دانشگاه صنعتی شریف

دانشکده مهندسی کامپیوتر

آزمایشگاه شبکه‌های کامپیوتری

**آشنایی با نرم‌افزار Wireshark**

گردآورندگان:

# امیرحسن فتحی

مصطفی قدیمی

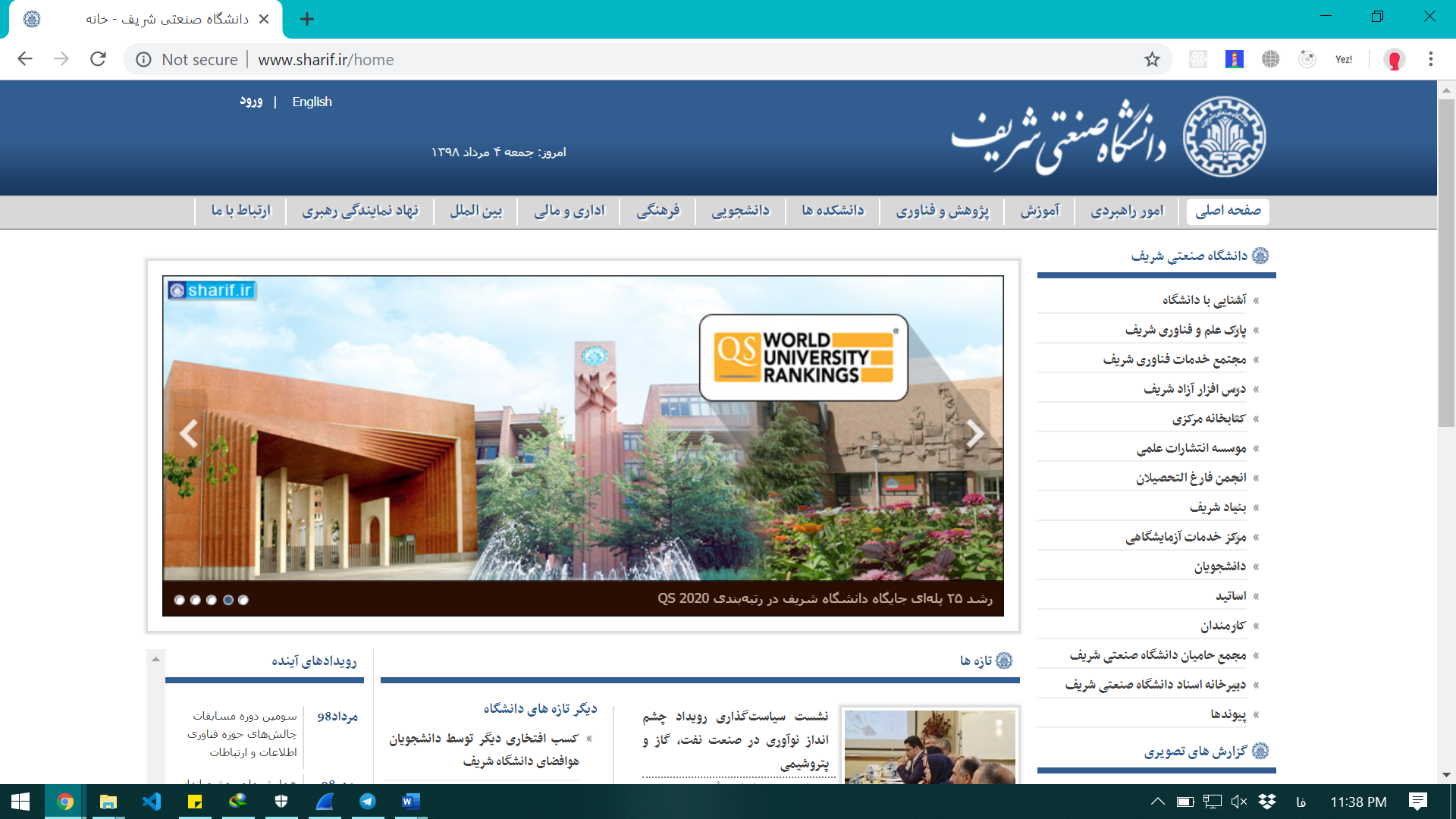
استاد:

مهدی جعفری سیاوشانی

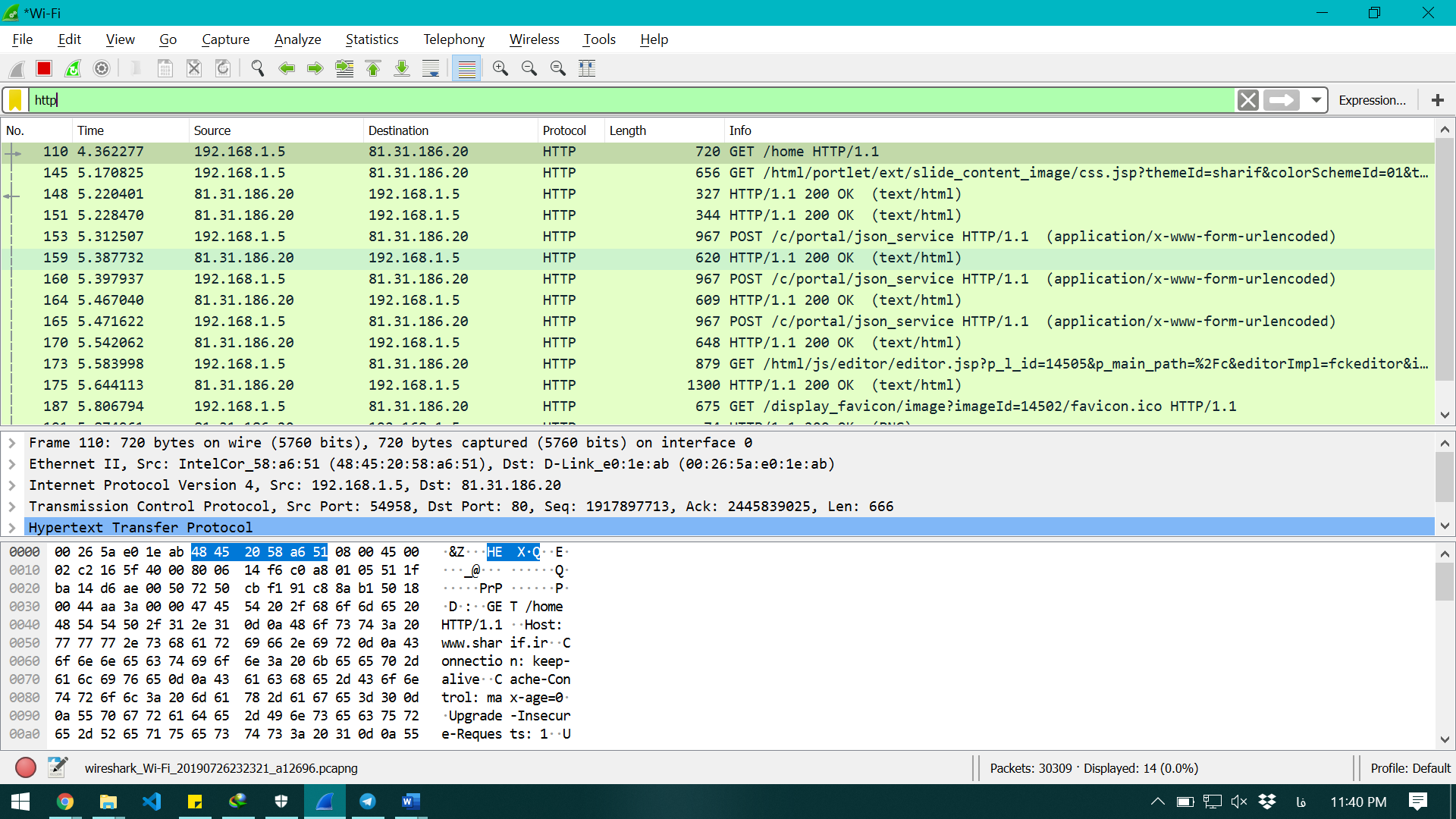
تابستان 98

**بخش اول (فهم اولیه از HTTP):**

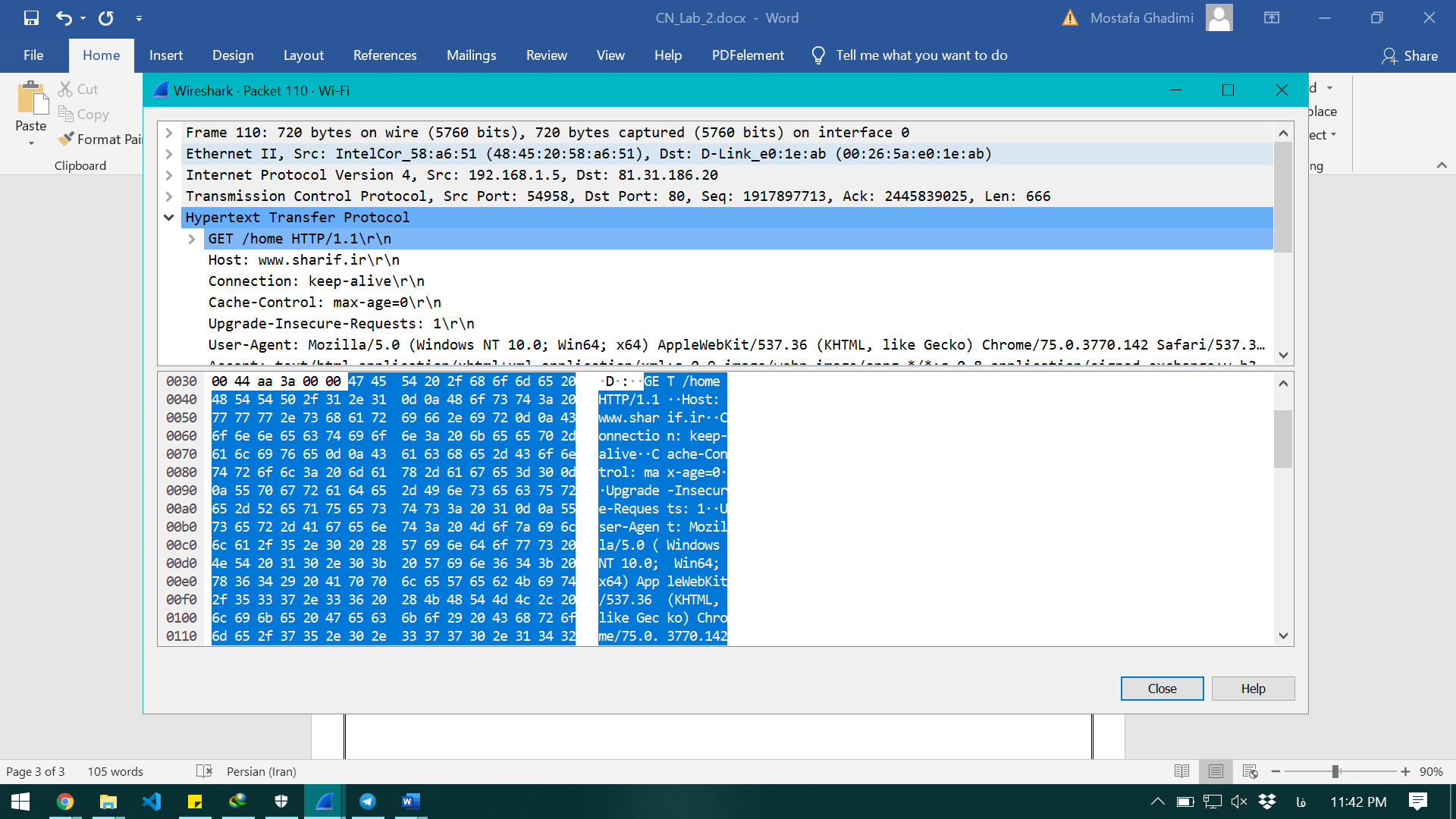
ابتدا مرورگر chrome را باز کرده و پس از قرار دادن نرم‌افزار wireshark به حالت capture، وارد صفحه اصلی سایت دانشگاه صنعتی شریف به آدرس sharif.edu می‌شویم.



حال به نرم‌افزار wireshark برگشته و حالت capture را متوقف می‌کنیم. سپس درون نوار فیلتر، عبارت http را تایپ می‌کنیم تا فقط درخواست‌هایی با پروتکل HTTP را به نمایش دهد.



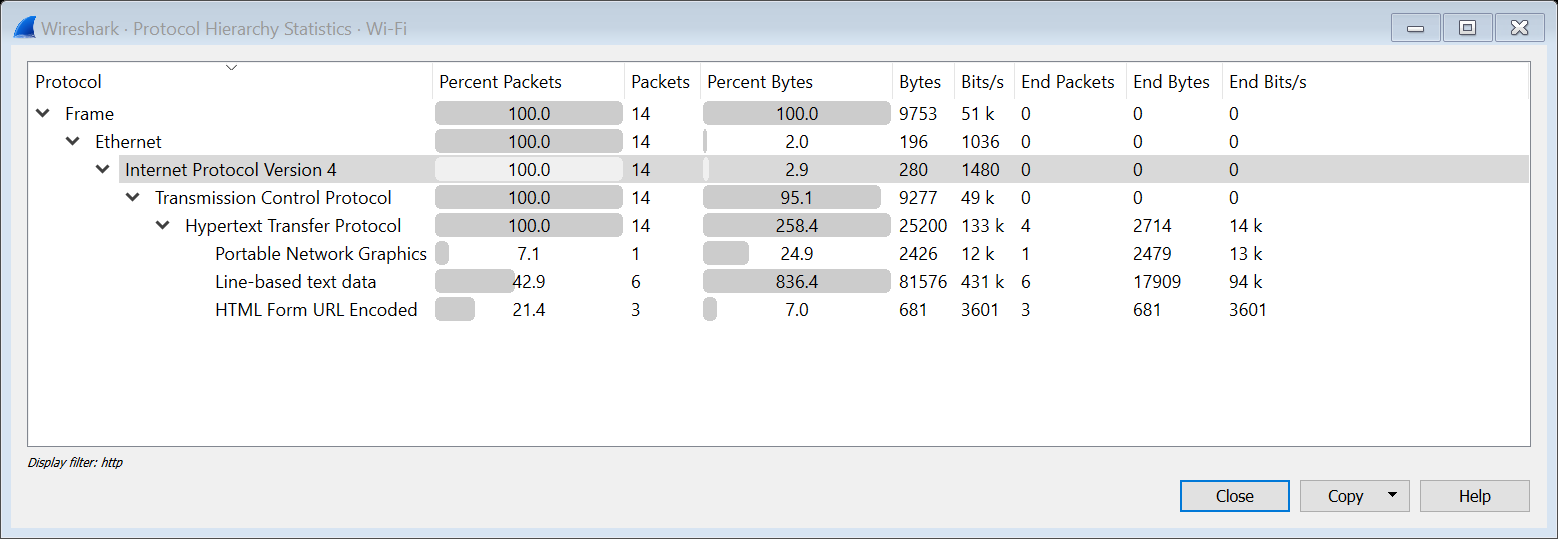
سپس روی درخواست اول کلیک می‌کنیم تا مطمئن شویم Host آن با آدرس موردنظر ما مطابقت داشته باشد.



**سوالات:**

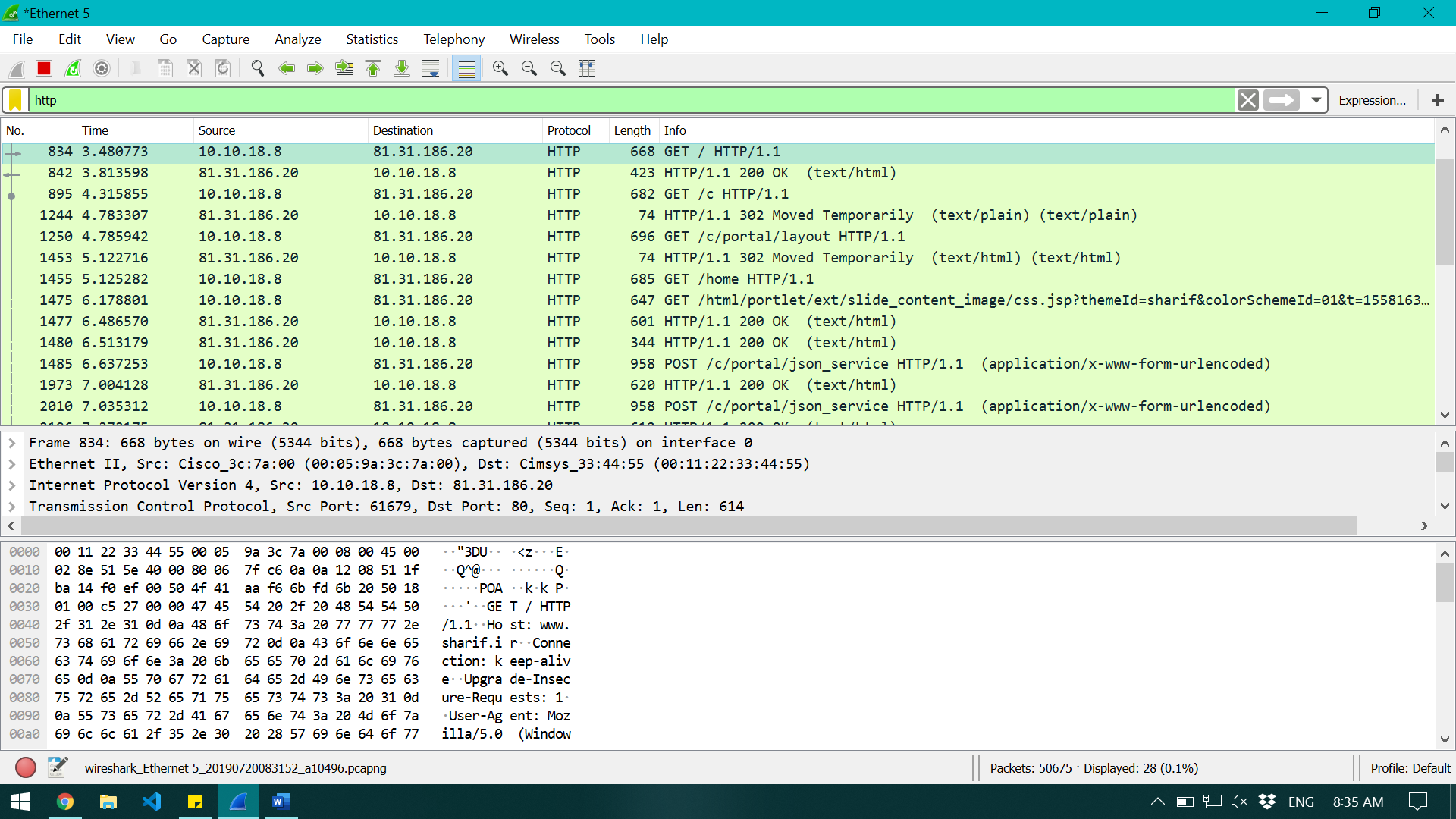
1- حجم عمده پیام‌های رد و بدل شده مربوط به کدام پروتکل‌ها است؟ هرکدام را به تفکیک اعلام کنید.

حجم عمده‌ی پیام‌های رد و بدل شده مربوط به پروتکل TCP است. برای این کار از Statistics > Protocol Hierarchy را انتخاب کرده و سپس با توجه به اعمال فیلتر، دریافتیم که اکثر درخواست‌ها مربوط به این پروتکل هستند.

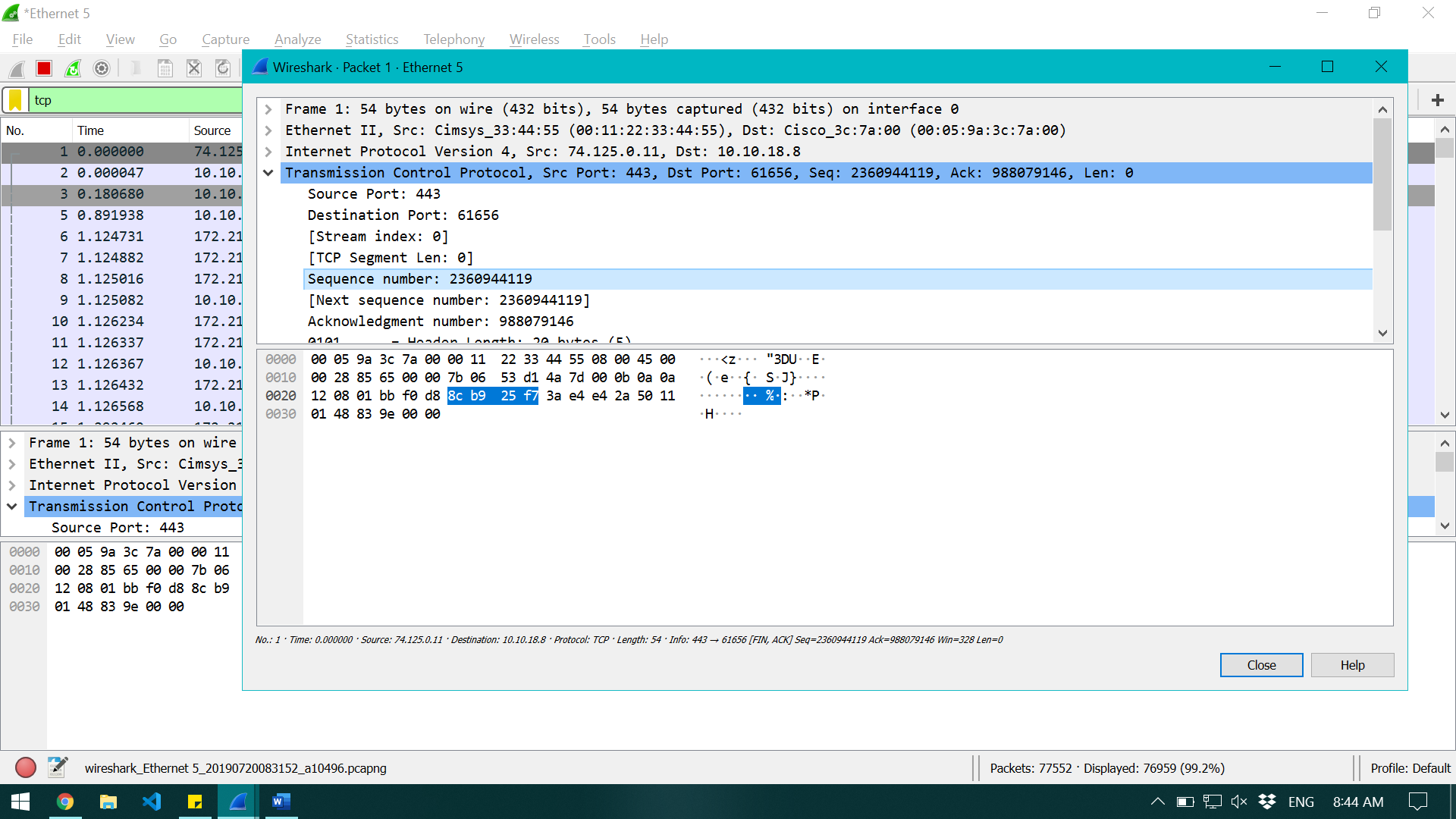


2- اختلاف زمانی بین ارسال درخواست GET HTTP و دریافت پاسخ OK HTTP چقدر است؟ شماره ترتیب مطلق اولین ارتباط TCP در این فایل را پیدا کنید.

همان‌طور که در تصویر مشاهده می‌کنیم، اختلاف زمانی بین هر درخواست GET HTTP و دریافت پاسخ OK HTTP برابر با 3.813598 – 3.480773 است.

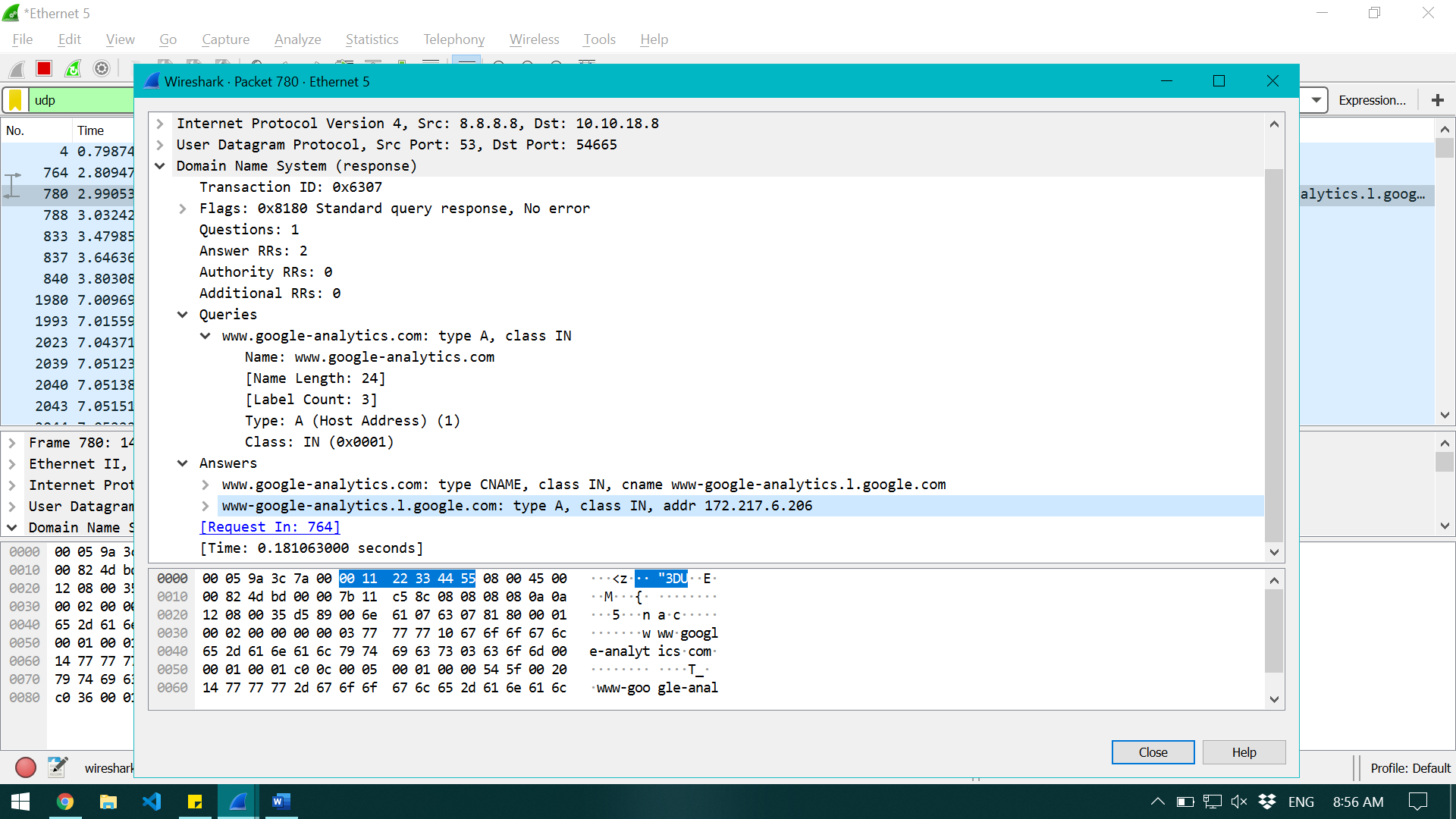


شماره ترتیب مطلق اولین ارتباط TCP برابر با 2360944119 است. برای نمایش شماره ترتیب مطلق (absolute sequence number) به مسیر Edit > Preferences > Protocols > TCP مراجعه کرده و تیک Relative Sequence Number را برداشتیم.



3- نوع کوئری درخواست‌های DNS و پاسخ آن‌ها چیست؟

نوع درخواست‌ها از type A هستند و خود DNS از پروتکل UDP استفاده می‌کند. پاسخ (همان‌طور که از کار DNS برمی‎آید) آن به صورت یک آدرس اینترنتی است.

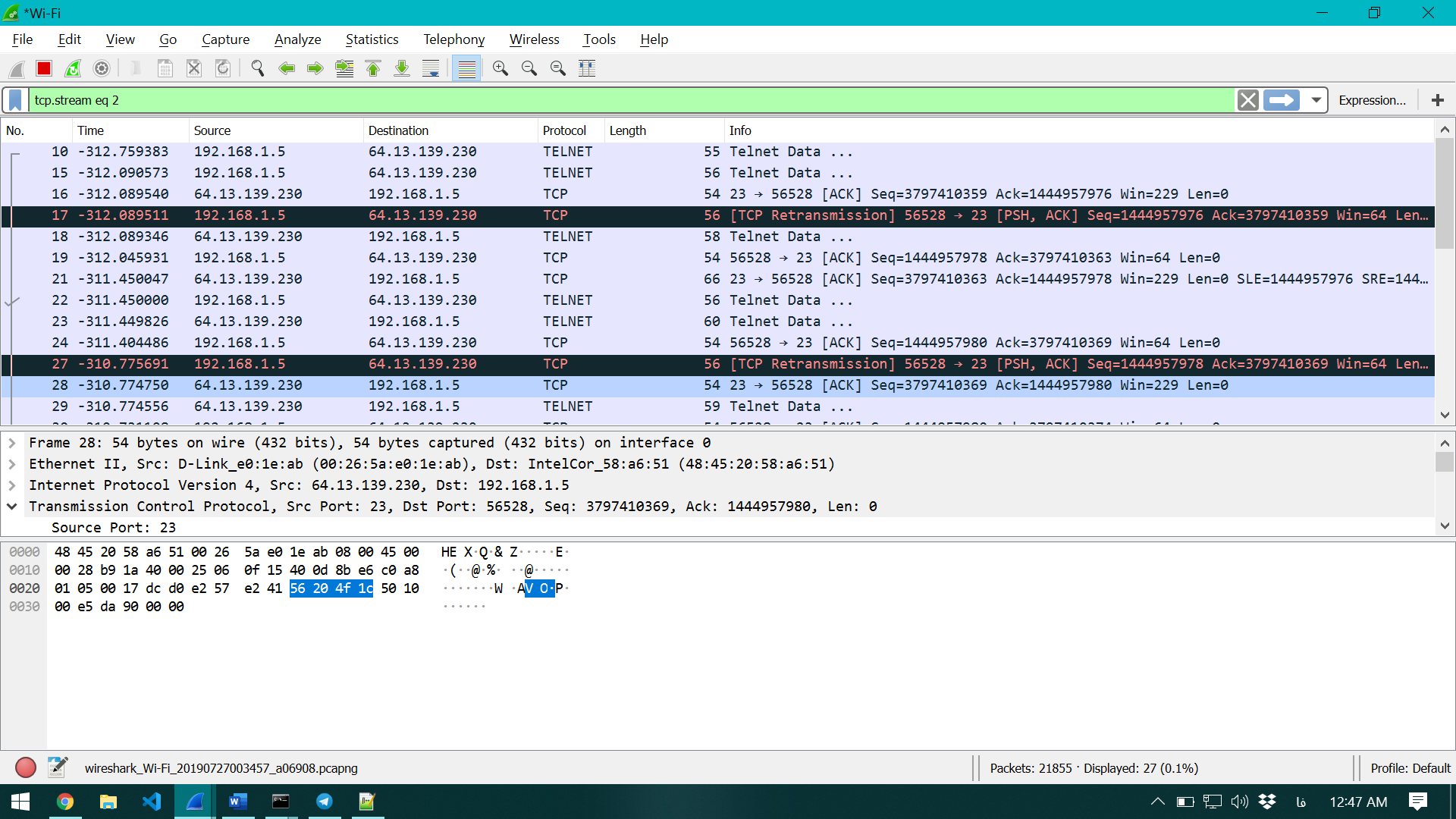


4- با استفاده از وارد کردن دستور frame contains ‘image’ در قسمت فیلتر به راحتی می‌توان به تمامی تصاویر دسترسی پیدا و آن‌ها را ذخیره و بازیابی کرد.

**بخش دوم (بررسی ارتباط از طریق telnet):**

1- آدرس IP کلاینت و سرور را پیدا کنید.

IP کلاینت: 192.168.1.5 IP سرور: 64.13.139.230

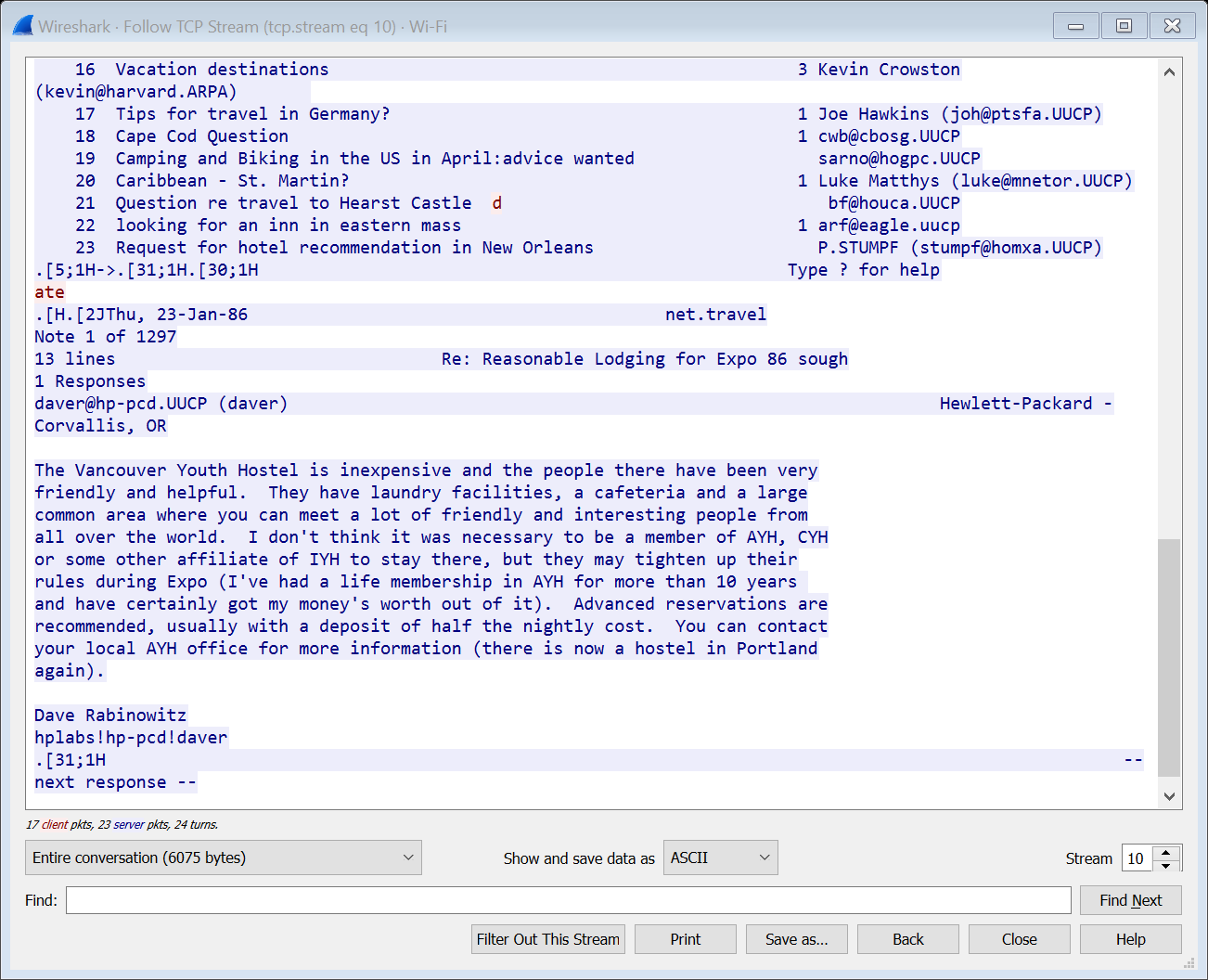


2- رمز عبوری که کلاینت برای لاگین استفاده کرده را بازیابی کنید

برای بازیابی رمزعبور به Analyze > Follow > TCP Stream می‌رویم و رمزعبور در آن‌جا نوشته شده است.

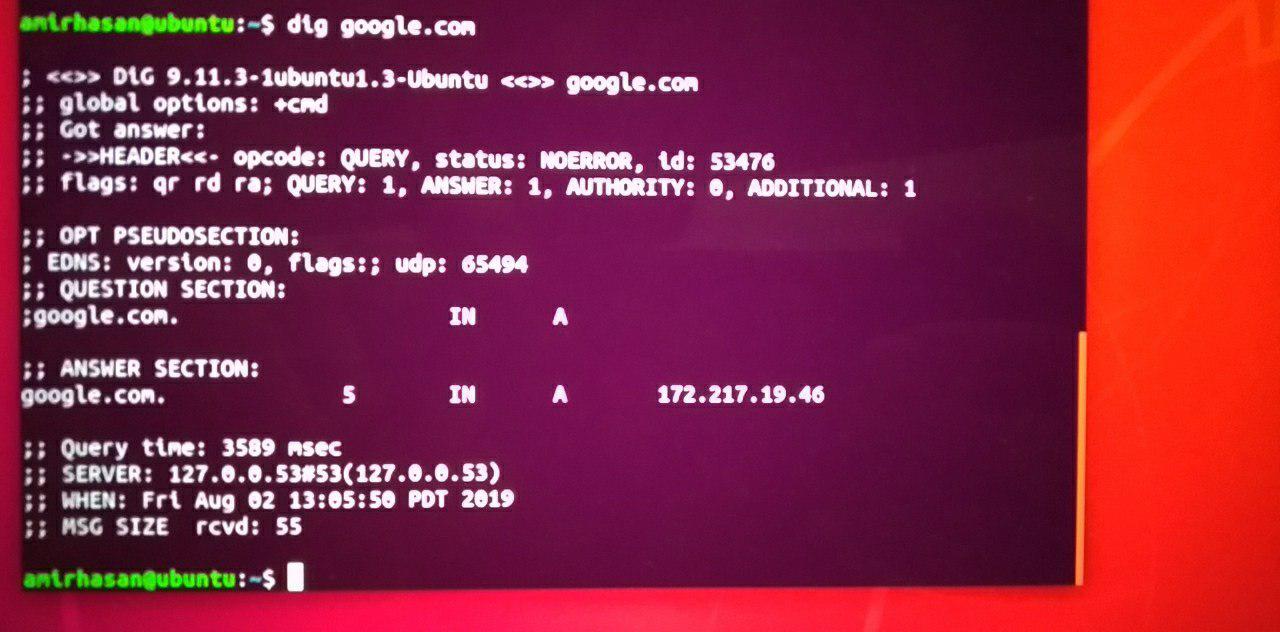
3- دستوراتی که توسط کلاینت اجرا شده‌اند را مشخص کنید.

همانند قسمت «2» به Analyze > Follow > TCP Stream می‌رویم و دستورات در آن‌جا نوشته شده است.



**بخش سوم (بررسی درخواست و پاسخ‌های DNS):**

1- در دستور dig درخواست برای کدام سرور ارسال می‌شود؟ پاسخ‌ها از کدام سرور دریافت می‌شود؟



پاسخ از سرور به آدرس 172.217.19.46 دریافت می‌گردد و به 127.0.0.53 ارسال می‌گردد.

2- هدر پیام‌های request و reply مربوط به پروتکل DNS را تحلیل کنید.

در عکس بالا مشهود است.