به نام خدا

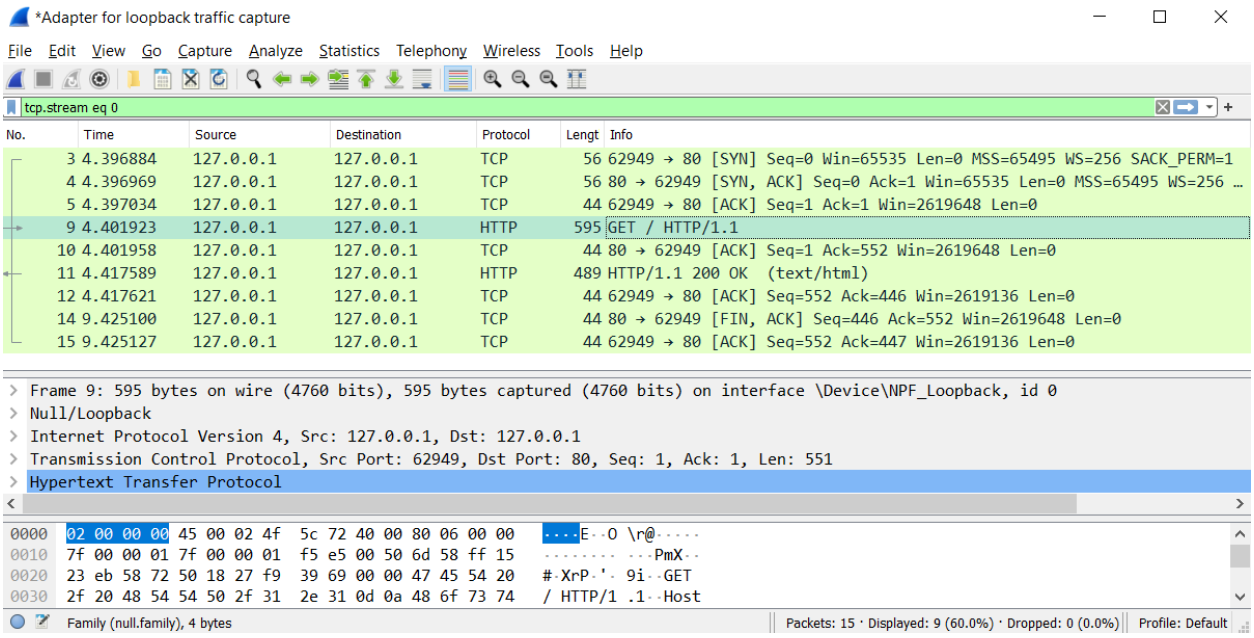
محمدمهدی هجرتی	۹۷۲۳۱۰۰
آزمایشگاه شبکه - آزمایش چهارم	راه اندازی سرویس های Web و FTP
استاد نقی زاده	۳۰ فروردین ۱۴۰۰

سوال ۱

آدرس پورت مبدا ۸۰ و پورت مقصد ۶۲۹۴۹ می باشد.

برای برقراری ارتباط، ابتدا یک Tcp handshake شکل می گیرد. سپس در صورت موفقیت آمیز بودن، به ترتیب آبجکت های صفحه ی مورد نظر برای کلاینت فرستاده می شود.

در اینجا چون سرور بر روی سیستم خودمان اجرا شده است، با مراجعه به hosts آدرس سایت را تشخیص می دهد.



سوال ۲

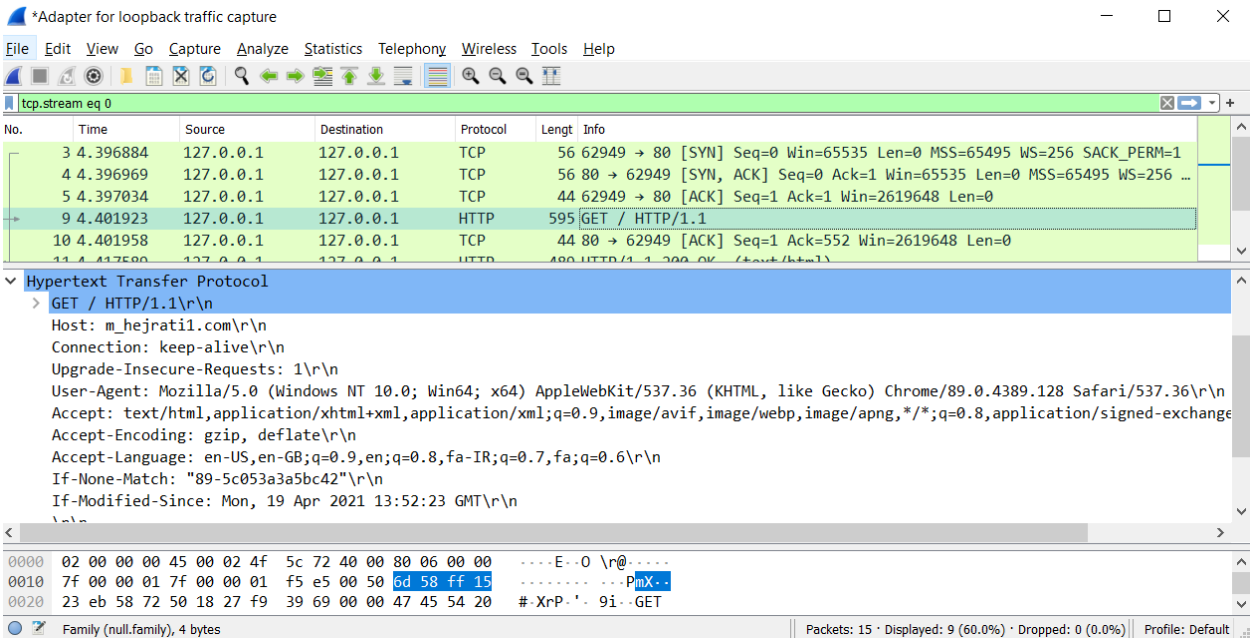
مقدار connection، keep-alive می باشد.

نوع درخواست GET می باشد.

مقدار user-agent، به صورت زیر می باشد.

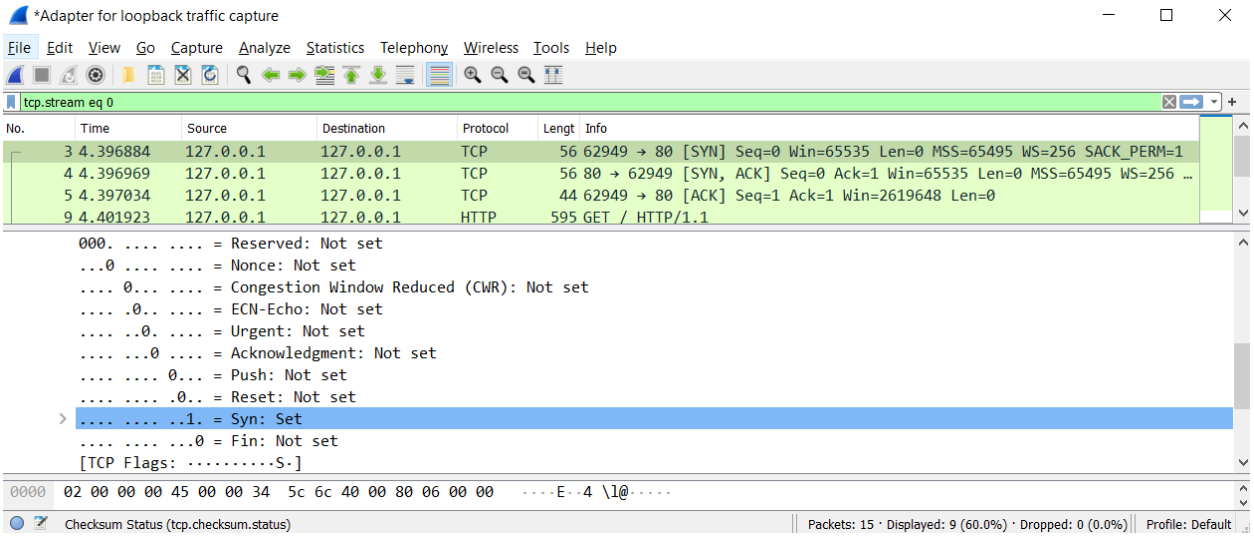
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/89.0.4389.128 Safari/537.36\r\n

این مقدار بیانگر، مشخصات سیستم عامل، مرورگر و ... مربوط به کلاینت درخواست دهنده می باشد.



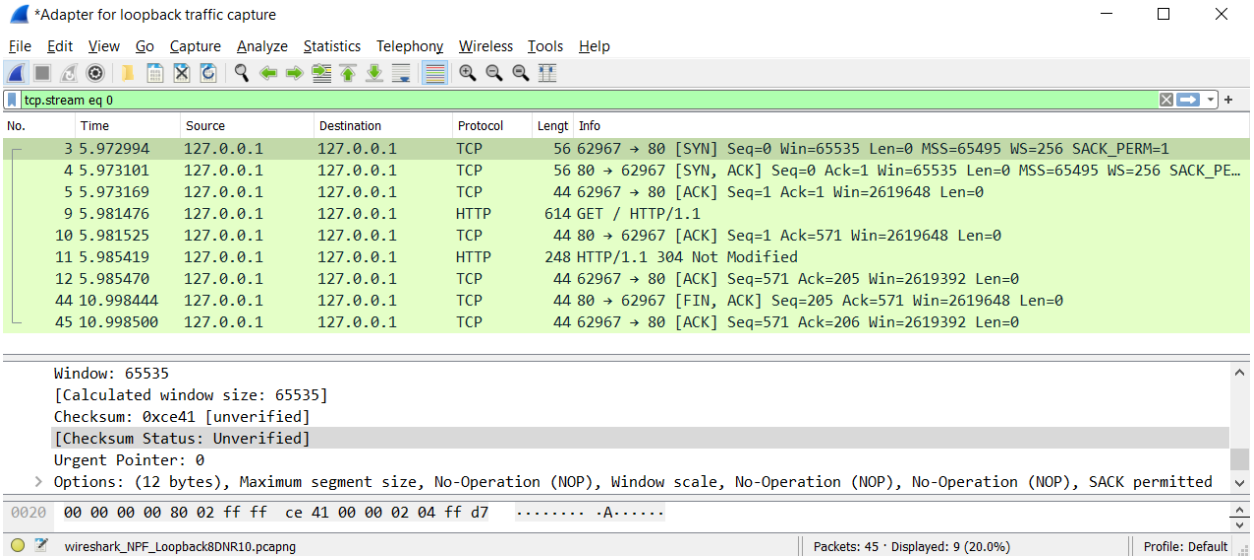
سوال ۳

اعداد تنظیم شده برای فلگ های این بسته در شکل زیر نشان داده شده است.



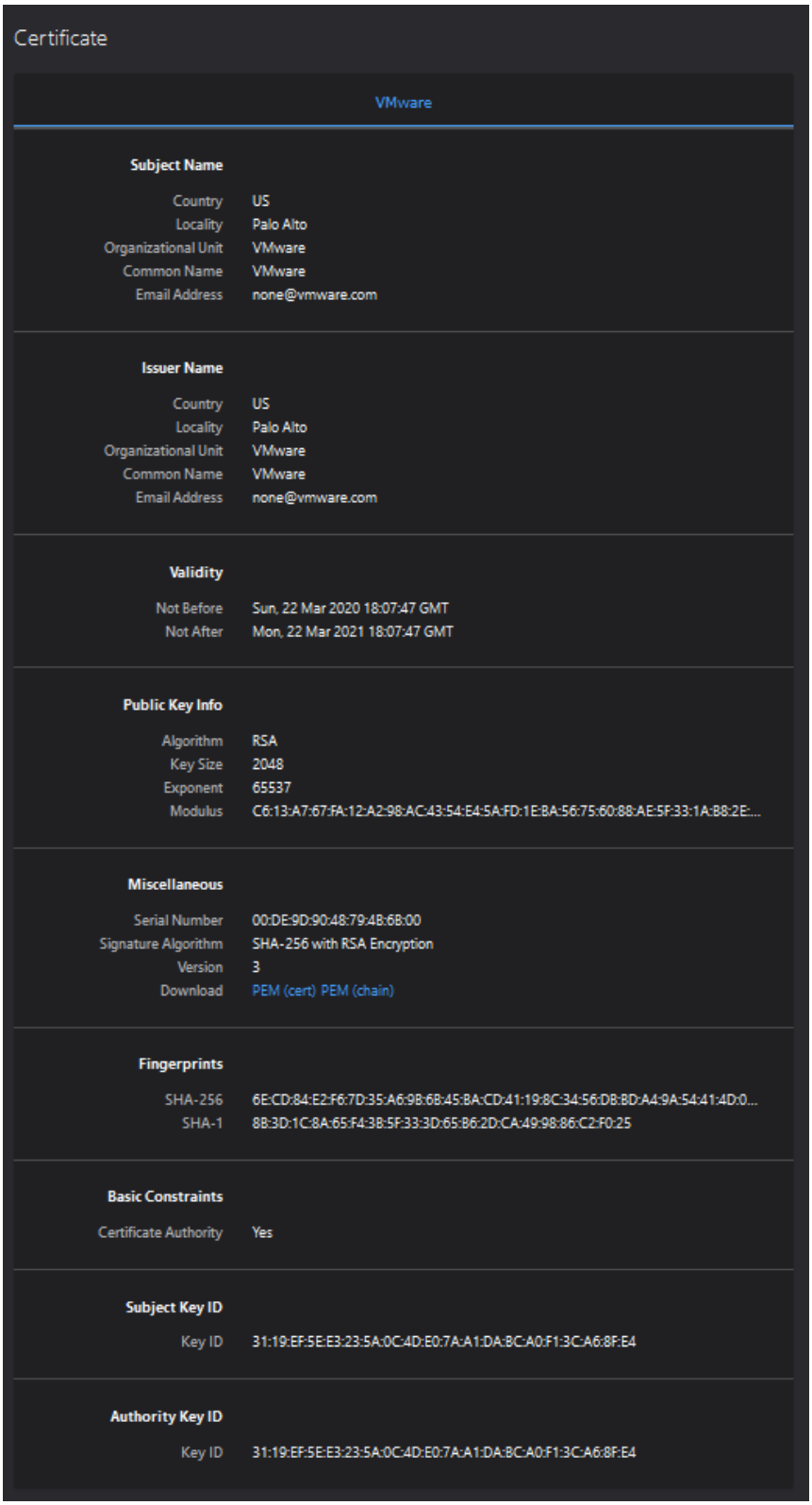
سوال ۴

تفاوت بسته های دو سایت، در نام هاست و پورت مقصد می باشد.



سوال ۵

تصویر گواهی در زیر آورده شده است.


Certificate

VMware

Subject Name

Country	US
Locality	Palo Alto
Organizational Unit	VMware
Common Name	VMware
Email Address	none@vmware.com

Issuer Name

Country	US
Locality	Palo Alto
Organizational Unit	VMware
Common Name	VMware
Email Address	none@vmware.com

Validity

Not Before	Sun, 22 Mar 2020 18:07:47 GMT
Not After	Mon, 22 Mar 2021 18:07:47 GMT

Public Key Info

Algorithm	RSA
Key Size	2048
Exponent	65537
Modulus	C6:13:A7:67:FA:12:A2:98:AC:43:54:E4:5A:FD:1E:BA:56:75:60:88:AE:5F:33:1A:B8:2E:...

Miscellaneous

Serial Number	00:DE:9D:90:48:79:4B:6B:00
Signature Algorithm	SHA-256 with RSA Encryption
Version	3
Download	PEM (cert) PEM (chain)

Fingerprints

SHA-256	6E:CD:84:E2:F6:7D:35:A6:9B:6B:45:BA:CD:41:19:8C:34:56:DB:BD:A4:9A:54:41:4D:0...
SHA-1	8B:3D:1C:8A:65:F4:3B:5F:33:3D:65:B6:2D:CA:49:98:86:C2:F0:25

Basic Constraints

Certificate Authority	Yes

Subject Key ID

Key ID	31:19:EF:5E:E3:23:5A:0C:4D:E0:7A:A1:DA:BC:A0:F1:3C:A6:8F:E4

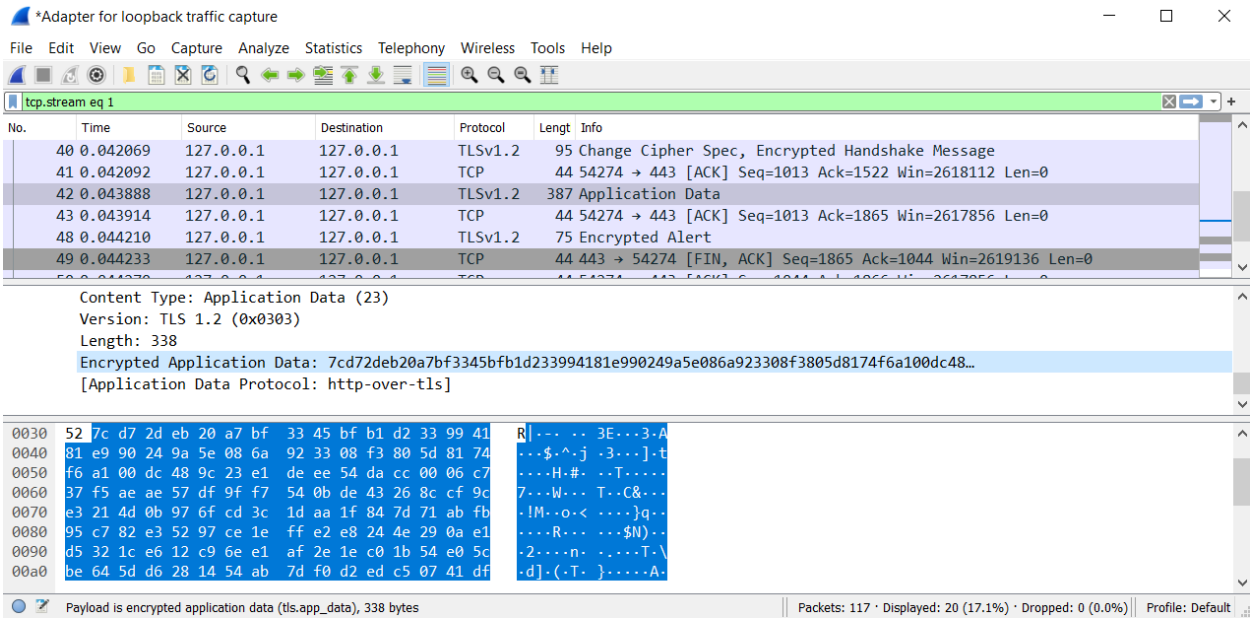
Authority Key ID

Key ID	31:19:EF:5E:E3:23:5A:0C:4D:E0:7A:A1:DA:BC:A0:F1:3C:A6:8F:E4

گواهی را دستگاه VMware برای خودش صادر کرده است.
اعتبار گواهی تا تاریخ ۲۲ مارس ۲۰۲۱ می باشد.
کلید عمومی از الگوریتم RSA استفاده می کند و سایز آن ۲۰۴۸ می باشد.
امضای دیجیتال از الگوریتم SHA-256 با رمزگذاری RSA انجام شده است.

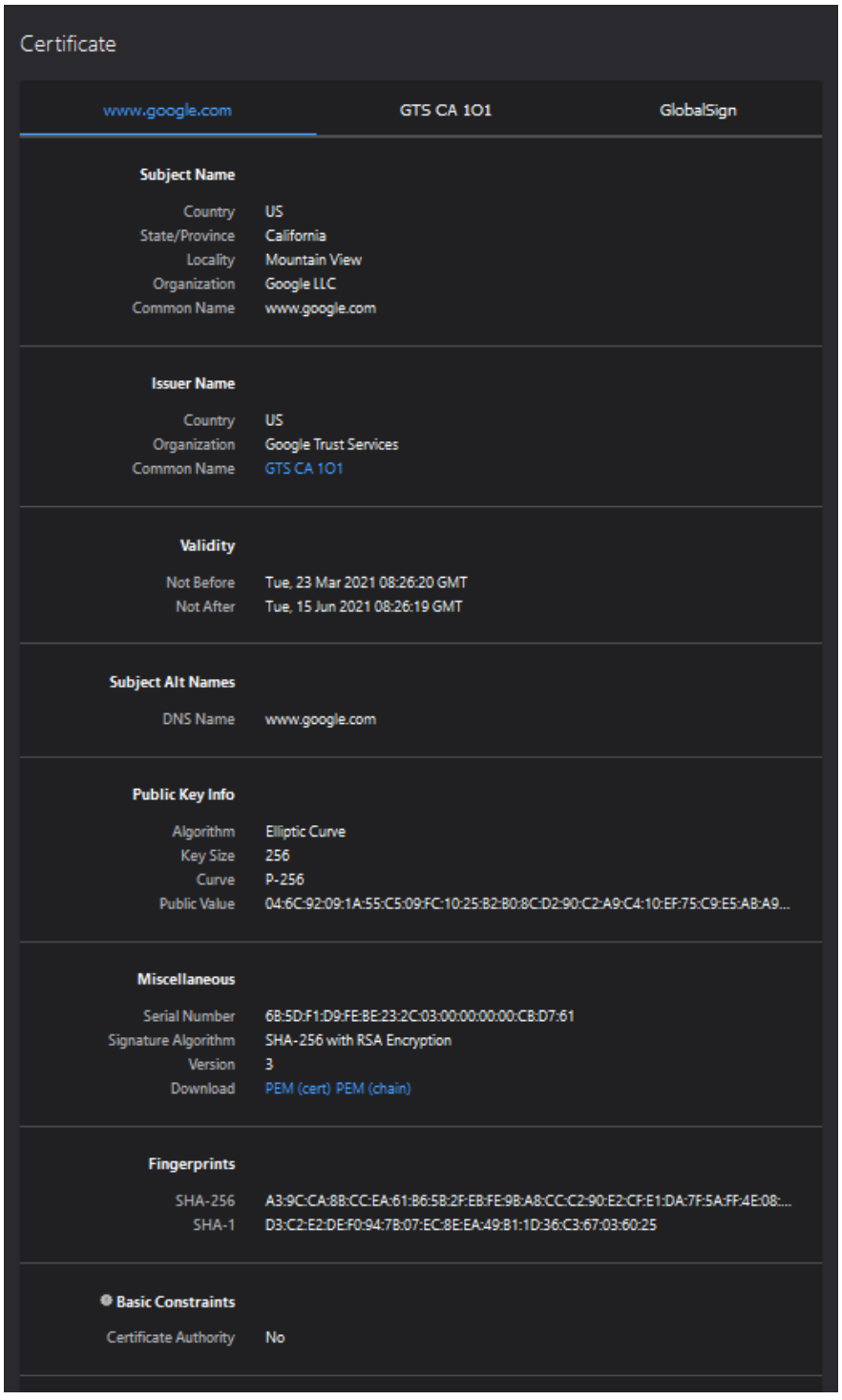
سوال ۶

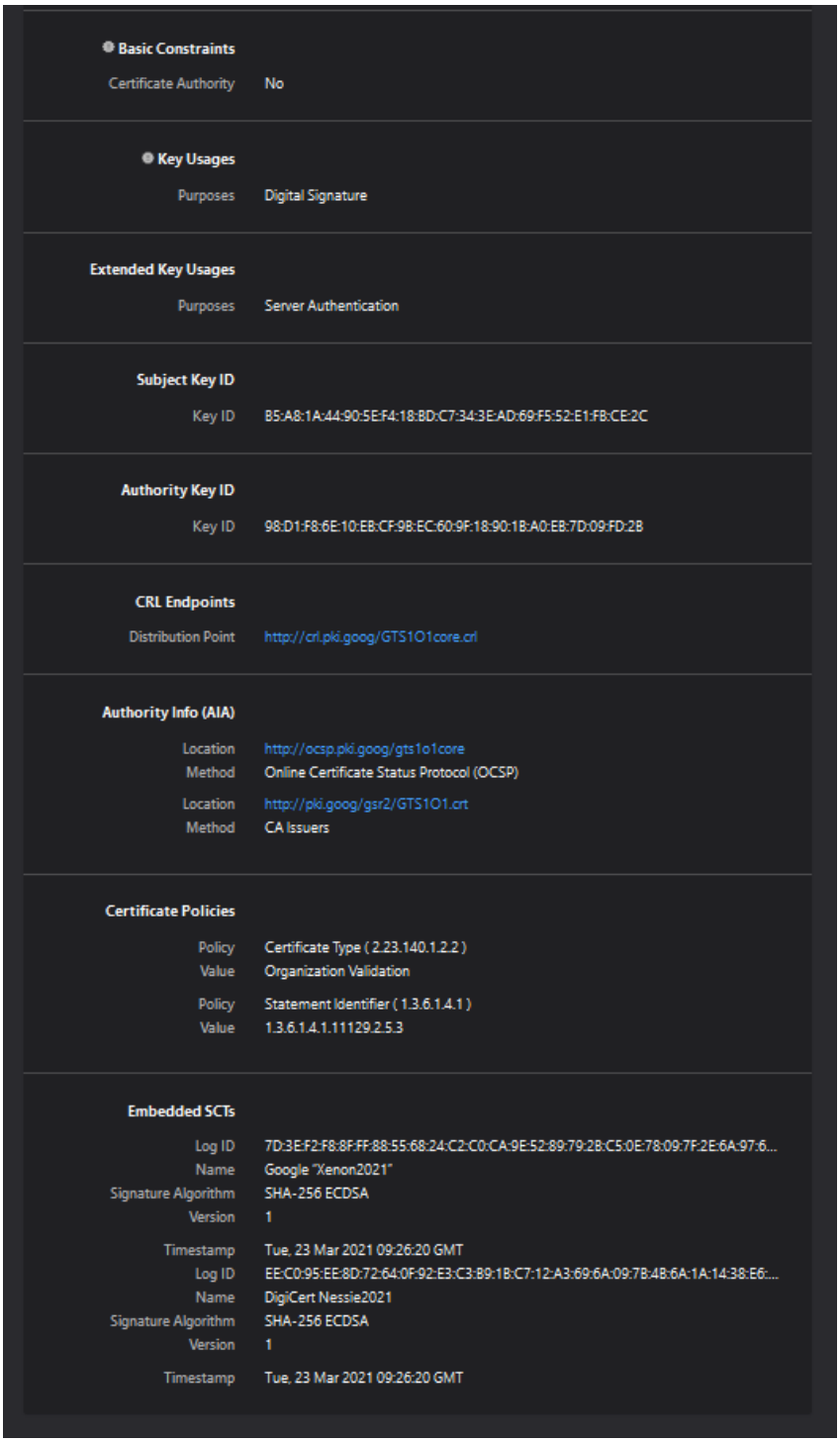
خیر. چون داده ها به صورت رمزگذاری شده منتقل می شوند، امکان خواندن آن ها وجود ندارد. در واقع متن پیام، بی معنی به نظر می رسند.



سوال ۷

تصویر گواهی گوگل در زیر آورده شده است.

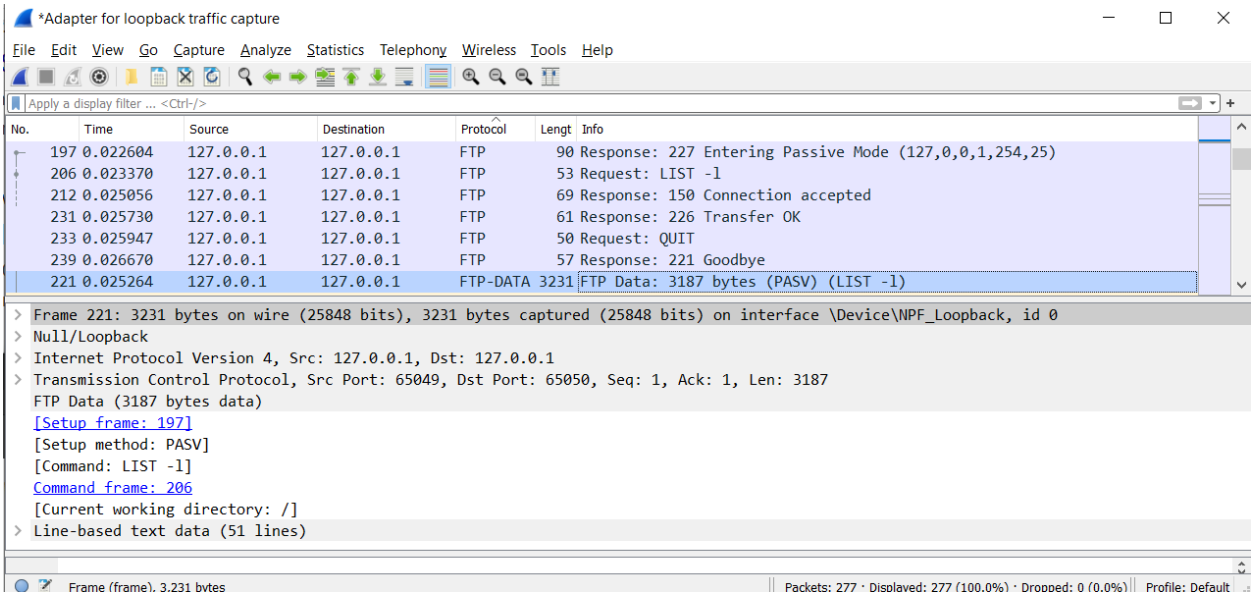




تفاوت های زیادی وجود دارد. از جمله تاریخ اعتبار، صادر کننده ی گواهی، کلید و نوع رمزنگاری و ...

سوال ۸

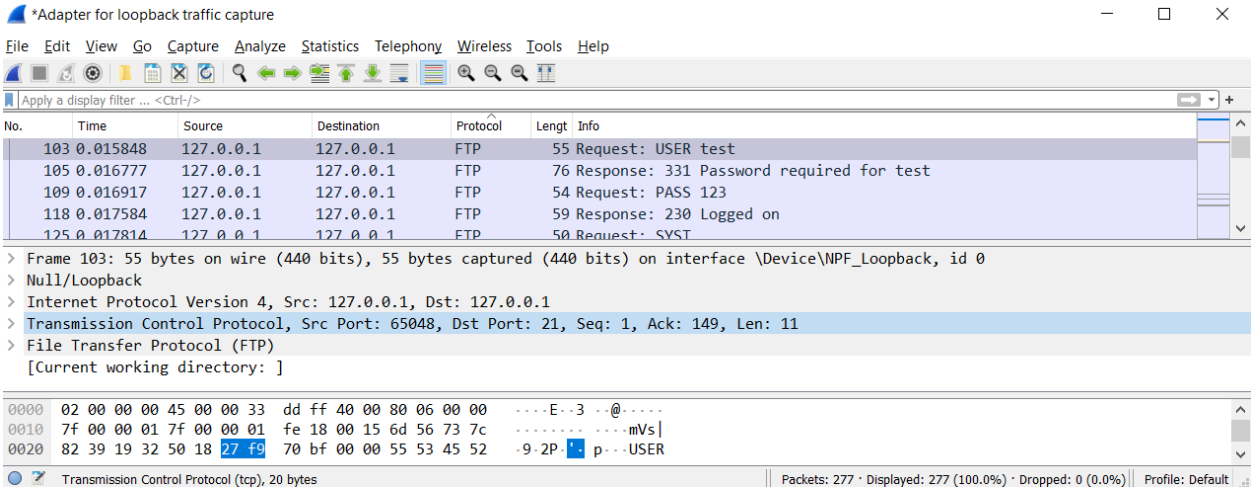
با دستور l- list فایل های درون دایرکتوری لیست شده اند.



همان طور که در تصویر زیر مشخص است کاربر از یوزر test و رمز 123 استفاده کرده است.

پروتکل لایه ترنسپورت TCP می باشد.

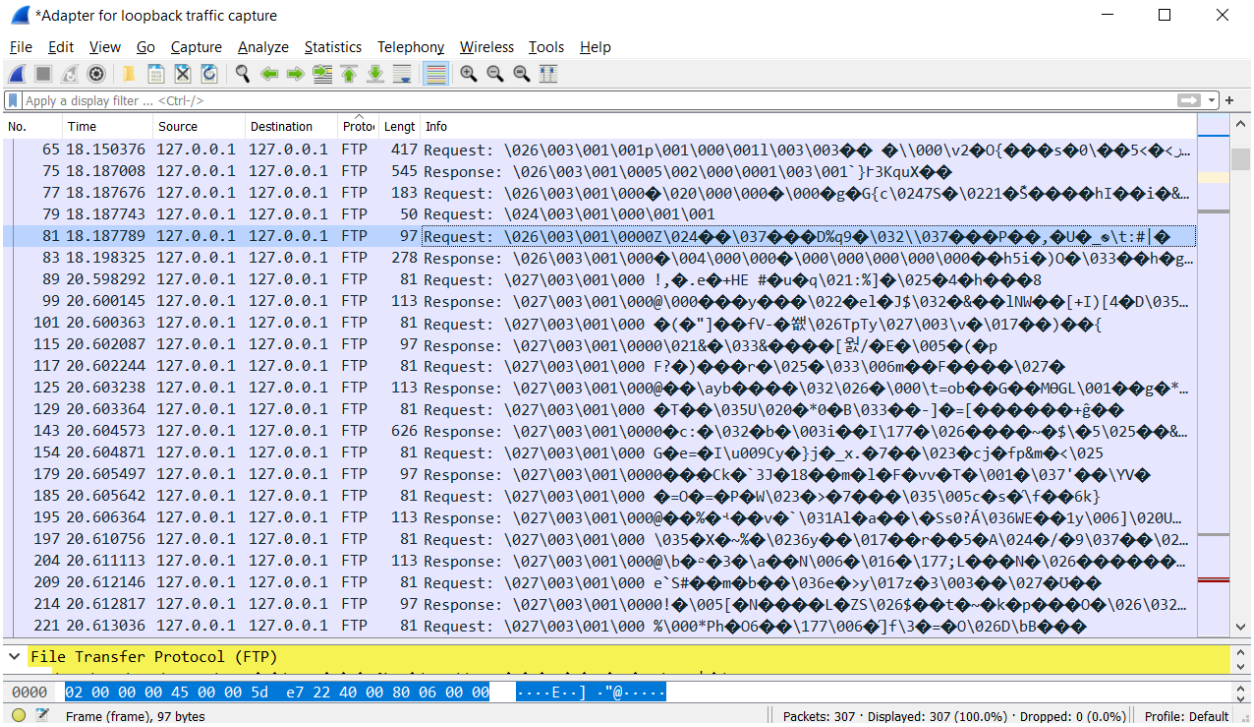
پورت مبدا ۶۵۰۴۸ و پورت مقصد ۲۱ می باشد.



سوال ۹

بعد از فعال کردن SSL، امکان برقراری ارتباط از طریق مرورگر وجود ندارد.

با استفاده از نرم افزار FileZilla دوباره ارتباط را متصل کردیم. که چون داده ها رمزگذاری شده اند، پس قابل خواندن نیستند.



بخش پروتکل HTTP

با توجه به اینکه وبسایت اصلی دانشگاه از پروتکل https استفاده می کند. پس به سایت pbo.aut.ac.ir درخواست دادیم تا بتوان بسته های http را مشاهده کرد.

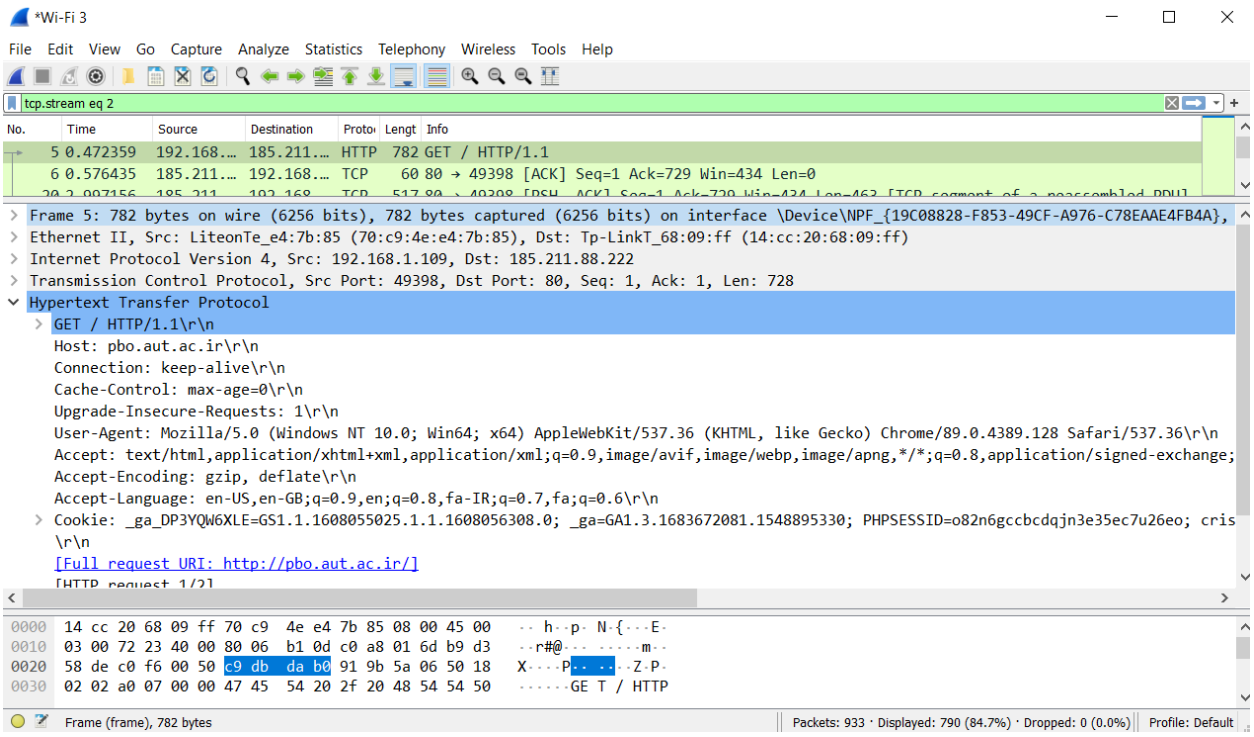
مقدار connection، keep-alive می باشد.

درخواست از نوع GET است.

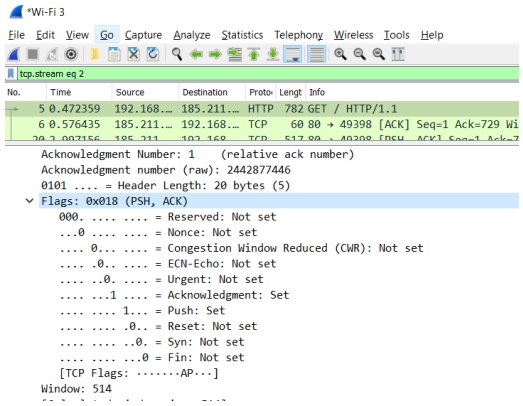
مقدار user-agent، به صورت زیر می باشد.

User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/89.0.4389.128 Safari/537.36\r\n

این مقدار بیانگر، مشخصات سیستم عامل، مرورگر و ... مربوط به کلاینت درخواست دهنده می باشد.



مقدار فلگ های مربوطه را در تصویر زیر می بینیم.



بخش پروتکل FTP

پروتکل لایه ی ترنسپورت در این بسته ها TCP می باشد.

پورت مبدا ۴۹۵۰۲ و پورت مقصد ۲۱ است.

مقدار username به صورت anonymous مشخص شده است.

مقدار password ثبت شده، chrome@example.com می باشد.