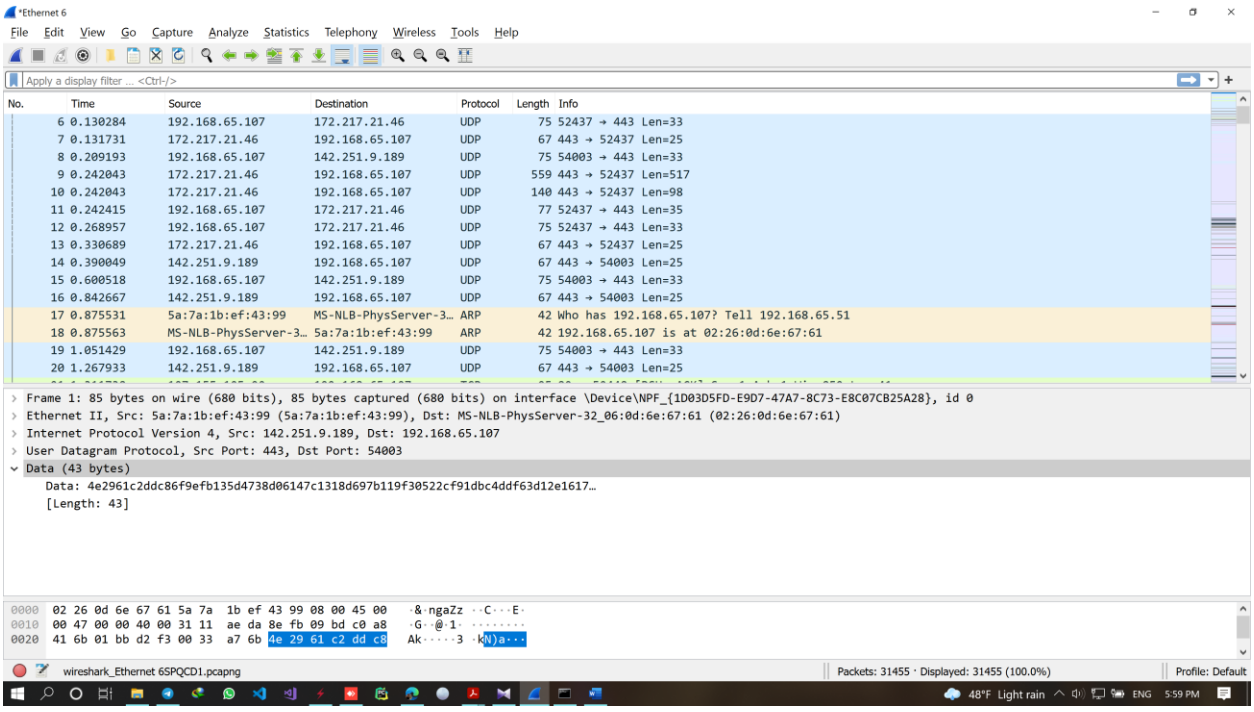
به نام خدا

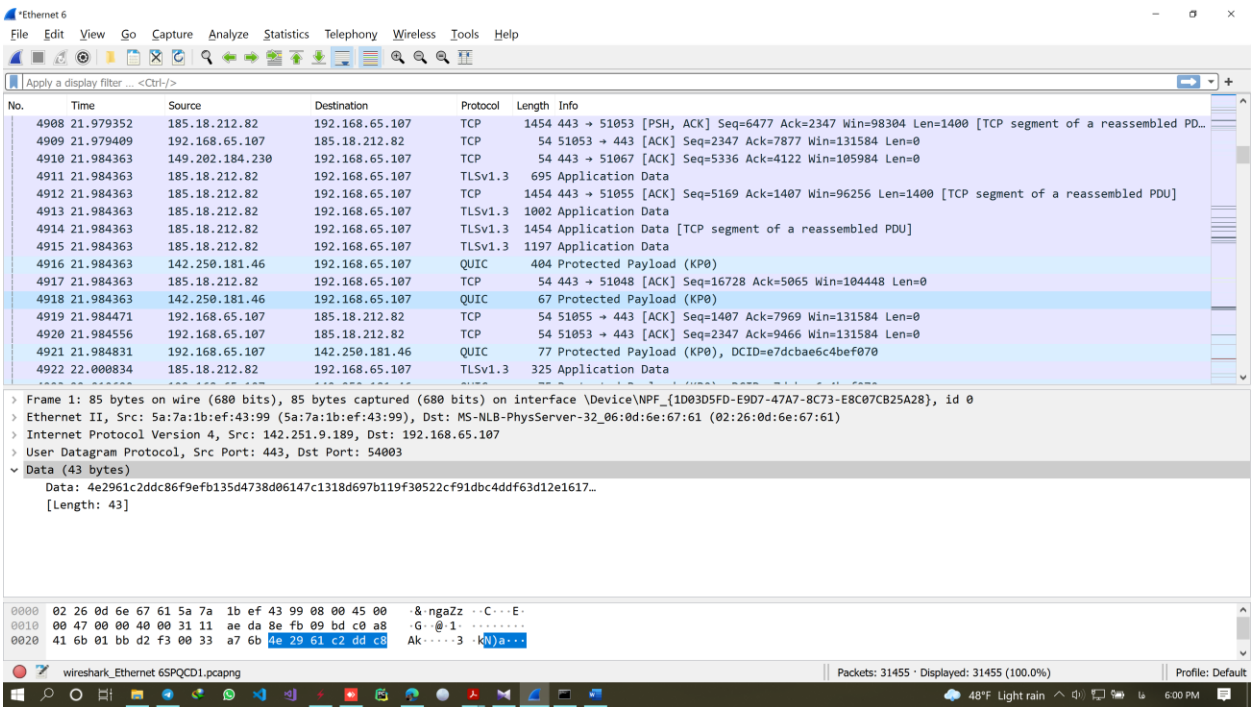
آرتا اسدی
9731006

گزارش آزمایش کار با WireShark

سوال 1 ->

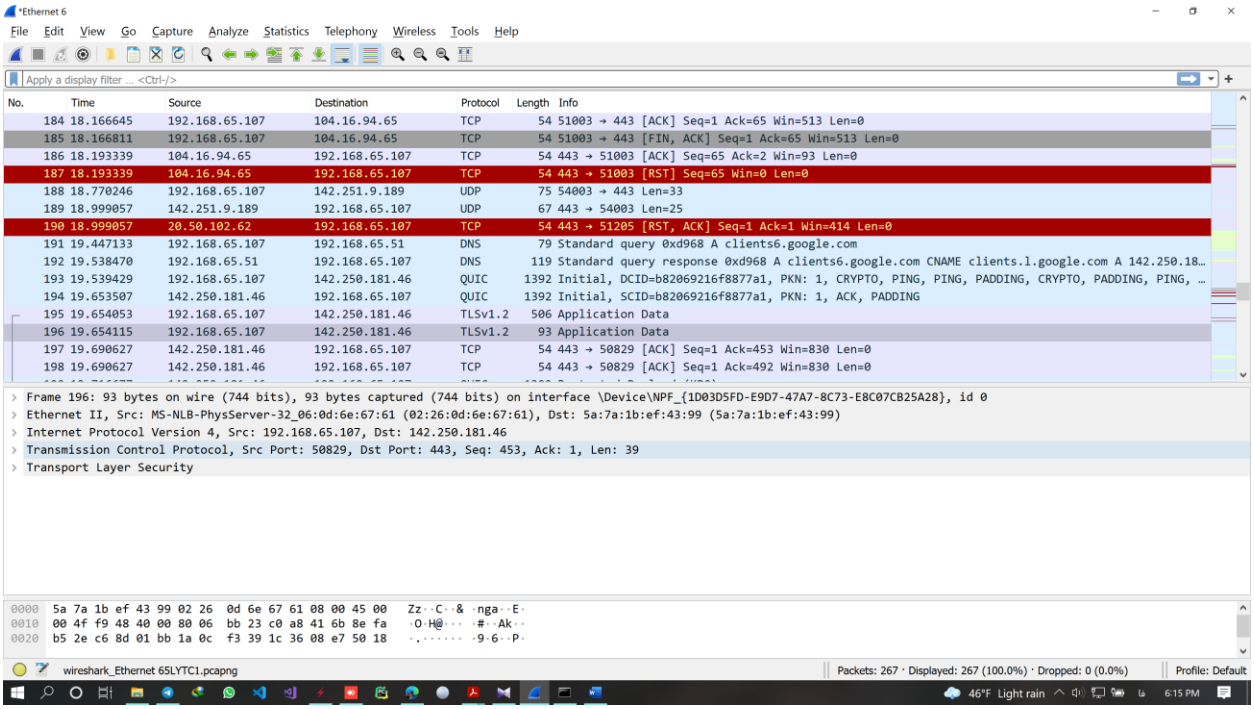
پروتکل هایی مانند TCP، UDP، ARP، TLSv1.2، QUIC مشاهده می شود :





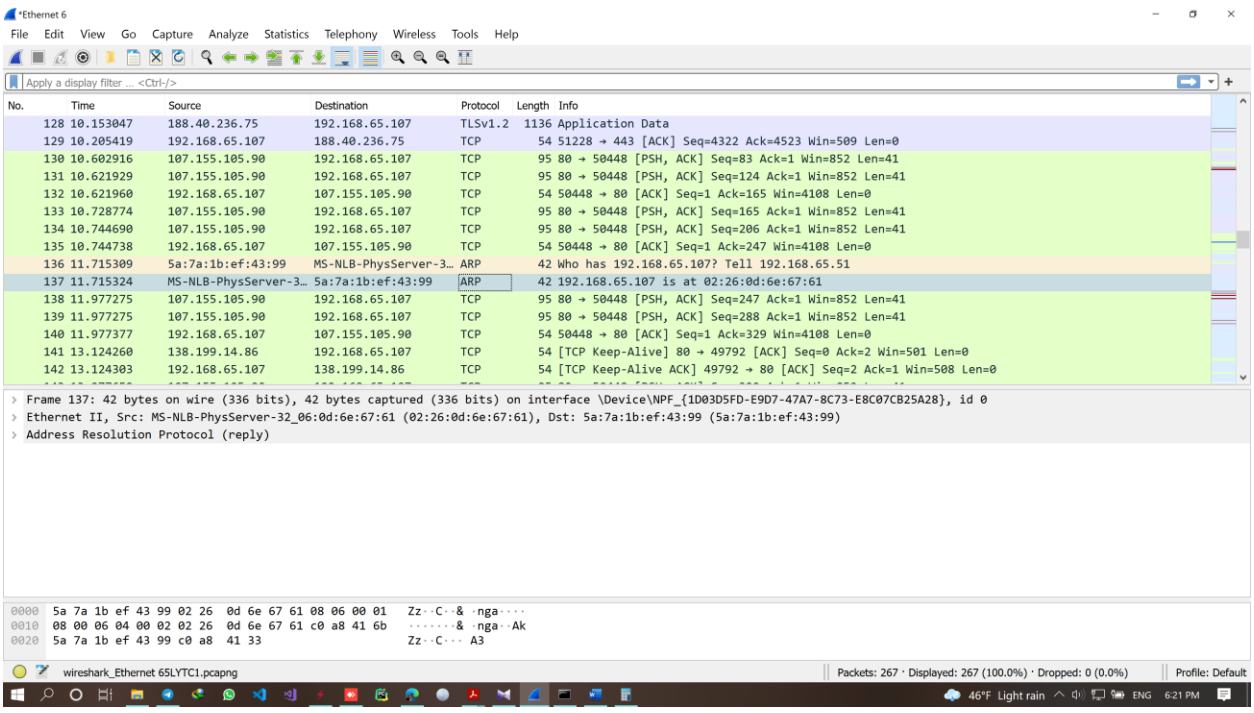
سوال 2 ->

بسته ی انتخاب شده در لایه application پروتکل TLSv1.2 دارد و در لایه transport نیز پروتکل TCP دارد و همین طور IPv4 پروتکل لایه network آن است. اندازه frame آن 196 بوده و اندازه کل بسته آن در لایه سوم 79 است.



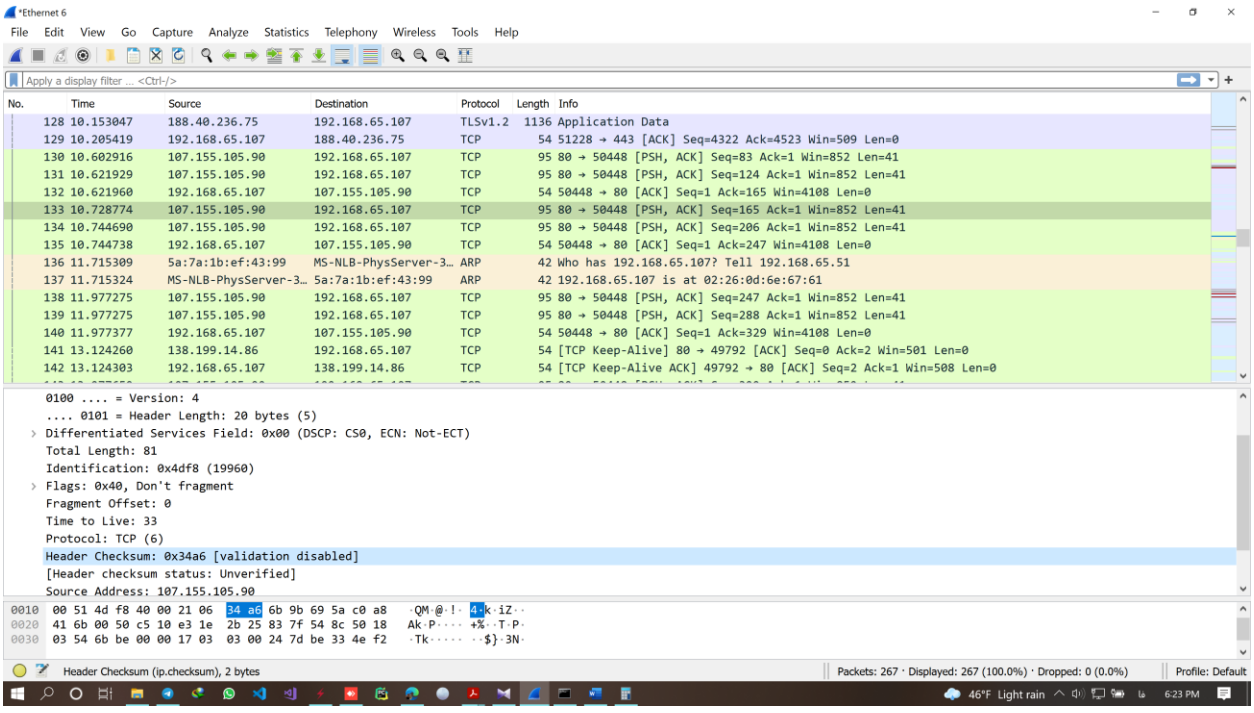
سوال 3 ->

بله، بسته های با پروتکل ARP



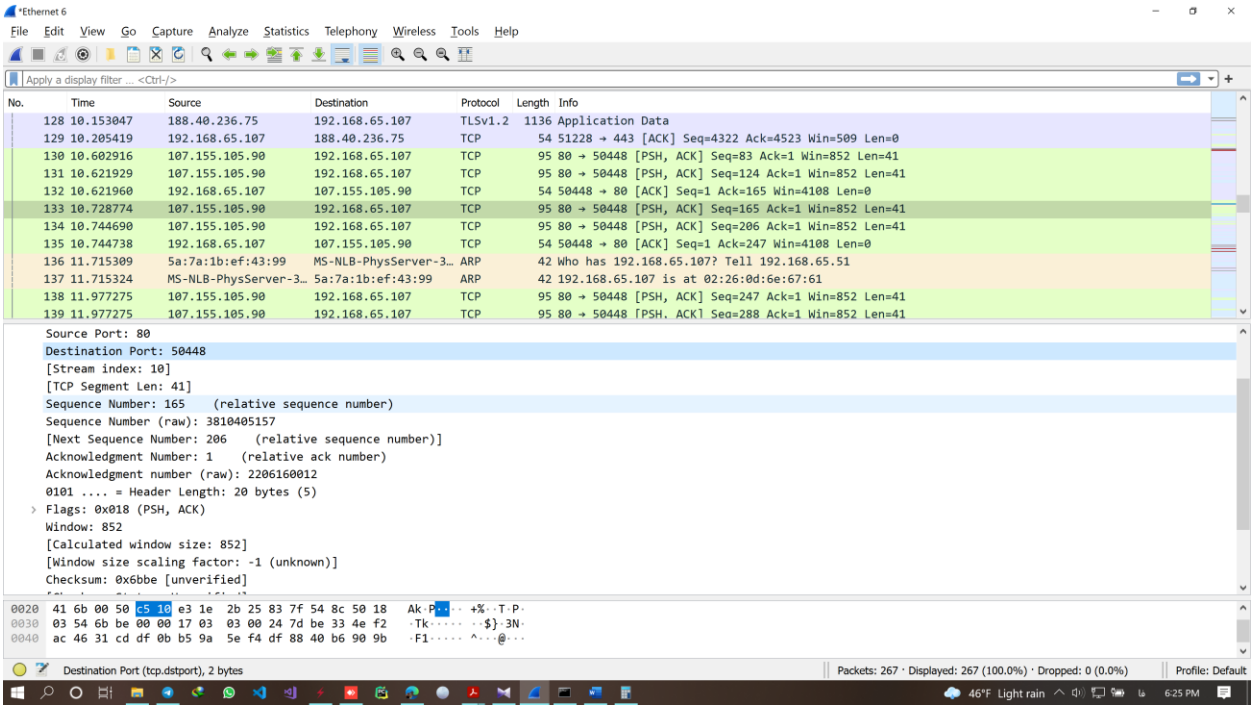
سوال 4 ->

0x34a6

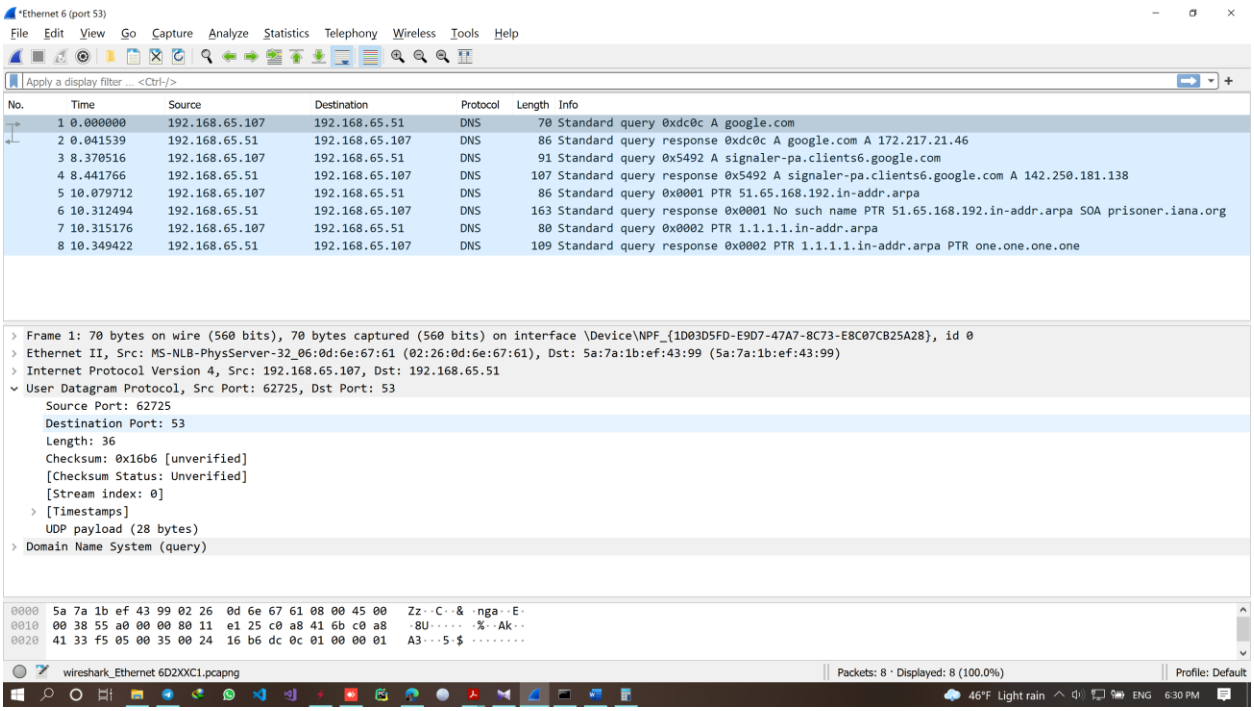


سوال 5 ->

پورت مبدا (فرستنده) 80 و پورت مقصد (گیرنده) 50448 می باشد. پورت گیرنده که در اینجا مربوط به client است به صورت تصادفی انتخاب شده. همینطور checksum برابر 0x6bbe می باشد.



کار با فیلتر کننده بسته ها

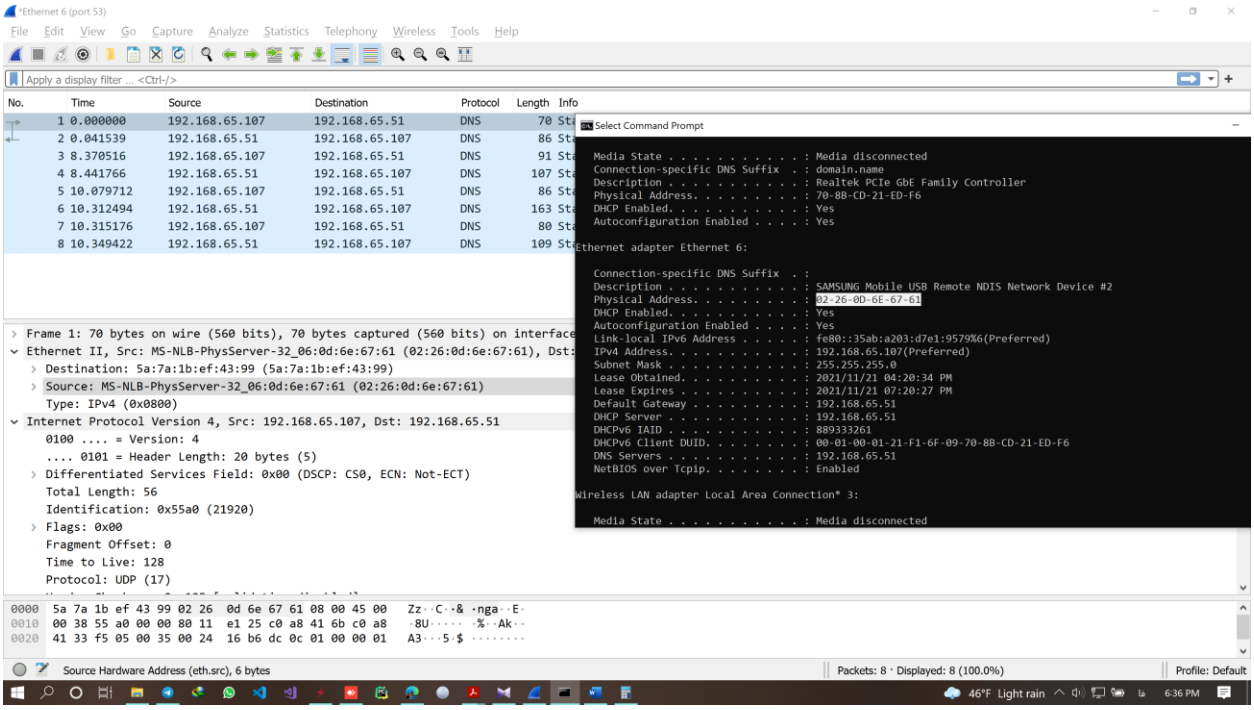


سوال 6 ->

پروتکل لایه transport، UDP بوده و ip مقصد 192.168.65.51 است. آدرس 192.168.65.107 هم آدرس مبدا است که سیستم ما می باشد.

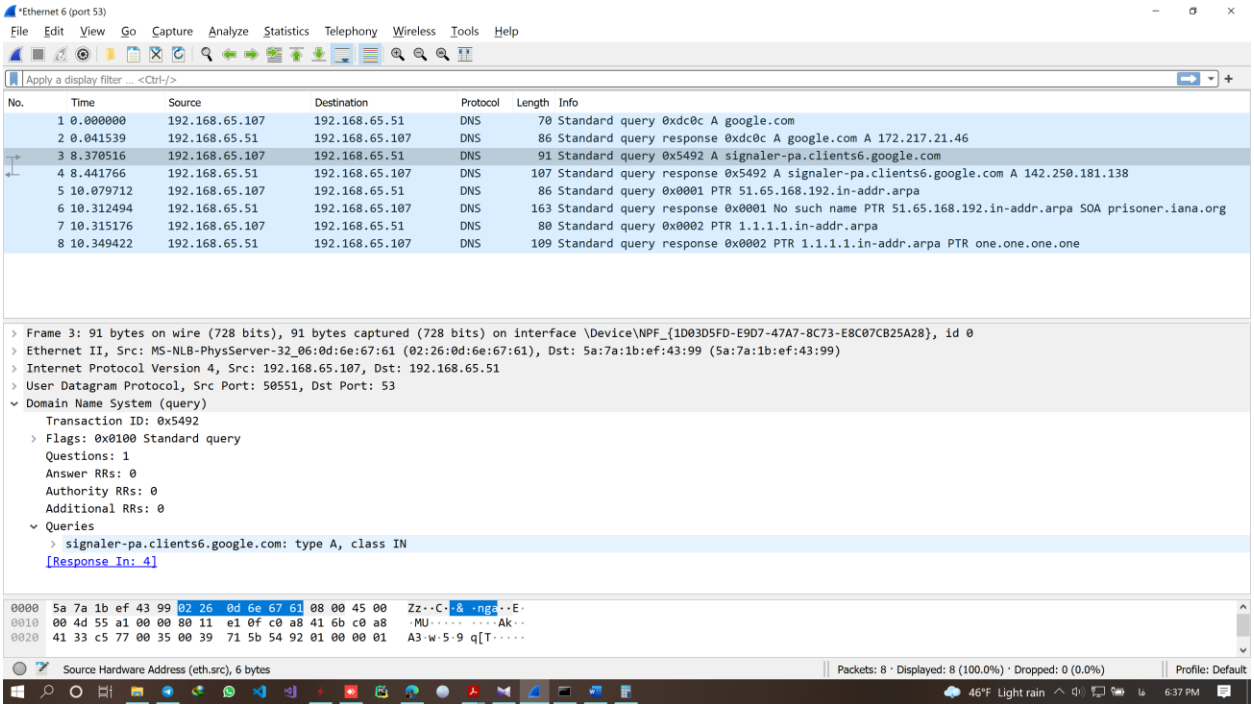
سوال 7 ->

آدرس فیزیکی و آدرس مبدا



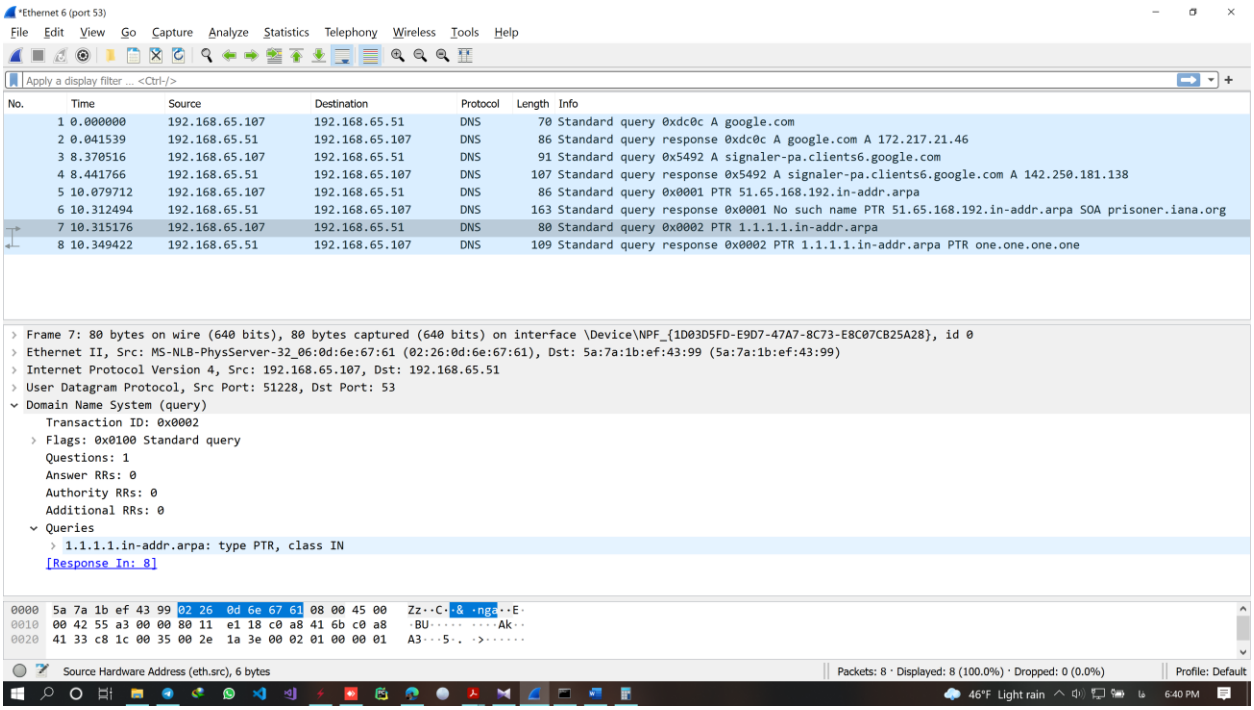
سوال 8 ->

Type A، برای مپ کردن host name به ip address



سوال 9 ->

تایپ PTR که نام دامنه را باز میگرداند

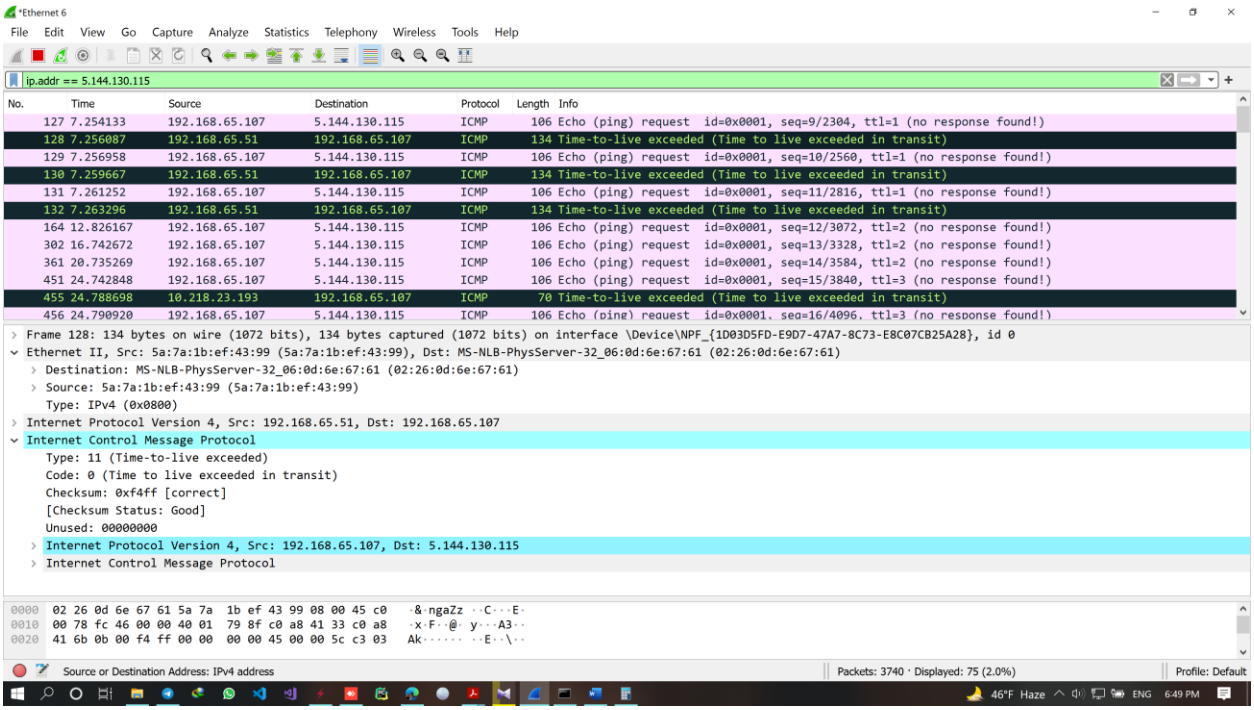


سوال 10 ->

AAAA, APL, CDS, CERT

سوال 11 ->

مقصد یا مبدا همه آدرس داده شده است و همه پروتکل ICMP دارند.



سوال 12 ->

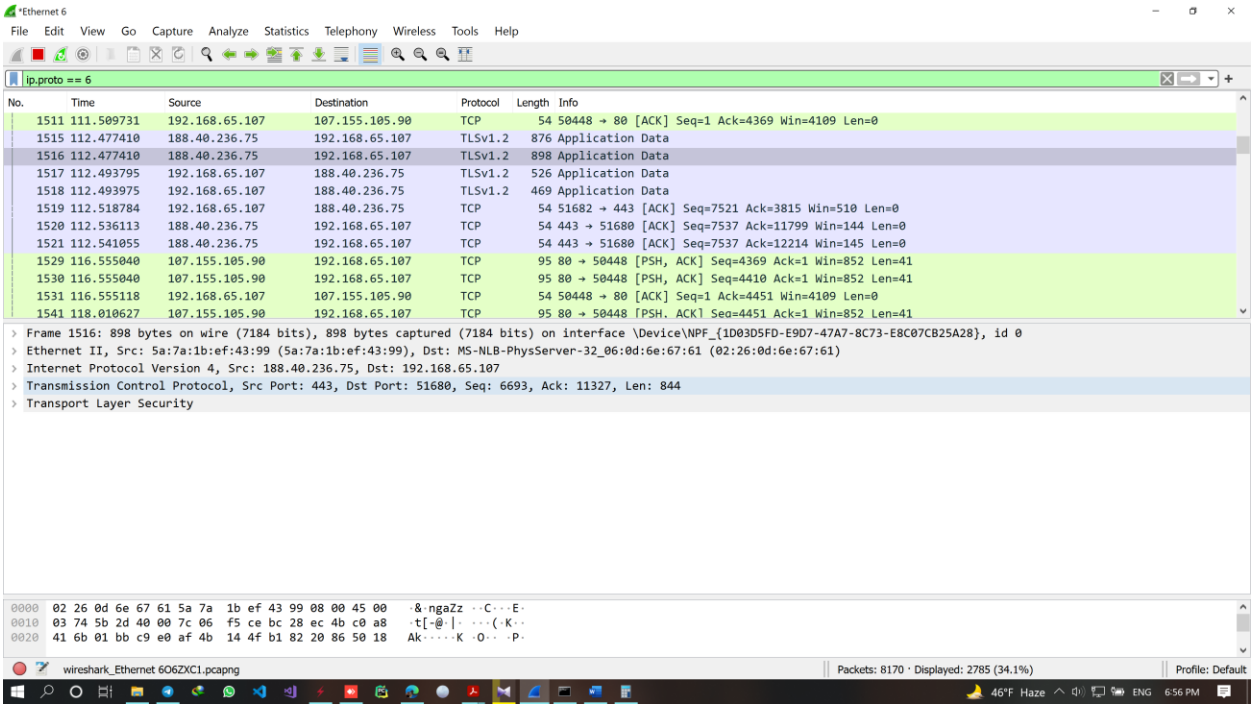
تایپ 11 و TTL 64 می باشد.

سوال 13 ->

TTL مدت زمانی است که بسته می تواند بماند و از بین نرود یعنی اگر 64 باشد یعنی تا 64 گام می ماند. به نظر بنده TTL گاهی در مراحلی افزایش می یابد که بتواند زنده بماند.

سوال 14 ->

تنها اینترنت پروتکل TCP را نشان می دهد.


*Ethernet 6
File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help
ip.proto == 6
No. Time Source Destination Protocol Length Info
1511 111.509731 192.168.65.107 107.155.105.90 TCP 54 50448 → 80 [ACK] Seq=1 Ack=4369 Win=4109 Len=0
1515 112.477410 188.40.236.75 192.168.65.107 TLSv1.2 876 Application Data
1516 112.477410 188.40.236.75 192.168.65.107 TLSv1.2 898 Application Data
1517 112.493795 192.168.65.107 188.40.236.75 TLSv1.2 526 Application Data
1518 112.493975 192.168.65.107 188.40.236.75 TLSv1.2 469 Application Data
1519 112.518784 192.168.65.107 188.40.236.75 TCP 54 51682 → 443 [ACK] Seq=7521 Ack=3815 Win=510 Len=0
1520 112.536113 188.40.236.75 192.168.65.107 TCP 54 443 → 51680 [ACK] Seq=7537 Ack=11799 Win=144 Len=0
1521 112.541055 188.40.236.75 192.168.65.107 TCP 54 443 → 51680 [ACK] Seq=7537 Ack=12214 Win=145 Len=0
1529 116.555040 107.155.105.90 192.168.65.107 TCP 95 80 → 50448 [PSH, ACK] Seq=4369 Ack=1 Win=852 Len=41
1530 116.555040 107.155.105.90 192.168.65.107 TCP 95 80 → 50448 [PSH, ACK] Seq=4410 Ack=1 Win=852 Len=41
1531 116.555118 192.168.65.107 107.155.105.90 TCP 54 50448 → 80 [ACK] Seq=1 Ack=4451 Win=4109 Len=0
1541 118.010627 107.155.105.90 192.168.65.107 TCP 95 80 → 50448 [PSH, ACK] Seq=4451 Ack=1 Win=852 Len=41
Frame 1516: 898 bytes on wire (7184 bits), 898 bytes captured (7184 bits) on interface \Device\NPF_{1D03D5FD-E9D7-47A7-8C73-E8C07CB25A28}, id 0
Ethernet II, Src: 5a:7a:1b:ef:43:99 (5a:7a:1b:ef:43:99), Dst: MS-NLB-PhysServer-32_06:0d:6e:67:61 (02:26:0d:6e:67:61)
Internet Protocol Version 4, Src: 188.40.236.75, Dst: 192.168.65.107
Transmission Control Protocol, Src Port: 443, Dst Port: 51680, Seq: 6693, Ack: 11327, Len: 844
Transport Layer Security
0000 02 26 0d 6e 67 61 5a 7a 1b ef 43 99 08 00 45 00
0010 03 74 5b 2d 40 00 7c 06 f5 ce bc 28 ec 4b c0 a8
0020 41 6b 01 bb c9 e0 af 4b 14 4f b1 82 20 86 50 18
wireshark_Ethernet 6O6ZXC1.pcapng
Packets: 8170 · Displayed: 2785 (34.1%)
Profile: Default
46°F Haze
ENG
6:56 PM