آزمایشگاه شبکه های کامپیوتری

آزمایش دوم

تهیه کننده:

سارا تاجرنیا

استاد مربوطه:

استاد صادقیان

۱۴۰۱/۱/۳۰

۳- آشنایی با نرم‌افزار Wireshark

۳-۱- هدف آزمایش

هدف از این آزمایش آشنایی با نرم‌افزار Wireshark و بررسی پروتکل‌ها در لایه مختلف معماری TCP/IP است.

سوال ۱: به یک بخش دلخواه از بسته‌های شنود شده مراجعه کنید. چه پروتکل‌هایی را مشاهده می‌کنید. لیست آن‌ها را یادداشت کنید.

لیست پروتکل های دریافت شده شامل موارد زیر است:

- TCP
- UDP
- DNS
- ICMP
- SSDP
- TLSv1
- TLSv1.2
- TLSv1.3
- MDNS
- IGMPv2
- SSL
- ARP

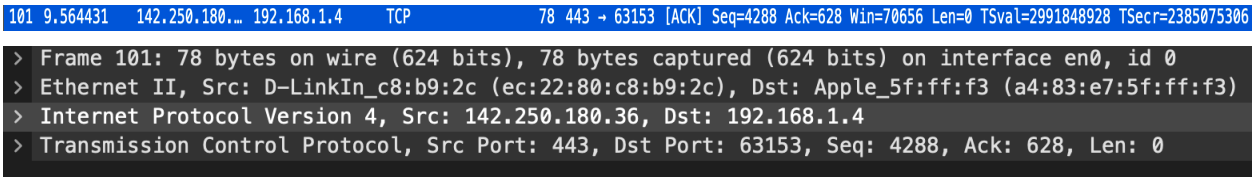
برای برخی مثال های زیر:

2.062732	192.168.1.4	17.248.173.68	TCP	78	[TCP Retransmission] [TCP Port numbers reused] 63150 → 443 [SYN] Seq=0 Win=65535
3.000614	192.168.1.4	217.218.127.127	DNS	82	Standard query 0x7d87 HTTPS api.apple-cloudkit.com
3.000829	192.168.1.4	217.218.127.127	DNS	82	Standard query 0x4f48 A api.apple-cloudkit.com
3.004242	D-LinkIn_c8:…	Apple_5f:ff:f3	ARP	42	192.168.1.1 is at ec:22:80:c8:b9:2c
3.028168	217.218.127.…	192.168.1.4	ICMP	110	Destination unreachable (Port unreachable)
3.198517	192.168.1.4	17.248.173.68	TLSv1	583	Client Hello
3.446697	192.168.1.4	52.232.209.85	TLSv1.2	486	Application Data
4.740048	192.168.1.4	224.0.0.251	MDNS	225	Standard query response 0x0000 TXT, cache flush NSEC, cache flush sara’s MacBook
4.740126	fe80::10e6:7…	ff02::fb	MDNS	245	Standard query response 0x0000 TXT, cache flush NSEC, cache flush sara’s MacBook
8.742654	192.168.1.4	142.250.180.36	TLSv1.3	583	Client Hello
21.566975	192.168.1.1	239.255.255.250	SSDP	375	NOTIFY * HTTP/1.1
21.567440	192.168.1.1	239.255.255.250	SSDP	305	NOTIFY * HTTP/1.1

سوال ۲: یک بسته را به‌دلخواه انتخاب کنید. مشخص کنید که چه پروتکل‌هایی در لایه‌های مختلف آن استفاده شده است. ترتیب قرارگیری بیت‌ها داخل بسته چه ارتباطی با لایه‌های مختلف دارد؟ اندازه فریم لایه دو این بسته چقدر است؟ اندازه بسته لایه ۳ چقدر است؟

1) این بسته دارای پروتکل TCP است و در پروتکل های مختلفی در لایه های آن قرار دارند.

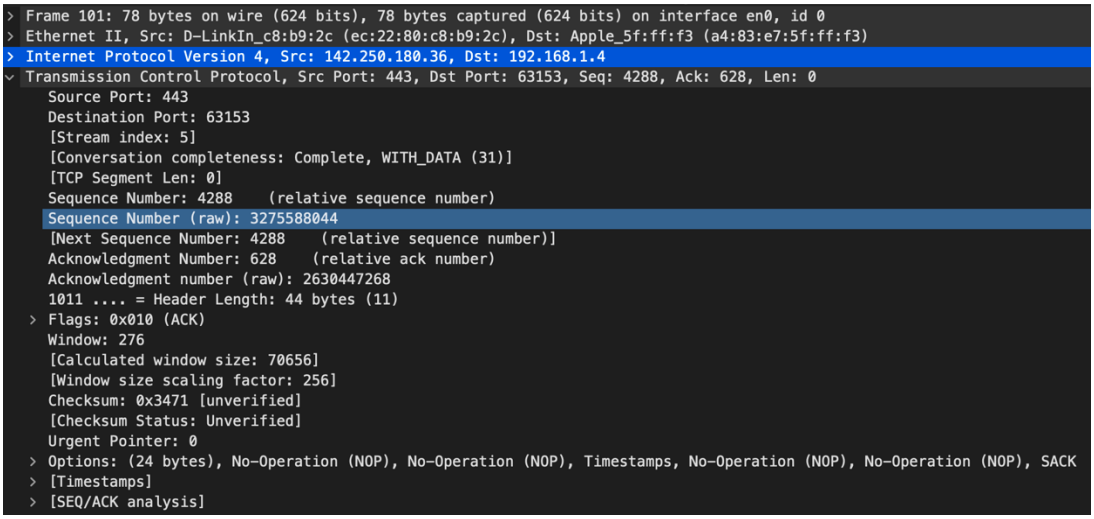
- Transmission Control Protocol(TCP) در لایه transport
- Transmission Control Protocol(TCP) در لایه application
- Internet Protocol Version4 (IPv4) در لایه network



2) ترتیب قرارگیری بیت ها به ترتیب لایه هاست به طوری که بیت اول برای لایه اول و...

3) اندازه frame برابر 101 و بایت آن برابر 78 است.

4)



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

همان طور که از عکس هم پیداست بسته ARP از هیچ یک از پروتکل هایی که گفته شد استفاده نکرده و فقط ARP مخصوص خودش را دارد.

```
3.004242    D-LinkIn_c8:… Apple_5f:ff:f3   ARP                 42 192.168.1.1 is at ec:22:80:c8:b9:2c
```

```
> Frame 11: 42 bytes on wire (336 bits), 42 bytes captured (336 bits) on interface en0, id 0
> Ethernet II, Src: D-LinkIn_c8:b9:2c (ec:22:80:c8:b9:2c), Dst: Apple_5f:ff:f3 (a4:83:e7:5f:ff:
> Address Resolution Protocol (reply)
```

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

```
21.583163   192.168.1.1    239.255.255.250 SSDP              362 NOTIFY * HTTP/1.1
```

```
Header Checksum: 0x38bb [validation disabled]
[Header checksum status: Unverified]
Source Address: 192.168.1.1
Destination Address: 239.255.255.250
er Datagram Protocol, Src Port: 1900, Dst Port: 1900
mple Service Discovery Protocol
```

```
01 5c cb 32 00 00 04 11  38 bb c0 a8 01 01 ef ff   ·\·2···· 8······
ff fa 07 6c 07 6c 01 48  08 4c 4e 4f 54 49 46 59   ···l·l·H ·LNOTIFY
20 2a 20 48 54 54 50 2f  31 2e 31 20 0d 0a 48 4f    * HTTP/ 1.1 ··HO
53 54 3a 20 32 33 39 2e  32 35 35 2e 32 35 35 2e   ST: 239. 255.255.
32 35 30 3a 31 39 30 30  0d 0a 43 41 43 48 45 2d   250:1900 ··CACHE-
43 4f 4e 54 52 4f 4c 3a  20 6d 61 78 2d 61 67 65   CONTROL:  max-age
3d 33 30 30 30 0d 0a 4c  4f 43 41 54 49 4f 4e 3a   =3000··L OCATION:
20 68 74 74 70 73 3a 2f  2f 31 39 32 2e 31 36 38    https:/ /192.168
2e 31 2e 31 3a 36 35 37  39 2f 64 65 76 69 63 65   .1.1:657 9/device
64 65 73 63 2e 78 6d 6c  0d 0a 53 45 52 56 45 52   desc.xml ··SERVER
```

بسته مشخص شده در قسمت Internet Protocol(IP) دارای Harder Checksum: 0x38bb بود که بایت مشخص کننده آن هم نمایش داده شده است.

سوال ۵: از یکی از بسته‌ها 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 می‌کند؟ Checksum مربوط به پروتکل‌های TCP و UDP را مشخص کنید.

در TCP :

```
27.481894   192.168.1.4    142.250.180.36   TCP              86 [TCP Window Update] 63153 → 443
```

```
Source Port: 63153
Destination Port: 443
```

```
Checksum: 0x98e7 [unverified]
[Checksum Status: Unverified]
```

در UDP :

```
79.910047   192.168.1.4    192.168.1.255    UDP              86 57621 → 57621 Len=44
```

```
Source Port: 57621
Destination Port: 57621
```

```
Checksum: 0x3e67 [unverified]
[Checksum Status: Unverified]
```

پورت مبدا و مقصد که به ترتیب souce port و destination port نشان دهنده آنها است. در پورت مبدا اعداد 63153 و 57621 را داریم که از طریق client تولید میشوند و دندوم اند، پورت مقصد هم با اعداد 443 و 57621 پورت های مخصوص سرور اند که برای ارتباط client به server مورد استفاده قرار میگیرند.

سوال ۶: یکی از بسته‌ها 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.

با استفاده از دستوری که گفته شد فهمیدم که IP لپ تاپ برابر 192.168.1.4 است پس بسته زیر را انتخاب کردم.

```
201 60.528969   192.168.1.4    5.200.200.200    DNS                75 Standard query
```

پروتکل لایه transport آن از نوع User Datagram Protocol(UDP) است.

```
Internet Protocol Version 4, Src: 192.168.1.4, Dst: 5.200.200.200
```

در لایه دوم آدرس مبدا و مقصد به همان طور که در شکل مشخص است به صورت زیر هستند:

Source: 192.168.1.4

Destination: 5.200.200.200

سوال ۷: کدام‌یک از آدرس‌های پیدا کرده در بخش قبل را می‌توانید در خروجی دستورall/ ipconfig مشاهده کنید؟

همان طور که در فیلم گفته شد با این دستور آدرس IPv4 Address مشخص میشود. البته از آنجایی که برای من این دستور کار نمیکرد از توی setting این آدرس را پیدا کردم، که همان آدرس فرستنده یا source در قسمت قبل است.

```
IPv4 Address:  192.168.1.4
Subnet Mask:  255.255.255.0
      Router:  192.168.1.1
```

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؟

```
387 767.750439 192.168.1.4   5.200.200.200   DNS          70 Standard query 0x7caa A google.com
```

```
Domain Name System (query)
   Transaction ID: 0x7caa
 > 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
       [Name Length: 10]
       [Label Count: 2]
       Type: A (Host Address) (1)
       Class: IN (0x0001)
```

دارای type A است که این درخواست DNS برای وصل کردن hostname به ip مقصد است.

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؟

```
38.210002   192.168.1.4   5.200.200.200   DNS          86 Standard query 0xf13b
```

```
Domain Name System (query)
   Transaction ID: 0xf13b
 > Flags: 0x0100 Standard query
   Questions: 1
   Answer RRs: 0
   Authority RRs: 0
   Additional RRs: 0
 v Queries
   v b._dns-sd._udp.domain.name: type PTR, class IN
       Name: b._dns-sd._udp.domain.name
       [Name Length: 26]
       [Label Count: 5]
       Type: PTR (domain name PoinTeR) (12)
       Class: IN (0x0001)
```

در اینجا type از نوع PTR است که از این رو که با دستور lookup میخواهیم server را به client وصل کنیم و دامنه ای را به client برسانیم پس type به صورت PTR در نظر گرفته میشود.

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

- TXT
- MG
- HTTPS

```
38.657355   5.200.200.200 192.168.1.4      DNS                 308 Standard query
```

```
Domain Name System (response)
   Transaction ID: 0xd658
 > Flags: 0x8180 Standard query response, No error
   Questions: 1
   Answer RRs: 4
   Authority RRs: 1
   Additional RRs: 0
 ⌄ Queries
   ⌄ gsp-ssl.ls.apple.com: type HTTPS, class IN
        Name: gsp-ssl.ls.apple.com
        [Name Length: 20]
        [Label Count: 4]
        Type: HTTPS (HTTPS Specific Service Endpoints) (65)
        Class: IN (0x0001)
```

از آنجایی که سرعت وای فای بسیار پایین بود نتوانستم مثال های دیگر را نشان دهم.

سوال ۱۱: بعد از کلیک کردن بر روی OK چه اتفاقی می‌افتد؟ در بسته‌هایی که مشخص شده‌اند چه پروتکل‌هایی را مشاهده می‌کنید؟

از آنجایی که دستور گفته شده در لپ تاپ من کار نمیکرد، در تمام بسته هایی که نشان داده شده است مبدا یا مقصد آن برابر ip داده شده است که در اینجا ip ماست که برابر 192.168.1.4 است.

در ادامه اگر ip p30download.com را وارد کنیم پس از ok کردن پروتکل بسته ها به صورت ICMP نشان داده میشوند.

ip.addr == 5.144.130.115

```
  7 2.562284    192.168.1.1    192.168.1.4      ICMP
  9 2.564694    192.168.1.1    192.168.1.4      ICMP
 11 2.589761    2.177.128.1    192.168.1.4      ICMP
131 32.623748   2.177.128.1    192.168.1.4      ICMP
133 32.649272   2.177.128.1    192.168.1.4      ICMP
135 32.674572   10.22.26.102   192.168.1.4      ICMP
137 32.701567   10.22.26.102   192.168.1.4      ICMP
139 32.736293   10.22.26.102   192.168.1.4      ICMP
141 32.764592   10.22.26.101   192.168.1.4      ICMP
143 32.790679   10.22.26.101   192.168.1.4      ICMP
145 32.815208   10.22.26.101   192.168.1.4      ICMP
147 32.841588   10.22.26.113   192.168.1.4      ICMP
```

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.

```
7  2.562284    192.168.1.1    192.168.1.4      ICMP                70
```

```
Internet Control Message Protocol
   Type: 11 (Time-to-live exceeded)
   Code: 0 (Time to live exceeded in transit)
   Checksum: 0x3ee1 [correct]
   [Checksum Status: Good]
   Unused: 00000000
```

```
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: 52
   Identification: 0x8c1e (35870)
>  Flags: 0x00
   ...0 0000 0000 0000 = Fragment Offset: 0
>  Time to Live: 0
```

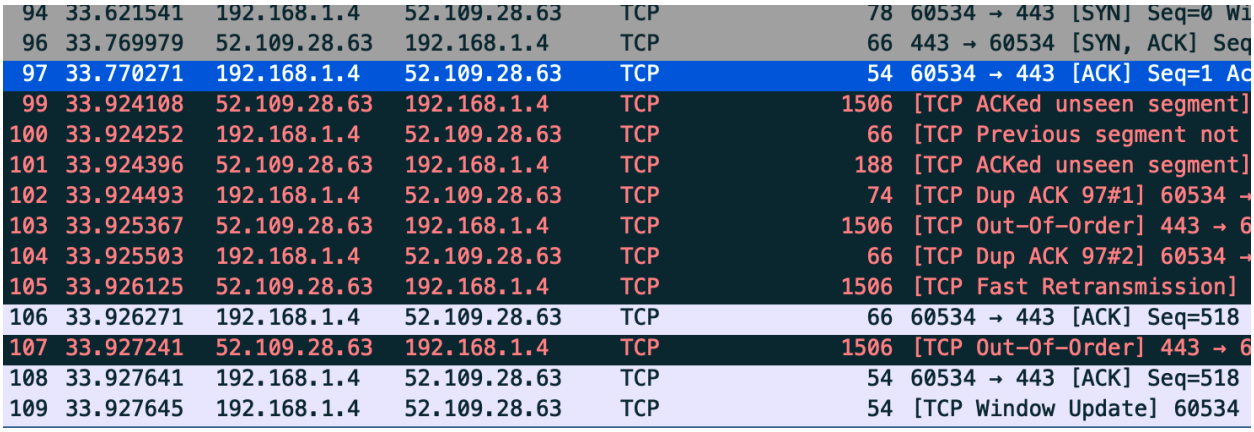
مقدار type = 11 و مقدار Time To Live(TTL) = 0 است.

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

با استفاده از دستور tracert میفهمیم TTL در ابتدا 0 بوده و در گذر زمان افزایش میابد. هدف از این تغییرات این است که بسته های موجود در گذر زمان افزایش میابد.

۷. از بخش فیلتر، مقدار فیلتر را به دستور ip.proto == 6 تغییر دهید.

سوال ۱۴: این فیلتر چه کاری انجام می‌دهد؟



94	33.621541	192.168.1.4	52.109.28.63	TCP	78	60534 → 443 [SYN] Seq=0 Wi
96	33.769979	52.109.28.63	192.168.1.4	TCP	66	443 → 60534 [SYN, ACK] Seq
97	33.770271	192.168.1.4	52.109.28.63	TCP	54	60534 → 443 [ACK] Seq=1 Ac
99	33.924108	52.109.28.63	192.168.1.4	TCP	1506	[TCP ACKed unseen segment]
100	33.924252	192.168.1.4	52.109.28.63	TCP	66	[TCP Previous segment not
101	33.924396	52.109.28.63	192.168.1.4	TCP	188	[TCP ACKed unseen segment]
102	33.924493	192.168.1.4	52.109.28.63	TCP	74	[TCP Dup ACK 97#1] 60534 →
103	33.925367	52.109.28.63	192.168.1.4	TCP	1506	[TCP Out-Of-Order] 443 → 6
104	33.925503	192.168.1.4	52.109.28.63	TCP	66	[TCP Dup ACK 97#2] 60534 →
105	33.926125	52.109.28.63	192.168.1.4	TCP	1506	[TCP Fast Retransmission]
106	33.926271	192.168.1.4	52.109.28.63	TCP	66	60534 → 443 [ACK] Seq=518
107	33.927241	52.109.28.63	192.168.1.4	TCP	1506	[TCP Out-Of-Order] 443 → 6
108	33.927641	192.168.1.4	52.109.28.63	TCP	54	60534 → 443 [ACK] Seq=518
109	33.927645	192.168.1.4	52.109.28.63	TCP	54	[TCP Window Update] 60534

تنها پروتکل های TCP نشان داده میشوند.