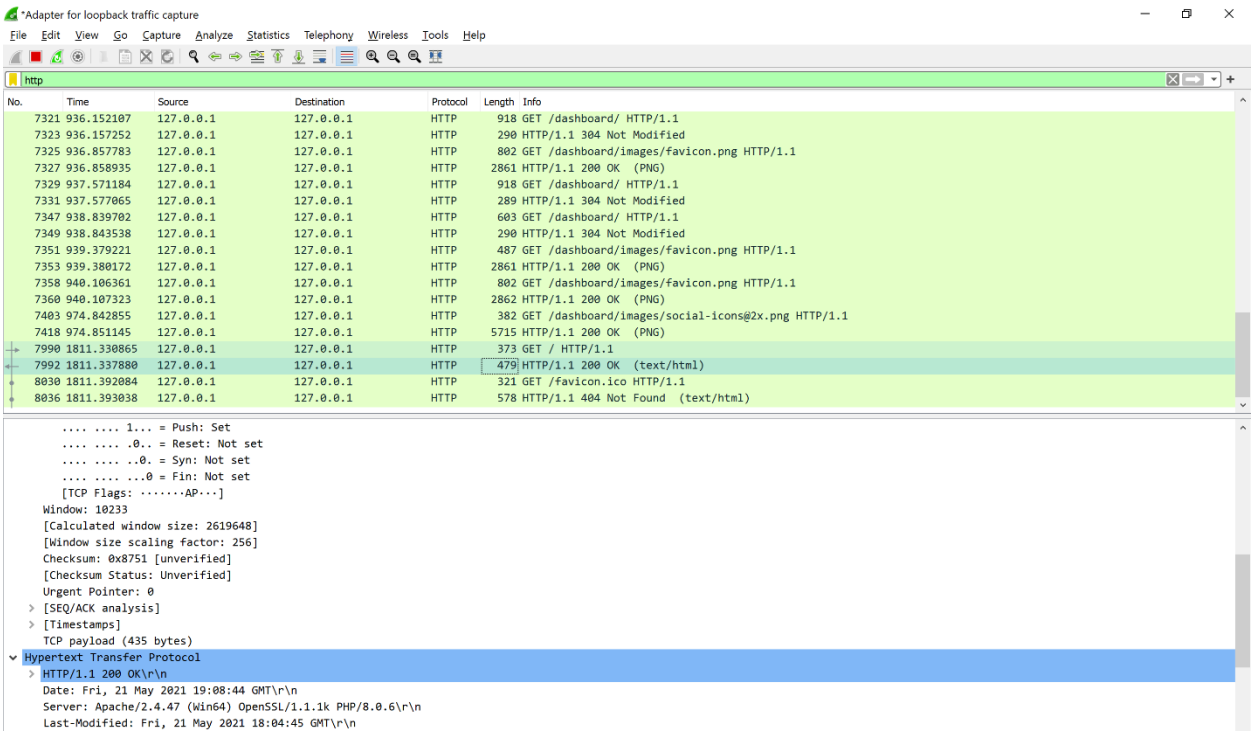
امیرمحمد راعی ۹۷۳۱۰۸۳

1

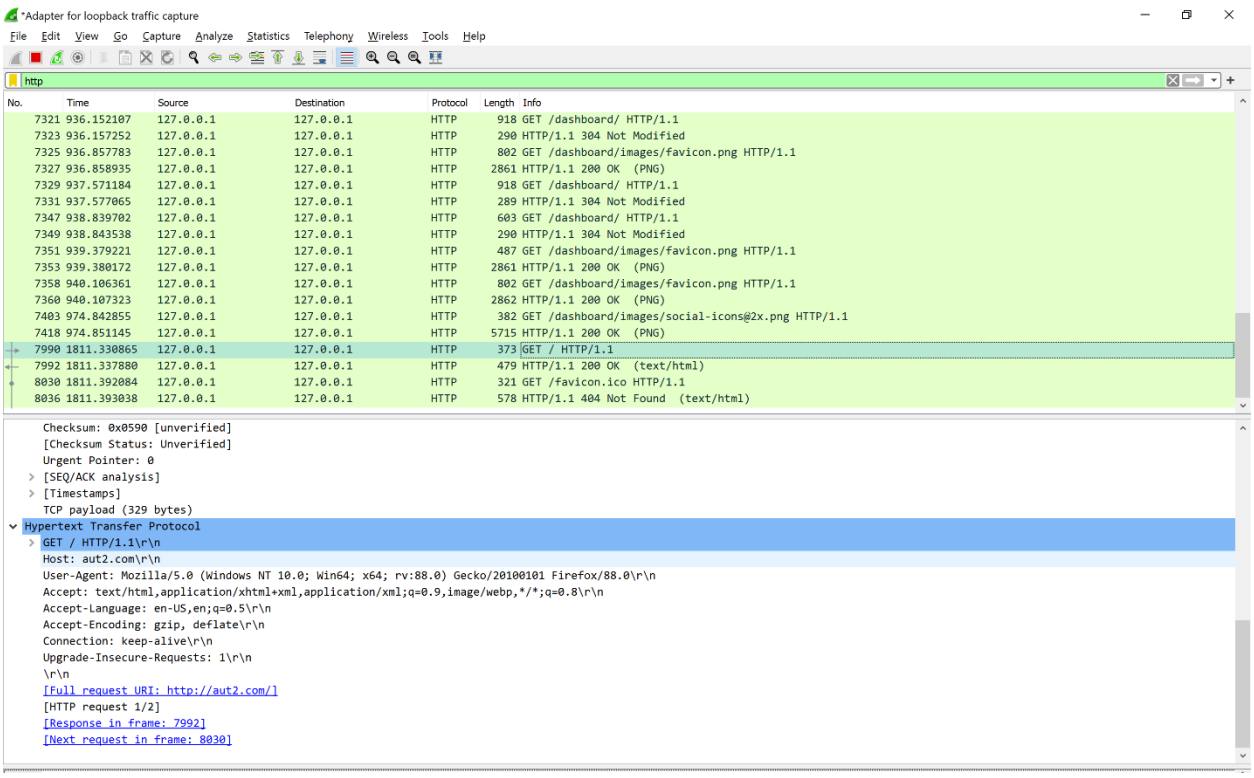


بر اساس تصویر پورت مبدا ۸۰ و پورت مقصد 54211

برای انکه ارتباط برقرار شود نیاز است tcp handshake به وجود اید. حال اگر این عملیات با موفقیت انجام شد موارد مورد نیاز برای کاربر و client فرستاده می‌شود

Clientبه وسیله فایل host که در ان ما ip web service را به ان اختصاص داده ایم ادرس را شناسایی می کند.

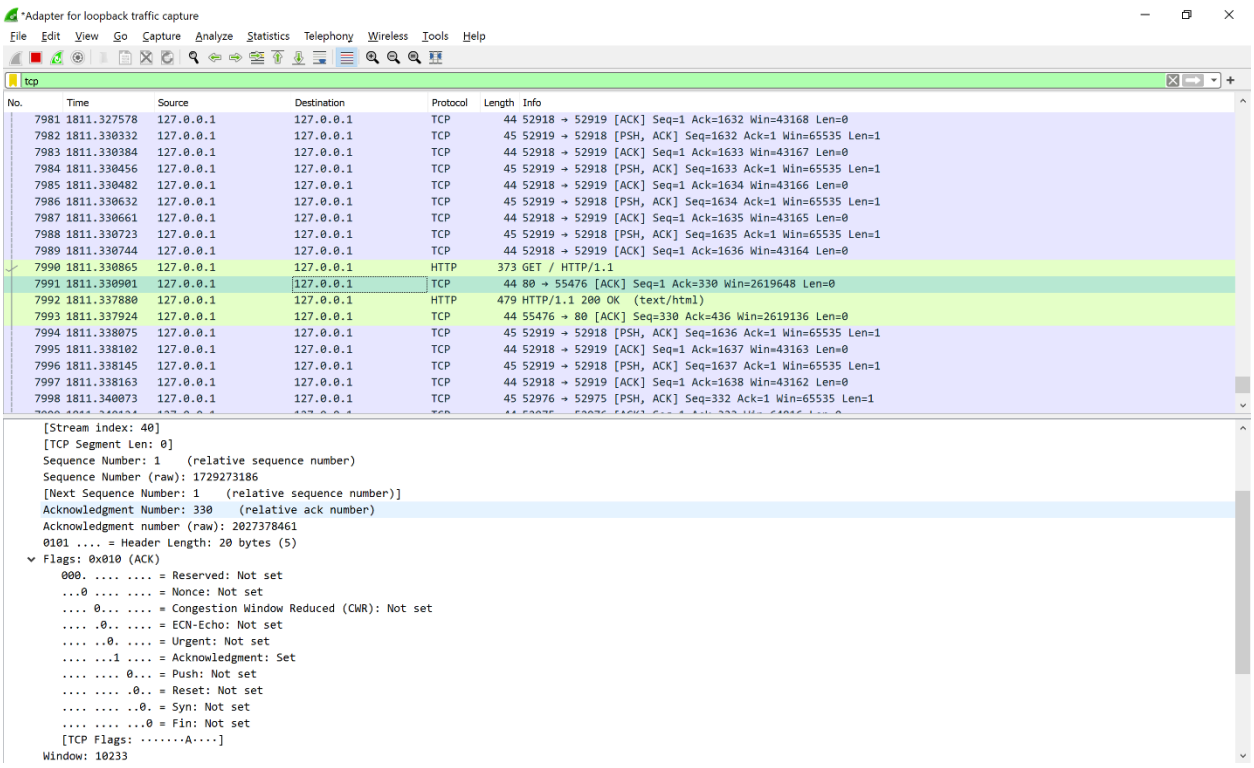
۲



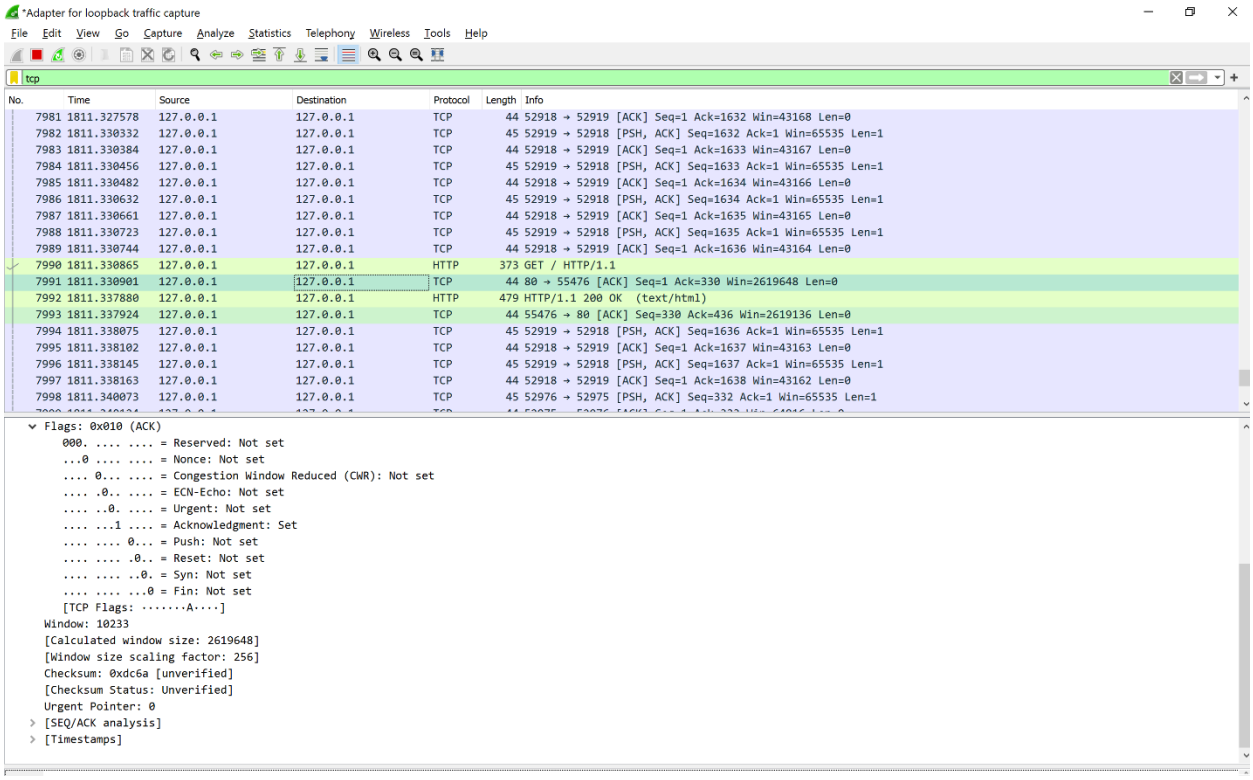
Connectionبه صورت keep aliveاست و درخواست به صورت get

User agent = Mozilla/5.0 (Windows NT 10.0; Win64; x64; rv:88.0) Gecko/20100101 Firefox/88.0

نشان دهنده نوع سیستم عامل و نوع browserو اطلاعات سیستمی دیگر ما است.

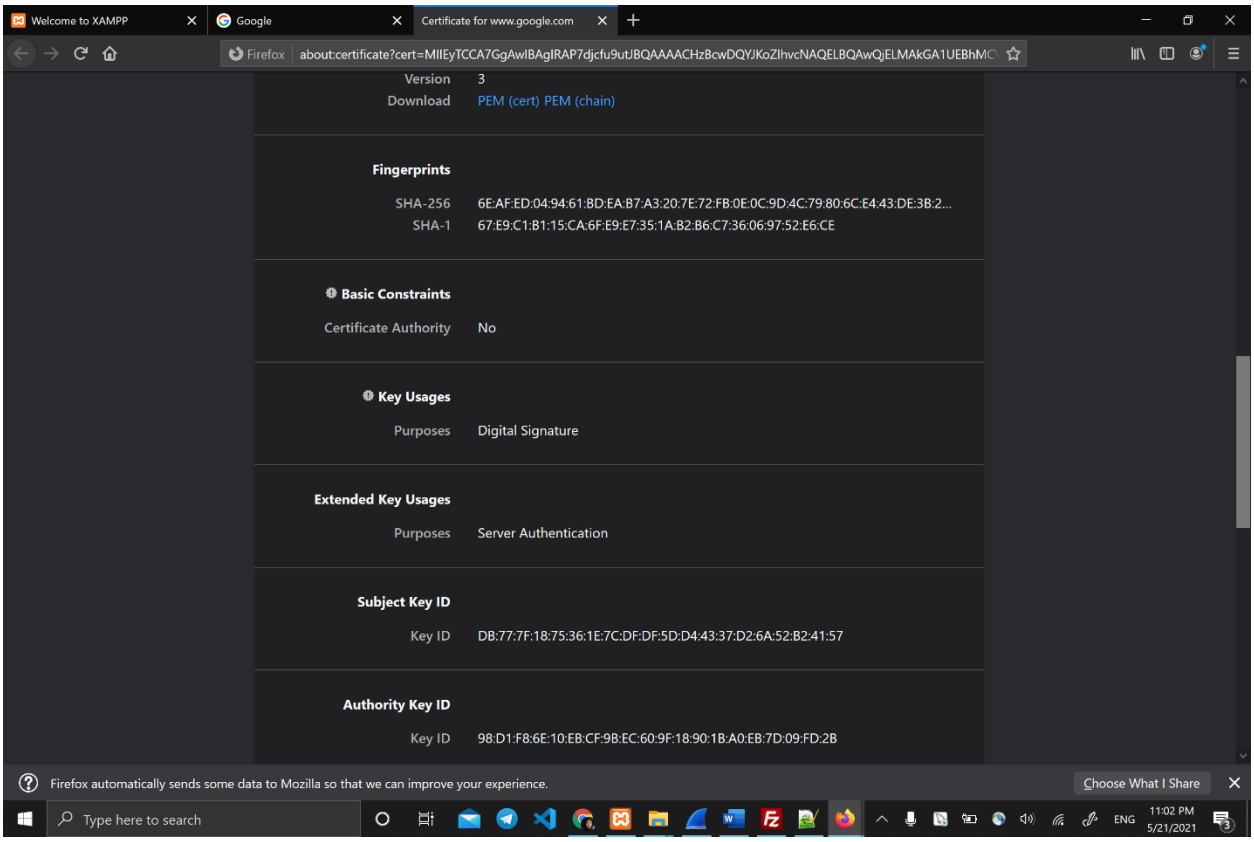


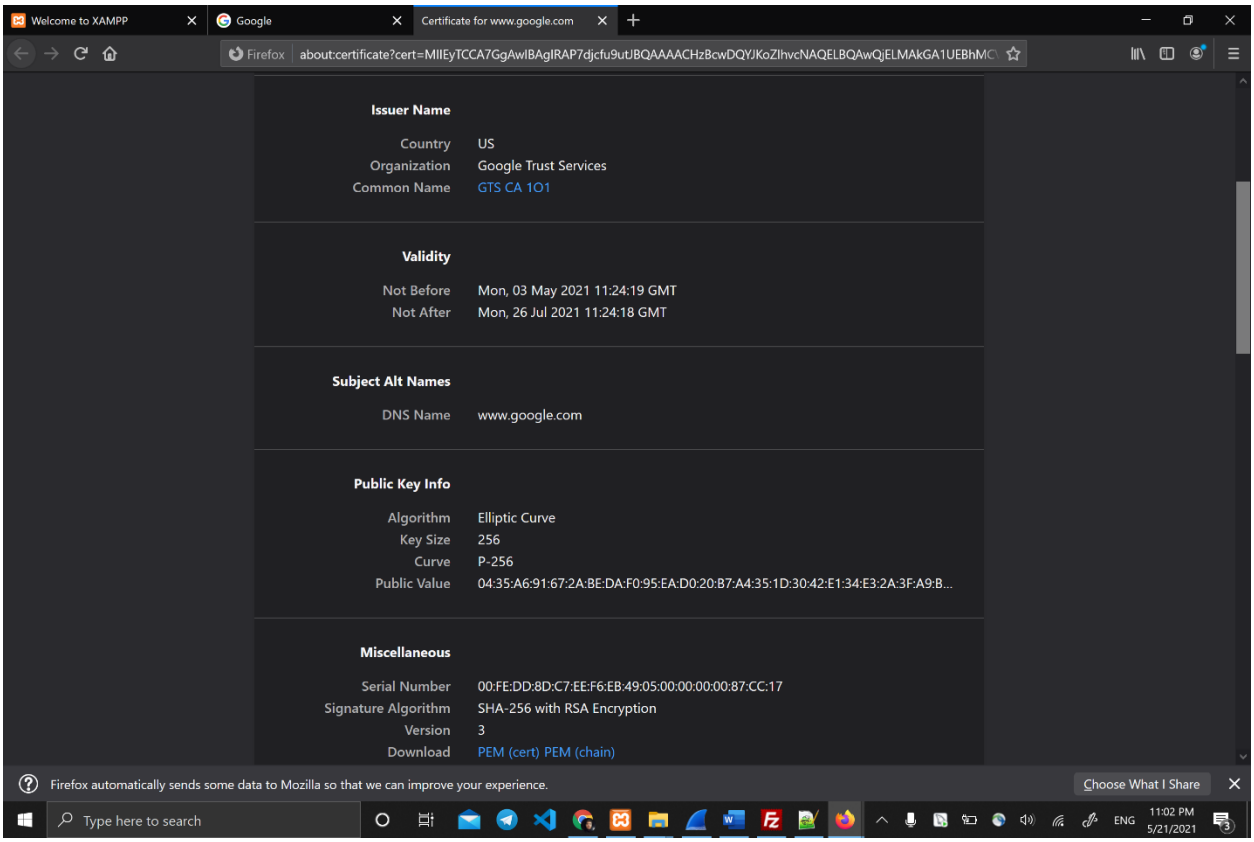
در شکل بالا مقادیر نشان داده شده اند.



Host port frame مقادیر متفاوت هستند.

۵


Welcome to XAMPP
Google
Certificate for www.google.com
Firefox
about:certificate?cert=MIIEyTCCA7GgAwIBAgIRAP7djcfu9utJBQAAAACHzBcwDQYJKoZIhvcNAQELBQAwQjELMAkGA1UEBhMC
Version 3
Download PEM (cert) PEM (chain)
Fingerprints
SHA-256 6E:AF:ED:04:94:61:BD:EA:B7:A3:20:7E:72:FB:0E:0C:9D:4C:79:80:6C:E4:43:DE:3B:2...
SHA-1 67:E9:C1:B1:15:CA:6F:E9:E7:35:1A:B2:B6:C7:36:06:97:52:E6:CE
Basic Constraints
Certificate Authority No
Key Usages
Purposes Digital Signature
Extended Key Usages
Purposes Server Authentication
Subject Key ID
Key ID DB:77:7F:18:75:36:1E:7C:DF:DF:5D:D4:43:37:D2:6A:52:B2:41:57
Authority Key ID
Key ID 98:D1:F8:6E:10:EB:CF:9B:EC:60:9F:18:90:1B:A0:EB:7D:09:FD:2B
Firefox automatically sends some data to Mozilla so that we can improve your experience.
Choose What I Share
Type here to search
ENG
11:02 PM
5/21/2021


Welcome to XAMPP
Google
Certificate for www.google.com
Firefox
about:certificate?cert=MIIEyTCCA7GgAwIBAgIRAP7djcfu9utJBQAAAACHzBcwDQYJKoZIhvcNAQELBQAwQjELMAkGA1UEBhMC
Issuer Name
Country US
Organization Google Trust Services
Common Name GTS CA 1O1
Validity
Not Before Mon, 03 May 2021 11:24:19 GMT
Not After Mon, 26 Jul 2021 11:24:18 GMT
Subject Alt Names
DNS Name www.google.com
Public Key Info
Algorithm Elliptic Curve
Key Size 256
Curve P-256
Public Value 04:35:A6:91:67:2A:BE:DA:F0:95:EA:D0:20:B7:A4:35:1D:30:42:E1:34:E3:2A:3F:A9:B...
Miscellaneous
Serial Number 00:FE:DD:8D:C7:EE:F6:EB:49:05:00:00:00:00:87:CC:17
Signature Algorithm SHA-256 with RSA Encryption
Version 3
Download PEM (cert) PEM (chain)
Firefox automatically sends some data to Mozilla so that we can improve your experience.
Choose What I Share
Type here to search
ENG
11:02 PM
5/21/2021

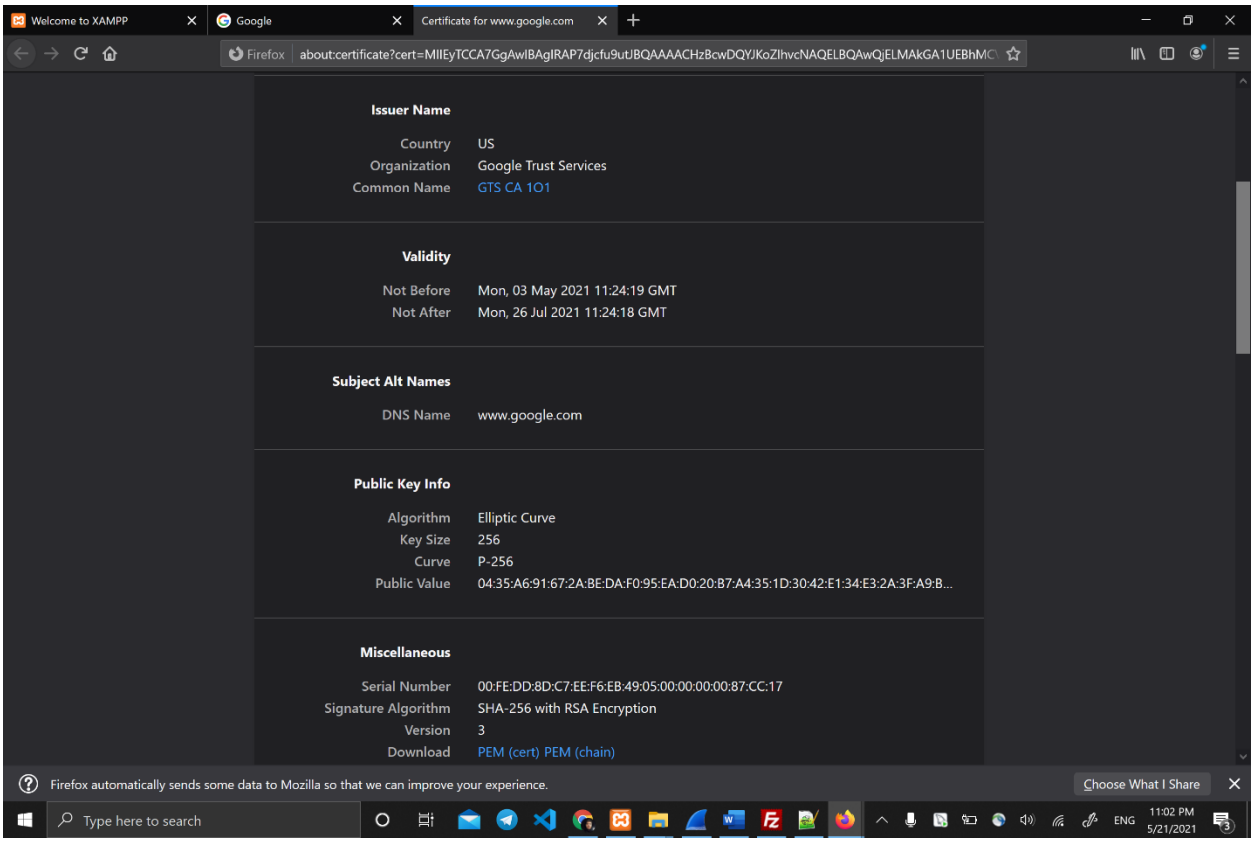
گواهی به وسیله google ساخته شده و تا ۳ مارس ۲۰۲۱ اعتبار دارد و از rsaاستفاده میکند و سایز ان 256است

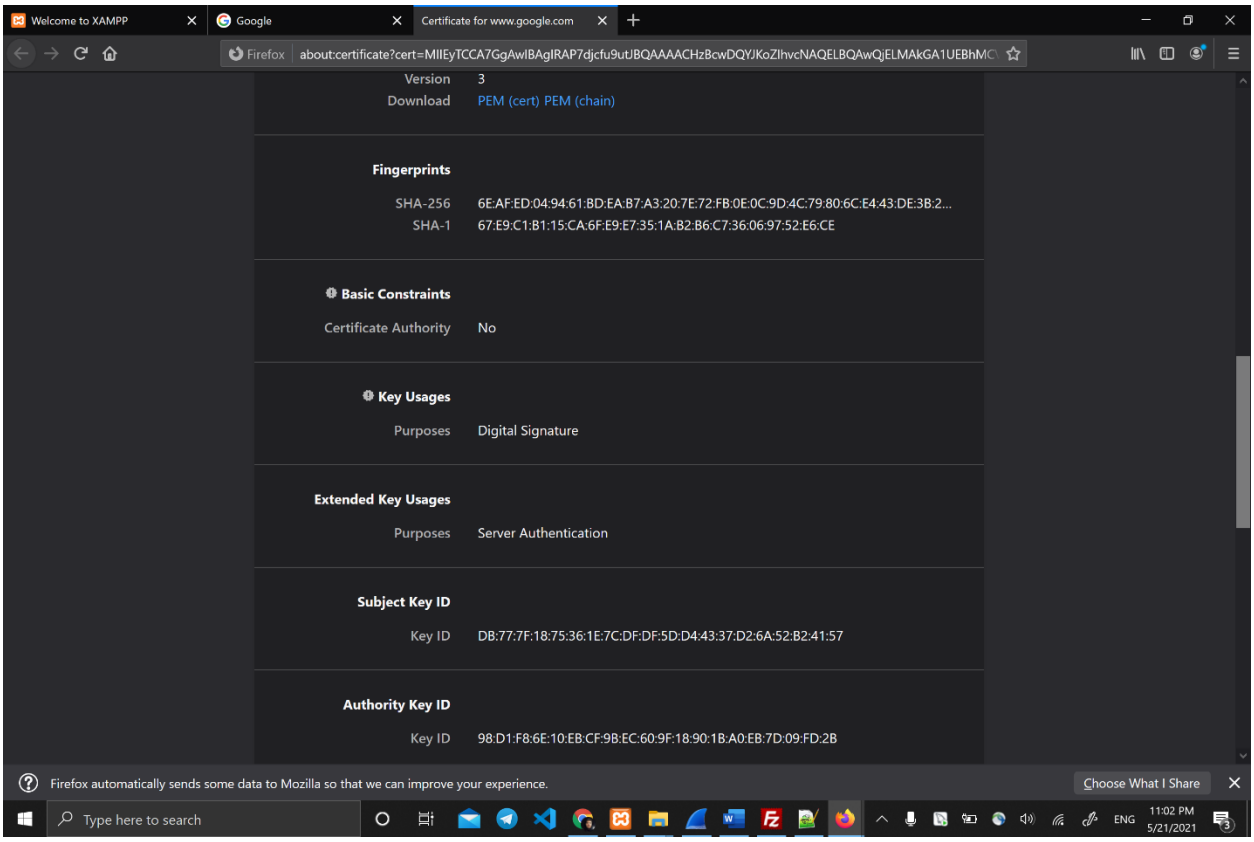
امضای دیجیتال از rsa , sha-256استفاده میکند.

6

به دلیل انکه پیام به صورت رمزی انتقال پیدا میکند امکان شنود و خواندن انها برای ما ممکن نیست.

۷





به طور مثال در زمان اعتبار، صادر کننده و اگوریتم کلید عمومی و certسایت کنونی و میزان اعتبار ان از جمله تفاوت های موجود است

۸

به وسیله دستور list-l فایل لیست شده اند و به مانند اطلاعات داده شده user خود را test و گذرواژه 123 را انتخاب کرده ایم.

پروتکل لایه tcp می باشد و port مبدا 56178 و مقصد 21 است.

۹

با فعال کردن ssl دیگر قابلیت دسترسی به وسیله browser از بین میرود و باید با استفاده از filezilla ارتباط خود را مجددا برقرار نماییم و به دلیل رمزنگاری شدن قابلیت خواندن از بین می‌رود

http

باید در ابتدا به سایت pbo.aut.ac.ir درخواست خود را ارسال کنیم تا توانایی مشاهده بسته های http باشد. دلیل ان هم این است که سایت اصلی به صورت https است. مقدار connection هم به صورت keep-alive است

User agent = Mozilla/5.0 (Windows NT 10.0; Win64; x64; rv:88.0) Gecko/20100101 Firefox/88.0

مقدار بالا هن برابر با user_agent است که اطلاعات سیستمی ما را نمایش میدهد.

ftp

به صورت tcp می باشد و port مبدا ۲۱ و مقصد 50261 میباشد.

و برای username مقدار anonymous و گذرواژه mozila@example.com را داریم.