آزمایشگاه شبکه های کامپیوتری
آزمایش سوم

تهیه کننده:
سارا تاجرنیا

استاد مربوطه:
استاد صادقیان

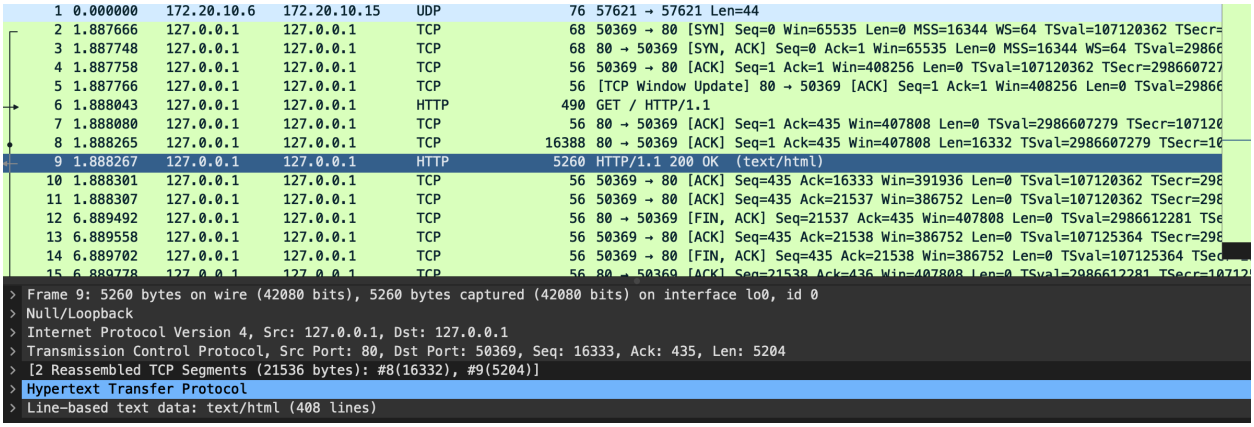
۱۴۰۱/۲/۱۶

۱-۱- هدف آزمایش

هدف این آزمایش، آشنایی با تنظیمات مقدماتی مربوط بـه راه‌انـدازی سـرویس‌هـای Web و FTP و تحلیل بسته‌های HTTP و FTP است.

سوال ۱: آدرس پورت‌های مبدا و مقصد چیست؟ رونـد برقـراری ارتبـاط در پروتکـل HTTP چگونـه است؟ وب سرور چگونه آدرس سایت درخواستی شما را تشخیص می‌دهد؟

آدرس سایتی که ساختیم: http://www.sara.com
آدرس پورت مبدا: 127.0.0.1
آدرس پورت مقصد: 127.0.0.1
روند برقراری ارتباط در پروتکل HTTP به این صورت است که هر صفحه از اینترنت شامل یک لینک Hyperlink است تا از این طریق بتوان به صفحات مختلف رفت. هر وب سرور علاوه بر صفحات موجود خود یک diamond دارد که برای دریافت و پاسخ گویی به درخواست هاست.
در این پروتکل ابتدا ارتباط TCP با وب سوکت برقرار میشود. مرورگر وب در واقع یک سرویس گیرنده HTTP است که درخواست را برای سرور میفرستد. به این صورت که وقتی کاربر یک آدرس IP یا URL وارد میکند مرورگر درخواستی به صورت HTTP برای سرور آن فایل ارسال میکند به این صورت است که HTTP Request فرستاده میشود و اگر ارتباط توسط سرور پذیرفته شد و صفحه وجود داست(ارور ۴۰۴ نخورد) پاسخ یا پیام سرور به کلاینت به صورت HTTP Respond دریافت میشود.
آدرس درخواستی ما به این صورت مشخص میشود که آدرس IP ما توسط DNS به وسیله Query گرفته میشود.



۲. بر روی اولین بسته در پنجره باز شده کلیک کنید. بخش‌های مختلف پروتکل HTTP را مشاهده کنید.

سوال ۲: مقدار بخش Connection چیست؟ درخواست HTTP از نوع GET بوده است یا از نوع POST؟ مقدار User Agent چیست؟ به نظر شما این مقدار بیانگر چه چیزی است؟

```
GET / HTTP/1.1
Host: saras-macbook-pro.local
Upgrade-Insecure-Requests: 1
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,*/*;q=0.8
User-Agent: Mozilla/5.0 (Macintosh; Intel Mac OS X 10_15_7) AppleWebKit/605.1.15 (KHTML, like
Gecko) Version/15.4 Safari/605.1.15
Accept-Language: en-US,en;q=0.9
Accept-Encoding: gzip, deflate
Connection: keep-alive

HTTP/1.1 200 OK
Date: Wed, 18 May 2022 10:30:00 GMT
Server: Apache/2.4.53 (Unix) OpenSSL/1.1.1n PHP/8.1.5 mod_perl/2.0.12 Perl/v5.34.1
Last-Modified: Tue, 22 Feb 2022 20:01:29 GMT
ETag: "52cc-5d8a0d08fb840"
Accept-Ranges: bytes
Content-Length: 21196
Keep-Alive: timeout=5, max=100
Connection: Keep-Alive
Content-Type: text/html

<!DOCTYPE html>
<html>

<head>
    <link rel="stylesheet" href="style.css">
    <link href="https://cdn.jsdelivr.net/npm/bootstrap@5.1.3/dist/css/bootstrap.min.css"
rel="stylesheet"
        integrity="sha384-1BmE4kWBq78iYhFldvKuhfTAU6auU8tT94WrHftjDbrCEXSU1oBoqyl2QvZ6jIW3"
crossorigin="anonymous">
    <meta name="viewport" content="width=device-width, initial-scale=1">
    <script src="https://cdn.jsdelivr.net/npm/@popperjs/core@2.10.2/dist/umd/popper.min.js"
    integrity="sha384-7+zCNj/IqJ95wo16oMtfsKbZ9ccEh31eOz1HGyDuCQ6wgnyJNSYdrPa03rtR1zdB"
crossorigin="anonymous"></script>
    <script src="https://cdn.jsdelivr.net/npm/bootstrap@5.1.3/dist/js/bootstrap.min.js"
    integrity="sha384-QJHtvGhmr9XOIpI6YVutG+2QOK9T+ZnN4kzFN1RtK3zEFEIsxhlmWl5/YESvpZ13"
crossorigin="anonymous"></script>
</head>

<body>
```

همان طور که از عکس هم پیدا است، connection برابر keep alive است یعنی میخواهد همچنان ارتباط را حفظ کند.
درخواست HTTP ما از نوع GET است.
مقدار user agent برابر مقدار مشخص شده در عکس است که نشان دهنده سیستم عامل، مرورگر و ورژن آن است.

سوال ۳: در پنجره باز شده، اولین بسته را انتخـاب کنیـد. سـپس مقـدار Flags در پروتکـل TCP را مشاهده کنید. چه مقادیری برای این بسته تنظیم شده است؟

مقادیر تنظیم شده برای flag ها به شکل زیر است:

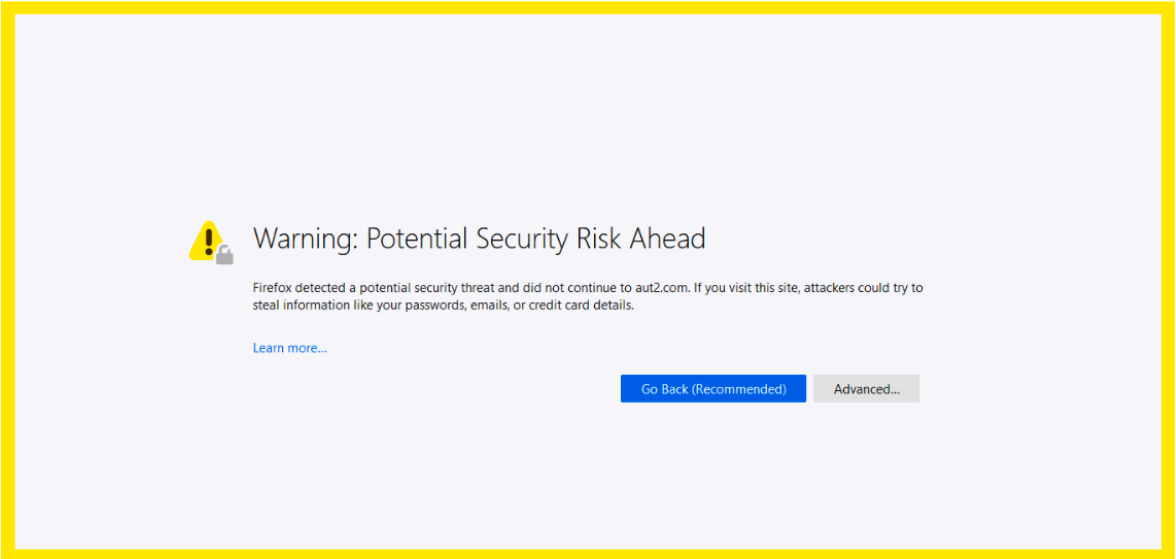
```
Flags: 0x018 (PSH, ACK)
   000. .... .... = Reserved: Not set
   ...0 .... .... = Nonce: Not set
   .... 0... .... = Congestion Window Reduced (CWR): Not set
   .... .0.. .... = ECN-Echo: Not set
   .... ..0. .... = Urgent: Not set
   .... ...1 .... = Acknowledgment: Set
   .... .... 1... = Push: Set
   .... .... .0.. = Reset: Not set
   .... .... ..0. = Syn: Not set
   .... .... ...0 = Fin: Not set
   [TCP Flags: ·······AP···]
```

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؟

بسته های دریافتی در دو سایت مختلف متفاوت خواهد بود به طوری که برای مثال پروتکل های بسته اول همگی HTTP و یا TCP بودند اما در سایت دوم علاوه بر این دو پروتکل هایی مثل UDP را شنود کردیم.

۳. حال آدرس https://www.example.com/ را در مرورگر خود باز کنید. دقت کنید که به‌جای test.com آدرس سایت خود را قرار دهید.

۴. سایت را در مرورگر باز کنید. خطای نشان داده شده در شکل (۱-۲) نمایش داده می‌شود.

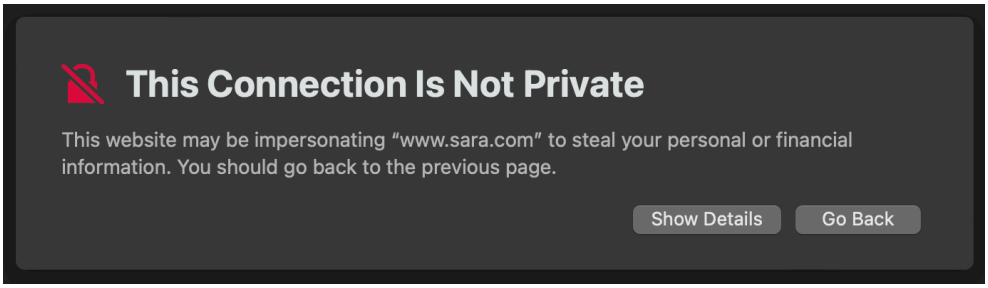


شکل (۱-۲) خطای نمایش داده شده

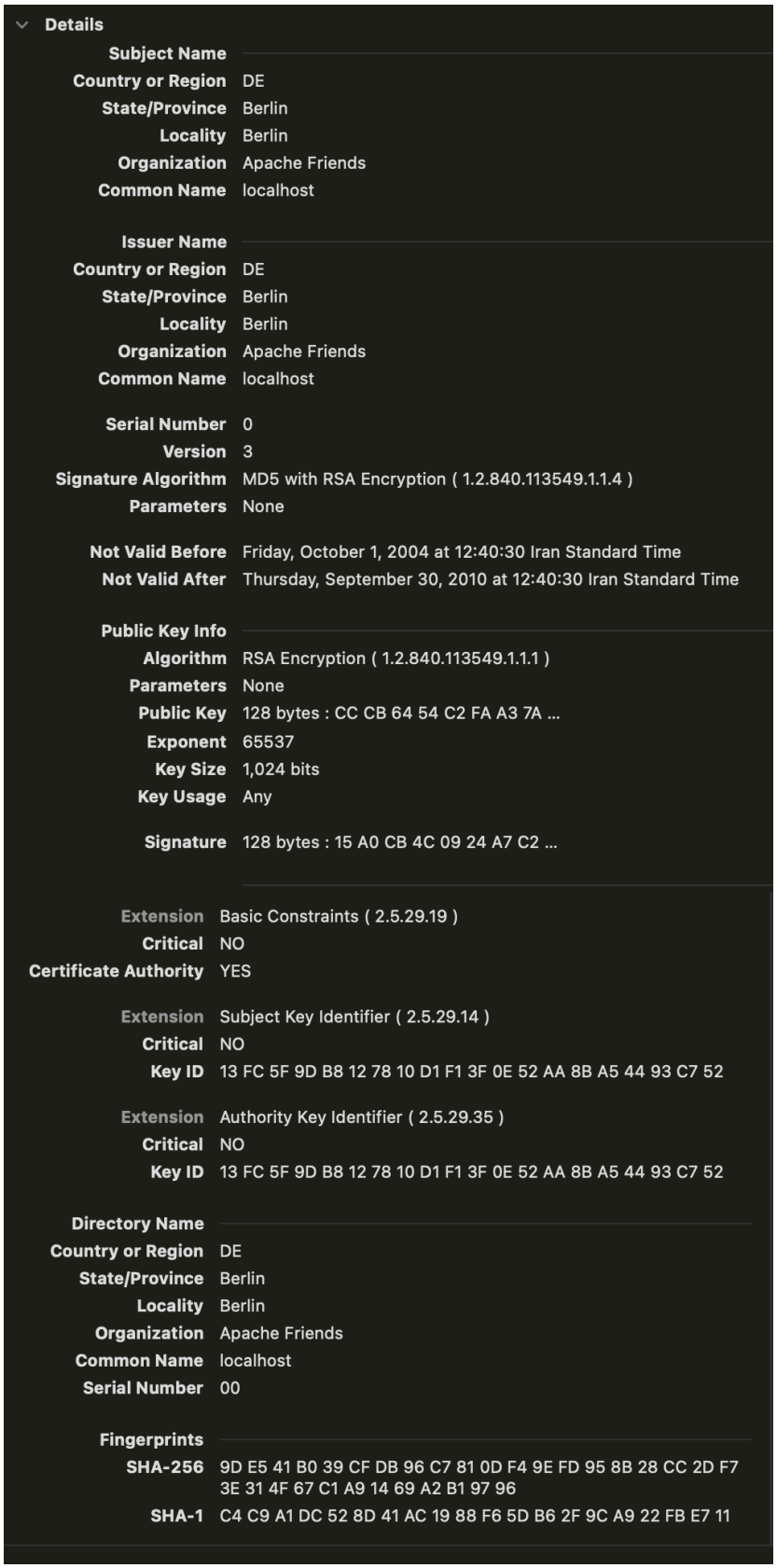
۵. بر روی Advanced کلیک کرده و دکمه View Certificate را فشار دهید.

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

ابتدا سایت https://www.sara.com را سرچ کردیم و با خطای زیر مواجه شدیم:



در قسمت view certificate مقادیر زیر قابل مشاهده است:



Details

Subject Name	
Country or Region	DE
State/Province	Berlin
Locality	Berlin
Organization	Apache Friends
Common Name	localhost
Issuer Name	
Country or Region	DE
State/Province	Berlin
Locality	Berlin
Organization	Apache Friends
Common Name	localhost
Serial Number	0
Version	3
Signature Algorithm	MD5 with RSA Encryption (1.2.840.113549.1.1.4)
Parameters	None
Not Valid Before	Friday, October 1, 2004 at 12:40:30 Iran Standard Time
Not Valid After	Thursday, September 30, 2010 at 12:40:30 Iran Standard Time
Public Key Info	
Algorithm	RSA Encryption (1.2.840.113549.1.1.1)
Parameters	None
Public Key	128 bytes : CC CB 64 54 C2 FA A3 7A ...
Exponent	65537
Key Size	1,024 bits
Key Usage	Any
Signature	128 bytes : 15 A0 CB 4C 09 24 A7 C2 ...
Extension	Basic Constraints (2.5.29.19)
Critical	NO
Certificate Authority	YES
Extension	Subject Key Identifier (2.5.29.14)
Critical	NO
Key ID	13 FC 5F 9D B8 12 78 10 D1 F1 3F 0E 52 AA 8B A5 44 93 C7 52
Extension	Authority Key Identifier (2.5.29.35)
Critical	NO
Key ID	13 FC 5F 9D B8 12 78 10 D1 F1 3F 0E 52 AA 8B A5 44 93 C7 52
Directory Name	
Country or Region	DE
State/Province	Berlin
Locality	Berlin
Organization	Apache Friends
Common Name	localhost
Serial Number	00
Fingerprints	
SHA-256	9D E5 41 B0 39 CF DB 96 C7 81 0D F4 9E FD 95 8B 28 CC 2D F7 3E 31 4F 67 C1 A9 14 69 A2 B1 97 96
SHA-1	C4 C9 A1 DC 52 8D 41 AC 19 88 F6 5D B6 2F 9C A9 22 FB E7 11

چه کسی صادر کرده:
مشخصات صادر کننده در قسمت اول عکس مشخص است.

برای چه کسی صادر کرده:
مشخصات دریافت کننده در قسمت دوم عکس مشخص است.

مدت زمان اعتبار گواهی:
از زمان Friday, October 1, 2004 at 12:40:30 Iran Standard Time تا Thursday, September 30, 2010 at 12:40:30 Iran Standard Time اعتبار دارد.

کلید عمومی صادر کننده:
در قسمت public key info عکس جزئیات کلید عمومی صادر کننده مشخص است.

امضای دیجیتال انجام شده توسط کدام الگوریتم:
همان طور که مشخص است الگوریتم برابر (1.2.840.113549.1.1.1) RSA Encryption است.

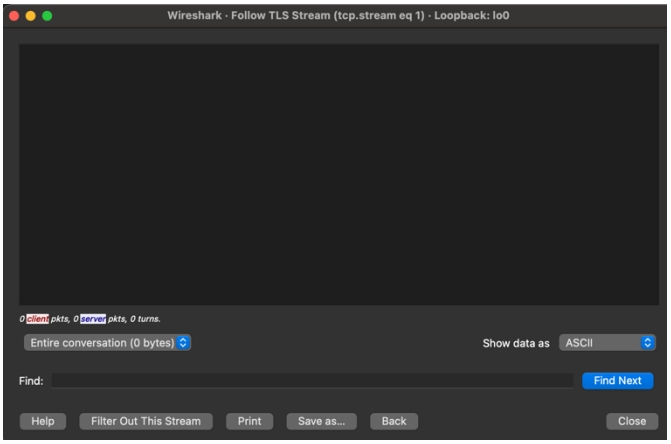
۶. حال ارتباط را با وایرشارک شنود کنید. بر روی بسته TLS مربوط به این ارتباط کلیک راست کرده و Follow SSL Stream را انتخاب کنید. صفحه‌ای مطابق شکل (۱-۳) نمایش داده می‌شود.

سوال ۶: آیا می‌توانید متن ارتباط را بخوانید؟ چرا؟

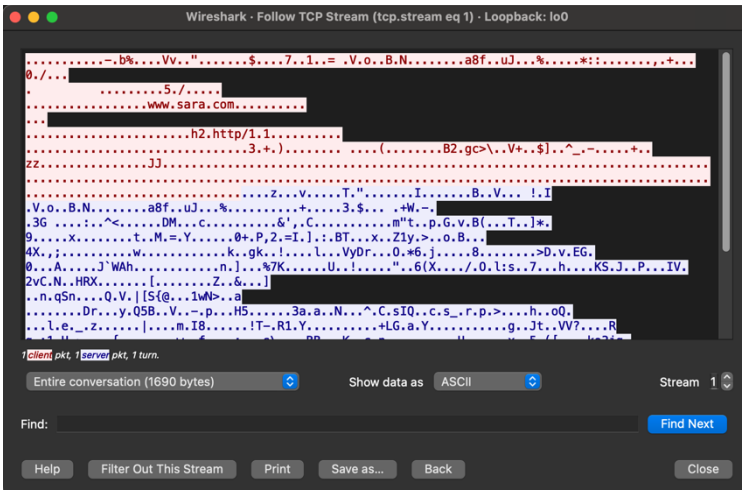
نمونه بسته TLS به صورت زیر ا ست:

13	0.057905	127.0.0.1	127.0.0.1	TCP	68	51988 → 443 [SYN] Seq=0 Win=65535 Len=0 MSS=16344 WS=64 TSval=3388821454 TSecr=0 SA
14	0.058029	127.0.0.1	127.0.0.1	TCP	68	443 → 51988 [SYN, ACK] Seq=0 Ack=1 Win=65535 Len=0 MSS=16344 WS=64 TSval=4239224295
15	0.058045	127.0.0.1	127.0.0.1	TCP	56	51988 → 443 [ACK] Seq=1 Ack=1 Win=408256 Len=0 TSval=3388821454 TSecr=4239224295
16	0.058057	127.0.0.1	127.0.0.1	TCP	56	[TCP Window Update] 443 → 51988 [ACK] Seq=1 Ack=1 Win=408256 Len=0 TSval=4239224295
17	0.058392	127.0.0.1	127.0.0.1	TLSv1.3	573	Client Hello
18	0.058449	127.0.0.1	127.0.0.1	TCP	56	443 → 51988 [ACK] Seq=1 Ack=518 Win=407744 Len=0 TSval=4239224296 TSecr=3388821454
19	0.059068	127.0.0.1	127.0.0.1	TLSv1.3	1229	Server Hello, Change Cipher Spec, Application Data, Application Data, Application D
20	0.059122	127.0.0.1	127.0.0.1	TCP	56	51988 → 443 [ACK] Seq=518 Ack=1174 Win=407104 Len=0 TSval=3388821455 TSecr=42392242
21	0.062750	127.0.0.1	127.0.0.1	TCP	56	51988 → 443 [FIN, ACK] Seq=518 Ack=1174 Win=407104 Len=0 TSval=3388821460 TSecr=423
22	0.062771	127.0.0.1	127.0.0.1	TCP	56	443 → 51988 [ACK] Seq=1174 Ack=519 Win=407744 Len=0 TSval=4239224301 TSecr=3388821
23	0.062829	127.0.0.1	127.0.0.1	TCP	56	443 → 51988 [FIN, ACK] Seq=1174 Ack=519 Win=407744 Len=0 TSval=4239224301 TSecr=338
24	0.062864	127.0.0.1	127.0.0.1	TCP	56	51988 → 443 [ACK] Seq=519 Ack=1175 Win=407104 Len=0 TSval=3388821460 TSecr=4239224

نمونه TLS Steam آن به صورت مقابل است که از آنجایی که سایت رمز نگاری شده نمیتواند به ما نشان دهد.



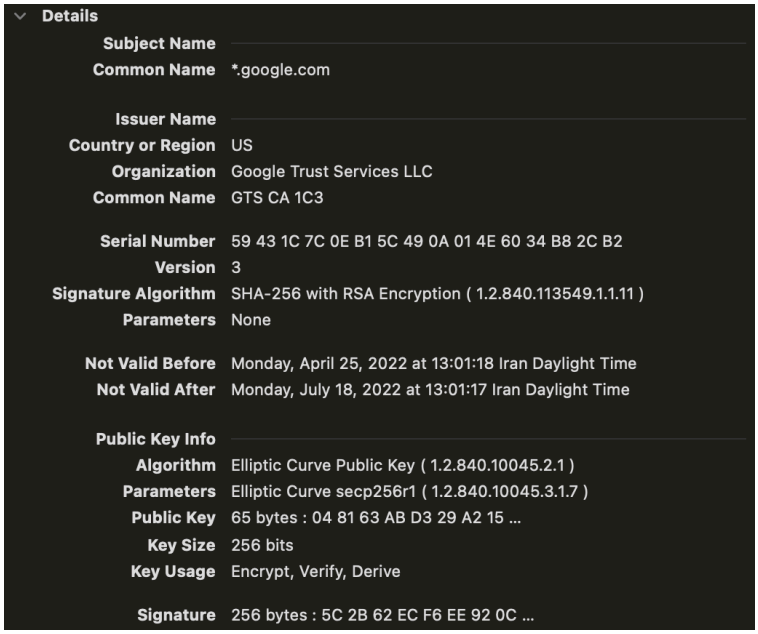
نمونه TCP Steam آن به صورت مقابل است که رمز نگاری شده و عملا ما نمیتوانیم چیزی از آن دریافت کنیم.

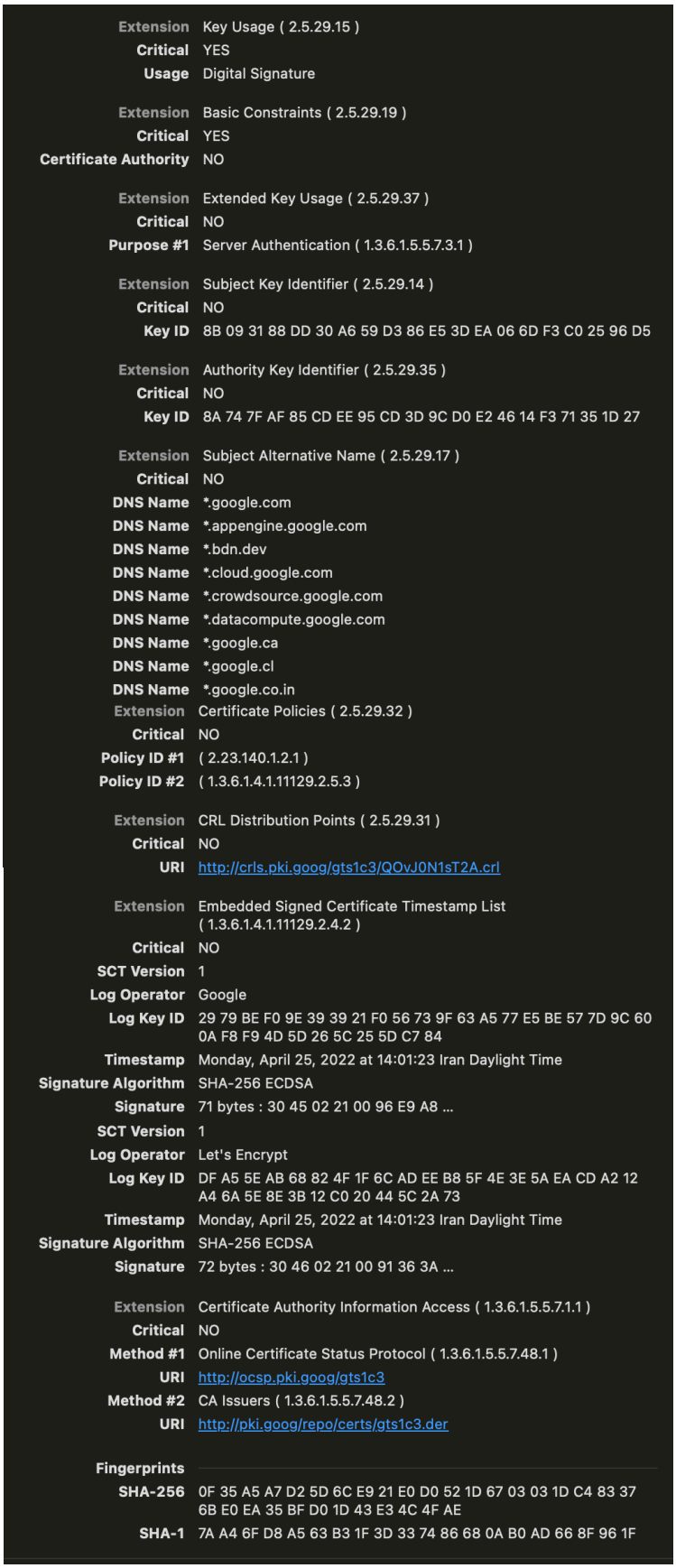


به یک سایت مانند https://google.com وصل شده، گواهی آن را بررسی کنید. برای اینکار بر روی علامت قفل در کنار آدرس سایت کلیک کنید. سپس بر روی علامت > در روبروی عبارت Connection Secure و سپس More Information کلیک کنید. در پنجره جدید باز شده از طریق View Certificate اطلاعات مربوط به گواهی وبسایت https://www.google.com/ قابل مشاهده است.

سوال ۷: گواهی آن سایت با گواهی سایت شما چه تفاوت‌هایی دارد؟

گواهی به صورت زیر است(لیست DNS ها خیلی بیشتر است):





Extension	Key Usage (2.5.29.15)
Critical	YES
Usage	Digital Signature
Extension	Basic Constraints (2.5.29.19)
Critical	YES
Certificate Authority	NO
Extension	Extended Key Usage (2.5.29.37)
Critical	NO
Purpose #1	Server Authentication (1.3.6.1.5.5.7.3.1)
Extension	Subject Key Identifier (2.5.29.14)
Critical	NO
Key ID	8B 09 31 88 DD 30 A6 59 D3 86 E5 3D EA 06 6D F3 C0 25 96 D5
Extension	Authority Key Identifier (2.5.29.35)
Critical	NO
Key ID	8A 74 7F AF 85 CD EE 95 CD 3D 9C D0 E2 46 14 F3 71 35 1D 27
Extension	Subject Alternative Name (2.5.29.17)
Critical	NO
DNS Name	*.google.com
DNS Name	*.appengine.google.com
DNS Name	*.bdn.dev
DNS Name	*.cloud.google.com
DNS Name	*.crowdsource.google.com
DNS Name	*.datacompute.google.com
DNS Name	*.google.ca
DNS Name	*.google.cl
DNS Name	*.google.co.in
Extension	Certificate Policies (2.5.29.32)
Critical	NO
Policy ID #1	(2.23.140.1.2.1)
Policy ID #2	(1.3.6.1.4.1.11129.2.5.3)
Extension	CRL Distribution Points (2.5.29.31)
Critical	NO
URI	http://crls.pki.goog/gts1c3/QOvJ0N1sT2A.crl
Extension	Embedded Signed Certificate Timestamp List (1.3.6.1.4.1.11129.2.4.2)
Critical	NO
SCT Version	1
Log Operator	Google
Log Key ID	29 79 BE F0 9E 39 39 21 F0 56 73 9F 63 A5 77 E5 BE 57 7D 9C 60 0A F8 F9 4D 5D 26 5C 25 5D C7 84
Timestamp	Monday, April 25, 2022 at 14:01:23 Iran Daylight Time
Signature Algorithm	SHA-256 ECDSA
Signature	71 bytes : 30 45 02 21 00 96 E9 A8 ...
SCT Version	1
Log Operator	Let's Encrypt
Log Key ID	DF A5 5E AB 68 82 4F 1F 6C AD EE B8 5F 4E 3E 5A EA CD A2 12 A4 6A 5E 8E 3B 12 C0 20 44 5C 2A 73
Timestamp	Monday, April 25, 2022 at 14:01:23 Iran Daylight Time
Signature Algorithm	SHA-256 ECDSA
Signature	72 bytes : 30 46 02 21 00 91 36 3A ...
Extension	Certificate Authority Information Access (1.3.6.1.5.5.7.1.1)
Critical	NO
Method #1	Online Certificate Status Protocol (1.3.6.1.5.5.7.48.1)
URI	http://ocsp.pki.goog/gts1c3
Method #2	CA Issuers (1.3.6.1.5.5.7.48.2)
URI	http://pki.goog/repo/certs/gts1c3.der
Fingerprints	
SHA-256	0F 35 A5 A7 D2 5D 6C E9 21 E0 D0 52 1D 67 03 03 1D C4 83 37 6B E0 EA 35 BF D0 1D 43 E3 4C 4F AE
SHA-1	7A A4 6F D8 A5 63 B3 1F 3D 33 74 86 68 0A B0 AD 66 8F 96 1F

گواهی آن از جمله اینکه چه کسی صادر کرده، برای چه کسی صادر کرده، مدت زمان اعتبار گواهی، جرئیات کلید عمومی صادر کننده، امضای دیجیتال انجام شده توسط کدام الگوریتم متفاوت است.

۱-۳-۲- تنظیمات سرور FTP

۷. ابتدا از طریق XAMPP ماژول FileZilla را استارت کنید. سپس طبق آموزش یک اکانت با رمز عبور دلخواه ایجاد کنین. سپس مسیر دلخواه برای به اشتراک‌گذاری را مشخص کنید.

۸. به آدرس ftp://127.0.0.1/ بروید. ارتباط را با وایرشارک شنود کنید.

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 ارتباط را مشخص کنید.

دستور استفاده شده برای لیست کردن:
List

نام کاربری:
نام کاربری به اسم sara است.

پروتکل لایه transport برای بسته ها:
TCP

آدرس پورت مبدا و مقصد:
پورت مبدا: 52981 پورت مقصد:21