**به نام خدا**

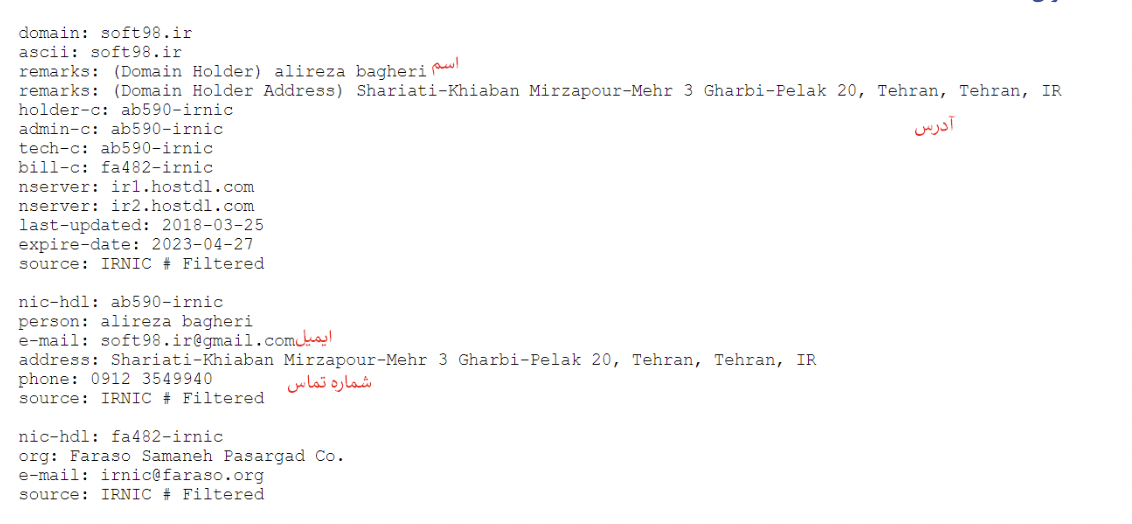
**نام و نام‌خانوادگی : روژینا کاشفی شماره دانشجویی:۹۸۳۱۱۱۸**

**کار با کاربرد‌های Web، DNS، سوکت و پویش سرویس‌ها**

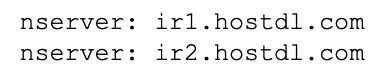
* **کارکرد DNS**

**سوال ۱) نام و اطلاعات فردی که دامنه به اسم ثبت شده است چیست؟**

دامنه به نام عليرضا باقري ثبت شده است. بخشي از اطلاعات اين دامنه مانند آدرس و تلفن مالك آن را در زير مي‌بينيم.

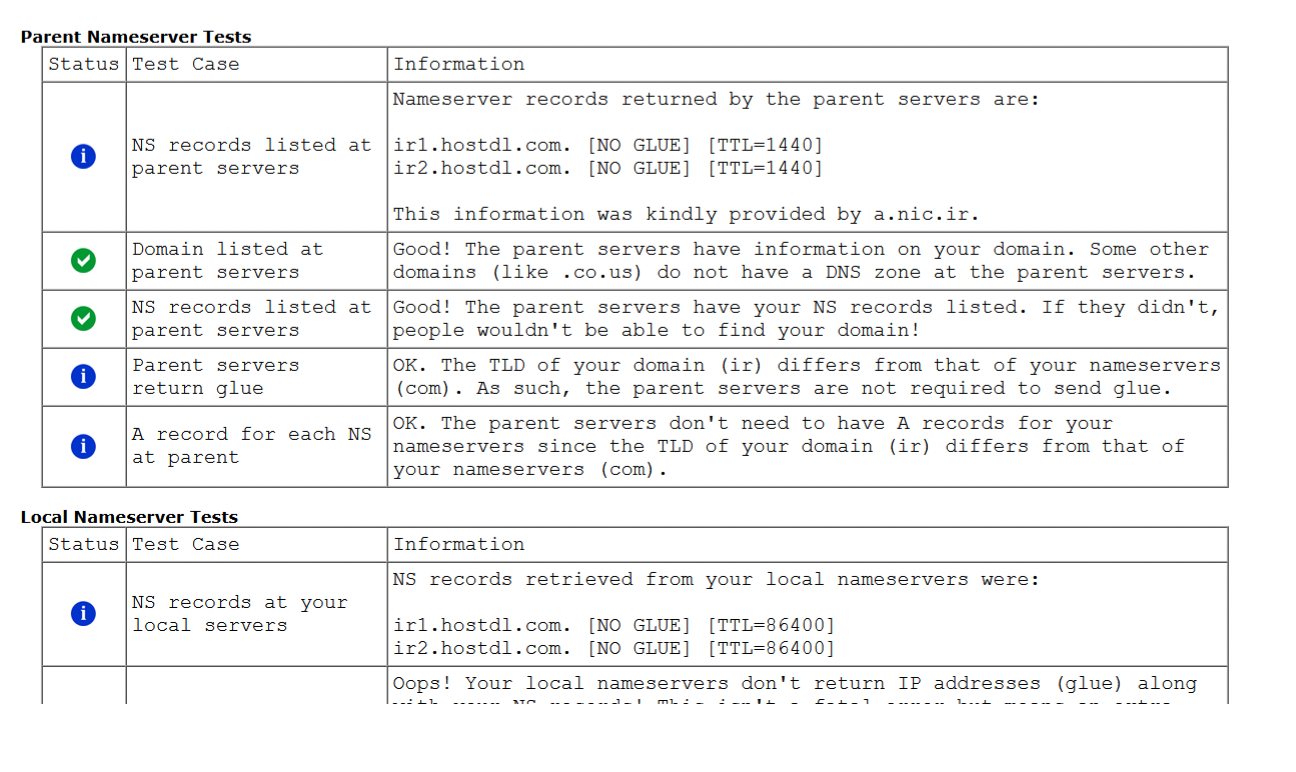
****

**سوال ۲) آدرس name server آن چیست؟**

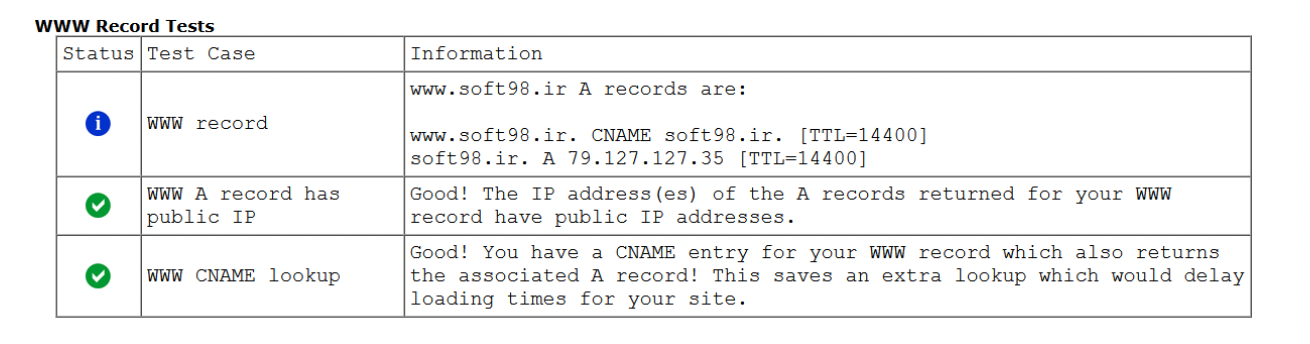
****

**سوال ۳) رکورد‌های NS، A، TXT، MX را مشخص کنید. هر یک از این رکورد‌ها چه چیزی را مشخص می‌کنند؟**

رکورد NS : این رکوردها مشخص می‌کنند که در ادامه‌ی فرآیند ترجمه نام دامنه به آدرس IP باید به کدام name server های معتبر درخواست بفرستیم.

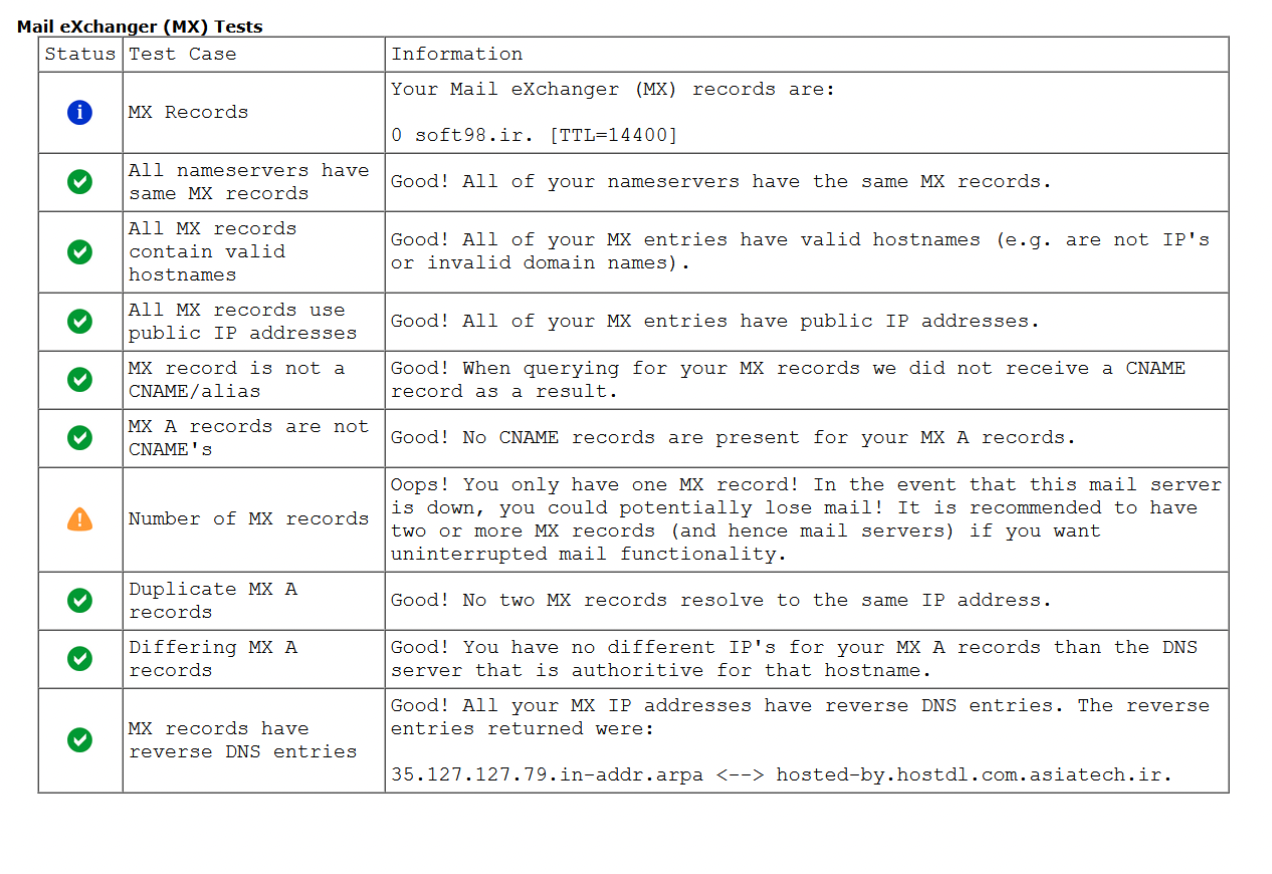


رکورد A : این رکورد که نام آن مخفف Address است، شامل آدرس IP درخواستی است.

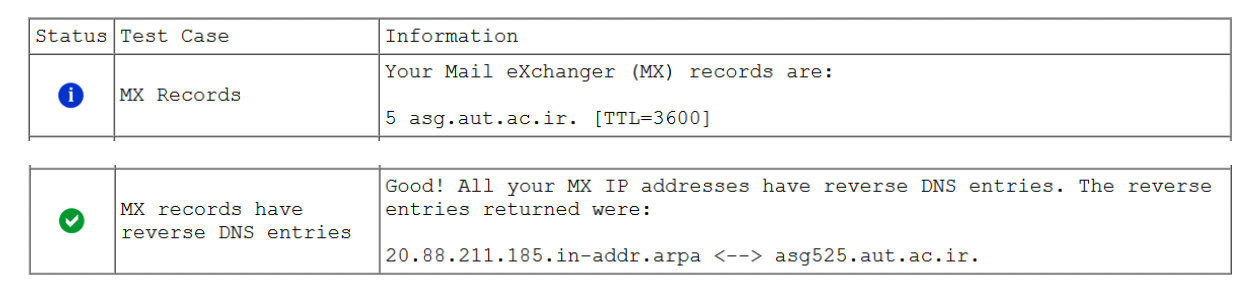
****

رکورد TXT: مخفف text است. رکوردی است که در آن اطلاعات اضافی می‌شود که توسط domain در رکوردهای DNS مربوط به آن گذاشته می‌شود و می‌تواند شامل یک سری دستورالعمل‌ها برای انسان‌ها یا ماشین‌ها باشد یا برای شناسایی قابل اطمینان بودن منبع ایمیل مورد استفاده قرار گیرد. که البته در این پویش چنین رکوردی یافت نشد.

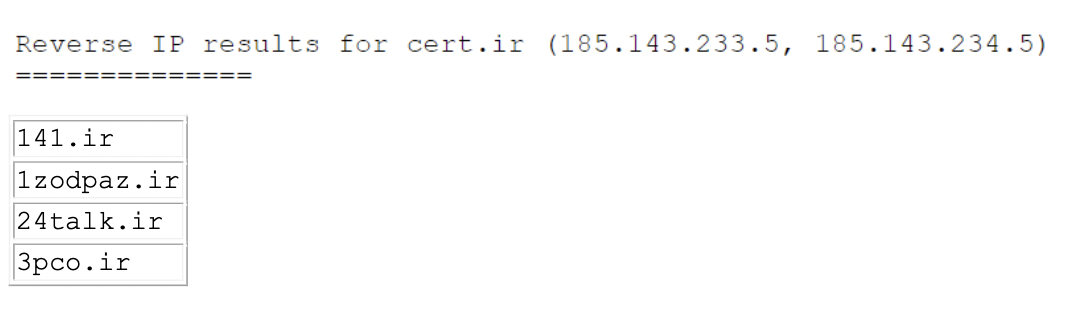
رکورد MX: استفاده از این رکورد برای مشخص کردن mail server ایست که مسئول دریافت ایمیل‌های این دامنه می‌باشد.

**سوال ۴) در قسمت DNS Report با وارد کردن دامنه‌ی دانشگاه (aut.ac.ir)، mail server دانشگاه را مشخص کنید. آیا ادرس IP آن را می‌توانید مشخص کنید؟**

برای این کار باید رکوردهای MX را بررسی کنیم که در تصویر زیر می‌بینیم. ادرس mail server دانشگاه عبارت است از asg.aut.ac.ir و ادرس IP آن هم 185.211.88.20 می‌باشد که از A رکورد بدست می‌اید.



**سوال ۵) چه وب‌سایت‌های دیگری بر روی همین سرور قرار دارند؟ چند مورد از آن‌ها را نام ببرید.**

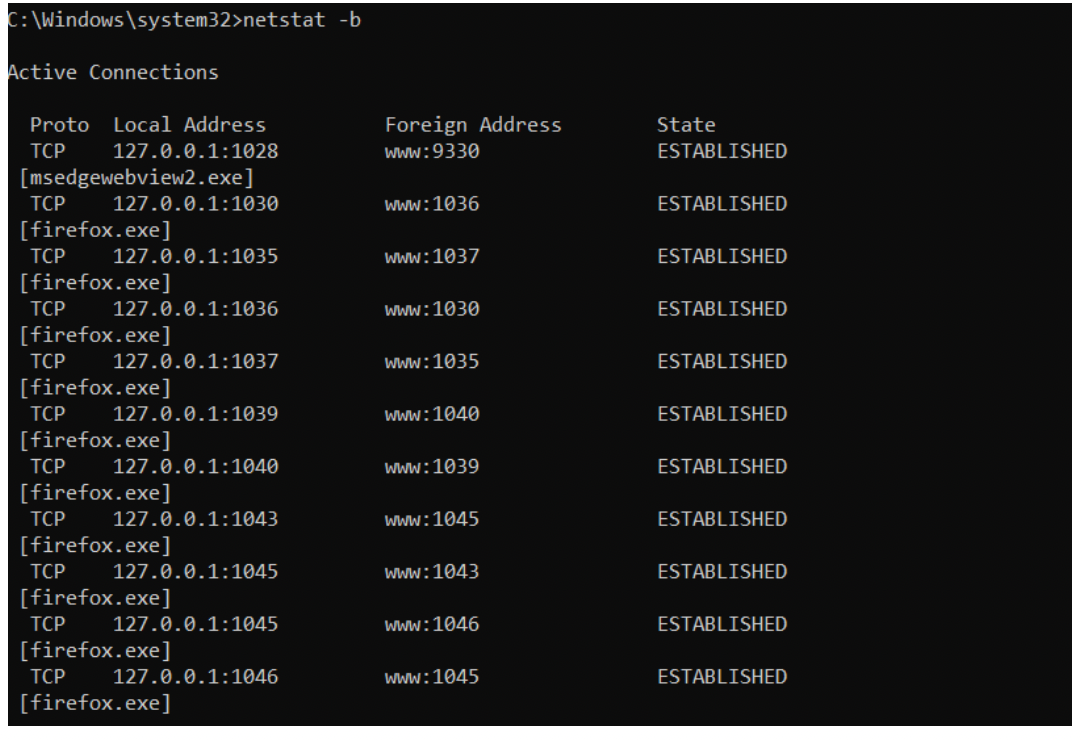


**سوال ۶) به نظر شما سرور چگونه وب سرور درخواست شده را تشخیص می‌دهد؟ ایا این روش نیز نوعی Multiplexing است؟**

زماني كه مرورگر يك درخواست HTTP ارسال مي كند، در هدر آن مقدار Host را برابر نام دامنه مورد نظر قرار مي دهد ا اين روش كه به نوعي Multiplexing است، ميتوان نام دامنه‌هاي زيادي را روي يك سرور ميزباني كرد.

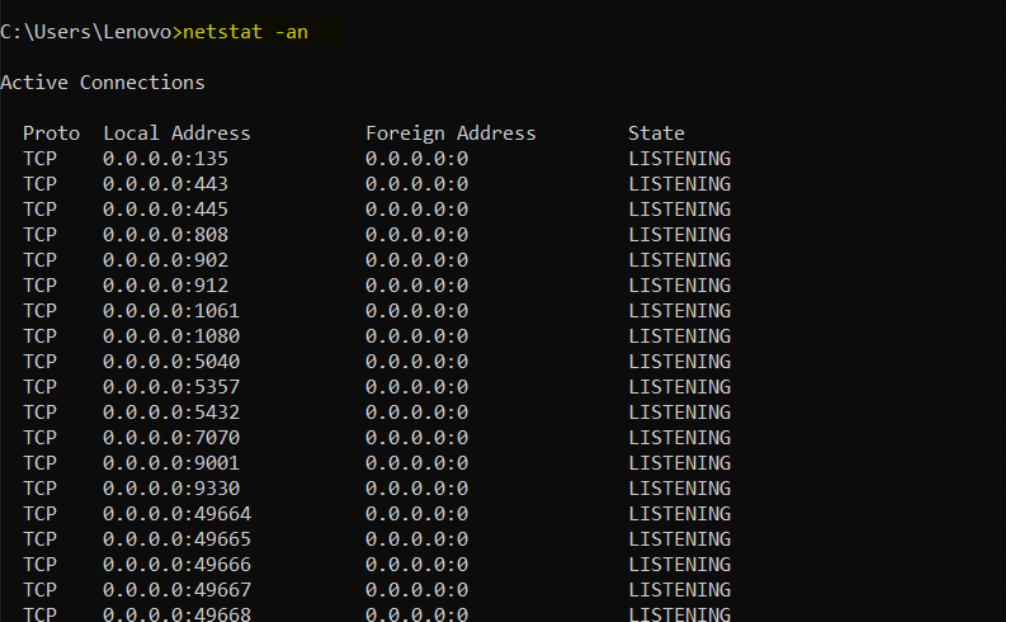
**سوال ۷) برای لیست کردن برنامه‌هایی که در حال حاضر پورت‌های لایه انتقال را بر روی سیستم بازکرده‌اند، از چه دستور خط فرمانی استفاده می‌شود؟**

با دستور netstat -b می‌توان برنامه‌هايي كه پورتي را استفاده مي‌كنند مشاهده كرد. سوييچ b- شماره پراسس برنامه‌ها نشان مي‌دهند.



**سوال ۸) دستوری را پیدا کنید که به وسیله آن تمام پورت‌های سیستم در هر وضعیت اتصالی همراه با مبدا و مقصد اتصال به صورت عددی لیست شوند.**

براي اين كار از همان netstat با سوييچ‌هاي a- براي نشان‌ دادن تمام پورت‌ها و n- براي نشان دادن به صورت عددي استفاده كرد. (netstat -an)



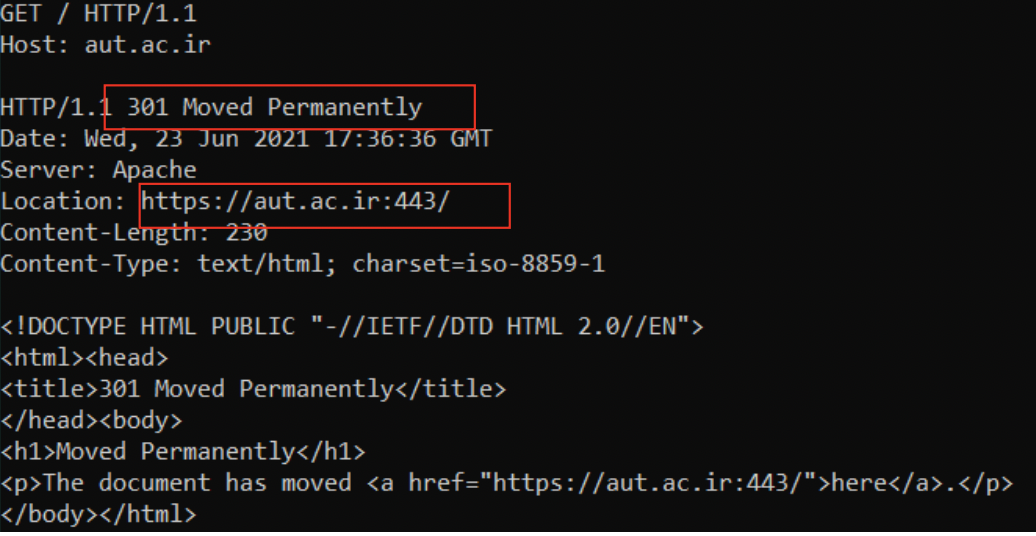
* **کارکرد Web**

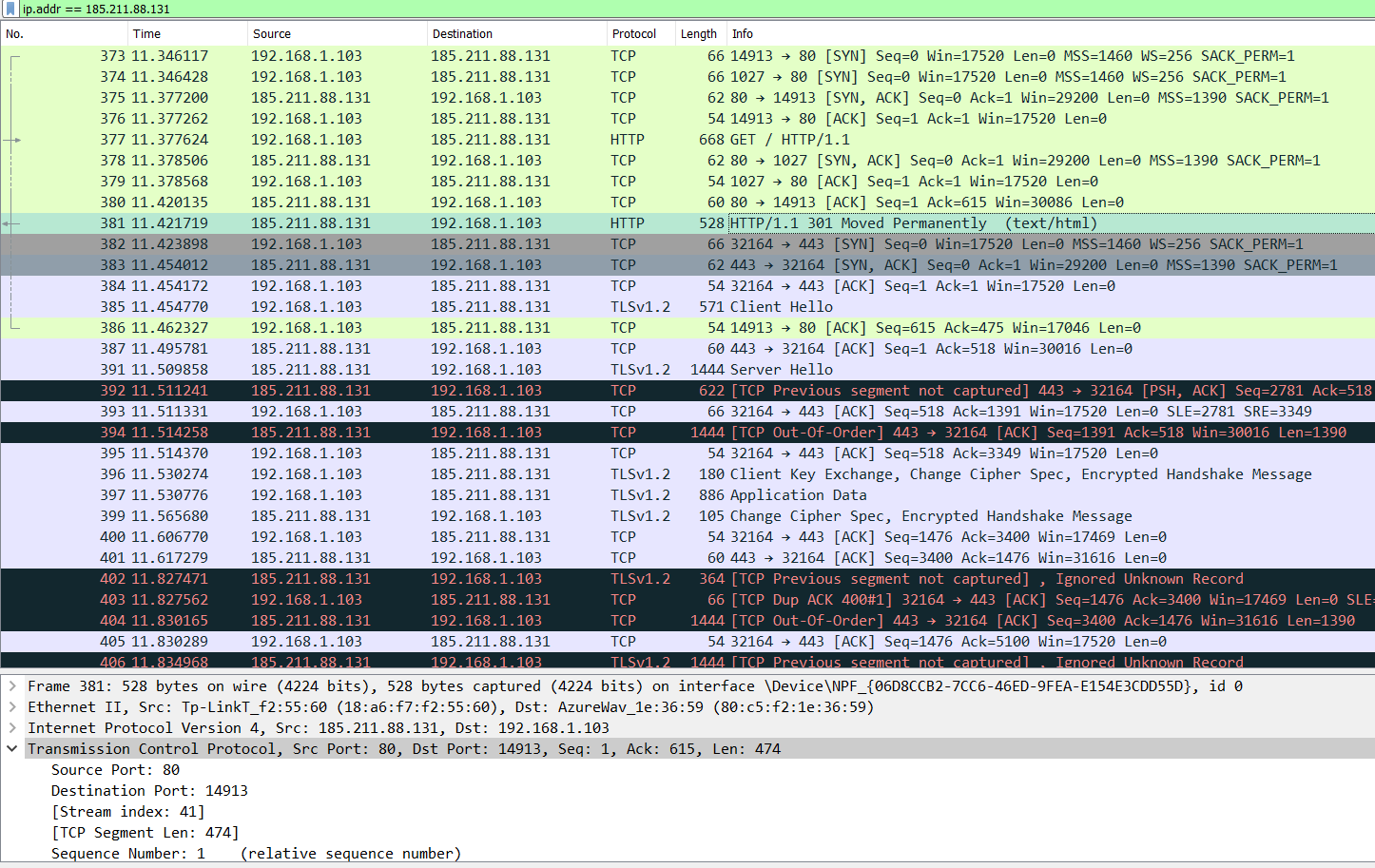
**سوال ۹) دلیل وارد کردن دو enter پشت سر هم چیست؟**

جدا کننده request Header و request Body یک خط خالی است. پس برای نشان دادن اینکه header ها تمام شده باید یک بار دیگر enter بزنیم.

**سوال ۱۰) پیامی که در پاسخ تقاضای شما داده می‌شود چیست؟ صفحه اصلی در کجا قرار دارد؟ ادعای خود را با استفاده از تقاضا به همین صفحه در مرورگر و ضبط پیام‌ها با استفاده از wireshark اثبات کنید.**

پاسخ درخواست به صورت زیر است و با ارور 301 مواجه می‌شویم که به معنی moved permanently است و با بررسی این پاسخ مشخص است که آدرس جدیدی که دامنه به آن منتقل شده است https://aut.ac.ir:433 می‌باشد.





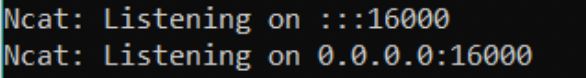
همانطوری که مشاهده می‌کنید، ابتدا درخواست HTTP برای پورت 80 سرور فرستاده می‌شود و با پیام moved permanently رو به رو می‌شود و پس از استفاده از پروتکل TLS و به دست آوردن key، ادامه‌ی ارتباط روی پورت 443 خواهد بود.

**سوال ۱۱) ایا این ارتباط persistent است؟**

از آنجایی که در هدر درخواست HTTP مشخص نکردیم که مقدار Keep-Alive چه باشد و نوعConnection را نیز تعیین نکردیم، این مقادیر به در ورژن 1.1 HTTP به صورت دیفالت برای یک اتصال persistent تنظیم می‌شوند.

**سوال ۱۲) این پورت بر کدام آدرس IP، bind شده است؟ بعد از برقراری ارتباط با این سوکت، برنامه CMD نیز اجرا می‌شود. در ادامه دستوراتی که فرستنده ارسال کند به این برنامه داده می‌شوند و خروجی دستورات از طریق ارتباط برقرار شده منتقل خواهد شد.**

با ورود این دستور، هرگاه به پورت 16000 درخواستی فرستاده شود، cmd تجرا خواهد شد. آدرس IP bind شده 0.0.0.0 است.

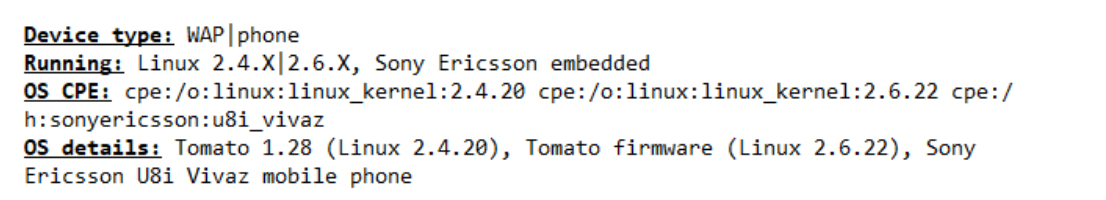
****

**سوال ۱۳) دقت کنید یک خط خالی بین HTTP و <html> باید وجود داشته باشد. به نظر شما دلیل وجود خط اول در این فایل چیست؟ یک فایل دیگر بدون خطا اول این فایل بسازید و نتیجه را امتحان کنید.**

دلیل وجود خط اول آن است که بعد از اینکه درخواست http برای این سرور ارسال شد، این سرور در پاسخی که برای کلاینت ارسال می‌کند ابتدا در یک خط status code به درخواست http پاسح م‌یدهد که وجود این خط در پاسخ‌های http الزامی است در حالی که هدرهای بعد از آن اختیاری هستند و در انتهای خطوط مربوط به هدر یک enter اضافی می‌گذاریم که اتمام هدر http را نشان می‌دهد و در سوال 9 نیز به آن اشاره کردیم که این enter نهایی هم اجباری است و در نهایت data مورد درخواست کاربر که یک فایل html است را قرار می‌دهیم.

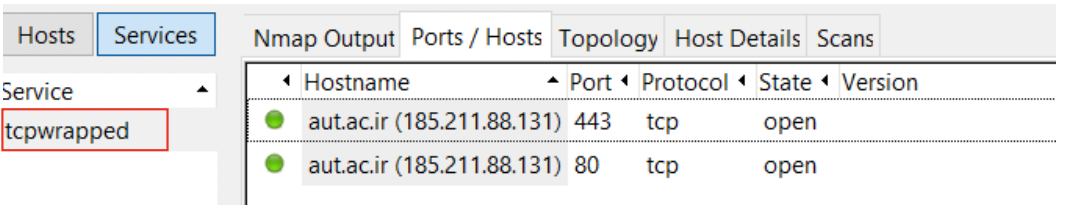
* **پویش سرویس‌ها**

**سوال ۱۴) سیستم‌عامل این وب‌سایت چیست؟**

****

**سوال ۱۵) چه پورت‌هایی روی این سرور باز است؟**

**https 443/http 80**

****

**سوال ۱۶) سرویس‌هایی که از طریق این پورت‌ها ارائه می‌شود چیست؟**

سرویس tcpwrapped در این پورت‌ها ارائه می‌شود. روی پورت ۸۰ http و ۴۴۳ https ارائه می‌شود.