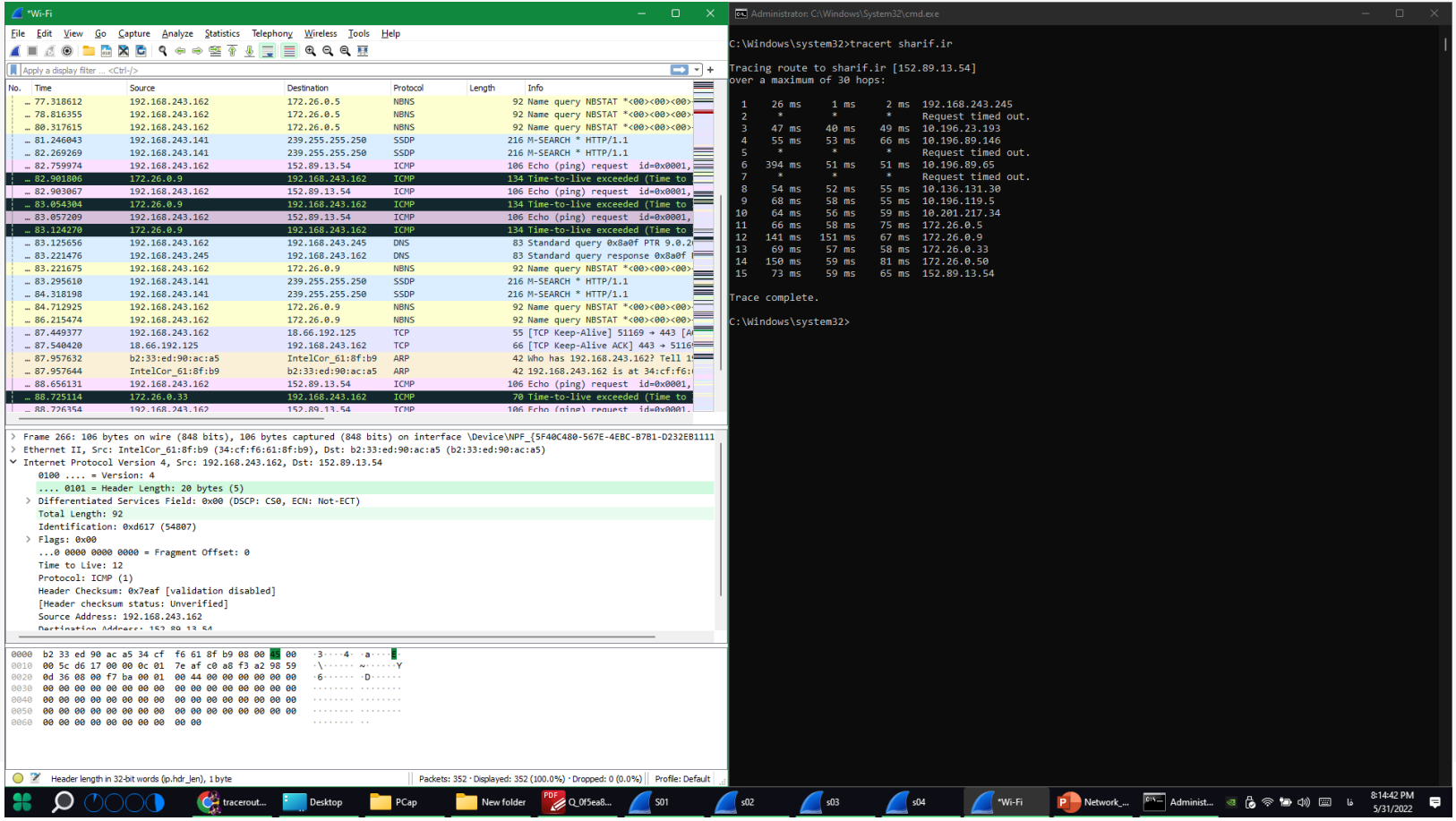
شبکه های کامپیوتری

امتحان وایرشارک

مصطفی فضلی - ۹۸۲۲۸۰۳

سوال 1


*Wi-Fi
File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help
Apply a display filter ... <Ctrl-/>
No. Time Source Destination Protocol Length Info
77.318612 192.168.243.162 172.26.0.5 NBNS 92 Name query NBSTAT *<00><00><00>
78.816355 192.168.243.162 172.26.0.5 NBNS 92 Name query NBSTAT *<00><00><00>
80.317615 192.168.243.162 172.26.0.5 NBNS 92 Name query NBSTAT *<00><00><00>
81.246043 192.168.243.141 239.255.255.250 SSDP 216 M-SEARCH * HTTP/1.1
82.269269 192.168.243.141 239.255.255.250 SSDP 216 M-SEARCH * HTTP/1.1
82.759974 192.168.243.162 152.89.13.54 ICMP 106 Echo (ping) request id=0x0001,
82.901806 172.26.0.9 192.168.243.162 ICMP 134 Time-to-live exceeded (Time to
82.903067 192.168.243.162 152.89.13.54 ICMP 106 Echo (ping) request id=0x0001,
83.054304 172.26.0.9 192.168.243.162 ICMP 134 Time-to-live exceeded (Time to
83.057209 192.168.243.162 152.89.13.54 ICMP 106 Echo (ping) request id=0x0001,
83.124270 172.26.0.9 192.168.243.162 ICMP 134 Time-to-live exceeded (Time to
83.125656 192.168.243.162 192.168.243.245 DNS 83 Standard query 0x8a0f PTR 9.0.2
83.221476 192.168.243.245 192.168.243.162 DNS 83 Standard query response 0x8a0f
83.221675 192.168.243.162 172.26.0.9 NBNS 92 Name query NBSTAT *<00><00><00>
83.295610 192.168.243.141 239.255.255.250 SSDP 216 M-SEARCH * HTTP/1.1
84.318198 192.168.243.141 239.255.255.250 SSDP 216 M-SEARCH * HTTP/1.1
84.712925 192.168.243.162 172.26.0.9 NBNS 92 Name query NBSTAT *<00><00><00>
86.215474 192.168.243.162 172.26.0.9 NBNS 92 Name query NBSTAT *<00><00><00>
87.449377 192.168.243.162 18.66.192.125 TCP 55 [TCP Keep-Alive] 51169 → 443 [A
87.540420 18.66.192.125 192.168.243.162 TCP 66 [TCP Keep-Alive ACK] 443 → 5116
87.957632 b2:33:ed:90:ac:a5 IntelCor_61:8f:b9 ARP 42 Who has 192.168.243.162? Tell 1
87.957644 IntelCor_61:8f:b9 b2:33:ed:90:ac:a5 ARP 42 192.168.243.162 is at 34:cf:f6:
88.656131 192.168.243.162 152.89.13.54 ICMP 106 Echo (ping) request id=0x0001,
88.725114 172.26.0.33 192.168.243.162 ICMP 70 Time-to-live exceeded (Time to
Frame 266: 106 bytes on wire (848 bits), 106 bytes captured (848 bits) on interface \Device\NPF_{5F40C480-567E-4EBC-B7B1-D232EB1111
Ethernet II, Src: IntelCor_61:8f:b9 (34:cf:f6:61:8f:b9), Dst: b2:33:ed:90:ac:a5 (b2:33:ed:90:ac:a5)
Internet Protocol Version 4, Src: 192.168.243.162, Dst: 152.89.13.54
0100 .... = Version: 4
.... 0101 = Header Length: 20 bytes (5)
Differentiated Services Field: 0x00 (DSCP: CS0, ECN: Not-ECT)
Total Length: 92
Identification: 0xd617 (54807)
Flags: 0x00
...0 0000 0000 0000 = Fragment Offset: 0
Time to Live: 12
Protocol: ICMP (1)
Header Checksum: 0x7eaf [validation disabled]
[Header checksum status: Unverified]
Source Address: 192.168.243.162
0000 b2 33 ed 90 ac a5 34 cf f6 61 8f b9 08 00 45 00
0010 00 5c d6 17 00 00 0c 01 7e af c0 a8 f3 a2 98 59
0020 0d 36 08 00 f7 ba 00 01 00 44 00 00 00 00 00 00
0030 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
0040 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
0050 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
0060 00 00 00 00 00 00 00 00 00 00
Header length in 32-bit words (ip.hdr_len), 1 byte
Packets: 352 · Displayed: 352 (100.0%) · Dropped: 0 (0.0%)
Profile: Default
Administrator: C:\Windows\System32\cmd.exe
C:\Windows\system32>tracert sharif.ir
Tracing route to sharif.ir [152.89.13.54]
over a maximum of 30 hops:
1 26 ms 1 ms 2 ms 192.168.243.245
2 * * * Request timed out.
3 47 ms 40 ms 49 ms 10.196.23.193
4 55 ms 53 ms 66 ms 10.196.89.146
5 * * * Request timed out.
6 394 ms 51 ms 51 ms 10.196.89.65
7 * * * Request timed out.
8 54 ms 52 ms 55 ms 10.136.131.30
9 68 ms 58 ms 55 ms 10.196.119.5
10 64 ms 56 ms 59 ms 10.201.217.34
11 66 ms 58 ms 75 ms 172.26.0.5
12 141 ms 151 ms 67 ms 172.26.0.9
13 69 ms 57 ms 58 ms 172.26.0.33
14 150 ms 59 ms 81 ms 172.26.0.50
15 73 ms 59 ms 65 ms 152.89.13.54
Trace complete.
C:\Windows\system32>
tracerout...
Desktop
PCap
New folder
Q_0f5ea8...
S01
s02
s03
s04
*Wi-Fi
Network_...
Administ...
8:14:42 PM
5/31/2022

دستور traceroute در cmd ویندوز فعال نیست، به همین دلیل از دستور tracert استفاده می کنیم که همانند این دستور است. اسکرین شات این بخش در نیمه سمت راست صفحه نمایش آمده است.

بخش اول

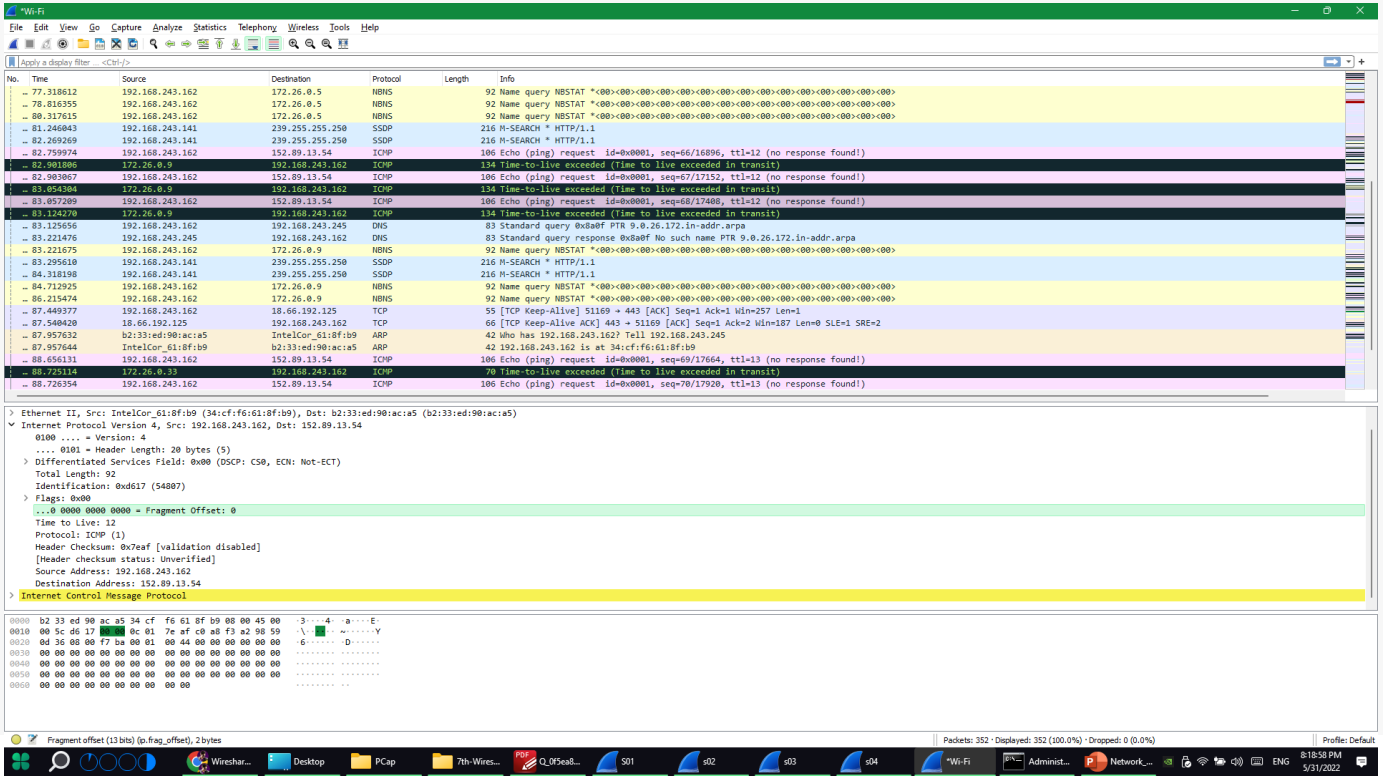
همزمان با این دستور فرآیند رهگیری پکت‌ها وایرشارک را فعال می کنیم، در این هنگام می توانیم طول هدر را مشاهده می کنیم که برابر ۲۰ بایت است.

طول payload برابر طول کل پکت منهای طول هدر فایل است که طول کل پکت برابر ۹۲ بایت است و اگر ۲۰ بایت را از آن کم کنیم برابر ۷۲ بایت است.

92−20=72

بخش دوم

اگر بخش fragment offset برابر صفر باشد، بدین معناست که این پکت دارای تکه بعدی نمی باشد.



بخش سوم

فیلد هایی که ثابت می مانند:

ورژن (بخاطر این است که همه پکت ها از یک ورژن آیپی استفاده می کنند)

طول هدر (همه پکت ها از نوع ICMP هستند)

آیپی مبدا (اطلاعات از یک مبدا ارسال می شوند)

آیپی مقصد (اطلاعات به یک مقصد ارسال می شوند)

لایه بالایی پروتکل (هنگامی که همه پکت ها از نوع ICMP هستند)

خدمات مختلف

فیلد هایی که باید ثابت بمانند:

ورژن (بخاطر این است که همه پکت ها از یک ورژن آیپی استفاده می کنند)

طول هدر (همه پکت ها از نوع ICMP هستند)

آیپی مبدا (اطلاعات از یک مبدا ارسال می شوند)

آیپی مقصد (اطلاعات به یک مقصد ارسال می شوند)

لایه بالایی پروتکل (هنگامی که همه پکت ها از نوع ICMP هستند)

خدمات های مختلف

فیلد هایی که باید تغییر کنند:

شناسایی (آیدی های پکت های مختلف باید متفاوت باشند)

Time To Live (TTL) با دستور traceroute هر پکت زیرشاخه افزایش می یابد)

Checksum هدر: این بخش با تغییر هدر تغییر میکند)

بخش چهارم

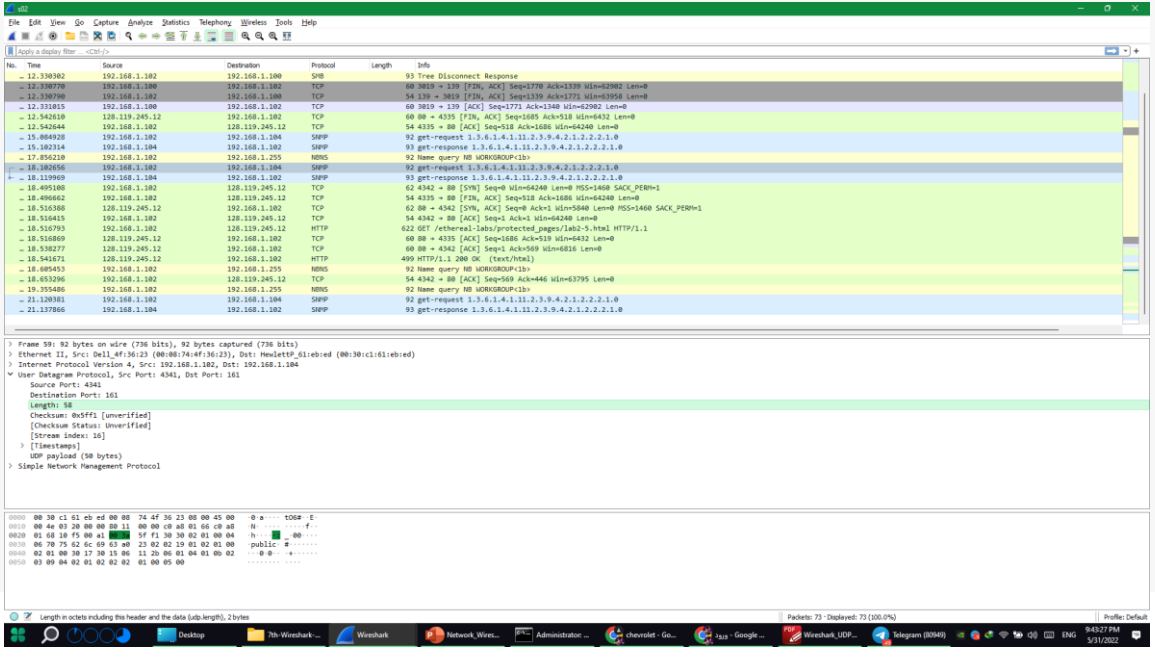
با توجه به طول پکت های ارسال شده مشاهده می شود که از یک تکه (fragment) تشکیل شده است.

در قسمت توضیحات اسلاید می توان متوجه شد که اگر با استفاده از نرم افزار PingPlotter طول پکت های ارسالی را افزایش دهیم، این بخش دارای تکه ها(fragment)های بیشتری می شود.

TCP/UDP .۲

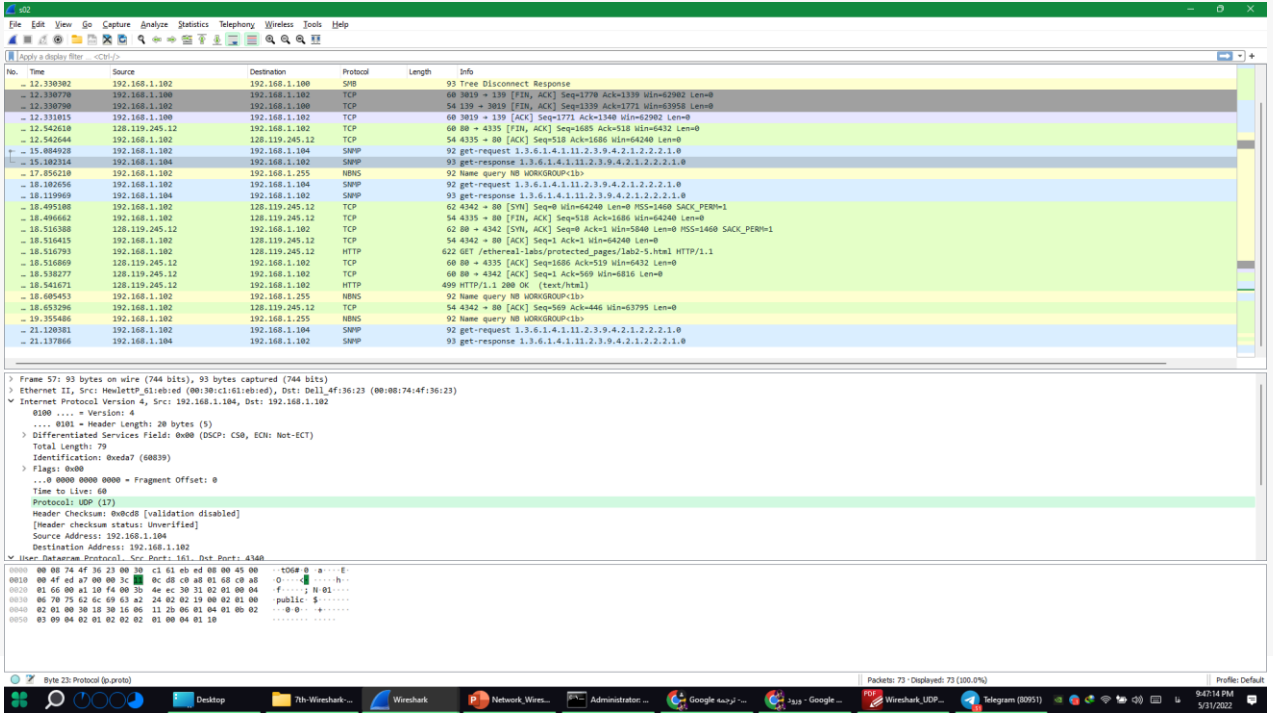
بخش اول

فیلد طول UDPطول فیلدهای هدر و داده های بخش UDPاست.
در بایت اندازه گیری می شود). بسته نمایش داده شده دارای طول فیلد ۵۸ بایت است. ما می دانیم که ۸ بایت هدر وجود دارد. اگر به قسمت محتوای بسته نگاه کنیم، همچنین ۵۰ بایت داده هگزادسیمال یا کدگذاری شده با ASCIIرا پیدا می کنیم که مربوط به بار این بخش UDPاست.



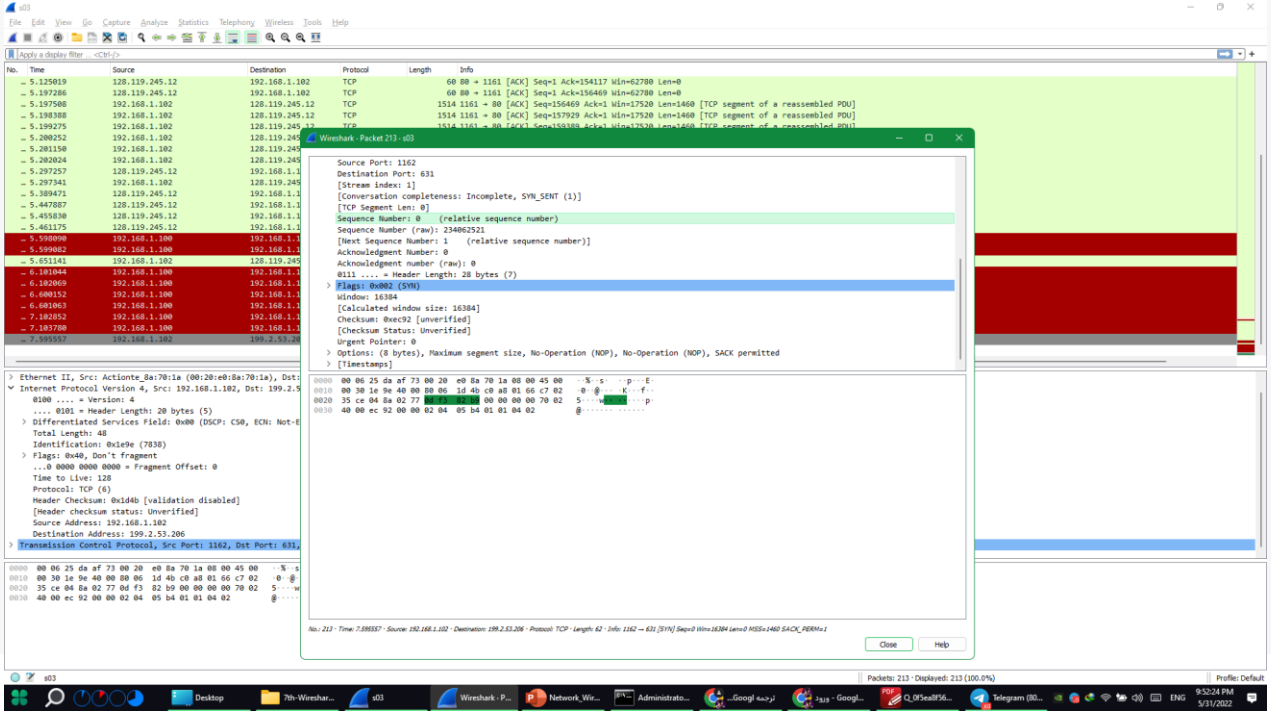
بخش دوم

پورت آن برابر ۱۷ است و عدد هگزادسیمال آن از بخش پائین نمایش داده می شود که برابر ۱۱ در بمنای ۱۶ است.



بخش سوم

این مقدار برابر ترتیب پکت های ارسالی می باشد. و در اینجا برابر ۰ می باشد.



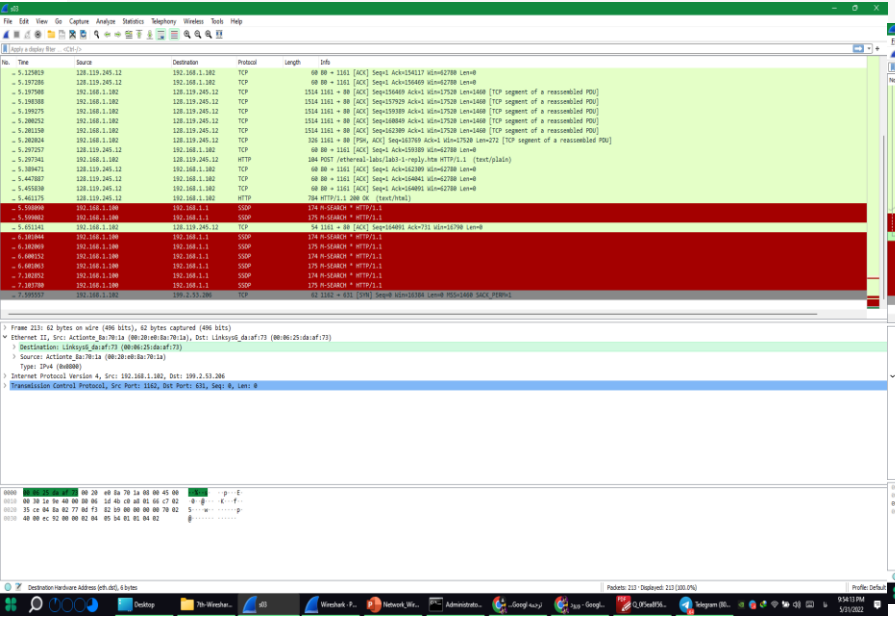
بخش چهارم

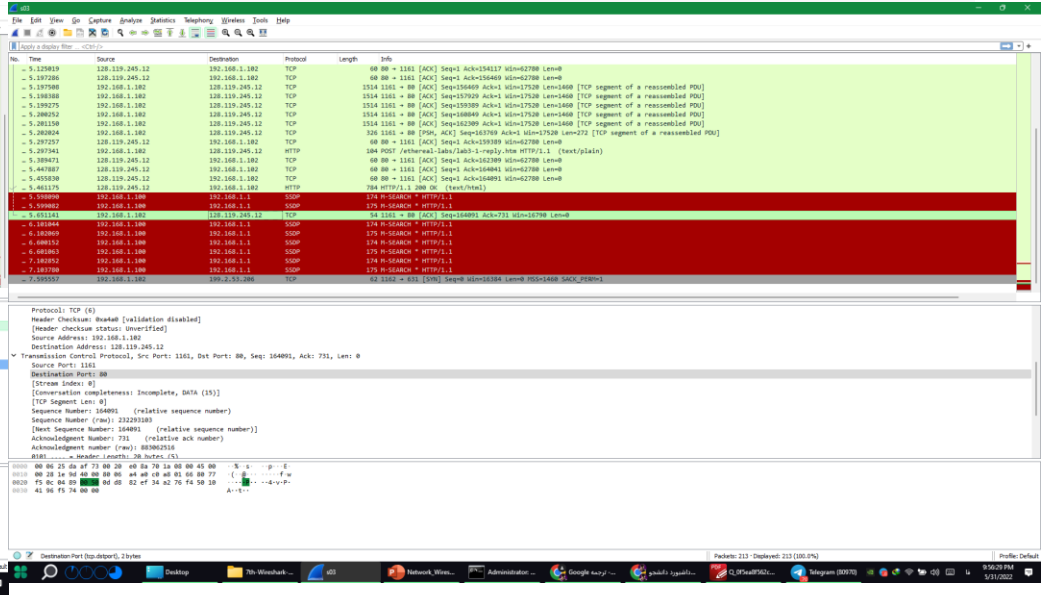
پورت و آیپی با توجه به شکل ها

آیپی مبدا ۱۹۲.۱۶۸.۱.۱۰۲

پورت مبدا ۱۱۶۱ یا ۱۱۶۲

پورت مقصد ۸۰

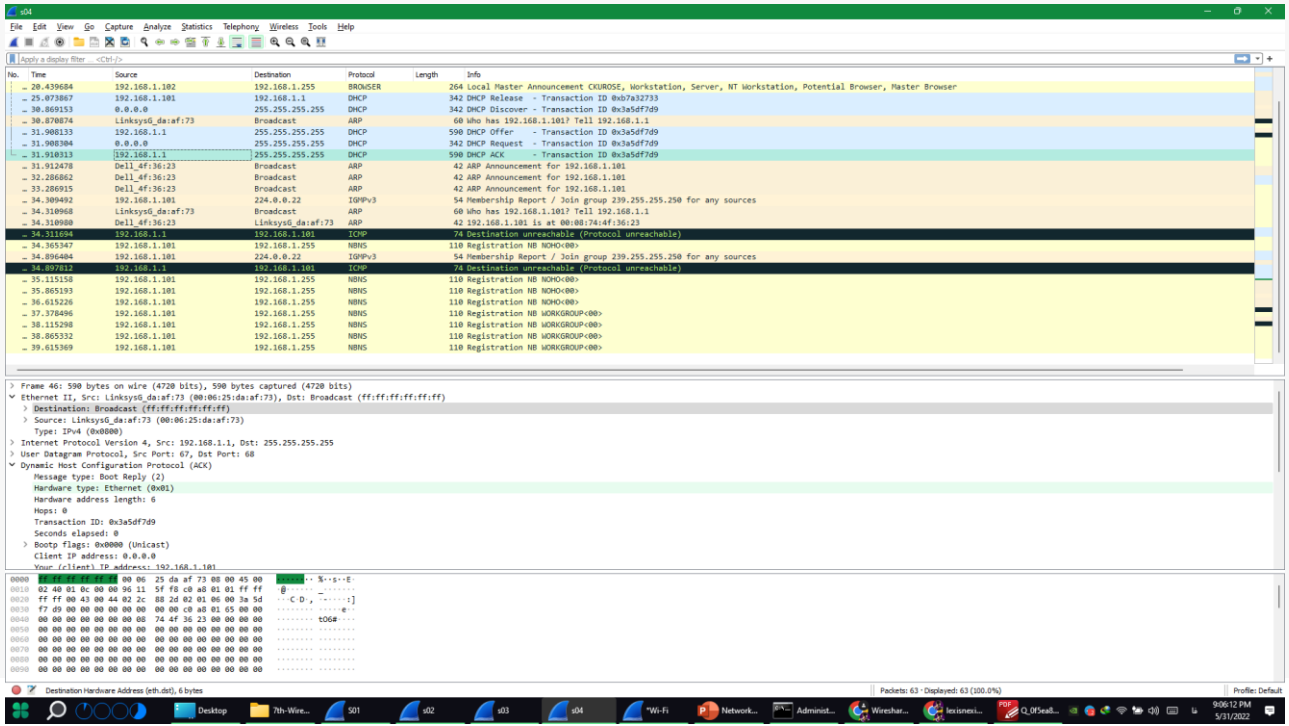




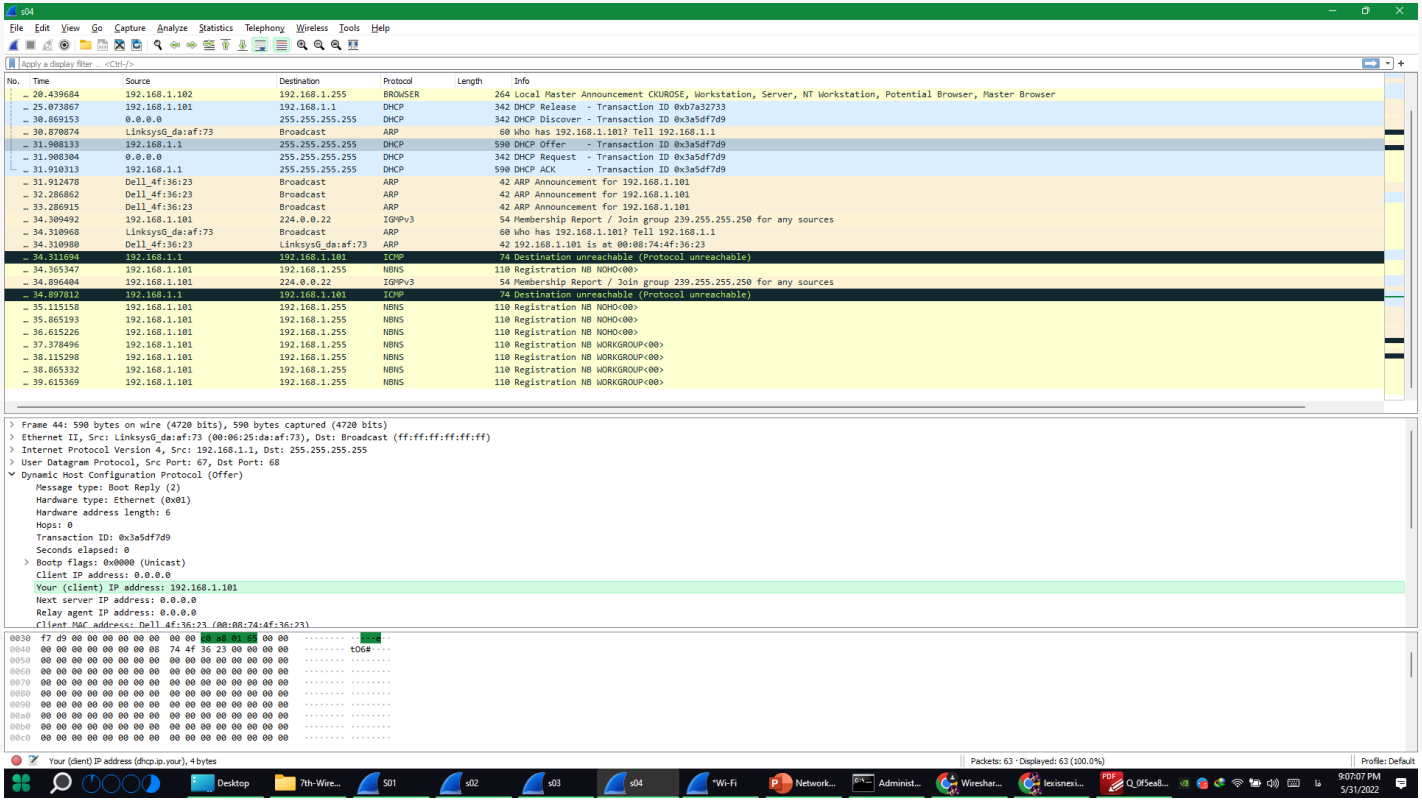
DHCP .۳

بخش اول

آدرس آیپی آن برابر 192.168.1.1 می باشد



بخش دوم
آدرس آیپی پیشنهادی آن برابر ۱۹۲.۱۶۸.۱.۱۰۱ است.



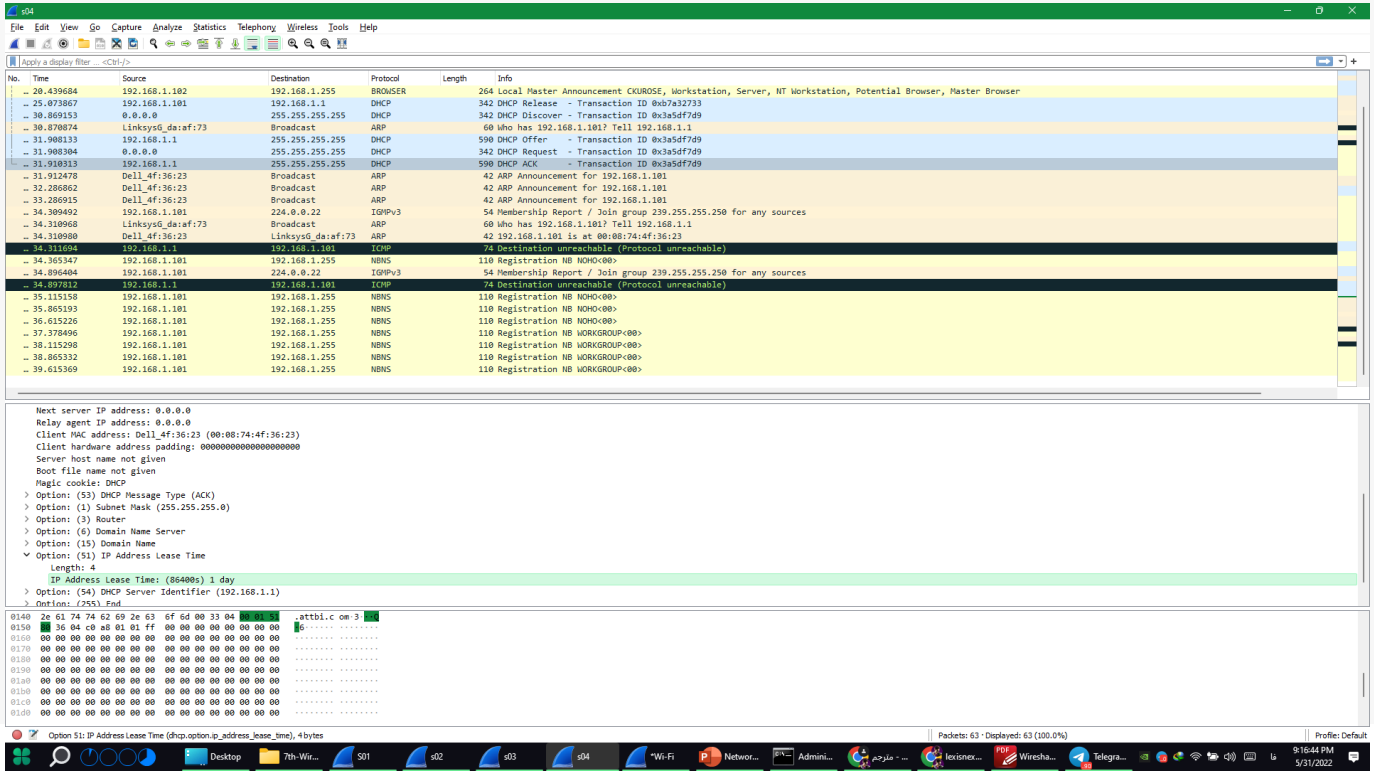
بخش سوم

خط روتر نشان دهنده Default Getwayاست و خط ماسک زیرشبکه را به کلاینت اطلاع رسانی می کند.

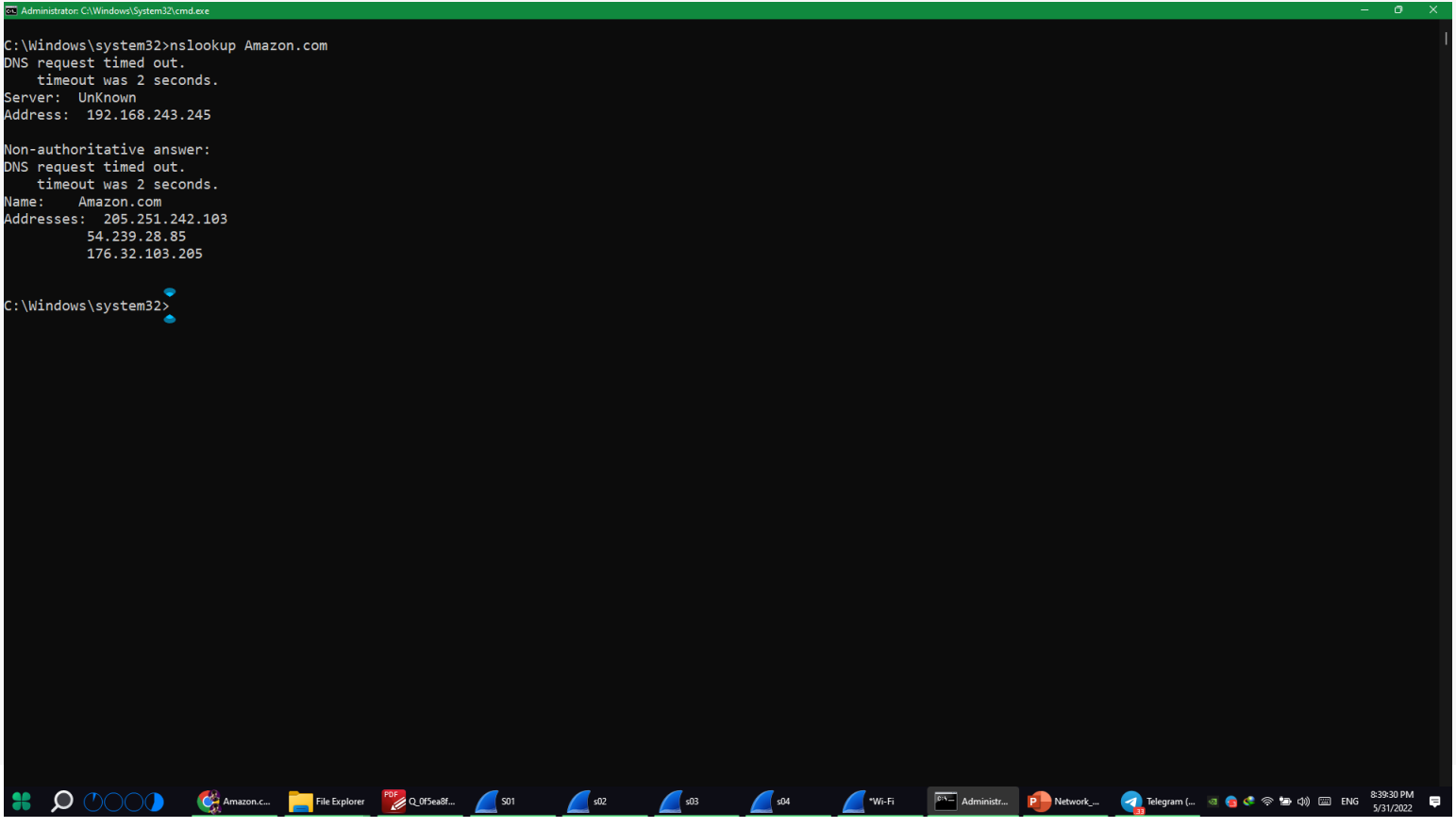
بخش چهارم

این مدت زمانی که که سرور DHCP یک آیپی را به یک کلاینت اختصاص می دهد، در طول این مدت زمان سرور نباید این آیپی را به کس دیگری اختصاص دهد مگر آنکه زمان اجاره آن منقضی شده باشد.

(در این قسمت این مقدار برابر یک روز می باشد)

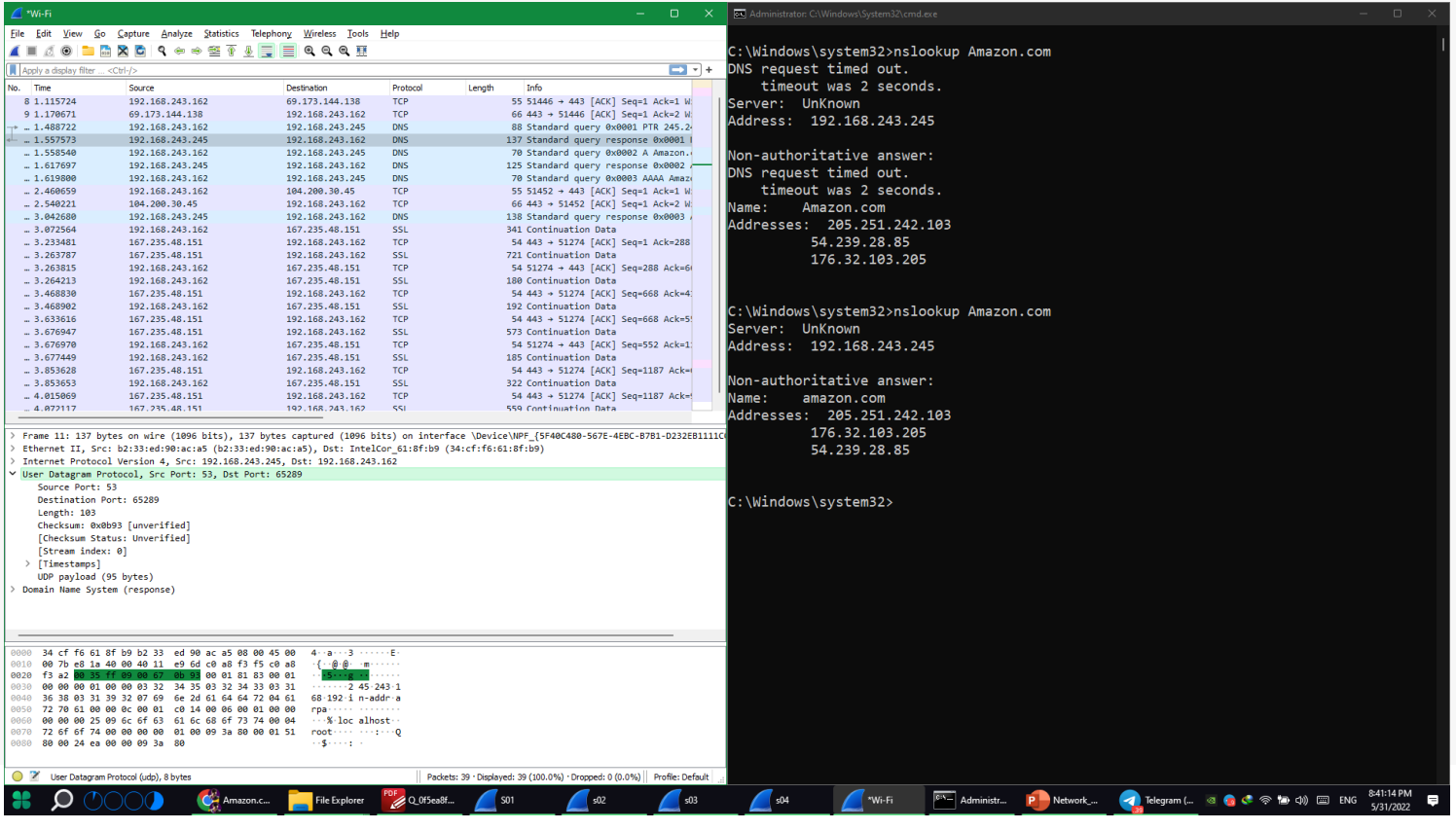


۴. بخش اول DNS


Administrator: C:\Windows\System32\cmd.exe
C:\Windows\system32>nslookup Amazon.com
DNS request timed out.
timeout was 2 seconds.
Server: UnKnown
Address: 192.168.243.245
Non-authoritative answer:
DNS request timed out.
timeout was 2 seconds.
Name: Amazon.com
Addresses: 205.251.242.103
54.239.28.85
176.32.103.205
C:\Windows\system32>

بخش دوم

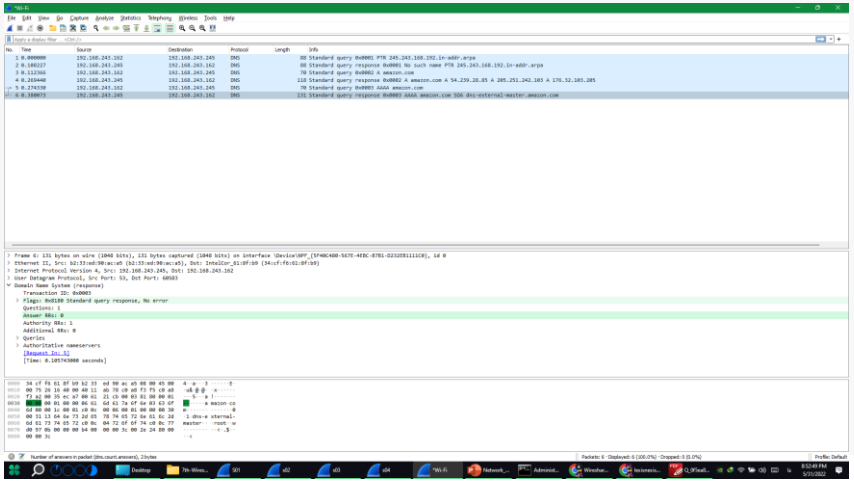
با استفاده از پروتکل های DNS و مشاهده بخش User Datagram Protocol (UDP) می توان این نتیجه را گرفت که بر پایه UDP است.

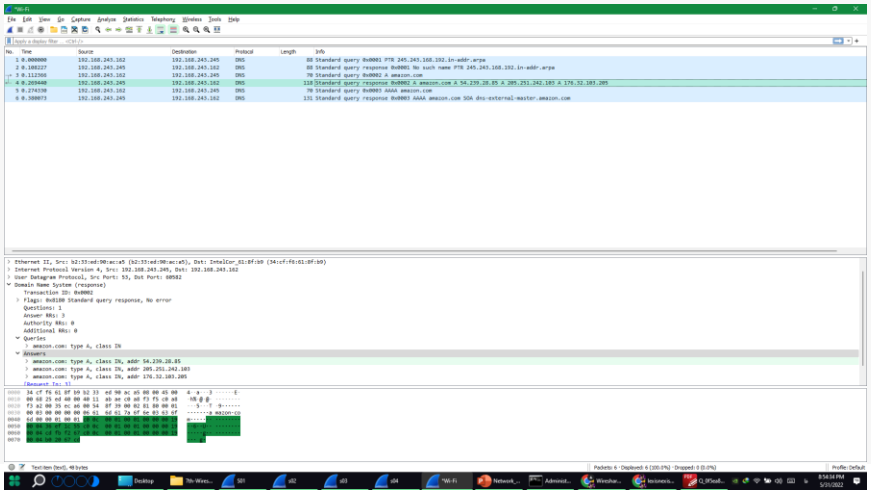


بخش سوم

برخی پکت های ارسال شده خیر این بخش هیچ پاسخی ندارد(اسکرین شات سمت چپ) و برخی چندین پاسخ دارند (اسکرین شات سمت راست).

(طبق پاسخ حل المسائل)



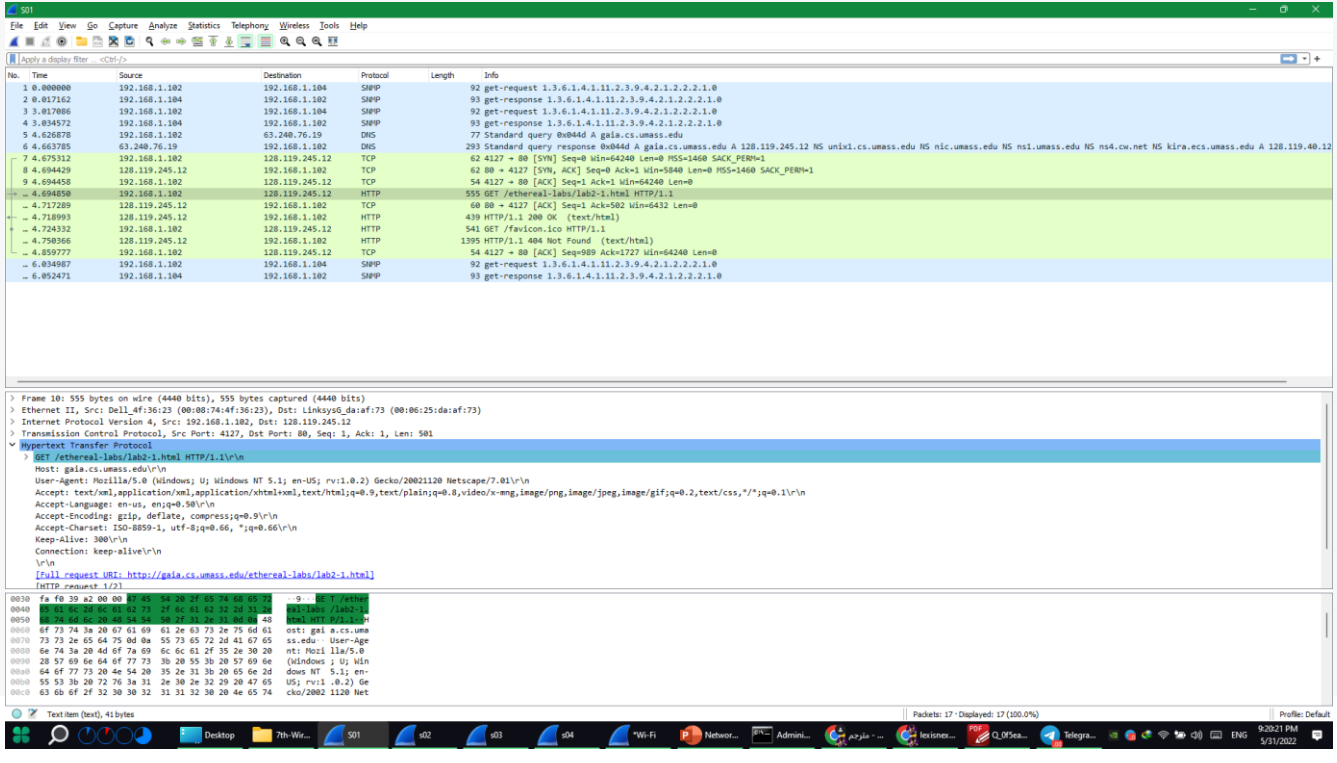


بخش چهارم

خیر اگر سایتی شامل چند عکس باشد هربار در هنگام لود سایت پیش از دریافت عکس ها dns query انجام نمی شود.

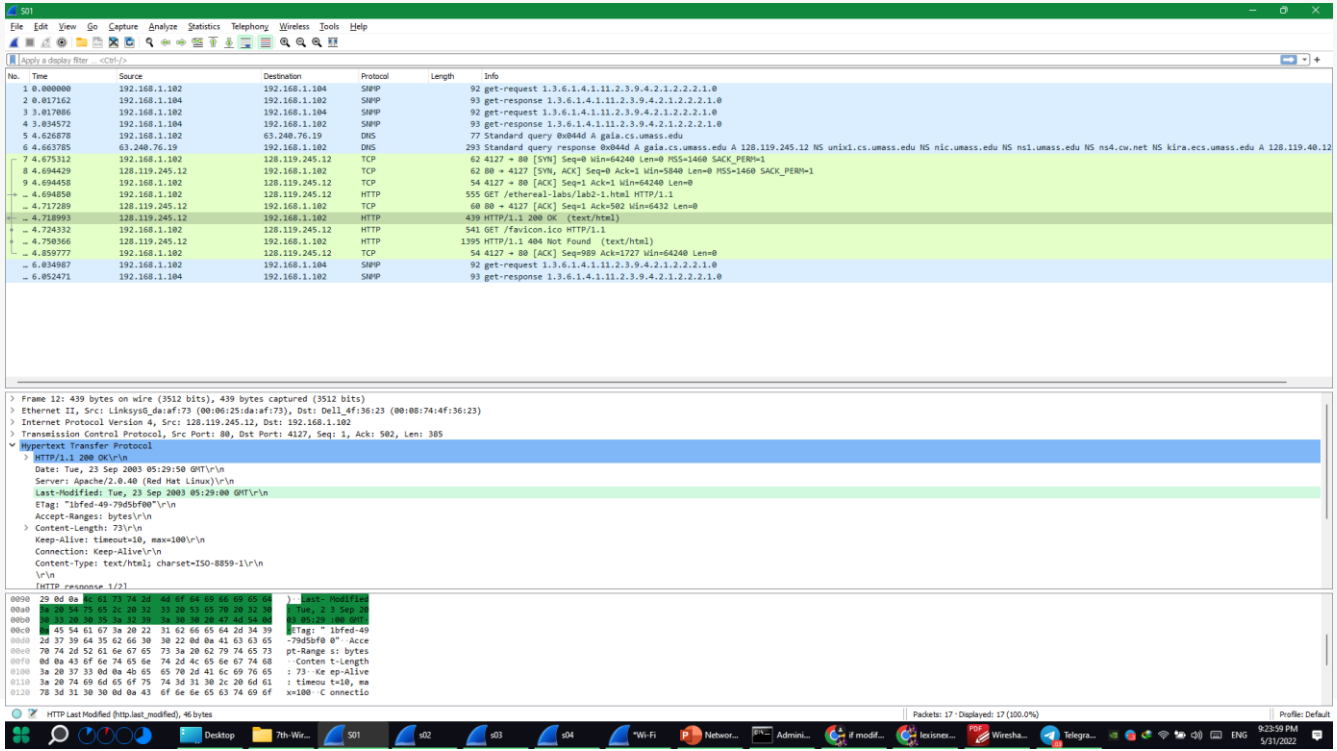
۵. بخش اول HTTP

ورژن **HTTP** برابر ۱.۱ است.



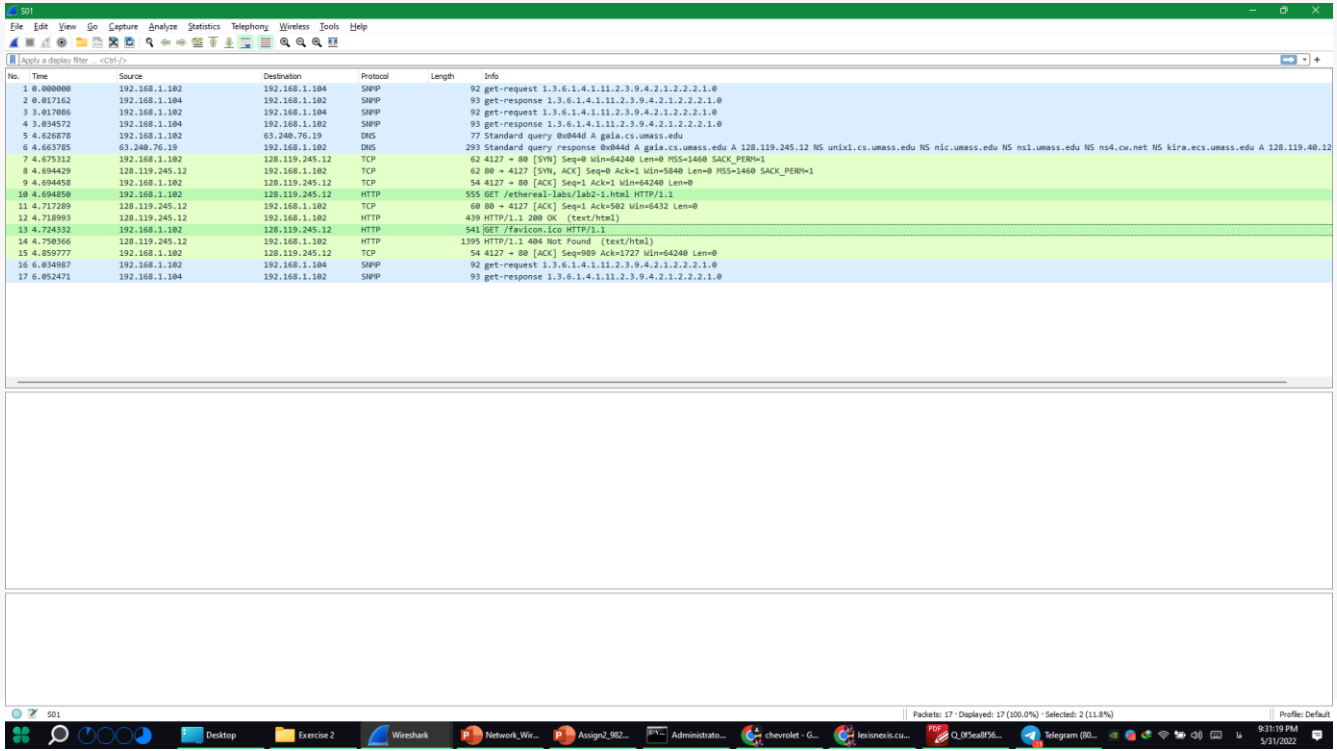
بخش دوم

پروتکل معلوم بررسی میکند که آیا از تاریخی که شئی ذخیره شده در سرور تغییری کرده است یا خیر، اگر این فایل تغییری کرده باشد، سرور شئی را دوباره ارسال میکند، در غیر اینصورت پیغام ۳۰۴ not modified را ارسال میکند تا سرور کش از فایل درون دیتابیس خود استفاده کند.



بخش سوم

با شمارش بخش ها، دارای دو درخواست **Get** است و آدرس آیپی سرور مقصد آن ۱۲۸.۱۱۹.۲۴۵.۱۲ می باشد.



بخش چهارم

بخش **OK** داده شده پروتکل **HTTP** دارای طول ۷۳ بایت است