

فرم گزارش کار آزمایشگاه شبکه

| نام و نام خانوادگی | کیان پورآذر | شماره دانشجویی | نام و شماره آزمایش | راهنمایی با تنظیمات مقدماتی مربوط به راه اندازی سرویسهای Web و FTP و تحلیل بسته های HTTP و FTP |
|--------------------|-------------|---|---|---|
| ابزارهای مورد نیاز | آزمایش | هدف آزمایش | برنامه Filezilla نسخه 1.0.17.3 و سیستم عامل ترجیحاً ویندوز 7 | کامپیوتر با سیستم عامل ترجیحاً ویندوز 7 و برنامه Filezilla نسخه 1.0.17.3 |
| شرح آزمایش | آزمایش | در ابتدا تنظیمات مربوط به سرور وب را انجام میدهیم. سپس تنظیمات مربوط به اضافه کردن سایت تست در iis را انجام میدهیم و فایل تست را مینویسیم. | سوال 1: با توجه به اینکه اطلاعات را داخل فایل hosts اضافه نکردیم، وب سرور به صورت گلوبال دنبال هاست میگردد و به صورت لوکال سایت بالا نماید. بعد از اضافه کردن اطلاعات و پاک کردن کش، سایت نمایش داده میشود. | سوال 1: با توجه به اینکه اطلاعات را داخل فایل hosts اضافه نکردیم، وب سرور به صورت گلوبال دنبال هاست میگردد و به صورت لوکال سایت بالا نماید. بعد از اضافه کردن اطلاعات و پاک کردن کش، سایت نمایش داده میشود. |
| آزمایش | آزمایش | آزمایش | سوال 2: وایرشارک نمیتواند هیچ بسته ای از سایت ما را شنود کند چون وایرشارک نمیتواند ترافیک مربوط به آدرس های loopback را شنود کند. برای حل این مشکل از Rawcap استفاده میکنیم و بسته ها را با آن شنود میکنیم سپس فایلی که اطلاعات شنود شده در آن قرار دارد را با وایرشارک باز میکنیم و اطلاعات را میخوانیم. | سوال 2: وایرشارک نمیتواند هیچ بسته ای از سایت ما را شنود کند چون وایرشارک نمیتواند ترافیک مربوط به آدرس های loopback را شنود کند. برای حل این مشکل از Rawcap استفاده میکنیم و بسته ها را با آن شنود میکنیم سپس فایلی که اطلاعات شنود شده در آن قرار دارد را با وایرشارک باز میکنیم و اطلاعات را میخوانیم. |
| آزمایش | آزمایش | آزمایش | سوال 3: طبق عکس پورت مبدأ 64743 و پورت مقصد 80 است. برقراری ارتباط با استفاده از پروتکل TCP و به روش handshaking صورت میگیرد. به گونه ای که ابتدا سیستم یک درخواست به سایت میفرستد و سپس از سایت یک پاسخ میگیرد که به معنای برقراری ارتباط است. با توجه به اینکه ما در فایل hosts مشخص کرده ایم که به از ای www.test.com ، آپی مورد نظر ما چی باشد و ب سرور دیگر برای گرفتن ip متناظر سراغ DNS نمیرود و سایت ما نمایش داده میشود. | سوال 3: طبق عکس پورت مبدأ 64743 و پورت مقصد 80 است. برقراری ارتباط با استفاده از پروتکل TCP و به روش handshaking صورت میگیرد. به گونه ای که ابتدا سیستم یک درخواست به سایت میفرستد و سپس از سایت یک پاسخ میگیرد که به معنای برقراری ارتباط است. با توجه به اینکه ما در فایل hosts مشخص کرده ایم که به از ای www.test.com ، آپی مورد نظر ما چی باشد و ب سرور دیگر برای گرفتن ip متناظر سراغ DNS نمیرود و سایت ما نمایش داده میشود. |

سوال 4: مقدار connection برابر است با keep-alive است و نشان دهنده این است که ارتباط بعد از فرستادن درخواست و گرفتن جواب از بین نمیرود و باز هم میشود با این ارتباط درخواست ارسال کرد.

درخواست HTTP، از نوع GET است به معنی اینکه میخواهد دیتا دریافت کند. مقدار user agent هم در تصویر زیر مشخص است.

مقدار user agent نشان دهنده نوع سیستم عامل و مرورگر است.

سوال 5: طبق تصویر مقدار flag برابر است با 018x0

سوال 6: سایت جدید hostname و پورت متفاوتی با سایت اولی دارد و در request type و زمان ارسال و حجم بسته ها متفاوت هستند.

سوال 7: با توجه به اینکه پورتی تعریف نشده و دو تا domain برای یک ip درنظرگرفته شده است پس هیچکدام از سایت ها نمایش داده نمیشوند.

سوال 8: بله با مشکل مواجه شدیم. دلیل این اتفاق هم این است که چون در certificate مرورگر و سایت اشتراکی وجود ندارد این دو نمیتوانند با هم ارتباط حفاظت شده برقرار کنند. با استفاده از rawcap اطلاعات را شنود میکنیم و با واپرشارک بسته ها را مشاهد میکنیم. در ابتدا درخواست اتصال فرستاده میشود و مرورگر یک key برミگرداند و از انجایی که key ای که توسط مرورگر فرستاده شده با key موجود یکسان نمیباشد اتصال امن برقرار نمیشود.

سوال 9: طبق تصویر گواهی به نام خودم است که توسط خودم ایجاد شده است. مدت زمان آن یکسال است و الگوریتم آن RSA است و کلید عمومی صادرکننده هم در عکس مشخص است.

سوال 10: خیر نمیتوانیم متن ارتباط را بخوانیم چون توسط TLS رمزنگاری شده است.

سوال 11: طبق عکس این دو خیلی متفاوت هستند برای مثال در الگوریتم رمزنگارش شده، کلید رمزنگاری و تاریخ انقضای گواهی متفاوت هستند.

از دستور LIST برای لیست کردن دایرکتوری ها استفاده میکنیم Username, password. توجه به اینکه در وضعیت ناشناس هستیم قابل مشاهده نیست پروتکل لایه انتقال FTP است. آدرس پورت مبدأ 21 و مقصد 51126 است.

سوال 13: تنظیمات عوض میکنیم و دوباره شنود را انجام میدهیم این بار با توجه به اینکه احراز هویت در وضعیت basic قرار دارد میتوانیم رمز عبور را مشاهده کنیم.

سوال 14: 2 سطح دسترسی basic و anonymous وجود دارد. حالا سطح دسترسی داده شده برابر است با:

Authentication = basic
permissions= read
authorization= all users

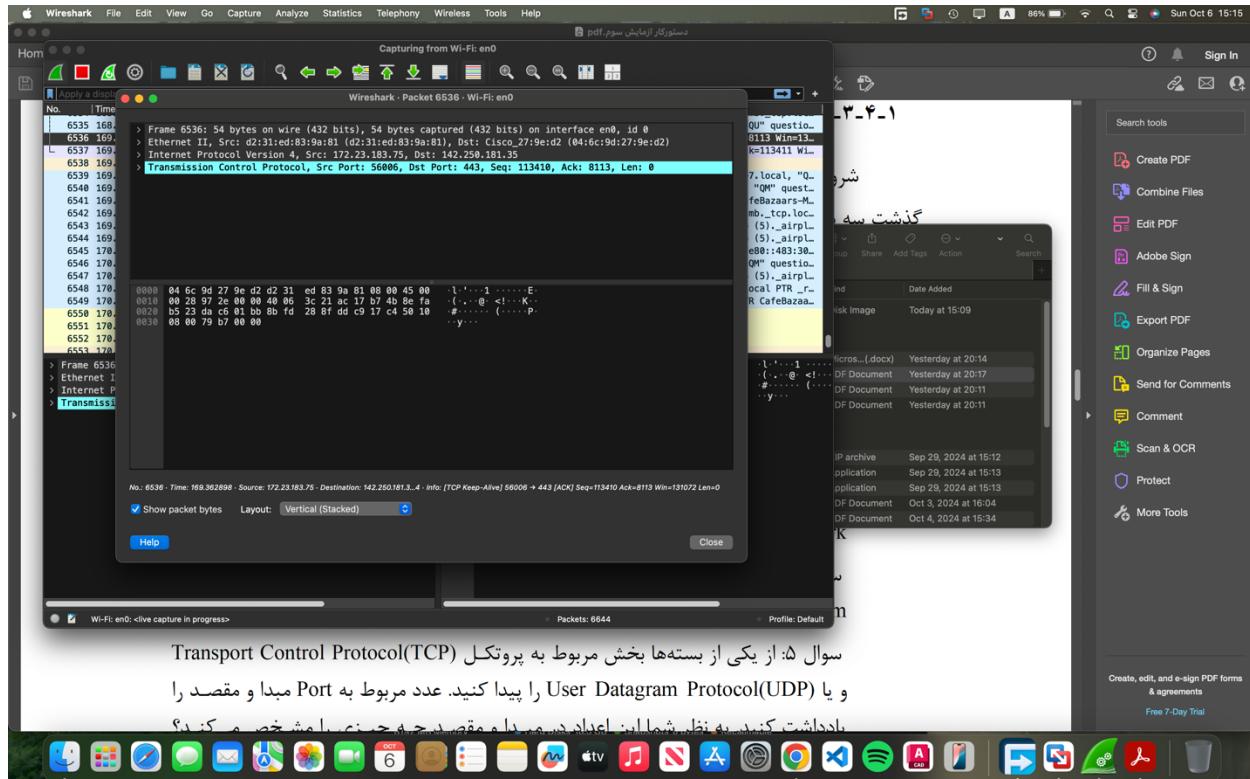
سوال 15: خیر نمیتوانیم وارد شویم.

سوال 16: این خطاب زمانی رخ میدهد که کاربر بخواهد با http یا FTP به جای TLS استفاده کند و سرور دارد کلاینت را ملزم به این میکند تا یک ارتباط TLS ایجاد کند.

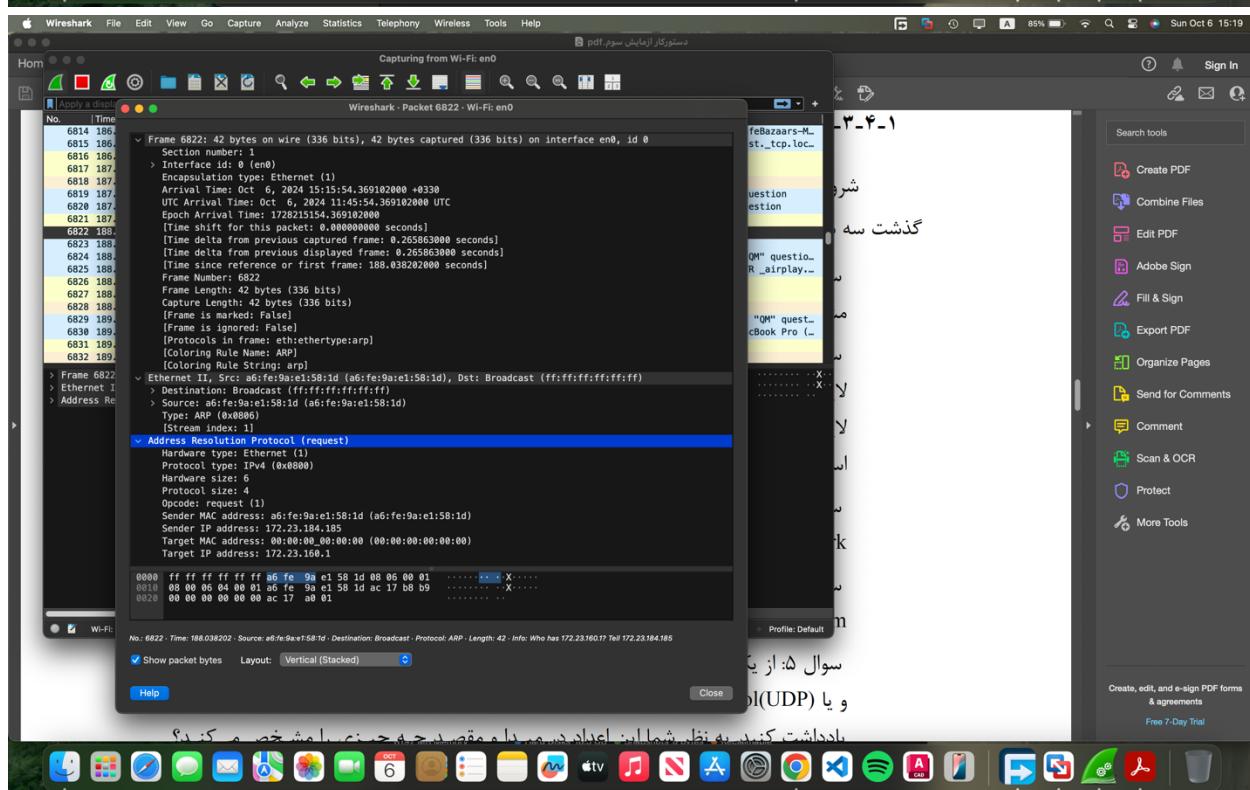
با پروتکل های HTTP و FTP و نحوه شنود با استفاده از Rawcap آشنا شدیم. توانستیم بسته های HTTP و FTP را تحلیل کنیم. همچنین نحوه بالا اوردن یک سایت و نحوه اعمال انواع تنظیمات برای آن و نحوه رمزگاری برای آن یکی از نتایج مهم این آزمایش است.

نتیجه-
گیری

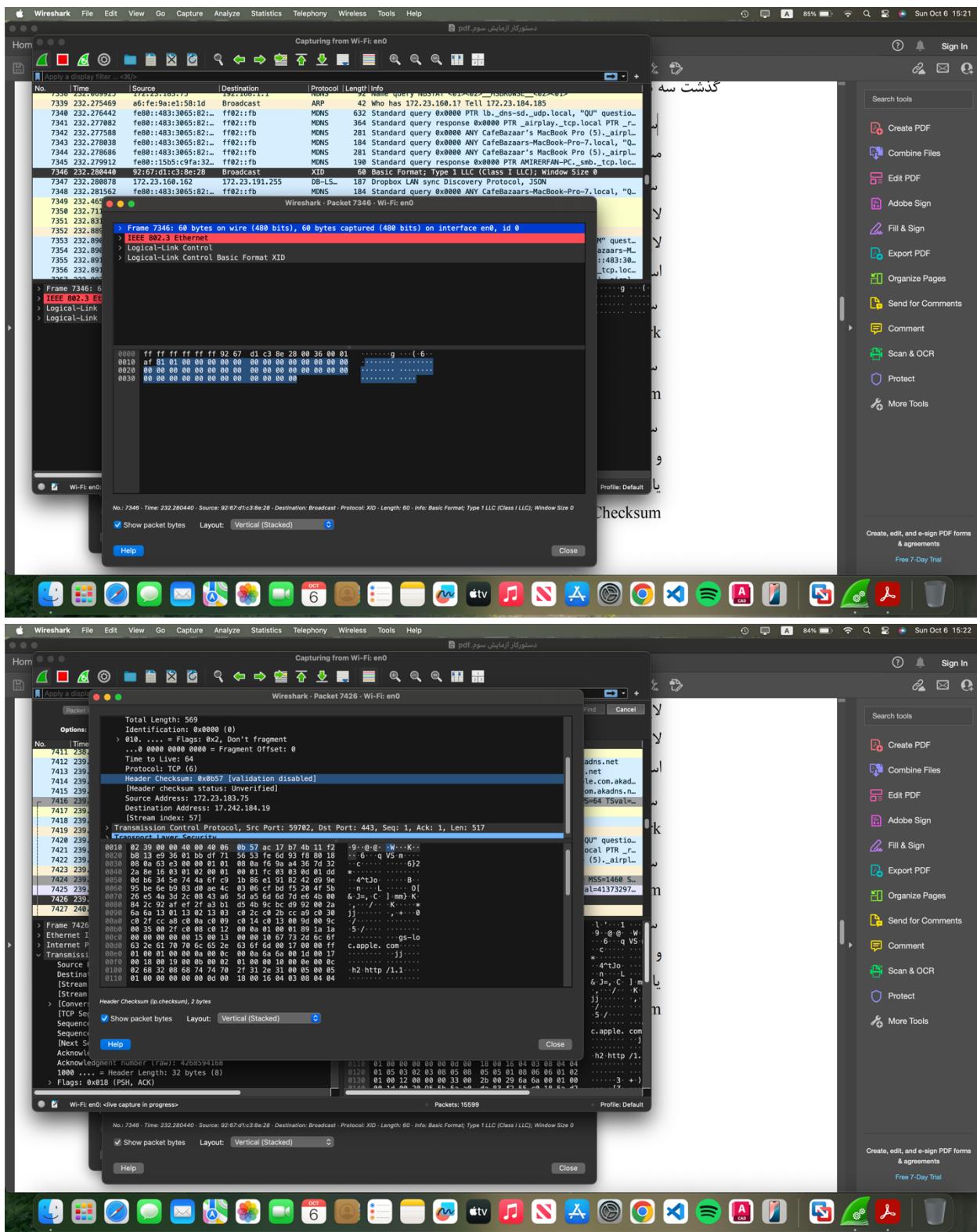
اسکرین شات‌ها:

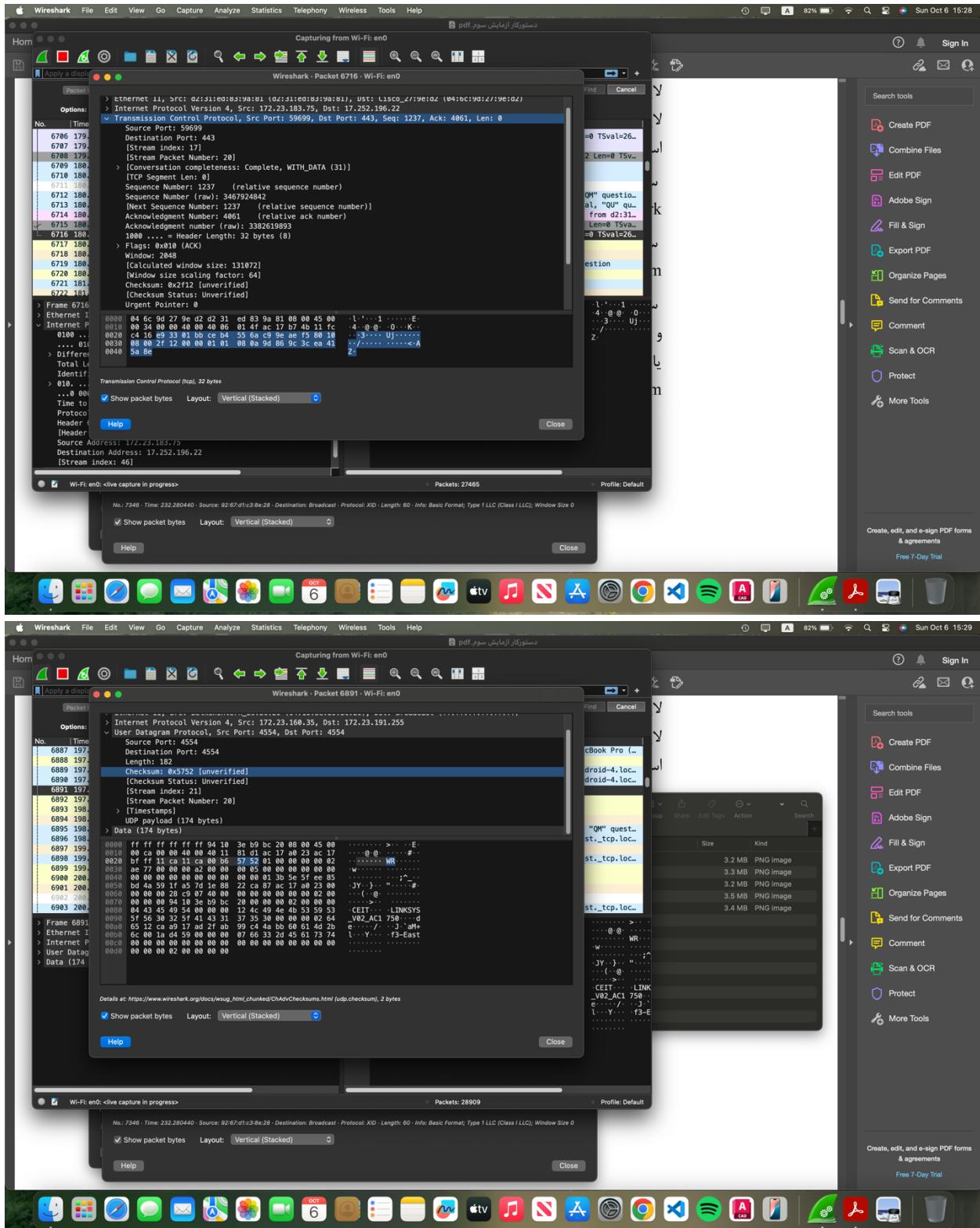


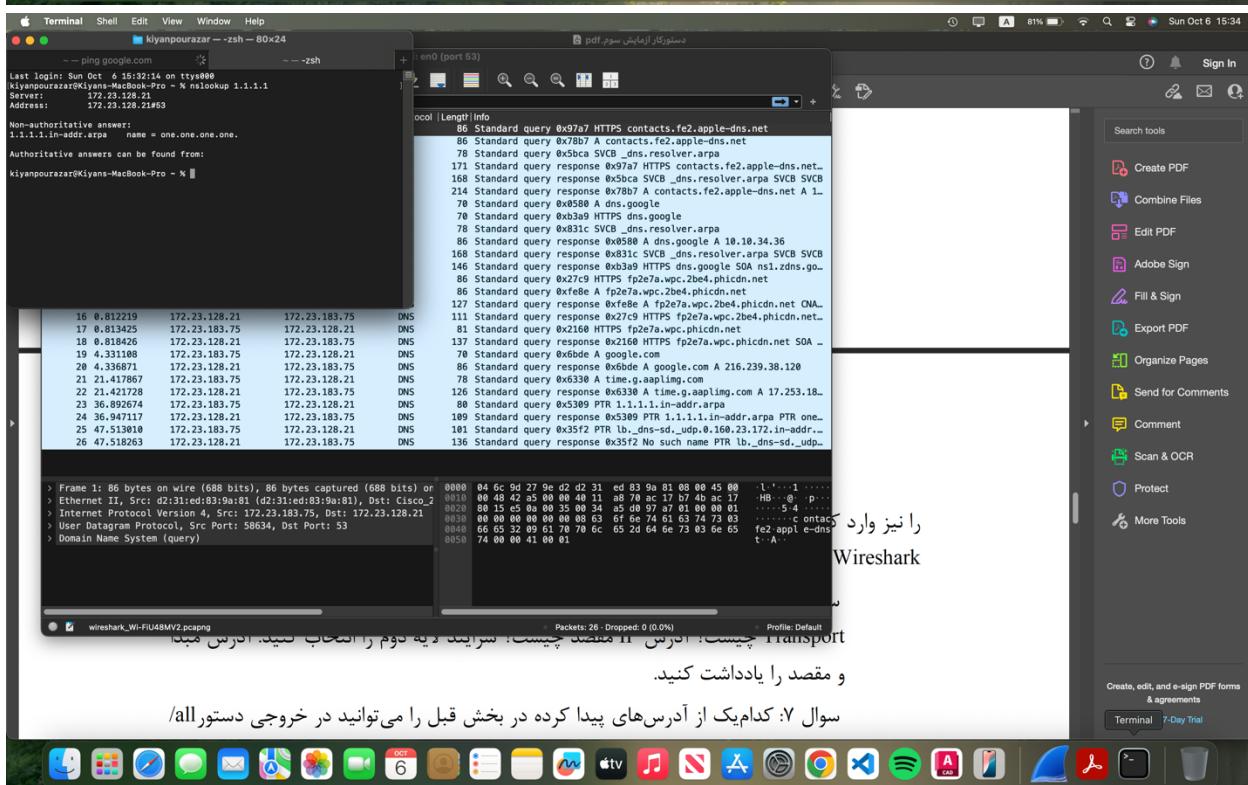
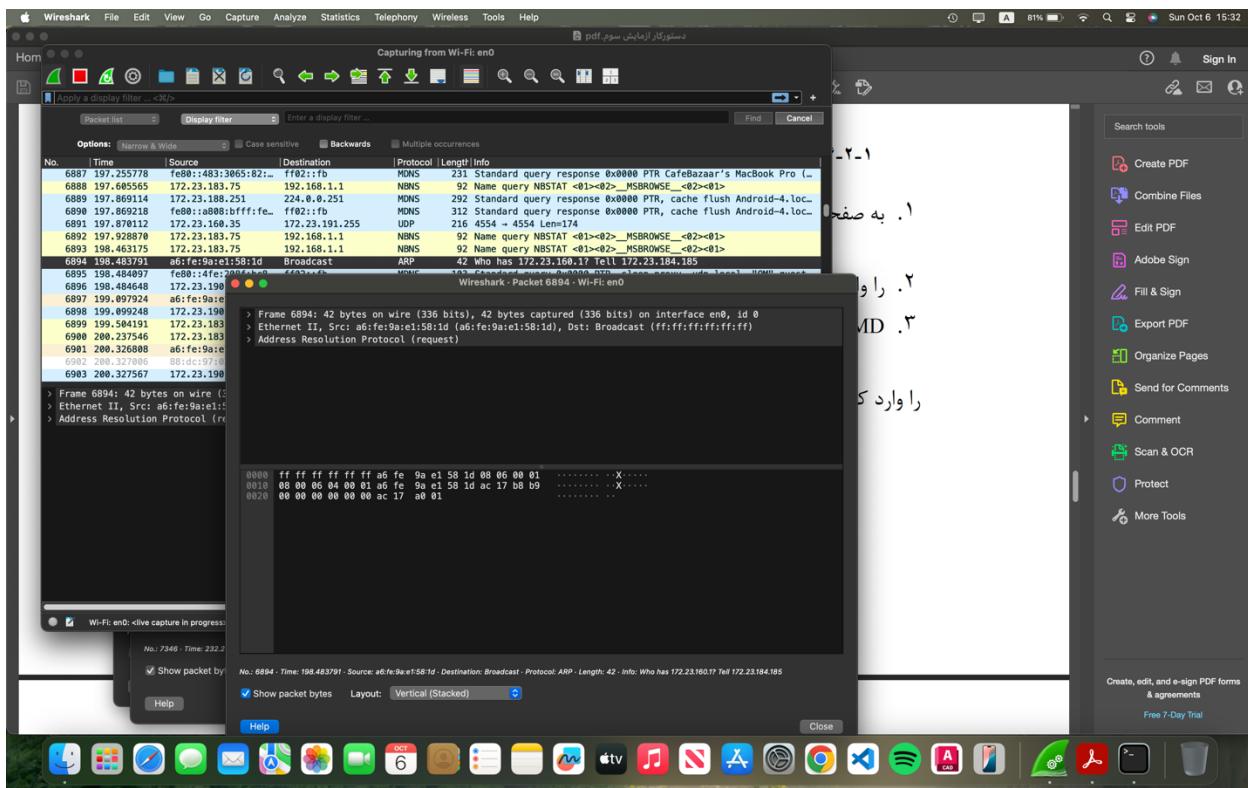
سوال ۵: از یکی از بسته‌ها بخش مربوط به پروتکل Transport Control Protocol(TCP) و یا User Datagram Protocol(UDP) را پیدا کنید. عدد مربوط به Port مبدأ و مقصد را بادلشت کنید و نظرشماست اعداد دو رقمی مقصود جو حوزه نامشخص می‌گردید؟

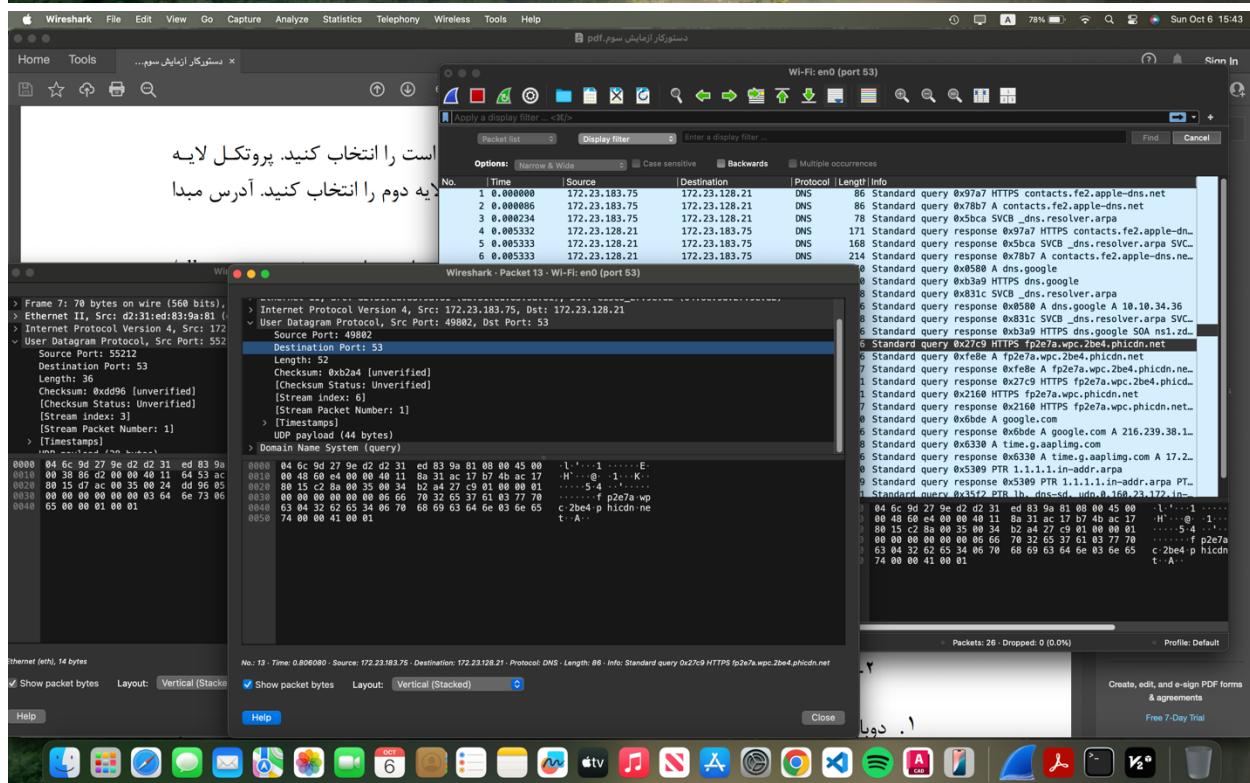
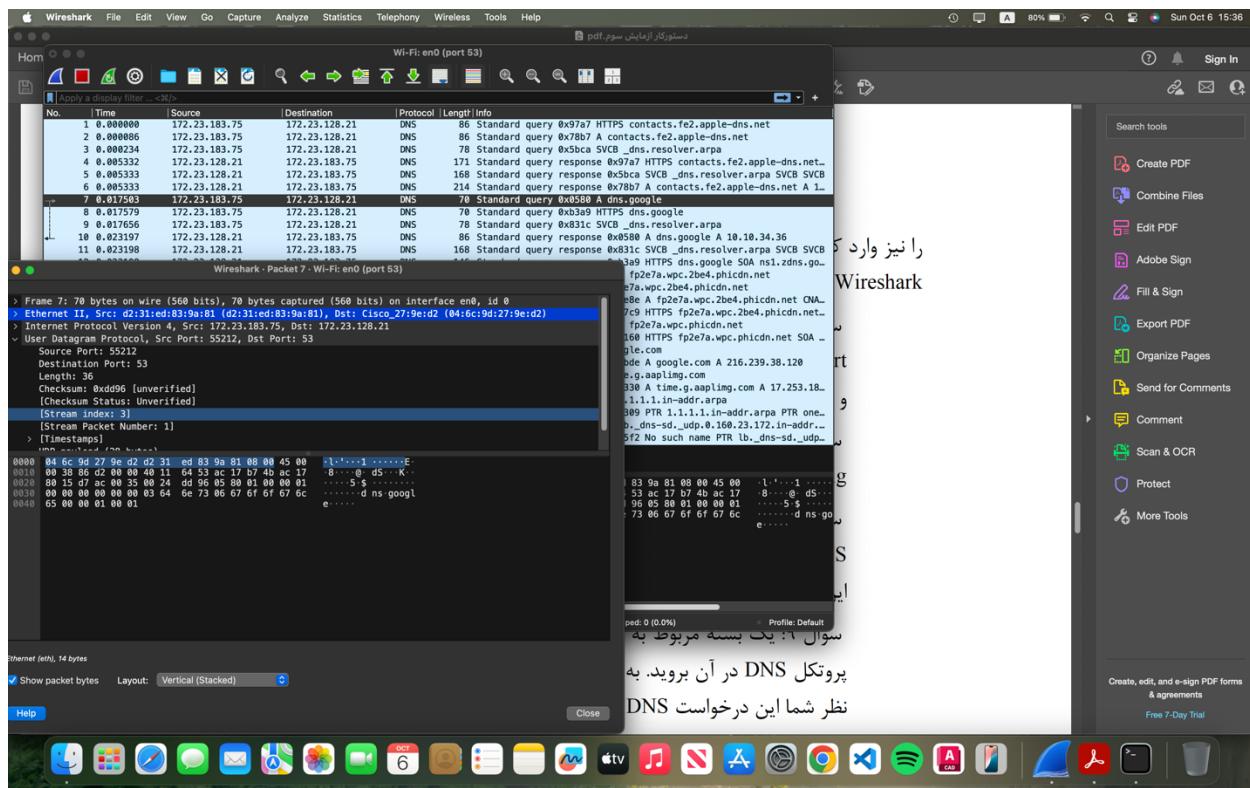


سوال ۵: از یکی از بسته‌ها بخش مربوط به پروتکل UDP و یا ARP را پیدا کنید. عدد مربوط به Port مبدأ و مقصد را بادلشت کنید و نظرشماست اعداد دو رقمی مقصود جو حوزه نامشخص می‌گردید؟









سوال ۷: یک بسته مربوط به دستور queries در آن بروید. به بخش DNS این درخواست برای چه کاری پرداخته شده است؟

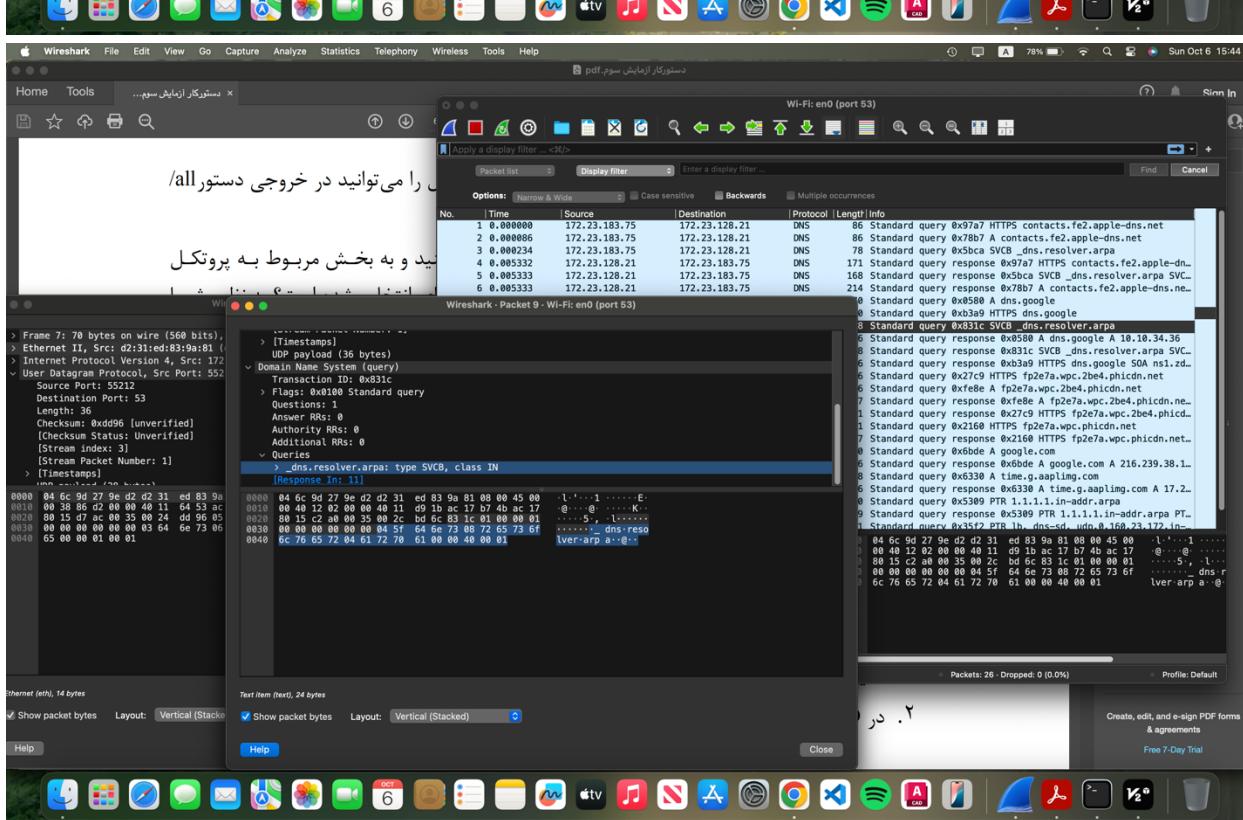
سوال ۸: یک بسته مربوط به دستور queries در آن بروید. به بخش DNS این درخواست برای چه کاری پرداخته شده است؟

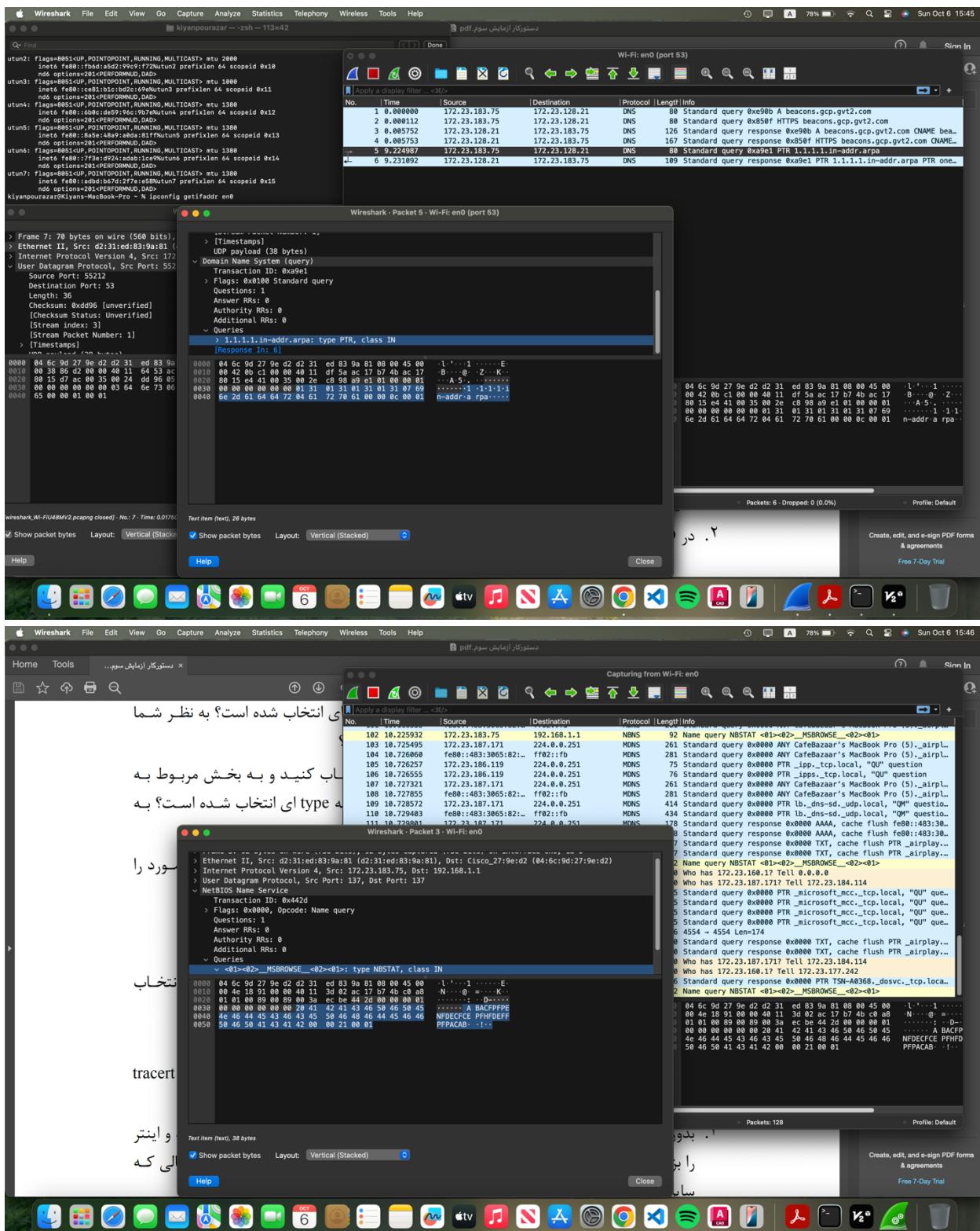
سوال ۹: یک بسته مربوط به دستور queries در آن بروید. به بخش DNS این درخواست برای چه کاری پرداخته شده است؟

سوال ۱۰: به نظر شما چه type های دیگری ممکن است وجود داشته باشد؟ سه مورد را یادداشت کنید.

Display Filter - کار با ۲-۴-۳-۲

۱. دوباره به صفحه اول برنامه بروید. این بار اینترفیس را بدون هیچ Capture Filter ای انتخاب کنید.





مسنونه از این پایش سوچ

نحوه انتخاب شده است؟ به نظر شما

لاب کنید و به بخش مربوط به type ای انتخاب شده است؟ به

پورت را

نتخاب

tracert

و اینتر

الی که

بود و به بخش مربوط به پروتکل

ای انتخاب شده است؟ به نظر شما

لاب کنید و به بخش مربوط به type ای انتخاب شده است؟ به

پورت را

نتخاب

tracert

و اینتر

الی که

مسنونه از این پایش سوچ

نحوه انتخاب شده است؟ به نظر شما

لاب کنید و به بخش مربوط به DNS

ای انتخاب شده است؟ به نظر شما

پورت را

نتخاب

tracert

و اینتر

الی که

مسنونه از این پایش سوچ

نحوه انتخاب شده است؟ به نظر شما

لاب کنید و به بخش مربوط به DNS

ای انتخاب شده است؟ به نظر شما

پورت را

نتخاب

tracert

و اینتر

الی که

