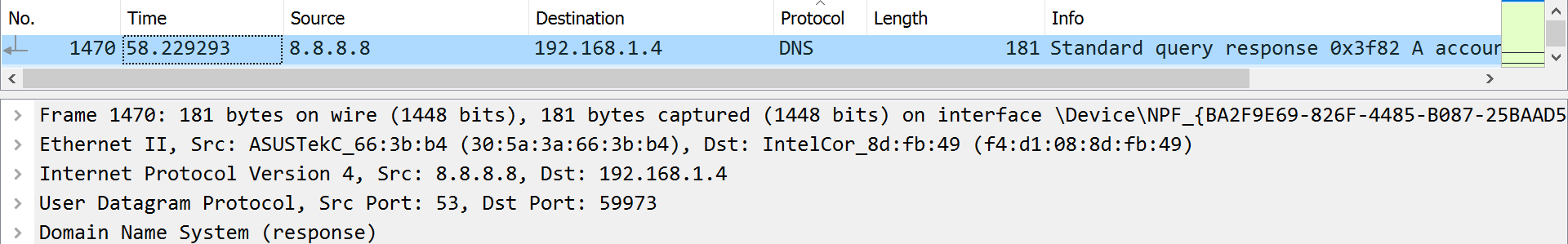
# سوال۱

پروتکل هایی که مشاهده شدند:

TCP – TLSv1.2 – UDP – DNS – NBNS

# سوال۲

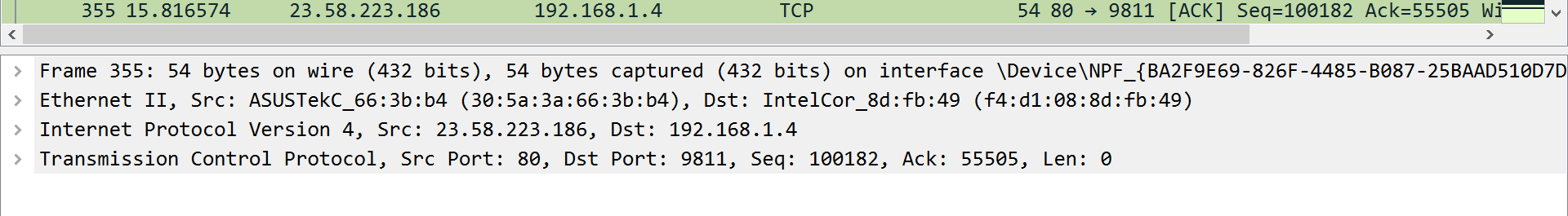
بسته ای که انتخاب کردیم:



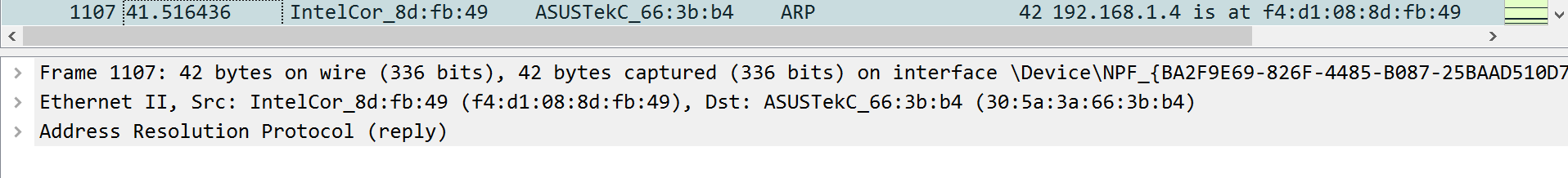
|  |  |
| --- | --- |
| **پروتکل لایه ها:** | Application: **DNS**  Transport: **UDP**  Network: **IPv4**  Data Link: **Ethernet II** |
| **ترتیب بیت ها:** | ترتیب قرار گیری بیت ها به ترتیب لایه ها میباشد . یعنی بیت های اول مربوط به لایه ی اول، دسته بیت های دوم مربوط به لایه ی دوم و به همین ترتیب برای سایر لایه ها میباشد. در واقع در هر لایه، headerآن لایه به payloadقبلی ها اضافه میشود . |
| **اندازه فریم:** | Frame Length: 181 bytes (1448 bits) |
| **اندازه لایه سوم:** | Total Length: 167 |

# سوال۳

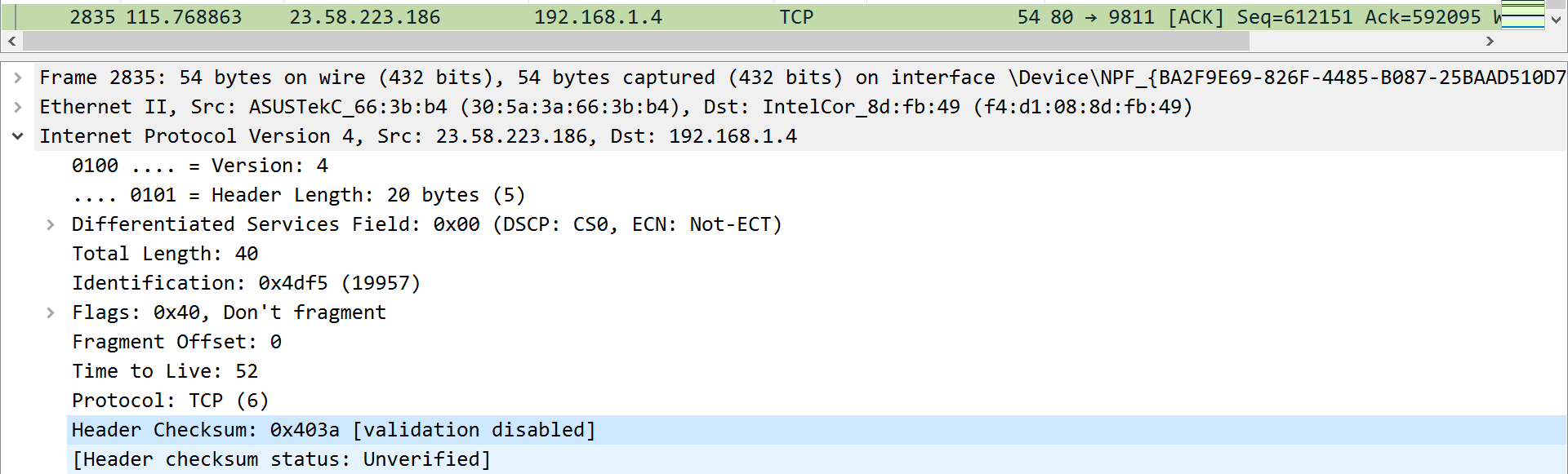
این بسته به عنوان مثال لایه application ندارد.



یا این بسته APR لایه transport ندارد.

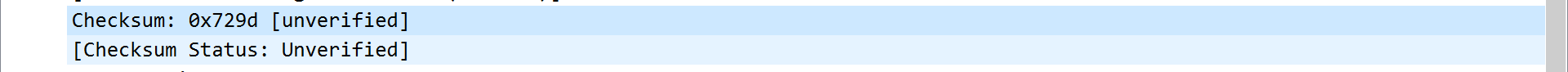
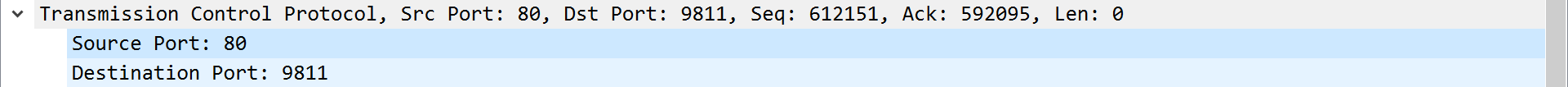


# سوال۴



# سوال۵

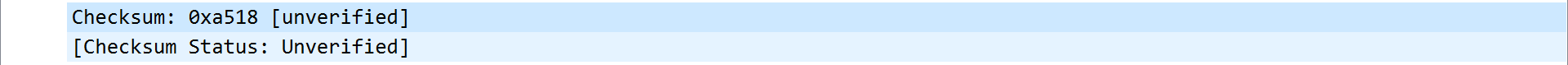
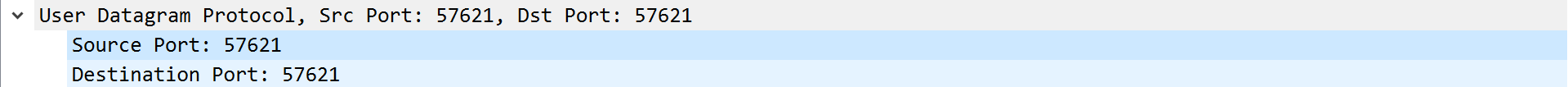
## برای TCP



پورت مبدا 80 و پورت مقصد 9811 میباشد.

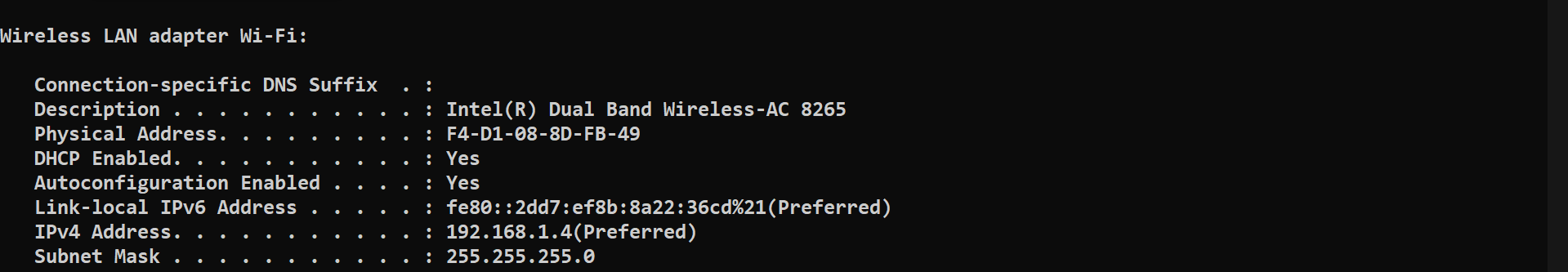
پورت 80 مربوط به HTTP است.

## برای UDP

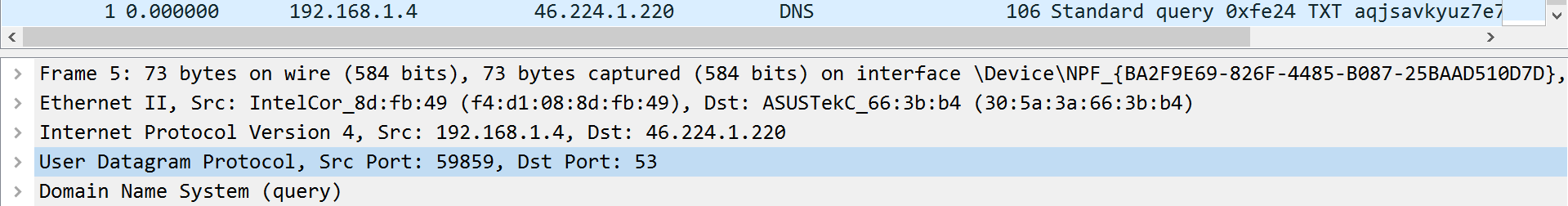


پورت مبدا ۵۷۶۲۱ و پورت مقصد ۵۷۶۲۱ میباشد.

# سوال۶

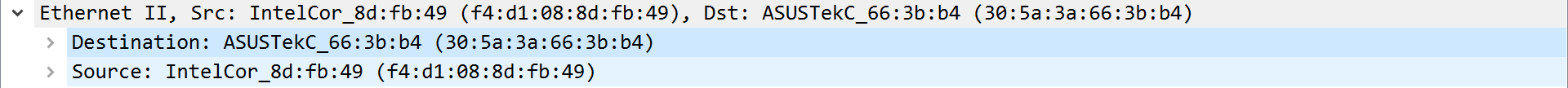


از آنجا که IP سیستم ما برابر است با 192.168.1.4 ، بسته ای که انتخاب میکنیم باید از سمت این IP فرستاده شده باشد.



پروتکل لایه transport پروتکل UDP است. همچنین IP مقصد برابر است با 46.224.1.220

آدرس مبدا و مقصد در سرآیند لایه دوم به صورت زیر میباشد:

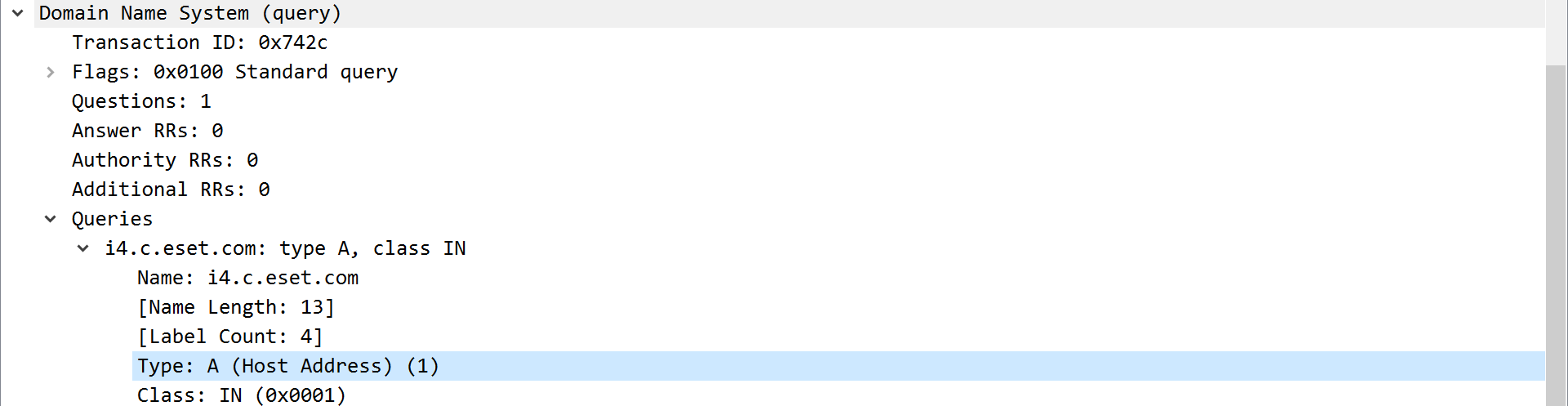


# سوال۷

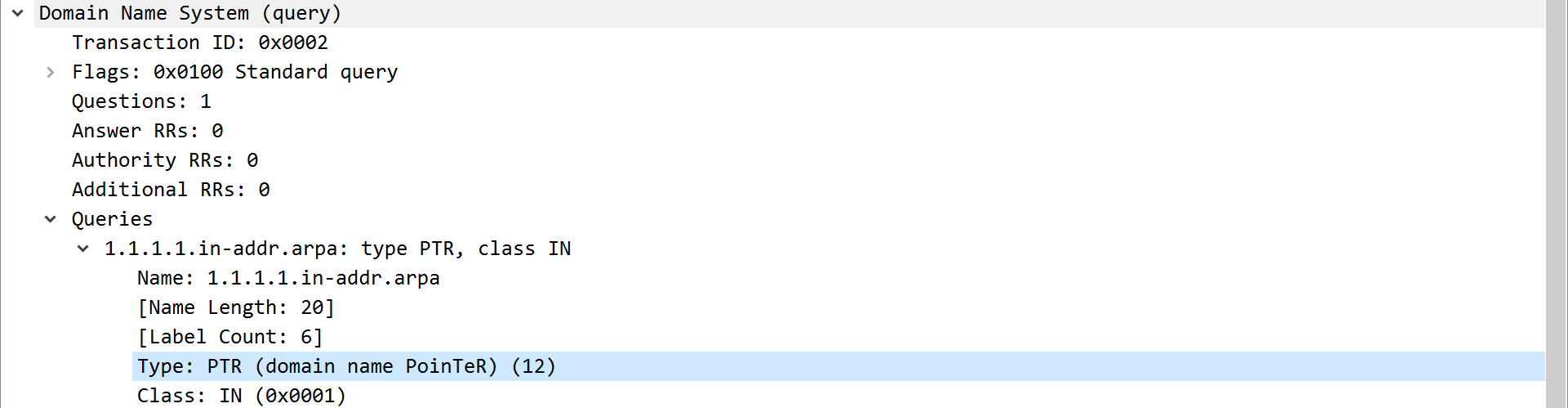
آدرس 192.168.1.4 آدرس سیستم ما بود که در عکس بالای همین صفحه قابل در بخش IPv4 Address مشاهده است.

# سوال۸

از همان بسته قسمت قبل استفاده میکنیم:

تایپ این Query ، Aاست که به آن Address mapping record(همچنین DNS host record )گفته میشود که از آن برای گرفتن آدرس IPV4مقصد که 32 بیتی است استفاده میشود .(برایmap کردن hostname ها به IP آن ها کاربرد دارد ) . همچنین از آن در DNSBLsو ذخیره سازی subnet maskها در RFC 1101 استفاده میشود .

# سوال۹



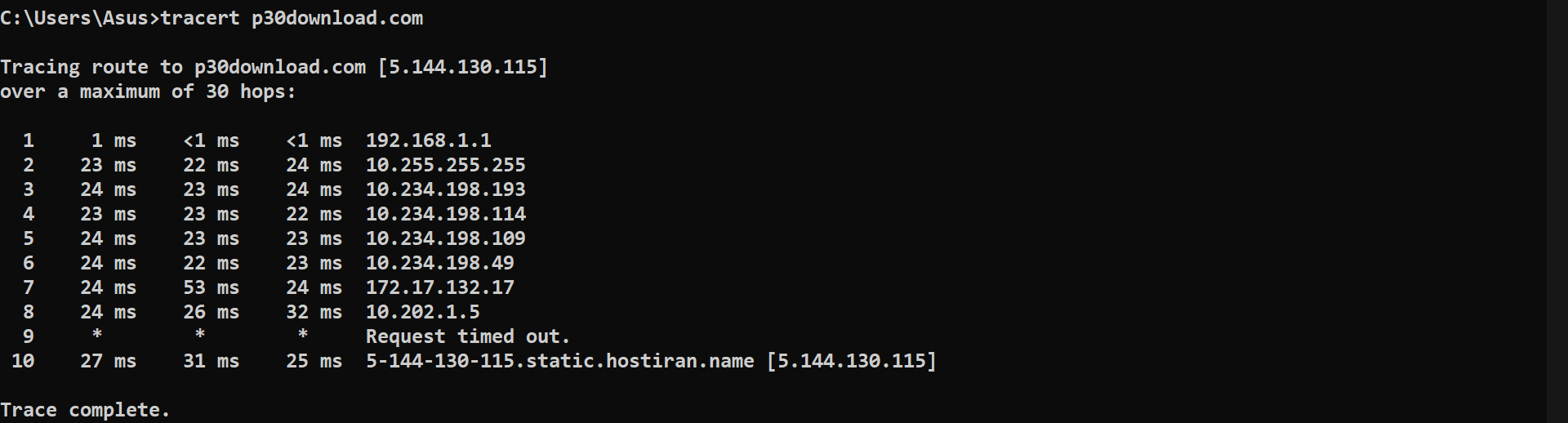
تایپ این Query ، PTR است . این تایپ پوینتری به canonical name میباشد .

# سوال۱۰

تایپ های زیادی وجود دارند که تعدادی از آن ها به شرح زیر است :

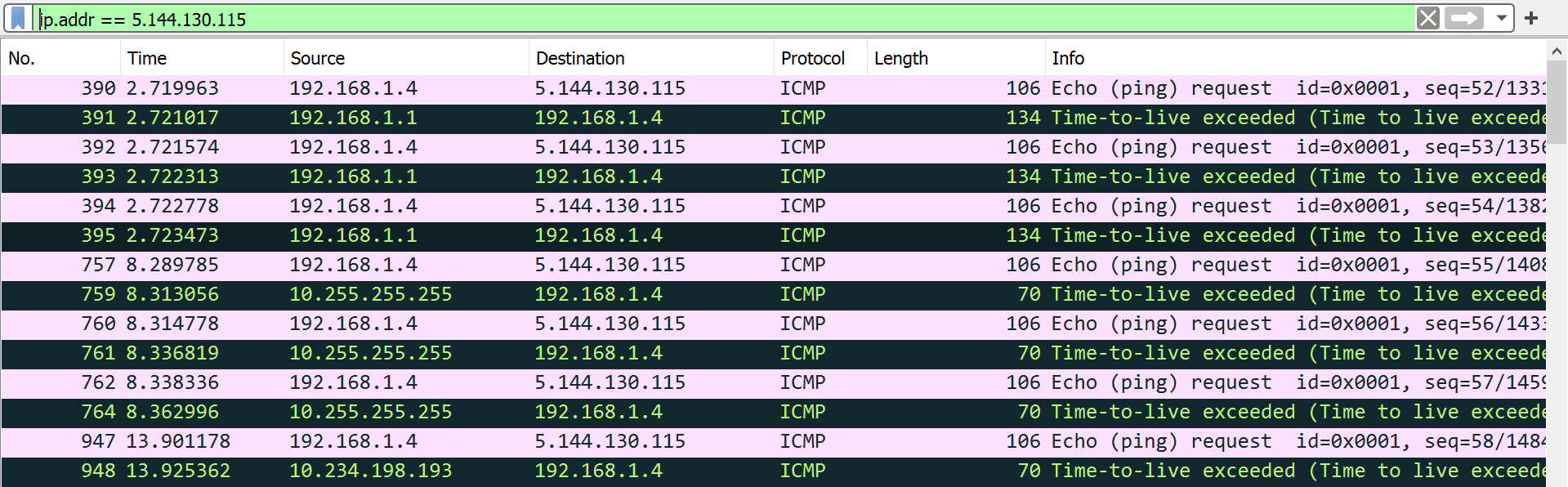
|  |  |
| --- | --- |
| **LOC** | منطقه ی جغرافیایی مرتبط با یک domain name را مشخص میکند . |
| **RP** | اطلاعاتی درباره ی شخص یا اشخاصی که مسئولیت domainرا دارند است که معمولا آن اطلاعات شامل ادرس ایمیلی که @ آن با a جایگزین شده است میباشد . |
| **HINFO** | پاسخ هایی با سایز مینیمال برای dns query هایی با تایپ QTYPE=ANY تامین میکند. |

# سوال۱۱



بعد از زدن okبسته ها با فیلتری که در filterمشخص کردیم نمایش داده میشوند . برای مثال بنا به دستور کار ما بسته هایی را انتخاب کردیم که IP مبدا یا مقصد آن ها ، 5.144.130.115 که IPمربوط به سایت مورد نظر است نمایش داده میشوند .پس از طی کردن گام های دستور کار ، فیلتر بدین صورت میباشد :

ip.addr == 5.144.130.115

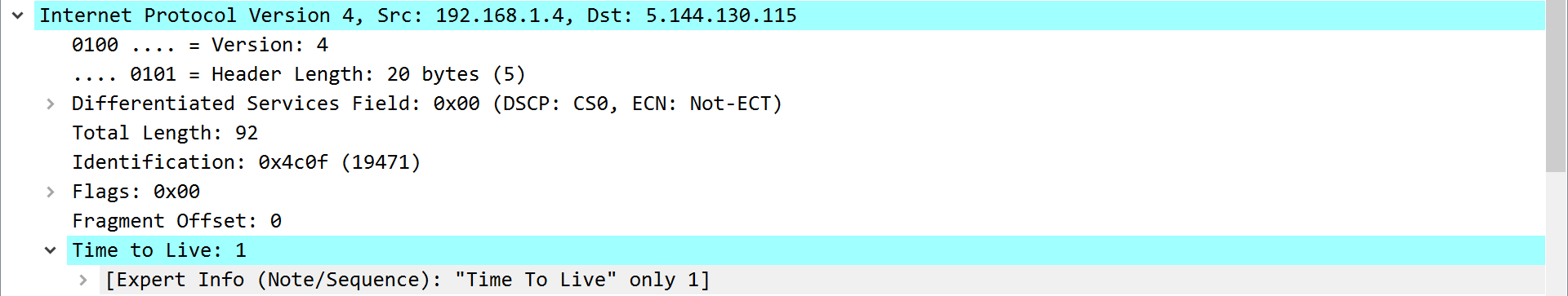


تمام پروتکل ها ICMP میباشد.

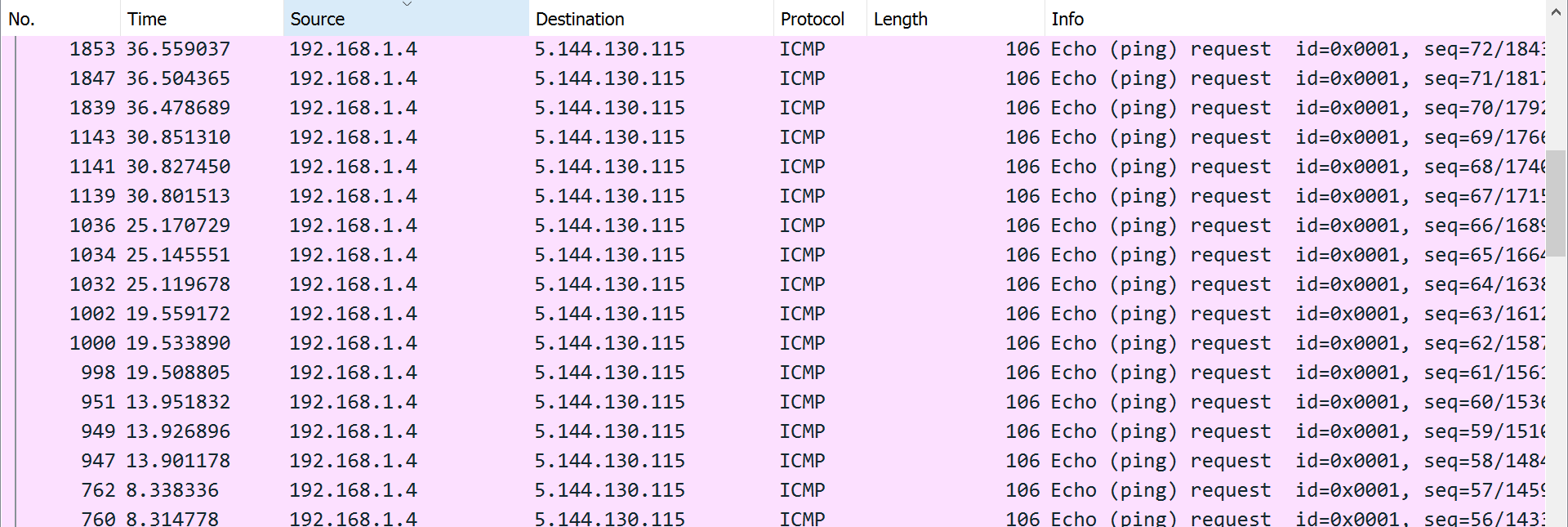
# سوال۱۲



حال به بخش IP میرویم:



روی قسمت مبدا کلیک میکنیم که بسته ها بر اساس آنها مرتب شوند و سپش به سراغ IP سیستم خودمان میرویم:



# سوال۱۳

در این بسته ها TTL از مقدار ۱۰ تا ۱ میباشد زیرا همانگونه که در بخش tracert مشاهده کردیم این عمل در ۱۰ گام انجام شد. در هر گام ۳ بسته وجود دارد، یعنی در کل ۳۰ بسته وجود داشت که هر ۳ تای آنها TTL یکی از اعداد ۱ تا ۱۰ را به طور مشابه دارند.

در هر گامی که یک بسته طی میکند، یک واحد از TTL آن کاسته میشود و در صورت صفر شدن آن، بسته از بستر شبکه drop شده و باید مجددا آن را ارسال کنیم.

# سوال ۱۴

بسته ها را بر اساس پروتکل انتخاب میکنیم. که 6 بیانگر IPv6 میباشد. قسمت مشترک تمامی نتایج این فیلترینگ قسمت زیر میباشد:

