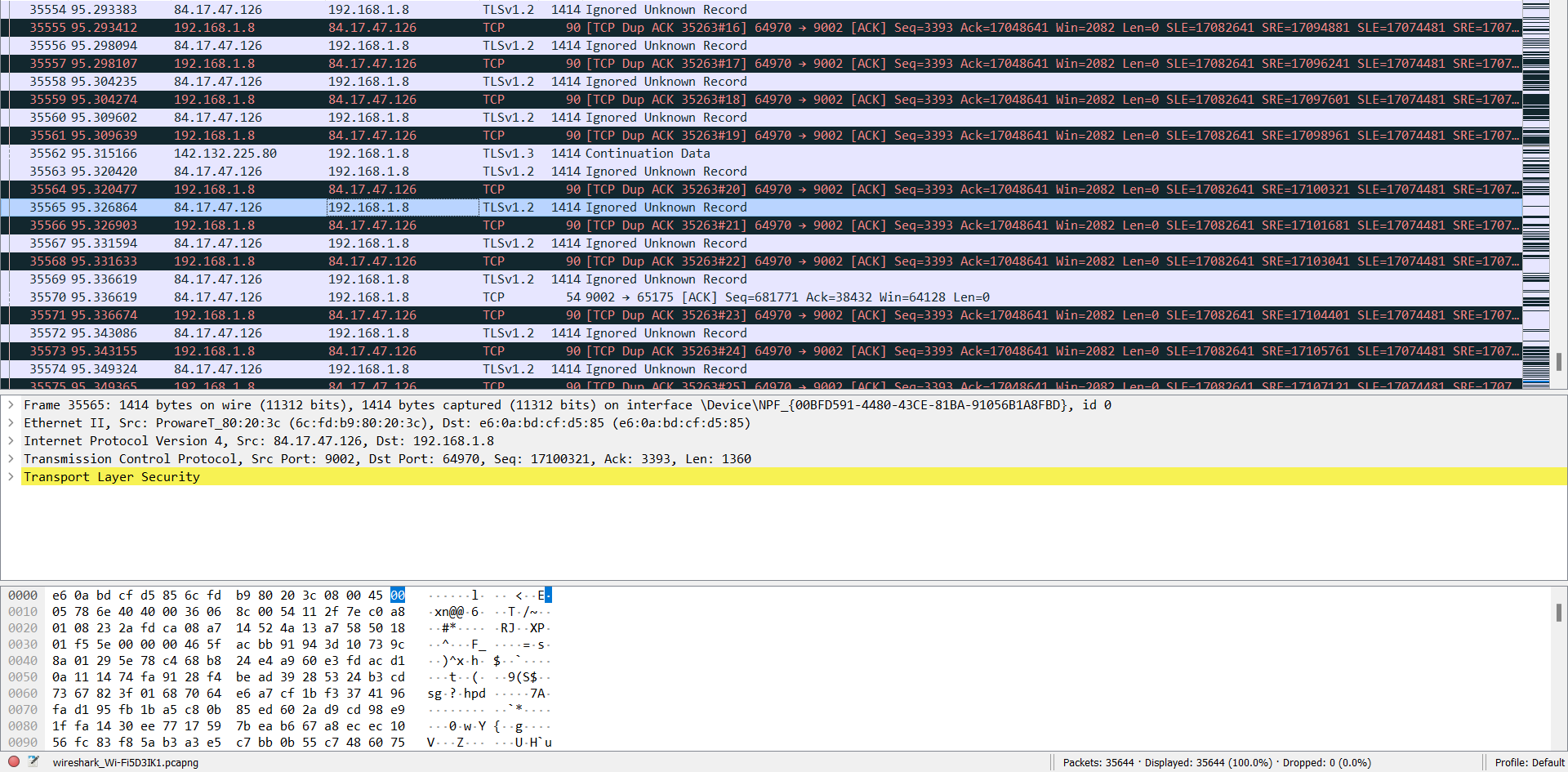
## سوال اول)

سایت های جست و جو شده: YouTube، Reddit، Twitter، GitHub، Gmail

لیست پروتکل های مشاهده شده:

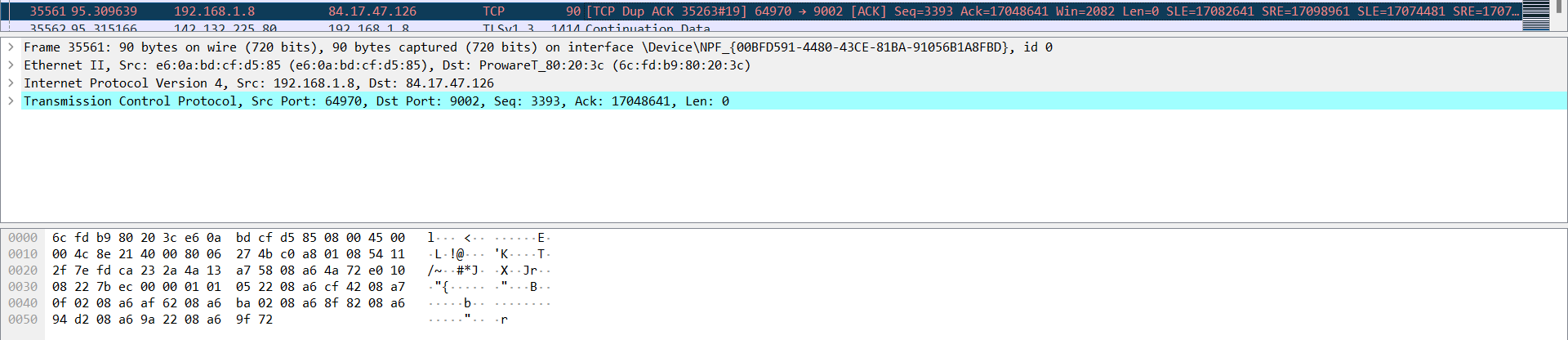
TCP, TLSv1.2, TLSv1.3, HTTP, TLS, HTTPS, DNS



## سوال دوم)

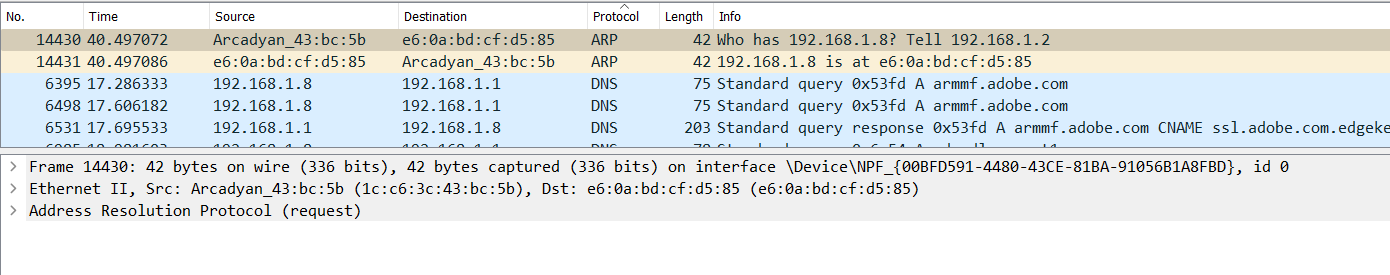
در package انتخابی، دو پروتکل استفاده شده: Internet Protocol Version 4 و Transmission Control Protocol. لایه Transmission Control Protocol بعد از Internet Protocol Version 4 و آن هم بعد از Ethernet II و آن هم بعد از Frame آمده است. به عبارتی ترتیب قرارگیری به خارجی ترین است.

اندازه Frame لایه دو این بسته برابر 90 بایت است. جزئیات این package را مشاهده میکنید:



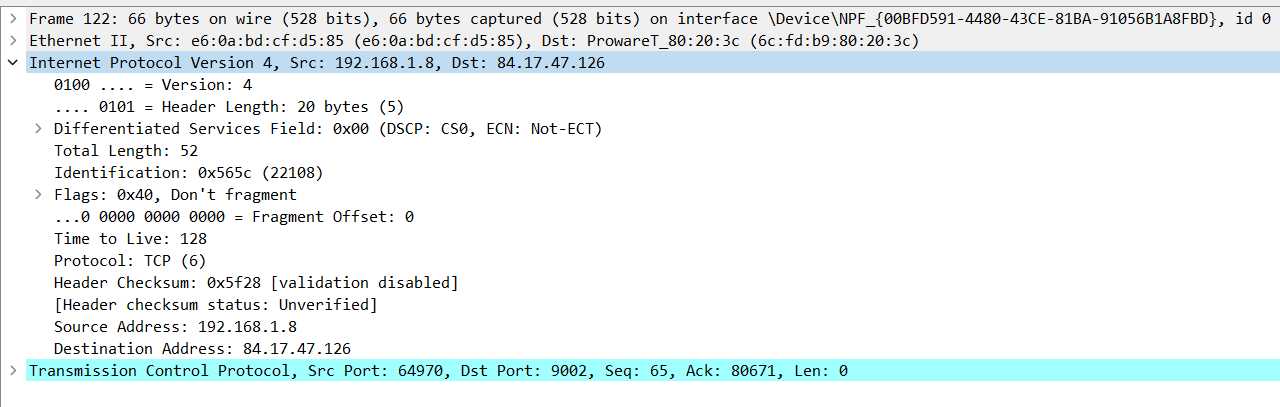
## سوال سوم)

بله. همانطور که در عکس پایین مشاهده میشود Package های ARP دارای لایه های Network، Application و Transport نیستند. پروتکل استفاده شده در این package ها برای Data Link هستند:



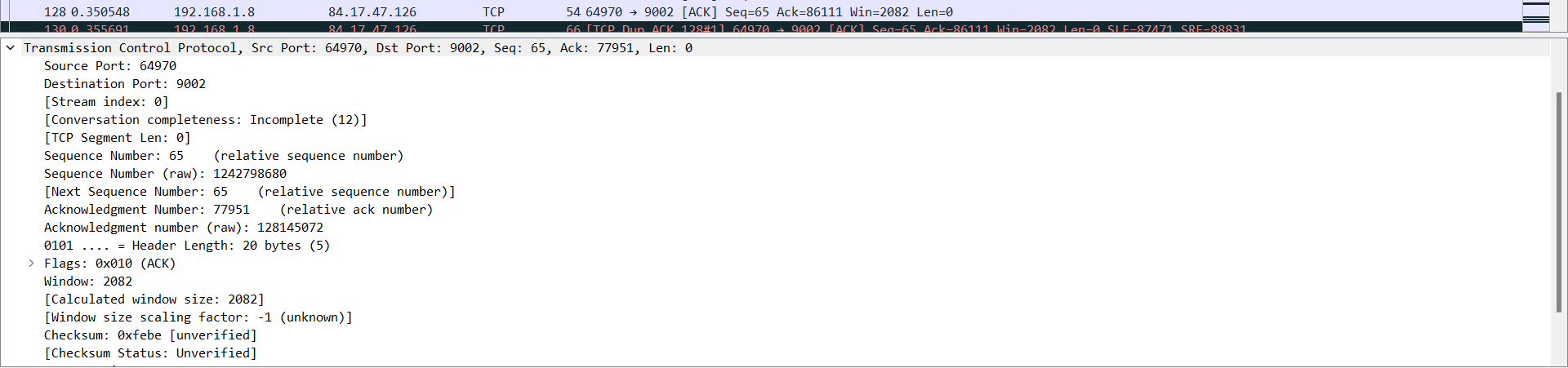
## سوال چهارم)

در برنامه Wireshark یک package انتخاب شده و سپس مشخصات لایه Internet Protocol Version 4 باز شد. همانطور که مشاهده میشود Header Checksum برابر 0x5f28 است. در شکل زیر درستی این حرف اثبات میشود:

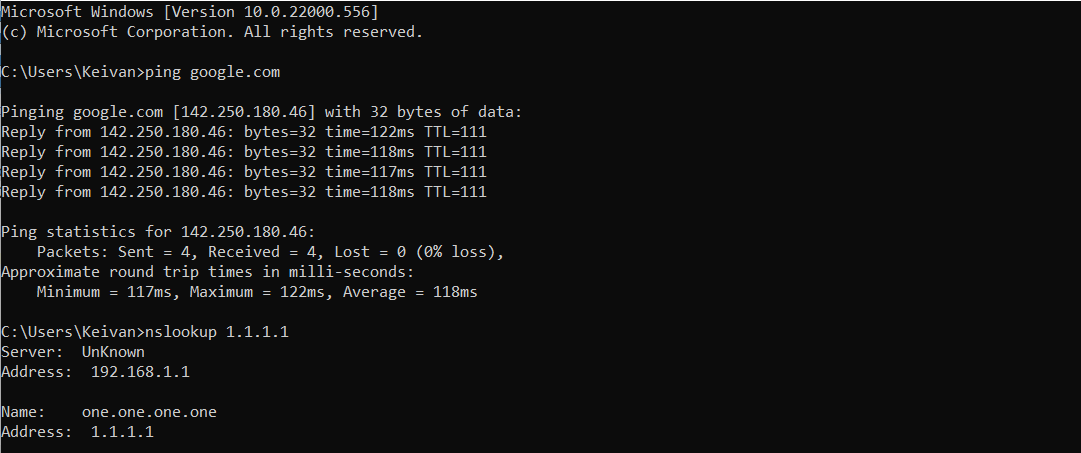
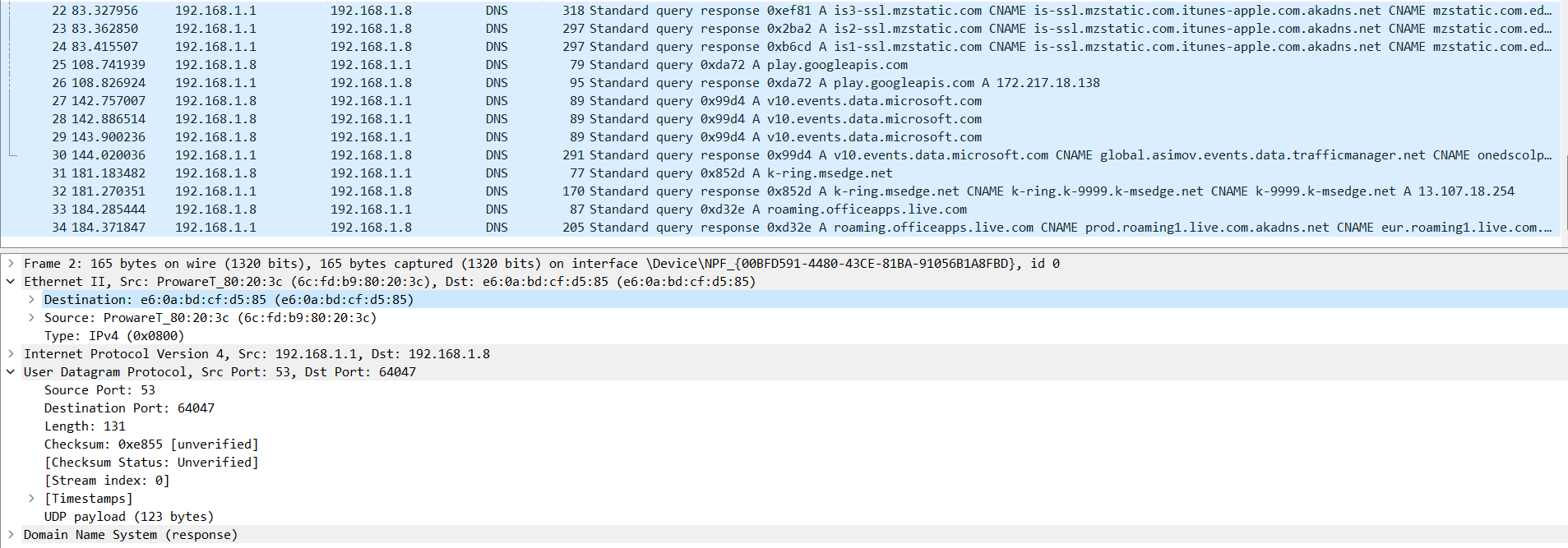


## سوال پنجم)

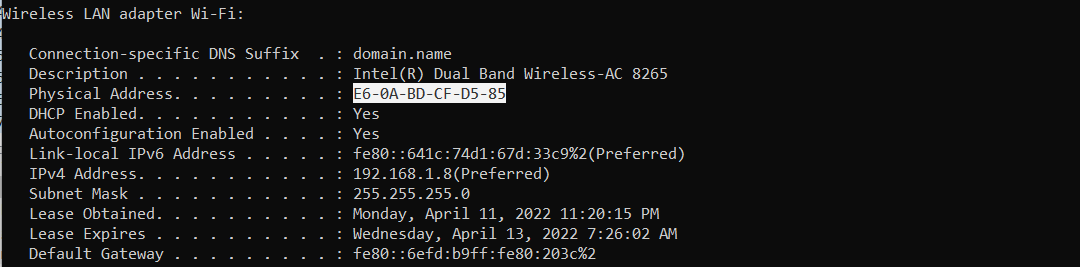
پورت ها برای انتقال دیتا حیاتی هستند. دو پورت Source برابر 64970 و Destination برابر 9002 است. بین این پورت ها میتوان دیتا فرستاد یا دریافت کرد. Checksum پروتکل TCP برابر 0xfebeو پروتکل UDP برابر 0x35c5 است.



## سوال ششم)

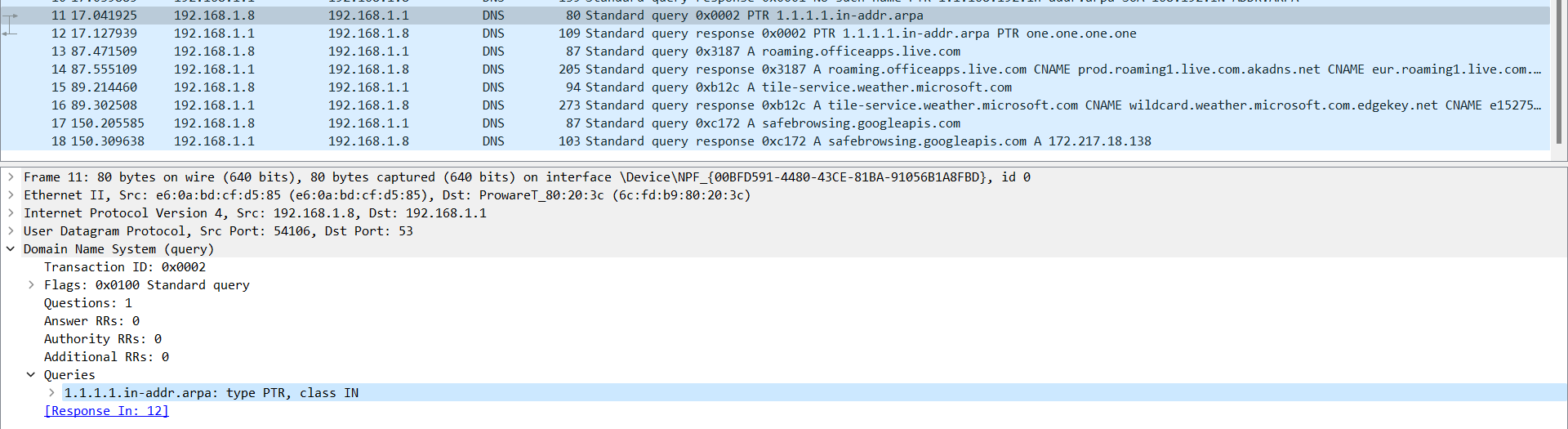
پروتکل لایه Transport برابر UDP بوده و پورت مقصد برابر 192.168.1.8 است. لایه دوم Ethernet II است که آدرس مبدا 6c:fd:b9:80:20:3c و آدرس مقصد e6:0a:bd:cf:d5:85 است. 

## سوال هفتم)

از آن جایی که interface انتخابی WIFI بوده، آدرس آن را در ipconfig/all مشاهده میکنیم.

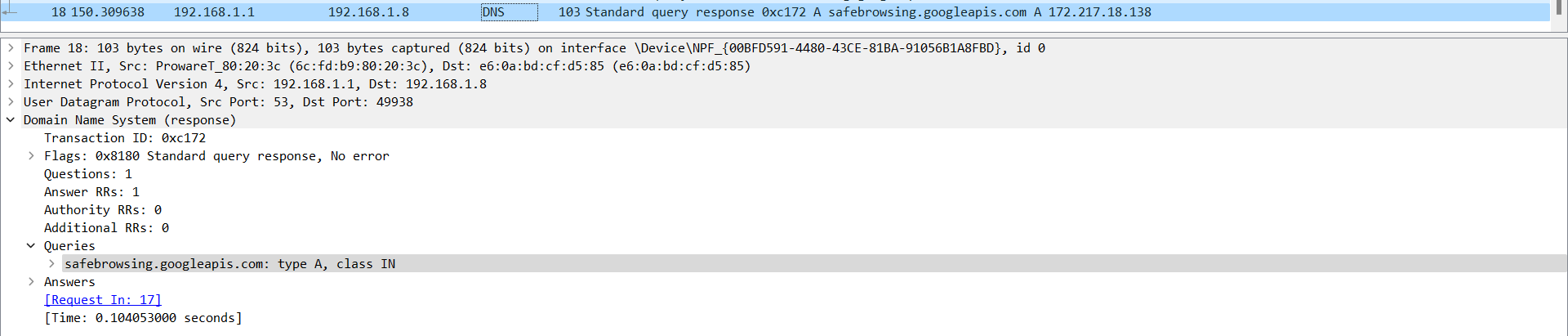
همانطور که مشاهده میشود Physical Address چاپ شده با سوال ششم همخوانی دارد.

## سوال هشتم)

در لایه Query و بخش Query تایپ PTR انتخاب شده. این تایپ برای تبدیل یک IP Address به Host Name استفاده میشود. (برعکس این تایپ یعنی تایپ A، عکس این عملیات را انجام میدهد.)

در عکس، سطر تایپ انتخاب شده.

## سوال نهم)

برای دستور nslookup تایپ A استفاده شده است. این تایپ برای تبدیل یک Host Name به IP Address استفاده میشود. (برعکس لایه سوال قبل، (PTR

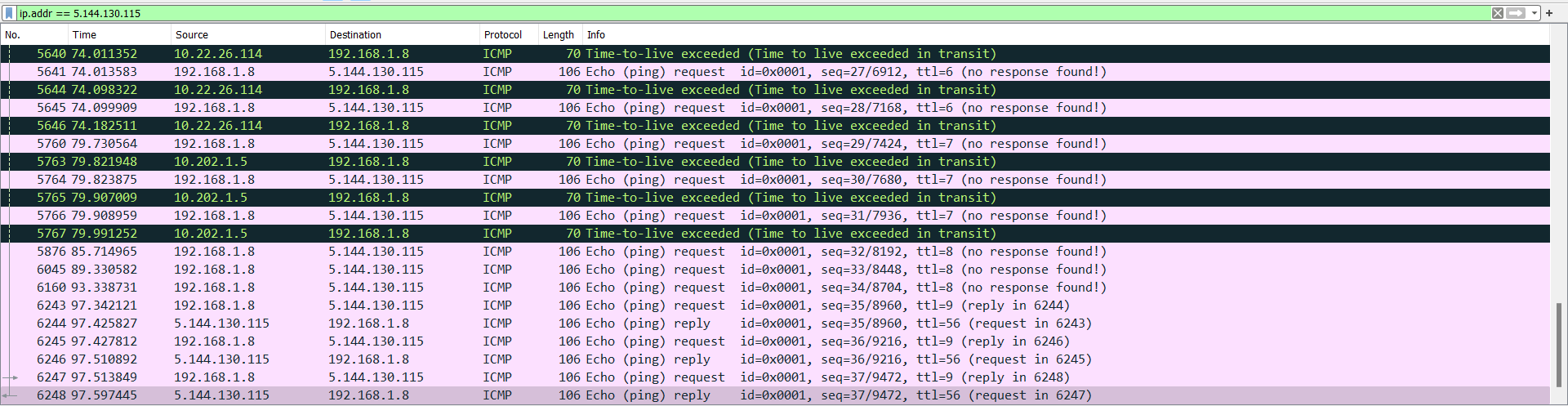
## سوال دهم)

سه نوع کوئری دیگر:

* کوئری تایپ MD مربوط به Mail Destination
* کوئری تایپ TXT مربوط به Text Strings
* کوئری تایپ HINF0 مربوط به Host Information

## سوال یازدهم)

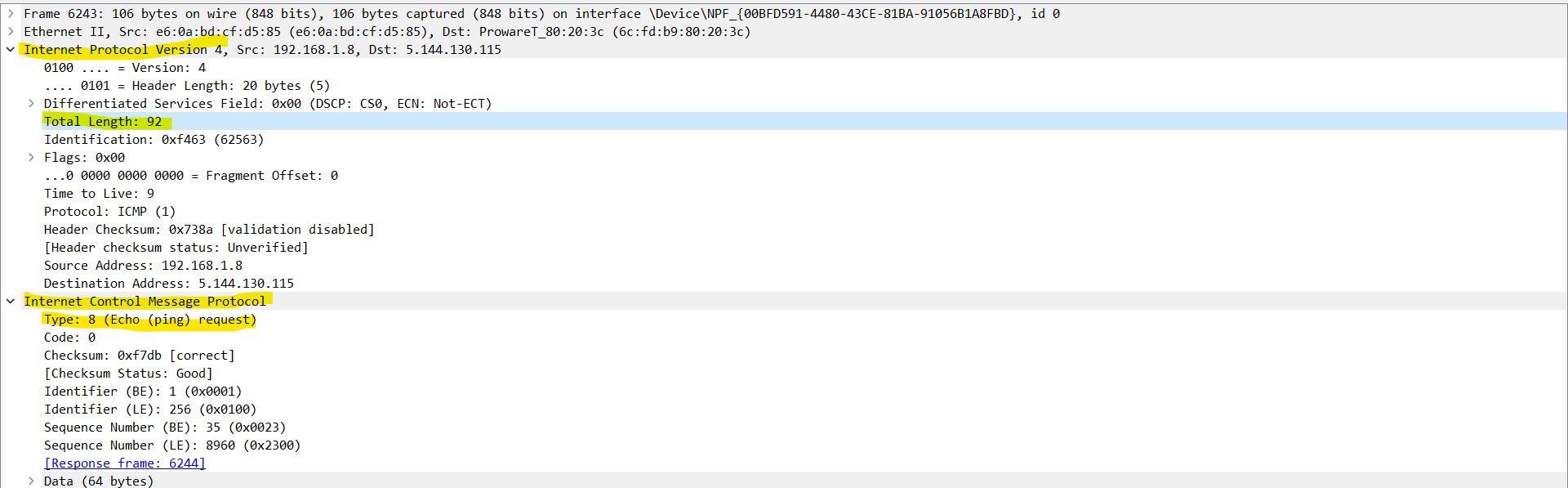
درصورت انتخاب این فیلتر فقط package هایی که IP مقصد یا مبدا آنها برابر IP که دادیم بود نمایش داده میشوند. از طرفی تمام پروتکل های مشاهده شده برابر ICMP میشود. همانطور که در شکل مشاهده میشود فیلتر اعمال شده:



از آنجایی که IP Address سایت p30download.com برابر 5.144.130.115 است، فیلتر اعمال شده:

ip.addr == 5.144.130.115

## سوال دوازدهم)

در قسمت Internet Control Message Protocol، تایپ برابر Echo (ping) Request است. از طرفی TTL یا Time To Live برابر 9 بوده است. در شکل مشاهده میشود:

## سوال سیزدهم)

بله، مقادیر در حال تغییر هستند زیرا در صورت بروز هر خطایی در دریافت/ارسال بسته ها TTLیا Time To Live از گیر کردن در حلقه بینهایت جلوگیری میکند.

## سوال چهاردهم)

این فیلتر برا نمایش پروتکل های TCP است. سایت [Wikipedia](https://en.wikipedia.org/wiki/List_of_IP_protocol_numbers) این مشاهده را تایید میکند.