

1

Wireshark packet capture interface showing HTTP traffic. The packet list shows a GET request for /dashboard/ and a 200 OK response. The packet details pane shows the HTTP response structure, including status bar, date, server, and last-modified headers.

No.	Time	Source	Destination	Protocol	Length	Info
7321	936.152107	127.0.0.1	127.0.0.1	HTTP	918	GET /dashboard/ HTTP/1.1
7323	936.157252	127.0.0.1	127.0.0.1	HTTP	290	HTTP/1.1 304 Not Modified
7325	936.857783	127.0.0.1	127.0.0.1	HTTP	802	GET /dashboard/images/favicon.png HTTP/1.1
7327	936.858935	127.0.0.1	127.0.0.1	HTTP	2861	HTTP/1.1 200 OK (PNG)
7329	937.571184	127.0.0.1	127.0.0.1	HTTP	918	GET /dashboard/ HTTP/1.1
7331	937.577065	127.0.0.1	127.0.0.1	HTTP	289	HTTP/1.1 304 Not Modified
7347	938.839702	127.0.0.1	127.0.0.1	HTTP	603	GET /dashboard/ HTTP/1.1
7349	938.843538	127.0.0.1	127.0.0.1	HTTP	290	HTTP/1.1 304 Not Modified
7351	939.379221	127.0.0.1	127.0.0.1	HTTP	487	GET /dashboard/images/favicon.png HTTP/1.1
7353	939.380172	127.0.0.1	127.0.0.1	HTTP	2861	HTTP/1.1 200 OK (PNG)
7358	940.106361	127.0.0.1	127.0.0.1	HTTP	802	GET /dashboard/images/favicon.png HTTP/1.1
7360	940.107323	127.0.0.1	127.0.0.1	HTTP	2862	HTTP/1.1 200 OK (PNG)
7403	974.842855	127.0.0.1	127.0.0.1	HTTP	382	GET /dashboard/images/social-icons@2x.png HTTP/1.1
7418	974.851145	127.0.0.1	127.0.0.1	HTTP	5715	HTTP/1.1 200 OK (PNG)
7990	1811.330865	127.0.0.1	127.0.0.1	HTTP	373	GET / HTTP/1.1
7992	1811.337880	127.0.0.1	127.0.0.1	HTTP	479	HTTP/1.1 200 OK (text/html)
8030	1811.392084	127.0.0.1	127.0.0.1	HTTP	321	GET /favicon.ico HTTP/1.1
8036	1811.393038	127.0.0.1	127.0.0.1	HTTP	578	HTTP/1.1 404 Not Found (text/html)

... .. 1... = Push: Set  
... .. .0... = Reset: Not set  
... .. .0... = Syn: Not set  
... .. .0... = Fin: Not set  
[TCP Flags: .....AP...]  
Window: 10233  
[Calculated window size: 2619648]  
[Window size scaling factor: 256]  
Checksum: 0x8751 [unverified]  
[Checksum Status: Unverified]  
Urgent Pointer: 0  
> [SEQ/ACK analysis]  
> [Timestamps]  
TCP payload (435 bytes)  
▼ Hypertext Transfer Protocol  
> HTTP/1.1 200 OK\r\n  
Date: Fri, 21 May 2021 19:08:44 GMT\r\n  
Server: Apache/2.4.47 (Win64) OpenSSL/1.1.1k PHP/8.0.6\r\n  
Last-Modified: Fri, 21 May 2021 18:04:45 GMT\r\n

بر اساس تصویر پورت مبدا ۸۰ و پورت مقصد 54211

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

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

۲

\*Adapter for loopback traffic capture

File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help

http

No.	Time	Source	Destination	Protocol	Length	Info
7321	936.152107	127.0.0.1	127.0.0.1	HTTP	918	GET /dashboard/ HTTP/1.1
7323	936.157252	127.0.0.1	127.0.0.1	HTTP	290	HTTP/1.1 304 Not Modified
7325	936.857783	127.0.0.1	127.0.0.1	HTTP	802	GET /dashboard/images/favicon.png HTTP/1.1
7327	936.858935	127.0.0.1	127.0.0.1	HTTP	2861	HTTP/1.1 200 OK (PNG)
7329	937.571184	127.0.0.1	127.0.0.1	HTTP	918	GET /dashboard/ HTTP/1.1
7331	937.577065	127.0.0.1	127.0.0.1	HTTP	289	HTTP/1.1 304 Not Modified
7347	938.839702	127.0.0.1	127.0.0.1	HTTP	603	GET /dashboard/ HTTP/1.1
7349	938.843538	127.0.0.1	127.0.0.1	HTTP	290	HTTP/1.1 304 Not Modified
7351	939.379221	127.0.0.1	127.0.0.1	HTTP	487	GET /dashboard/images/favicon.png HTTP/1.1
7353	939.380172	127.0.0.1	127.0.0.1	HTTP	2861	HTTP/1.1 200 OK (PNG)
7358	940.106361	127.0.0.1	127.0.0.1	HTTP	802	GET /dashboard/images/favicon.png HTTP/1.1
7360	940.107323	127.0.0.1	127.0.0.1	HTTP	2862	HTTP/1.1 200 OK (PNG)
7403	974.842855	127.0.0.1	127.0.0.1	HTTP	382	GET /dashboard/images/social-icons@2x.png HTTP/1.1
7418	974.851145	127.0.0.1	127.0.0.1	HTTP	5715	HTTP/1.1 200 OK (PNG)
7990	1811.330865	127.0.0.1	127.0.0.1	HTTP	373	GET / HTTP/1.1
7992	1811.337880	127.0.0.1	127.0.0.1	HTTP	479	HTTP/1.1 200 OK (text/html)
8030	1811.392084	127.0.0.1	127.0.0.1	HTTP	321	GET /favicon.ico HTTP/1.1
8036	1811.393038	127.0.0.1	127.0.0.1	HTTP	578	HTTP/1.1 404 Not Found (text/html)

Checksum: 0x0590 [unverified]  
[Checksum Status: Unverified]  
Urgent Pointer: 0  
> [SEQ/ACK analysis]  
> [Timestamps]  
TCP payload (329 bytes)  
▼ Hypertext Transfer Protocol  
> GET / HTTP/1.1\r\n  
Host: aut2.com\r\n  
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64; rv:88.0) Gecko/20100101 Firefox/88.0\r\n  
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/webp,\*/\*;q=0.8\r\n  
Accept-Language: en-US,en;q=0.5\r\n  
Accept-Encoding: gzip, deflate\r\n  
Connection: keep-alive\r\n  
Upgrade-Insecure-Requests: 1\r\n  
\r\n  
[Full request URI: http://aut2.com/]  
[HTTP request 1/2]  
[Response in frame: 7992]  
[Next request in frame: 8030]

Connection به صورت keep alive است 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 browser و اطلاعات سیستمی دیگر ما است.

\*Adapter for loopback traffic capture

File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help

tcp

No.	Time	Source	Destination	Protocol	Length	Info
7981	1811.327578	127.0.0.1	127.0.0.1	TCP	44	52918 → 52919 [ACK] Seq=1 Ack=1632 Win=43168 Len=0
7982	1811.330332	127.0.0.1	127.0.0.1	TCP	45	52919 → 52918 [PSH, ACK] Seq=1632 Ack=1 Win=65535 Len=1
7983	1811.330384	127.0.0.1	127.0.0.1	TCP	44	52918 → 52919 [ACK] Seq=1 Ack=1633 Win=43167 Len=0
7984	1811.330456	127.0.0.1	127.0.0.1	TCP	45	52919 → 52918 [PSH, ACK] Seq=1633 Ack=1 Win=65535 Len=1
7985	1811.330482	127.0.0.1	127.0.0.1	TCP	44	52918 → 52919 [ACK] Seq=1 Ack=1634 Win=43166 Len=0
7986	1811.330632	127.0.0.1	127.0.0.1	TCP	45	52919 → 52918 [PSH, ACK] Seq=1634 Ack=1 Win=65535 Len=1
7987	1811.330661	127.0.0.1	127.0.0.1	TCP	44	52918 → 52919 [ACK] Seq=1 Ack=1635 Win=43165 Len=0
7988	1811.330723	127.0.0.1	127.0.0.1	TCP	45	52919 → 52918 [PSH, ACK] Seq=1635 Ack=1 Win=65535 Len=1
7989	1811.330744	127.0.0.1	127.0.0.1	TCP	44	52918 → 52919 [ACK] Seq=1 Ack=1636 Win=43164 Len=0
7990	1811.330865	127.0.0.1	127.0.0.1	HTTP	373	GET / HTTP/1.1
7991	1811.330901	127.0.0.1	127.0.0.1	TCP	44	80 → 55476 [ACK] Seq=1 Ack=330 Win=2619648 Len=0
7992	1811.337880	127.0.0.1	127.0.0.1	HTTP	479	HTTP/1.1 200 OK (text/html)
7993	1811.337924	127.0.0.1	127.0.0.1	TCP	44	55476 → 80 [ACK] Seq=330 Ack=436 Win=2619136 Len=0
7994	1811.338075	127.0.0.1	127.0.0.1	TCP	45	52919 → 52918 [PSH, ACK] Seq=1636 Ack=1 Win=65535 Len=1
7995	1811.338102	127.0.0.1	127.0.0.1	TCP	44	52918 → 52919 [ACK] Seq=1 Ack=1637 Win=43163 Len=0
7996	1811.338145	127.0.0.1	127.0.0.1	TCP	45	52919 → 52918 [PSH, ACK] Seq=1637 Ack=1 Win=65535 Len=1
7997	1811.338163	127.0.0.1	127.0.0.1	TCP	44	52918 → 52919 [ACK] Seq=1 Ack=1638 Win=43162 Len=0
7998	1811.340073	127.0.0.1	127.0.0.1	TCP	45	52976 → 52975 [PSH, ACK] Seq=332 Ack=1 Win=65535 Len=1

[Stream index: 40]  
 [TCP Segment Len: 0]  
 Sequence Number: 1 (relative sequence number)  
 Sequence Number (raw): 1729273186  
 [Next Sequence Number: 1 (relative sequence number)]  
 Acknowledgment Number: 330 (relative ack number)  
 Acknowledgment number (raw): 2027378461  
 0101 .... = Header Length: 20 bytes (5)  
 ▾ Flags: 0x010 (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  
 ....0... .... = Push: Not set  
 ....0. .... = Reset: Not set  
 ....0. .... = Syn: Not set  
 ....0. .... = Fin: Not set  
 [TCP Flags: .....A....]  
 Window: 10233

در شکل بالا مقادیر نشان داده شده اند.

Adapter for loopback traffic capture

File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help

tcp

No.	Time	Source	Destination	Protocol	Length	Info
7981	1811.327578	127.0.0.1	127.0.0.1	TCP	44	52918 → 52919 [ACK] Seq=1 Ack=1632 Win=43168 Len=0
7982	1811.330332	127.0.0.1	127.0.0.1	TCP	45	52919 → 52918 [PSH, ACK] Seq=1632 Ack=1 Win=65535 Len=1
7983	1811.330384	127.0.0.1	127.0.0.1	TCP	44	52918 → 52919 [ACK] Seq=1 Ack=1633 Win=43167 Len=0
7984	1811.330456	127.0.0.1	127.0.0.1	TCP	45	52919 → 52918 [PSH, ACK] Seq=1633 Ack=1 Win=65535 Len=1
7985	1811.330482	127.0.0.1	127.0.0.1	TCP	44	52918 → 52919 [ACK] Seq=1 Ack=1634 Win=43166 Len=0
7986	1811.330632	127.0.0.1	127.0.0.1	TCP	45	52919 → 52918 [PSH, ACK] Seq=1634 Ack=1 Win=65535 Len=1
7987	1811.330661	127.0.0.1	127.0.0.1	TCP	44	52918 → 52919 [ACK] Seq=1 Ack=1635 Win=43165 Len=0
7988	1811.330723	127.0.0.1	127.0.0.1	TCP	45	52919 → 52918 [PSH, ACK] Seq=1635 Ack=1 Win=65535 Len=1
7989	1811.330744	127.0.0.1	127.0.0.1	TCP	44	52918 → 52919 [ACK] Seq=1 Ack=1636 Win=43164 Len=0
7990	1811.330865	127.0.0.1	127.0.0.1	HTTP	373	GET / HTTP/1.1
7991	1811.330901	127.0.0.1	127.0.0.1	TCP	44	80 → 55476 [ACK] Seq=1 Ack=330 Win=2619648 Len=0
7992	1811.337880	127.0.0.1	127.0.0.1	HTTP	479	HTTP/1.1 200 OK (text/html)
7993	1811.337924	127.0.0.1	127.0.0.1	TCP	44	55476 → 80 [ACK] Seq=330 Ack=436 Win=2619136 Len=0
7994	1811.338075	127.0.0.1	127.0.0.1	TCP	45	52919 → 52918 [PSH, ACK] Seq=1636 Ack=1 Win=65535 Len=1
7995	1811.338102	127.0.0.1	127.0.0.1	TCP	44	52918 → 52919 [ACK] Seq=1 Ack=1637 Win=43163 Len=0
7996	1811.338145	127.0.0.1	127.0.0.1	TCP	45	52919 → 52918 [PSH, ACK] Seq=1637 Ack=1 Win=65535 Len=1
7997	1811.338163	127.0.0.1	127.0.0.1	TCP	44	52918 → 52919 [ACK] Seq=1 Ack=1638 Win=43162 Len=0
7998	1811.340073	127.0.0.1	127.0.0.1	TCP	45	52976 → 52975 [PSH, ACK] Seq=332 Ack=1 Win=65535 Len=1

Flags: 0x010 (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  
 ....0... = Push: Not set  
 ....0... = Reset: Not set  
 ....0... = Syn: Not set  
 ....0... = Fin: Not set  
 [TCP Flags: .....A....]  
 Window: 10233  
 [Calculated window size: 2619648]  
 [Window size scaling factor: 256]  
 Checksum: 0xdc6a [unverified]  
 [Checksum Status: Unverified]  
 Urgent Pointer: 0  
 > [SEQ/ACK analysis]  
 > [Timestamps]

Host port frame مقادير متفاوت هستند.

Firefox | about:certificate?cert=MIIEyTCCA7GgAwIBAgIRAP7djcfu9utJBQAAAAChZ8cwDQYJKoZIhvcNAQELBQAwQjELMAkGA1UEBhMC...

Version	3
Download	<a href="#">PEM (cert)</a> <a href="#">PEM (chain)</a>
<b>Fingerprints</b>	
SHA-256	6EAFED: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
<b>Basic Constraints</b>	
Certificate Authority	No
<b>Key Usages</b>	
Purposes	Digital Signature
<b>Extended Key Usages</b>	
Purposes	Server Authentication
<b>Subject Key ID</b>	
Key ID	DB:77:7F:18:75:36:1E:7C:DF:5D:D4:43:37:D2:6A:52:B2:41:57
<b>Authority Key ID</b>	
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

11:02 PM 5/21/2021

Firefox | about:certificate?cert=MIIEyTCCA7GgAwIBAgIRAP7djcfu9utJBQAAAAChZ8cwDQYJKoZIhvcNAQELBQAwQjELMAkGA1UEBhMC...

<b>Issuer Name</b>	
Country	US
Organization	Google Trust Services
Common Name	<a href="#">GTS CA 101</a>
<b>Validity</b>	
Not Before	Mon, 03 May 2021 11:24:19 GMT
Not After	Mon, 26 Jul 2021 11:24:18 GMT
<b>Subject Alt Names</b>	
DNS Name	www.google.com
<b>Public Key Info</b>	
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...
<b>Miscellaneous</b>	
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	<a href="#">PEM (cert)</a> <a href="#">PEM (chain)</a>

Firefox automatically sends some data to Mozilla so that we can improve your experience. Choose What I Share

Type here to search

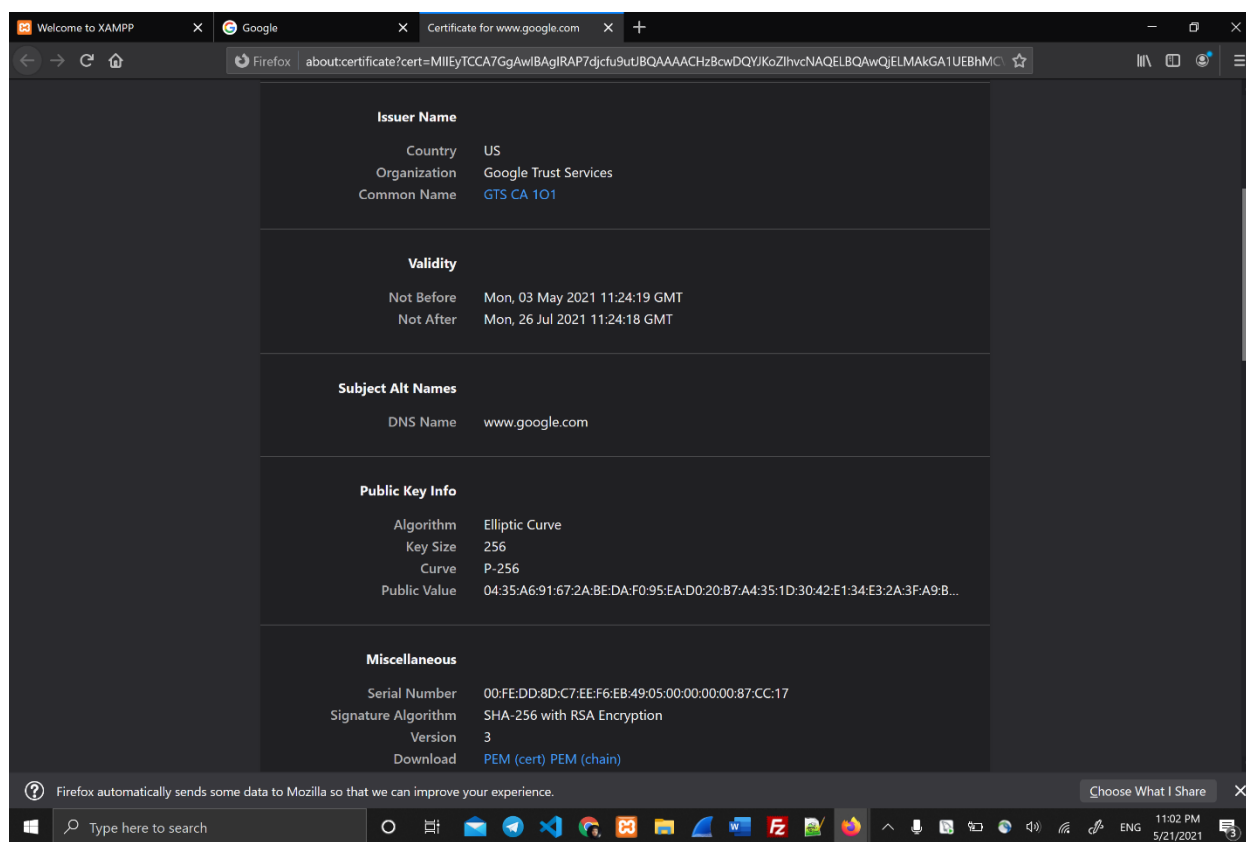
11:02 PM 5/21/2021

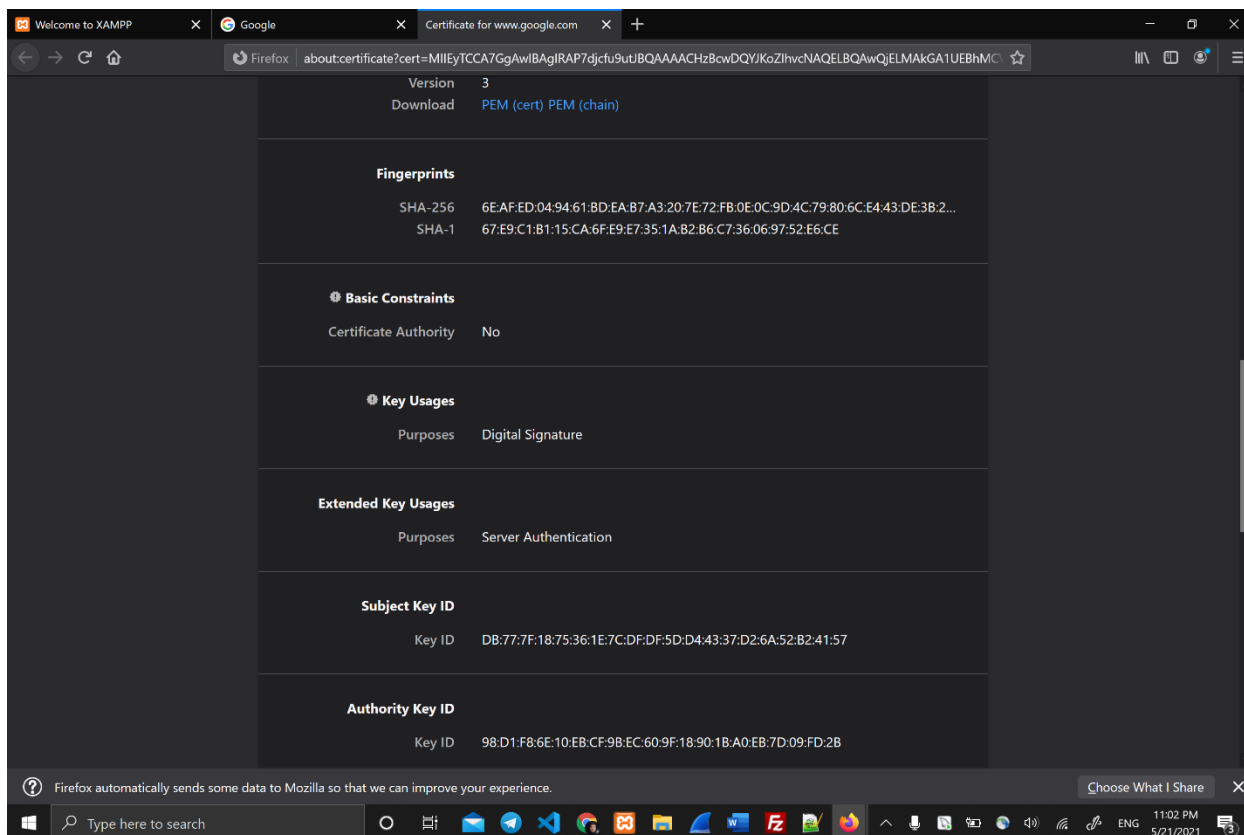
گواهی به وسیله google ساخته شده و تا ۳ مارس ۲۰۲۱ اعتبار دارد و از rsa استفاده میکند و سایز آن 256 است  
امضای دیجیتال از sha-256 , rsa استفاده میکند.

6

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

۷





به طور مثال در زمان اعتبار، صادر کننده و الگوریتم کلید عمومی و **cert** سایت کنونی و میزان اعتبار آن از جمله تفاوت های موجود است

۸

به وسیله دستور **l-list** فایل لیست شده اند و به مانند اطلاعات داده شده **user** خود را **test** و گذرواژه **123** را انتخاب کرده ایم. پورتکل لایه **tcp** می باشد و **port** مبدأ **56178** و مقصد **21** است.

۹

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

**http**

باید در ابتدا به سایت **pbo.aut.ac.ir** درخواست خود را ارسال کنیم تا توانایی مشاهده بسته های **http** باشد. دلیل آن 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 مبداء ۲۱ و مقصد 50261 میباشد.

و برای username مقدار anonymous و گذرواژه [mozilla@example.com](mailto:mozilla@example.com) را داریم.