

به نام خدا

۹۷۲۳۱۰۰	محمد مهدی هجرتی
آشنایی با وایرشارک	آزمایشگاه شبکه - آزمایش سوم
۱۶ فروردین ۱۴۰۰	استاد نقی زاده

سوال ۱

پروتکل های TCP, TLS, DNS, SSL, ARP, QUIC, IGMP, SSDP, RIP دیده می شود.

سوال ۲

به ترتیب پروتکل Ethernet II در لایه ی data link، IPv4 در لایه ی internet، TCP در لایه ی transport، TLS application استفاده شده است.

*Wi-Fi 3

File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help

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

No.	Time	Source	Destination	Protocol	Length	Info
143	8.406985	13.107.21.200	192.168.1.109	TCP	1454	[TCP Out-Of-Order] 443 → 61849
144	8.408685	13.107.21.200	192.168.1.109	TCP	1454	[TCP Out-Of-Order] 443 → 61849
145	8.434329	13.107.21.200	192.168.1.109	TCP	66	443 → 61849 [SYN, ACK] Seq=1401
146	8.434406	192.168.1.109	13.107.21.200	TCP	54	61849 → 443 [ACK] Seq=1 Ack=1401
147	8.434737	192.168.1.109	13.107.21.200	TLSv1.2	520	Client Hello
148	8.536843	13.107.21.200	192.168.1.109	TCP	60	443 → 61849 [ACK] Seq=1 Ack=1401
149	8.547411	13.107.21.200	192.168.1.109	TCP	1454	443 → 61849 [ACK] Seq=1 Ack=1401
150	8.550668	13.107.21.200	192.168.1.109	TCP	1454	443 → 61849 [ACK] Seq=1401 Ack=1401
151	8.550750	192.168.1.109	13.107.21.200	TCP	54	61849 → 443 [ACK] Seq=467 Ack=1401
152	8.551537	13.107.21.200	192.168.1.109	TCP	1454	443 → 61849 [ACK] Seq=2801 Ack=1401

< >

> Frame 147: 520 bytes on wire (4160 bits), 520 bytes captured (4160 bits) on interface \Device\NPF_{19C08828-F8...}

> Ethernet II, Src: LiteonTe_e4:7b:85 (70:c9:4e:e4:7b:85), Dst: Tp-LinkT_68:09:ff (14:cc:20:68:09:ff)

> Internet Protocol Version 4, Src: 192.168.1.109, Dst: 13.107.21.200

> Transmission Control Protocol, Src Port: 61849, Dst Port: 443, Seq: 1, Ack: 1, Len: 466

> Transport Layer Security

< >

```

0000  14 cc 20 68 09 ff 70 c9 4e e4 7b 85 08 00 45 00  ..h.p.N-{-E-
0010  01 fa f8 6b 40 00 80 06 1b 4a c0 a8 01 6d 0d 6b  ...k@...J...m.k
0020  15 c8 f1 99 01 bb 7b ed e0 4c ff 19 8c 51 50 18  ....-{-L...QP-
0030  02 02 85 07 00 00 16 03 03 01 cd 01 00 01 c9 03  ....-{-L...QP-
0040  03 60 6b 2c 7e 97 41 54 d4 e7 1a d2 8a 0b 63 b7  ..`k,~AT .....c-
0050  f1 48 94 96 1c e5 64 b2 39 77 d5 a7 6d b4 fd ad  ..H...d..9w...m...
0060  a4 20 7e 31 00 00 ea 31 34 10 e3 b3 e8 de ad 3e  ..~1...1 4.....>
0070  df 09 71 83 a7 ab 0b 3d cc af c6 5e de 9a f8 b2  ..q....= ...^....

```

Frame (frame), 520 bytes Packets: 18344 · Displayed: 18344 (100.0%) · Dropped: 0 (0.0%) Profile: Default

ترتیب قرارگیری بیت ها، به ترتیب شماره لایه ها می باشد. یعنی ابتدا بیت های مربوط به لایه ی data link قرار گرفته است و پس از آن لایه ی internet، transport و در آخر application قرار گرفته است.

Wi-Fi 3

File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help

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

No.	Time	Source	Destination	Protocol	Length	Info
143	8.406985	13.107.21.200	192.168.1.109	TCP	1454	[TCP Out-Of-Order] 443 → 61
144	8.408685	13.107.21.200	192.168.1.109	TCP	1454	[TCP Out-Of-Order] 443 → 61
145	8.434329	13.107.21.200	192.168.1.109	TCP	66	443 → 61849 [SYN, ACK] Seq=
146	8.434406	192.168.1.109	13.107.21.200	TCP	54	61849 → 443 [ACK] Seq=1 Ack=
147	8.434737	192.168.1.109	13.107.21.200	TLSv1.2	520	Client Hello
148	8.536843	13.107.21.200	192.168.1.109	TCP	60	443 → 61849 [ACK] Seq=1 Ack=
149	8.547411	13.107.21.200	192.168.1.109	TCP	1454	443 → 61849 [ACK] Seq=1 Ack=

> Frame 147: 520 bytes on wire (4160 bits), 520 bytes captured (4160 bits) on interface \Device\NPF_{19C08828-F8...}

> Ethernet II, Src: LiteonTe_e4:7b:85 (70:c9:4e:e4:7b:85), Dst: Tp-LinkT_68:09:ff (14:cc:20:68:09:ff)

> Internet Protocol Version 4, Src: 192.168.1.109, Dst: 13.107.21.200

> Transmission Control Protocol, Src Port: 61849, Dst Port: 443, Seq: 1, Ack: 1, Len: 466

> Transport Layer Security

0000 14 cc 20 68 09 ff 70 c9 4e e4 7b 85 08 00 45 00 .. h..p.. N{...E..

0010 01 fa f8 6b 40 00 80 06 1b 4a c0 a8 01 6d 0d 6b ...k@...J...m.k

0020 15 c8 f1 99 01 bb 7b ed e0 4c ff 19 8c 51 50 18{..L...QP..

0030 02 02 85 07 00 00 16 03 03 01 cd 01 00 01 c9 03
0040 03 60 6b 2c 7e 97 41 54 d4 e7 1a d2 8a 0b 63 b7 ..k,~.ATc..

0050 f1 48 94 96 1c e5 64 b2 39 77 d5 a7 6d b4 fd ad ..H....d..9w...m...>

0060 a4 20 7e 31 00 00 ea 31 34 10 e3 b3 e8 de ad 3e ..~1...1 4.....>

0070 df 09 71 83 a7 ab 0b 3d cc af c6 5e de 9a f8 b2 ..q.....=...^.....

0080 27 e7 00 2a c0 2c c0 2b c0 30 c0 2f 00 9f 00 9e '..*...+..0./.....

0090 c0 24 c0 23 c0 28 c0 27 c0 0a c0 09 c0 14 c0 13 ..\$.#.(.'.....

00a0 00 9d 00 9c 00 3d 00 3c 00 35 00 2f 00 0a 01 00<..5./.....

Ethernet (eth), 14 bytes | Packets: 18344 · Displayed: 18344 (100.0%) · Dropped: 0 (0.0%) | Profile: Default

Wi-Fi 3

File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help

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

No.	Time	Source	Destination	Protocol	Length	Info
143	8.406985	13.107.21.200	192.168.1.109	TCP	1454	[TCP Out-Of-Order] 443 → 61
144	8.408685	13.107.21.200	192.168.1.109	TCP	1454	[TCP Out-Of-Order] 443 → 61
145	8.434329	13.107.21.200	192.168.1.109	TCP	66	443 → 61849 [SYN, ACK] Seq=
146	8.434406	192.168.1.109	13.107.21.200	TCP	54	61849 → 443 [ACK] Seq=1 Ack=
147	8.434737	192.168.1.109	13.107.21.200	TLSv1.2	520	Client Hello
148	8.536843	13.107.21.200	192.168.1.109	TCP	60	443 → 61849 [ACK] Seq=1 Ack=
149	8.547411	13.107.21.200	192.168.1.109	TCP	1454	443 → 61849 [ACK] Seq=1 Ack=

> Frame 147: 520 bytes on wire (4160 bits), 520 bytes captured (4160 bits) on interface \Device\NPF_{19C08828-F8...}

> Ethernet II, Src: LiteonTe_e4:7b:85 (70:c9:4e:e4:7b:85), Dst: Tp-LinkT_68:09:ff (14:cc:20:68:09:ff)

> Internet Protocol Version 4, Src: 192.168.1.109, Dst: 13.107.21.200

> Transmission Control Protocol, Src Port: 61849, Dst Port: 443, Seq: 1, Ack: 1, Len: 466

> Transport Layer Security

0000 14 cc 20 68 09 ff 70 c9 4e e4 7b 85 08 00 45 00 .. h..p.. N{...E..

0010 01 fa f8 6b 40 00 80 06 1b 4a c0 a8 01 6d 0d 6b ...k@...J...m.k

0020 15 c8 f1 99 01 bb 7b ed e0 4c ff 19 8c 51 50 18{..L...QP..

0030 02 02 85 07 00 00 16 03 03 01 cd 01 00 01 c9 03
0040 03 60 6b 2c 7e 97 41 54 d4 e7 1a d2 8a 0b 63 b7 ..k,~.ATc..

0050 f1 48 94 96 1c e5 64 b2 39 77 d5 a7 6d b4 fd ad ..H....d..9w...m...>

0060 a4 20 7e 31 00 00 ea 31 34 10 e3 b3 e8 de ad 3e ..~1...1 4.....>

0070 df 09 71 83 a7 ab 0b 3d cc af c6 5e de 9a f8 b2 ..q.....=...^.....

0080 27 e7 00 2a c0 2c c0 2b c0 30 c0 2f 00 9f 00 9e '..*...+..0./.....

0090 c0 24 c0 23 c0 28 c0 27 c0 0a c0 09 c0 14 c0 13 ..\$.#.(.'.....

00a0 00 9d 00 9c 00 3d 00 3c 00 35 00 2f 00 0a 01 00<..5./.....

Internet Protocol Version 4 (ip), 20 bytes | Packets: 18344 · Displayed: 18344 (100.0%) · Dropped: 0 (0.0%) | Profile: Default

*Wi-Fi 3

File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help

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

No.	Time	Source	Destination	Protocol	Length	Info
143	8.406985	13.107.21.200	192.168.1.109	TCP	1454	[TCP Out-Of-Order] 443 → 61849
144	8.408685	13.107.21.200	192.168.1.109	TCP	1454	[TCP Out-Of-Order] 443 → 61849
145	8.434329	13.107.21.200	192.168.1.109	TCP	66	443 → 61849 [SYN, ACK] Seq=61849
146	8.434406	192.168.1.109	13.107.21.200	TCP	54	61849 → 443 [ACK] Seq=1 Ack=61849
147	8.434737	192.168.1.109	13.107.21.200	TLsv1.2	520	Client Hello
148	8.536843	13.107.21.200	192.168.1.109	TCP	60	443 → 61849 [ACK] Seq=1 Ack=61849
149	8.547411	13.107.21.200	192.168.1.109	TCP	1454	443 → 61849 [ACK] Seq=1 Ack=61849

> Frame 147: 520 bytes on wire (4160 bits), 520 bytes captured (4160 bits) on interface \Device\NPF_{19C08828-F8...}

> Ethernet II, Src: LiteonTe_e4:7b:85 (70:c9:4e:e4:7b:85), Dst: Tp-LinkT_68:09:ff (14:cc:20:68:09:ff)

> Internet Protocol Version 4, Src: 192.168.1.109, Dst: 13.107.21.200

> Transmission Control Protocol, Src Port: 61849, Dst Port: 443, Seq: 1, Ack: 1, Len: 466

> Transport Layer Security

0020 15 c8 f1 99 01 bb 7b ed e0 4c ff 19 8c 51 50 18{..L...QP..

0030 02 02 85 07 00 00 16 03 03 01 cd 01 00 01 c9 03k...AT.....c..

0040 03 60 6b 2c 7e 97 41 54 d4 e7 1a d2 8a 0b 63 b7 ..H...d..9w...m...>

0050 f1 48 94 96 1c e5 64 b2 39 77 d5 a7 6d b4 fd ad ..~1...1 4.....>

0060 a4 20 7e 31 00 00 ea 31 34 10 e3 b3 e8 de ad 3e ..q...=...^.....

0070 df 09 71 83 a7 ab 0b 3d cc af c6 5e de 9a f8 b2 '..*...+..0./.....

0080 27 e7 00 2a c0 2c c0 2b c0 30 c0 2f 00 9f 00 9e ..\$.#.(.'.....

0090 c0 24 c0 23 c0 28 c0 27 c0 0a c0 09 c0 14 c0 13=<..5./.....

00a0 00 9d 00 9c 00 3d 00 3c 00 35 00 2f 00 0a 01 00 ..V.....www.b

00b0 01 56 00 00 11 00 0f 00 00 0c 77 77 77 2e 62 ..ing.com.....

00c0 69 6e 67 2e 63 6f 6d 00 0a 00 08 00 06 00 1d 00 ..

Transmission Control Protocol (tcp), 20 bytes | Packets: 18344 · Displayed: 18344 (100.0%) · Dropped: 0 (0.0%) | Profile: Default

*Wi-Fi 3

File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help

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

No.	Time	Source	Destination	Protocol	Length	Info
143	8.406985	13.107.21.200	192.168.1.109	TCP	1454	[TCP Out-Of-Order] 443 → 61849
144	8.408685	13.107.21.200	192.168.1.109	TCP	1454	[TCP Out-Of-Order] 443 → 61849
145	8.434329	13.107.21.200	192.168.1.109	TCP	66	443 → 61849 [SYN, ACK] Seq=61849
146	8.434406	192.168.1.109	13.107.21.200	TCP	54	61849 → 443 [ACK] Seq=1 Ack=61849
147	8.434737	192.168.1.109	13.107.21.200	TLsv1.2	520	Client Hello
148	8.536843	13.107.21.200	192.168.1.109	TCP	60	443 → 61849 [ACK] Seq=1 Ack=61849
149	8.547411	13.107.21.200	192.168.1.109	TCP	1454	443 → 61849 [ACK] Seq=1 Ack=61849

> Frame 147: 520 bytes on wire (4160 bits), 520 bytes captured (4160 bits) on interface \Device\NPF_{19C08828-F8...}

> Ethernet II, Src: LiteonTe_e4:7b:85 (70:c9:4e:e4:7b:85), Dst: Tp-LinkT_68:09:ff (14:cc:20:68:09:ff)

> Internet Protocol Version 4, Src: 192.168.1.109, Dst: 13.107.21.200

> Transmission Control Protocol, Src Port: 61849, Dst Port: 443, Seq: 1, Ack: 1, Len: 466

> Transport Layer Security

0030 02 02 85 07 00 00 16 03 03 01 cd 01 00 01 c9 03k...AT.....c..

0040 03 60 6b 2c 7e 97 41 54 d4 e7 1a d2 8a 0b 63 b7 ..H...d..9w...m...>

0050 f1 48 94 96 1c e5 64 b2 39 77 d5 a7 6d b4 fd ad ..~1...1 4.....>

0060 a4 20 7e 31 00 00 ea 31 34 10 e3 b3 e8 de ad 3e ..q...=...^.....

0070 df 09 71 83 a7 ab 0b 3d cc af c6 5e de 9a f8 b2 '..*...+..0./.....

0080 27 e7 00 2a c0 2c c0 2b c0 30 c0 2f 00 9f 00 9e ..\$.#.(.'.....

0090 c0 24 c0 23 c0 28 c0 27 c0 0a c0 09 c0 14 c0 13=<..5./.....

00a0 00 9d 00 9c 00 3d 00 3c 00 35 00 2f 00 0a 01 00 ..V.....www.b

00b0 01 56 00 00 11 00 0f 00 00 0c 77 77 77 2e 62 ..ing.com.....

00c0 69 6e 67 2e 63 6f 6d 00 0a 00 08 00 06 00 1d 00 ..

00d0 17 00 18 00 0b 00 02 01 00 00 0d 00 1a 00 18 08 ..

Transport Layer Security (tls), 466 bytes | Packets: 18344 · Displayed: 18344 (100.0%) · Dropped: 0 (0.0%) | Profile: Default

اندازه ی فریم ۵۲۰ بایت و اندازه ی پکت ۵۰۶ بایت است.

*Wi-Fi 3

File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help

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

No.	Time	Source	Destination	Protocol	Length	Info
143	8.406985	13.107.21.200	192.168.1.109	TCP	1454	[TCP Out-Of-Order] 443 → 61849
144	8.408685	13.107.21.200	192.168.1.109	TCP	1454	[TCP Out-Of-Order] 443 → 61849
145	8.434329	13.107.21.200	192.168.1.109	TCP	66	443 → 61849 [SYN, ACK] Seq=1
146	8.434406	192.168.1.109	13.107.21.200	TCP	54	61849 → 443 [ACK] Seq=1 Ack=
147	8.434737	192.168.1.109	13.107.21.200	TLSv1.2	520	Client Hello
148	8.536843	13.107.21.200	192.168.1.109	TCP	60	443 → 61849 [ACK] Seq=1 Ack=
149	8.547411	13.107.21.200	192.168.1.109	TCP	1454	443 → 61849 [ACK] Seq=1 Ack=

> Frame 147: 520 bytes on wire (4160 bits), 520 bytes captured (4160 bits) on interface \Device\NPF_{19C08828-...}

> Ethernet II, Src: LiteonTe_e4:7b:85 (70:c9:4e:e4:7b:85), Dst: Tp-LinkT_68:09:ff (14:cc:20:68:09:ff)

Internet Protocol Version 4, Src: 192.168.1.109, Dst: 13.107.21.200

- 0100 = Version: 4
- 0101 = Header Length: 20 bytes (5)
- > Differentiated Services Field: 0x00 (DSCP: CS0, ECN: Not-ECT)
- Total Length: 506
- Identification: 0xf86b (63595)
- > Flags: 0x40, Don't fragment
- Fragment Offset: 0

0010 01 fa f8 6b 40 00 80 06 1b 4a c0 a8 01 6d 0d 6b ..k@... .J...m.k

0020 15 c8 f1 99 01 bb 7b ed e0 4c ff 19 8c 51 50 18{. .L...QP.

0030 02 02 85 07 00 00 16 03 03 01 cd 01 00 01 c9 03

0040 03 60 6b 2c 7e 97 41 54 d4 e7 1a d2 8a 0b 63 b7 .`k,~.ATC.

0050 f1 48 94 96 1c e5 64 b2 39 77 d5 a7 6d b4 fd ad .H....d. 9w..m...

0060 a4 20 7e 31 00 00 ea 31 34 10 e3 b3 e8 de ad 3e . ~1...1 4.....>

Total Length (ip.len), 2 bytes | Packets: 18344 · Displayed: 18344 (100.0%) · Dropped: 0 (0.0%) | Profile: Default

سوال ۳

این بسته از پروتکل ARP استفاده می کند.

*Wi-Fi 3

File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help

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

No.	Time	Source	Destination	Protocol	Length	Info
38	7.477666	13.107.21.200	192.168.1.109	TCP	60	443 → 61848 [ACK] Seq=5149
39	7.477666	13.107.21.200	192.168.1.109	TLSv1.2	380	New Session Ticket, Change
40	7.479770	192.168.1.109	13.107.21.200	TLSv1.2	145	Application Data
41	7.486603	de:cc:3f:1b:fb:09	Broadcast	ARP	42	Who has 192.168.1.1? Tell 1
42	7.639283	13.107.21.200	192.168.1.109	TCP	60	443 → 61848 [ACK] Seq=5475
43	7.761676	13.107.21.200	192.168.1.109	TCP	1454	[TCP Previous segment not c
44	7.761729	192.168.1.109	13.107.21.200	TCP	66	[TCP Dup ACK 40#1] 61848 →
45	7.761806	13.107.21.200	192.168.1.109	TCP	407	443 → 61848 [PSH, ACK] Seq=
46	7.761824	192.168.1.109	13.107.21.200	TCP	66	[TCP Dup ACK 40#2] 61848 →

> Frame 41: 42 bytes on wire (336 bits), 42 bytes captured (336 bits) on interface \Device\NPF_{19C08828-F853-49}

> Ethernet II, Src: de:cc:3f:1b:fb:09 (de:cc:3f:1b:fb:09), Dst: Broadcast (ff:ff:ff:ff:ff:ff)

> Address Resolution Protocol (request)

```

0000  ff ff ff ff ff ff de cc 3f 1b fb 09 08 06 00 01  ..... ?.....
0010  08 00 06 04 00 01 de cc 3f 1b fb 09 c0 a8 01 69  ..... ?.....i
0020  00 00 00 00 00 00 c0 a8 01 01  ..... ..
  
```

wireshark_Wi-Fi 33ITY00.pcapng | Packets: 18344 · Displayed: 18344 (100.0%) · Dropped: 0 (0.0%) | Profile: Default

سوال ۴

نمایش هگز checksum این پکت به صورت d02d می باشد که به معنای validation disabled است.

The image shows a Wireshark packet capture window titled '*Wi-Fi 3'. The packet list pane shows several packets, with packet 149 selected. The packet details pane shows the structure of the selected packet, and the packet bytes pane shows the raw data in hexadecimal and ASCII.

Packet List:

No.	Time	Source	Destination	Protocol	Length	Info
147	8.434737	192.168.1.109	13.107.21.200	TLSv1.2	520	Client Hello
148	8.536843	13.107.21.200	192.168.1.109	TCP	60	443 → 61849 [ACK] Seq=1 Ack=...
149	8.547411	13.107.21.200	192.168.1.109	TCP	1454	443 → 61849 [ACK] Seq=1 Ack=...
150	8.550668	13.107.21.200	192.168.1.109	TCP	1454	443 → 61849 [ACK] Seq=1401 Ack=...
151	8.550750	192.168.1.109	13.107.21.200	TCP	54	61849 → 443 [ACK] Seq=467 Ack=...

Packet Details:

- Differentiated Services Field: 0x00 (DSCP: CS0, ECN: Not-ECT)
 - Total Length: 1440
 - Identification: 0x55e2 (21986)
- Flags: 0x40, Don't fragment
 - Fragment Offset: 0
 - Time to Live: 106
 - Protocol: TCP (6)
 - Header Checksum: 0xd02d [validation disabled]
 - [Header checksum status: Unverified]
 - Source Address: 13.107.21.200
 - Destination Address: 192.168.1.109
- Transmission Control Protocol, Src Port: 443, Dst Port: 61849, Seq: 1, Ack: 467, Len: 1400

Packet Bytes:

Offset	Hex	ASCII
0010	05 a0 55 e2 40 00 6a 06 d0 2d 0d 6b 15 c8 c0 a8	..U.@.j. .k...
0020	01 6d 01 bb f1 99 ff 19 8c 51 7b ed e2 1e 50 10	.m.....-Q{...P.
0030	08 00 71 e9 00 00 16 03 03 14 17 02 00 00 55 03	..q.....U.
0040	03 60 6b 2c 7f 65 d4 ea 52 39 a3 ee 3f a2 d6 7a	..k,.e..R9..?..z
0050	7b e7 09 cd 5d 79 c2 ae 5e f1 9d 73 5c 8d c0 c5	{...}y..^..s\...
0060	20 20 0b 4c 00 00 1d 27 c8 f8 6b da f4 38 69 57	.L... ' ..k..8iW

Header Checksum: (ip.checksum), 2 bytes

Statistics: Packets: 18344 · Displayed: 18344 (100.0%) · Dropped: 0 (0.0%) Profile: Default

سوال ۵

این بسته از پروتکل TCP استفاده می کند.

پورت مبدا آن ۴۴۳ و مقصد ۶۱۸۵۰ می باشد.

عدد پورت، اپلیکیشنی را در سیستم مبدا یا مقصد مشخص می کند که قرار است با آن ارتباط برقرار شود و پکت ها مربوط به آن هستند.

نمایش هگز checksum پروتکل TCP این پک به صورت 4920 می باشد که unverified است.

The image shows a Wireshark packet capture window titled '*Wi-Fi 3'. The packet list on the left shows three packets. The selected packet (No. 336) is a TCP segment from 79.175.170.215 to 192.168.1.109, Seq=11529, Len=1454. The packet details pane shows the following information:

- Transmission Control Protocol, Src Port: 443, Dst Port: 61850, Seq: 12929, Ack: 1413, Len: 903
- Source Port: 443
- Destination Port: 61850
- [Stream index: 12]
- [TCP Segment Len: 903]
- Sequence Number: 12929 (relative sequence number)
- Sequence Number (raw): 4109391494
- [Next Sequence Number: 13832 (relative sequence number)]
- Acknowledgment Number: 1413 (relative ack number)
- Acknowledgment number (raw): 3018213415
- 0101 = Header Length: 20 bytes (5)
- > Flags: 0x018 (PSH, ACK)
- Window: 249
- [Calculated window size: 31872]
- [Window size scaling factor: 128]
- Checksum: 0x4920 [unverified]

The packet bytes pane shows the raw data in hexadecimal and ASCII. The ASCII part shows the text 'I...m 2...'. The packet summary at the bottom indicates the frame is 957 bytes and the reassembled TCP segment is 10703 bytes. The status bar shows 18344 packets displayed, 0 dropped, and the profile is Default.

سوال ۶

پروتکل لایه ی Transport در این پکت، UDP می باشد.

آدرس آی پی مبدا 192.168.1.109 است.

آدرس آی پی مقصد 192.168.1.1 است.

آدرس آی پی ورژن ۶ مبدا 70:c9:4e:7b:85 و مقصد 14:cc:68:09:ff است.

*Wi-Fi 3 (port 53)

File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help

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

No.	Time	Source	Destination	Proto	Length	Info
1	0.000000	192.168.1.109	192.168.1.1	DNS	70	Standard query 0x0951 A google.com
2	0.052118	192.168.1.1	192.168.1.109	DNS	86	Standard query response 0x0951 A google.com A 216.58.21
3	7.666344	192.168.1.109	192.168.1.1	DNS	84	Standard query 0x0001 PTR 1.1.168.192.in-addr.arpa
4	7.722172	192.168.1.1	192.168.1.109	DNS	143	Standard query response 0x0001 No such name PTR 1.1.168
5	7.727947	192.168.1.109	192.168.1.1	DNS	80	Standard query 0x0002 PTR 1.1.1.1.in-addr.arpa
6	7.779306	192.168.1.1	192.168.1.109	DNS	109	Standard query response 0x0002 PTR 1.1.1.1.in-addr.arpa

< >

> Frame 1: 70 bytes on wire (560 bits), 70 bytes captured (560 bits) on interface \Device\NPF_{19C08828-F853-49C}

> Ethernet II, Src: LiteonTe_e4:7b:85 (70:c9:4e:e4:7b:85), Dst: Tp-LinkT_68:09:ff (14:cc:20:68:09:ff)

> Internet Protocol Version 4, Src: 192.168.1.109, Dst: 192.168.1.1

> User Datagram Protocol, Src Port: 63602, Dst Port: 53

> Domain Name System (query)

< >

0000	14 cc 20 68 09 ff 70 c9 4e e4 7b 85 08 00 45 00	.. h..p. N..{...E..
0010	00 38 8e bf 00 00 80 11 28 37 c0 a8 01 6d c0 a8	..8.....(7...m..
0020	01 01 f8 72 00 35 00 24 66 35 09 51 01 00 00 01	...r.5.\$ f5.Q....
0030	00 00 00 00 00 00 06 67 6f 6f 67 6c 65 03 63 6fg oogle.co

Ethernet (eth), 14 bytes

Packets: 6 • Displayed: 6 (100.0%) • Dropped: 0 (0.0%) Profile: Default

سوال ۷

آدرس آی پی اینترفیس انتخاب شده برای کپیچر کردن پکت (وای فای ۳) همان آدرس مبدا در سوال قبل می باشد.

```
Command Prompt
DHCPv6 Client DUID. . . . . : 00-01-00-01-24-56-4F-21-8C-16-45-4F-E3-55
DNS Servers . . . . . : fec0:0:0:ffff::1%1
                        fec0:0:0:ffff::2%1
                        fec0:0:0:ffff::3%1
NetBIOS over Tcpip. . . . . : Enabled

Wireless LAN adapter Wi-Fi 3:

    Connection-specific DNS Suffix  . : 
    Description . . . . . : Qualcomm Atheros QCA9377 Wireless Network
Adapter #3
    Physical Address. . . . . : 70-C9-4E-E4-7B-85
    DHCP Enabled. . . . . : Yes
    Autoconfiguration Enabled . . . . : Yes
    Link-local IPv6 Address . . . . . : fe80::1898:a501:b7aa:ef45%4(Preferred)
    IPv4 Address. . . . . : 192.168.1.109(Preferred)
    Subnet Mask . . . . . : 255.255.255.0
    Lease Obtained. . . . . : Monday, 5 April, 2021 20:41:56
    Lease Expires . . . . . : Thursday, 8 April, 2021 22:20:39
    Default Gateway . . . . . : 192.168.1.1
    DHCP Server . . . . . : 192.168.1.1
    DHCPv6 IAID . . . . . : 108054862
    DHCPv6 Client DUID. . . . . : 00-01-00-01-24-56-4F-21-8C-16-45-4F-E3-55

    DNS Servers . . . . . : 192.168.1.1
    NetBIOS over Tcpip. . . . . : Enabled
```

سوال ۸

رکورد از نوع A زده شده است.

بدین معنا که آدرس آی پی ورژن ۴ سایت گوگل با DNS خواسته شده است.

The image shows a Wireshark packet capture window titled '*Wi-Fi 3 (port 53)'. The packet list shows four packets: a DNS standard query (No. 1), a DNS standard query response (No. 2), a DNS standard query (No. 3), and a DNS standard query response (No. 4). The selected packet is No. 2, a DNS standard query response from 192.168.1.1 to 192.168.1.109. The packet details pane shows the domain name system response with transaction ID 0x0951, flags 0x8180, and one query for google.com. The packet bytes pane shows the raw data of the response, including the domain name and the IP address 216.146.132.100.

Wireshark packet capture window showing a DNS query and response. The selected packet is a DNS standard query response (No. 2) from 192.168.1.1 to 192.168.1.109. The packet details pane shows the domain name system response with transaction ID 0x0951, flags 0x8180, and one query for google.com. The packet bytes pane shows the raw data of the response, including the domain name and the IP address 216.146.132.100.

No.	Time	Source	Destination	Proto	Length	Info
1	0.000000	192.168.1.109	192.168.1.1	DNS	70	Standard query 0x0951 A google.com
2	0.052118	192.168.1.1	192.168.1.109	DNS	86	Standard query response 0x0951 A google.com A 216
3	7.666344	192.168.1.109	192.168.1.1	DNS	84	Standard query 0x0001 PTR 1.1.168.192.in-addr.arp
4	7.722172	192.168.1.1	192.168.1.109	DNS	143	Standard query response 0x0001 No such name PTR 1

Domain Name System (response)

Transaction ID: 0x0951

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

0030 00 01 00 00 00 00 06 67 6f 6f 67 6c 65 03 63 6fg oogle.co

0040 6d 00 00 01 00 01 c0 0c 00 01 00 01 00 00 00 70 m.....p

0050 00 04 d8 3a d2 4e ...:N

Text item (text), 16 bytes

Packets: 6 · Displayed: 6 (100.0%) · Dropped: 0 (0.0%) Profile: Default

سوال ۹

رکورد از نوع PTR یا pointer زده شده است.

بدین معنا که با وارد کردن آدرس آی پی، می‌خواهیم اسم دامنه ی سایت مورد نظر را بدست بیاوریم.

The image shows a Wireshark packet capture window titled '*Wi-Fi 3 (port 53)'. The packet list shows four packets:

No.	Time	Source	Destination	Proto	Length	Info
1	0.000000	192.168.1.109	192.168.1.1	DNS	70	Standard query 0x0951 A google.com
2	0.052118	192.168.1.1	192.168.1.109	DNS	86	Standard query response 0x0951 A google.com A 216
3	7.666344	192.168.1.109	192.168.1.1	DNS	84	Standard query 0x0001 PTR 1.1.168.192.in-addr.arpa
4	7.722172	192.168.1.1	192.168.1.109	DNS	143	Standard query response 0x0001 No such name PTR 1

The packet details pane for packet 3 shows:

- Domain Name System (query)
 - Transaction ID: 0x0001
 - Flags: 0x0100 Standard query
 - Questions: 1
 - Answer RRs: 0
 - Authority RRs: 0
 - Additional RRs: 0
 - Queries
 - 1.1.168.192.in-addr.arpa: type PTR, class IN
 - Name: 1.1.168.192.in-addr.arpa
 - [Name Length: 24]
 - [Label Count: 6]
 - Type: PTR (domain name PoinTeR) (12)
 - Class: IN (0x0001)

The packet bytes pane shows the raw data for packet 3:

```

0030  00 00 00 00 00 00 01 31 01 31 03 31 36 38 03 31  .....1.1.168.1
0040  39 32 07 69 6e 2d 61 64 64 72 04 61 72 70 61 00  92.in-addr.arpa.
0050  00 0c 00 01  ....
  
```

The status bar at the bottom indicates: Text item (text), 30 bytes | Packets: 6 · Displayed: 6 (100.0%) · Dropped: 0 (0.0%) | Profile: Default

سوال ۱۰

AAAA: مشابه رکورد A می باشد با این تفاوت که آی پی ورژن ۶ درخواست شده است.

NS: آدرس DNS server معتبر برای این دامنه را ثبت می کند.

MX: برای هدایت ایمیل ها به سمت سرور ایمیل استفاده می شود.

سوال ۱۱

بسته های نمایش داده شده تماما از پروتکل ICMP می باشد.

*Wi-Fi 3

File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help

ip.addr == 5.144.130.115

No.	Time	Source	Destination	Proto	Length	Info
67	34.770150	192.168.1.109	5.144.130.115	ICMP	106	Echo (ping) request id=0x0001, seq=19/4864, ttl=1
68	34.772144	192.168.1.1	192.168.1.109	ICMP	70	Time-to-live exceeded (Time to live exceeded in tr
69	34.773147	192.168.1.109	5.144.130.115	ICMP	106	Echo (ping) request id=0x0001, seq=20/5120, ttl=1
70	34.775876	192.168.1.1	192.168.1.109	ICMP	70	Time-to-live exceeded (Time to live exceeded in tr
71	34.778806	192.168.1.109	5.144.130.115	ICMP	106	Echo (ping) request id=0x0001, seq=21/5376, ttl=1
72	34.780628	192.168.1.1	192.168.1.109	ICMP	70	Time-to-live exceeded (Time to live exceeded in tr
144	40.388452	192.168.1.109	5.144.130.115	ICMP	106	Echo (ping) request id=0x0001, seq=22/5632, ttl=2
145	40.428391	172.20.2.50	192.168.1.109	ICMP	70	Time-to-live exceeded (Time to live exceeded in tr
146	40.431659	192.168.1.109	5.144.130.115	ICMP	106	Echo (ping) request id=0x0001, seq=23/5888, ttl=2
147	40.471040	172.20.2.50	192.168.1.109	ICMP	70	Time-to-live exceeded (Time to live exceeded in tr
148	40.473145	192.168.1.109	5.144.130.115	ICMP	106	Echo (ping) request id=0x0001, seq=24/6144, ttl=2
149	40.512406	172.20.2.50	192.168.1.109	ICMP	70	Time-to-live exceeded (Time to live exceeded in tr
168	46.038517	192.168.1.109	5.144.130.115	ICMP	106	Echo (ping) request id=0x0001, seq=25/6400, ttl=3
169	46.186626	172.16.32.217	192.168.1.109	ICMP	70	Time-to-live exceeded (Time to live exceeded in tr
170	46.190016	192.168.1.109	5.144.130.115	ICMP	106	Echo (ping) request id=0x0001, seq=26/6656, ttl=3
171	46.239082	172.16.32.217	192.168.1.109	ICMP	70	Time-to-live exceeded (Time to live exceeded in tr
172	46.242342	192.168.1.109	5.144.130.115	ICMP	106	Echo (ping) request id=0x0001, seq=27/6912, ttl=3

> Frame 67: 106 bytes on wire (848 bits), 106 bytes captured (848 bits) on interface \Device\NPF_{19C08828-F853-...}

> Ethernet II, Src: LiteonTe_e4:7b:85 (70:c9:4e:e4:7b:85), Dst: Tp-LinkT_68:09:ff (14:cc:20:68:09:ff)

> Internet Protocol Version 4, Src: 192.168.1.109, Dst: 5.144.130.115

> Internet Control Message Protocol

0000 14 cc 20 68 09 ff 70 c9 4e e4 7b 85 08 00 45 00 .. h..p. N-{...E.

0010 00 5c b6 85 00 00 01 01 b9 03 c0 a8 01 6d 05 90 ..\.....m..

Source or Destination Address: IPv4 address | Packets: 732 · Displayed: 59 (8.1%) | Profile: Default

سوال ۱۲

عدد type برابر ۸ می باشد به معنای ping request

مقدار عدد time to live برابر ۱ می باشد.

Wi-Fi 3

File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help

ip.addr == 5.144.130.115

No.	Time	Source	Destination	Proto	Length	Info
67	34.770150	192.168.1.109	5.144.130.115	ICMP	106	Echo (ping) request id=0x0001, seq=19/4864, ttl=1
68	34.772144	192.168.1.1	192.168.1.109	ICMP	70	Time-to-live exceeded (Time to live exceeded in tr
69	34.773147	192.168.1.109	5.144.130.115	ICMP	106	Echo (ping) request id=0x0001, seq=20/5120, ttl=1
70	34.775876	192.168.1.1	192.168.1.109	ICMP	70	Time-to-live exceeded (Time to live exceeded in tr
71	34.778806	192.168.1.109	5.144.130.115	ICMP	106	Echo (ping) request id=0x0001, seq=21/5376, ttl=1

Flags: 0x00
Fragment Offset: 0

Time to Live: 1

[Expert Info (Note/Sequence): "Time To Live" only 1]
["Time To Live" only 1]
[Severity level: Note]
[Group: Sequence]

Protocol: ICMP (1)
Header Checksum: 0xb903 [validation disabled]
[Header checksum status: Unverified]
Source Address: 192.168.1.109
Destination Address: 5.144.130.115

Internet Control Message Protocol

Type: 8 (Echo (ping) request)
Code: 0
Checksum: 0xf7eb [correct]

0010 00 5c b6 85 00 00 01 01 b9 03 c0 a8 01 6d 05 90 .\....-.....m..
0020 82 73 08 00 f7 eb 00 01 00 13 00 00 00 00 00 00 .S.....

Time to Live (ip.ttl), 1 byte

Packets: 1041 · Displayed: 59 (5.7%)

Profile: Default

سوال ۱۳

مقدار عدد ttl برای بسته های ارسالی از ۱ تا ۱۱ افزایش یافته است.

از طرفی با توجه به بررسی tracertr میبینیم که ۱۱ گره در مسیر تا مقصد وجود دارد.

به نظر می رسد فرستنده ی پکت ها با توجه به فاصله ی مبدا تا گره ها، ttl را تنظیم می کند تا هر چه دروتر می شود، پکت برای زمان بیشتری زنده بماند.

۶ == ip.proto های با پروتکل tcp را فیلتر می کند.

*Wi-Fi 3

File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help

ip.proto == 6

No.	Time	Source	Destination	Protocol	Length	Info
1	0.000000	192.168.1.109	23.35.236.137	TCP	55	56260 → 443 [ACK] Seq=1 Ack=1 Win=512 Len=
2	0.222620	23.35.236.137	192.168.1.109	TCP	66	443 → 56260 [ACK] Seq=1 Ack=2 Win=501 Len=
3	2.218485	192.168.1.109	108.177.15.188	TCP	55	[TCP segment of a reassembled PDU]
4	2.485627	108.177.15.188	192.168.1.109	TCP	66	5228 → 56230 [ACK] Seq=1 Ack=2 Win=265 Len=
5	12.442285	192.168.1.109	52.218.31.16	TCP	55	56270 → 443 [ACK] Seq=1 Ack=1 Win=513 Len=
6	12.601649	52.218.31.16	192.168.1.109	TCP	60	443 → 56270 [RST, ACK] Seq=1 Ack=1 Win=0 Len=
10	16.513241	192.168.1.109	20.44.232.74	TCP	1454	56271 → 443 [ACK] Seq=1 Ack=1 Win=512 Len=
11	16.513241	192.168.1.109	20.44.232.74	TLSv1.2	202	Application Data
12	16.515679	192.168.1.109	20.44.232.74	TCP	1454	56271 → 443 [ACK] Seq=1549 Ack=1 Win=512 Len=
13	16.515679	192.168.1.109	20.44.232.74	TLSv1.2	410	Application Data
14	16.849918	20.44.232.74	192.168.1.109	TCP	60	443 → 56271 [ACK] Seq=1 Ack=1549 Win=2050
15	16.878282	20.44.232.74	192.168.1.109	TCP	60	443 → 56271 [ACK] Seq=1 Ack=3305 Win=2050
16	16.883376	20.44.232.74	192.168.1.109	TCP	1454	443 → 56271 [ACK] Seq=1 Ack=3305 Win=2050
17	16.884406	20.44.232.74	192.168.1.109	TLSv1.2	958	Application Data
18	16.884505	192.168.1.109	20.44.232.74	TCP	54	56271 → 443 [ACK] Seq=3305 Ack=2305 Win=51
19	16.897154	192.168.1.109	20.44.232.74	TCP	1454	56271 → 443 [ACK] Seq=3305 Ack=2305 Win=51

> Frame 143: 810 bytes on wire (6480 bits), 810 bytes captured (6480 bits) on interface \Device\NPF_{19C08828-...}

> Ethernet II, Src: LiteonTe_e4:7b:85 (70:c9:4e:e4:7b:85), Dst: Tp-LinkT_68:09:ff (14:cc:20:68:09:ff)

<

0010	03 1c 6d 0f 40 00 80 06 4a 1a c0 a8 01 6d 34 72	..m.@... J...4r
0020	4a 2b db d1 01 bb c4 af 22 d2 54 39 9b 0f 50 18	J+.....".T9..P.
0030	03 fd 33 91 00 00 bb 94 60 f1 1e b4 e8 48 4a a4	..3.....`...HJ.
0040	dd 47 3c 51 63 b3 10 11 3d e9 53 63 99 07 a0 0c	.G<Qc... =.Sc...

Frame (810 bytes) Reassembled TCP (2156 bytes)

Source Address (ip.src), 4 bytes

Packets: 1398 · Displayed: 900 (64.4%) · Dropped: 0 (0.0%) Profile: Default