

به نام خدا



---

# راه اندازی سرویس های WEB, FTP

---

آزمایش یک، فصل دو



محمد جواد زندیه ۹۸۳۱۰۳۲

۱۴ اردیبهشت ۱۴۰۰

دانشکده مهندسی کامپیوتر، دانشگاه صنعتی امیرکبیر

## سوال ۱

آدرس پورت مبدا و مقصد: 127.0.0.1

روند برقراری ارتباط در HTTP:

۱. ایجاد ارتباط با سرور

۲. ارسال درخواست به سرور

۳. دریافت پاسخ از سرور

۴. قطع ارتباط

در فایل hosts مقدار 127.0.0.1 را معادل آدرس [www.aut2.ac.ir](http://www.aut2.ac.ir) قرار دادیم و هرگاه که آدرس این سایت را وارد می کنیم، وب سرور میداند که منظور ما همان [www.aut2.ac.ir](http://www.aut2.ac.ir) است.

مرورگر های وب، در اولین گام باید IP آدرس دامنه را شناسایی کنند. مرورگر با استفاده از حافظه cache خود و یا با استفاده از DNS ها، آدرس IP را بدست می آورد.

13	1.870846	127.0.0.1	127.0.0.1	HTTP	835 GET / HTTP/1.1
15	1.876554	127.0.0.1	127.0.0.1	HTTP	316 HTTP/1.1 304 Not Modified
10	1.862503	127.0.0.1	127.0.0.1	TCP	56 54438 → 80 [SYN] Seq=0 Win=65535 Len=0 MSS=65495 WS=256 SACK_PERM=1
11	1.862589	127.0.0.1	127.0.0.1	TCP	56 80 → 54438 [SYN, ACK] Seq=0 Ack=1 Win=65535 Len=0 MSS=65495 WS=256 SACK_PERM=1
12	1.862659	127.0.0.1	127.0.0.1	TCP	44 54438 → 80 [ACK] Seq=1 Ack=1 Win=2619648 Len=0
14	1.870938	127.0.0.1	127.0.0.1	TCP	44 80 → 54438 [ACK] Seq=1 Ack=792 Win=2619648 Len=0
16	1.876599	127.0.0.1	127.0.0.1	TCP	44 54438 → 80 [ACK] Seq=792 Ack=273 Win=2619392 Len=0
21	2.703842	127.0.0.1	127.0.0.1	TCP	44 54438 → 80 [FIN, ACK] Seq=792 Ack=273 Win=2619392 Len=0
22	2.703895	127.0.0.1	127.0.0.1	TCP	44 80 → 54438 [ACK] Seq=273 Ack=793 Win=2619648 Len=0
23	2.703922	127.0.0.1	127.0.0.1	TCP	44 80 → 54438 [FIN, ACK] Seq=273 Ack=793 Win=2619648 Len=0
24	2.703980	127.0.0.1	127.0.0.1	TCP	44 54438 → 80 [ACK] Seq=793 Ack=274 Win=2619392 Len=0

## سوال ۲

مقدار بخش Connection: keep-alive

درخواست از نوع GET بوده است.

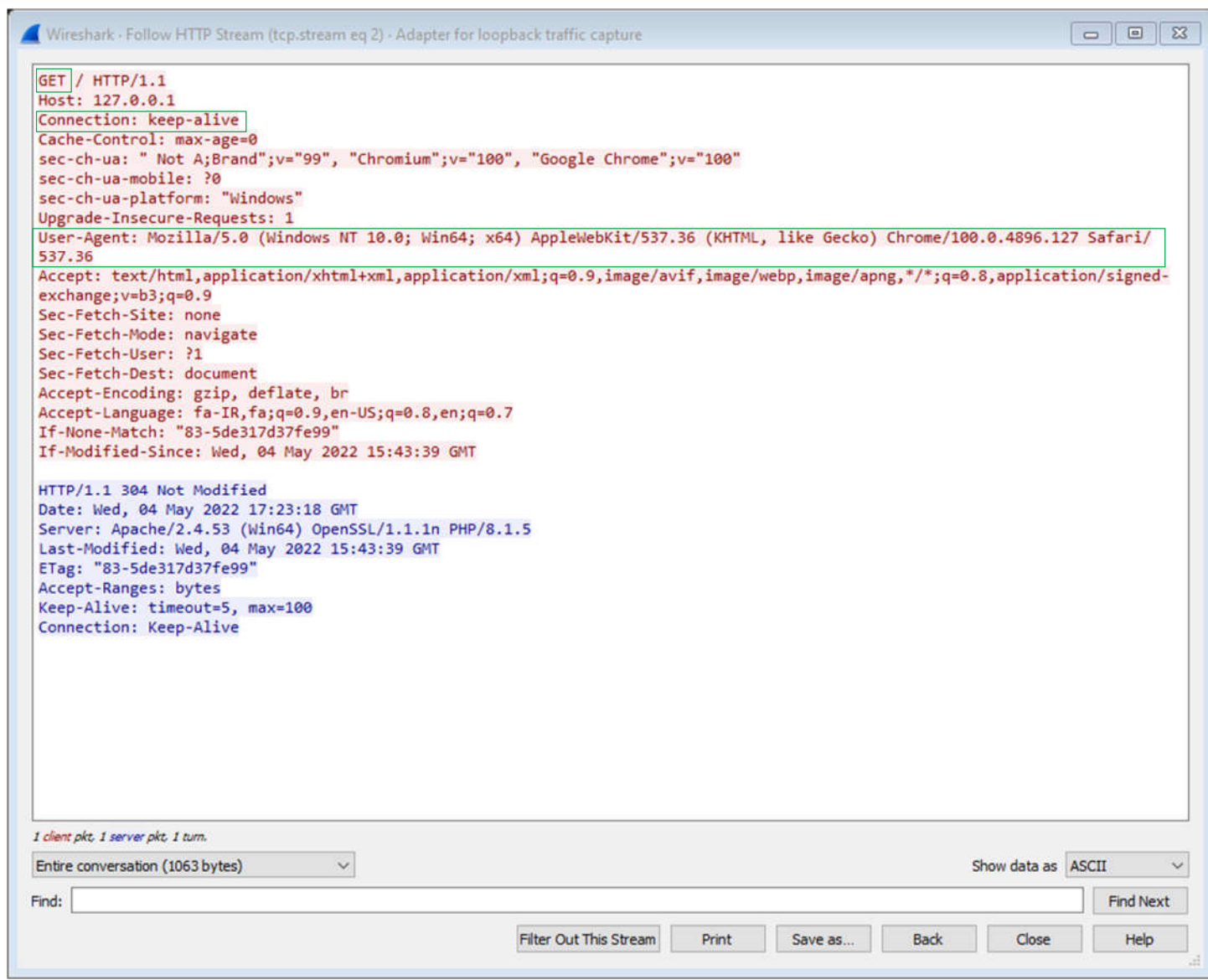
مقدار User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko)

Chrome/100.0.4896.127 Safari/537.36

User agent در حقیقت شبیه به کارت شناسایی است و به web master ها و طراحان وب اجازه می دهد که جزئیات خاصی در مورد مرورگر بازدیدکننده و سیستم عاملی که وی برای مراجعه به سایت استفاده کرده را بررسی کنند و در صورت نیاز، آنچه برای مرورگر کاربر ارسال می شود را به صورت سفارشی، انتخاب و تنظیم کنند. به عنوان مثال سایتی که دو نسخه دستیابی و موبایلی دارد، با توجه به اینکه بازدیدکننده از چه سیستم عامل و مرورگری استفاده می کند، به شکل متفاوتی بارگذاری می شود. در وسایل موبایل نسخه موبایل به صورت پیش فرض لود می شود و در وسایل دستیابی مثل کامپیوتر، موبوک یا لپ تاپ و حتی تبلت های بزرگ، نسخه اصلی سایت یا به عبارتی نسخه Desktop بارگذاری می شود. در نسخه Mobile با صلاح دید طراحی سایت، ممکن است منوها متفاوت باشد، برخی المان ها به شکل متفاوتی طراحی و لود شوند و در مجموع ظاهر سایت برای استفاده در نمایشگر کوچک و لمسی گوشی ها، بهینه شده باشد.

تفاوت بین مرورگرها نیز وجود دارد و ممکن است آنچه در مرورگر قدیمی Internet Explorer بارگذاری می‌شود، با مرورگر مدرنی مثل Google Chrome یا Microsoft Edge اندکی متفاوت باشد و این تفاوت برای حفظ عملکرد و ظاهر سایت ضروری است.

در مثال زیر، مقدار User agent می‌گوید که درخواست از طریق Windows ۶۴ بیتی ارسال شده است و مرورگر هم Chrome بوده است.

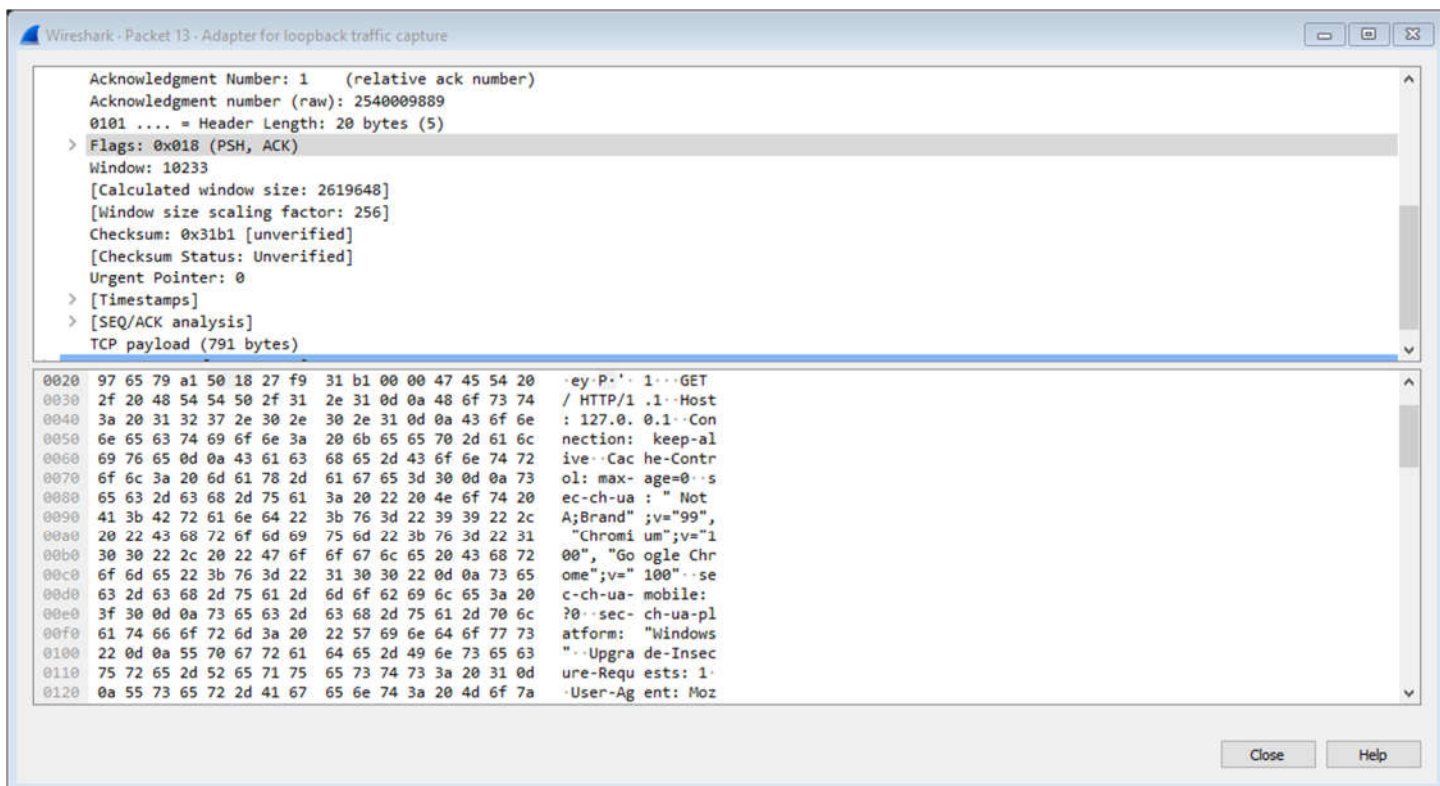


```
GET / HTTP/1.1
Host: 127.0.0.1
Connection: keep-alive
Cache-Control: max-age=0
sec-ch-ua: " Not A;Brand";v="99", "Chromium";v="100", "Google Chrome";v="100"
sec-ch-ua-mobile: ?0
sec-ch-ua-platform: "Windows"
Upgrade-Insecure-Requests: 1
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/100.0.4896.127 Safari/537.36
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/avif,image/webp,image/apng,*/*;q=0.8,application/signed-exchange;v=b3;q=0.9
Sec-Fetch-Site: none
Sec-Fetch-Mode: navigate
Sec-Fetch-User: ?1
Sec-Fetch-Dest: document
Accept-Encoding: gzip, deflate, br
Accept-Language: fa-IR,fa;q=0.9,en-US;q=0.8,en;q=0.7
If-None-Match: "83-5de317d37fe99"
If-Modified-Since: Wed, 04 May 2022 15:43:39 GMT

HTTP/1.1 304 Not Modified
Date: Wed, 04 May 2022 17:23:18 GMT
Server: Apache/2.4.53 (Win64) OpenSSL/1.1.1n PHP/8.1.5
Last-Modified: Wed, 04 May 2022 15:43:39 GMT
ETag: "83-5de317d37fe99"
Accept-Ranges: bytes
Keep-Alive: timeout=5, max=100
Connection: Keep-Alive
```

سوال ۳

مقدار Falgs = 0x018



سوال ۴

پورتی که با پورت ۸۰ ارتباط برقرار می کند، در دو سایت متفاوت است: در اینجا برای aut2.com پورت های 60371 و 60372 برای عملیات های SYN و FIN استفاده شده است.

6	1.964341	127.0.0.1	127.0.0.1	TCP	56 60371 → 80 [SYN] Seq=0 Win=65535 Len=0 MSS=65495 WS=256 SACK_PERM=1
7	1.964455	127.0.0.1	127.0.0.1	TCP	56 80 → 60371 [SYN, ACK] Seq=0 Ack=1 Win=65535 Len=0 MSS=65495 WS=256 SACK_PERM=1
8	1.964567	127.0.0.1	127.0.0.1	TCP	44 60371 → 80 [ACK] Seq=1 Ack=1 Win=2619648 Len=0
9	1.965100	127.0.0.1	127.0.0.1	TCP	56 60372 → 80 [SYN] Seq=0 Win=65535 Len=0 MSS=65495 WS=256 SACK_PERM=1
10	1.965191	127.0.0.1	127.0.0.1	TCP	56 80 → 60372 [SYN, ACK] Seq=0 Ack=1 Win=65535 Len=0 MSS=65495 WS=256 SACK_PERM=1
11	1.965267	127.0.0.1	127.0.0.1	TCP	44 60372 → 80 [ACK] Seq=1 Ack=1 Win=2619648 Len=0
24	8.783569	127.0.0.1	127.0.0.1	TCP	44 60372 → 80 [FIN, ACK] Seq=1 Ack=1 Win=2619648 Len=0
25	8.783672	127.0.0.1	127.0.0.1	TCP	44 80 → 60372 [ACK] Seq=1 Ack=2 Win=2619648 Len=0
26	8.783814	127.0.0.1	127.0.0.1	TCP	44 80 → 60372 [FIN, ACK] Seq=1 Ack=2 Win=2619648 Len=0
27	8.783906	127.0.0.1	127.0.0.1	TCP	44 60371 → 80 [FIN, ACK] Seq=1 Ack=1 Win=2619648 Len=0
28	8.783923	127.0.0.1	127.0.0.1	TCP	44 60372 → 80 [ACK] Seq=2 Ack=2 Win=2619648 Len=0
29	8.784042	127.0.0.1	127.0.0.1	TCP	44 80 → 60371 [ACK] Seq=1 Ack=2 Win=2619648 Len=0
30	8.784072	127.0.0.1	127.0.0.1	TCP	44 80 → 60371 [FIN, ACK] Seq=1 Ack=2 Win=2619648 Len=0
31	8.784137	127.0.0.1	127.0.0.1	TCP	44 60371 → 80 [ACK] Seq=2 Ack=2 Win=2619648 Len=0

برای aut3.com پورت های 60390 و 60391 برای عملیات های SYN و FIN استفاده شده است.

7	2.511873	127.0.0.1	127.0.0.1	TCP	56 60390 → 80 [SYN] Seq=0 Win=65535 Len=0 MSS=65495 WS=256 SACK_PERM=1
8	2.511991	127.0.0.1	127.0.0.1	TCP	56 80 → 60390 [SYN, ACK] Seq=0 Ack=1 Win=65535 Len=0 MSS=65495 WS=256 SACK_PERM=1
9	2.512079	127.0.0.1	127.0.0.1	TCP	44 60390 → 80 [ACK] Seq=1 Ack=1 Win=2619648 Len=0
10	2.512323	127.0.0.1	127.0.0.1	TCP	56 60391 → 80 [SYN] Seq=0 Win=65535 Len=0 MSS=65495 WS=256 SACK_PERM=1
11	2.512412	127.0.0.1	127.0.0.1	TCP	56 80 → 60391 [SYN, ACK] Seq=0 Ack=1 Win=65535 Len=0 MSS=65495 WS=256 SACK_PERM=1
12	2.512479	127.0.0.1	127.0.0.1	TCP	44 60391 → 80 [ACK] Seq=1 Ack=1 Win=2619648 Len=0
13	2.518638	127.0.0.1	127.0.0.1	HTTP	604 GET / HTTP/1.1
14	2.518724	127.0.0.1	127.0.0.1	TCP	44 80 → 60391 [ACK] Seq=1 Ack=561 Win=2619648 Len=0
15	2.525638	127.0.0.1	127.0.0.1	HTTP	316 HTTP/1.1 304 Not Modified
16	2.525711	127.0.0.1	127.0.0.1	TCP	44 60391 → 80 [ACK] Seq=561 Ack=273 Win=2619392 Len=0

23	5.145684	127.0.0.1	127.0.0.1	TCP	44 60390 → 80 [FIN, ACK] Seq=1 Ack=1 Win=2619648 Len=0
24	5.145781	127.0.0.1	127.0.0.1	TCP	44 80 → 60390 [ACK] Seq=1 Ack=2 Win=2619648 Len=0
25	5.145956	127.0.0.1	127.0.0.1	TCP	44 80 → 60390 [FIN, ACK] Seq=1 Ack=2 Win=2619648 Len=0
26	5.146027	127.0.0.1	127.0.0.1	TCP	44 60391 → 80 [FIN, ACK] Seq=561 Ack=273 Win=2619392 Len=0
27	5.146042	127.0.0.1	127.0.0.1	TCP	44 60390 → 80 [ACK] Seq=2 Ack=2 Win=2619648 Len=0
28	5.146147	127.0.0.1	127.0.0.1	TCP	44 80 → 60391 [ACK] Seq=273 Ack=562 Win=2619648 Len=0
29	5.146195	127.0.0.1	127.0.0.1	TCP	44 80 → 60391 [FIN, ACK] Seq=273 Ack=562 Win=2619648 Len=0
30	5.146258	127.0.0.1	127.0.0.1	TCP	44 60391 → 80 [ACK] Seq=562 Ack=274 Win=2619392 Len=0

سوال ۵

گواهی را کشور آمریکا برای آمریکا صادر کرده است (ارگان 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

مدت اعتبار: ۱۰ اکتبر سال ۲۰۲۲

Validity	
Not Before	Sun, 10 Oct 2021 08:59:51 GMT
Not After	Mon, 10 Oct 2022 08:59:51 GMT

کلید عمومی با الگوریتم RSA تولید شده است و مقدار آن در زیر بیان شده است:



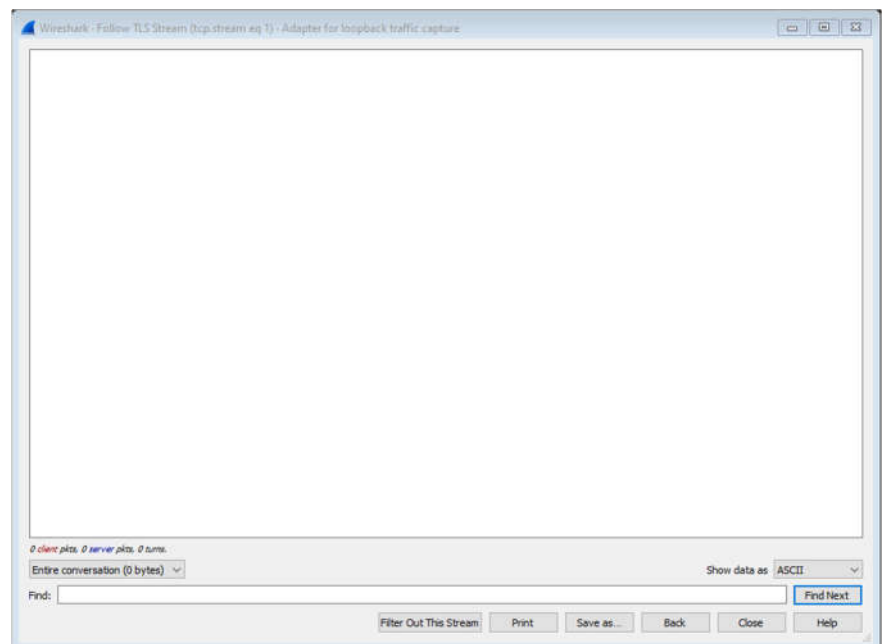
Public Key Info	
Algorithm	RSA
Key Size	2048
Exponent	65537
Modulus	B2:BC:12:AF:D6:02:83:4E:B8:7C:A4:ED:67:1B:E2:E7:72:DE:CD:37:7B:27:B4:8F:14:9E:38:4C:3E:5F:0A:6E:8C:C8:AD:6F:C1:03:FB:1C:D1:9B:32:3F:78:45:1A:AC:98:35:D2:C6:77:50:EB:90:EB:DF:2F:B0:43:89:A0:31:D8:10:9E:0D:F5:1B:1F:3B:0E:16:97:D0:12:2D:DF:CE:E7:BB:0C:50:D9:6B:EF:0A:C9:D8:54:21:D1:84:3B:C5:04:92:8E:BD:1E:C9:BF:57:E6:59:0A:18:08:27:8F:C5:E3:BE:0C:59:44:B7:F7:9A:F9:DF:48:E3:2F:93:6A:6E:81:33:9E:1B:90:0A:0C:C3:85:74:42:EE:11:E0:02:C1:9B:0B:D8:A9:A5:E1:5C:10:18:D6:6C:CF:E8:77:14:B1:AB:75:8A:06:1D:CF:B8:78:1E:94:66:28:F0:5A:14:D5:9B:36:86:F9:72:8D:D9:16:18:40:67:24:D6:FB:87:9C:69:B2:83:2F:75:DF:5F:3A:5C:06:EC:9E:1A:A8:C8:02:A6:D9:DC:36:9F:5A:58:2A:C3:02:3D:CE:D3:28:4D:10:D5:48:ED:49:C8:1A:6A:18:64:78:B0:B3:FD:02:91:62:FC:86:6B:F5:80:BB:C0:53:CE:9E:E0:9D:76:29:1B:E3

امضای دیجیتال با الگوریتم SHA انجام شده است:

Fingerprints	
SHA-256	F9:74:D9:EE:F6:66:F9:FC:CA:7F:FD:39:0A:A1:77:5F:D7:6B:32:37:25:D3:4D:A2:0C:99:D4:84:99:4E:55:DF
SHA-1	8E:AD:5E:DD:31:5E:2E:B3:C0:D6:D8:A9:D6:1F:84:74:58:BE:CC:8E

سوال ۶

خیر، صفحه جزئیات ارتباط خالی است:



با آنکه تمام مراحل handshake به درستی انجام شده است، اما به علت اینکه ارتباط امن نیست و گواهی لازم را نداریم نمیتوان متن ارتباط را خواند.

مراحل handshake.

239	3.787035	127.0.0.1	127.0.0.1	TLSv1.2	561 Client Hello
245	3.795303	127.0.0.1	127.0.0.1	TLSv1.2	1514 Server Hello, Certificate, Server Key Exchange, Server Hello Done
249	3.807153	127.0.0.1	127.0.0.1	TLSv1.2	170 Client Key Exchange, Change Cipher Spec, Encrypted Handshake Message
269	3.811843	127.0.0.1	127.0.0.1	TLSv1.2	95 Change Cipher Spec, Encrypted Handshake Message
303	3.819586	127.0.0.1	127.0.0.1	TLSv1.2	75 Encrypted Alert

سوال ۷

تفاوت ها:

۱. الگوریتم کلید عمومی متفاوتی دارد با سایت ما، و سایز کلید عمومی آن هم متفاوت است

Public Key Info	
Algorithm	Elliptic Curve
Key Size	256
Curve	P-256
Public Value	04:26:EE:04:F8:22:C0:E9:A4:4B:50:FF:E7:B6:A2:E9:90:E5:81:49:4A:ED:41:56:69:3C:6B:E6:61:FD:E3:5D:2E:39:9E:25:B1:73:A1:96:27:60:78:7F:AA:42:62:6C:2E:0C:4A:81:52:6A:F4:B8:F8:29:99:CA:FE:D5:44:EC:29

۲. برخلاف سایت ما، دارای سیاست هایی برای گواهی است

Certificate Policies	
Policy	Certificate Type ( 2.23.140.1.2.1 )
Value	Domain Validation
Policy	Statement Identifier ( 1.3.6.1.4.1 )
Value	1.3.6.1.4.1.11129.2.5.3

۳. دارای Embedded SCT است

Embedded SCTs	
Log 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:2...
Name	Google "Argon2022"
Signature Algorithm	SHA-256 ECDSA
Version	1
Timestamp	Mon, 18 Apr 2022 09:32:25 GMT
Log ID	41:C8:CA:B1:DF:22:46:4A:10:C6:A1:3A:09:42:87:5E:4E:31:8B:1B:03:EB:EB:4B:C7:68:...
Name	Cloudflare "Nimbus2022"
Signature Algorithm	SHA-256 ECDSA
Version	1
Timestamp	Mon, 18 Apr 2022 09:32:25 GMT

۴. دارای CA یعنی Certificate Authority میباشد

### Authority Info (AIA)

Location	<a href="http://ocsp.pki.goog/gts1c3">http://ocsp.pki.goog/gts1c3</a>
Method	Online Certificate Status Protocol (OCSP)
Location	<a href="http://pki.goog/repo/certs/gts1c3.der">http://pki.goog/repo/certs/gts1c3.der</a>
Method	CA Issuers

۵. دارای کلید Authority است

### Authority Key ID

Key ID	8A:74:7F:AF:85:CD:EE:95:CD:3D:9C:D0:E2:46:14:F3:71:35:1D:27
--------	---

۶. تعداد زیادی DNS name دارد

### Subject Alt Names

DNS Name	*.google.com
DNS Name	*.appengine.google.com
DNS Name	*.bdn.dev
DNS Name	*.cloud.google.com
DNS Name	*.crowdsourcing.google.com
DNS Name	*.datacompute.google.com
DNS Name	*.google.ca
DNS Name	*.google.cl
DNS Name	*.google.co.in
DNS Name	*.google.co.jp
DNS Name	*.google.co.uk
DNS Name	*.google.com.ar
DNS Name	*.google.com.au
DNS Name	*.google.com.br
DNS Name	*.google.com.co
DNS Name	*.google.com.mx
DNS Name	*.google.com.tr
DNS Name	*.google.com.vn

۷. بخش های زیر را دارد که سایت ما نداشت

\*.google.com

GTS CA 1C3

GTS Root R1

GlobalSign Root CA



دستور لیست کردن فایل های دایرکتوری: CWD

نام کاربری: test

پروتکل لایه TCP:Transport

آدرس پورت مبدا و مقصد: 127.0.0.1