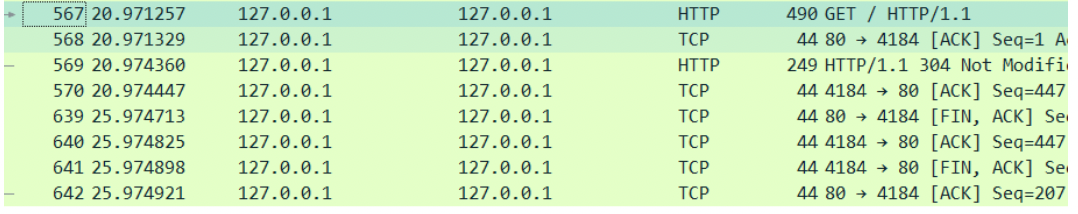
**راه‌اندازی سرویس Web و FTP**

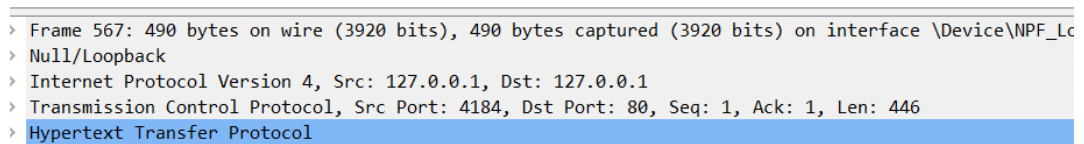
نام و نام‌خانوادگی: روژینا کاشفی شماره دانشجویی : ۹۸۳۱۱۱۸

* **تنظیمات سرور web**

**سوال ۱) ادرس پورت مبدا مقصد چیست؟ روند برقراری ارتباط در پروتکل HTTP چگونه است؟ وب سرور چگونه ادرس سایت درخواستی شما را تشخیص می‌دهد؟**

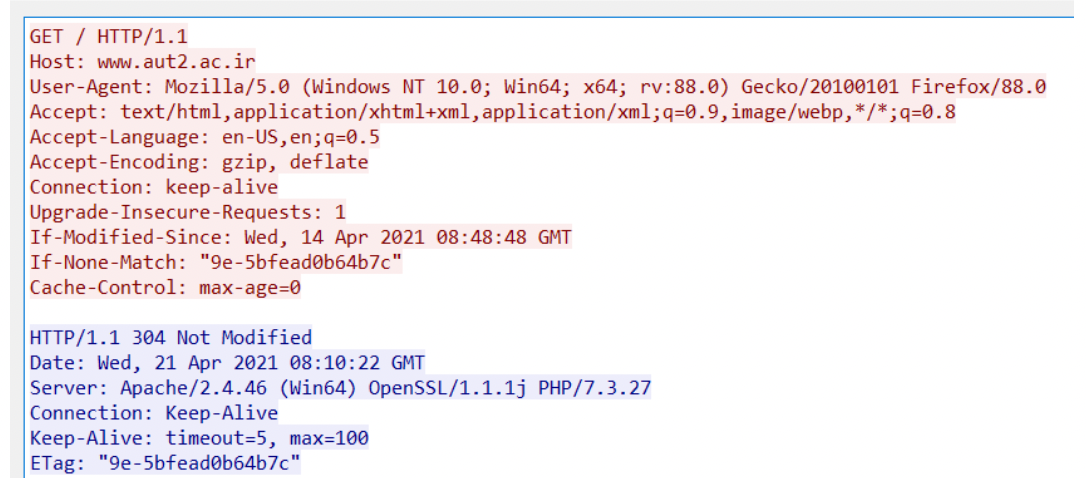
ادرس پورت مبدا و مقصد در شکل مشخص شده است.





برقراری ارتباط از طریق سوکت TCP می‌باشد و روند در خواست به این شکل است که ایتدا یکtcp handshake اتفاق می‌افتد و یک درخواست از سمت host به (sync) destination فرستاده می‌شود و سپس dest پاسخ ack می‌دهد که بدان معناست که connection برقرار شده است و سپس درخواست http زده می‌شود وب سرور ادرس سایت را که داخل etc/hosts دخیره شده که در آن لوکال هاست را به www.aut2.ac.ir مپ کرده بودیم تشخیص می دهد و همچنین اگر در قایل ذکر شده ادرس مورد نظر پیدا نشود آنگاه سلسه مراتب query زدن DNS طی می‌شود.

با استفاده از دستور HOST ادرس سایت درخواستی مشخص می‌شود.



**سوال ۲) مقدار بخش connection چیست؟ درخواست HTTP از نوع get بوده یا post؟ مقدار useragent چیست؟ به نظر شما این مقدار بیانگر چه چیزی است؟**

مقدار connection برابر با keep-alive است و این بدان معناست که سوکت TCP بعد از ارسال جواب در یافتن آن این ارتباط قطع نمی‌شود و برای درخواست های آینده باز می‌ماند و persistent است.



از نوع get

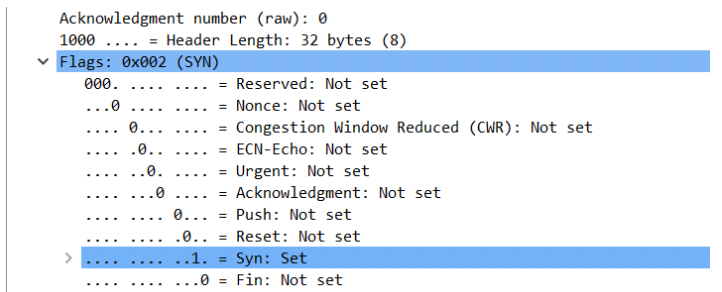


Useragent نشان‌گر استفاده ما از نوع مرورگر و سیستم‌عامل ما است.



**سوال ۳)** **در پنجره باز شده، اولین بسته را انتخاب کنید. سپس مقدار FLAGS در پروتکل TCP را مشاهده کنید. چه مقادیری برای این بسته تنظیم شده است؟**

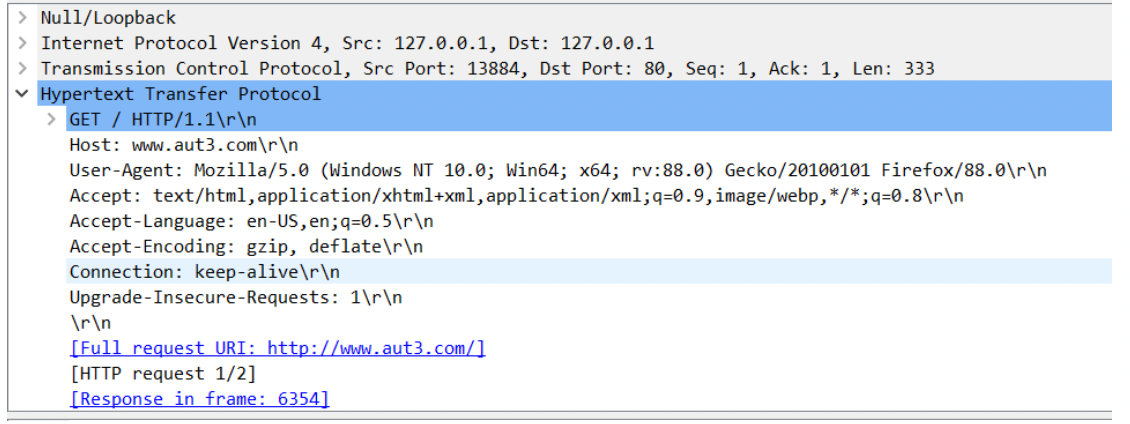
در اولین بسته انتخابی SYN=1 است.



**سوال ۴)** **یک سایت دیگر با نام دلخواه ایجاد کنید و بسته‌های مربوط به آن را شنود کنید. چه تفاوتی بین این دو سایت وجود دارد؟**

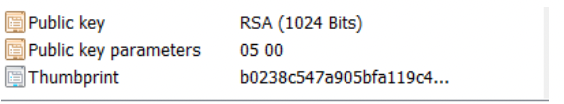
این بار از ادرس aut3.com استفاده کردیم. همانطوری که مشاهده می‌کنید:

1. آدرس پورت مبدا متفاوت است تا بتوان بسته‌های مربوط به آن‌ها را از هم جدا کرد.
2. طول بسته‌های آنها نیز متفاوت است.
3. پارامترهای acknowledge number و sequence number هم متفاوت است.
4. مقدار پورت مقصد یکسان است.
5. زمان ارسال درخواست متفاوت است.
6. اسم هاست‌ها متفاوت است.

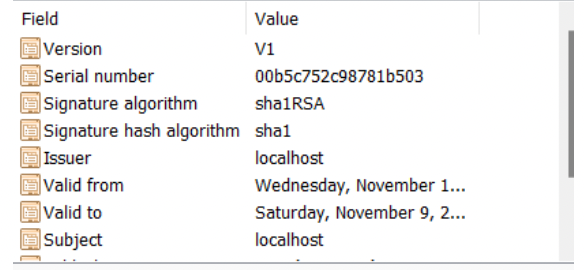


**سوال ۵) مشخص کنید که گواهی را چه کسی برای چه کسی صادر کرده، مدت اعتبار گواهی چقدر است، کلید عمومی صادرکننده چیست و امضای دیجیتال انجام شده با چه الگوریتم‌هایی انجام شده است.**

گواهی توسط localhost برای localhost صادر شده است. مدت اعتبار آن ۱۰ سال است، اما تاریخ اعتبار آن گذشته است. صادر کننده کلید عمومی RSA است.

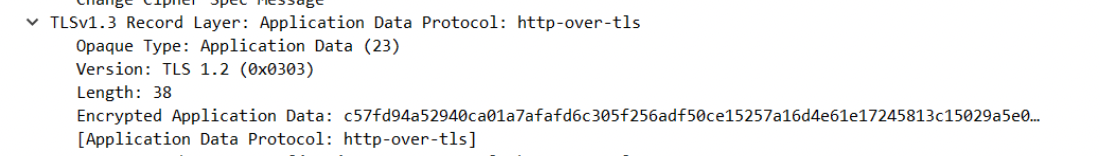


امضای دیجیتال با الگوریتم SHA1RSA و الگوریتم هش SHA1 انجام شده است.



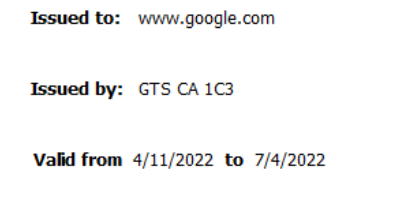
**سوال ۶) آیا می‌توانید متن ارتباط را بخوانید؟ چرا؟**

خیر. از آنجایی که از پروتکل tls استفاده شده است، متن این ارتباط قابل خواندن نیست. پروتکل tls وظیفه‌ی رمزگذاری (encryption) ارتباط بین سرور و کلاینت را به عهده دارد.



**سوال ۷) گواهی آن سایت با سایت شما چه تفاوت‌هایی دارد؟**

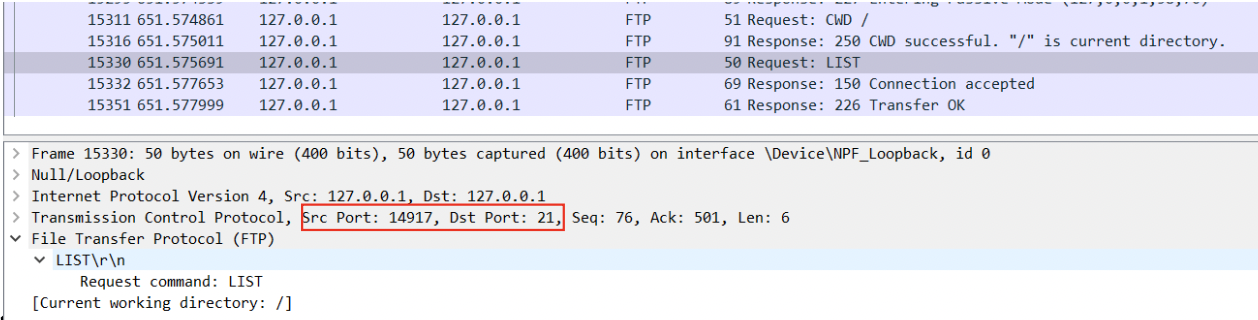
1. تفاوت ان که گواهی سایت گوگل معتبر است و از طرف GTS CA 1C3 صادر شده است.
2. الگوریتم رمزنگاری به‌کار رفته نیز ECC صادر شده است.
3. همچنین مدت اعتبار گواهی برخلاف سایت ما منقضی نشده است.



* **تنظیمات سرور FTP**

**سوال ۸) مشخص کنید چه دستوری برای لیست کردن فایل‌های دایرکتوری استفاده شده است. مشخص کنید چه نام کاربری برای دسترسی به سایت استفاده شده است. پروتکل لایه Transport استفاده شده برای این بسته‌ها چیست؟ آدرس پورت مبدا و مقصد را مشخص کنید.**

از دستور LIST برای گرفتن لیست فایل‌ها استفاده می‌شود. نام کاربری استفاده شده در اینجا test است (همانطوری که در تنظیمات FileZilla ایجادش کردیم و با ان لاگین کردیم)



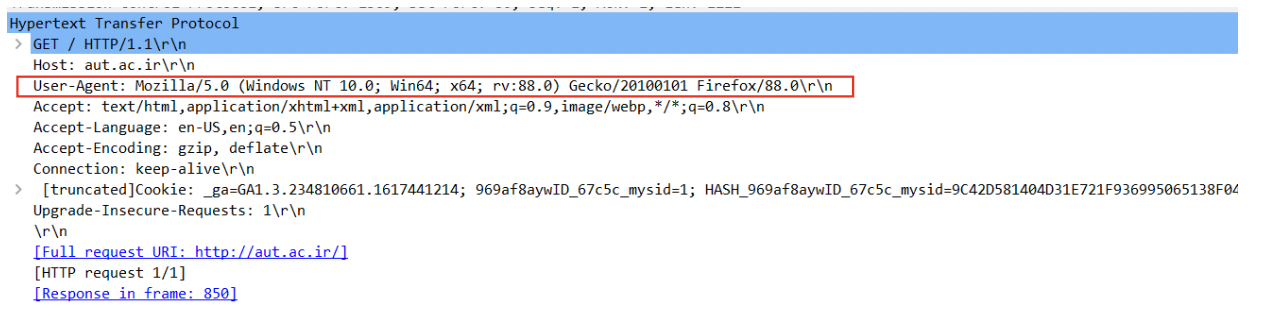
**سوال ۹) سعی کنید دوباره مرورگر را باز کنید. آیا می‌توانید به سایت وارد شوید؟**

طبق گفته مدرسین حذف شده.

* **پروتکل HTTPHار**

۱) شنود انجام و متوقف شد.

۲)



۳)

Connection = keep alive

درخواست از نوع get است.

User agent نبز در شکل مشخص شده است و بیانگر این موضوع است که درخواست از طریق firefox ارسال شده و نشان‌دهنده اطلاعات مبدا است.

۴)

