دانشکده مهندسی
کامپیوتر وفناوری اطلاعات

دانشگاه صنعتی امیرکبیر
(پلی‌تکنیک تهران)
دانشکده مهندسی کامپیوتر

دانشگاه صنعتی امیرکبیر
(پلی تکنیک تهران)

آزمایشگاه شبکه های کامپیوتری

(پاییز ۱۴۰۰)

جلسه دوم

آشنایی با ابزار Whire shark

محمد چوپان ۹۸۳۱۱۲۵

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.

۳-۲- مطالب مقدماتی

۳-۳- قطعات و ابزارهای موردنیاز

ابزارهای موردنیاز در این آزمایش عبارت‌اند از:

- برنامه Wireshark نسخه ۲ به بعد
- یک کامپیوتر با سیستم‌عامل ویندوز 7 به بعد با دسترسی به اینترنت

۳-۴- شرح آزمایش

در تمام بخش‌های آزمایش، واسطی که با آن دسترسی به اینترنت دارید را برای شنود بسته انتخاب کنید.

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

پروتکل های TCP,UDP,ARP,SSDP,MDNS,NBNS,TLS,ICMPV6, قابل مشاهده است.

No.	Time	Source	Destination	Protocol	Length	Info
2060	135.294829	172.23.191.91	239.255.255.250	SSDP	169	M-SEARCH * HTTP/1.1
2061	135.295143	172.23.191.91	239.255.255.250	SSDP	167	M-SEARCH * HTTP/1.1
2062	135.295465	172.23.191.91	239.255.255.250	SSDP	169	M-SEARCH * HTTP/1.1
2063	135.295781	172.23.191.91	239.255.255.250	SSDP	179	M-SEARCH * HTTP/1.1
2064	135.296003	172.23.191.91	224.0.0.251	MDNS	82	Standard query 0x0000 PTI
2065	135.296210	172.23.191.91	224.0.0.251	MDNS	82	Standard query 0x0000 PTI
2066	135.296376	172.23.191.91	224.0.0.251	MDNS	82	Standard query 0x0000 PTI
2067	135.296694	172.23.191.91	224.0.0.251	MDNS	82	Standard query 0x0000 PTI
2068	135.600323	172.23.160.34	172.23.191.255	UDP	216	4554 → 4554 Len=174
2069	135.600420	Cisco_27:9e:d2	Broadcast	ARP	60	Who has 172.23.177.56? T
2070	135.600829	172.23.169.38	239.255.255.250	SSDP	217	M-SEARCH * HTTP/1.1
2071	135.601191	172.23.169.38	239.255.255.250	SSDP	217	M-SEARCH * HTTP/1.1
2072	135.805761	40.101.92.194	172.23.182.228	TLSv1.2	83	Application Data
2073	135.805855	172.23.182.228	40.101.92.194	TCP	54	49973 → 443 [ACK] Seq=1
2074	135.907435	Giga-Byt_b3:3d:1f	Broadcast	ARP	60	Who has 172.23.165.111?
2075	135.907912	172.23.177.137	239.255.255.250	SSDP	328	NOTIFY * HTTP/1.1
2076	136.522591	172.23.187.148	224.0.0.251	MDNS	590	Standard query response
2077	136.523377	fe80::fdea:d4b0:118…	ff02::fb	MDNS	610	Standard query response
2078	136.523887	172.23.160.14	172.23.191.255	UDP	221	4554 → 4554 Len=179
2079	136.531240	172.23.182.228	13.104.208.162	TLSv1.2	562	Application Data
2080	136.531480	172.23.182.228	13.104.208.162	TLSv1.2	305	Application Data
2081	136.727249	13.104.208.162	172.23.182.228	TCP	60	443 → 50688 [ACK] Seq=60
2082	136.829190	172.23.168.165	239.255.255.250	SSDP	217	M-SEARCH * HTTP/1.1
2083	136.829448	Cisco_27:9e:d2	Broadcast	ARP	60	Who has 172.23.180.65? T
2084	136.829448	Giga-Byt_b3:3d:1f	Broadcast	ARP	60	Who has 172.23.165.112?
2085	136.931977	13.104.208.162	172.23.182.228	TLSv1.2	916	Application Data
2086	136.983253	172.23.182.228	13.104.208.162	TCP	54	50688 → 443 [ACK] Seq=60

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؟

```
> Frame 21784: 55 bytes on wire (440 bits), 55 bytes captured (440 bits) on inter
> Ethernet II, Src: LiteonTe_59:ca:e5 (94:08:53:59:ca:e5), Dst: D-LinkIn_d9:6d:24
> Internet Protocol Version 4, Src: 192.168.1.38, Dst: 151.101.115.10
> Transmission Control Protocol, Src Port: 51918, Dst Port: 443, Seq: 1082, Ack:
> Data (1 byte)
```

این بسته در لایه application از پروتکل TCP و در لایه Transport نیز از همین پروتکل استفاده می کند و در لایه network از IPV4 استفاده میکند.

شماره frame آن ۲۱۷۸۴ و مقدار آن برابر با ۵۵ بایت است.

```
Internet Protocol Version 4, Src: 192.168.1.38, Dst: 151.101.115.10
    0100 .... = Version: 4
    .... 0101 = Header Length: 20 bytes (5)
    Differentiated Services Field: 0x00 (DSCP: CS0, ECN: Not-ECT)
        0000 00.. = Differentiated Services Codepoint: Default (0)
        .... ..00 = Explicit Congestion Notification: Not ECN-Capable Transpor
    Total Length: 41
    Identification: 0x97e7 (38887)
    Flags: 0x40, Don't fragment
    ...0 0000 0000 0000 = Fragment Offset: 0
    Time to Live: 128
```

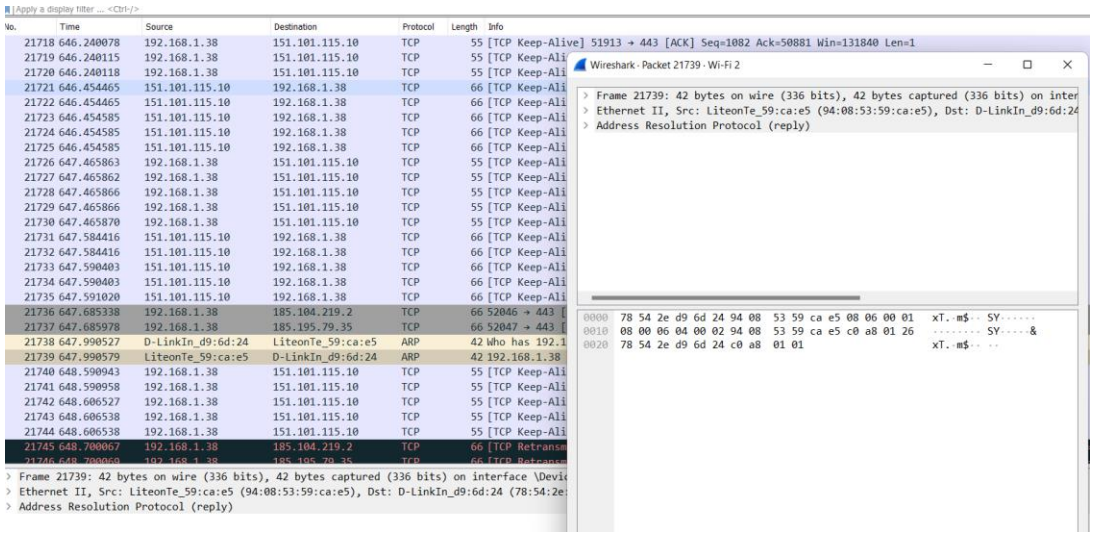
اندازه کل آن در این لایه برابر ٤١ بایت و در لایه بعدی برابر با :

```
Transmission Control Protocol, Src Port: 51918, Dst Port: 443, Seq: 1082, Acl
    Source Port: 51918
    Destination Port: 443
    [Stream index: 148]
    [Conversation completeness: Incomplete, DATA (15)]
    [TCP Segment Len: 1]
    Sequence Number: 1082    (relative sequence number)
    Sequence Number (raw): 723659343
    [Next Sequence Number: 1083    (relative sequence number)]
    Acknowledgment Number: 14136    (relative ack number)
    Acknowledgment number (raw): 2181240692
    0101 .... = Header Length: 20 bytes (5)
    Flags: 0x010 (ACK)
```

برابر با ۲۰ بایت هدر و ۱ بایت داده است.

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

بله بسته با پروتکل ARP :



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

```
    .... 0101 = Header Length: 20 bytes (5)
  > Differentiated Services Field: 0x00 (DSCP: CS0, ECN: Not-ECT)
    Total Length: 52
    Identification: 0xf65e (63070)
  > Flags: 0x40, Don't fragment
    ...0 0000 0000 0000 = Fragment Offset: 0
    Time to Live: 53
    Protocol: TCP (6)
    Header Checksum: 0x8327 [validation disabled]
    [Header checksum status: Unverified]
    Source Address: 151.101.115.10
    Destination Address: 192.168.1.38
> Transmission Control Protocol, Src Port: 443, Dst Port: 51913, Seq: 50881, A

0000  94 08 53 59 ca e5 78 54  2e d9 6d 24 08 00 45 00   ··SY··xT ··m$··E·
0010  00 34 f6 5e 40 00 35 06  83 27 97 65 73 0a c0 a8   ·4·^@·5· ·'·es···
0020  01 26 01 bb ca c9 04 2a  d3 0b fa 3d 01 4c 80 10   ·&·····* ···=·L··
0030  01 16 16 12 00 00 01 01  05 0a fa 3d 01 4b fa 3d   ........ ···=·K·=
0040  01 4c                                              ·L
```

مقدار مورد نظر در تصویر مشخص 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.

برای پروتکل TCP :

21764	650.325606	192.168.1.38	23.58.223.184	TCP	54 51997 → 80 [RST, ACK] Seq=692 Ack=1114919 Win=0 Len=0
21765	650.680074	192.168.1.38	185.104.219.2	TCP	66 52048 → 443 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 WS=256 SACK_PERM=1
21766	650.680884	192.168.1.38	185.195.79.35	TCP	66 52049 → 443 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 WS=256 SACK_PERM=1
21767	650.681430	192.168.1.38	185.195.79.19	TCP	66 52050 → 443 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 WS=256 SACK_PERM=1
21768	651.044361	192.168.1.38	151.101.115.10	TCP	55 [TCP Keep-Alive] 51889 → 443 [ACK] Seq=1451 Ack=62252 Win=131840 Len=1
21769	651.044554	192.168.1.38	151.101.115.10	TCP	55 [TCP Keep-Alive] 51920 → 443 [ACK] Seq=1059 Ack=45860 Win=131840 Len=1
21770	651.044578	192.168.1.38	151.101.115.10	TCP	55 [TCP Keep-Alive] 51917 → 443 [ACK] Seq=1080 Ack=22879 Win=131840 Len=1
21771	651.044578	192.168.1.38	151.101.115.10	TCP	55 [TCP Keep-Alive] 51918 → 443 [ACK] Seq=1082 Ack=14136 Win=131840 Len=1
21772	651.044580	192.168.1.38	151.101.115.10	TCP	55 [TCP Keep-Alive] 51913 → 443 [ACK] Seq=1082 Ack=50881 Win=131840 Len=1
21773	651.268845	151.101.115.10	192.168.1.38	TCP	66 [TCP Keep-Alive ACK] 443 → 51913 [ACK] Seq=50881 Ack=1083 Win=142336 Len=0 SLE=1
21774	651.268845	151.101.115.10	192.168.1.38	TCP	66 [TCP Keep-Alive ACK] 443 → 51889 [ACK] Seq=62252 Ack=1452 Win=143360 Len=0 SLE=1
21775	651.268966	151.101.115.10	192.168.1.38	TCP	66 [TCP Keep-Alive ACK] 443 → 51920 [ACK] Seq=45860 Ack=1060 Win=142336 Len=0 SLE=1

```
> Frame 21775: 66 bytes on wire (528 bits), 66 bytes captured (528 bits) on interface \Device\NPF_{F0D913A0-99F6-4AA5-8B5B-20F036CBD26D}, id 0
> Ethernet II, Src: D-LinkIn_d9:6d:24 (78:54:2e:d9:6d:24), Dst: LiteonTe_59:ca:e5 (94:08:53:59:ca:e5)
> Internet Protocol Version 4, Src: 151.101.115.10, Dst: 192.168.1.38
v Transmission Control Protocol, Src Port: 443, Dst Port: 51920, Seq: 45860, Ack: 1060, Len: 0
    Source Port: 443
    Destination Port: 51920
    [Stream index: 150]
    [Conversation completeness: Incomplete, DATA (15)]
    [TCP Segment Len: 0]
    Sequence Number: 45860    (relative sequence number)
    Sequence Number (raw): 1742386258
    [Next Sequence Number: 45860    (relative sequence number)]
    Acknowledgment Number: 1060    (relative ack number)
    Acknowledgment number (raw): 1561938404
    1000 .... = Header Length: 32 bytes (8)
  > Flags: 0x010 (ACK)
    Window: 278
    [Calculated window size: 142336]
    [Window size scaling factor: 512]
    Checksum: 0xceb8 [unverified]
    [Checksum Status: Unverified]
    Urgent Pointer: 0
```

که هر سه در تصویر مشخص اند .

برای UDP :

2386	69.545133	fe80::c2a:b5cb:1d01…	ff02::fb	MDNS	174 Standard query 0x0000 PTR _companion-link._tcp.local, "QM" question PT
2385	69.536761	192.168.1.35	224.0.0.251	MDNS	154 Standard query 0x0000 PTR _companion-link._tcp.local, "QM" question PT
2324	66.560166	fe80::c2a:b5cb:1d01…	ff02::fb	MDNS	174 Standard query 0x0000 PTR _companion-link._tcp.local, "QM" question PT
2323	66.560166	192.168.1.35	224.0.0.251	MDNS	154 Standard query 0x0000 PTR _companion-link._tcp.local, "QM" question PT
2286	65.536238	fe80::c2a:b5cb:1d01…	ff02::fb	MDNS	174 Standard query 0x0000 PTR _companion-link._tcp.local, "QU" question PT
2285	65.535817	192.168.1.35	224.0.0.251	MDNS	154 Standard query 0x0000 PTR _companion-link._tcp.local, "QU" question PT
1163	29.606941	192.168.1.38	224.0.0.251	MDNS	288 Standard query response 0x0000 PTR, cache flush MaMAdss.local PTR, cac
1159	29.466401	192.168.1.38	224.0.0.251	MDNS	467 Standard query response 0x0000 TXT, cache flush PTR _nvstream_dbd._tcp
20007	567.102792	fe80::1	fe80::9e8:15a7:8b2d…	DNS	220 Standard query response 0xfb06 A tile-service.weather.microsoft.com CN
20004	567.035405	fe80::9e8:15a7:8b2d…	fe80::1	DNS	114 Standard query 0xfb06 A tile-service.weather.microsoft.com
19834	562.216004	fe80::1	fe80::9e8:15a7:8b2d…	DNS	110 Standard query response 0x261c A ecs.office.com A 52.113.194.132

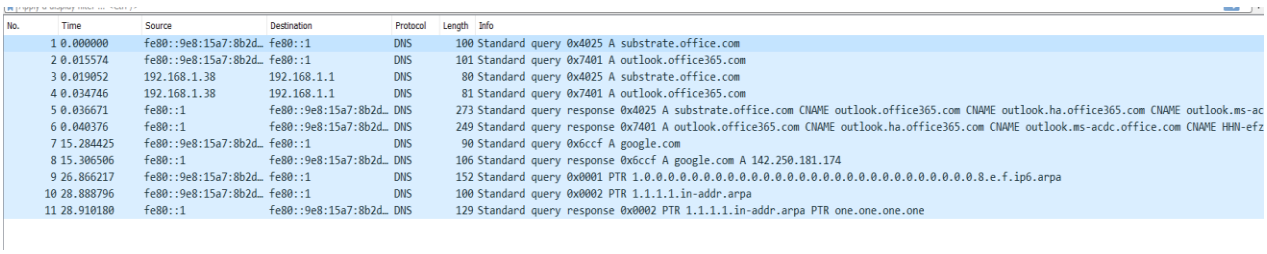
```
> Frame 19245: 107 bytes on wire (856 bits), 107 bytes captured (856 bits) on interface \Device\NPF_{F0D913A0-99F6-4AA5-8B5B-20F036CBD26D}, id 0
> Ethernet II, Src: LiteonTe_59:ca:e5 (94:08:53:59:ca:e5), Dst: D-LinkIn_d9:6d:24 (78:54:2e:d9:6d:24)
> Internet Protocol Version 6, Src: fe80::9e8:15a7:8b2d:f1b6, Dst: fe80::1
v User Datagram Protocol, Src Port: 55859, Dst Port: 53
    Source Port: 55859
    Destination Port: 53
    Length: 53
    Checksum: 0xc946 [unverified]
    [Checksum Status: Unverified]
    [Stream index: 24]
  > [Timestamps]
    UDP payload (45 bytes)
> Domain Name System (query)
```

پورت source که همان فرستنده یا مبدا است که در هر دو مقداری رندوم است که اینجا به دلیل اینکه داخلی است و client خود لپتاپ است مقادیری رندوم است . ولی برای مقصد ۵۳ و ۴۴۳ هستند که پورت های مشخص شده برای ارتباط ها اند. Chekcsum نیز در هر دو تصویر مشخص شده است.

کار با فیلترکننده بسته ها:

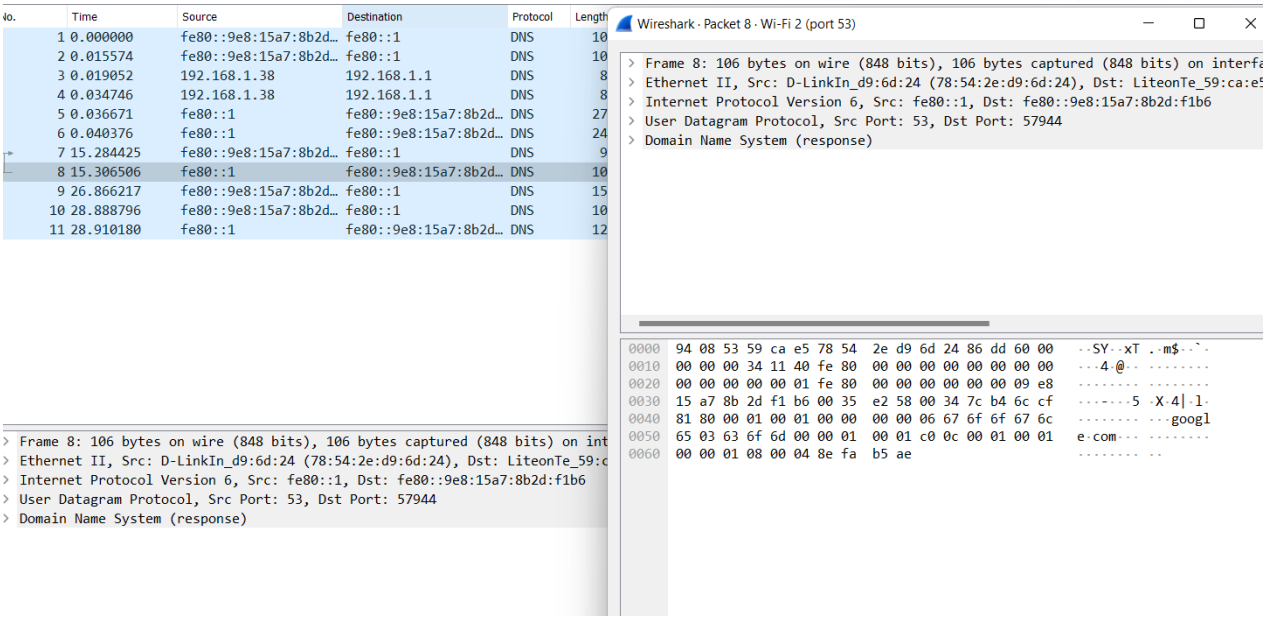
۳-۴-۲- کار با فیلتر کننده بسته‌ها

پس از انجام مراحل گفته شده به نتیجه زیر میرسیم :



No.	Time	Source	Destination	Protocol	Length	Info
1	0.000000	fe80::9e8:15a7:8b2d…	fe80::1	DNS	100	Standard query 0x4025 A substrate.office.com
2	0.015574	fe80::9e8:15a7:8b2d…	fe80::1	DNS	101	Standard query 0x7401 A outlook.office365.com
3	0.019052	192.168.1.38	192.168.1.1	DNS	80	Standard query 0x4025 A substrate.office.com
4	0.034746	192.168.1.38	192.168.1.1	DNS	81	Standard query 0x7401 A outlook.office365.com
5	0.036671	fe80::1	fe80::9e8:15a7:8b2d…	DNS	273	Standard query response 0x4025 A substrate.office.com CNAME outlook.office365.com CNAME outlook.ha.office365.com CNAME outlook.ms-ac
6	0.040376	fe80::1	fe80::9e8:15a7:8b2d…	DNS	249	Standard query response 0x7401 A outlook.office365.com CNAME outlook.ha.office365.com CNAME outlook.ms-acdc.office.com CNAME HHN-efz
7	15.284425	fe80::9e8:15a7:8b2d…	fe80::1	DNS	90	Standard query 0x6ccf A google.com
8	15.306506	fe80::1	fe80::9e8:15a7:8b2d…	DNS	106	Standard query response 0x6ccf A google.com A 142.250.181.174
9	26.866217	fe80::9e8:15a7:8b2d…	fe80::1	DNS	152	Standard query 0x0001 PTR 1.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.8.e.f.ip6.arpa
10	28.888796	fe80::9e8:15a7:8b2d…	fe80::1	DNS	100	Standard query 0x0002 PTR 1.1.1.1.in-addr.arpa
11	28.910180	fe80::1	fe80::9e8:15a7:8b2d…	DNS	129	Standard query response 0x0002 PTR 1.1.1.1.in-addr.arpa PTR one.one.one.one

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.



همانطور که مشاهده میکنیم پروتکل لایه transport پروتکل UDP است.

و آدرس ها به صورت فیزیکی‌اند که اگر تغییر دهیم به شکل زیر در می آیند .

به دلیل مشکل به وجود آمده که تنها در wireshark درخواست های ipv6 را نشان می داد مجبور به عوض کردن اینترنت شدم.

مجددا نتایج حاصل شده :

No.	Time	Source	Destination	Protocol	Length	Info
1	0.000000	172.20.10.3	172.20.10.1	DNS	83	Standard query 0x6896 A rum18.perf.linkedin.com
2	0.056255	172.20.10.1	172.20.10.3	DNS	133	Standard query response 0x6896 A rum18.perf.linkedin.com CNAME l-0005.dc-msedge.net A 13.107.43.14
3	0.756010	172.20.10.3	172.20.10.1	DNS	72	Standard query 0x72be A www.bing.com
4	0.810456	172.20.10.1	172.20.10.3	DNS	193	Standard query response 0x72be A www.bing.com CNAME a-0001.a-afdentry.net.trafficmanager.net CNAME dual-a-0001.a-msedge.net A
5	0.822868	172.20.10.3	172.20.10.1	DNS	77	Standard query 0xe274 A k-ring.msedge.net
6	0.856448	172.20.10.1	172.20.10.3	DNS	144	Standard query response 0xe274 A k-ring.msedge.net CNAME k-ring.k-9999.k-msedge.net CNAME k-9999.k-msedge.net A 13.107.18.254
7	10.727477	172.20.10.3	172.20.10.1	DNS	70	Standard query 0x9409 A google.com
8	10.771602	172.20.10.1	172.20.10.3	DNS	86	Standard query response 0x9409 A google.com A 142.250.181.174
9	25.247312	172.20.10.3	172.20.10.1	DNS	84	Standard query 0x0001 PTR 1.10.20.172.in-addr.arpa
10	25.390514	172.20.10.1	172.20.10.3	DNS	143	Standard query response 0x0001 No such name PTR 1.10.20.172.in-addr.arpa SOA localhost
11	25.393007	172.20.10.3	172.20.10.1	DNS	80	Standard query 0x0002 PTR 1.1.1.1.in-addr.arpa
12	27.409926	172.20.10.1	172.20.10.3	DNS	109	Standard query response 0x0002 PTR 1.1.1.1.in-addr.arpa PTR one.one.one.one

```
> Frame 7: 70 bytes on wire (560 bits), 70 bytes captured (560 bits) on interface \Device\NPF_{D4EC111C-D8D4-41D9-9561-5198FB0C6183}, id 0
v Ethernet II, Src: 3e:2e:f9:ed:1f:47 (3e:2e:f9:ed:1f:47), Dst: 3e:2e:f9:de:b6:64 (3e:2e:f9:de:b6:64)
  > Destination: 3e:2e:f9:de:b6:64 (3e:2e:f9:de:b6:64)
  > Source: 3e:2e:f9:ed:1f:47 (3e:2e:f9:ed:1f:47)
    Type: IPv4 (0x0800)
v Internet Protocol Version 4, Src: 172.20.10.3 (172.20.10.3), Dst: 172.20.10.1 (172.20.10.1)
    0100 .... = Version: 4
    .... 0101 = Header Length: 20 bytes (5)
  > Differentiated Services Field: 0x00 (DSCP: CS0, ECN: Not-ECT)
    Total Length: 56
    Identification: 0xd00a (53258)
  > Flags: 0x00
    ...0 0000 0000 0000 = Fragment Offset: 0
```

آدرس لایه های مبدا و مقصد که مبدا سیستم ما است در تصویر مشخص است .

و هم چنان پروتکل ما در لایه UDP transport است.

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

```
Ethernet adapter Ethernet 3:

   Connection-specific DNS Suffix  . :
   Description . . . . . . . . . . . : Apple Mobile Device Ethernet
   Physical Address. . . . . . . . . : 3E-2E-F9-ED-1F-47
   DHCP Enabled. . . . . . . . . . . : Yes
   Autoconfiguration Enabled . . . . : Yes
   Link-local IPv6 Address . . . . . : fe80::8918:aa72:36bf:45a4%23(Preferred)
   IPv4 Address. . . . . . . . . . . : 172.20.10.3(Preferred)
   Subnet Mask . . . . . . . . . . . : 255.255.255.240
   Lease Obtained. . . . . . . . . . : Wednesday, April 20, 2022 5:10:04 PM
   Lease Expires . . . . . . . . . . : Thursday, April 21, 2022 5:10:03 PM
   Default Gateway . . . . . . . . . : 172.20.10.1
   DHCP Server . . . . . . . . . . . : 172.20.10.1
   DHCPv6 IAID . . . . . . . . . . . : 423505657
   DHCPv6 Client DUID. . . . . . . . : 00-01-00-01-26-8C-C2-F2-F0-2F-74-4B-4C-AD
   DNS Servers . . . . . . . . . . . : 172.20.10.1
   NetBIOS over Tcpip. . . . . . . . : Enabled
```

همانطور که میبینم آدرس 172.20.10.3 که آدرس مبدا و آدرس ما است قابل مشاهده است.

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؟

```
> User Datagram Protocol, Src Port: 52023 (52
v Domain Name System (query)
    Transaction ID: 0x9409
  > Flags: 0x0100 Standard query
    Questions: 1
    Answer RRs: 0
    Authority RRs: 0
    Additional RRs: 0
  v Queries
    > google.com: type A, class IN
    [Response In: 8]
```

همانطور که میبینم Type A انتخاب شده است. این تایپ برای این است که در اصطلاح DNS را متصل کند یعنی hostname را به آدرس ip مرتبط به آن متصل 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 ای انتخاب شده است؟ به نظر شما این درخواست DNS برای چه کاری استفاده شده است؟

```
> User Datagram Protocol, Src Port: 52073 (52073), Dst Port: domain (53)
v Domain Name System (query)
    Transaction ID: 0x0002
  > Flags: 0x0100 Standard query
    Questions: 1
    Answer RRs: 0
    Authority RRs: 0
    Additional RRs: 0
  v Queries
    > 1.1.1.1.in-addr.arpa: type PTR, class IN
    [Response In: 12]
```

در اینجا Type PTR انتخاب شده است . برای این است که دامنه مربوطه را باز میگردانند یعنی معکوس عملی که در قسمت قبل بوده است. که در بخش مربوطه همان Domain name pointer است.

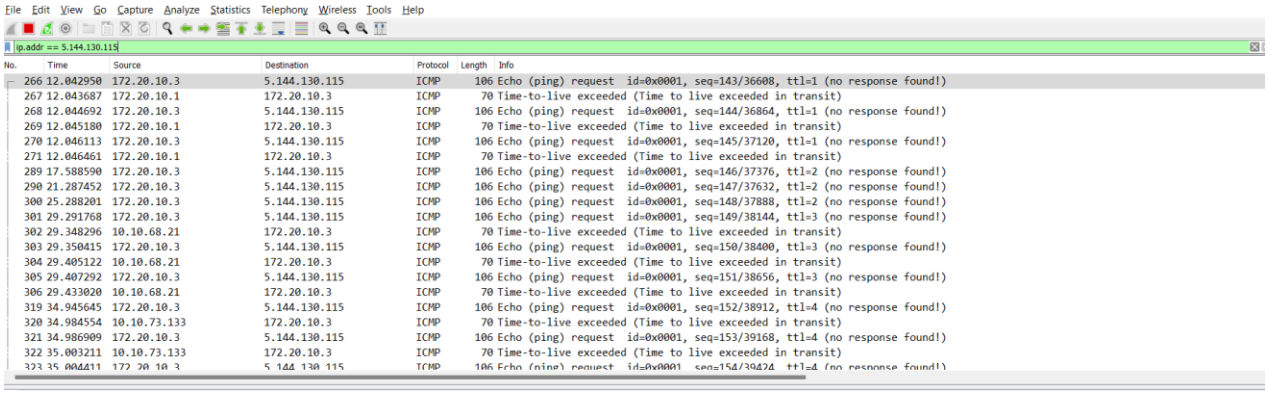
سوال ۱۰: به نظر شما چه type های دیگری ممکن است وجود داشته باشد؟ سه مورد یادداشت کنید.

MB & MG & MR & TXT که مربوط به ایمیل ها دامنه جعبه ایمیل ، شماره گروه ایمیل ها و تغییر نام ایمیل است. و آخری هم برای فایل های تکست.

۳-۴-۲-۲- کار با Display Filter

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

پروتکل تمامی بسته ها به ICMP تغییر می کند و مقصد یا مبدا تمامی بسته ها ip داده شده است.



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.

```
    Destination Address: 5.144.130.115 (5.144.130.115)
  ⌄ Internet Control Message Protocol
      Type: 8 (Echo (ping) request)
      Code: 0
      Checksum: 0xf76f [correct]
      [Checksum Status: Good]
      Identifier (BE): 1 (0x0001)
      Identifier (LE): 256 (0x0100)
      Sequence Number (BE): 143 (0x008f)
      Sequence Number (LE): 36608 (0x8f00)
    ⌄ [No response seen]
      > [Expert Info (Warning/Sequence): No response seen to ICMP request]
    > Data (64 bytes)
```

مقدار type برابر با ۸ است.

```
      Identification: 0xdcd4 (56532)
    > Flags: 0x00
      ...0 0000 0000 0000 = 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: 0x9eb2 [validation disabled]
```

```
      ...0 0000 0000 0000 = Fragment Offset: 0
      Time to Live: 20
      Protocol: ICMP (1)
      Header Checksum: 0x8b79 [validation disabled]
      [Header checksum status: Unverified]
      Source Address: 172.20.10.3 (172.20.10.3)
      Destination Address: 5.144.130.115 (5.144.130.115)
```

TTL برای بسته که پاسخ ندارد که بسته اول است ۱ و برای بسته ای که پاسخ دارد برابر ۲۰ است .

به دلیل اینکه بسته اول پاسخی نداشت بسته دیگری نشان داده شده است.

همان طور که میبینیم برای بسته دیگری نیز ۶۴ است.

```
    .... 0101 = Header Length: 20 bytes (5)
  > Differentiated Services Field: 0x00 (DSCP: CS0, ECN: Not-ECT)
    Total Length: 56
    Identification: 0x16fb (5883)
  > Flags: 0x00
    ...0 0000 0000 0000 = Fragment Offset: 0
    Time to Live: 64
    Protocol: ICMP (1)
    Header Checksum: 0xf79d [validation disabled]
    [Header checksum status: Unverified]
    Source Address: 172.20.10.1 (172.20.10.1)
    Destination Address: 172.20.10.3 (172.20.10.3)
> Internet Control Message Protocol
```

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

برای بسته هایی که مبدا آن ماشین خودم است این مقدار برابر است با مقادیری مانند ۱ تا ۱۰ که به نسبت پایین ترند.

دستور tracert مسیر های رسیدن به یک ip را طی میکند و نشان میدهد. TTL مدت زمانی یا تعداد گام هایی است که یک بسته میتواند باقی بماند با آن ip .حال با طی هر مرحله TTL کاهش می یابد و وقتی که صفر می شود از بین می رود. دلیل اینکه در بسته های موجودی من در ابتدا ۱ بوده است و زیاد نبوده احتمالا این است که پاسخی دریافت نکرده و نیازی به بودن بسته نیست .

	Time	Source	Destination	Protocol	Length	Info
266	12.042950	172.20.10.3	5.144.130.115	ICMP	106	Echo (ping) request id=0x0001, seq=143/36608, ttl=1 (no response found!)
267	12.043687	Mohamads-iphone.local	172.20.10.3	ICMP	70	Time-to-live exceeded (Time to live exceeded in transit)
268	12.044692	172.20.10.3	5.144.130.115	ICMP	106	Echo (ping) request id=0x0001, seq=144/36864, ttl=1 (no response found!)
269	12.045180	Mohamads-iphone.local	172.20.10.3	ICMP	70	Time-to-live exceeded (Time to live exceeded in transit)
270	12.046113	172.20.10.3	5.144.130.115	ICMP	106	Echo (ping) request id=0x0001, seq=145/37120, ttl=1 (no response found!)
271	12.046461	Mohamads-iphone.local	172.20.10.3	ICMP	70	Time-to-live exceeded (Time to live exceeded in transit)
289	17.588590	172.20.10.3	5.144.130.115	ICMP	106	Echo (ping) request id=0x0001, seq=146/37376, ttl=2 (no response found!)
290	21.287452	172.20.10.3	5.144.130.115	ICMP	106	Echo (ping) request id=0x0001, seq=147/37632, ttl=2 (no response found!)
300	25.288201	172.20.10.3	5.144.130.115	ICMP	106	Echo (ping) request id=0x0001, seq=148/37888, ttl=2 (no response found!)
301	29.291768	172.20.10.3	5.144.130.115	ICMP	106	Echo (ping) request id=0x0001, seq=149/38144, ttl=3 (no response found!)
302	29.348296	10.10.68.21	172.20.10.3	ICMP	70	Time-to-live exceeded (Time to live exceeded in transit)
303	29.350415	172.20.10.3	5.144.130.115	ICMP	106	Echo (ping) request id=0x0001, seq=150/38400, ttl=3 (no response found!)
304	29.405122	10.10.68.21	172.20.10.3	ICMP	70	Time-to-live exceeded (Time to live exceeded in transit)
305	29.407292	172.20.10.3	5.144.130.115	ICMP	106	Echo (ping) request id=0x0001, seq=151/38656, ttl=3 (no response found!)
306	29.433020	10.10.68.21	172.20.10.3	ICMP	70	Time-to-live exceeded (Time to live exceeded in transit)
319	34.945645	172.20.10.3	5.144.130.115	ICMP	106	Echo (ping) request id=0x0001, seq=152/38912, ttl=4 (no response found!)
320	34.984554	10.10.73.133	172.20.10.3	ICMP	70	Time-to-live exceeded (Time to live exceeded in transit)
321	34.986909	172.20.10.3	5.144.130.115	ICMP	106	Echo (ping) request id=0x0001, seq=153/39168, ttl=4 (no response found!)
322	35.003211	10.10.73.133	172.20.10.3	ICMP	70	Time-to-live exceeded (Time to live exceeded in transit)
323	35.004411	172.20.10.3	5.144.130.115	ICMP	106	Echo (ping) request id=0x0001, seq=154/39424, ttl=4 (no response found!)

اما همانطور که میبینیم در بسته دوم هم در اطلاعات آن نوشته TTL افزایش یافته است .

و اگر در بسته نگاه کنیم ۶۴ شده است.

```
> Source: Mohamads-iphone.local (3e:2e:f9:de:b6:64)
  Type: IPv4 (0x0800)
v Internet Protocol Version 4, Src: Mohamads-iphone.local (172.20.10.1), Dst:
  0100 .... = Version: 4
  .... 0101 = Header Length: 20 bytes (5)
> Differentiated Services Field: 0x00 (DSCP: CS0, ECN: Not-ECT)
  Total Length: 56
  Identification: 0x16fb (5883)
> Flags: 0x00
  ...0 0000 0000 0000 = Fragment Offset: 0
  Time to Live: 64
  Protocol: ICMP (1)
  Header Checksum: 0xf79d [validation disabled]
```

دلیل این فرایند می تواند استفاده از hotspot موبایل نیز باشد.

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

سوال ۱۴: این فیلتر چه کاری انجام می‌دهد؟

ip.proto==6

No.	Time	Source	Destination	Protocol	Length	Info
313	33.682140	172.20.10.3	52.97.232.226	TCP	54	52090 → https(443) [ACK] Seq=1 Ack=117 Win=1022 Len=0
316	34.460847	Mohamads-iphone.local	172.20.10.3	TLSv1…	403	Application Data
317	34.461348	172.20.10.3	Mohamads-iphone.local	TLSv1…	318	Application Data
318	34.461994	Mohamads-iphone.local	172.20.10.3	TCP	54	51464 → 52056 [ACK] Seq=1397 Ack=1057 Win=8183 Len=0
341	45.000256	52.97.232.226	172.20.10.3	TLSv1…	83	Application Data
342	45.000367	172.20.10.3	52.97.232.226	TCP	54	52090 → https(443) [ACK] Seq=1 Ack=146 Win=1022 Len=0
343	45.455498	Mohamads-iphone.local	172.20.10.3	TLSv1…	403	Application Data
344	45.455997	172.20.10.3	Mohamads-iphone.local	TLSv1…	318	Application Data
345	45.456903	Mohamads-iphone.local	172.20.10.3	TCP	54	51464 → 52056 [ACK] Seq=1746 Ack=1321 Win=8183 Len=0
359	49.335485	172.20.10.3	eur.roaming1.live.com.…	TCP	66	50202 → https(443) [SYN] Seq=0 Win=64240 Len=0 MSS=1460 WS=256 SACK_PERM=
361	50.343605	172.20.10.3	eur.roaming1.live.com.…	TCP	66	[TCP Retransmission] [TCP Port numbers reused] 50202 → https(443) [SYN] S
371	52.359755	172.20.10.3	eur.roaming1.live.com.…	TCP	66	[TCP Retransmission] [TCP Port numbers reused] 50202 → https(443) [SYN] S
373	53.495102	52.97.232.226	172.20.10.3	TLSv1…	83	Application Data
374	53.495177	172.20.10.3	52.97.232.226	TCP	54	52090 → https(443) [ACK] Seq=1 Ack=175 Win=1022 Len=0
376	56.293655	Mohamads-iphone.local	172.20.10.3	TLSv1…	403	Application Data
377	56.294063	172.20.10.3	Mohamads-iphone.local	TLSv1…	318	Application Data

تنها پروتکل های TLSv1 و TCP را نشان می دهد که احتمالا دلیل نشان دادن TLSv1 نیز هم وجود TCP در لایه های آن و هم مجددا استفاده از hotspot تلفن همراه است.