نام و نام خانوادگی: **امیرحسین علی‌بخشی**
شماره‌ی دانشجویی: **۹۷۳۱۰۹۶**

آشنایی با وایرشارک

استاد: **خانم نقی‌پور**
درس: **آزمایشگاه شبکه های کامپیوتری**

سوال۱

پروتکل هایی که مشاهده شدند:

TCP – TLSv1.2 – UDP – DNS – NBNS

سوال۲

بسته ای که انتخاب کردیم:

No.	Time	Source	Destination	Protocol	Length	Info
1470	58.229293	8.8.8.8	192.168.1.4	DNS	181	Standard query response 0x3f82 A accour

```
> Frame 1470: 181 bytes on wire (1448 bits), 181 bytes captured (1448 bits) on interface \Device\NPF_{BA2F9E69-826F-4485-B087-25BAAD5
> Ethernet II, Src: ASUSTekC_66:3b:b4 (30:5a:3a:66:3b:b4), Dst: IntelCor_8d:fb:49 (f4:d1:08:8d:fb:49)
> Internet Protocol Version 4, Src: 8.8.8.8, Dst: 192.168.1.4
> User Datagram Protocol, Src Port: 53, Dst Port: 59973
> Domain Name System (response)
```

پروتکل لایه ها:

Application: **DNS**
Transport: **UDP**
Network: **IPv4**
Data Link: **Ethernet II**

ترتیب بیت ها: ترتیب قرار گیری بیت ها به ترتیب لایه ها میباشد . یعنی بیت های اول مربوط به لایه ی اول، دسته بیت های دوم مربوط به لایه ی دوم و به همین ترتیب برای سایر لایه ها میباشد. در واقع در هر لایه، header آن لایه بهpayload قبلی ها اضافه میشود.

اندازه فریم: Frame Length: 181 bytes (1448 bits)

اندازه لایه سوم: Total Length: 167

سوال۳

این بسته به عنوان مثال لایه application ندارد.

```
355 15.816574    23.58.223.186    192.168.1.4    TCP    54 80 → 9811 [ACK] Seq=100182 Ack=55505 Wi
> Frame 355: 54 bytes on wire (432 bits), 54 bytes captured (432 bits) on interface \Device\NPF_{BA2F9E69-826F-4485-B087-25BAAD510D7D
> Ethernet II, Src: ASUSTekC_66:3b:b4 (30:5a:3a:66:3b:b4), Dst: IntelCor_8d:fb:49 (f4:d1:08:8d:fb:49)
> Internet Protocol Version 4, Src: 23.58.223.186, Dst: 192.168.1.4
> Transmission Control Protocol, Src Port: 80, Dst Port: 9811, Seq: 100182, Ack: 55505, Len: 0
```

یا این بسته APR لایه transport ندارد.

```
1107 41.516436   IntelCor_8d:fb:49   ASUSTekC_66:3b:b4   ARP   42 192.168.1.4 is at f4:d1:08:8d:fb:49
> Frame 1107: 42 bytes on wire (336 bits), 42 bytes captured (336 bits) on interface \Device\NPF_{BA2F9E69-826F-4485-B087-25BAAD510D7
> Ethernet II, Src: IntelCor_8d:fb:49 (f4:d1:08:8d:fb:49), Dst: ASUSTekC_66:3b:b4 (30:5a:3a:66:3b:b4)
> Address Resolution Protocol (reply)
```

سوال۴

```
2835 115.768863   23.58.223.186   192.168.1.4   TCP   54 80 → 9811 [ACK] Seq=612151 Ack=592095 W
> Frame 2835: 54 bytes on wire (432 bits), 54 bytes captured (432 bits) on interface \Device\NPF_{BA2F9E69-826F-4485-B087-25BAAD510D7
> Ethernet II, Src: ASUSTekC_66:3b:b4 (30:5a:3a:66:3b:b4), Dst: IntelCor_8d:fb:49 (f4:d1:08:8d:fb:49)
v Internet Protocol Version 4, Src: 23.58.223.186, Dst: 192.168.1.4
    0100 .... = Version: 4
    .... 0101 = Header Length: 20 bytes (5)
  > Differentiated Services Field: 0x00 (DSCP: CS0, ECN: Not-ECT)
    Total Length: 40
    Identification: 0x4df5 (19957)
  > Flags: 0x40, Don't fragment
    Fragment Offset: 0
    Time to Live: 52
    Protocol: TCP (6)
    Header Checksum: 0x403a [validation disabled]
    [Header checksum status: Unverified]
```

سوال۵

برای TCP

```
v Transmission Control Protocol, Src Port: 80, Dst Port: 9811, Seq: 612151, Ack: 592095, Len: 0
    Source Port: 80
    Destination Port: 9811
    Checksum: 0x729d [unverified]
    [Checksum Status: Unverified]
```

پورت مبدا ۸۰ و پورت مقصد ۹۸۱۱ میباشد.

پورت ۸۰ مربوط به HTTP است.

برای UDP

```
v User Datagram Protocol, Src Port: 57621, Dst Port: 57621
    Source Port: 57621
    Destination Port: 57621
    Checksum: 0xa518 [unverified]
    [Checksum Status: Unverified]
```

پورت مبدا ۵۷۶۲۱ و پورت مقصد ۵۷۶۲۱ میباشد.

سوال ۶

```
Wireless LAN adapter Wi-Fi:

   Connection-specific DNS Suffix  . :
   Description . . . . . . . . . . . : Intel(R) Dual Band Wireless-AC 8265
   Physical Address. . . . . . . . . : F4-D1-08-8D-FB-49
   DHCP Enabled. . . . . . . . . . . : Yes
   Autoconfiguration Enabled . . . . : Yes
   Link-local IPv6 Address . . . . . : fe80::2dd7:ef8b:8a22:36cd%21(Preferred)
   IPv4 Address. . . . . . . . . . . : 192.168.1.4(Preferred)
   Subnet Mask . . . . . . . . . . . : 255.255.255.0
```

از آنجا که IP سیستم ما برابر است با ۱۹۲.۱۶۸.۱.۴ ، بسته ای که انتخاب میکنیم باید از سمت این IP فرستاده شده باشد.

```
1 0.000000    192.168.1.4    46.224.1.220    DNS    106 Standard query 0xfe24 TXT aqjsavkyuz7e7
> Frame 5: 73 bytes on wire (584 bits), 73 bytes captured (584 bits) on interface \Device\NPF_{BA2F9E69-826F-4485-B087-25BAAD510D7D},
> Ethernet II, Src: IntelCor_8d:fb:49 (f4:d1:08:8d:fb:49), Dst: ASUSTekC_66:3b:b4 (30:5a:3a:66:3b:b4)
> Internet Protocol Version 4, Src: 192.168.1.4, Dst: 46.224.1.220
> User Datagram Protocol, Src Port: 59859, Dst Port: 53
> Domain Name System (query)
```

پروتکل لایه transport پروتکل UDP است. همچنین IP مقصد برابر است با ۴۶.۲۲۴.۱.۲۲۰

آدرس مبدا و مقصد در سرآیند لایه دوم به صورت زیر میباشد:

```
v Ethernet II, Src: IntelCor_8d:fb:49 (f4:d1:08:8d:fb:49), Dst: ASUSTekC_66:3b:b4 (30:5a:3a:66:3b:b4)
  > Destination: ASUSTekC_66:3b:b4 (30:5a:3a:66:3b:b4)
  > Source: IntelCor_8d:fb:49 (f4:d1:08:8d:fb:49)
```

سوال ۷

آدرس ۱۹۲.۱۶۸.۱.۴ آدرس سیستم ما بود که در عکس بالای همین صفحه قابل در بخش IPv4 Address مشاهده است.

سوال ۸

از همان بسته قسمت قبل استفاده میکنیم:

```
v Domain Name System (query)
    Transaction ID: 0x742c
  > Flags: 0x0100 Standard query
    Questions: 1
    Answer RRs: 0
    Authority RRs: 0
    Additional RRs: 0
  v Queries
    v i4.c.eset.com: type A, class IN
        Name: i4.c.eset.com
        [Name Length: 13]
        [Label Count: 4]
        Type: A (Host Address) (1)
        Class: IN (0x0001)
```

تایپ این Query، A است که به آن Address mapping record(همچنین DNS host record)گفته

میشود که از آن برای گرفتن آدرس IPV4 مقصد که ۳۲ بیتی است استفاده میشود .(برای map کردن hostname ها به IP آن ها کاربرد دارد) . همچنین از آن در DNSBLs و ذخیره سازی subnet mask ها در RFC 1101 استفاده میشود .

سوال۹

```
Domain Name System (query)
    Transaction ID: 0x0002
  > Flags: 0x0100 Standard query
    Questions: 1
    Answer RRs: 0
    Authority RRs: 0
    Additional RRs: 0
  v Queries
    v 1.1.1.1.in-addr.arpa: type PTR, class IN
        Name: 1.1.1.1.in-addr.arpa
        [Name Length: 20]
        [Label Count: 6]
        Type: PTR (domain name PoinTeR) (12)
        Class: IN (0x0001)
```

تایپ این Query، PTR است . این تایپ پوینتری به canonical name میباشد .

سوال۱۰

تایپ های زیادی وجود دارند که تعدادی از آن ها به شرح زیر است :

LOC منطقه ی جغرافیایی مرتبط با یک domain name را مشخص میکند .

RP اطلاعاتی درباره ی شخص یا اشخاصی که مسئولیت domain را دارند است که معمولا آن اطلاعات شامل ادرس ایمیلی که @ آن با a جایگزین شده است میباشد .

HINFO پاسخ هایی با سایز مینیمال برای dns query هایی با تایپ QTYPE=ANY تامین میکند.

سوال۱۱

```
C:\Users\Asus>tracert p30download.com

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

  1     1 ms    <1 ms    <1 ms  192.168.1.1
  2    23 ms    22 ms    24 ms  10.255.255.255
  3    24 ms    23 ms    24 ms  10.234.198.193
  4    23 ms    23 ms    22 ms  10.234.198.114
  5    24 ms    23 ms    23 ms  10.234.198.109
  6    24 ms    22 ms    23 ms  10.234.198.49
  7    24 ms    53 ms    24 ms  172.17.132.17
  8    24 ms    26 ms    32 ms  10.202.1.5
  9     *        *        *     Request timed out.
 10    27 ms    31 ms    25 ms  5-144-130-115.static.hostiran.name [5.144.130.115]

Trace complete.
```

بعد از زدن ok بسته ها با فیلتری که در filter مشخص کردیم نمایش داده میشوند . برای مثال بنا به دستور کار ما بسته هایی را انتخاب کردیم که IP مبدا یا مقصد آن ها ، ۵.۱۴۴.۱۳۰.۱۱۵ که IP مربوط به سایت مورد نظر است نمایش داده میشوند .پس از طی کردن گام های دستور کار ، فیلتر بدین صورت میباشد :

ip.addr == ۵.۱۴۴.۱۳۰.۱۱۵

ip.addr == 5.144.130.115

No.	Time	Source	Destination	Protocol	Length	Info
390	2.719963	192.168.1.4	5.144.130.115	ICMP	106	Echo (ping) request id=0x0001, seq=52/133
391	2.721017	192.168.1.1	192.168.1.4	ICMP	134	Time-to-live exceeded (Time to live exceede
392	2.721574	192.168.1.4	5.144.130.115	ICMP	106	Echo (ping) request id=0x0001, seq=53/135
393	2.722313	192.168.1.1	192.168.1.4	ICMP	134	Time-to-live exceeded (Time to live exceede
394	2.722778	192.168.1.4	5.144.130.115	ICMP	106	Echo (ping) request id=0x0001, seq=54/138
395	2.723473	192.168.1.1	192.168.1.4	ICMP	134	Time-to-live exceeded (Time to live exceede
757	8.289785	192.168.1.4	5.144.130.115	ICMP	106	Echo (ping) request id=0x0001, seq=55/140
759	8.313056	10.255.255.255	192.168.1.4	ICMP	70	Time-to-live exceeded (Time to live exceede
760	8.314778	192.168.1.4	5.144.130.115	ICMP	106	Echo (ping) request id=0x0001, seq=56/143
761	8.336819	10.255.255.255	192.168.1.4	ICMP	70	Time-to-live exceeded (Time to live exceede
762	8.338336	192.168.1.4	5.144.130.115	ICMP	106	Echo (ping) request id=0x0001, seq=57/145
764	8.362996	10.255.255.255	192.168.1.4	ICMP	70	Time-to-live exceeded (Time to live exceede
947	13.901178	192.168.1.4	5.144.130.115	ICMP	106	Echo (ping) request id=0x0001, seq=58/148
948	13.925362	10.234.198.193	192.168.1.4	ICMP	70	Time-to-live exceeded (Time to live exceede

تمام پروتکل ها ICMP میباشد.

سوال ۱۲

```
Internet Control Message Protocol
    Type: 8 (Echo (ping) request)
```

حال به بخش IP میرویم:

```
Internet Protocol Version 4, Src: 192.168.1.4, 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: 0x4c0f (19471)
  > Flags: 0x00
    Fragment Offset: 0
  v Time to Live: 1
    > [Expert Info (Note/Sequence): "Time To Live" only 1]
```

روی قسمت مبدا کلیک میکنیم که بسته ها بر اساس آنها مرتب شوند و سپش به سراغ IP سیستم خودمان میرویم:

No.	Time	Source	Destination	Protocol	Length	Info
1853	36.559037	192.168.1.4	5.144.130.115	ICMP	106	Echo (ping) request id=0x0001, seq=72/184
1847	36.504365	192.168.1.4	5.144.130.115	ICMP	106	Echo (ping) request id=0x0001, seq=71/181
1839	36.478689	192.168.1.4	5.144.130.115	ICMP	106	Echo (ping) request id=0x0001, seq=70/179
1143	30.851310	192.168.1.4	5.144.130.115	ICMP	106	Echo (ping) request id=0x0001, seq=69/176
1141	30.827450	192.168.1.4	5.144.130.115	ICMP	106	Echo (ping) request id=0x0001, seq=68/174
1139	30.801513	192.168.1.4	5.144.130.115	ICMP	106	Echo (ping) request id=0x0001, seq=67/171
1036	25.170729	192.168.1.4	5.144.130.115	ICMP	106	Echo (ping) request id=0x0001, seq=66/168
1034	25.145551	192.168.1.4	5.144.130.115	ICMP	106	Echo (ping) request id=0x0001, seq=65/166
1032	25.119678	192.168.1.4	5.144.130.115	ICMP	106	Echo (ping) request id=0x0001, seq=64/163
1002	19.559172	192.168.1.4	5.144.130.115	ICMP	106	Echo (ping) request id=0x0001, seq=63/161
1000	19.533890	192.168.1.4	5.144.130.115	ICMP	106	Echo (ping) request id=0x0001, seq=62/158
998	19.508805	192.168.1.4	5.144.130.115	ICMP	106	Echo (ping) request id=0x0001, seq=61/156
951	13.951832	192.168.1.4	5.144.130.115	ICMP	106	Echo (ping) request id=0x0001, seq=60/153
949	13.926896	192.168.1.4	5.144.130.115	ICMP	106	Echo (ping) request id=0x0001, seq=59/151
947	13.901178	192.168.1.4	5.144.130.115	ICMP	106	Echo (ping) request id=0x0001, seq=58/148
762	8.338336	192.168.1.4	5.144.130.115	ICMP	106	Echo (ping) request id=0x0001, seq=57/145
760	8.314778	192.168.1.4	5.144.130.115	ICMP	106	Echo (ping) request id=0x0001, seq=56/143

سوال ۱۳

در این بسته ها TTL از مقدار ۱۰ تا ۱ میباشد زیرا همانگونه که در بخش tracert مشاهده کردیم این عمل در ۱۰ گام انجام شد. در هر گام ۳ بسته وجود دارد، یعنی در کل ۳۰ بسته وجود داشت که هر ۳ تای آنها TTL یکی از اعداد ۱ تا ۱۰ را به طور مشابه دارند.

در هر گامی که یک بسته طی میکند، یک واحد از TTL آن کاسته میشود و در صورت صفر شدن آن، بسته از بستر شبکه drop شده و باید مجددا آن را ارسال کنیم.

سوال ۱۴

بسته ها را بر اساس پروتکل انتخاب میکنیم. که 6 بیانگر IPv6 میباشد. قسمت مشترک تمامی نتایج این فیلترینگ قسمت زیر میباشد:

```
> Frame 59176: 346 bytes on wire (2768 bits), 346 bytes captured (2768 bits) on interface \Device\NPF_{BA2F9E69-826F-4485-B087-25BAAD
> Ethernet II, Src: ASUSTekC_66:3b:b4 (30:5a:3a:66:3b:b4), Dst: IntelCor_8d:fb:49 (f4:d1:08:8d:fb:49)
v Internet Protocol Version 4, Src: 50.21.176.89, Dst: 192.168.1.4
    0100 .... = Version: 4
    .... 0101 = Header Length: 20 bytes (5)
  > Differentiated Services Field: 0x00 (DSCP: CS0, ECN: Not-ECT)
    Total Length: 332
    Identification: 0x9a00 (39424)
  > Flags: 0x40, Don't fragment
    Fragment Offset: 0
    Time to Live: 45
    Protocol: TCP (6)
    Header Checksum: 0x0e91 [validation disabled]
    [Header checksum status: Unverified]
    Source Address: 50.21.176.89
    Destination Address: 192.168.1.4
> Transmission Control Protocol, Src Port: 554, Dst Port: 10626, Seq: 8001485, Ack: 5133729, Len: 292
```