به نام ایزد یکتا

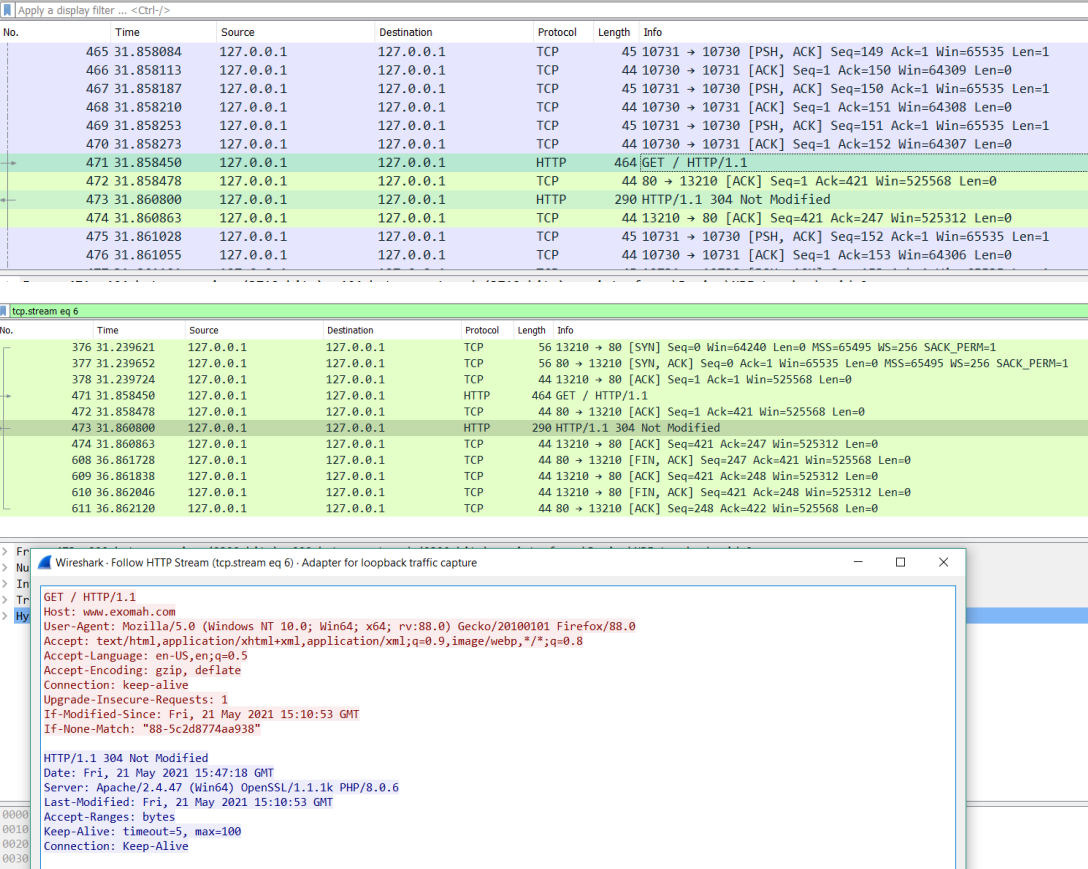
آزمایش سوم درس آزمایشگاه شبکه‌های کامپیوتری

­­

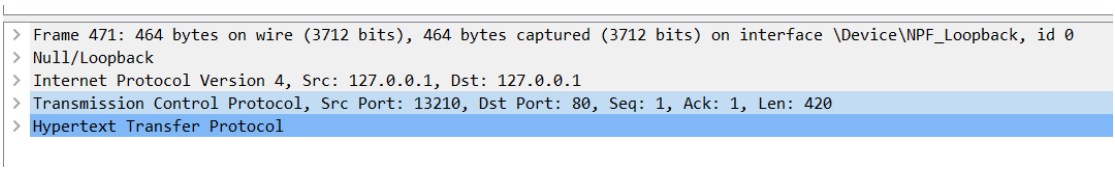
گروه دوم

تهیه کننده: بردیا اردکانیان

۹۸۳۱۰۷۲



سوال ۱)



شماره پورت مبدا: ۱۲۳۱۰

شماره پورت مقصد: ۸۰

در ابتدای برقراری اتصال http یک کانکشن tcp ایجاد می‌شود و پس از آن html base file از سرور درخواست و دریافت می‌شود و پس از آن با توجه به فایلhtml ، درخواستهایی برای دریافت آبجکت‌های وب فرستاده می‌شود. آدرس ip سایت درخواستی برای وب سرور فرستاده می‌شود و از این راه می‌تواند سایت درخواستی را تشخیص دهد.

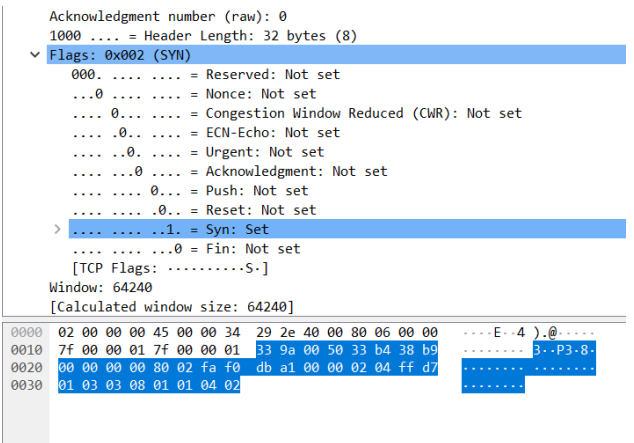
سوال ۲)



مقدار بخش keep alive: connection (یعنی ارتباط tcp بسته نشود این نوع ارتباط http از نوع پایا یا persistent می‌باشد)

درخواست از نوع GET است. مقدار UA که در شکل نیز مشخص شده است بیانگر مشخصات مرورگر مبدا است.

سوال ۳)



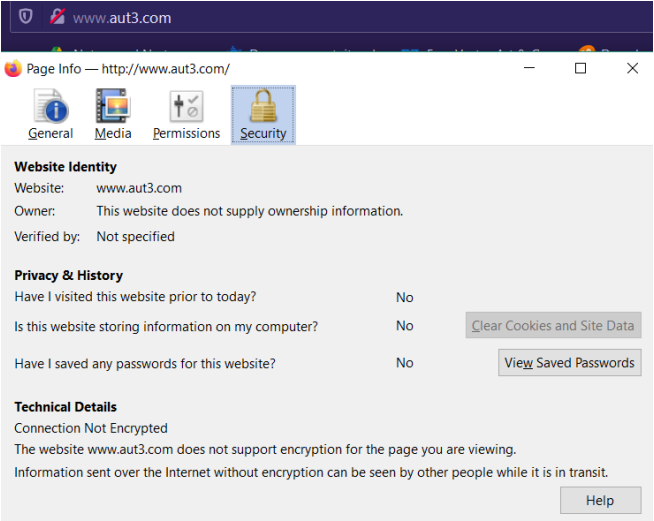
مقدار flagهایی که در اولین بستهی پروتکل TCP ست شدهاند در تصویر باال قابل مشاهده است.

سوال ۴)

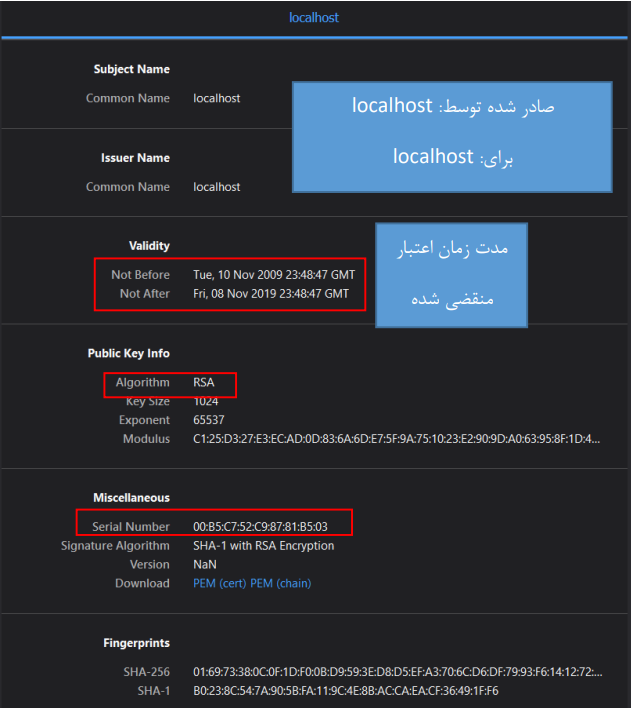


این بار از ادرس aut3.comاستفاده کردیم. همانطوری که مشاهده میکنید آدرس پورت مبدا متفاوت است تا بتوان بستههای مربوط به آنها را از هم جدا کرد. طول بستههای آنها نیز متفاوت است. پارامترهای acknowledge number و sequence number هر دو که به صورت raw تنظیم شدهاست هم متفاوت است.

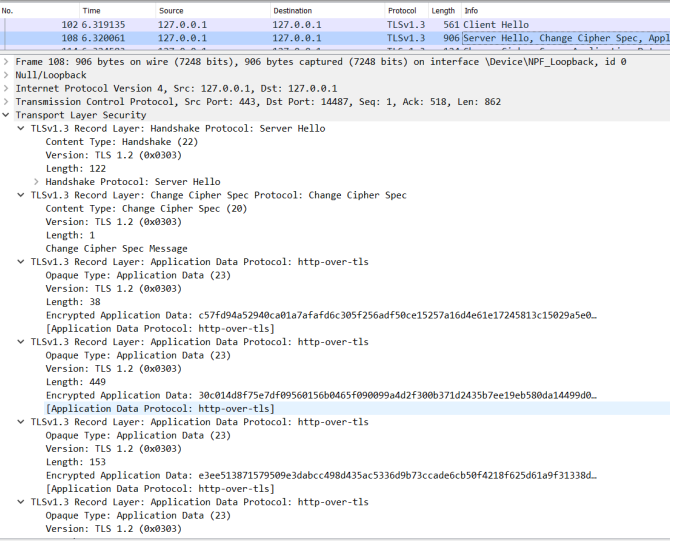
سوال ۵)



حالا برای کانکشن https برای همین دامنه، اطالعات مربوط به certificate:



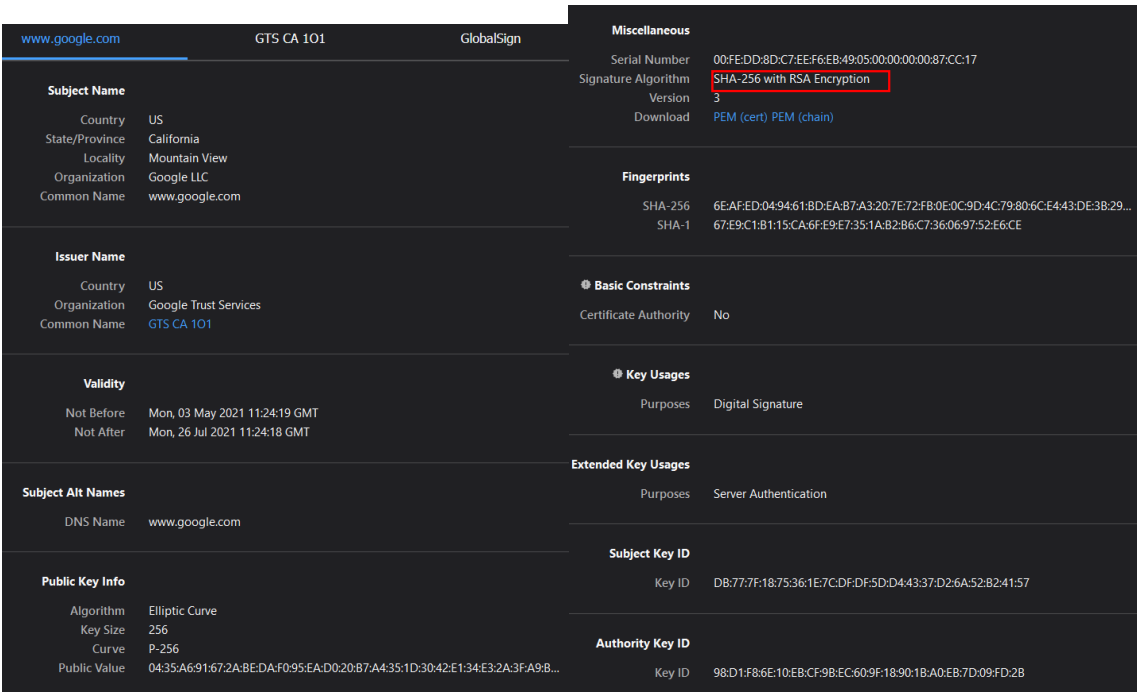
سوال ۶)

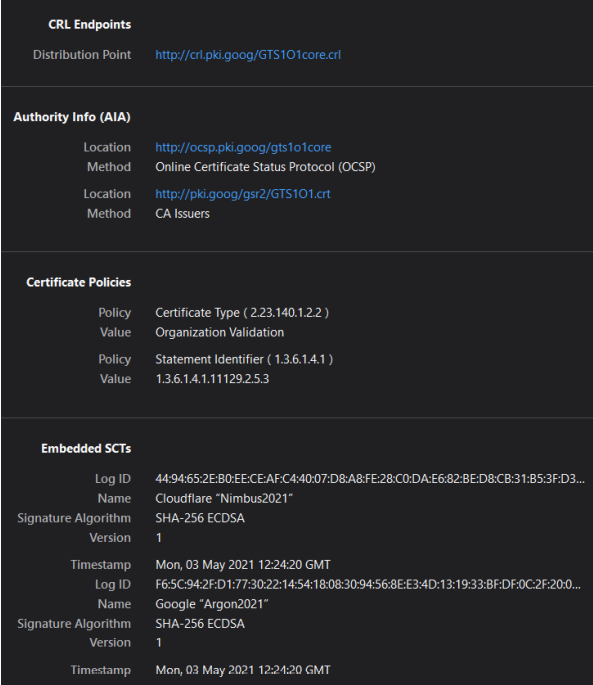


خیر. از آنجایی که از پروتکل tls استفاده شده است، متن این ارتباط قابل خواندن نیست. پروتکل tls وظیفهی رمزگذاری encryptionارتباط بین سرور و کالینت را به عهده دارد.

سوال ۷)

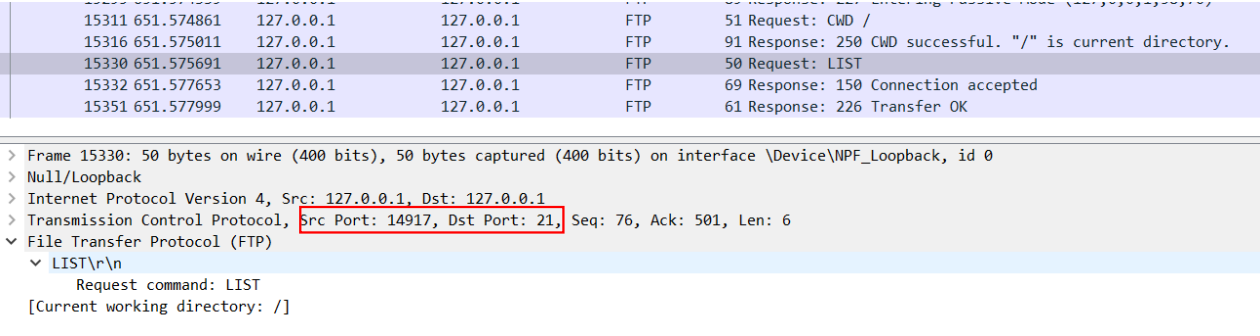
نتایج مشاهدهی certificate سایت گوگل:

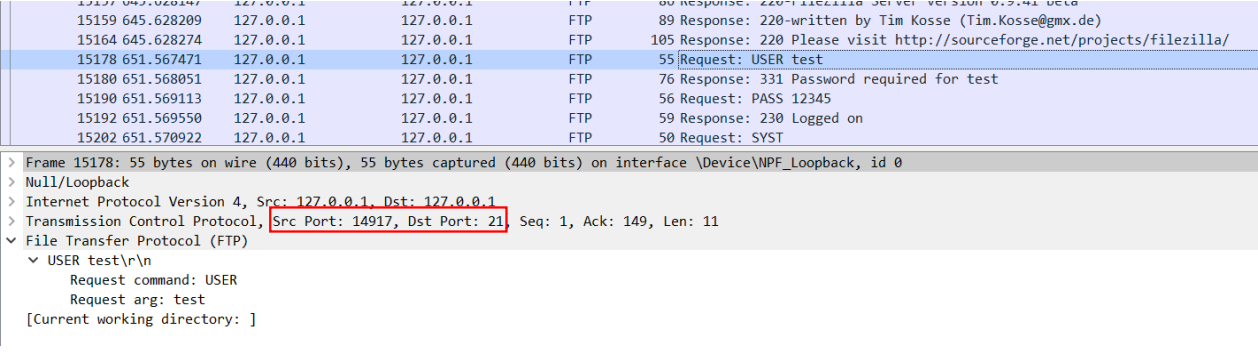




این مدرک، اطالعات بیشتری را شامل میشود. به عنوان اولین تفاوت می‌توان به تفاوت صادر کننده و دریافت‌کننده مدرک اشاره کرد و اینکه مدرک گوگل منقضی نشده است و تا تاریخ 26 جوالی 2021 اعتبار دارد. الگوریتم به کار رفته برای امضا نیز متفاوت می‌باشد.

سوال ۸)

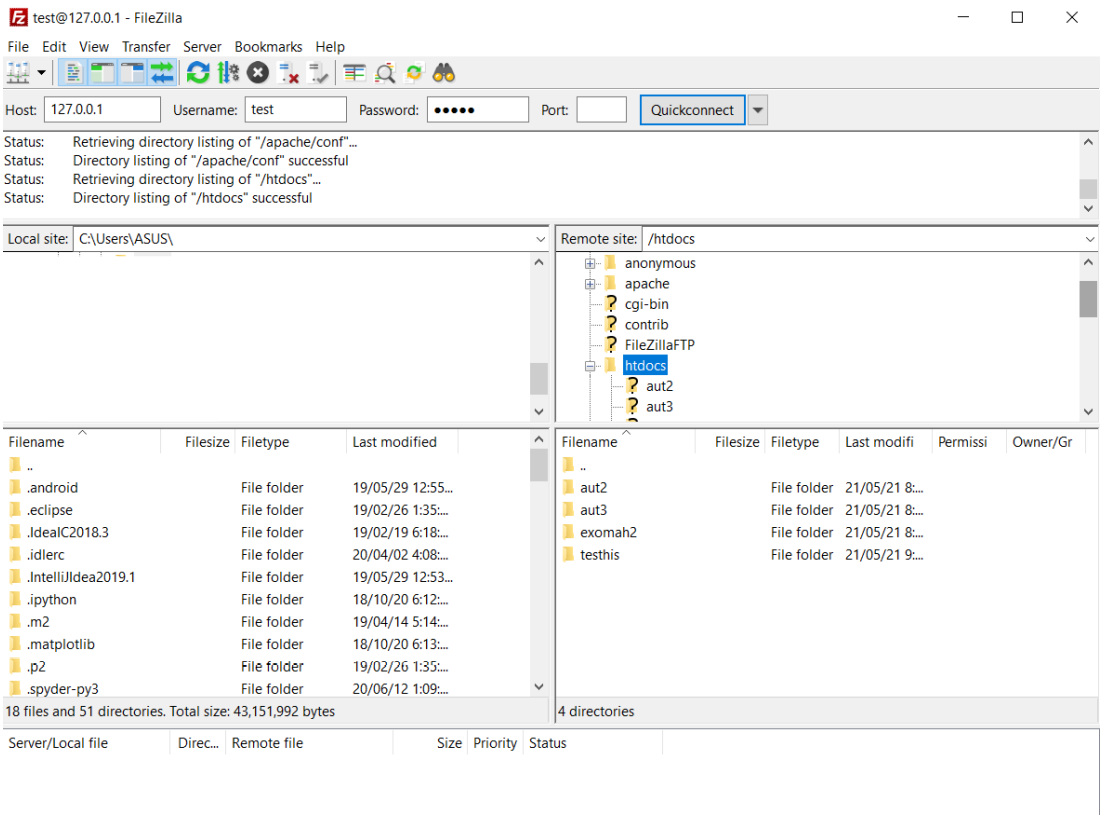


از دستور LIST برای گرفتن لیست فایلها استفاده میشود. نام کاربری استفاده شده در اینجا test است (همانطوری که در تنظیمات FileZilla ایجادش کردیم و با آن الگین کردیم) 

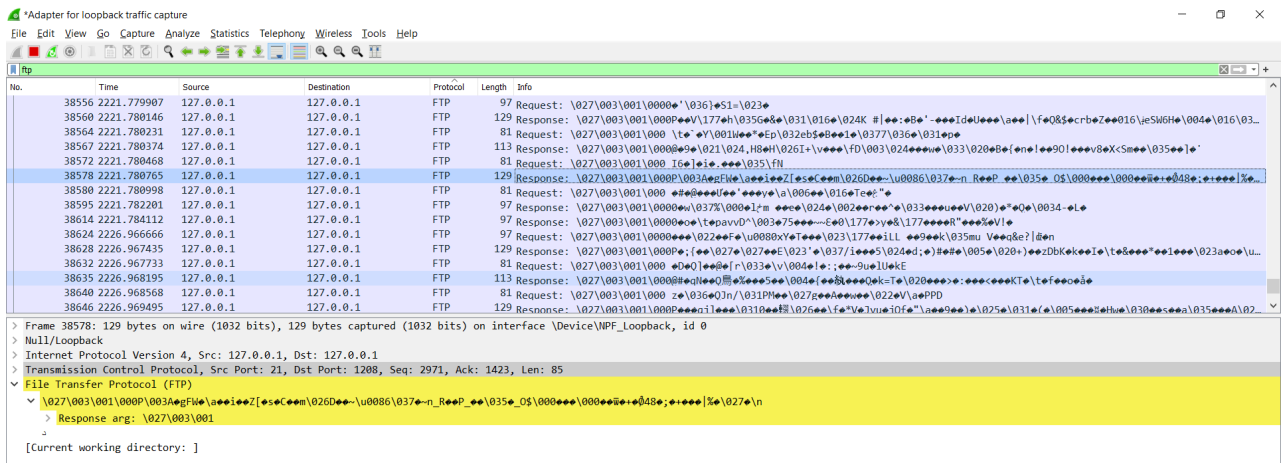
در این ارتباطات ار پروتکل TCP استفاده شده است، با شماره پورت مبدا 14917 و مقصد 21 که در تصاویر باال نیز مشخص شده است.

سوال ۹)

این بار دیگر سایت باز نمی‌شود و مرورگر پیام میدهد که برای اتصال باید از اپلیکیشن دیگری استفاده کنیم که در اینجا ما از FileZilla استفاده می‌کنیم.

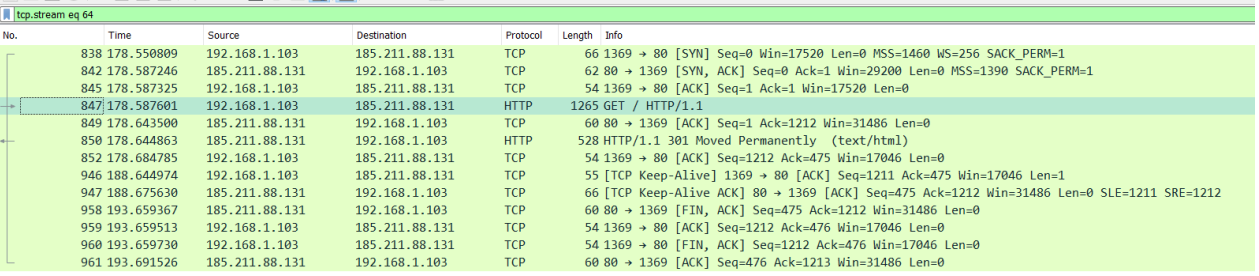


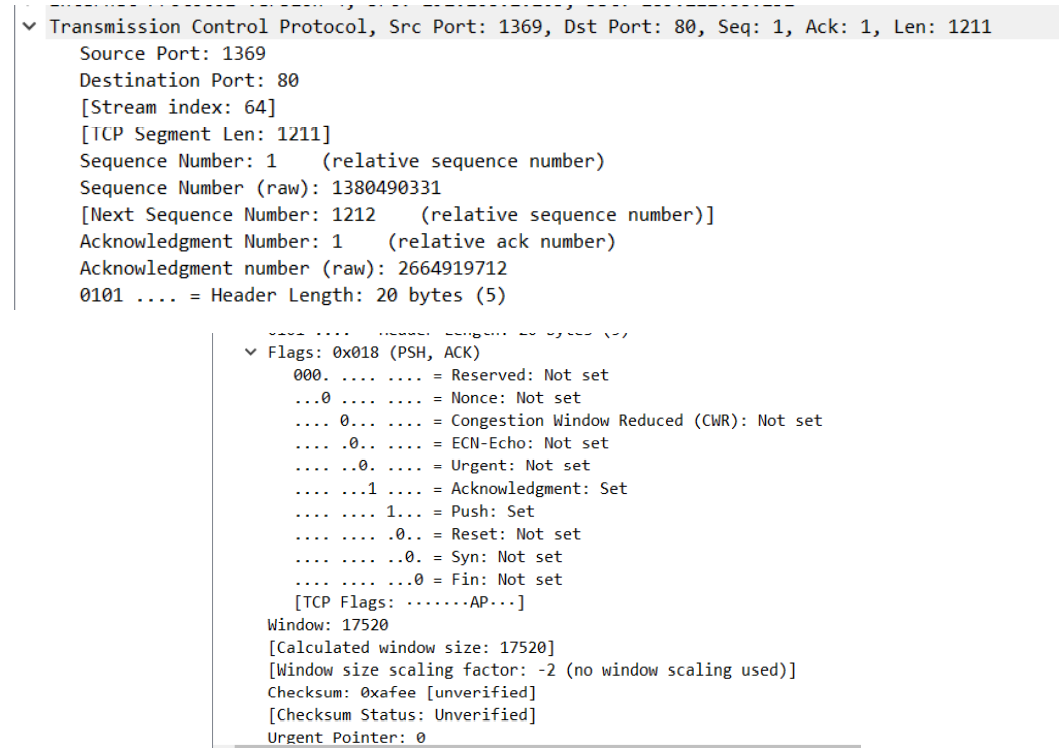
اگر بسته‌های مربوط به این ارتباطات را از وایرشارک شنود کنیم، نمیتوانیم هیچ اطالعاتی را از آن بخوانیم.



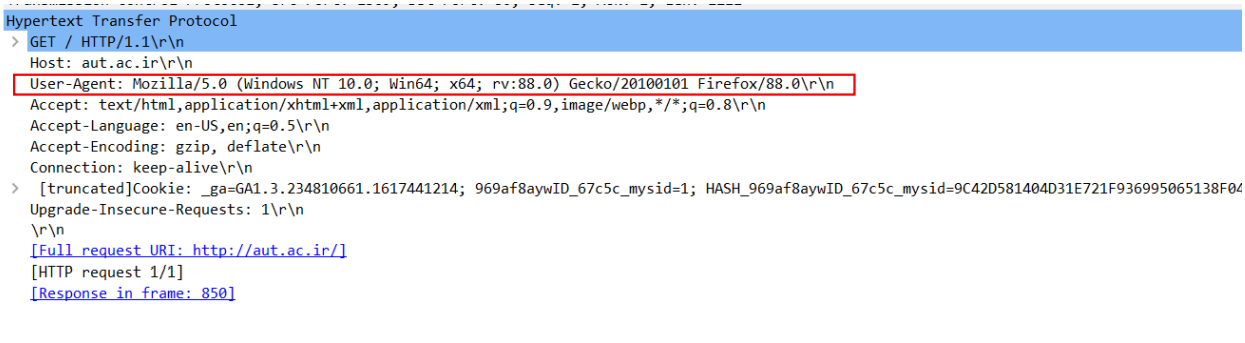
پروتوکل HTTP:

در اینجا، بسته‌های مربوط به follow HTTP Stream را مشاهده می‌کنیم.



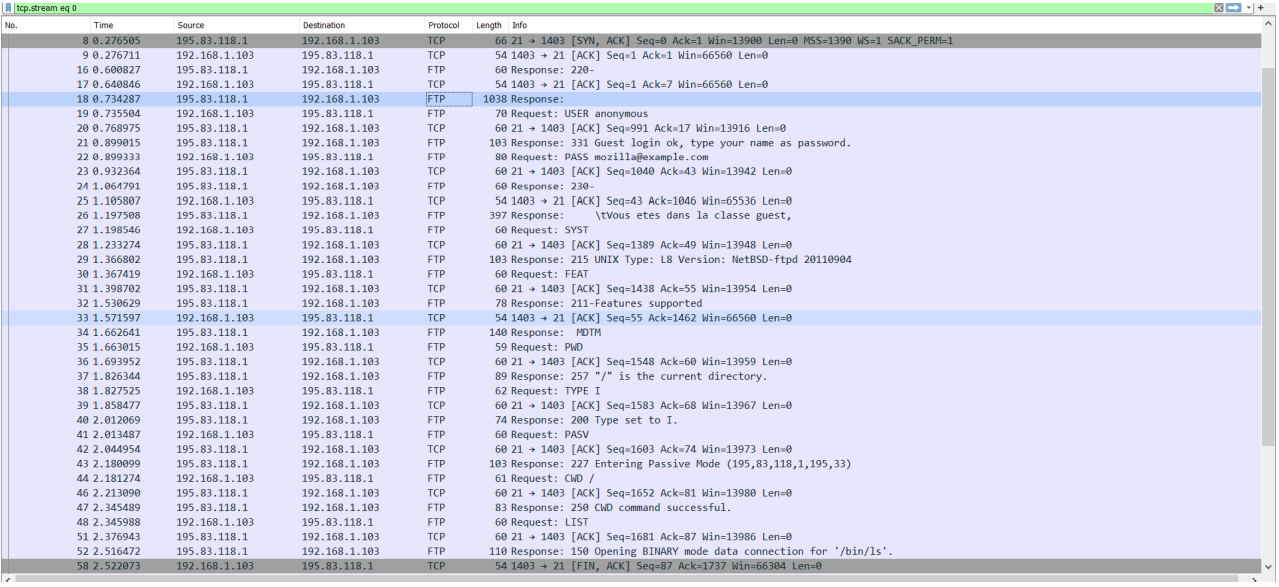
اطلاعات مربوط به پروتکل tcp و فلگ‌ها: (در این کانکشن از این پروتکل لایه انتقال استفاده می‌شود(

اطالعات مربوط به پروتکل http:

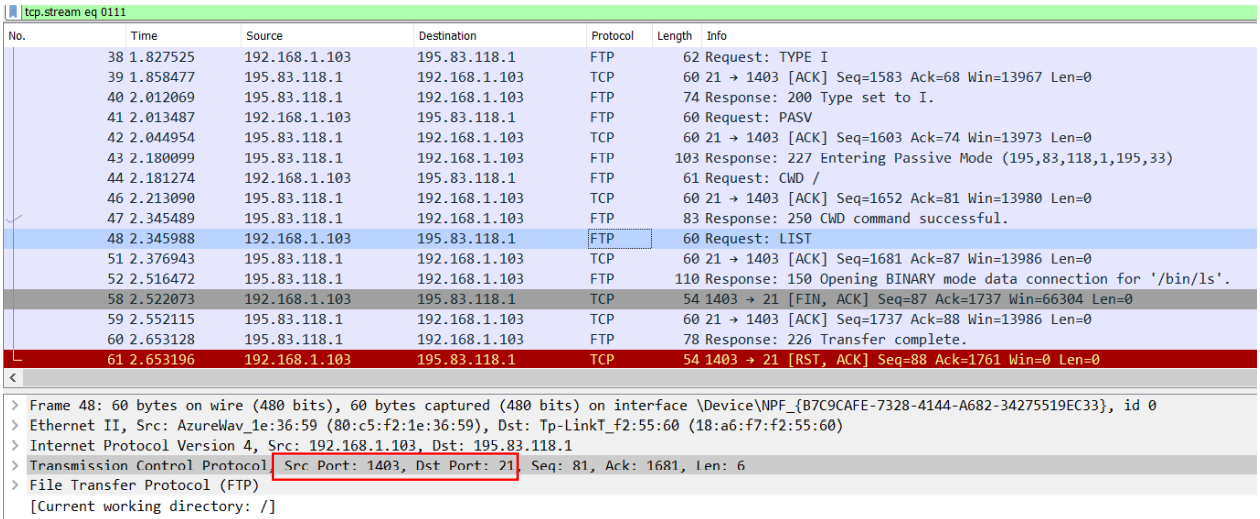


همانطور که مشاهده می‌شود، اتصال از نوع keep-aliveاست که کانکشن tcp باز بماند. نوع پروتکل نیز get است. مقدار UA در تصویر مشخص شده است که نشان دهندهی اطالعات مرورگر مبدا است.

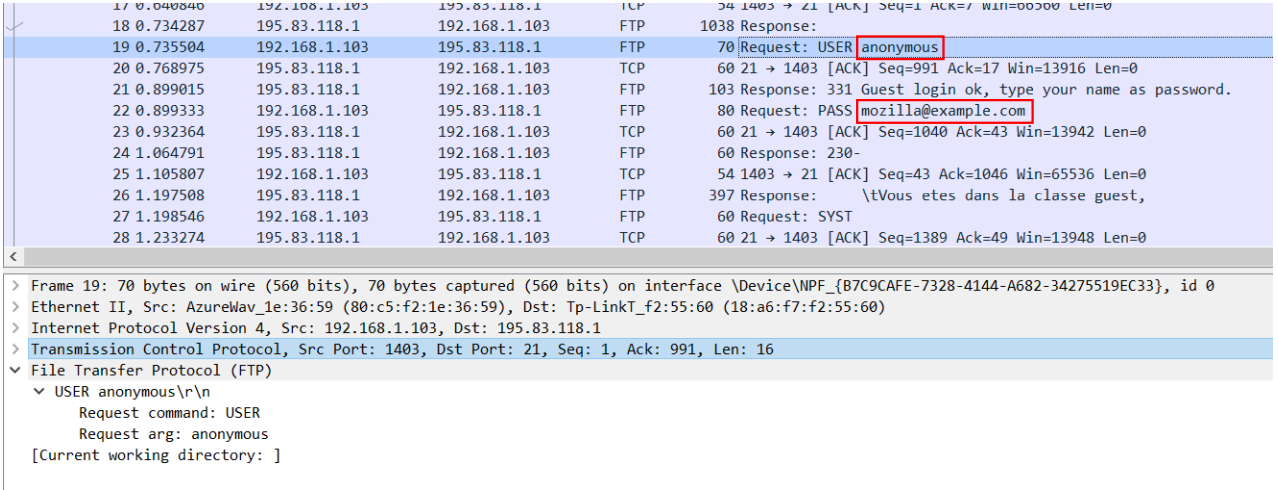
پروتکل FTP: در اینجا بسته‌های مربوط به follow HTTP Streamرا مشاده می‌کنیم.



پروتکل استفاده شده در این اتصال، پروتکل TCP است. پورت مقصد 21 و پورت مبدا 1403 است.



مقدار یوزنیم و پسوورد به ترتیب anonymous و com.exmaple@mozilla می‌باشد که در تصویر بعدی نیز مشخص شده است:



اگر روی این بسته‌ها کلیک کنیم نیز همین مقادیر را به عنوان نام کاربری و رمز عبور مشاهده خواهیم کرد.