

به نام خدا
آرتا اسدی
9731006

گزارش آزمایش کار با Wireshark

سوال 1 ->

پروتکل هایی مانند TCP، UDP، ARP، TLSv1.2، QUIC مشاهده می شود :

The image shows a Wireshark network traffic capture. The main packet list displays several UDP packets from 192.168.65.107 to 192.168.65.107 and 142.251.9.189. Two ARP packets are highlighted in yellow, showing a request and response between 5a:7a:1b:ef:43:99 and 192.168.65.107. The packet details pane shows the structure of the selected packet, including Ethernet II, Internet Protocol Version 4, User Datagram Protocol, and Data (43 bytes). The packet bytes pane shows the raw data in hexadecimal and ASCII.

No.	Time	Source	Destination	Protocol	Length	Info
6	0.130284	192.168.65.107	172.217.21.46	UDP	75	52437 → 443 Len=33
7	0.131731	172.217.21.46	192.168.65.107	UDP	67	443 → 52437 Len=25
8	0.209193	192.168.65.107	142.251.9.189	UDP	75	54003 → 443 Len=33
9	0.242043	172.217.21.46	192.168.65.107	UDP	559	443 → 52437 Len=517
10	0.242043	172.217.21.46	192.168.65.107	UDP	140	443 → 52437 Len=98
11	0.242415	192.168.65.107	172.217.21.46	UDP	77	52437 → 443 Len=35
12	0.268957	192.168.65.107	172.217.21.46	UDP	75	52437 → 443 Len=33
13	0.330689	172.217.21.46	192.168.65.107	UDP	67	443 → 52437 Len=25
14	0.390049	142.251.9.189	192.168.65.107	UDP	67	443 → 54003 Len=25
15	0.600518	192.168.65.107	142.251.9.189	UDP	75	54003 → 443 Len=33
16	0.842667	142.251.9.189	192.168.65.107	UDP	67	443 → 54003 Len=25
17	0.875531	5a:7a:1b:ef:43:99	MS-NLB-PhysServer-3...	ARP	42	Who has 192.168.65.107? Tell 192.168.65.51
18	0.875563	MS-NLB-PhysServer-3...	5a:7a:1b:ef:43:99	ARP	42	192.168.65.107 is at 02:26:0d:6e:67:61
19	1.051429	192.168.65.107	142.251.9.189	UDP	75	54003 → 443 Len=33
20	1.267933	142.251.9.189	192.168.65.107	UDP	67	443 → 54003 Len=25

Frame 1: 85 bytes on wire (680 bits), 85 bytes captured (680 bits) on interface \Device\NPF_{1D03D5FD-E9D7-47A7-8C73-E8C07CB25A28}, id 0
Ethernet II, Src: 5a:7a:1b:ef:43:99 (5a:7a:1b:ef:43:99), Dst: MS-NLB-PhysServer-32_06:0d:6e:67:61 (02:26:0d:6e:67:61)
Internet Protocol Version 4, Src: 142.251.9.189, Dst: 192.168.65.107
User Datagram Protocol, Src Port: 443, Dst Port: 54003
Data (43 bytes)
Data: 4e2961c2ddc86f9efb135d4738d06147c1318d697b119f30522cf91dbc4ddf63d12e1617...
[Length: 43]

0000 02 26 0d 6e 67 61 5a 7a 1b ef 43 99 08 00 45 00 &ngaZz --C...E-
0010 00 47 00 00 40 00 31 11 ae da 8e fb 09 bd c0 a8 :G..@:1:
0020 41 6b 01 bb d2 f3 00 33 a7 6b 4e 29 61 c2 dd c8 Ak.....3 -kN)a+..

Wireshark_Ethernet_6SPQCD1.pcapng | Packets: 31455 | Displayed: 31455 (100.0%) | Profile: Default

Wireshark packet capture showing a TLSv1.3 connection. The packet list shows a sequence of frames from 4908 to 4922. The packet details pane shows the structure of a TLSv1.3 packet, including the TLSv1.3 header, application data, and protected payload. The packet bytes pane shows the raw data in hexadecimal and ASCII.

سوال 2 ->

بسته ی انتخاب شده در لایه application پروتکل TLSv1.2 دارد و در لایه transport نیز پروتکل TCP دارد و همین طور IPv4 پروتکل لایه network آن است. اندازه frame آن 196 بوده و اندازه کل بسته آن در لایه سوم 79 است.

Wireshark packet capture showing a TLSv1.2 connection. The packet list shows a sequence of frames from 184 to 198. The packet details pane shows the structure of a TLSv1.2 packet, including the TLSv1.2 header, application data, and protected payload. The packet bytes pane shows the raw data in hexadecimal and ASCII.

سوال 3 ->

بله، بسته های با پروتکل ARP

Wireshark capture of Ethernet traffic. The packet list shows a sequence of TCP and ARP packets. Packet 137 is highlighted, showing an ARP request from 107.155.105.90 to 192.168.65.107. The packet details pane shows the Ethernet II header and the ARP request structure. The packet bytes pane shows the raw data in hexadecimal and ASCII.

No.	Time	Source	Destination	Protocol	Length	Info
128	10.153047	188.40.236.75	192.168.65.107	TLSv1.2	1136	Application Data
129	10.205419	192.168.65.107	188.40.236.75	TCP	54	51228 → 443 [ACK] Seq=4322 Ack=4523 Win=509 Len=0
130	10.602916	107.155.105.90	192.168.65.107	TCP	95	80 → 50448 [PSH, ACK] Seq=83 Ack=1 Win=852 Len=41
131	10.621929	107.155.105.90	192.168.65.107	TCP	95	80 → 50448 [PSH, ACK] Seq=124 Ack=1 Win=852 Len=41
132	10.621960	192.168.65.107	107.155.105.90	TCP	54	50448 → 80 [ACK] Seq=1 Ack=165 Win=4108 Len=0
133	10.728774	107.155.105.90	192.168.65.107	TCP	95	80 → 50448 [PSH, ACK] Seq=165 Ack=1 Win=852 Len=41
134	10.744690	107.155.105.90	192.168.65.107	TCP	95	80 → 50448 [PSH, ACK] Seq=206 Ack=1 Win=852 Len=41
135	10.744738	192.168.65.107	107.155.105.90	TCP	54	50448 → 80 [ACK] Seq=1 Ack=247 Win=4108 Len=0
136	11.715309	5a:7a:1b:ef:43:99	MS-NLB-PhysServer-3...	ARP	42	Who has 192.168.65.107? Tell 192.168.65.51
137	11.715324	MS-NLB-PhysServer-3...	5a:7a:1b:ef:43:99	ARP	42	192.168.65.107 is at 02:26:0d:6e:67:61
138	11.977275	107.155.105.90	192.168.65.107	TCP	95	80 → 50448 [PSH, ACK] Seq=247 Ack=1 Win=852 Len=41
139	11.977275	107.155.105.90	192.168.65.107	TCP	95	80 → 50448 [PSH, ACK] Seq=288 Ack=1 Win=852 Len=41
140	11.977377	192.168.65.107	107.155.105.90	TCP	54	50448 → 80 [ACK] Seq=1 Ack=329 Win=4108 Len=0
141	13.124260	138.199.14.86	192.168.65.107	TCP	54	[TCP Keep-Alive] 80 → 49792 [ACK] Seq=0 Ack=2 Win=501 Len=0
142	13.124303	192.168.65.107	138.199.14.86	TCP	54	[TCP Keep-Alive ACK] 49792 → 80 [ACK] Seq=2 Ack=1 Win=508 Len=0

Frame 137: 42 bytes on wire (336 bits), 42 bytes captured (336 bits) on interface \Device\NPF_{1083D5FD-E9D7-47A7-8C73-E8C07CB25A28}, id 0
Ethernet II, Src: MS-NLB-PhysServer-32_06:0d:6e:67:61 (02:26:0d:6e:67:61), Dst: 5a:7a:1b:ef:43:99 (5a:7a:1b:ef:43:99)
Address Resolution Protocol (reply)

0000 5a 7a 1b ef 43 99 02 26 0d 6e 67 61 08 06 00 01 Zz..C..& nga....
0010 08 00 06 04 00 02 02 26 0d 6e 67 61 c0 a8 41 6b& nga..Ak
0020 5a 7a 1b ef 43 99 c0 a8 41 33 Zz..C... A3

سوال 4 ->

0x34a6

Wireshark capture of Ethernet traffic. The packet list shows a sequence of TCP and ARP packets. Packet 137 is highlighted, showing an ARP request from 107.155.105.90 to 192.168.65.107. The packet details pane shows the Ethernet II header and the ARP request structure. The packet bytes pane shows the raw data in hexadecimal and ASCII.

No.	Time	Source	Destination	Protocol	Length	Info
128	10.153047	188.40.236.75	192.168.65.107	TLSv1.2	1136	Application Data
129	10.205419	192.168.65.107	188.40.236.75	TCP	54	51228 → 443 [ACK] Seq=4322 Ack=4523 Win=509 Len=0
130	10.602916	107.155.105.90	192.168.65.107	TCP	95	80 → 50448 [PSH, ACK] Seq=83 Ack=1 Win=852 Len=41
131	10.621929	107.155.105.90	192.168.65.107	TCP	95	80 → 50448 [PSH, ACK] Seq=124 Ack=1 Win=852 Len=41
132	10.621960	192.168.65.107	107.155.105.90	TCP	54	50448 → 80 [ACK] Seq=1 Ack=165 Win=4108 Len=0
133	10.728774	107.155.105.90	192.168.65.107	TCP	95	80 → 50448 [PSH, ACK] Seq=165 Ack=1 Win=852 Len=41
134	10.744690	107.155.105.90	192.168.65.107	TCP	95	80 → 50448 [PSH, ACK] Seq=206 Ack=1 Win=852 Len=41
135	10.744738	192.168.65.107	107.155.105.90	TCP	54	50448 → 80 [ACK] Seq=1 Ack=247 Win=4108 Len=0
136	11.715309	5a:7a:1b:ef:43:99	MS-NLB-PhysServer-3...	ARP	42	Who has 192.168.65.107? Tell 192.168.65.51
137	11.715324	MS-NLB-PhysServer-3...	5a:7a:1b:ef:43:99	ARP	42	192.168.65.107 is at 02:26:0d:6e:67:61
138	11.977275	107.155.105.90	192.168.65.107	TCP	95	80 → 50448 [PSH, ACK] Seq=247 Ack=1 Win=852 Len=41
139	11.977275	107.155.105.90	192.168.65.107	TCP	95	80 → 50448 [PSH, ACK] Seq=288 Ack=1 Win=852 Len=41
140	11.977377	192.168.65.107	107.155.105.90	TCP	54	50448 → 80 [ACK] Seq=1 Ack=329 Win=4108 Len=0
141	13.124260	138.199.14.86	192.168.65.107	TCP	54	[TCP Keep-Alive] 80 → 49792 [ACK] Seq=0 Ack=2 Win=501 Len=0
142	13.124303	192.168.65.107	138.199.14.86	TCP	54	[TCP Keep-Alive ACK] 49792 → 80 [ACK] Seq=2 Ack=1 Win=508 Len=0

0100 = Version: 4
.... 0101 = Header Length: 20 bytes (5)
> Differentiated Services Field: 0x00 (DSCP: CS0, ECN: Not-ECT)
Total Length: 81
Identification: 0x4df8 (19960)
> Flags: 0x40, Don't fragment
Fragment Offset: 0
Time to Live: 33
Protocol: TCP (6)
Header Checksum: 0x34a6 [validation disabled]
[Header checksum status: Unverified]
Source Address: 107.155.105.90

0010 00 51 4d f8 40 00 21 06 34 a6 6b 0b 69 5a c0 a8 QM@! : k iz..
0020 41 6b 00 50 c5 10 e3 1e 2b 25 83 7f 54 8c 50 18 Ak P.... %..T.P..
0030 03 54 6b be 00 00 17 03 03 00 24 7d be 33 4e f2 -Tk.....-\$}-3N-

سوال 5 ->

پورت مبدا (فرستنده) 80 و پورت مقصد (گیرنده) 50448 می باشد. پورت گیرنده که در اینجا مربوط به client است به صورت تصادفی انتخاب شده. همینطور checksum برابر 0x6bbe می باشد.

Wireshark packet capture showing a TCP connection. The packet list shows a sequence of packets from source 192.168.65.107 to destination 192.168.65.107. The packet details pane shows the selected packet (No. 133) with source port 80 and destination port 50448. The packet bytes pane shows the raw data of the packet.

کار با فیلتر کننده بسته ها

Wireshark packet capture showing DNS queries. The packet list shows a sequence of DNS queries from source 192.168.65.107 to destination 192.168.65.51. The packet details pane shows the selected packet (No. 1) with source port 62725 and destination port 53. The packet bytes pane shows the raw data of the packet.

سوال 6 ->

پروتکل لایه transport، UDP بوده و ip مقصد 192.168.65.51 است. آدرس 192.168.65.107 هم آدرس مبدا است که سیستم ما می باشد.

سوال 7 ->

آدرس فیزیکی و آدرس مبدا

The image shows a Wireshark packet capture analysis. The main packet list shows a DNS query from 192.168.65.107 to 192.168.65.51. The packet details pane shows the Ethernet II header and the Internet Protocol Version 4 header. The packet bytes pane shows the raw data of the packet. A right-click context menu is open, showing options like 'Follow', 'Export', and 'Copy'. The network interface details pane on the right shows the physical address and other information for the Ethernet adapter.

No.	Time	Source	Destination	Protocol	Length	Info
1	0.000000	192.168.65.107	192.168.65.51	DNS	70	Standard query query
2	0.041539	192.168.65.51	192.168.65.107	DNS	86	Standard query response
3	8.370516	192.168.65.107	192.168.65.51	DNS	91	Standard query query
4	8.441766	192.168.65.51	192.168.65.107	DNS	107	Standard query response
5	10.079712	192.168.65.107	192.168.65.51	DNS	86	Standard query query
6	10.312494	192.168.65.51	192.168.65.107	DNS	163	Standard query response
7	10.315176	192.168.65.107	192.168.65.51	DNS	80	Standard query query
8	10.349422	192.168.65.51	192.168.65.107	DNS	109	Standard query response

Packet 1 details:

- Ethernet II, Src: MS-NLB-PhysServer-32_06:0d:6e:67:61 (02:26:0d:6e:67:61), Dst: 02:26:0d:6e:67:61 (02:26:0d:6e:67:61)
- Internet Protocol Version 4, Src: 192.168.65.107, Dst: 192.168.65.51
- UDP, Src Port: 5555, Dst Port: 53
- DNS Standard query query (id: 0)

Network interface details (Ethernet adapter Ethernet 6):

- Media State: Media disconnected
- Connection-specific DNS Suffix: domain.name
- Description: Realtek PCIe GbE Family Controller
- Physical Address: 70-8B-CD-21-ED-F6
- DHCP Enabled: Yes
- Autoconfiguration Enabled: Yes

سوال 8 ->

Type A، برای مپ کردن host name به ip address

*Ethernet 6 (port 53)

File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help

Apply a display filter ... <Ctrl-F>

No.	Time	Source	Destination	Protocol	Length	Info
1	0.000000	192.168.65.107	192.168.65.51	DNS	70	Standard query 0xdc0c A google.com
2	0.041539	192.168.65.51	192.168.65.107	DNS	86	Standard query response 0xdc0c A google.com A 172.217.21.46
3	8.370516	192.168.65.107	192.168.65.51	DNS	91	Standard query 0x5492 A signaler-pa.clients6.google.com
4	8.441766	192.168.65.51	192.168.65.107	DNS	107	Standard query response 0x5492 A signaler-pa.clients6.google.com A 142.250.181.138
5	10.079712	192.168.65.107	192.168.65.51	DNS	86	Standard query 0x0001 PTR 51.65.168.192.in-addr.arpa
6	10.312494	192.168.65.51	192.168.65.107	DNS	163	Standard query response 0x0001 No such name PTR 51.65.168.192.in-addr.arpa SOA prisoner.iana.org
7	10.315176	192.168.65.107	192.168.65.51	DNS	80	Standard query 0x0002 PTR 1.1.1.1.in-addr.arpa
8	10.349422	192.168.65.51	192.168.65.107	DNS	109	Standard query response 0x0002 PTR 1.1.1.1.in-addr.arpa PTR one.one.one.one

> Frame 3: 91 bytes on wire (728 bits), 91 bytes captured (728 bits) on interface \Device\NPF_{1D03D5FD-E9D7-47A7-8C73-E8C07CB25A28}, id 0

> Ethernet II, Src: MS-NLB-PhysServer-32_06:0d:6e:67:61 (02:26:0d:6e:67:61), Dst: 5a:7a:1b:ef:43:99 (5a:7a:1b:ef:43:99)

> Internet Protocol Version 4, Src: 192.168.65.107, Dst: 192.168.65.51

> User Datagram Protocol, Src Port: 50551, Dst Port: 53

▼ Domain Name System (query)

Transaction ID: 0x5492

Flags: 0x0100 Standard query

Questions: 1

Answer RRs: 0

Authority RRs: 0

Additional RRs: 0

▼ Queries

> signaler-pa.clients6.google.com: type A, class IN

[Response In: 4]

0000 5a 7a 1b ef 43 99 02 26 0d 6e 67 61 08 00 45 00 Zz...C...b...ng...E...
 0010 00 4d 55 a1 00 00 11 e1 0f c0 a8 41 6b c0 a8 .MU.....Ak...
 0020 41 33 c5 77 00 35 00 39 71 5b 54 92 01 00 00 01 A3...5...->.....

Source Hardware Address (eth.src), 6 bytes

Packets: 8 · Displayed: 8 (100.0%) · Dropped: 0 (0.0%)

Profile: Default

48°F Light rain 6:37 PM

سوال 9 -<

تایپ PTR که نام دامنه را باز میگرداند

*Ethernet 6 (port 53)

File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help

Apply a display filter ... <Ctrl-F>

No.	Time	Source	Destination	Protocol	Length	Info
1	0.000000	192.168.65.107	192.168.65.51	DNS	70	Standard query 0xdc0c A google.com
2	0.041539	192.168.65.51	192.168.65.107	DNS	86	Standard query response 0xdc0c A google.com A 172.217.21.46
3	8.370516	192.168.65.107	192.168.65.51	DNS	91	Standard query 0x5492 A signaler-pa.clients6.google.com
4	8.441766	192.168.65.51	192.168.65.107	DNS	107	Standard query response 0x5492 A signaler-pa.clients6.google.com A 142.250.181.138
5	10.079712	192.168.65.107	192.168.65.51	DNS	86	Standard query 0x0001 PTR 51.65.168.192.in-addr.arpa
6	10.312494	192.168.65.51	192.168.65.107	DNS	163	Standard query response 0x0001 No such name PTR 51.65.168.192.in-addr.arpa SOA prisoner.iana.org
7	10.315176	192.168.65.107	192.168.65.51	DNS	80	Standard query 0x0002 PTR 1.1.1.1.in-addr.arpa
8	10.349422	192.168.65.51	192.168.65.107	DNS	109	Standard query response 0x0002 PTR 1.1.1.1.in-addr.arpa PTR one.one.one.one

> Frame 7: 80 bytes on wire (640 bits), 80 bytes captured (640 bits) on interface \Device\NPF_{1D03D5FD-E9D7-47A7-8C73-E8C07CB25A28}, id 0

> Ethernet II, Src: MS-NLB-PhysServer-32_06:0d:6e:67:61 (02:26:0d:6e:67:61), Dst: 5a:7a:1b:ef:43:99 (5a:7a:1b:ef:43:99)

> Internet Protocol Version 4, Src: 192.168.65.107, Dst: 192.168.65.51

> User Datagram Protocol, Src Port: 51228, Dst Port: 53

▼ Domain Name System (query)

Transaction ID: 0x0002

Flags: 0x0100 Standard query

Questions: 1

Answer RRs: 0

Authority RRs: 0

Additional RRs: 0

▼ Queries

> 1.1.1.1.in-addr.arpa: type PTR, class IN

[Response In: 8]

0000 5a 7a 1b ef 43 99 02 26 0d 6e 67 61 08 00 45 00 Zz...C...b...ng...E...
 0010 00 42 55 a3 00 00 11 e1 18 c0 a8 41 6b c0 a8 .BU.....Ak...
 0020 41 33 c8 1c 00 35 00 2e 1a 3e 00 02 01 00 00 01 A3...5...->.....

Source Hardware Address (eth.src), 6 bytes

Packets: 8 · Displayed: 8 (100.0%) · Dropped: 0 (0.0%)

Profile: Default

48°F Light rain 6:40 PM

سوال 10 ->

AAAA, APL, CDS, CERT

سوال 11 ->

مقصد یا مبدا همه آدرس داده شده است و همه پروتکل ICMP دارند.

The screenshot shows a Wireshark packet capture on the 'Ethern6' interface. The filter is 'ip.addr == 5.144.130.115'. The packet list shows several ICMP Echo (ping) requests and responses. Notably, packets 128, 129, 130, 131, and 132 are marked as 'Time-to-live exceeded (Time to live exceeded in transit)'. The packet details for packet 128 are expanded, showing the Ethernet II, Internet Protocol Version 4, and Internet Control Message Protocol (Type: 11) fields. The packet bytes are also visible at the bottom.

سوال 12 ->

تایپ 11 و 64 TTL می باشد.

سوال 13 ->

TTL مدت زمانی است که بسته می تواند بماند و از بین نرود یعنی تا 64 باشد یعنی تا 64 گام می ماند. به نظر بنده TTL گاهی در مراحل افزایش می یابد که بتواند زنده بماند.

سوال 14 ->

تنها اینترنت پروتکل TCP را نشان می دهد.

Ethernet 6

File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help

ip.proto == 6

No.	Time	Source	Destination	Protocol	Length	Info
1511	111.509731	192.168.65.107	107.155.105.90	TCP	54	50448 → 80 [ACK] Seq=1 Ack=4369 Win=4109 Len=0
1515	112.477410	188.40.236.75	192.168.65.107	TLSv1.2	876	Application Data
1516	112.477410	188.40.236.75	192.168.65.107	TLSv1.2	898	Application Data
1517	112.493795	192.168.65.107	188.40.236.75	TLSv1.2	526	Application Data
1518	112.493795	192.168.65.107	188.40.236.75	TLSv1.2	469	Application Data
1519	112.518784	192.168.65.107	188.40.236.75	TCP	54	51682 → 443 [ACK] Seq=7521 Ack=3815 Win=510 Len=0
1520	112.536113	188.40.236.75	192.168.65.107	TCP	54	443 → 51680 [ACK] Seq=7537 Ack=11799 Win=144 Len=0
1521	112.541055	188.40.236.75	192.168.65.107	TCP	54	443 → 51680 [ACK] Seq=7537 Ack=12214 Win=145 Len=0
1529	116.555040	107.155.105.90	192.168.65.107	TCP	95	80 → 50448 [PSH, ACK] Seq=4369 Ack=1 Win=852 Len=41
1530	116.555040	107.155.105.90	192.168.65.107	TCP	95	80 → 50448 [PSH, ACK] Seq=4410 Ack=1 Win=852 Len=41
1531	116.555118	192.168.65.107	107.155.105.90	TCP	54	50448 → 80 [ACK] Seq=1 Ack=4451 Win=4109 Len=0
1541	118.010627	107.155.105.90	192.168.65.107	TCP	95	80 → 50448 [PSH, ACK] Seq=4451 Ack=1 Win=852 Len=41

> Frame 1516: 898 bytes on wire (7184 bits), 898 bytes captured (7184 bits) on interface \Device\NPF_{1D03D5FD-E9D7-47A7-8C73-E8C07CB25A28}, id 0

> Ethernet II, Src: 5a:7a:1b:ef:43:99 (5a:7a:1b:ef:43:99), Dst: MS-NLB-PhysServer-32_06:0d:6e:67:61 (02:26:0d:6e:67:61)

> Internet Protocol Version 4, Src: 188.40.236.75, Dst: 192.168.65.107

> Transmission Control Protocol, Src Port: 443, Dst Port: 51680, Seq: 6693, Ack: 11327, Len: 844

> Transport Layer Security

0000 02 26 0d 6e 67 61 5a 7a 1b ef 43 99 08 00 45 00 :&ngaZz ..C...E:

0010 03 74 5b 2d 40 00 7c 06 f5 ce bc 28 ec 4b c0 a8 :t[-@|: ... (K..

0020 41 6b 01 bb c9 e0 af 4b 14 4f b1 82 20 86 50 18 :Ak....K .0...P.

wireshark, Ethernet 606ZXC1.pcapng

Packets: 8170 · Displayed: 2785 (34.1%)

Profile: Default

45°F Haze 6:56 PM