به نام خدا

آشنایی با نرم افزار WIRESHARK

فصل یک، آزمایش سه

محمد جواد زندیه ۹۸۳۱۰۳۲

۳ مهر ۱۴۰۱

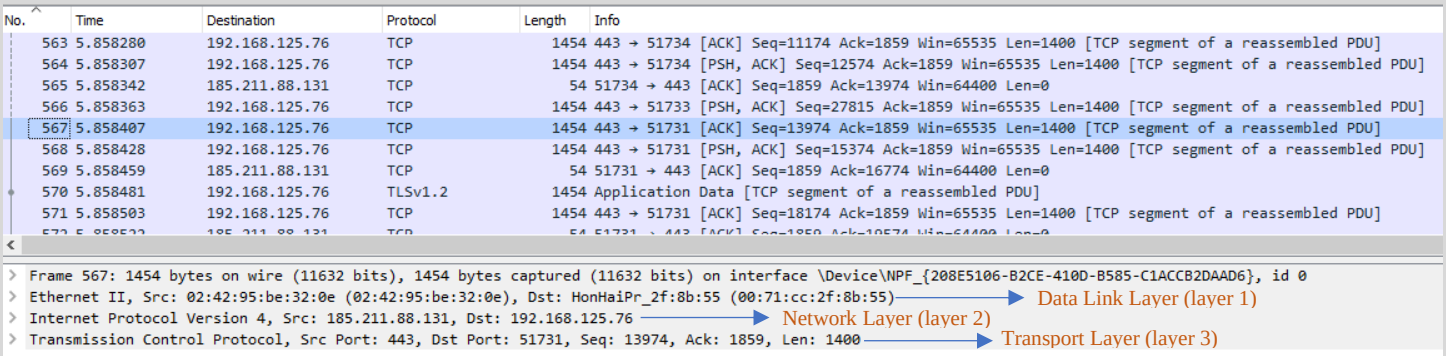
دانشگاه صنعتی امیرکبیر، دانشکده مهندسی کامپیوتر، آزمایشگاه شبکه های کامپیوتری

سوال ۱: به یک بخش دلخواه از بسته های شنود شده مراجعه کنید. چه پروتکل هایی را مشاهده می کنید. لیست آن ها را یادداشت کنید.

UDP, TLSv1.3, TLSv1.2, TCP, SSDP, QUIC, MDNS, LLMNR, IGMPv2, ICMPv6, ICMP, HTTP, DNS, DHCPv6, ARP

سوال ۲: یک بسته را به دلخواه انتخاب کنید. مشخص کنید که چه پروتکل هایی در لایه های مختلف آن استفاده شده است. ترتیب قرارگیری بیت ها داخل بسته چه ارتباطی با لایه های مختلف دارد؟ اندازه فریم لایه دو این بسته چقدر است؟ اندازه بسته لایه سه چقدر است؟

بسته شماره ۵۶۷ در این capture را برای پاسخ به این سوال بررسی می کنیم(این بسته از پروتکل TCP که دارای ۳ لایه است استفاده می کند).



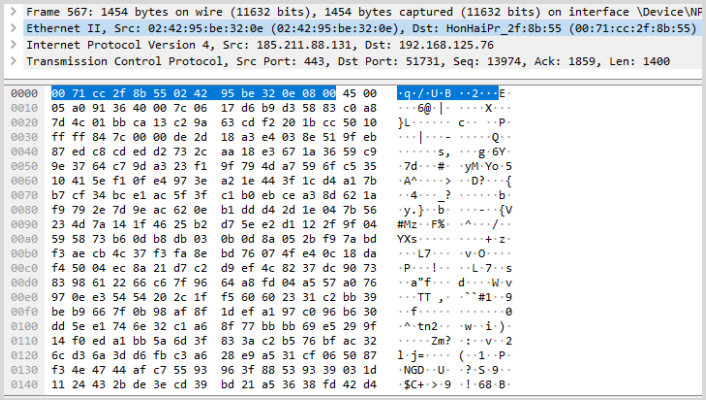
شکل (۱) بسته شماره ۵۶۷ به همراه اسم و شماره لایه ها[1]

پروتکل لایه های مختلف:

لایه اول(Data Link Layer): Ethernet II لایه دوم(Network Layer): IP version 4 لایه سوم(Transport Layer): TCP

بررسی ارتباط بین ترتیب قرار گیری بیت ها با لایه های مختلف:

اگر روی هر یک از لایه ها در نرم افزار Wireshark کلیک کنیم، بیت های مربوط به آن لایه در بسته را با رنگ آبی highlight می کند. با انجام این کار متوجه می شویم که ابتدا بیت های مربوط به لایه اول، سپس بیت های مربوط به لایه دوم و در آخر بیت های مربوط به لایه سوم در بسته قرار گرفته اند. یعنی بیت های لایه های بالاتر، در آدرس های پایین تر در بسته قرار دارند(توجه به نمایش Hex بسته). در شکل های زیر این موضوع را نمایش داده ایم:



شکل (۲) بیت های مربوط به لایه اول (Ethernet II)

[1] Wireshark packet layers

```
> Frame 567: 1454 bytes on wire (11632 bits), 1454 bytes captured (11632 bits) on interface \Device\NF
> Ethernet II, Src: 02:42:95:be:32:0e (02:42:95:be:32:0e), Dst: HonHaiPr_2f:8b:55 (00:71:cc:2f:8b:55)
> Internet Protocol Version 4, Src: 185.211.88.131, Dst: 192.168.125.76
> Transmission Control Protocol, Src Port: 443, Dst Port: 51731, Seq: 13974, Ack: 1859, Len: 1400

0000  00 71 cc 2f 8b 55 02 42  95 be 32 0e 08 00 45 00   ·q·/·U·B ··2···E·
0010  05 a0 91 36 40 00 7c 06  17 d6 b9 d3 58 83 c0 a8   ···6@·|· ····X···
0020  7d 4c 01 bb ca 13 c2 9a  63 cd f2 20 1b cc 50 10   }L······ c··· ··P·
0030  ff ff 84 7c 00 00 de 2d  18 a3 e4 03 8e 51 9f eb   ···|···- ·····Q··
0040  87 ed c8 cd ed d2 73 2c  aa 18 e3 67 1a 36 59 c9   ····· ·· ···g·6Y·
0050  9e 37 64 c7 9d a3 23 f1  9f 79 4d a7 59 6f c5 35   ·7d···#· ·yM·Yo·5
0060  10 41 5e f1 0f e4 97 3e  a2 1e 44 3f 1c d4 a1 7b   ·A^····> ··D?···{
0070  b7 cf 34 bc e1 ac 5f 3f  c1 b0 eb ce a3 8d 62 1a   ··4···_? ·····b·
0080  f9 79 2e 7d 9e ac 62 0e  b1 dd d4 2d 1e 04 7b 56   ·y.}··b· ···-··{V
0090  23 4d 7a 14 1f 46 25 b2  d7 5e e2 d1 12 2f 9f 04   #Mz··F%· ·^···/··
00a0  59 58 73 b6 0d b8 db 03  0b 0d 8a 05 2b f9 7a bd   YXs····· ····+·z·
00b0  f3 ae cb 4c 37 f3 fa 8e  bd 76 07 4f e4 0c 18 da   ···L7··· ·v·O····
00c0  f4 50 04 ec 8a 21 d7 c2  d9 ef 4c 82 37 dc 90 73   ·P···!·· ··L·7··s
00d0  83 98 61 22 66 c6 7f 96  64 a8 fd 04 a5 57 a0 76   ··a"f··· d····W·v
00e0  97 0e e3 54 54 20 2c 1f  f5 60 60 23 31 c2 bb 39   ···TT ,· ·``#1··9
00f0  be b9 66 7f 0b 98 af 8f  1d ef a1 97 c0 96 b6 30   ··f····· ·******0
0100  dd 5e e1 74 6e 32 c1 a6  8f 77 bb bb 69 e5 29 9f   ·^·tn2·· ·w··i·)·
0110  14 f0 ed a1 bb 5a 6d 3f  83 3a c2 b5 76 bf ac 32   ····· Zm? ·:··v··2
0120  6c d3 6a 3d d6 fb c3 a6  28 e9 a5 31 cf 06 50 87   l·j=···· (··1··P·
0130  f3 4e 47 44 af c7 55 93  96 3f 88 53 93 39 03 1d   ·NGD··U· ·?·S·9··
0140  11 24 43 2b de 3e cd 39  bd 21 a5 36 38 fd 42 d4   ·$C+·>·9 ·!·68·B·
```

شکل (۳) بیت های مربوط به لایه دوم (IP version 4)

```
> Frame 567: 1454 bytes on wire (11632 bits), 1454 bytes captured (11632 bits) on interface \Device\N
> Ethernet II, Src: 02:42:95:be:32:0e (02:42:95:be:32:0e), Dst: HonHaiPr_2f:8b:55 (00:71:cc:2f:8b:55)
> Internet Protocol Version 4, Src: 185.211.88.131, Dst: 192.168.125.76
> Transmission Control Protocol, Src Port: 443, Dst Port: 51731, Seq: 13974, Ack: 1859, Len: 1400

0000  00 71 cc 2f 8b 55 02 42  95 be 32 0e 08 00 45 00   ·q·/·U·B ··2···E·
0010  05 a0 91 36 40 00 7c 06  17 d6 b9 d3 58 83 c0 a8   ···6@·|· ····X···
0020  7d 4c 01 bb ca 13 c2 9a  63 cd f2 20 1b cc 50 10   }L······ c··· ··P·
0030  ff ff 84 7c 00 00 de 2d  18 a3 e4 03 8e 51 9f eb   ···|···- ·····Q··
0040  87 ed c8 cd ed d2 73 2c  aa 18 e3 67 1a 36 59 c9   ····· ·· ···g·6Y·
0050  9e 37 64 c7 9d a3 23 f1  9f 79 4d a7 59 6f c5 35   ·7d···#· ·yM·Yo·5
0060  10 41 5e f1 0f e4 97 3e  a2 1e 44 3f 1c d4 a1 7b   ·A^····> ··D?···{
0070  b7 cf 34 bc e1 ac 5f 3f  c1 b0 eb ce a3 8d 62 1a   ··4···_? ·····b·
0080  f9 79 2e 7d 9e ac 62 0e  b1 dd d4 2d 1e 04 7b 56   ·y.}··b· ···-··{V
0090  23 4d 7a 14 1f 46 25 b2  d7 5e e2 d1 12 2f 9f 04   #Mz··F%· ·^···/··
00a0  59 58 73 b6 0d b8 db 03  0b 0d 8a 05 2b f9 7a bd   YXs····· ····+·z·
00b0  f3 ae cb 4c 37 f3 fa 8e  bd 76 07 4f e4 0c 18 da   ···L7··· ·v·O····
00c0  f4 50 04 ec 8a 21 d7 c2  d9 ef 4c 82 37 dc 90 73   ·P···!·· ··L·7··s
00d0  83 98 61 22 66 c6 7f 96  64 a8 fd 04 a5 57 a0 76   ··a"f··· d····W·v
00e0  97 0e e3 54 54 20 2c 1f  f5 60 60 23 31 c2 bb 39   ···TT ,· ·``#1··9
00f0  be b9 66 7f 0b 98 af 8f  1d ef a1 97 c0 96 b6 30   ··f····· ·******0
0100  dd 5e e1 74 6e 32 c1 a6  8f 77 bb bb 69 e5 29 9f   ·^·tn2·· ·w··i·)·
0110  14 f0 ed a1 bb 5a 6d 3f  83 3a c2 b5 76 bf ac 32   ····· Zm? ·:··v··2
0120  6c d3 6a 3d d6 fb c3 a6  28 e9 a5 31 cf 06 50 87   l·j=···· (··1··P·
0130  f3 4e 47 44 af c7 55 93  96 3f 88 53 93 39 03 1d   ·NGD··U· ·?·S·9··
0140  11 24 43 2b de 3e cd 39  bd 21 a5 36 38 fd 42 d4   ·$C+·>·9 ·!·68·B·
```

شکل (۴) بیت های مربوط به لایه سوم (TCP)

اندازه فریم لایه دوم این بسته: ۱۴۴۰ بایت

```
> Frame 567: 1454 bytes on wire (11632 bits), 1454 bytes captured (11632 bits) on interface \Device\NI
> Ethernet II, Src: 02:42:95:be:32:0e (02:42:95:be:32:0e), Dst: HonHaiPr_2f:8b:55 (00:71:cc:2f:8b:55)
v Internet Protocol Version 4, Src: 185.211.88.131, Dst: 192.168.125.76
    0100 .... = Version: 4
    .... 0101 = Header Length: 20 bytes (5)
  > Differentiated Services Field: 0x00 (DSCP: CS0, ECN: Not-ECT)
    Total Length: 1440
    Identification: 0x9136 (37174)
  > Flags: 0x40, Don't fragment
    ...0 0000 0000 0000 = Fragment Offset: 0
    Time to Live: 124
    Protocol: TCP (6)
    Header Checksum: 0x17d6 [validation disabled]
    [Header checksum status: Unverified]
    Source Address: 185.211.88.131
    Destination Address: 192.168.125.76
> Transmission Control Protocol, Src Port: 443, Dst Port: 51731, Seq: 13974, Ack: 1859, Len: 1400
```

شکل (۵) اندازه فریم لایه دوم (Total Length)

اندازه بسته لایه سوم: ۱۴۰۰ بایت

```
> Frame 567: 1454 bytes on wire (11632 bits), 1454 bytes captured (11632 bits) on interface \Device\NF
> Ethernet II, Src: 02:42:95:be:32:0e (02:42:95:be:32:0e), Dst: HonHaiPr_2f:8b:55 (00:71:cc:2f:8b:55)
> Internet Protocol Version 4, Src: 185.211.88.131, Dst: 192.168.125.76
v Transmission Control Protocol, Src Port: 443, Dst Port: 51731, Seq: 13974, Ack: 1859, Len: 1400
    Source Port: 443
    Destination Port: 51731
    [Stream index: 7]
    [Conversation completeness: Complete, WITH_DATA (63)]
    [TCP Segment Len: 1400]
    Sequence Number: 13974    (relative sequence number)
```

شکل (۶) اندازه بسته لایه سوم (TCP Segment Len)

سوال ۳: آیا می توانید بسته هایی را پیدا کنید که بدون پروتکل های لایه های Application, Transport, Network باشند؟ این بسته ها از چه پروتکلی استفاده کرده اند؟

بله، از پروتکل ARP استفاده کرده اند.

سوال ۴: از یکی از بسته ها بخش مربوط به پروتکل Internet Protocol(IP) را پیدا کنید. Checksum پروتکل IP را پیدا کنید و یادداشت کنید.

Checksum پروتکل IP برای بسته شماره ۵۶۷: 0x17d6

```
> Frame 567: 1454 bytes on wire (11632 bits), 1454 bytes captured (11632 bits) on interface \Device\NF
> Ethernet II, Src: 02:42:95:be:32:0e (02:42:95:be:32:0e), Dst: HonHaiPr_2f:8b:55 (00:71:cc:2f:8b:55)
v Internet Protocol Version 4, Src: 185.211.88.131, Dst: 192.168.125.76
    0100 .... = Version: 4
    .... 0101 = Header Length: 20 bytes (5)
  > Differentiated Services Field: 0x00 (DSCP: CS0, ECN: Not-ECT)
    Total Length: 1440
    Identification: 0x9136 (37174)
  > Flags: 0x40, Don't fragment
    ...0 0000 0000 0000 = Fragment Offset: 0
    Time to Live: 124
    Protocol: TCP (6)
    Header Checksum: 0x17d6 [validation disabled]
    [Header checksum status: Unverified]
    Source Address: 185.211.88.131
    Destination Address: 192.168.125.76
> Transmission Control Protocol, Src Port: 443, Dst Port: 51731, Seq: 13974, Ack: 1859, Len: 1400
```

شکل (۸) Checksum پروتکل IP بسته شماره ۵۶۷

سوال ۵: از یکی از بسته ها بخش مربوط به پروتکل Transport Control Protocol(TCP) و یا User Datagram Protocol(UDP) را پیدا کنید. عدد مربوط به port مبدا و مقصد را یادداشت کنید. به نظر شما این اعداد در مبدا و مقصد چه چیزی را مشخص می کند؟ Checksum مربوط به پروتکل های TCP و UDP را مشخص کنید.

Checksum پروتکل TCP برای بسته شماره ۵۶۷: 0x847c

Port مبدا: ۴۴۳ Port مقصد: ۵۱۷۱۳

برای آنکه به صورت یکتا بتوانیم ارتباط بین مبدا و مقصد را برقرار کنیم، علاوه بر آدرس IP نیاز به port مبدا و مقصد نیز داریم، زیرا ممکن است یک مبدا بیش از یک ارتباط(connection) با مقصد داشته باشد و این تمایز بین ارتباط ها با شماره های port مختلف در مبدا برطرف می شود و همچنین همین روند در مقصد هم ممکن است اتفاق بیفتد. پس با (Src IP, Src Port, Dst IP, Dst Port) میتوان به صورت یکتا ارتباط ها را مشخص کرد.

```
> Frame 567: 1454 bytes on wire (11632 bits), 1454 bytes captured (11632 bits) on interface \Device\NF
> Ethernet II, Src: 02:42:95:be:32:0e (02:42:95:be:32:0e), Dst: HonHaiPr_2f:8b:55 (00:71:cc:2f:8b:55)
> Internet Protocol Version 4, Src: 185.211.88.131, Dst: 192.168.125.76
v Transmission Control Protocol, Src Port: 443, Dst Port: 51731, Seq: 13974, Ack: 1859, Len: 1400
    Source Port: 443
    Destination Port: 51731
    [Stream index: 7]
    [Conversation completeness: Complete, WITH_DATA (63)]
    [TCP Segment Len: 1400]
    Sequence Number: 13974    (relative sequence number)
    Sequence Number (raw): 3264897997
    [Next Sequence Number: 15374    (relative sequence number)]
    Acknowledgment Number: 1859    (relative ack number)
    Acknowledgment number (raw): 4062190540
    0101 .... = Header Length: 20 bytes (5)
  > Flags: 0x010 (ACK)
    Window: 65535
    [Calculated window size: 65535]
    [Window size scaling factor: -2 (no window scaling used)]
    Checksum: 0x847c [unverified]
    [Checksum Status: Unverified]
```

شکل (۹) پروتکل TCP برای بسته شماره ۵۶۷

سوال ۶: یکی از بسته ها که از سیستم شما ارسال شده است را انتخاب کنید. پروتکل لایه Transport چیست؟ آدرس IP مقصد چیست؟ سرایند لایه دوم را انتخاب کنید. آدرس مبدا و مقصد را یادداشت کنید.

ابتدا ip کامپیوتر خودمان را بدست می آوریم و بسته هایی که ip مبدا آنها برابر با ip کامپیوتر ما باشند، یعنی از سیستم ما ارسال شده اند.

IPv4 Address = 192.168.229.76

```
Wireless LAN adapter Wi-Fi:

   Connection-specific DNS Suffix  . :
   Description . . . . . . . . . . . : Ralink RT3290 802.11bgn Wi-Fi Adapter
   Physical Address. . . . . . . . . : 00-71-CC-2F-8B-55
   DHCP Enabled. . . . . . . . . . . : Yes
   Autoconfiguration Enabled . . . . : Yes
   Link-local IPv6 Address . . . . . : fe80::7048:32ef:b10f:f518%4(Preferred)
   IPv4 Address. . . . . . . . . . . : 192.168.229.76(Preferred)
   Subnet Mask . . . . . . . . . . . : 255.255.255.0
   Lease Obtained. . . . . . . . . . : Thursday, March 24, 2022 10:59:16 AM
   Lease Expires . . . . . . . . . . : Thursday, March 24, 2022 11:59:15 AM
   Default Gateway . . . . . . . . . : 192.168.229.35
   DHCP Server . . . . . . . . . . . : 192.168.229.35
   DHCPv6 IAID . . . . . . . . . . . : 67137996
   DHCPv6 Client DUID. . . . . . . . : 00-01-00-01-26-BF-5D-52-C4-34-6B-04-53-A3
   DNS Servers . . . . . . . . . . . : 192.168.229.35
   NetBIOS over Tcpip. . . . . . . . : Enabled
```

شکل (۱۰) بدست آوردن ip سیستم با دستور ipconfig /all

بسته شماره ۳ را که ip مبدا آن 192.168.229.76 است انتخاب می کنیم.

```
> Frame 3: 87 bytes on wire (696 bits), 87 bytes captured (696 bits) on interface \Device\NPF_{208E5106-B2CE-410D-B585-C1ACCB2DAAD6}, id 0
> Ethernet II, Src: HonHaiPr_2f:8b:55 (00:71:cc:2f:8b:55), Dst: 02:42:95:be:32:0e (02:42:95:be:32:0e)
> Internet Protocol Version 4, Src: 192.168.229.76, Dst: 192.168.229.35
> User Datagram Protocol, Src Port: 55375, Dst Port: 53
> Domain Name System (query)
```

شکل (۱۱) بسته شماره ۳ با ip مبدا 192.168.229.76

پروتکل لایه Transport: UDP

```
> Frame 3: 87 bytes on wire (696 bits), 87 bytes captured (696 bits) on interface \Device\NPF_{208E5106-B2CE-410D-B585-C1ACCB2DAAD6}, id 0
> Ethernet II, Src: HonHaiPr_2f:8b:55 (00:71:cc:2f:8b:55), Dst: 02:42:95:be:32:0e (02:42:95:be:32:0e) ---> Data Link Layer (layer 1)
> Internet Protocol Version 4, Src: 192.168.229.76, Dst: 192.168.229.35 ---> Network Layer (layer 2)
> User Datagram Protocol, Src Port: 55375, Dst Port: 53 ---> Transport Layer (layer 3)
> Domain Name System (query)
```

شکل (۱۲) پروتکل لایه های مختلف بسته ای با پروتکل DNS

آدرس ip مقصد: 192.168.229.35 (در شکل (۱۱) قابل مشاهده است)

سوال ۷: کدام یک از آدرس های پیدا کرده در بخش قبل را می توانید در خروجی دستور ipconfig /all مشاهده کنید؟

آی پی 192.168.229.76 مربوط به سیستم ما می باشد.

آی پی 192.168.229.35 مربوط به مودم ما می باشد.

در واقع بسته های ارسالی از طرف سیستم ما برای مودم ارسال می شوند و مودم مابقی کار ها را می کند....

به شکل های (۱۱) و (۱۳) دقت شود.

```
Wireless LAN adapter Wi-Fi:

   Connection-specific DNS Suffix  . :
   Description . . . . . . . . . . . : Ralink RT3290 802.11bgn Wi-Fi Adapter
   Physical Address. . . . . . . . . : 00-71-CC-2F-8B-55
   DHCP Enabled. . . . . . . . . . . : Yes
   Autoconfiguration Enabled . . . . : Yes
   Link-local IPv6 Address . . . . . : fe80::7048:32ef:b10f:f518%4(Preferred)
   IPv4 Address. . . . . . . . . . . : 192.168.229.76(Preferred)
   Subnet Mask . . . . . . . . . . . : 255.255.255.0
   Lease Obtained. . . . . . . . . . : Thursday, March 24, 2022 10:59:16 AM
   Lease Expires . . . . . . . . . . : Thursday, March 24, 2022 11:59:15 AM
   Default Gateway . . . . . . . . . : 192.168.229.35
   DHCP Server . . . . . . . . . . . : 192.168.229.35
   DHCPv6 IAID . . . . . . . . . . . : 67137996
   DHCPv6 Client DUID. . . . . . . . : 00-01-00-01-26-BF-5D-52-C4-34-6B-04-53-A3
   DNS Servers . . . . . . . . . . . : 192.168.229.35
   NetBIOS over Tcpip. . . . . . . . : Enabled
```

شکل (۱۳) خروجی ipconfig /all

سوال ۸: یک بسته مربوط به دستور Ping را انتخاب کنید و به بخش مربوط به پروتکل DNS در آن بروید. به بخش Queries بروید. چه type ای انتخاب شده است؟ به نظر شما این درخواست DNS برای چه کاری استفاده شده است؟

تایپ A انتخاب شده است. تایپ A به منظور نگاشت hostname به ip address استفاده می شود.

If *Type=A*, then *Name* is a hostname and *Value* is the IP address for the hostname. Thus, a Type A record provides the standard hostname-to-IP address mapping. As an example, *(relay1.bar.foo.com, 145.37.93.126, A)* is a Type A record.

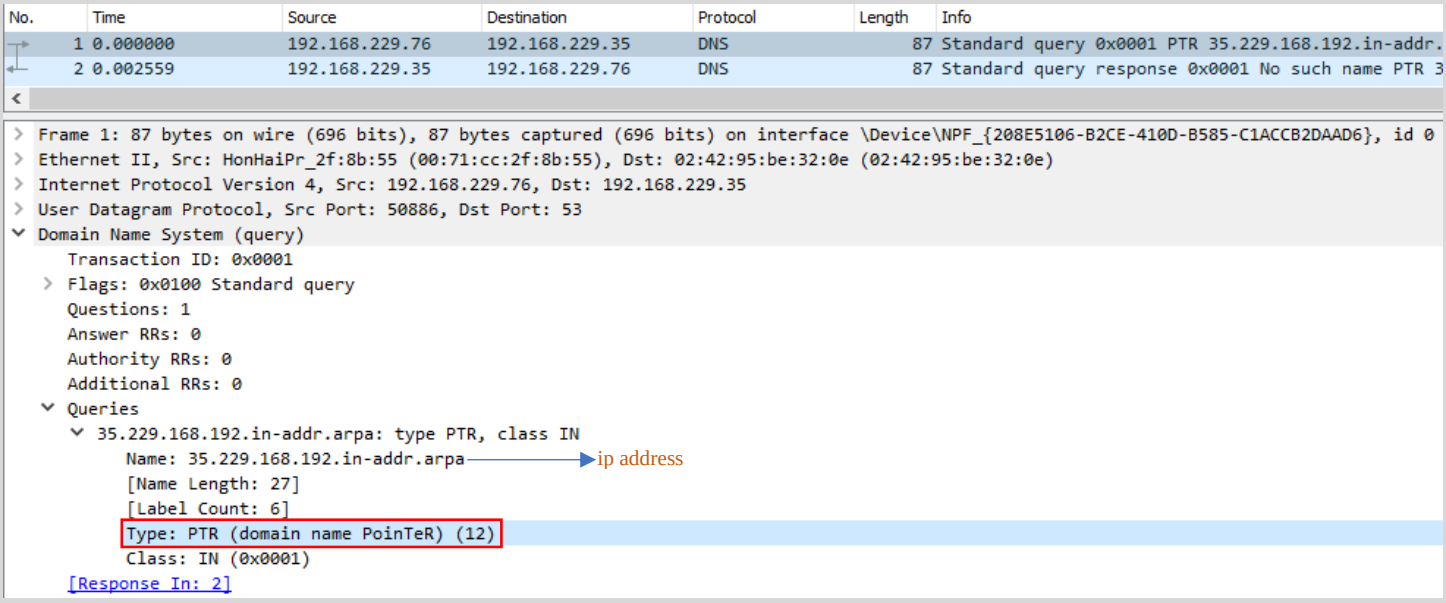
No.	Time	Source	Destination	Protocol	Length	Info
1	0.000000	192.168.229.76	192.168.229.35	DNS	70	Standard query 0xc023 A google.com
2	0.189146	192.168.229.35	192.168.229.76	DNS	86	Standard query response 0xc023 A google.com A 142.250.187.142

```
> Frame 1: 70 bytes on wire (560 bits), 70 bytes captured (560 bits) on interface \Device\NPF_{208E5106-B2CE-410D-B585-C1ACCB2DAAD6}, id 0
> Ethernet II, Src: HonHaiPr_2f:8b:55 (00:71:cc:2f:8b:55), Dst: 02:42:95:be:32:0e (02:42:95:be:32:0e)
> Internet Protocol Version 4, Src: 192.168.229.76, Dst: 192.168.229.35
> User Datagram Protocol, Src Port: 56080, Dst Port: 53
v Domain Name System (query)
    Transaction ID: 0xc023
  > Flags: 0x0100 Standard query
    Questions: 1
    Answer RRs: 0
    Authority RRs: 0
    Additional RRs: 0
  v Queries
    v google.com: type A, class IN
        Name: google.com ---------> hostname
        [Name Length: 10]
        [Label Count: 2]
        Type: A (Host Address) (1)
        Class: IN (0x0001)
    [Response In: 2]
```

شکل (۱۴) type بخش Queries برای دستور ping

سوال ۹: یک بسته مربوط به دستور nslookup را انتخاب کنید و به بخش مربوط به پروتکل DNS در آن بروید. به بخش Queries بروید. چه type ای انتخاب شده است؟ به نظر شما این درخواست DNS برای چه کاری استفاده شده است؟

تایپ PTR است. دقیقا بر خلاف تایپ A است و hostname متناسب با ip address را بر میگرداند یعنی در واقع نگاشت ip address به hostname را انجام میدهد.



شکل (۱۵) type بخش Queries برای دستور nslookup

سوال ۱۰: به نظر شما چه type های دیگری ممکن است وجود داشته باشد؟ سه مورد را یادداشت کنید.

NS: فیلد Name در آن یک domain است و فیلد Value در آن hostname مربوط به یک DNS server است که میداند چگونه ip address مربوط به host را در domain بدست آورد. این تایپ به منظور مسیر یابی DNS query ها در زنجیره query ها استفاده می شود.

CNAME: فیلد Name در آن یک نام مستعار (alias hostname) است و فیلد Value در آن یک نام رسمی (canonical hostname) است. این تایپ میتواند نام رسمی یک نام مستعار را بدست آورد.

MX: فیلد Name در آن یک نام مستعار (alias hostname) است و فیلد Value در آن یک نام رسمی (canonical name) مربوط به mail server است. این تایپ به hostname یک mail server اجازه میدهد تا یک نام مستعار برای خود داشته باشد.

اطلاعات تکمیلی:

If `Type=NS`, then `Name` is a domain (such as **`foo.com`**) and `Value` is the hostname of an authoritative DNS server that knows how to obtain the IP addresses for hosts in the domain. This record is used to route DNS queries further along in the query chain. As an example, **`(foo.com, dns.foo.com, NS)`** is a Type NS record.

If `Type=CNAME`, then `Value` is a canonical hostname for the alias hostname `Name`. This record can provide querying hosts the canonical name for a hostname. As an example, **`(foo.com, relay1.bar.foo.com, CNAME)`** is a CNAME record.

If `Type=MX`, then `Value` is the canonical name of a mail server that has an alias hostname `Name`. As an example, **`(foo.com, mail.bar.foo.com, MX)`** is an MX record. MX records allow the hostnames of mail servers to have simple aliases.

سوال ۱۱: بعد از کلیک کردن بر روی OK چه اتفاقی می افتد؟ در بسته هایی که مشخص شده اند چه پروتکل هایی را مشاهده می کنید؟

تمامی بسته هایی که مبدا یا مقصد آنها ip مربوط به p30download.com (یعنی 5.144.130.115) باشد را نشان می دهد، زیرا فیلتر ip.addr همانطور که در توضیحات جلوی آن نوشته است ip های با مبدا و مقصد را بررسی میکند طبق عملگری که روی آن میگذاریم.

پروتکل ها: SSDP, TCP, ARP, TLSv1.2, MDNS, LLMNR, NBNS

ip.addr == 5.144.130.115

No.	Time	Source	Destination	Protocol	Length	Info
530	543.566830	192.168.229.76	192.168.229.255	NBNS	92	Name query NB WPAD<00>
531	543.567549	192.168.229.76	224.0.0.251	MDNS	70	Standard query 0x0000 A wpad.local, "QM" question
532	543.568068	fe80::7048:32ef:b…	ff02::fb	MDNS	90	Standard query 0x0000 A wpad.local, "QM" question
533	543.568530	fe80::7048:32ef:b…	ff02::1:3	LLMNR	84	Standard query 0x2a03 A wpad
534	543.568749	192.168.229.76	224.0.0.252	LLMNR	64	Standard query 0x2a03 A wpad
535	543.569886	192.168.229.76	224.0.0.251	MDNS	70	Standard query 0x0000 A wpad.local, "QM" question
536	543.570352	fe80::7048:32ef:b…	ff02::fb	MDNS	90	Standard query 0x0000 A wpad.local, "QM" question
537	543.750910	192.168.229.76	192.168.229.35	DNS	75	Standard query 0x607e A iup.360safe.com
538	543.835170	54.254.196.234	192.168.229.76	TCP	66	80 → 55103 [SYN, ACK] Seq=0 Ack=1 Win=17922 Len=0 MSS=1400 SACK_PERM=1 WS=512
539	543.835312	192.168.229.76	54.254.196.234	TCP	54	55103 → 80 [ACK] Seq=1 Ack=1 Win=131584 Len=0
540	543.835475	192.168.229.76	54.254.196.234	HTTP	269	GET /safei18n/update_v3.htm?id=TASK_UPDATE_MODULE&edition=TS&pt=1&mid=7e235eac0ce0443c7c0f6e08830970
541	543.838864	192.168.229.35	192.168.229.76	DNS	182	Standard query response 0x607e A iup.360safe.com CNAME d11opja9k668h0.cloudfront.net A 18.66.97.47 A
542	543.846942	fe80::7048:32ef:b…	ff02::1:3	LLMNR	84	Standard query 0xd7c9 A wpad
543	543.846946	192.168.229.76	18.66.97.47	TCP	66	55104 → 80 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 WS=256 SACK_PERM=1
544	543.847124	192.168.229.76	224.0.0.252	LLMNR	64	Standard query 0xd7c9 A wpad
545	543.879543	54.254.196.234	192.168.229.76	TCP	54	80 → 55103 [ACK] Seq=1 Ack=216 Win=94720 Len=0
546	543.989945	fe80::7048:32ef:b…	ff02::1:3	LLMNR	84	Standard query 0x2a03 A wpad
547	543.990253	192.168.229.76	224.0.0.252	LLMNR	64	Standard query 0x2a03 A wpad
548	544.039191	18.66.97.47	192.168.229.76	TCP	66	80 → 55104 [SYN, ACK] Seq=0 Ack=1 Win=65535 Len=0 MSS=1400 SACK_PERM=1 WS=512
549	544.039321	192.168.229.76	18.66.97.47	TCP	54	55104 → 80 [ACK] Seq=1 Ack=1 Win=131584 Len=0
550	544.039475	192.168.229.76	18.66.97.47	HTTP	296	GET /iv3/pc/360safe/isafeup_lib.cab?mid=7e235eac0ce0443c7c0f6e0883097089&ver=10.8.0.1400&lan=en&os=1
551	544.087249	18.66.97.47	192.168.229.76	TCP	54	80 → 55104 [ACK] Seq=1 Ack=243 Win=94720 Len=0
552	544.124135	54.254.196.234	192.168.229.76	TCP	54	[TCP Previous segment not captured] 80 → 55103 [FIN, ACK] Seq=210 Ack=216 Win=94720 Len=0
553	544.124204	192.168.229.76	54.254.196.234	TCP	54	[TCP Dup ACK 539#1] 55103 → 80 [ACK] Seq=216 Ack=1 Win=131584 Len=0
554	544.125102	54.254.196.234	192.168.229.76	TCP	263	[TCP Out-Of-Order] 80 → 55103 [PSH, ACK] Seq=1 Ack=216 Win=94720 Len=209

شکل (۱۶) بخشی از بسته های فیلتر شده ip.addr == 5.144.130.115

```
C:\Users\Javad\Desktop\cmder
λ tracert p30download.com

Tracing route to p30download.com [5.144.130.115]
over a maximum of 30 hops:

  1    1 ms     4 ms     2 ms  192.168.229.35
  2     *        *        *    Request timed out.
  3   110 ms    45 ms    45 ms  10.196.23.193
  4   101 ms   112 ms    57 ms  10.196.89.139
  5     *        *        *    Request timed out.
  6    97 ms    35 ms    36 ms  10.196.89.65
  7     *        *        *    Request timed out.
  8    47 ms    34 ms    43 ms  10.136.131.30
  9    59 ms    40 ms    49 ms  10.196.119.5
 10    49 ms    44 ms    46 ms  172.17.132.9
 11     *        *        *    Request timed out.
 12   119 ms    86 ms   103 ms  10.202.1.5
 13     *        *        *    Request timed out.
 14    47 ms    49 ms    64 ms  5-144-130-115.static.hostiran.name [5.144.130.115]

Trace complete.
```

شکل (۱۷) tracert p30download.com و بدست آوردن ip آن

سوال ۱۲: اولین بسته را انتخاب کنید. به بخش پروتکل Internet Control Message Protocol بروید. مقدار type را مشخص کنید. به بخش مربوط به پروتکل IP بروید و مقدار TTL را یادداشت کنید.

مقدار type بخش ICMP برابر با 8 (Echo (ping) request) است [شکل (۱۸)]

مقدار TTL هم در بخش پروتکل IP برابر با 1 می باشد[شکل (۱۹)]

ip.addr == 5.144.130.115

No.	Time	Source	Destination	Protocol	Length	Info
1	0.000000	192.168.229.76	239.255.255.250	SSDP	143	M-SEARCH * HTTP/1.1
2	0.137936	02:42:95:be:32:0e	HonHaiPr_2f:8b:55	ARP	42	Who has 192.168.229.76? Tell 192.168.229.35
3	0.137961	HonHaiPr_2f:8b:55	02:42:95:be:32:0e	ARP	42	192.168.229.76 is at 00:71:cc:2f:8b:55
4	3.662097	192.168.229.76	192.168.229.35	DNS	75	Standard query 0x0835 A p30download.com
5	3.859710	192.168.229.76	192.168.229.35	DNS	75	Standard query 0x0835 A p30download.com
6	3.985683	192.168.229.35	192.168.229.76	DNS	91	Standard query response 0x0835 A p30download.com A 5.144.130.115
7	4.005543	192.168.229.76	5.144.130.115	ICMP	106	Echo (ping) request id=0x0001, seq=25/6400, ttl=1 (no response found!)
8	4.007144	192.168.229.35	192.168.229.76	ICMP	134	Time-to-live exceeded (Time to live exceeded in transit)
9	4.009032	192.168.229.76	5.144.130.115	ICMP	106	Echo (ping) request id=0x0001, seq=26/6656, ttl=1 (no response found!)

```
> Frame 7: 106 bytes on wire (848 bits), 106 bytes captured (848 bits) on interface \Device\NPF_{208E5106-B2CE-410D-B585-C1ACCB2DAAD6}, id 0
> Ethernet II, Src: HonHaiPr_2f:8b:55 (00:71:cc:2f:8b:55), Dst: 02:42:95:be:32:0e (02:42:95:be:32:0e)
> Internet Protocol Version 4, Src: 192.168.229.76, Dst: 5.144.130.115
v Internet Control Message Protocol
    Type: 8 (Echo (ping) request)
    Code: 0
    Checksum: 0xf7e5 [correct]
    [Checksum Status: Good]
    Identifier (BE): 1 (0x0001)
    Identifier (LE): 256 (0x0100)
    Sequence Number (BE): 25 (0x0019)
    Sequence Number (LE): 6400 (0x1900)
  > [No response seen]
  > Data (64 bytes)
```

شکل (۱۸) مقدار type بخش پروتکل ICMP

ip.addr == 5.144.130.115

No.	Time	Source	Destination	Protocol	Length	Info
1	0.000000	192.168.229.76	239.255.255.250	SSDP	143	M-SEARCH * HTTP/1.1
2	0.137936	02:42:95:be:32:0e	HonHaiPr_2f:8b:55	ARP	42	Who has 192.168.229.76? Tell 192.168.229.35
3	0.137961	HonHaiPr_2f:8b:55	02:42:95:be:32:0e	ARP	42	192.168.229.76 is at 00:71:cc:2f:8b:55
4	3.662097	192.168.229.76	192.168.229.35	DNS	75	Standard query 0x0835 A p30download.com
5	3.859710	192.168.229.76	192.168.229.35	DNS	75	Standard query 0x0835 A p30download.com
6	3.985683	192.168.229.35	192.168.229.76	DNS	91	Standard query response 0x0835 A p30download.com A 5.144.130.115
7	4.005543	192.168.229.76	5.144.130.115	ICMP	106	Echo (ping) request id=0x0001, seq=25/6400, ttl=1 (no response found!)
8	4.007144	192.168.229.35	192.168.229.76	ICMP	134	Time-to-live exceeded (Time to live exceeded in transit)
9	4.009032	192.168.229.76	5.144.130.115	ICMP	106	Echo (ping) request id=0x0001, seq=26/6656, ttl=1 (no response found!)

```
> Frame 7: 106 bytes on wire (848 bits), 106 bytes captured (848 bits) on interface \Device\NPF_{208E5106-B2CE-410D-B585-C1ACCB2DAAD6}, id 0
> Ethernet II, Src: HonHaiPr_2f:8b:55 (00:71:cc:2f:8b:55), Dst: 02:42:95:be:32:0e (02:42:95:be:32:0e)
v Internet Protocol Version 4, Src: 192.168.229.76, 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: 0xe774 (59252)
  > Flags: 0x00
    ...0 0000 0000 0000 = Fragment Offset: 0
  > Time to Live: 1
    Protocol: ICMP (1)
    Header Checksum: 0xa434 [validation disabled]
    [Header checksum status: Unverified]
    Source Address: 192.168.229.76
    Destination Address: 5.144.130.115
> Internet Control Message Protocol
```

شکل (۱۹) مقدار Time to live بخش پروتکل IP

سوال ۱۳: به نظر شما هدف از تغییر این مقدار(TTL) چیست؟ می توانید با مراجعه به هدف دستور tracert آن را شرح دهید.

هر بسته در مسیری از مبدا به مقصد از میان دستگاه های مختلفی عبور می کند که هر یک از آنها یک hop هستند. TTL ارتباط مستقیمی با تعداد گام های مسیری که بسته از آن عبور می کند دارد. با عبور از هر hop، یک واحد از TTL بسته کاسته می شود. هنگامی که یک بسته با مقدار hop صفر به دستگاهی می رسد که مقصدش نیست، توسط آن دستگاه دور ریخته می شود و یک پیغام خطای ICMP را برای میزبانی ارسال می کند که اقدام به ارسال بسته کرده است. هنگامی که مقدار به صفر یا یک برسد و بسته به دستگاه مقصد رسیده باشد، پیغام Accept را برای میزبان ارسال می کند. پس TTL مقدار زمانی است که بسته در شبکه اعتبار دارد. TTL همچنین به ارسال کننده بسته اجازه می دهد از تعداد گام ها در طول مسیر اطلاع پیدا کند، پس میتوان از TTL برای ارزیابی عملکرد شبکه استفاده کرد.

سوال ۱۴: این فیلتر(ip.proto==6) چه کاری انجام می دهد؟

پروتکل شماره ۶ همان TCP است و این فیلتر میگوید که بسته های با پروتکل TCP نمایش داده شود [شکل (۳۰)].

ip.proto==6

No.	Time	Source	Destination	Protocol	Length	Info
45	26.821821	192.168.229.76	20.198.162.78	TLSv1.2	155	Application Data
46	26.870075	20.198.162.78	192.168.229.76	TCP	54	443 → 56727 [ACK] Seq=1 Ack=102 Win=65535 Len=0
47	26.988096	20.198.162.78	192.168.229.76	TLSv1.2	225	Application Data
48	27.028551	192.168.229.76	20.198.162.78	TCP	54	56727 → 443 [ACK] Seq=102 Ack=172 Win=511 Len=0
77	46.633581	54.77.108.94	192.168.229.76	TCP	54	80 → 56720 [ACK] Seq=1 Ack=1 Win=735 Len=0
78	46.633666	192.168.229.76	54.77.108.94	TCP	54	[TCP ACKed unseen segment] 56720 → 80 [ACK] Seq=1 Ack=2 Win=509 Len=0
96	60.103537	20.135.20.1	192.168.229.76	TCP	54	443 → 55089 [RST, ACK] Seq=1 Ack=1 Win=370 Len=0
98	61.585081	13.107.42.12	192.168.229.76	TCP	54	443 → 55091 [RST, ACK] Seq=1 Ack=1 Win=384 Len=0
101	63.629921	20.135.20.1	192.168.229.76	TCP	54	443 → 55090 [RST, ACK] Seq=1 Ack=1 Win=388 Len=0
128	85.035411	54.77.52.141	192.168.229.76	TCP	54	80 → 56721 [ACK] Seq=1 Ack=1 Win=236 Len=0
129	85.035496	192.168.229.76	54.77.52.141	TCP	54	[TCP ACKed unseen segment] 56721 → 80 [ACK] Seq=1 Ack=2 Win=509 Len=0
168	114.758530	20.54.232.160	192.168.229.76	TCP	54	443 → 55093 [RST, ACK] Seq=1 Ack=1 Win=440 Len=0
214	163.960377	192.168.229.76	52.208.22.58	TCP	66	55097 → 80 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 WS=256 SACK_PERM=1
215	164.128778	52.208.22.58	192.168.229.76	TCP	62	80 → 55097 [SYN, ACK] Seq=0 Ack=1 Win=17922 Len=0 MSS=1400 WS=128
216	164.128882	192.168.229.76	52.208.22.58	TCP	54	55097 → 80 [ACK] Seq=1 Ack=1 Win=131584 Len=0
217	164.139076	192.168.229.76	52.208.22.58	HTTP	560	POST /scan HTTP/1.1 (application/x-www-form-urlencoded)
218	164.178908	52.208.22.58	192.168.229.76	TCP	54	80 → 55097 [ACK] Seq=1 Ack=507 Win=94720 Len=0
219	164.313999	52.208.22.58	192.168.229.76	TCP	54	[TCP Previous segment not captured] 80 → 55097 [FIN, ACK] Seq=265 Ack=507 Win=94720 Len=0
220	164.314069	192.168.229.76	52.208.22.58	TCP	54	[TCP Dup ACK 216#1] 55097 → 80 [ACK] Seq=507 Ack=1 Win=131584 Len=0
221	164.314151	52.208.22.58	192.168.229.76	TCP	318	[TCP Out-Of-Order] 80 → 55097 [PSH, ACK] Seq=1 Ack=507 Win=94720 Len=264
222	164.314203	192.168.229.76	52.208.22.58	TCP	54	55097 → 80 [ACK] Seq=507 Ack=266 Win=131328 Len=0
223	164.314300	192.168.229.76	52.208.22.58	TCP	54	55097 → 80 [FIN, ACK] Seq=507 Ack=266 Win=131328 Len=0
224	164.348892	52.208.22.58	192.168.229.76	TCP	54	80 → 55097 [ACK] Seq=266 Ack=508 Win=94720 Len=0
226	166.948948	54.77.108.94	192.168.229.76	TCP	54	[TCP Dup ACK 77#1] 80 → 56720 [ACK] Seq=1 Ack=1 Win=735 Len=0
227	166.949034	192.168.229.76	54.77.108.94	TCP	54	[TCP Dup ACK 78#1] [TCP ACKed unseen segment] 56720 → 80 [ACK] Seq=1 Ack=2 Win=509 Len=0
237	195.999717	192.168.229.76	54.77.108.94	TCP	70	[TCP ACKed unseen segment] 56720 → 80 [PSH, ACK] Seq=1 Ack=2 Win=509 Len=16
238	196.333226	192.168.229.76	54.77.108.94	TCP	70	[TCP ACKed unseen segment] [TCP Retransmission] 56720 → 80 [PSH, ACK] Seq=1 Ack=2 Win=509 Len=16
239	196.338717	54.77.108.94	192.168.229.76	TCP	70	[TCP Previous segment not captured] 80 → 56720 [PSH, ACK] Seq=2 Ack=1 Win=735 Len=16
240	196.342439	54.77.108.94	192.168.229.76	TCP	54	80 → 56720 [ACK] Seq=18 Ack=17 Win=735 Len=0
241	196.381343	192.168.229.76	54.77.108.94	TCP	54	[TCP ACKed unseen segment] 56720 → 80 [ACK] Seq=17 Ack=18 Win=509 Len=0
242	196.880406	54.77.108.94	192.168.229.76	TCP	54	[TCP Dup ACK 240#1] 80 → 56720 [ACK] Seq=18 Ack=17 Win=735 Len=0

شکل (۲۰) فیلتر ip.proto==6