length	Info
435	192.427175	172.217.18.138	192.168.1.106	TCP	60	443 → 3393 [ACK] Seq=7054 Ack=1409 Win=68864 Len=0
436	192.449263	172.217.18.138	192.168.1.106	TCP	60	443 → 3393 [FIN, ACK] Seq=7054 Ack=1409 Win=68864 Len=0
437	193.371108	172.217.18.138	192.168.1.106	TCP	60	443 → 3393 [ACK] Seq=7055 Ack=1410 Win=68864 Len=0
438	202.064972	192.168.1.106	216.58.209.131	TCP	55	[TCP Keep-Alive] 3394 → 80 [ACK] Seq=387 Ack=702 Win=16640 Len=1
439	202.177732	67.198.134.186	192.168.1.106	TCP	69	433 → 1548 [PSH, ACK] Seq=46 Ack=133 Win=257 Len=15
440	202.178079	192.168.1.106	67.198.134.186	TCP	60	1548 → 433 [ACK] Seq=133 Ack=61 Win=67 Len=0
441	202.436040	216.58.209.131	192.168.1.106	TCP	60	80 → 3393 [ACK] Seq=387 Ack=1410 Win=68864 Len=0
442	202.643771	67.198.134.186	192.168.1.106	TCP	60	1548 → 433 [ACK] Seq=133 Ack=61 Win=67 Len=0
443	202.643843	192.168.1.106	67.198.134.186	TCP	60	433 → 1548 [ACK] Seq=387 Ack=702 Win=16640 Len=1
444	202.653502	192.168.1.106	67.198.134.186	TCP	60	433 → 1548 [ACK] Seq=387 Ack=702 Win=16640 Len=1
445	202.689211	67.198.134.186	192.168.1.106	TCP	60	1548 → 433 [ACK] Seq=133 Ack=61 Win=67 Len=0
446	203.816266	67.198.134.186	192.168.1.106	TCP	60	1548 → 433 [ACK] Seq=133 Ack=61 Win=67 Len=0

Field Name

> IProvideClassInfo - DCOM IProvideClassInfo
 > IPSICTL - IPSICTL
 > IPv4 - Internet Protocol Version 4
 ip.addr - Source or Destination Address
 ip.bogus_header_length - Bogus IP header length
 ip.bogus_ip_length - Bogus IP length
 ip.bogus_ip_version - Bogus IP version
 ip.checksum - Header Checksum
 ip.checksum_status - Header checksum status
 ip.checksum_bad.expert - Bad checksum
 ip.checksum_calculated - Calculated Checksum
 ip.cipso.categories - Categories
 ip.cipso.doi - DOI

Relation

is present
 ==
 !=
 >
 Value (IPv4 address)
 5.144.130.115
 Predefined Values
 Range (offset:length)

Search:

ip.addr == 5.144.130.115

Click OK to insert this filter

OK Cancel Help

عکس 1-10

سوال یازدهم) ICMP

Wi-Fi

File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help

ip.addr == 5.144.130.115

No.	Time	Source	Destination	Protocol	Length	Info
42	47.547071	192.168.1.106	5.144.130.115	ICMP	106	Echo (ping) request id=0x0001, seq=27/6912, ttl=1 (no response found!)
43	47.758989	192.168.1.1	192.168.1.106	ICMP	70	Time-to-live exceeded (Time to live exceeded in transit)
44	47.759723	192.168.1.106	5.144.130.115	ICMP	106	Echo (ping) request id=0x0001, seq=28/7168, ttl=1 (no response found!)
45	48.066515	192.168.1.1	192.168.1.106	ICMP	70	Time-to-live exceeded (Time to live exceeded in transit)
46	48.069618	192.168.1.106	5.144.130.115	ICMP	106	Echo (ping) request id=0x0001, seq=29/7424, ttl=1 (no response found!)
47	48.373706	192.168.1.1	192.168.1.106	ICMP	70	Time-to-live exceeded (Time to live exceeded in transit)
56	50.173367	192.168.1.106	5.144.130.115	ICMP	106	Echo (ping) request id=0x0001, seq=30/7680, ttl=2 (no response found!)
58	50.421644	46.224.0.12	192.168.1.106	ICMP	70	Time-to-live exceeded (Time to live exceeded in transit)
59	50.424919	192.168.1.106	5.144.130.115	ICMP	106	Echo (ping) request id=0x0001, seq=31/7936, ttl=2 (no response found!)
60	50.728740	46.224.0.12	192.168.1.106	ICMP	70	Time-to-live exceeded (Time to live exceeded in transit)
61	50.732009	192.168.1.106	5.144.130.115	ICMP	106	Echo (ping) request id=0x0001, seq=32/8192, ttl=2 (no response found!)
62	51.035729	46.224.0.12	192.168.1.106	ICMP	70	Time-to-live exceeded (Time to live exceeded in transit)

Frame 42: 106 bytes on wire (848 bits), 106 bytes captured (848 bits) on interface \Device\NPF_{BFA4BADA-2C91-4476-AEFA-D0FB46DBC015}, id 0
 Ethernet II, Src: AzureWav_1e:36:59 (08:c5:f2:1e:36:59), Dst: Tp-LinkT_f2:55:60 (18:a6:f7:f2:55:60)
 Internet Protocol Version 4, Src: 192.168.1.106, Dst: 5.144.130.115
 Internet Control Message Protocol

عکس 1-11

تایپ B

ip.addr == 5.144.130.115						
No.	Time	Source	Destination	Protocol	Length	Info
42	47.547071	192.168.1.106	5.144.130.115	ICMP	106	Echo (ping) request id=0x0001, seq=27/6912, ttl=1 (no response found!)
43	47.758989	192.168.1.1	192.168.1.106	ICMP	70	Time-to-live exceeded (Time to live exceeded in transit)
44	47.759723	192.168.1.106	5.144.130.115	ICMP	106	Echo (ping) request id=0x0001, seq=28/7168, ttl=1 (no response found!)
45	48.066515	192.168.1.1	192.168.1.106	ICMP	70	Time-to-live exceeded (Time to live exceeded in transit)
46	48.069618	192.168.1.106	5.144.130.115	ICMP	106	Echo (ping) request id=0x0001, seq=29/7424, ttl=1 (no response found!)
47	48.373706	192.168.1.1	192.168.1.106	ICMP	70	Time-to-live exceeded (Time to live exceeded in transit)
56	50.173367	192.168.1.106	5.144.130.115	ICMP	106	Echo (ping) request id=0x0001, seq=30/7680, ttl=2 (no response found!)
58	50.421644	46.224.0.12	192.168.1.106	ICMP	70	Time-to-live exceeded (Time to live exceeded in transit)
59	50.424919	192.168.1.106	5.144.130.115	ICMP	106	Echo (ping) request id=0x0001, seq=31/7936, ttl=2 (no response found!)
60	50.728740	46.224.0.12	192.168.1.106	ICMP	70	Time-to-live exceeded (Time to live exceeded in transit)
61	50.732009	192.168.1.106	5.144.130.115	ICMP	106	Echo (ping) request id=0x0001, seq=32/8192, ttl=2 (no response found!)
62	51.035729	46.224.0.12	192.168.1.106	ICMP	70	Time-to-live exceeded (Time to live exceeded in transit)
> Frame 42: 106 bytes on wire (848 bits), 106 bytes captured (848 bits) on interface \Device\NPF_{BF4ABADA-2C91-4476-AEFA-D0FB46DBC015}, id 0 > Ethernet II, Src: AzureWav_1e:36:59 (80:c5:f2:1e:36:59), Dst: Tp-LinkT_f2:55:60 (18:a6:f7:f2:55:60) > Internet Protocol Version 4, Src: 192.168.1.106, Dst: 5.144.130.115 > Internet Control Message Protocol Type: 8 (Echo (ping) request) Code: 0 Checksum: 0xf7e3 [correct] [Checksum Status: Good] Identifier (BE): 1 (0x0001) Identifier (LE): 256 (0x0100) Sequence Number (BE): 27 (0x001b) Sequence Number (LE): 6912 (0x1b00) > [No response seen] > Data (64 bytes)						

عکس 1-12

TTL=1

ip.addr == 5.144.130.115						
No.	Time	Source	Destination	Protocol	Length	Info
42	47.547071	192.168.1.106	5.144.130.115	ICMP	106	Echo (ping) request id=0x0001, seq=27/6912, ttl=1 (no response found!)
43	47.758989	192.168.1.1	192.168.1.106	ICMP	70	Time-to-live exceeded (Time to live exceeded in transit)
44	47.759723	192.168.1.106	5.144.130.115	ICMP	106	Echo (ping) request id=0x0001, seq=28/7168, ttl=1 (no response found!)
45	48.066515	192.168.1.1	192.168.1.106	ICMP	70	Time-to-live exceeded (Time to live exceeded in transit)
46	48.069618	192.168.1.106	5.144.130.115	ICMP	106	Echo (ping) request id=0x0001, seq=29/7424, ttl=1 (no response found!)
47	48.373706	192.168.1.1	192.168.1.106	ICMP	70	Time-to-live exceeded (Time to live exceeded in transit)
56	50.173367	192.168.1.106	5.144.130.115	ICMP	106	Echo (ping) request id=0x0001, seq=30/7680, ttl=2 (no response found!)
58	50.421644	46.224.0.12	192.168.1.106	ICMP	70	Time-to-live exceeded (Time to live exceeded in transit)
59	50.424919	192.168.1.106	5.144.130.115	ICMP	106	Echo (ping) request id=0x0001, seq=31/7936, ttl=2 (no response found!)
60	50.728740	46.224.0.12	192.168.1.106	ICMP	70	Time-to-live exceeded (Time to live exceeded in transit)
61	50.732009	192.168.1.106	5.144.130.115	ICMP	106	Echo (ping) request id=0x0001, seq=32/8192, ttl=2 (no response found!)
62	51.035729	46.224.0.12	192.168.1.106	ICMP	70	Time-to-live exceeded (Time to live exceeded in transit)
Frame 42: 106 bytes on wire (848 bits), 106 bytes captured (848 bits) on interface \Device\NPF_{BF4ABADA-2C91-4476-AEFA-D0FB46DBC015}, id 0 Ethernet II, Src: AzureWav_1e:36:59 (80:c5:f2:1e:36:59), Dst: Tp-LinkT_f2:55:60 (18:a6:f7:f2:55:60) Internet Protocol Version 4, Src: 192.168.1.106, Dst: 5.144.130.115 0100 = Version: 4 0101 = Header Length: 20 bytes (5) > Differentiated Services Field: 0x00 (DSCP: CS0, ECN: Not-ECT) Total Length: 92 Identification: 0x4f37 (20279) > Flags: 0x00 Fragment Offset: 0 > Time to Live: 1 > [Expert Info (Note/Sequence): "Time To Live" only 1] Protocol: ICMP (1) Header Checksum: 0x2055 [validation disabled] [Header checksum status: Unverified] Source Address: 192.168.1.106						

عکس 2-12

سوال سیزدهم) همانطور که مشاهده می‌کنید هرچه در بسته‌هایی که از آدرس 192.168.1.106 ارسال شده‌اند پیش می‌رویم؛ TTL افزایش می‌یابد. باید از دستور **tracert** برای بررسی مسیری که یک بسته برای رسیدن به IP مقصد آن را طی می‌کند استفاده می‌کنیم.

این عدد از 1 تا 10 تغییر می‌کند چون **tracert** نیز در ده گام انجام شد.

No.	Time	Source	Destination	Protocol	Length	Info
42	47.547071	192.168.1.106	5.144.130.115	ICMP	106	Echo (ping) request id=0x0001, seq=27/6912, ttl=1 (no response found!)
43	47.758989	192.168.1.1	192.168.1.106	ICMP	70	Time-to-live exceeded (Time to live exceeded in transit)
44	47.759723	192.168.1.106	5.144.130.115	ICMP	106	Echo (ping) request id=0x0001, seq=28/7168, ttl=1 (no response found!)
45	48.066515	192.168.1.1	192.168.1.106	ICMP	70	Time-to-live exceeded (Time to live exceeded in transit)
46	48.069618	192.168.1.106	5.144.130.115	ICMP	106	Echo (ping) request id=0x0001, seq=29/7424, ttl=1 (no response found!)
47	48.373706	192.168.1.1	192.168.1.106	ICMP	70	Time-to-live exceeded (Time to live exceeded in transit)
56	50.173367	192.168.1.106	5.144.130.115	ICMP	106	Echo (ping) request id=0x0001, seq=30/7680, ttl=2 (no response found!)
58	50.421644	46.224.0.12	192.168.1.106	ICMP	70	Time-to-live exceeded (Time to live exceeded in transit)
59	50.424919	192.168.1.106	5.144.130.115	ICMP	106	Echo (ping) request id=0x0001, seq=31/7936, ttl=2 (no response found!)
60	50.728740	46.224.0.12	192.168.1.106	ICMP	70	Time-to-live exceeded (Time to live exceeded in transit)
61	50.732009	192.168.1.106	5.144.130.115	ICMP	106	Echo (ping) request id=0x0001, seq=32/8192, ttl=2 (no response found!)
62	51.035729	46.224.0.12	192.168.1.106	ICMP	70	Time-to-live exceeded (Time to live exceeded in transit)

> Frame 56: 106 bytes on wire (848 bits), 106 bytes captured (848 bits) on interface \Device\NPF_{BF4ABADA-2C91-4476-AEFA-D0FB46DBC015}, id 0
> Ethernet II, Src: AzureWav_1e:36:59 (80:c5:f2:1e:36:59), Dst: Tp-LinkT_f2:55:60 (18:a6:f7:f2:55:60)

▼ Internet Protocol Version 4, Src: 192.168.1.106, Dst: 5.144.130.115

- 0100 = Version: 4
- 0101 = Header Length: 20 bytes (5)
- > Differentiated Services Field: 0x00 (DSCP: CS0, ECN: Not-ECT)
- Total Length: 92
- Identification: 0x4f3a (20282)
- > Flags: 0x00
- Fragment Offset: 0
- ▼ Time to Live: 2
- > [Expert Info (Note/Sequence): "Time To Live" only 2]
- Protocol: ICMP (1)
- Header Checksum: 0xf152 [validation disabled]
- [Header checksum status: Unverified]
- Source Address: 192.168.1.106

عکس 1-13

No.	Time	Source	Destination	Protocol	Length	Info
68	52.162134	172.16.5.65	192.168.1.106	ICMP	70	Time-to-live exceeded (Time to live exceeded in transit)
69	52.163678	192.168.1.106	5.144.130.115	ICMP	106	Echo (ping) request id=0x0001, seq=34/8704, ttl=3 (no response found!)
70	52.367337	172.16.5.65	192.168.1.106	ICMP	70	Time-to-live exceeded (Time to live exceeded in transit)
71	52.370538	192.168.1.106	5.144.130.115	ICMP	106	Echo (ping) request id=0x0001, seq=35/8960, ttl=3 (no response found!)
72	52.571833	172.16.5.65	192.168.1.106	ICMP	70	Time-to-live exceeded (Time to live exceeded in transit)
77	53.632114	192.168.1.106	5.144.130.115	ICMP	106	Echo (ping) request id=0x0001, seq=36/9216, ttl=4 (no response found!)
79	54.005879	46.224.0.209	192.168.1.106	ICMP	70	Time-to-live exceeded (Time to live exceeded in transit)
80	54.009145	192.168.1.106	5.144.130.115	ICMP	106	Echo (ping) request id=0x0001, seq=37/9472, ttl=4 (no response found!)
81	54.313235	46.224.0.209	192.168.1.106	ICMP	70	Time-to-live exceeded (Time to live exceeded in transit)
82	54.316482	192.168.1.106	5.144.130.115	ICMP	106	Echo (ping) request id=0x0001, seq=38/9728, ttl=4 (no response found!)
83	55.951230	46.224.0.209	192.168.1.106	ICMP	70	Time-to-live exceeded (Time to live exceeded in transit)
87	56.216799	192.168.1.106	5.144.130.115	ICMP	106	Echo (ping) request id=0x0001, seq=39/9984, ttl=5 (no response found!)

> Frame 87: 106 bytes on wire (848 bits), 106 bytes captured (848 bits) on interface \Device\NPF_{BF4ABADA-2C91-4476-AEFA-D0FB46DBC015}, id 0
> Ethernet II, Src: AzureWav_1e:36:59 (80:c5:f2:1e:36:59), Dst: Tp-LinkT_f2:55:60 (18:a6:f7:f2:55:60)

▼ Internet Protocol Version 4, Src: 192.168.1.106, Dst: 5.144.130.115

- 0100 = Version: 4
- 0101 = Header Length: 20 bytes (5)
- > Differentiated Services Field: 0x00 (DSCP: CS0, ECN: Not-ECT)
- Total Length: 92
- Identification: 0x4f43 (20291)
- > Flags: 0x00
- Fragment Offset: 0
- Time to Live: 5
- Protocol: ICMP (1)
- Header Checksum: 0x1c49 [validation disabled]
- [Header checksum status: Unverified]
- Source Address: 192.168.1.106
- Destination Address: 5.144.130.115

عکس 2-13

ip.addr == 5.144.130.115						
No.	Time	Source	Destination	Protocol	Length	Info
151	65.781166	10.202.1.5	192.168.1.106	ICMP	70	Time-to-live exceeded (Time to live exceeded in transit)
152	65.782503	192.168.1.106	5.144.130.115	ICMP	106	Echo (ping) request id=0x0001, seq=50/12800, ttl=8 (no response found!)
153	66.190900	10.202.1.5	192.168.1.106	ICMP	70	Time-to-live exceeded (Time to live exceeded in transit)
158	67.075330	192.168.1.106	5.144.130.115	ICMP	106	Echo (ping) request id=0x0001, seq=51/13056, ttl=9 (no response found!)
159	71.003166	192.168.1.106	5.144.130.115	ICMP	106	Echo (ping) request id=0x0001, seq=52/13312, ttl=9 (no response found!)
160	75.003299	192.168.1.106	5.144.130.115	ICMP	106	Echo (ping) request id=0x0001, seq=53/13568, ttl=9 (no response found!)
169	79.006191	192.168.1.106	5.144.130.115	ICMP	106	Echo (ping) request id=0x0001, seq=54/13824, ttl=10 (reply in 173)
173	80.015132	5.144.130.115	192.168.1.106	ICMP	106	Echo (ping) reply id=0x0001, seq=54/13824, ttl=55 (request in 169)
174	80.018013	192.168.1.106	5.144.130.115	ICMP	106	Echo (ping) request id=0x0001, seq=55/14080, ttl=10 (reply in 175)
175	80.141846	5.144.130.115	192.168.1.106	ICMP	106	Echo (ping) reply id=0x0001, seq=55/14080, ttl=55 (request in 174)
176	80.145018	192.168.1.106	5.144.130.115	ICMP	106	Echo (ping) request id=0x0001, seq=56/14336, ttl=10 (reply in 181)
181	80.629461	5.144.130.115	192.168.1.106	ICMP	106	Echo (ping) reply id=0x0001, seq=56/14336, ttl=55 (request in 176)

> Frame 160: 106 bytes on wire (848 bits), 106 bytes captured (848 bits) on interface \Device\NPF_{BF4ABADA-2C91-4476-AEFA-D0FB46D8C015}, id 0

> Ethernet II, Src: AzureWav_1e:36:59 (80:c5:f2:1e:36:59), Dst: Tp-LinkT_f2:55:60 (18:a6:f7:f2:55:60)

Internet Protocol Version 4, Src: 192.168.1.106, Dst: 5.144.130.115

0100 = Version: 4

.... 0101 = Header Length: 20 bytes (5)

> Differentiated Services Field: 0x00 (DSCP: CS0, ECN: Not-ECT)

Total Length: 92

Identification: 0x4f51 (20305)

> Flags: 0x00

Fragment Offset: 0

Time to Live: 9

Protocol: ICMP (1)

Header Checksum: 0x183b [validation disabled]

[Header checksum status: Unverified]

Source Address: 192.168.1.106

Destination Address: 5.144.130.115

عکس 3-13

ip.addr == 5.144.130.115						
No.	Time	Source	Destination	Protocol	Length	Info
151	65.781166	10.202.1.5	192.168.1.106	ICMP	70	Time-to-live exceeded (Time to live exceeded in transit)
152	65.782503	192.168.1.106	5.144.130.115	ICMP	106	Echo (ping) request id=0x0001, seq=50/12800, ttl=8 (no response found!)
153	66.190900	10.202.1.5	192.168.1.106	ICMP	70	Time-to-live exceeded (Time to live exceeded in transit)
158	67.075330	192.168.1.106	5.144.130.115	ICMP	106	Echo (ping) request id=0x0001, seq=51/13056, ttl=9 (no response found!)
159	71.003166	192.168.1.106	5.144.130.115	ICMP	106	Echo (ping) request id=0x0001, seq=52/13312, ttl=9 (no response found!)
160	75.003299	192.168.1.106	5.144.130.115	ICMP	106	Echo (ping) request id=0x0001, seq=53/13568, ttl=9 (no response found!)
169	79.006191	192.168.1.106	5.144.130.115	ICMP	106	Echo (ping) request id=0x0001, seq=54/13824, ttl=10 (reply in 173)
173	80.015132	5.144.130.115	192.168.1.106	ICMP	106	Echo (ping) reply id=0x0001, seq=54/13824, ttl=55 (request in 169)
174	80.018013	192.168.1.106	5.144.130.115	ICMP	106	Echo (ping) request id=0x0001, seq=55/14080, ttl=10 (reply in 175)
175	80.141846	5.144.130.115	192.168.1.106	ICMP	106	Echo (ping) reply id=0x0001, seq=55/14080, ttl=55 (request in 174)
176	80.145018	192.168.1.106	5.144.130.115	ICMP	106	Echo (ping) request id=0x0001, seq=56/14336, ttl=10 (reply in 181)
181	80.629461	5.144.130.115	192.168.1.106	ICMP	106	Echo (ping) reply id=0x0001, seq=56/14336, ttl=55 (request in 176)

> Frame 174: 106 bytes on wire (848 bits), 106 bytes captured (848 bits) on interface \Device\NPF_{BF4ABADA-2C91-4476-AEFA-D0FB46D8C015}, id 0

> Ethernet II, Src: AzureWav_1e:36:59 (80:c5:f2:1e:36:59), Dst: Tp-LinkT_f2:55:60 (18:a6:f7:f2:55:60)

Internet Protocol Version 4, Src: 192.168.1.106, Dst: 5.144.130.115

0100 = Version: 4

.... 0101 = Header Length: 20 bytes (5)

> Differentiated Services Field: 0x00 (DSCP: CS0, ECN: Not-ECT)

Total Length: 92

Identification: 0x4f53 (20307)

> Flags: 0x00

Fragment Offset: 0

Time to Live: 10

Protocol: ICMP (1)

Header Checksum: 0x1739 [validation disabled]

[Header checksum status: Unverified]

Source Address: 192.168.1.106

Destination Address: 5.144.130.115

عکس 4-13

سوال چهاردهم)

این فیلتر بسته‌ها را بر اساس ورژن پروتکل IP آنها جداسازی می‌کند و بخش مشترک تمامی آنها، قسمت پروتکل در لایه سوم می‌باشد که برابر 6 است.

ip.proto == 6						
No.	Time	Source	Destination	Protocol	Length	Info
258	89.347239	194.225.33.19	192.168.1.106	TCP	66	993 → 3386 [SYN, ACK] Seq=0 Ack=1 Win=29200 Len=0 MSS=1390 SACK_PERM=1 WS=128
259	89.347239	194.225.33.19	192.168.1.106	TCP	60	993 → 3384 [RST] Seq=2 Win=0 Len=0
260	89.347474	192.168.1.106	194.225.33.19	TCP	54	3386 → 993 [ACK] Seq=1 Ack=1 Win=17408 Len=0
261	89.347618	192.168.1.106	194.225.33.19	GTP	63	SGSN context request
262	89.380329	194.225.33.19	192.168.1.106	TCP	60	993 → 3384 [RST] Seq=2 Win=0 Len=0
263	89.380329	194.225.33.19	192.168.1.106	TCP	60	993 → 3384 [RST] Seq=2 Win=0 Len=0
264	89.380781	194.225.33.19	192.168.1.106	TCP	60	993 → 3386 [ACK] Seq=1 Ack=10 Win=29312 Len=0
265	89.435983	194.225.33.19	192.168.1.106	TCP	60	993 → 3386 [RST, ACK] Seq=2 Ack=10 Win=29312 Len=0
266	89.436070	192.168.1.106	194.225.33.19	TCP	54	[TCP Dup ACK 260#1] 3386 → 993 [ACK] Seq=10 Ack=1 Win=17408 Len=0
267	89.466989	194.225.33.19	192.168.1.106	TCP	60	[TCP Out-Of-Order] 993 → 3386 [FIN, ACK] Seq=1 Ack=10 Win=29312 Len=0
268	89.467107	192.168.1.106	194.225.33.19	TCP	54	3386 → 993 [ACK] Seq=10 Ack=2 Win=17408 Len=0
269	89.467310	192.168.1.106	194.225.33.19	GTP	69	SGSN context response

> Frame 269: 69 bytes on wire (552 bits), 69 bytes captured (552 bits) on interface \Device\NPF_{BF4ABADA-2C91-4476-AEFA-D0FB46DBC015}, id 0

> Ethernet II, Src: AzureWav_1e:36:59 (80:c5:f2:1e:36:59), Dst: Tp-LinkT_f2:55:60 (18:a6:f7:f2:55:60)

Internet Protocol Version 4, Src: 192.168.1.106, Dst: 194.225.33.19

0100 = Version: 4

.... 0101 = Header Length: 20 bytes (5)

> Differentiated Services Field: 0x00 (DSCP: CS0, ECN: Not-ECT)

Total Length: 55

Identification: 0x2087 (8327)

> Flags: 0x40, Don't fragment

Fragment Offset: 0

Time to Live: 128

Protocol: TCP (6)

Header Checksum: 0x3433 [validation disabled]

[Header checksum status: Unverified]

Source Address: 192.168.1.106

Destination Address: 194.225.33.19

عکس 1-14