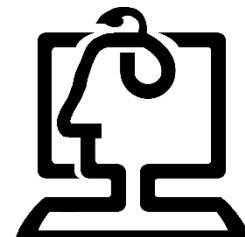


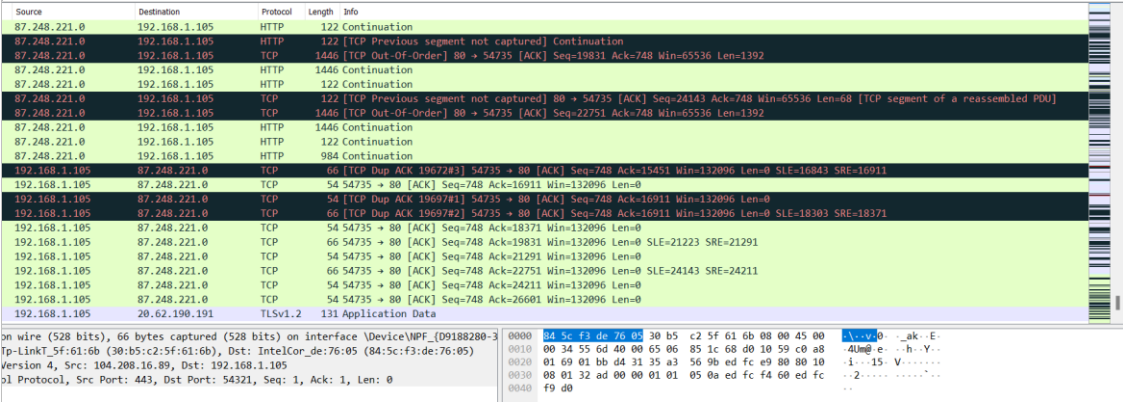
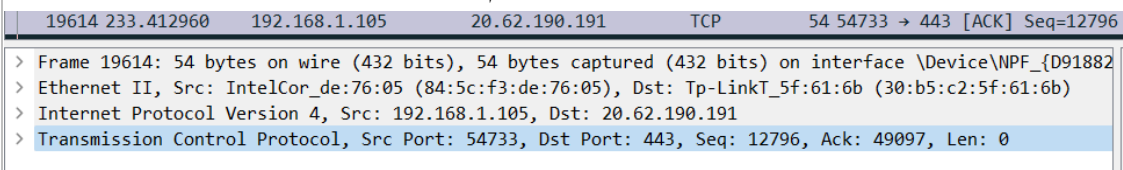


دانشگاه صنعتی امیرکبیر
(پلی تکنیک تهران)



دانشکده مهندسی کامپیوتر

فرم گزارش کار آزمایشگاه شبکه

نام و نام خانوادگی	فرهاد امان	شماره دانشجویی	9931006	نام و شماره آزمایش	3: آشنایی با نرم افزار Wireshark
هدف آزمایش	در این آزمایش علاوه با آشنایی با نرم افزار Wireshark با پروتکل ها در لایه های مختلف TCP/IP آشنایی پیدا می کنیم.				
ابزارها ی مورد نیاز	برنامه Wireshark نسخه 2 به بعد، یک کامپیوتر با سیستم عامل ویندوز 7 به بعد با دسترسی به اینترنت				
شرح آزمایش	<p>در ابتدا شروع به شنود بسته ها از اینترنت می کنیم و بعد از کمی وبگردی شنود بسته ها را متوقف می کنیم.</p> <p>بخشی از پروتکل هایی که مشاهده می کنیم: TCP, TLS, ICMP, QUIC, DNS, HTTP, SSDP.</p>  <p>حالا یک بسته را به دلخواه انتخاب کرده و آن را بررسی می کنیم.</p>  <p>این بسته در لایه های Applicaton و Transport از پروتکل TCP استفاده می کند و در لایه Network از پروتکل IPv4 استفاده می کند.</p>				

اندازه کل فریم آن برابر 54 بایت است. اندازه کل بسته لایه 3 برابر 40 بایت است.

بخش اول بایت‌ها مربوط به پروتکل Ethernet، بخش دوم مربوط به پروتکل IPv4 و بخش آخر مربوط به پروتکل TCP است.

آیا بسته‌ای وجود دارد که از پروتکل‌های لایه Application, Network, Transport استفاده نکند؟ بله بسته‌هایی با پروتکل ARP

```
> Frame 17142: 42 bytes on wire (336 bits), 42 bytes captured (336 bits) on interface \Device\NPF_{D91882...}
> Ethernet II, Src: IntelCor_de:76:05 (84:5c:f3:de:76:05), Dst: Tp-LinkT_5f:61:6b (30:b5:c2:5f:61:6b)
> Address Resolution Protocol (request)
```

حال از بخش مربوط به IP یکی از بسته‌ها بخش Checksum را نمایش می‌دهیم.

Header Checksum: 0xadbb9 [validation disabled]

حال در اینجا بخش مربوط به TCP یک بسته را پیدا کرده و Source port, Destination port, Checksum را مشخص می‌کنیم.

```
> Internet Protocol Version 4, Src: 192.168.1.105, Dst: 216.239.38.120
> Transmission Control Protocol, Src Port: 54563, Dst Port: 443, Seq: 1, Ack: 1, Len: 0
  Source Port: 54563
  Destination Port: 443
  [Stream index: 15]
  [Conversation completeness: Incomplete, DATA (15)]
  [TCP Segment Len: 0]
  Sequence Number: 1 (relative sequence number)
  Sequence Number (raw): 1015598210
  [Next Sequence Number: 1 (relative sequence number)]
  Acknowledgment Number: 1 (relative ack number)
  Acknowledgment number (raw): 4035070482
  0101 .... = Header Length: 20 bytes (5)
  > Flags: 0x010 (ACK)
  Window: 516
  [Calculated window size: 132096]
  [Window size scaling factor: 256]
  Checksum: 0xd1d8 [unverified]
  [Checksum Status: Unverified]
```

پورت Source مربوط به فرستنده است و یک عدد رندوم است. پورت Dest مربوط به مقصد است و یک عدد مشخص است و بستگی به این دارد که کامپیوتر مقصد روی کدام پورت گوش می‌کند.

کار با فیلترکننده بسته‌ها:

No.	Time	Source	Destination	Protocol	Length	Info
1	0.000000	185.51.200.2	192.168.1.105	DNS	187	Standard query response 0x83d8 AAAA sync-1-us-west1-g.sync.services.mozilla.com SOA ns-1976.awsdns-55.co.uk
2	0.765551	192.168.1.105	178.22.122.100	DNS	103	Standard query 0x71b1 AAAA sync-1-us-west1-g.sync.services.mozilla.com
3	1.270657	185.51.200.2	192.168.1.105	DNS	187	Standard query response 0x83d8 AAAA sync-1-us-west1-g.sync.services.mozilla.com SOA ns-1976.awsdns-55.co.uk
4	1.775418	192.168.1.105	185.51.200.2	DNS	103	Standard query 0x71b1 AAAA sync-1-us-west1-g.sync.services.mozilla.com
5	2.781429	192.168.1.105	185.51.200.2	DNS	103	Standard query 0x71b1 AAAA sync-1-us-west1-g.sync.services.mozilla.com
6	3.895270	192.168.1.105	178.22.122.100	DNS	78	Standard query 0x0b29 A udpcp.microsoft.com
7	4.788513	192.168.1.105	178.22.122.100	DNS	103	Standard query 0x71b1 AAAA sync-1-us-west1-g.sync.services.mozilla.com
8	4.788668	192.168.1.105	185.51.200.2	DNS	103	Standard query 0x71b1 AAAA sync-1-us-west1-g.sync.services.mozilla.com
9	4.898621	192.168.1.105	185.51.200.2	DNS	78	Standard query 0x0b29 A udpcp.microsoft.com
10	5.230668	178.22.122.100	192.168.1.105	DNS	201	Standard query response 0x0b29 A udpcp.microsoft.com CNAMRE ud-prod-cp.trafficmanager.net CNAMRE ud-prod-cp-eu-west-4-fe.westeuro...
11	6.772397	178.22.122.100	192.168.1.105	DNS	187	Standard query response 0x71b1 AAAA sync-1-us-west1-g.sync.services.mozilla.com SOA ns-1976.awsdns-55.co.uk
12	7.828413	185.51.200.2	192.168.1.105	DNS	187	Standard query response 0x71b1 AAAA sync-1-us-west1-g.sync.services.mozilla.com SOA ns-1976.awsdns-55.co.uk
13	12.948388	185.51.200.2	192.168.1.105	DNS	187	Standard query response 0x71b1 AAAA sync-1-us-west1-g.sync.services.mozilla.com SOA ns-1976.awsdns-55.co.uk
14	13.226983	185.51.200.2	192.168.1.105	DNS	201	Standard query response 0x0b29 A udpcp.microsoft.com CNAMRE ud-prod-cp.trafficmanager.net CNAMRE ud-prod-cp-eu-west-3-fe.westeuro...
15	13.252112	192.168.1.105	178.22.122.100	DNS	81	Standard query 0xbbb8 A events.gfe.nvidia.com
16	13.610575	192.168.1.105	178.22.122.100	DNS	78	Standard query 0x48f6 A google.com
17	14.261450	192.168.1.105	185.51.200.2	DNS	81	Standard query 0xbbb8 A events.gfe.nvidia.com
18	14.620421	192.168.1.105	185.51.200.2	DNS	78	Standard query 0x48f6 A google.com
19	14.742834	185.51.200.2	178.22.122.100	DNS	81	Standard query 0xbbb8 A events.gfe.nvidia.com

با اعمال فیلترهای مورد نظر و انجام دستورات گفته شده فقط بسته‌های DNS دریافت می‌شوند.

```

> Frame 16: 70 bytes on wire (560 bits), 70 bytes captured (560 bits) on interface \Device\NPF_{D9188280-
> Ethernet II, Src: IntelCor_de:76:05 (84:5c:f3:de:76:05), Dst: Tp-LinkT_5f:61:6b (30:b5:c2:5f:61:6b)
< Internet Protocol Version 4, Src: 192.168.1.105, Dst: 178.22.122.100
  0100 .... = Version: 4
  .... 0101 = Header Length: 20 bytes (5)
  > Differentiated Services Field: 0x00 (DSCP: CS0, ECN: Not-ECT)
    Total Length: 56
    Identification: 0xdff0 (57328)
  > 000. .... = Flags: 0x0
    ...0 0000 0000 0000 = Fragment Offset: 0
    Time to Live: 128
    Protocol: UDP (17)
    Header Checksum: 0x6c38 [validation disabled]
    [Header checksum status: Unverified]
    Source Address: 192.168.1.105
    Destination Address: 178.22.122.100
  > User Datagram Protocol, Src Port: 62650, Dst Port: 53
  > Domain Name System (query)

```

همانطور که مشخص است پروتکل لایه Transport پروتکل UDP است. همچنین آدرس مبدا و مقصد هر دو در تصویر مشخص هستند.

```

Wireless LAN adapter Wi-Fi:
15 1 255.255.255.255 192.168.1.105 178.22.122.100 DNS 81 Standard query 0xbbb0a A events.g
Connection-specific DNS Suffix . : 178.22.122.100 DNS 70 Standard query 0x48f6 A google.c
Description . . . . . : Intel(R) Wi-Fi 6 AX201 160MHz
Physical Address. . . . . : 84-5C-F3-DE-76-05
DHCP Enabled. . . . . : Yes
Autoconfiguration Enabled . . . . : Yes
IPv4 Address. . . . . : 192.168.1.105(Preferred)
Subnet Mask . . . . . : 255.255.255.0
Lease Obtained. . . . . : Monday, March 20, 2023 12:55:53 PM
Lease Expires . . . . . : Thursday, March 23, 2023 2:35:29 PM
Default Gateway . . . . . : 192.168.1.1
DHCP Server . . . . . : 192.168.1.1
DNS Servers . . . . . : 178.22.122.100
NetBIOS over Tcpip. . . . . : Enabled

```

حال اگر از دستور ipconfig /all استفاده کنیم. می‌توانیم در بخش IPv4 Address آدرس مبدا خود را مشاهده کنیم.

```

> 000. .... = Flags: 0x0
  ...0 0000 0000 0000 = Fragment Offset: 0
  Time to Live: 128
  Protocol: UDP (17)
  Header Checksum: 0x6c38 [validation disabled]
  [Header checksum status: Unverified]
  Source Address: 192.168.1.105
  Destination Address: 178.22.122.100
> User Datagram Protocol, Src Port: 62650, Dst Port: 53
< Domain Name System (query)
  Transaction ID: 0x48f6
  > Flags: 0x0100 Standard query
    Questions: 1
    Answer RRs: 0
    Authority RRs: 0
    Additional RRs: 0
  < Queries
    google.com; type A, class IN
    [Response In: 27]

```

در این بخش که مربوط به دستور Ping است Type A انتخاب شده است.

این Type در واقع برای تبدیل نام یک دامنه به یک IPv4 عمل می‌کند و در واقعاً به عنوان یک مترجم برای تبدیل نام دامنه به IP است.

```
Identification: 0xdff8 (57336)
> 000. .... = Flags: 0x0
...0 0000 0000 0000 = Fragment Offset: 0
Time to Live: 128
Protocol: UDP (17)
Header Checksum: 0x6c26 [validation disabled]
[Header checksum status: Unverified]
Source Address: 192.168.1.105
Destination Address: 178.22.122.100
> User Datagram Protocol, Src Port: 62923, Dst Port: 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
```

در این بخش که مربوط به دستور Nslookup است Type PTR انتخاب شده است. این Type برعکس A عمل می‌کند و وظیفه آن تبدیل کردن IP Address به نام دامنه است. Type‌های دیگری مانند NS, MX, TXT, SOA نیز وجود دارند. در مرحله بعد در ابتدا بدون اعمال هیچ فیلتری شروع به شنود بسته‌ها می‌کنیم. و در CMD از دستور `tracert p30download.com` استفاده می‌کنیم.

```
C:\Windows\system32\cmd.exe
C:\Users\farha>tracert p30download.com

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

  1  <1 ms    <1 ms     9 ms     192.168.1.1
  2  28 ms     29 ms     27 ms     2.180.64.1
  3  51 ms     41 ms     48 ms     10.0.75.118
  4  *          *          *         Request timed out.
  5  *          41 ms     47 ms     10.0.138.61
  6  *          42 ms     47 ms     10.10.180.174
  7  47 ms     42 ms     *         172.31.252.14
  8  *          41 ms     *         172.31.254.153
  9  195 ms    196 ms    204 ms    john.centraldnsserver.com [5.144.130.115]

Trace complete.
```

در قسمت اگر عبارت dns را بنویسیم فقط بسته‌هایی با پروتکل dns نمایش داده می‌شوند.

No.	Time	Source	Destination	Protocol	Length	Info
1	0.000000	178.22.122.100	192.168.1.105	DNS	187	Standard query response 0xe4d6 AAAA sync-1-us-west1-g.sync.services.mozilla.com SOA ns-1976.awsdns-55.co.uk
113	3.328943	192.168.1.105	178.22.122.100	DNS	84	Standard query 0x54ad A firestore.googleapis.com
114	3.369267	178.22.122.100	192.168.1.105	DNS	100	Standard query response 0x54ad A firestore.googleapis.com A 50.7.87.84
345	9.710738	192.168.1.105	178.22.122.100	DNS	73	Standard query 0xfa50 A www.google.ru
346	9.753204	178.22.122.100	192.168.1.105	DNS	89	Standard query response 0xfa50 A www.google.ru A 172.217.16.195
724	21.426223	192.168.1.105	178.22.122.100	DNS	75	Standard query 0x7331 A p30download.com
730	21.526184	192.168.1.105	185.51.200.2	DNS	91	Standard query response 0x7331 A p30download.com A 5.144.130.115
734	21.598848	178.22.122.100	192.168.1.105	DNS	84	Standard query 0x589e PTR 1.1.168.192.in-addr.arpa
741	21.616244	192.168.1.105	178.22.122.100	DNS	74	Standard query 0x4384 A dns.google.com
742	21.641531	192.168.1.105	178.22.122.100	DNS	143	Standard query response 0x589e No such name PTR 1.1.168.192.in-addr.arpa SOA localhost
743	21.665218	178.22.122.100	192.168.1.105	DNS	90	Standard query response 0x4384 A dns.google.com A 69.197.146.182
756	21.689179	178.22.122.100	192.168.1.105	DNS	91	Standard query response 0x7331 A p30download.com A 5.144.130.115
765	22.104512	185.51.200.2	192.168.1.105	DNS	83	Standard query 0xfbfb3 PTR 1.64.180.2.in-addr.arpa
925	27.300389	192.168.1.105	178.22.122.100	DNS	83	Standard query 0xfbfb3 PTR 1.64.180.2.in-addr.arpa
927	27.400537	192.168.1.105	185.51.200.2	DNS	143	Standard query response 0xfbfb3 No such name PTR 1.64.180.2.in-addr.arpa SOA pri.authdns.ripe.net
930	27.456376	178.22.122.100	192.168.1.105	DNS	143	Standard query response 0xfbfb3 No such name PTR 1.64.180.2.in-addr.arpa SOA pri.authdns.ripe.net
934	27.546097	185.51.200.2	192.168.1.105	DNS	84	Standard query 0x638c PTR 118.75.0.10.in-addr.arpa
1127	33.112055	192.168.1.105	178.22.122.100	DNS	143	Standard query response 0x638c No such name PTR 118.75.0.10.in-addr.arpa SOA localhost
1138	33.152104	178.22.122.100	192.168.1.105	DNS		

در مرحله بعدی فیلترهای مورد نظر را ایجاد می‌کنیم

Wireshark · Display Filter Expression

Field Name

IPProvideClassInfo · DCOM IPProvideClassInfo
> IPSICTL · IPSICTL
▼ IPv4 · Internet Protocol Version 4
ip.addr · Source or Destination Address
ip.bogus_header_length · Bogus IP header length
ip.bogus_ip_length · Bogus IP length
ip.bogus_ip_version · Bogus IP version
ip.checksum · Header Checksum
ip.checksum.status · Header checksum status
ip.checksum_bad.expert · Bad checksum
ip.checksum_calculated · Calculated Checksum
ip.cipso.categories · Categories
ip.cipso.doi · DOI
ip.cipso.malformed · Malformed CIPSO tag
ip.cipso.sensitivity_level · Sensitivity Level

Relation

is present
==
!=
===

Quantifier

☒ Any ☐ All

Value (IPv4 address)

5.144.130.115

Predefined Values

Range (offset:length)

Search: IP

ip.addr == 5.144.130.115

Click OK to insert this filter

همانطور که می‌بینید آدرس IP به مقدار آدرس سایت p30download که در دستور traceroute نشان داده شده بود است.

No.	Time	Source	Destination	Protocol	Length	Info
735	21.603821	192.168.1.105	5.144.130.115	ICMP	106	Echo (ping) request id=0x0001, seq=455/50945, ttl=1 (no response found!)
736	21.604570	192.168.1.1	192.168.1.105	ICMP	70	Time-to-live exceeded (Time to live exceeded in transit)
737	21.604977	192.168.1.105	5.144.130.115	ICMP	106	Echo (ping) request id=0x0001, seq=456/51201, ttl=1 (no response found!)
738	21.605609	192.168.1.1	192.168.1.105	ICMP	70	Time-to-live exceeded (Time to live exceeded in transit)
739	21.605973	192.168.1.105	5.144.130.115	ICMP	106	Echo (ping) request id=0x0001, seq=457/51457, ttl=1 (no response found!)
740	21.615516	192.168.1.1	192.168.1.105	ICMP	70	Time-to-live exceeded (Time to live exceeded in transit)
919	27.200215	192.168.1.105	5.144.130.115	ICMP	106	Echo (ping) request id=0x0001, seq=458/51713, ttl=2 (no response found!)
920	27.228784	2.180.64.1	192.168.1.105	ICMP	70	Time-to-live exceeded (Time to live exceeded in transit)
921	27.231828	192.168.1.105	5.144.130.115	ICMP	106	Echo (ping) request id=0x0001, seq=459/51969, ttl=2 (no response found!)
922	27.261180	2.180.64.1	192.168.1.105	ICMP	70	Time-to-live exceeded (Time to live exceeded in transit)
923	27.264616	192.168.1.105	5.144.130.115	ICMP	106	Echo (ping) request id=0x0001, seq=460/52225, ttl=2 (no response found!)
924	27.292176	2.180.64.1	192.168.1.105	ICMP	70	Time-to-live exceeded (Time to live exceeded in transit)
1116	32.967346	192.168.1.105	5.144.130.115	ICMP	106	Echo (ping) request id=0x0001, seq=461/52481, ttl=3 (no response found!)
1117	33.018391	10.0.75.118	192.168.1.105	ICMP	70	Time-to-live exceeded (Time to live exceeded in transit)
1118	33.019844	192.168.1.105	5.144.130.115	ICMP	106	Echo (ping) request id=0x0001, seq=462/52737, ttl=3 (no response found!)
1124	33.061232	10.0.75.118	192.168.1.105	ICMP	70	Time-to-live exceeded (Time to live exceeded in transit)
1125	33.062211	192.168.1.105	5.144.130.115	ICMP	106	Echo (ping) request id=0x0001, seq=463/52993, ttl=3 (no response found!)
1126	33.110318	10.0.75.118	192.168.1.105	ICMP	70	Time-to-live exceeded (Time to live exceeded in transit)
1310	39.451553	10.0.75.118	5.144.130.115	ICMP	106	Echo (ping) request id=0x0001, seq=464/53240, ttl=3 (no response found!)

پس از تایید کردن این فیلتر تنها بسته‌هایی با پروتکل ICMP که آدرس مقصد یا مبدا آن‌ها آدرس ورودی ما است نمایش داده می‌شوند.

```
> 000. .... = Flags: 0x0
...0 0000 0000 0000 = Fragment Offset: 0
> Time to Live: 1
Protocol: ICMP (1)
Header Checksum: 0x4282 [validation disabled]
[Header checksum status: Unverified]
Source Address: 192.168.1.105
Destination Address: 5.144.130.115
v Internet Control Message Protocol
Type: 8 (Echo (ping) request)
Code: 0
Checksum: 0xf637 [correct]
[Checksum Status: Good]
Identifier (BE): 1 (0x0001)
Identifier (LE): 256 (0x0100)
Sequence Number (BE): 455 (0x01c7)
Sequence Number (LE): 50945 (0xc701)
> [No response seen]
> Data (64 bytes)
v Internet Protocol Version 4, Src: 192.168.1.105, 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: 0x2d0b (11531)
> 000. .... = Flags: 0x0
...0 0000 0000 0000 = Fragment Offset: 0
Time to Live: 1
Protocol: ICMP (1)
Header Checksum: 0x4282 [validation disabled]
[Header checksum status: Unverified]
Source Address: 192.168.1.105
Destination Address: 5.144.130.115
```

در بخش Internet Control Message Protocol مقدار Type 8 مشخص شده است. همانطور که می‌بینید TTL این بسته هم برابر 1 مشخص شده است. که البته برای تمام بسته‌ها یکسان نیست. همانطور که می‌دانیم هنگامی که دستور tracert را اجرا می‌کنیم هر بار 3 بسته ICMP به سمت مقصد فرستاده می‌شود اما هر بار مقدار TTL اولیه بسته تغییر می‌کند. این باعث می‌شود که بسته ارسالی بعد از تعدادی hop یا در عمل گذر از تعدادی router منقضی شود به همین خاطر ما می‌توانیم متوجه این شویم که router هایی در سر رسیدن بسته ما به مقصد وجود دارند و همچنین تاخیر رسیدن بسته به هر کدام از آن‌ها را هم متوجه می‌شویم. در آخر هم فیلتر 6 ip.proto == 6 را اعمال می‌کنیم.

ip.proto == 6						
No.	Time	Source	Destination	Protocol	Length	Info
714	21.133711	192.168.1.105	142.250.185.68	TCP	66	[TCP Dup ACK 702#1] 58312 → 443 [ACK] Seq=518 Ack=1 Win=132096 Len=0 SLE=2785 SRE=4177
715	21.133753	192.168.1.105	142.250.185.68	TCP	66	[TCP Dup ACK 702#2] 58312 → 443 [ACK] Seq=518 Ack=1 Win=132096 Len=0 SLE=2785 SRE=4295
716	21.133833	142.250.185.68	192.168.1.105	TLSv1.3	1446	[TCP Fast Retransmission] , Server Hello, Change Cipher Spec
717	21.133895	192.168.1.105	142.250.185.68	TCP	66	58312 → 443 [ACK] Seq=518 Ack=1393 Win=132096 Len=0 SLE=2785 SRE=4295
718	21.135220	142.250.185.68	192.168.1.105	TCP	1446	[TCP Out-Of-Order] 443 → 58312 [PSH, ACK] Seq=1393 Ack=518 Win=66816 Len=1392 [TCP segment o
719	21.135389	192.168.1.105	142.250.185.68	TCP	54	58312 → 443 [ACK] Seq=518 Ack=4295 Win=132096 Len=0
720	21.138612	192.168.1.105	142.250.185.68	TLSv1.3	134	Change Cipher Spec, Application Data
721	21.280300	142.250.185.68	192.168.1.105	TCP	60	443 → 58312 [ACK] Seq=4295 Ack=598 Win=66816 Len=0
722	21.280334	192.168.1.105	142.250.185.68	TLSv1.3	401	Application Data
723	21.418943	142.250.185.68	192.168.1.105	TCP	60	443 → 58312 [ACK] Seq=4295 Ack=945 Win=67840 Len=0
725	21.520118	142.250.185.68	192.168.1.105	TLSv1.3	626	[TCP Previous segment not captured] , Continuation Data
726	21.520157	192.168.1.105	142.250.185.68	TCP	66	[TCP Dup ACK 719#1] 58312 → 443 [ACK] Seq=945 Ack=4295 Win=132096 Len=0 SLE=5687 SRE=6259
727	21.521106	142.250.185.68	192.168.1.105	TCP	1446	[TCP Out-Of-Order] 443 → 58312 [ACK] Seq=4295 Ack=945 Win=67840 Len=1392
728	21.521143	192.168.1.105	142.250.185.68	TCP	54	58312 → 443 [ACK] Seq=945 Ack=6259 Win=132096 Len=0
729	21.521976	142.250.185.68	192.168.1.105	TLSv1.3	486	Application Data
731	21.572033	192.168.1.105	142.250.185.68	TCP	54	58312 → 443 [ACK] Seq=945 Ack=6691 Win=131584 Len=0
732	21.583866	192.168.1.105	149.154.165.136	TCP	66	58315 → 443 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 WS=256 SACK_PERM
733	21.584750	192.168.1.105	149.154.165.136	TCP	66	58316 → 80 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 WS=256 SACK_PERM
746	21.670600	192.168.1.105	149.154.165.136	TCP	66	58317 → 443 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 WS=256 SACK_PERM

همانطور که مشاهده می‌شود بعد از اعمال این فیلتر تنها بسته‌هایی با پروتکل TCP و یا TLSv1 نمایش داده می‌شوند.

نرم افزار Wireshark یک نرم‌افزار کامل و جامع برای شنود و مانیتور کردن واسط‌های شبکه است. در این نرم‌افزار می‌توان بسته‌های رد و بدل شده توسط واسط‌های شبکه را به طور کامل مشاهده کرد و جزئیات مربوط به هرکدام را مشاهده کرد. همچنین این نرم‌افزار از دو نوع فیلتر کننده بسته استفاده می‌کند که کار با آن را بسیار منعطف‌تر کرده است.

نتیجه-
گیری