

دانشگاه صنعتی امیرکبیر

(پلی‌تکنیک تهران)

دانشکده مهندسی کامپیوتر

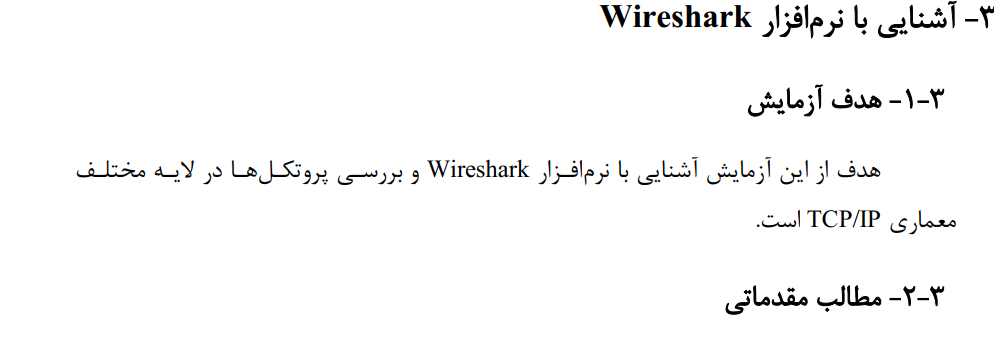
آزمایشگاه شبکه های کامپیوتری

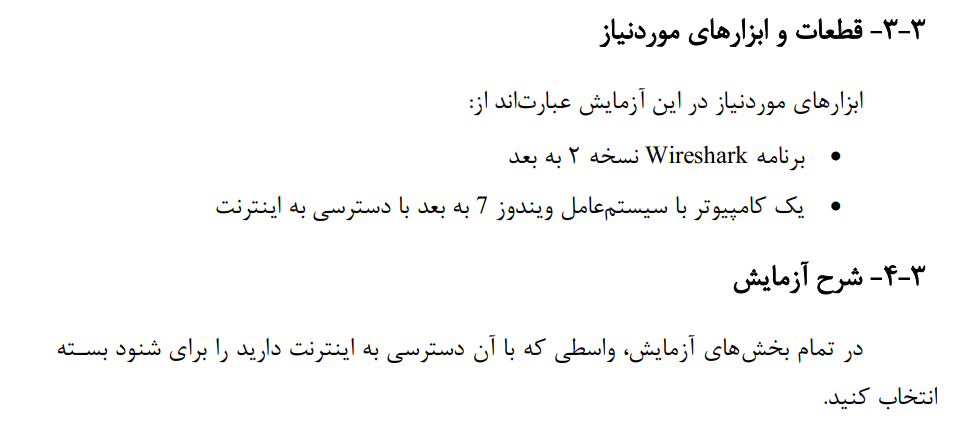
(پاییز ۱۴۰۰)

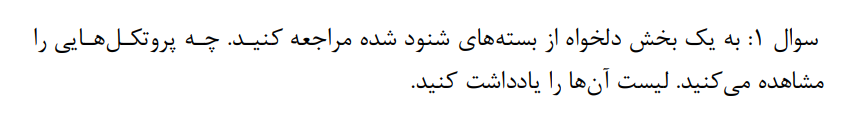
**جلسه دوم**

**آشنایی با ابزار Whire shark**

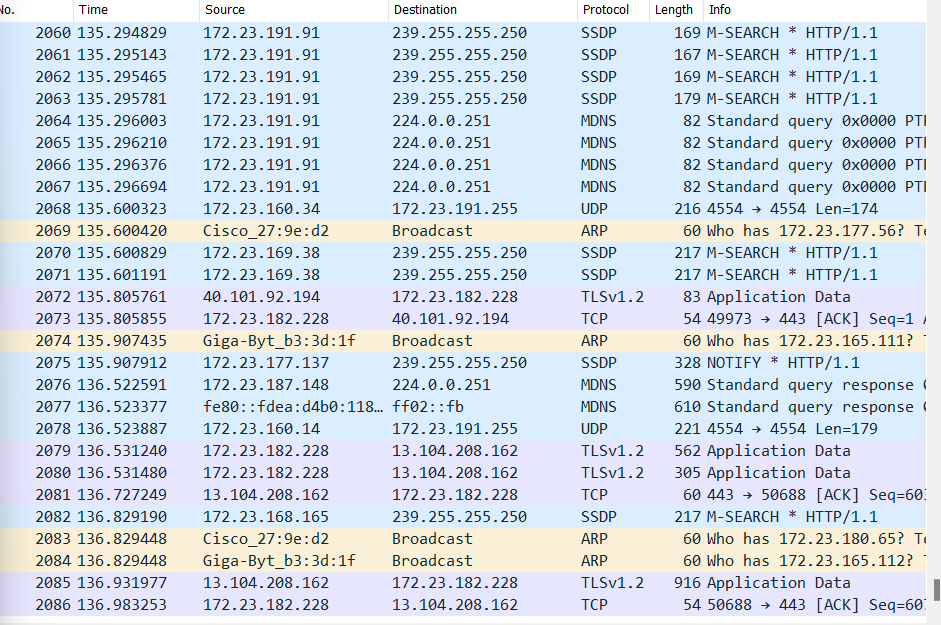
**محمد چوپان 9831125**

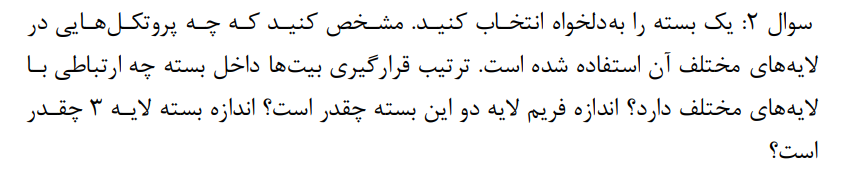


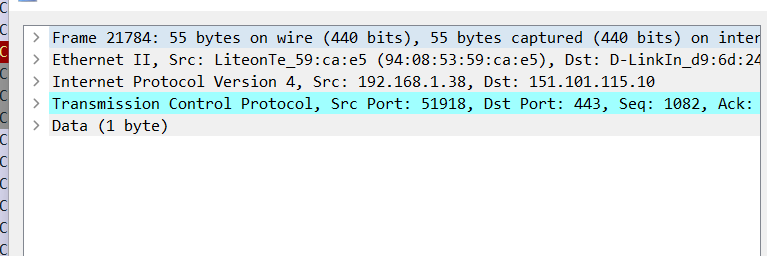




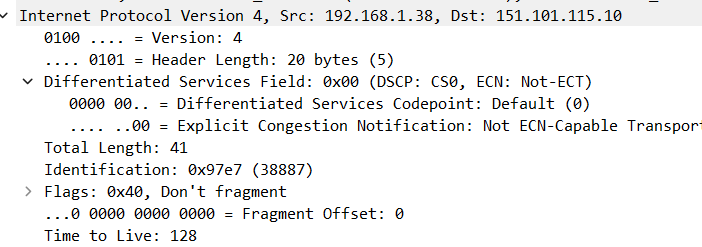
پروتکل های TCP,UDP,ARP,SSDP,MDNS,NBNS,TLS,ICMPV6, قابل مشاهده است.



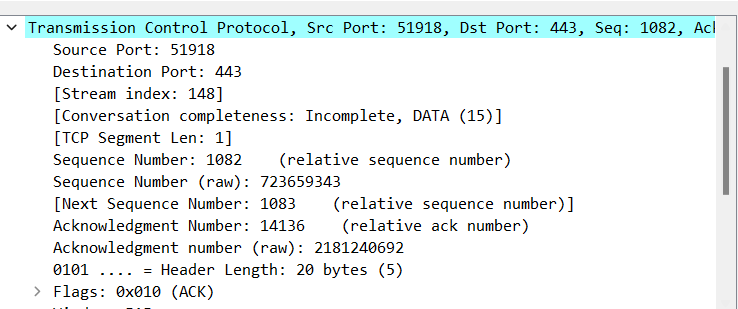




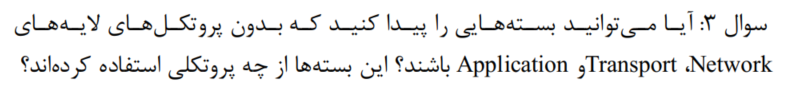
این بسته در لایه application از پروتکل TCP و در لایه Transport نیز از همین پروتکل استفاده می کند و در لایه network از IPV4 استفاده میکند.

شماره frame آن 21784 و مقدار آن برابر با 55 بایت است. 

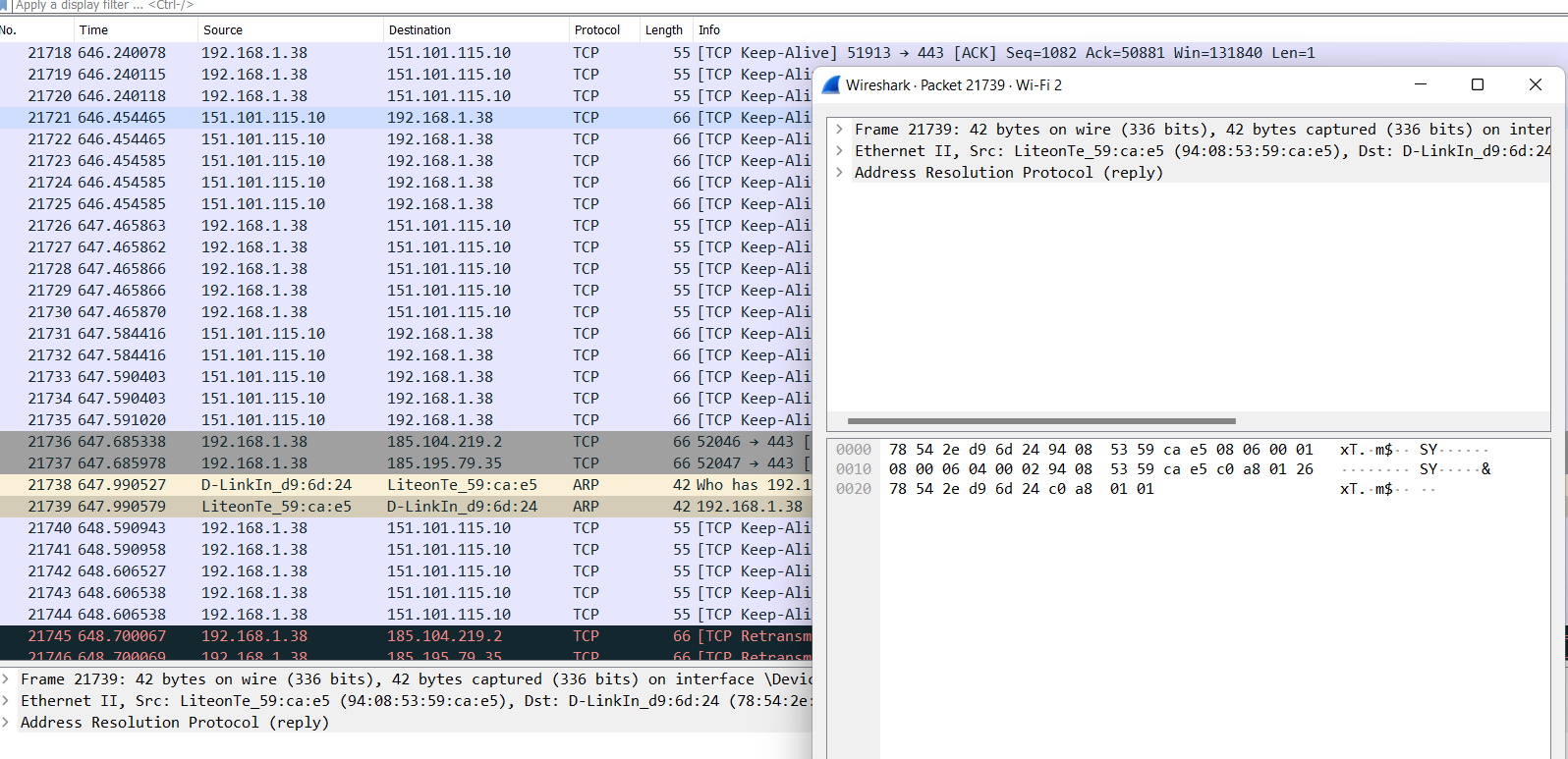
اندازه کل آن در این لایه برابر 41 بایت و در لایه بعدی برابر با :

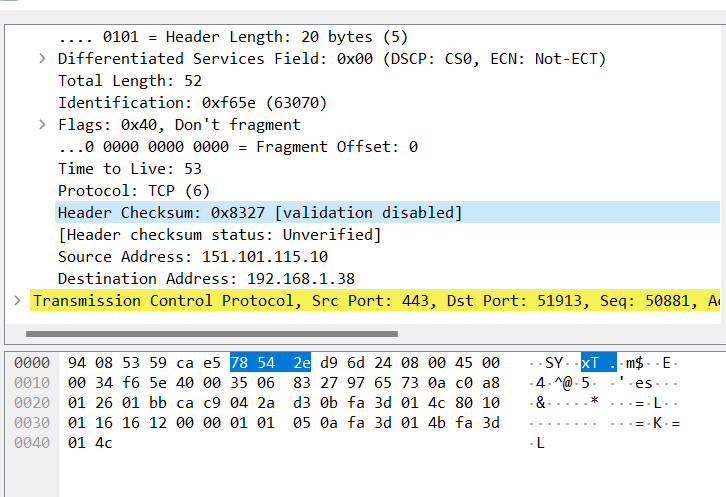
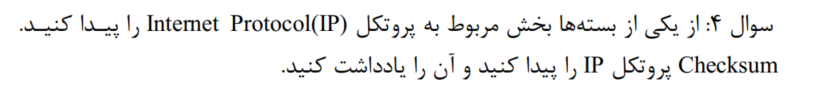


برابر با 20 بایت هدر و 1 بایت داده است.



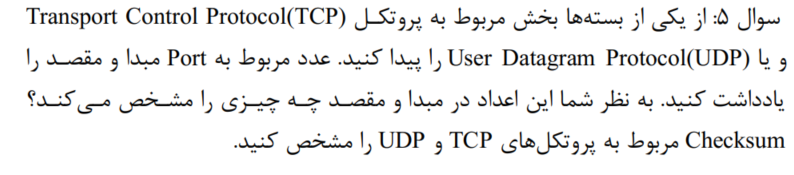
بله بسته با پروتکل ARP :



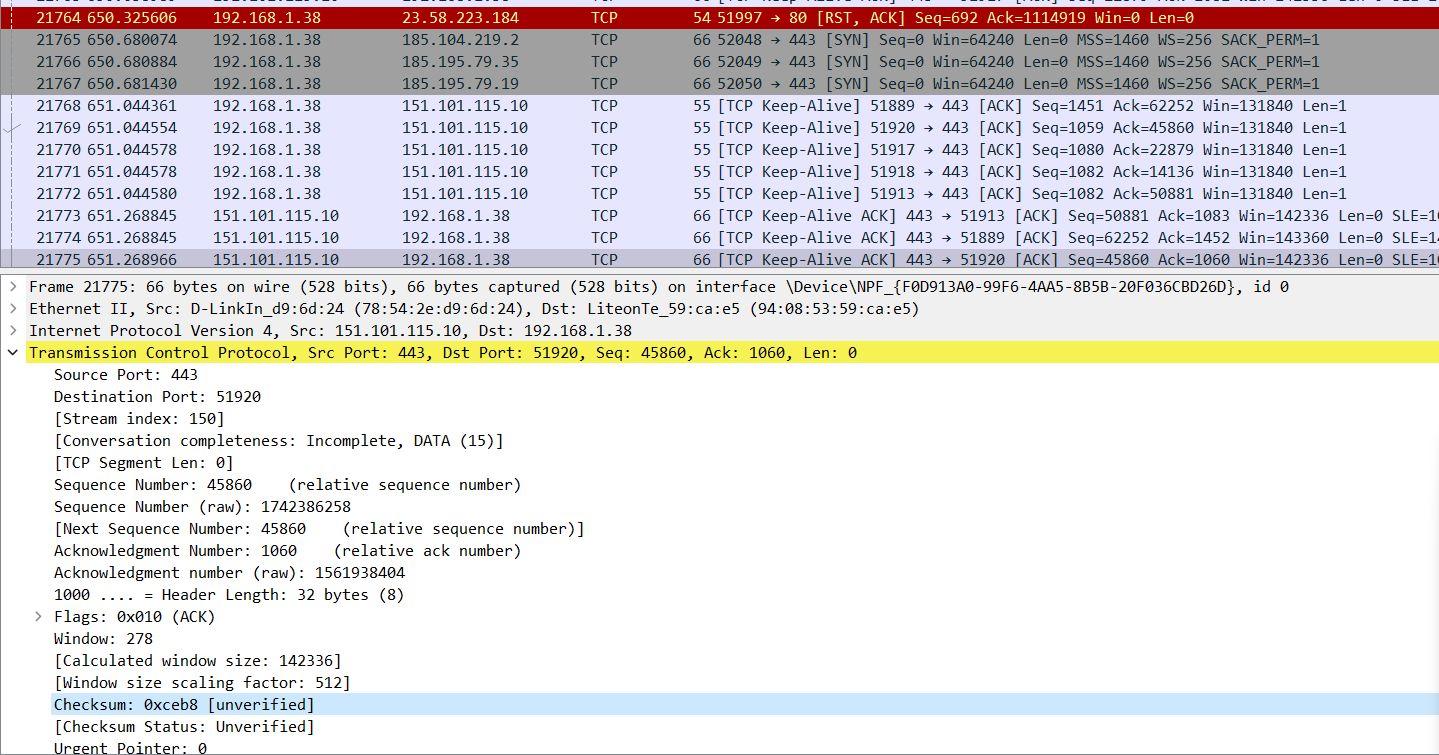




مقدار مورد نظر در تصویر مشخص شده است.



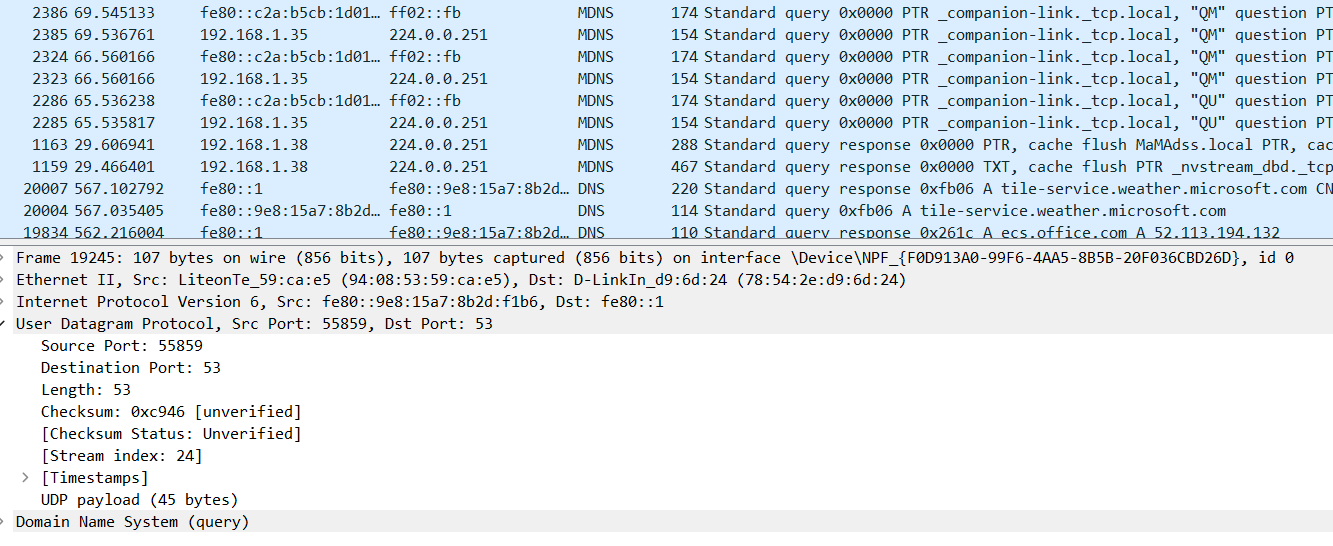
برای پروتکل TCP :





که هر سه در تصویر مشخص اند .

برای UDP :



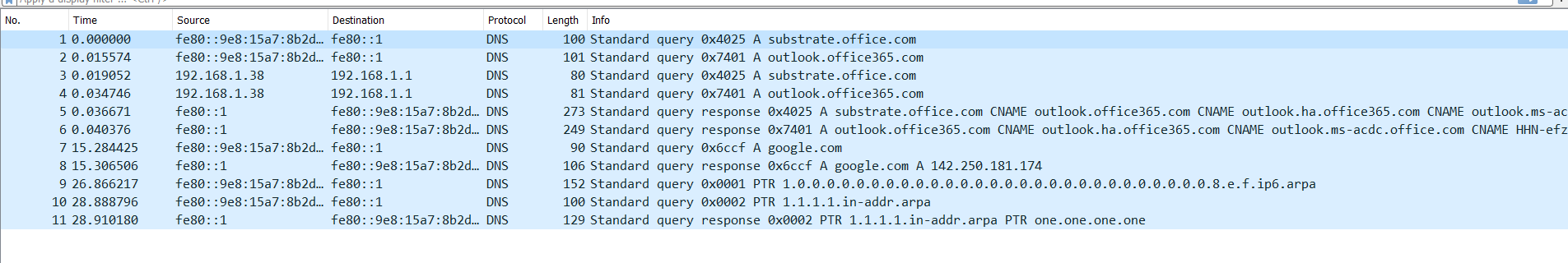


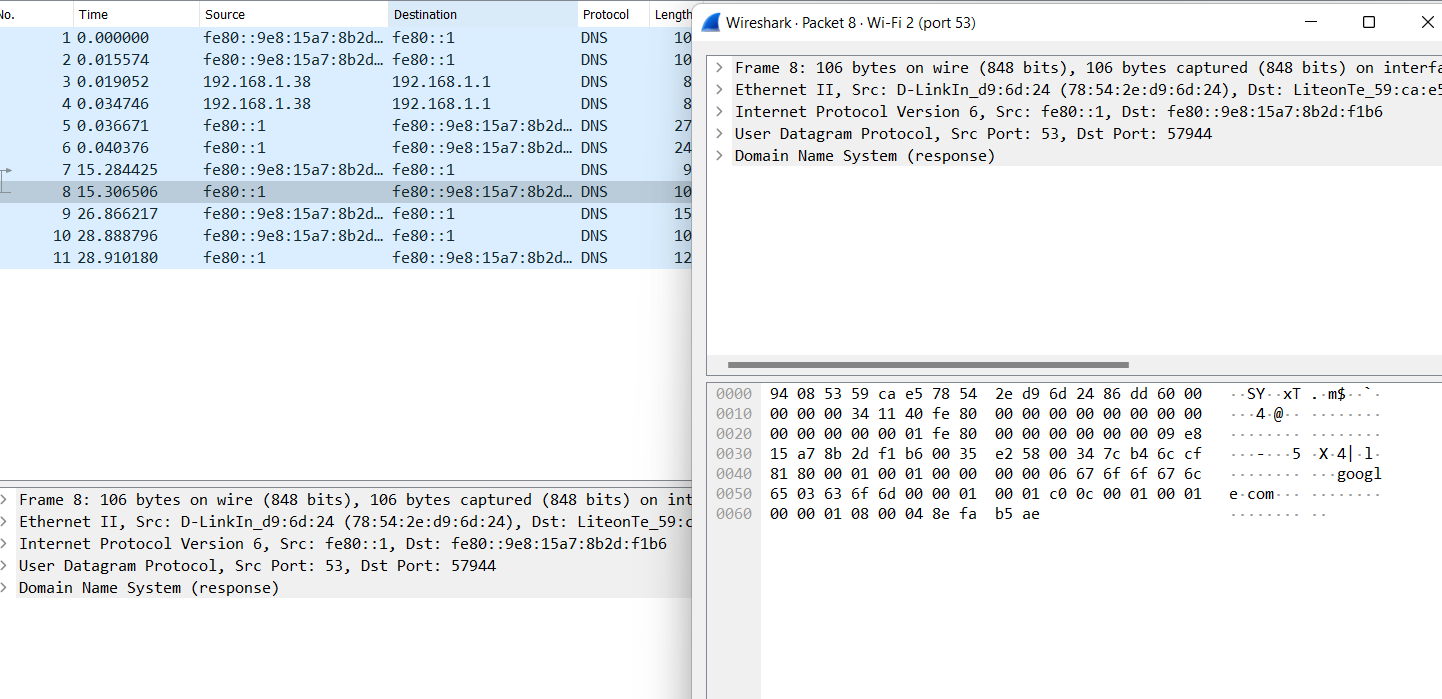
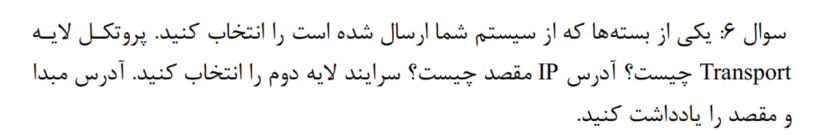
پورت source که همان فرستنده یا مبدا است که در هر دو مقداری رندوم است که اینجا به دلیل اینکه داخلی است و client خود لپتاپ است مقادیری رندوم است . ولی برای مقصد 53 و 443 هستند که پورت های مشخص شده برای ارتباط ها اند.Chekcsum نیز در هر دو تصویر مشخص شده است.

**کار با فیلتر کننده بسته ها:**



پس از انجام مراحل گفته شده به نتیجه زیر میرسیم :





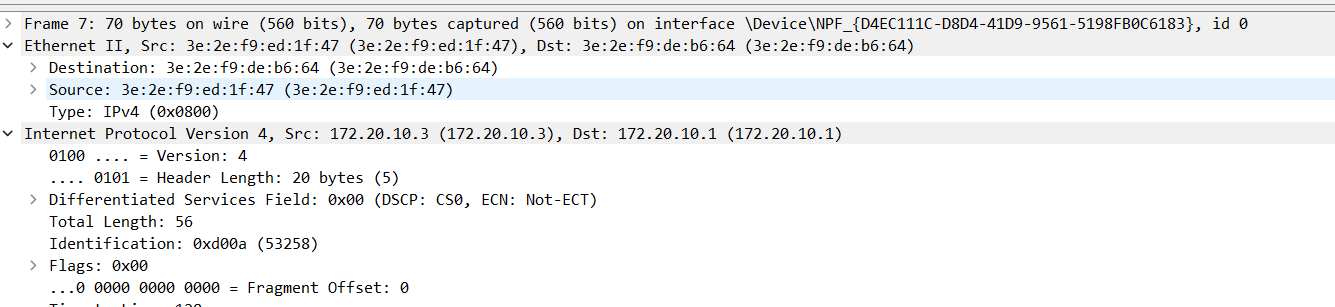
همانطور که مشاهده میکنیم پروتکل لایه transport پروتکل UDP است.

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 :

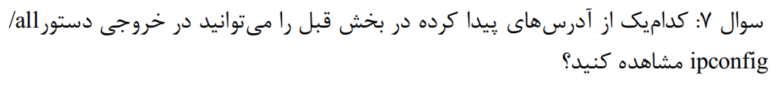






آدرس لایه های مبدا و مقصد که مبدا سیستم ما است در تصویر مشخص است .

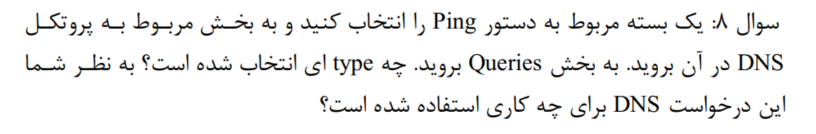
و هم چنان پروتکل ما در لایه transport UDP است.

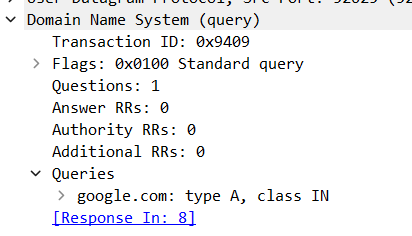






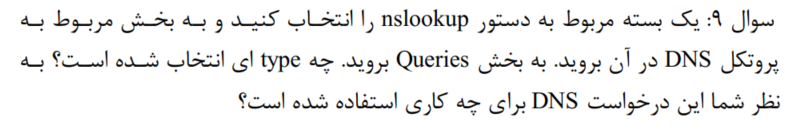
همانطور که میبینم آدرس 172.20.10.3 که آدرس مبدا و آدرس ما است قابل مشاهده است.

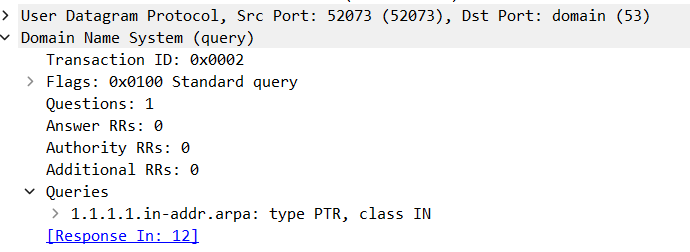






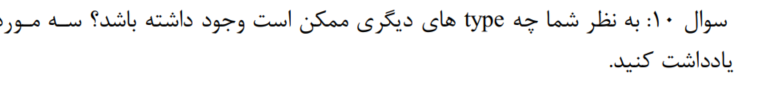
همانطور که میبینم Type A انتخاب شده است. این تایپ برای این است که در اصطلاح DNS را متصل کند یعنی hostname را به آدرس ip مرتبط به آن متصل کند.





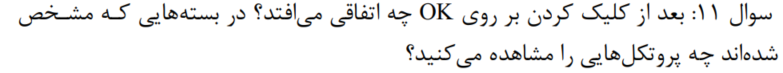


در اینجا Type PTR انتخاب شده است . برای این است که دامنه مربوطه را باز میگردانند یعنی معکوس عملی که در قسمت قبل بوده است. که در بخش مربوطه همان Domain name pointer است.

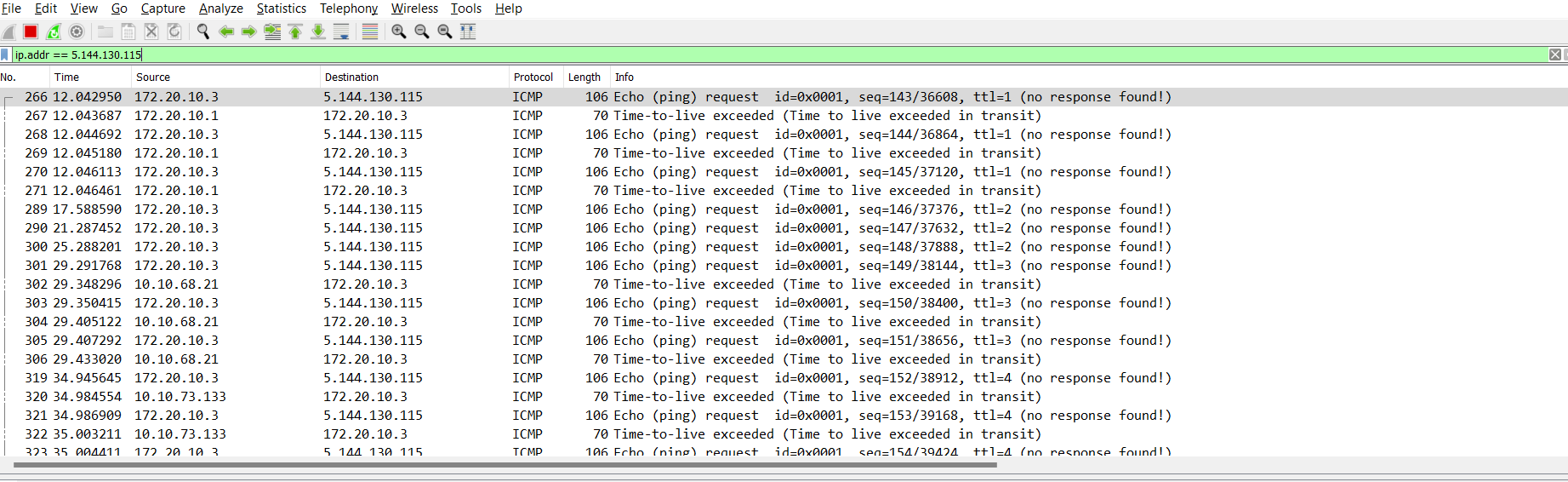


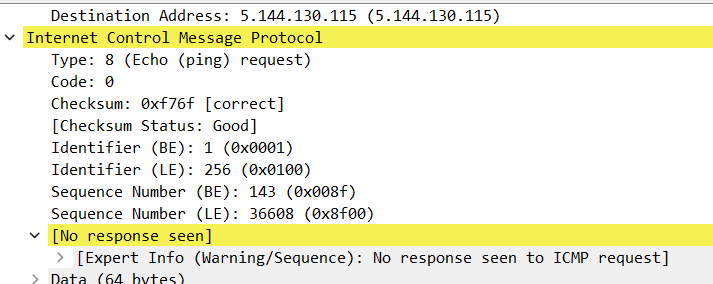
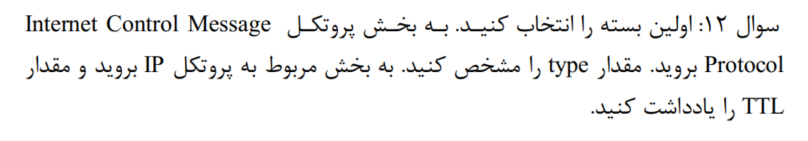
MB & MG & MR & TXT که مربوط به ایمیل ها دامنه جعبه ایمیل ، شماره گروه ایمیل ها و تغییر نام ایمیل است. و آخری هم برای فایل های تکست.





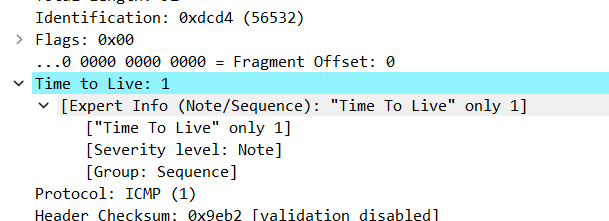
پروتکل تمامی بسته ها به ICMP تغییر می کند و مقصد یا مبدا تمامی بسته ها ip داده شده است.



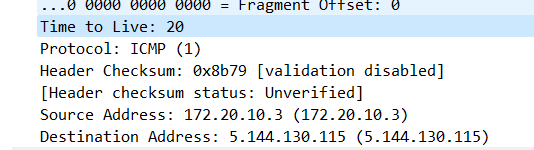




مقدار type برابر با 8 است.







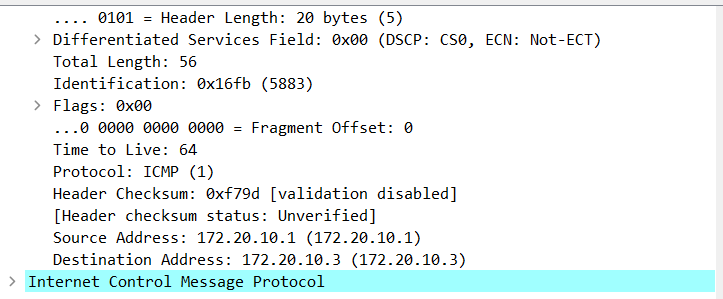


TTL برای بسته که پاسخ ندارد که بسته اول است 1 و برای بسته ای که پاسخ دارد برابر 20 است .

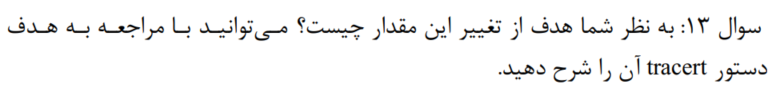


به دلیل اینکه بسته اول پاسخی نداشت بسته دیگری نشان داده شده است.

همان طور که میبینیم برای بسته دیگری نیز 64 است.

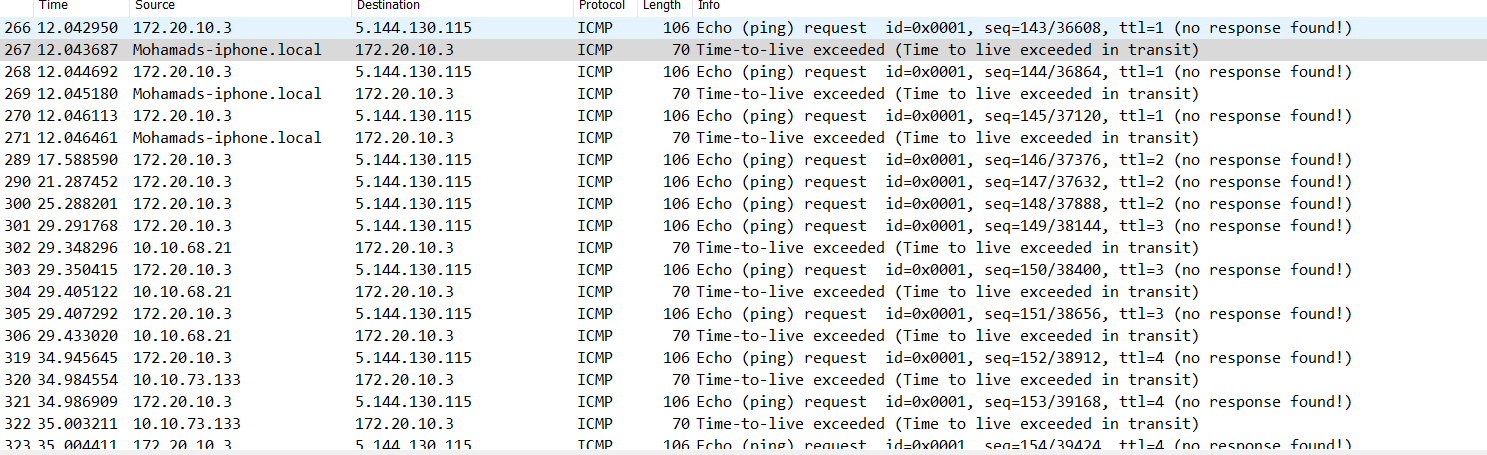






برای بسته هایی که مبدا آن ماشین خودم است این مقدار برابر است با مقادیری مانند 1 تا 10 که به نسبت پایین ترند.

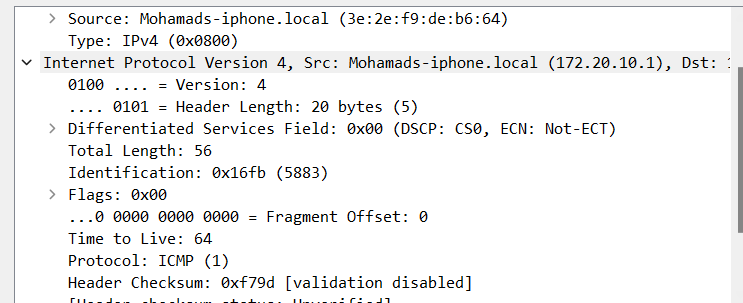
دستور tracert مسیر های رسیدن به یک ip را طی میکند و نشان میدهد. TTL مدت زمانی یا تعداد گام هایی است که یک بسته میتواند باقی بماند با آن ip .حال با طی هر مرحله TTL کاهش می یابد و وقتی که صفر می شود از بین می رود. دلیل اینکه در بسته های موجودی من در ابتدا 1 بوده است و زیاد نبوده احتمالا این است که پاسخی دریافت نکرده و نیازی به بودن بسته نیست .





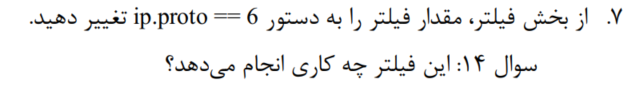
اما همانطور که میبینیم در بسته دوم هم در اطلاعات آن نوشته TTL افزایش یافته است .

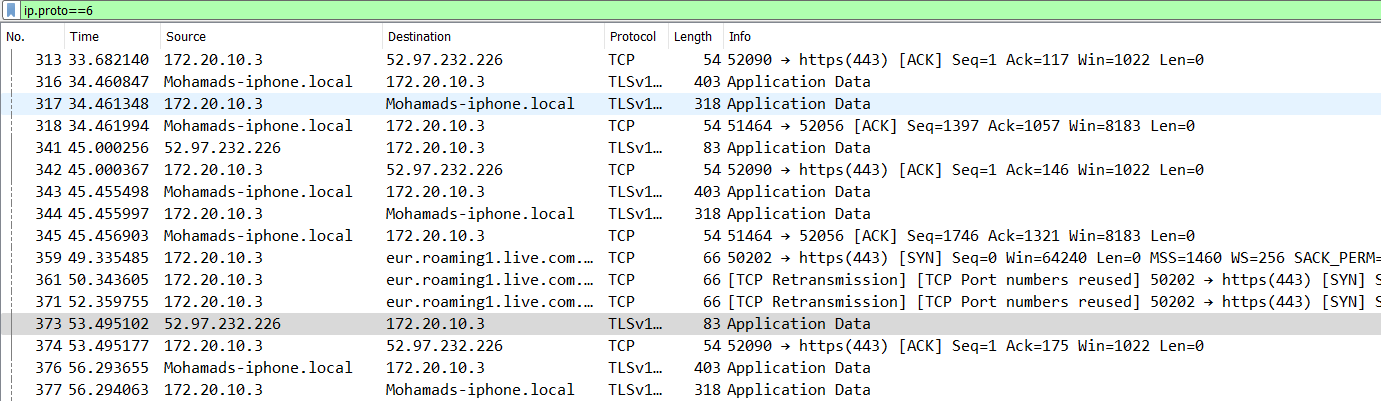
و اگر در بسته نگاه کنیم 64 شده است.





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







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.