



**دانشگاه صنعتی امیر کبیر
(پلی تکنیک تهران)**

گزارشکار از مایش سوم

گروه ۴

آشنایی با نرم افزار Wireshark

از مایشگاه شبکه های کامپیوتری

هلیاسادات هاشمی پور

۹۸۳۱۱۰۶

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

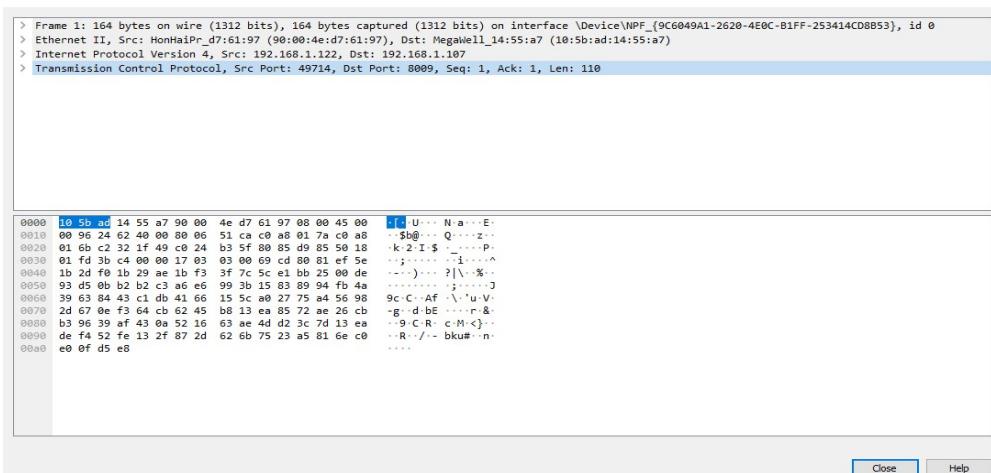
با توجه به خواسته سوال یک بخش دلخواه را (مثلا Wifi) انتخاب می کنیم سپس به ستون پروتکل رفته و لیست پروتکل ها را که مشاهده می کنیم می نویسیم:

TCP, DNS, TLSv1.2, MDNS , SSDP, ARP, UDP

130 50.144724	192.168.1.122	192.168.1.107	TCP	164 49714 → 8009 [PSH, ACK] Seq=1101 Ack=1101 Win=511 Len=110 [TCP segment of a reassembled PDU]
131 50.147529	192.168.1.187	192.168.1.122	TCP	164 8009 → 49714 [PSH, ACK] Seq=1101 Ack=1211 Win=1419 Len=110 [TCP segment of a reassembled PDU]
132 50.190385	192.168.1.122	192.168.1.107	TCP	54 49714 → 8009 [ACK] Seq=1211 Ack=1211 Win=511 Len=0
133 50.756922	fe80::5140:b7ab:b13...	fe80::fa9a:78ff:fe6...	DNS	101 Standard query 0xcb3a A update.googleapis.com
134 50.757354	fe80::5140:b7ab:b13...	fe80::fa9a:78ff:fe6...	DNS	101 Standard query 0xc323 AAAA update.googleapis.com
135 50.801818	fe80::fa9a:78ff:fe6...	fe80::5140:b7ab:b13...	DNS	117 Standard query response 0xcb3a A update.googleapis.com A 142.250.181.163
136 50.802088	fe80::fa9a:78ff:fe6...	fe80::5140:b7ab:b13...	DNS	129 Standard query response 0xc323 AAAA update.googleapis.com AAAA 2a00:1450:4018:809::2003
137 50.807125	192.168.1.122	142.250.181.163	TCP	66 49763 → 443 [SYN] Seq=0 Win=64240 MSS=1468 WS=256 SACK_PERM=1
138 50.886117	142.250.181.163	192.168.1.122	TCP	66 443 → 49763 [SYN, ACK] Seq=1 Ack=1 Win=65355 Len=0 MSS=1400 SACK_PERM=1 WS=256
139 50.886226	192.168.1.122	142.250.181.163	TCP	54 49763 → 443 [ACK] Seq=1 Ack=1 Win=131584 Len=0
140 50.887870	192.168.1.122	142.250.181.163	TLSv1.2	260 Client Hello
141 50.954927	142.250.181.163	192.168.1.122	TCP	54 443 → 49763 [ACK] Seq=1 Ack=207 Win=66816 Len=0
142 50.955320	142.250.181.163	192.168.1.122	TCP	54 [TCP Dup ACK 141#1] 443 → 49763 [ACK] Seq=1 Ack=207 Win=66816 Len=0
143 51.071389	142.250.181.163	192.168.1.122	TLSv1.2	1454 Server Hello
144 51.071865	142.250.181.163	192.168.1.122	TCP	1454 443 → 49763 [PSH, ACK] Seq=1401 Ack=207 Win=66816 Len=1400 [TCP segment of a reassembled PDU]
145 51.071993	192.168.1.122	142.250.181.163	TCP	1454 443 → 49763 [ACK] Seq=2081 Ack=2081 Win=131584 Len=0
146 51.072315	142.250.181.163	192.168.1.122	TCP	1454 443 → 49763 [ACK] Seq=2801 Ack=2801 Win=66816 Len=1400 [TCP segment of a reassembled PDU]
147 51.072315	142.250.181.163	192.168.1.122	TLSv1.2	455 Certificate, Server Key Exchange, Server Hello Done
148 51.072418	192.168.1.122	142.250.181.163	TCP	1454 443 → 49763 [ACK] Seq=207 Ack=4682 Win=131584 Len=0
149 51.181162	192.168.1.122	142.250.181.163	TLSv1.2	147 Client Key Exchange, Change Cipher Spec, Encrypted Handshake Message
150 51.162026	142.250.181.163	192.168.1.122	TCP	1454 443 → 49763 [ACK] Seq=4602 Ack=308 Win=66816 Len=0
151 51.164031	142.250.181.163	192.168.1.122	TLSv1.2	346 New Session Ticket, Change Cipher Spec, Encrypted Handshake Message
152 51.164418	142.250.181.163	192.168.1.122	TLSv1.2	123 Application Data
153 51.164533	192.168.1.122	142.250.181.163	TCP	54 49763 → 443 [ACK] Seq=300 Ack=4963 Win=131072 Len=0
154 51.192407	192.168.1.122	142.250.181.163	TLSv1.2	141 Application Data
155 51.192839	192.168.1.122	142.250.181.163	TLSv1.2	475 Application Data
156 51.193125	192.168.1.122	142.250.181.163	TLSv1.2	92 Application Data
157 51.193272	192.168.1.122	142.250.181.163	TLSv1.2	1228 Application Data
158 51.269063	142.250.181.163	192.168.1.122	TLSv1.2	92 Application Data

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 ۳ چقدر است؟

ابتدا یک بسته را انتخاب کرده و سپس با کلیک بر روی آن اطلاعات زیر را به ما نمایش می دهد:



در اطلاعات بیت‌های لایه‌ها به این ترتیب پشت سر آمده: ابتدا Ethernet II (در لایه data) و سپس IPv4 (در لایه network)، سپس در لایه transport پروتکل از TCP استفاده شده است.

- اندازه فریم لایه دوم: ۱۶۴ بایت یا ۱۳۱۲ بیت (همان خط اول اسکرین شات)

- اندازه بسته لایه سوم (لایه network): ۱۵۰ (بخش total length)

```
> Frame 1: 164 bytes on wire (1312 bits), 164 bytes captured (1312 bits) on interface \Device\NPF_{9C6049A1-2620-4E0C-B1FF-253414CD8B53}, id 0
> Ethernet II, Src: HonhaiPr_d7:61:97 (00:00:4e:d7:61:97), Dst: MegaWell_14:55:a7 (10:5b:ad:14:55:a7)
└ Internet Protocol Version 4, Src: 192.168.1.122, Dst: 192.168.1.107
  0100 .... = Version: 4
  .... 0101 = Header Length: 20 bytes (5)
  > Differentiated Services Field: 0x00 (DSCP: CS0, ECN: Not-ECT)
    Total Length: 150
    Identification: 0x2462 (9314)
  > Flags: 0x40, Don't fragment
    ...0 0000 0000 0000 = Fragment Offset: 0
    Time to Live: 128
    Protocol: TCP (6)
    Header Checksum: 0x51ca [validation disabled]
      [Header checksum status: Unverified]
    Source Address: 192.168.1.122
    Destination Address: 192.168.1.107
  > Transmission Control Protocol, Src Port: 49714, Dst Port: 8009, Seq: 1, Ack: 1, Len: 110
```

سوال ۳: آیا می‌توانید بسته‌هایی را پیدا کنید که بدون پروتکل‌های لایه‌های Network، Transport و Application باشند؟ این بسته‌ها از چه پروتکلی استفاده کرده‌اند؟

بله—برای مثال بسته زیر لایه‌های ذکر شده در سوال را ندارد.

Wireshark - Packet 3400 - Wi-Fi

```
> Frame 3400: 42 bytes on wire (336 bits), 42 bytes captured (336 bits) on interface \Device\NPF_{9C6049A1-2620-4E0C-B1FF-253414CD8B53}, id 0
> Ethernet II, Src: HonhaiPr_d7:61:97 (00:00:4e:d7:61:97), Dst: HuaweiTe_63:1a:3e (f8:9a:78:63:1a:3e)
  > Address Resolution Protocol (request)

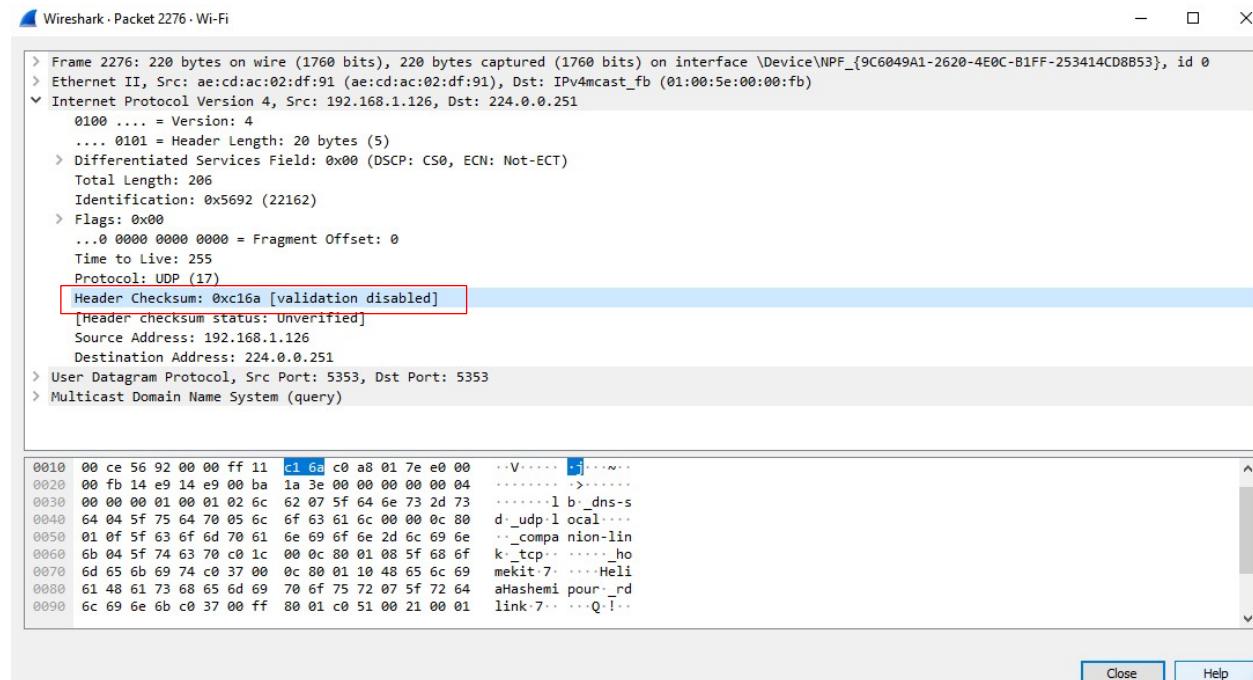
0000 f8 9a 78 63 1a 3e 90 00 4e d7 61 97 08 06 00 01 ::xc->... N:a.....
0010 08 00 06 04 00 01 90 00 4e d7 61 97 c0 a8 01 7a .....N:a....z
0020 f8 9a 78 63 1a 3e c0 a8 01 01 ::xc->... .
```

No.: 3400 · Time: 1592.857117 · Source: HonhaiPr_d7:61:97 · Destination: HuaweiTe_63:1a:3e · Protocol: ARP · Length: 42 · Info: Who has 192.168.1.1? Tell 192.168.1.122

همانطور که می‌بینیم این بسته‌ها از پروتکل ARP استفاده می‌کنند.

سوال ۴: از یکی از بسته‌ها بخش مربوط به پروتکل TCP را پیدا کنید. Checksum پروتکل IP را پیدا کنید و آن را یادداشت کنید.

برای مثال یکی از بسته‌های زیر را انتخاب و روی آن کلیک کردم. به بخش پروتکل IP ارجفته و checksum را مشاهده می‌کنیم که برابر با: 0xc16a



سوال ۵: از یکی از بسته‌ها بخش مربوط به پروتکل TCP و یا UDP را پیدا کنید. عدد مربوط به Port مبدا و مقصد را یادداشت کنید. به نظر شما این اعداد در مبدأ و مقصد چه چیزی را مشخص می‌کند؟

ابتدا بسته زیر را که دارای بخش UDP است را انتخاب می‌کنیم. عدد مربوط به پورت مبدأ (بسته از چه پورتی از مبدأ برای ما ارسال شده است) و مقصد (بسته به چه پورتی از مبدأ برای ما دریافت شده است)

آن به ترتیب برابر با ۰x5eea و ۶۲۹۶۵ است. آنchecksum برابر با:

```
> Frame 2561: 320 bytes on wire (2560 bits), 320 bytes captured (2560 bits) on interface \Device\NPF_{9C6049A1-2620-4E0C-B1FF-253414CD8B53}, id 0
> Ethernet II, Src: MegaWell_14:55:a7 (10:5b:ad:14:55:a7), Dst: HonHaiPr_d7:61:97 (90:00:4e:d7:61:97)
> Internet Protocol Version 4, Src: 192.168.1.107, Dst: 192.168.1.122
  User Datagram Protocol, Src Port: 47449, Dst Port: 62965
    Source Port: 47449
    Destination Port: 62965
    Length: 286
    Checksum: 0x5eea [unverified]
      [Checksum Status: Unverified]
      [Stream index: 134]
    > [Timestamps]
      UDP payload (278 bytes)
    > Data (278 bytes)
```

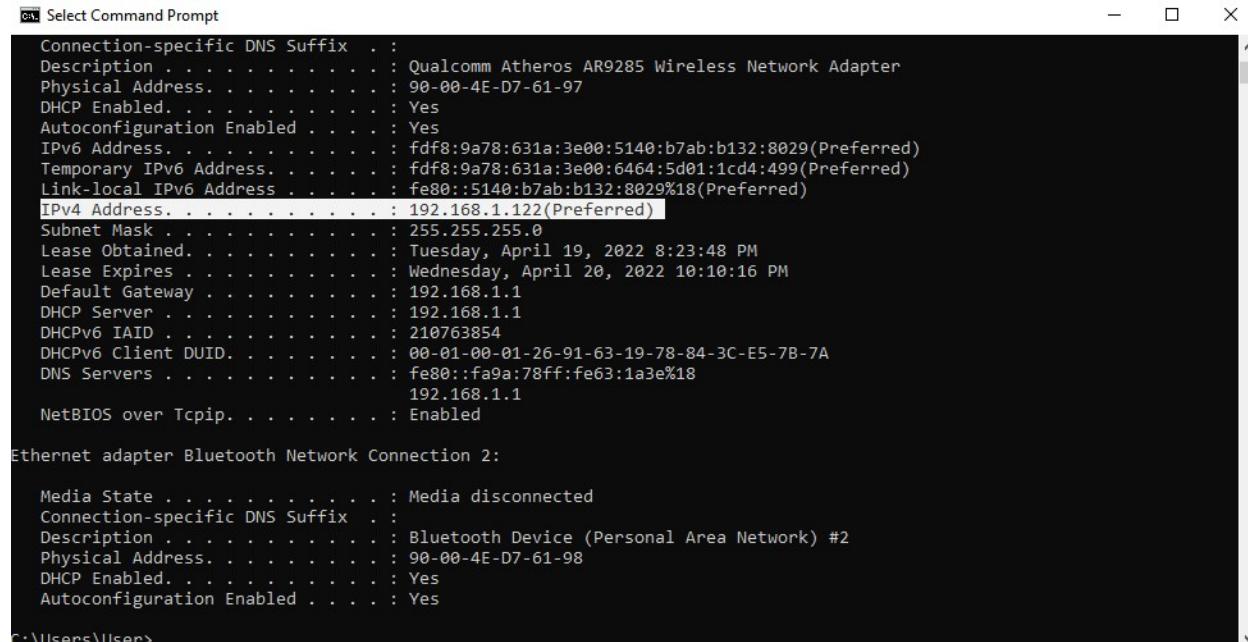
سپس بسته زیر را که دارای بخش TCP است را انتخاب می‌کنیم. و عدد مربوط به پورت مبدأ و مقصد آن به ترتیب برابر با ۰x0a85 و ۸۰۰۹ است. آنchecksum برابر با:

```
> Frame 2540: 164 bytes on wire (1312 bits), 164 bytes captured (1312 bits) on interface \Device\NPF_{9C6049A1-2620-4E0C-B1FF-253414CD8B53}, id 0
> Ethernet II, Src: HonHaiPr_d7:61:97 (90:00:4e:d7:61:97), Dst: MegaWell_14:55:a7 (10:5b:ad:14:55:a7)
> Internet Protocol Version 4, Src: 192.168.1.122, Dst: 192.168.1.107
  Transmission Control Protocol, Src Port: 49714, Dst Port: 8009, Seq: 26401, Ack: 26401, Len: 110
    Source Port: 49714
    Destination Port: 8009
    [Stream index: 0]
    [Conversation completeness: Incomplete (12)]
    [TCP Segment Len: 110]
    Sequence Number: 26401 (relative sequence number)
    Sequence Number (raw): 3223657087
    [Next Sequence Number: 26511 (relative sequence number)]
    Acknowledgment Number: 26401 (relative ack number)
    Acknowledgment number (raw): 2156282021
    0101 .... = Header Length: 20 bytes (5)
    > Flags: 0x018 (PSH, ACK)
    Window: 508
    [Calculated window size: 508]
    [Window size scaling factor: -1 (unknown)]
    Checksum: 0x0a85 [unverified]
      [Checksum Status: Unverified]
    Urgent Pointer: 0
```

برای رد و بدل کردن اطلاعات بین دو کامپیوتر استفاده می‌باشد.

سوال ۶: یکی از بسته‌ها که از سیستم شما ارسال شده است را انتخاب کنید. پروتکل لایه‌ی Transport آدرس IP مقصد چیست؟ سرایند لایه دوم را انتخاب کنید. درس مبدأ و مقصد را یادداشت کنید.

در ابتدا دستور cmd/all ipconfig را می‌نویسیم و حال تمامی اطلاعات مربوط به کارت شبکه‌های سیستم ما را می‌بینیم و حالIpv4 من برابر با ۱۹۲.۱۶۸.۱.۱۲۲ است.



```
cmd Select Command Prompt
Connection-specific DNS Suffix . :
Description . . . . . : Qualcomm Atheros AR9285 Wireless Network Adapter
Physical Address . . . . . : 90-00-4E-D7-61-97
DHCP Enabled. . . . . : Yes
Autoconfiguration Enabled . . . . . : Yes
IPv6 Address. . . . . : fdf8:9a78:631a:3e00:5140:b7ab:b132:8029(Preferred)
Temporary IPv6 Address . . . . . : fdf8:9a78:631a:3e00:6464:5d01:1cd4:499(Preferred)
Link-local IPv6 Address . . . . . : fe80::5140:b7ab:b132:8029%18(Preferred)
IPv4 Address. . . . . : 192.168.1.122(Preferred)
Subnet Mask . . . . . : 255.255.255.0
Lease Obtained. . . . . : Tuesday, April 19, 2022 8:23:48 PM
Lease Expires . . . . . : Wednesday, April 20, 2022 10:10:16 PM
Default Gateway . . . . . : 192.168.1.1
DHCP Server . . . . . : 192.168.1.1
DHCPv6 IAID . . . . . : 210763854
DHCPv6 Client DUID. . . . . : 00-01-00-01-26-91-63-19-78-84-3C-E5-7B-7A
DNS Servers . . . . . : fe80::fa9a:78ff:fe63:1a3e%18
                           192.168.1.1
NetBIOS over Tcpip. . . . . : Enabled

Ethernet adapter Bluetooth Network Connection 2:

Media State . . . . . : Media disconnected
Connection-specific DNS Suffix . . .
Description . . . . . : Bluetooth Device (Personal Area Network) #2
Physical Address. . . . . : 90-00-4E-D7-61-98
DHCP Enabled. . . . . : Yes
Autoconfiguration Enabled . . . . . : Yes

C:\Users\User>
```

سپس در لیست بسته‌های دریافت شده هر کدام از بسته‌هایی که در ستون source این آدرس را دارند، از سیستم ما ارسال شده است.

267	72.655958	192.168.1.122	13.107.6.254	TCP	54 49765 → 443 [ACK] Seq=817 Ack=7235 Win=261120 Len=0
268	72.658995	192.168.1.122	13.107.6.254	TLSv1.2	136 Application Data

```

> Frame 1192: 91 bytes on wire (728 bits), 91 bytes captured (728 bits) on interface \Device\NPF_{9C6049A1-2620-4E0C-B1FF-253414CD8B53}, id 0
> Ethernet II, Src: HonHaiPr_d7:61:97 (90:00:4e:d7:61:97), Dst: HuaweiTe_63:1a:3e (f8:9a:78:63:1a:3e)
> Internet Protocol Version 4, Src: 192.168.1.122, Dst: 192.168.1.1
    0100 .... = Version: 4
    .... 0101 = Header Length: 20 bytes (5)
> Differentiated Services Field: 0x00 (DSCP: CS0, ECN: Not-ECT)
    Total Length: 77
    Identification: 0xc462 (50274)
    Flags: 0x00
    ...0 0000 0000 0000 = Fragment Offset: 0
    Time to Live: 128
    Protocol: UDP (17)
    Header Checksum: 0xf271 [validation disabled]
    [Header checksum status: Unverified]
    Source Address: 192.168.1.122
    Destination Address: 192.168.1.1
> User Datagram Protocol, Src Port: 57388, Dst Port: 53
> Domain Name System (query)

```

طبق شکل پروتکل لایه transport آن UDP می باشد در اصل برای تمامی بسته های DNS پروتکل این لایه UDP است و آدرس IP مقصد ۱۹۲.۱۶۸.۱.۱ است.

Header checksum:0xf271

لایه دوم هم است طبق شکل:

آدرس مقصد:f8:9a:78:63:1a:3e

آدرس مبدأ:90:00:4e:d7:61:97

```

> Frame 1192: 91 bytes on wire (728 bits), 91 bytes captured (728 bits) on interface \Device\NPF_{9C6049A1-2620-4E0C-B1FF-253414CD8B53}, id 0
> Ethernet II, Src: HonHaiPr_d7:61:97 (90:00:4e:d7:61:97), Dst: HuaweiTe_63:1a:3e (f8:9a:78:63:1a:3e)
    > Destination: HuaweiTe_63:1a:3e (f8:9a:78:63:1a:3e)
    > Source: HonHaiPr_d7:61:97 (90:00:4e:d7:61:97)
    Type: IPv4 (0x0800)
> Internet Protocol Version 4, Src: 192.168.1.122, Dst: 192.168.1.1
> User Datagram Protocol, Src Port: 57388, Dst Port: 53
> Domain Name System (query)

```

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

با اجرای این دستور و مراجعه به بخش Wifi داریم:

```
Wireless LAN adapter Wi-Fi:
  Connection-specific DNS Suffix . . . . . : 
  Description . . . . . : Qualcomm Atheros AR9285 Wireless Network Adapter
  Physical Address. . . . . : 90-00-4E-D7-61-97
  DHCP Enabled. . . . . : Yes
  Autoconfiguration Enabled . . . . . : Yes
  IPv6 Address. . . . . : fdf8:9a78:631a:3e00:5140:b7ab:b132:8029(PREFERRED)
  Temporary IPv6 Address. . . . . : fdf8:9a78:631a:3e00:6464:5d01:1cd4:499(PREFERRED)
  Link-local IPv6 Address . . . . . : fe80::5140:b7ab:b132:8029%18(PREFERRED)
  IPv4 Address. . . . . : 192.168.1.122(PREFERRED)
  Subnet Mask . . . . . : 255.255.255.0
  Lease Obtained. . . . . : Tuesday, April 19, 2022 8:23:48 PM
  Lease Expires . . . . . : Wednesday, April 20, 2022 10:10:16 PM
  Default Gateway . . . . . : 192.168.1.1
  DHCP Server . . . . . : 192.168.1.1
  DHCPv6 IAID . . . . . : 210763854
  DHCPv6 Client DUID. . . . . : 00-01-00-01-26-91-63-19-78-84-3C-E5-7B-7A
  DNS Servers . . . . . : fe80::fa9a:78ff:fe63:1a3e%18
                           192.168.1.1
  NetBIOS over Tcpip. . . . . : Enabled

Ethernet adapter Bluetooth Network Connection 2:
  Media State . . . . . . . . . : Media disconnected
  Connection-specific DNS Suffix . . . . . : 
  Description . . . . . . . . . : Bluetooth Device (Personal Area Network) #2
  Physical Address. . . . . . . . . : 90-00-4E-D7-61-98
```

IPv4 Address در اصل همان آدرس مبدا در لایه transport است که مقدار آن هم برابر با ۱۹۲.۱۶۸.۱.۱۲۲ می باشد.

Default Gateway 192.168.1.1

آدرس فیزیکی مبدا در در بخش Ethernet adapter Bluetooth Network Connection نوشته شده:

Physical Address.....90-00-4E-D7-61-98

آدرس فیزیکی مقصد هم در جایی نوشته نشده است.

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

```
▼ Domain Name System (response)
  Transaction ID: 0x66d3
  > 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
  [Request In: 32190]
  [Time: 0.068309000 seconds]
```

تاپ مربوط به این کوئری از نوع A است.

در اصل این تاپ یکی از انواع Resource Record Types است که تاپ A در بین آنها به معنای Host Address است.

حال اگر یک query از نوع A باشد یعنی اینکه وظیفه دارد تا IPv4 Address و hostname را ذخیره کند تا در زمان مناسب آن را برگرداند (تا بتواند hostname را به IP address مپ کند)

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** انتخاب شده است؟ به نظر شما این درخواست DNS برای چه کاری استفاده شده است؟

```
▼ 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
      Name: 1.1.1.1.in-addr.arpa
      [Name Length: 20]
      [Label Count: 6]
      Type: PTR (domain name PoinTeR) (12)
      Class: IN (0x0001)
      [Response In: 6]
```

تاپ آن **PTR** است که در اصل این تاپ مشخص می‌کند که query درخواست شده، یک نوع DNS است.(یک رکورد DNS معکوس نامیده می‌شود) این query به اجزه می‌دهد که یک IP را بسازد و یک hostname برای آن دریافت کند. در واقع برای این استفاده می‌شود که اگر ما IP را داشته باشیم با این درخواست می‌خواهیم که اطلاعات بیشتری (مثل دامنه) کسب نماییم.

-
- سوال ۱۰: چه **type** های دیگری ممکن است وجود داشته باشد؟ سه مورد را یادداشت کنید.
- تایپ **AAAA** همان رکورد نوع A است اما با این تفاوت که ارتباط بین hostname و IPv6 address را ایجاد می‌کند.
 - تایپ **MX** در اصل رکورد MX پیام های ایمیل را به یک سوزور ایمیل خاص هدایت کرده که از یک هاست ایمیل تعیین شده در یک سرور دیگر به یک دامنه مرتبط می‌شود.
 - تایپ **TXT** اطلاعات قابل خواندن توسط ماشین را حمل می‌کند. (مثل داده‌های مربوط به رمزگذاری‌ها)(برای اضافه کردن هر گونه توضیح است)

سوال ۱: بعد از کلیک کردن روی OK چه اتفاقی می‌افتد؟ در بسته‌هایی که مشخص شده‌اند چه پروتکلهایی را مشاهده می‌کنید؟

در اصل با این کار تمام بسته‌هایی را که مبدأ و یا مقصدشان آدرس IP وارد شده می‌باشد را به ما نشان می‌دهد و فقط بسته‌هایی با پروتکل ICMP فرستاده و دریافت می‌شوند را می‌توان مشاهده کرد.(تایپ آن ۸ می‌باشد و TTL هم ۱ است)

سوال ۲: اولین بسته را انتخاب کنید. به بخش پروتکل ICMP بروید. مقدار type را مشخص کنید. به بخش مربوط به پروتکل IP بروید و مقدار TTL را یادداشت کنید.

در بخش Internet Control Message Protocol رفته و مقدار type را مشخص می‌کنیم که برابر با ۸ می‌باشد (تایپ پروتکل خواسته شده ping request است)

```
> Ethernet II, Src: HonHaiPr_d7:61:97 (90:00:4e:d7:61:97), Dst: HuaweiTe_63:1a:3e (f8:9a:78:63:1a:3e)
> Internet Protocol Version 4, Src: 192.168.1.122, Dst: 5.144.130.115
> Internet Control Message Protocol
  Type: 8 (Echo (ping) request)
  Code: 0
  Checksum: 0xf7f5 [correct]
  [Checksum Status: Good]
  Identifier (BE): 1 (0x0001)
  Identifier (LE): 256 (0x0100)
  Sequence Number (BE): 9 (0x0009)
  Sequence Number (LE): 2304 (0x0900)
  > [No response seen]
  > Data (64 bytes)
```

حال به بخش مربوط به پروتکل IP رفته و مقدار TTL برابر با ۱ می‌باشد.

```
> Frame 83602: 106 bytes on wire (848 bits), 106 bytes captured (848 bits) on interface \Device\NPF_{9C6049A1-2620-4E0C-B1FF-253414CD8B53}, id 0
> Ethernet II, Src: HonHaiPr_d7:61:97 (90:00:4e:d7:61:97), Dst: HuaweiTe_63:1a:3e (f8:9a:78:63:1a:3e)
> Internet Protocol Version 4, Src: 192.168.1.122, Dst: 5.144.130.115
  0100 .... = Version: 4
  .... 0101 = Header Length: 20 bytes (5)
  > Differentiated Services Field: 0x00 (DSGP: CS0, ECN: Not-ECT)
    Total Length: 92
    Identification: 0xa0d4 (41172)
    Flags: 0x00
    ...0 0000 0000 0000 = Fragment Offset: 0
  > Time to Live: 1
    Protocol: ICMP (1)
    Header Checksum: 0xcea7 [validation disabled]
    [Header checksum status: Unverified]
    Source Address: 192.168.1.122
    Destination Address: 5.144.130.115
> Internet Control Message Protocol
```

سوال ۱۳: به نظر شما هدف از این تغییر چیست؟ می‌توانید با مراجعه به هدف دستور tracert آن را شرح دهید.

این اعداد نشان‌دهنده‌ی شماره‌ی هر trace هستند. در اصل TTL با گذر از هر گره میانی یکی از آن کم شده و زمانیکه مقدار آن صفر شود همان گره ای است که یک بسته برای مبدأ می‌فرستد و دستور tracert به اینصورت عمل می‌کند که از TTL با مقدار ۱ شروع شده و افزایش می‌یابد تا به مقصد نهايی برسد و در نهايی تمام IP‌های گره‌های میانی به دست می‌ainد. به طور کل می‌توان گفت که اين دستور مسیری از داده‌ها را از يك نقطه از شبکه که به يك سرور معين می‌رسند، مشخص می‌کند.

سوال ۱۴: فیلتر ۶ == چه کاری انجام می‌دهد؟

عدد ۶ مربوط به پروتکل TCP می‌باشد. در واقع با آمدن این فیلتر تنها پروتکلهای TCP نمایش داده می‌شوند.

No.	Tl	Slowpan	Source	Destination	Protocol	Length	Info
29484	8807.516722		104.66.85.18	172.20.10.9	TCP	54	443 → 54294 [ACK] Seq=5820 Ack=348 Win=94720 Len=0
29485	8807.516722		104.66.85.18	172.20.10.9	TCP	54	443 → 54295 [ACK] Seq=5820 Ack=348 Win=94720 Len=0
29494	8807.567172		104.66.85.18	172.20.10.9	TCP	54	443 → 54292 [ACK] Seq=6110 Ack=871 Win=95744 Len=0
29499	8807.587249		172.20.10.9	142.250.181.170	TCP	66	54293 → 443 [SYN] Seq=0 Win=64249 Len=0 MSS=1460 WS=256 SACK_PERM=1
29500	8807.619238		142.250.27.188	172.20.10.9	TCP	66	5428 → 54297 [SYN, ACK] Seq=1 Ack=1 Win=65535 Len=0 MSS=1400 WS=256 SACK_PERM=1
29502	8807.619238		104.66.85.18	172.20.10.9	TCP	54	443 → 54296 [ACK] Seq=6110 Ack=871 Win=95744 Len=0
29503	8807.619238		104.66.85.18	172.20.10.9	TCP	54	443 → 54293 [ACK] Seq=6110 Ack=917 Win=95744 Len=0
29504	8807.619238		104.66.85.18	172.20.10.9	TCP	54	443 → 54291 [ACK] Seq=6110 Ack=897 Win=95744 Len=0
29505	8807.619238		104.66.85.18	172.20.10.9	TCP	54	443 → 54294 [ACK] Seq=6110 Ack=932 Win=95744 Len=0
29506	8807.619238		104.66.85.18	172.20.10.9	TCP	54	443 → 54295 [ACK] Seq=6110 Ack=915 Win=95744 Len=0
29507	8807.619678		172.20.10.9	142.250.27.188	TCP	54	54297 → 5228 [ACK] Seq=1 Ack=1 Win=131584 Len=0
29523	8807.645080		142.250.181.170	172.20.10.9	TCP	66	54293 → 443 [SYN, ACK] Seq=0 Ack=1 Win=65535 Len=0 MSS=1400 SACK_PERM=1 WS=256
29524	8807.645271		172.20.10.9	142.250.181.170	TCP	54	54298 → 443 [ACK] Seq=1 Ack=871 Win=95744 Len=0
29529	8807.664206		172.20.10.9	104.66.85.18	TCP	54	54292 → 443 [ACK] Seq=871 Ack=6521 Win=130560 Len=0
29530	8807.680050		142.250.181.170	172.20.10.9	TCP	54	443 → 54298 [ACK] Seq=1 Ack=596 Win=94720 Len=0
29540	8807.710152		172.20.10.9	104.66.85.18	TCP	54	54294 → 443 [ACK] Seq=932 Ack=6521 Win=130560 Len=0
29541	8807.713220		172.20.10.9	104.66.85.18	TCP	54	54295 → 443 [ACK] Seq=915 Ack=6522 Win=130560 Len=0
29542	8807.713314		172.20.10.9	104.66.85.18	TCP	54	54291 → 443 [ACK] Seq=897 Ack=6522 Win=130560 Len=0
29545	8807.772506		172.20.10.9	104.66.85.18	TCP	54	54293 → 443 [ACK] Seq=917 Ack=6522 Win=130560 Len=0
29546	8807.780937		142.250.27.188	172.20.10.9	TCP	54	5228 → 54297 [ACK] Seq=1 Ack=518 Win=66816 Len=0
29548	8807.785198		142.250.27.188	172.20.10.9	TCP	1454	5228 → 54297 [PSH, ACK] Seq=1401 Ack=518 Win=66816 Len=1400 [TCP segment of a reassembled PDU]
29549	8807.785270		172.20.10.9	142.250.27.188	TCP	54	54297 → 5228 [ACK] Seq=518 Ack=2801 Win=131584 Len=0
29550	8807.785524		142.250.27.188	172.20.10.9	TCP	1118	[TCP Previous segment not captured] 5228 → 54297 [PSH, ACK] Seq=5001 Ack=518 Win=66816 Len=1064 [TCP segment of a reassembled PDU]
29551	8807.785524		142.250.27.188	172.20.10.9	TCP	1454	[TCP Out-Of-Order] 5228 → 54297 [ACK] Seq=2801 Ack=518 Win=66816 Len=1400 [TCP segment of a reassembled PDU]
29552	8807.785647		172.20.10.9	142.250.27.188	TCP	66	[TCP Dup ACK 29549@1] 54297 → 5228 [ACK] Seq=518 Ack=2801 Win=131584 Len=0 SLE=5601 SRE=6665
29553	8807.785746		172.20.10.9	142.250.27.188	TCP	66	54297 → 5228 [ACK] Seq=518 Ack=4201 Win=131584 Len=0 SLE=5601 SRE=6665
29554	8807.785985		142.250.27.188	172.20.10.9	TCP	1454	[TCP Out-Of-Order] 5228 → 54297 [PSH, ACK] Seq=4201 Ack=518 Win=66816 Len=1400
29555	8807.786073		172.20.10.9	142.250.27.188	TCP	54	54297 → 5228 [ACK] Seq=518 Ack=6665 Win=131584 Len=0
29564	8807.876677		142.250.181.170	172.20.10.9	TCP	54	443 → 54298 [ACK] Seq=213 Ack=668 Win=94720 Len=0
29562	8807.931165		172.20.10.9	52.143.87.28	TCP	54	54286 → 443 [ACK] Seq=1323 Ack=2632 Win=131328 Len=0