

راهنمای Web و FTP

۱

9	21.503630	127.0.0.1	127.0.0.1	HTTP	593 GET / HTTP/1.1
10	21.503630	127.0.0.1	127.0.0.1	TCP	40 80 → 3081 [ACK] Seq=1 Ack=554 Win=26196
11	21.505624	127.0.0.1	127.0.0.1	HTTP	244 HTTP/1.1 304 Not Modified
12	21.505624	127.0.0.1	127.0.0.1	TCP	40 3081 → 80 [ACK] Seq=554 Ack=205 Win=261
13	21.505624	127.0.0.1	127.0.0.1	TCP	40 80 → 3081 [ACK] Seq=1 Ack=554 Win=261

> Frame 9: 593 bytes on wire (4744 bits), 593 bytes captured (4744 bits)
Raw packet data
> Internet Protocol Version 4, Src: 127.0.0.1, Dst: 127.0.0.1
> Transmission Control Protocol, Src Port: 3081, Dst Port: 80, Seq: 1, Ack: 1, Len: 553
> Hypertext Transfer Protocol

مبدأ: ۳۰۸۱

مقصد: ۸۰

در بسته ی انتخابی پورت مبدأ ۲۱۱۷ و پورت مقصد ۸۰ است . روند برقراری ارتباط در HTTP به این صورت است که ابتدا کلاینت درخواست ارتباط TCP به سرور که بر روی پورت ۸۰ در حال گوش کردن است میفرستد و سپس سرور به کلاینت پاسخ داده و ارتباط TCP برقرار میشود. پس از برقراری ارتباط سرور شی هایی که کلاینت درخواست کرده را برای او میفرستد و در نهایت ارتباط را میبندد . شایان ذکر است که اگر ارتباط keep alive باشد برای ارسال تمامی اشیا درخواست شده تنها یک بار بین سرور و کلاینت ارتباط TCP برقرار شده و در نهایت ارتباط بسته میشود . اما اگر از نوع keep alive نباشد (non-persistent) برای ارسال هر شی به برقراری یک ارتباط جدید نیاز داریم چرا که در این نوع از ارتباط سرور بعد از هر بار ارسال شی، connection را میبندد و برای شی جدید به connection جدید نیاز است . آدرس وب سایت درخواستی در header request ای که کلاینت به سرور میفرستد موجود است .

نام وبسایت یعنی www.aut2.ac.ir توسط فایل hosts روی 127.0.0.1 مپ شده.

۲

نوع: GET

کانکشن: keep-alive

User-Agent

اطلاعاتی را درباره ی برنامه و همچنین سیستم عاملی که درخواست را به سمت سرور ارسال کرده است و مسئول دریافت و نمایش محتوای http است را در اختیار ما قرار میدهد.

```
GET / HTTP/1.1
Host: www.aut2.ac.ir
Connection: keep-alive
Cache-Control: max-age=0
Upgrade-Insecure-Requests: 1
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like
Gecko) Chrome/90.0.4430.212 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
Accept-Encoding: gzip, deflate
Accept-Language: en-US,en;q=0.9,fa;q=0.8
If-None-Match: "93-5c03af8dbf84e"
If-Modified-Since: Sun, 18 Apr 2021 08:26:39 GMT
```

```
HTTP/1.1 304 Not Modified
Date: Mon, 17 May 2021 12:37:32 GMT
Server: Apache/2.4.41 (Win64) OpenSSL/1.1.1c PHP/7.4.2
Connection: Keep-Alive
Keep-Alive: timeout=5, max=100
ETag: "93-5c03af8dbf84e"
```

```
GET / HTTP/1.1
Host: www.aut2.ac.ir
Connection: keep-alive
Cache-Control: max-age=0
Upgrade-Insecure-Requests: 1
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like
Gecko) Chrome/90.0.4430.212 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
Accept-Encoding: gzip, deflate
Accept-Language: en-US,en;q=0.9,fa;q=0.8
If-None-Match: "93-5c03af8dbf84e"
If-Modified-Since: Sun, 18 Apr 2021 08:26:39 GMT
```

```
HTTP/1.1 304 Not Modified
Date: Mon, 17 May 2021 12:37:32 GMT
Server: Apache/2.4.41 (Win64) OpenSSL/1.1.1c PHP/7.4.2
Connection: Keep-Alive
Keep-Alive: timeout=5, max=100
ETag: "93-5c03af8dbf84e"
```

۳

```

Flags: 0x002 (SYN)
 000. .... = Reserved: Not set
...0 .... = Nonce: Not set
.... 0... = Congestion Window Reduced (CWR): Not set
.... .0.. = ECN-Echo: Not set
.... ..0. = Urgent: Not set
.... ...0 = Acknowledgment: Not set
.... .... 0... = Push: Not set
.... ..... .0.. = Reset: Not set
> .... .... ..1. = Syn: Set
.... .... ...0 = Fin: Not set
[TCP Flags: .....S.]

```

۴

لایه انتقال:

Source Port: 20340 Destination Port: 80 [Stream index: 0] [TCP Segment Len: 348] Sequence number: 1 (relative sequence number) Sequence number (raw): 2808739529 [Next sequence number: 349 (relative sequence number)] Acknowledgment number: 1 (relative ack number) Acknowledgment number (raw): 4170156556	Source Port: 20195 Destination Port: 80 [Stream index: 0] [TCP Segment Len: 348] Sequence number: 1 (relative sequence number) Sequence number (raw): 3706744083 [Next sequence number: 349 (relative sequence number)] Acknowledgment number: 1 (relative ack number) Acknowledgment number (raw): 4115294677
----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------	----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------

لایه شبکه:

Total Length: 388 Identification: 0x1c0a (7178) Flags: 0x4000, Don't fragment	Total Length: 388 Identification: 0x1bf8 (7160) Flags: 0x4000, Don't fragment
-------------------------------------------------------------------------------------	-------------------------------------------------------------------------------------

بالترین لایه:

[Time shift for this packet: 0.000000000 seconds] Epoch Time: 1606657888.165341000 seconds [Time delta from previous captured frame: 0.058075000 seconds] [Time delta from previous displayed frame: 0.059659000 seconds] [Time since reference or first frame: 4.860203000 seconds] Frame Number: 19	[Time shift for this packet: 0.000000000 seconds] Epoch Time: 1606657840.749128000 seconds [Time delta from previous captured frame: 0.054865000 seconds] [Time delta from previous displayed frame: 0.055223000 seconds] [Time since reference or first frame: 4.168054000 seconds] Frame Number: 20
----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------	----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------



Certificate	
localhost	
Subject Name	
Common Name	localhost
Issuer Name	
Common Name	The original certificate provided by the web server is untrusted.
Validity	
Not Before	Tue, 10 Nov 2009 23:48:47 GMT
Not After	Fri, 08 Nov 2019 23:48:47 GMT
Public Key Info	
Algorithm	RSA
Key Size	1024
Exponent	65537
Modulus	B2:A6:AC:0E:66:F6:E6:ED:41:A2:6A:80:36:16:68:5B:B4:F0:BD:F9:17:83:...
Miscellaneous	
Serial Number	72:75:85:67:50:84:94:A6:D0:43:99:F8:F7:A8:A9:7A
Signature Algorithm	SHA-1 with RSA Encryption
Version	3
Download	PEM (cert) PEM (chain)
Fingerprints	
SHA-256	19:70:CD:34:26:48:2B:D8:E6:37:75:1A:A7:57:C1:FA:D2:EE:2A:15:94:5B:...
SHA-1	D2:08:9A:44:CA:30:0D:C3:90:13:54:D1:DB:E2:FD:02:C9:49:F7:AB
🔑 Key Usages	
Purposes	Digital Signature, Key Encipherment

گواهی را localhost برای localhost صادر کرده است.

زمان اعتبار در عکس نشان داده شده

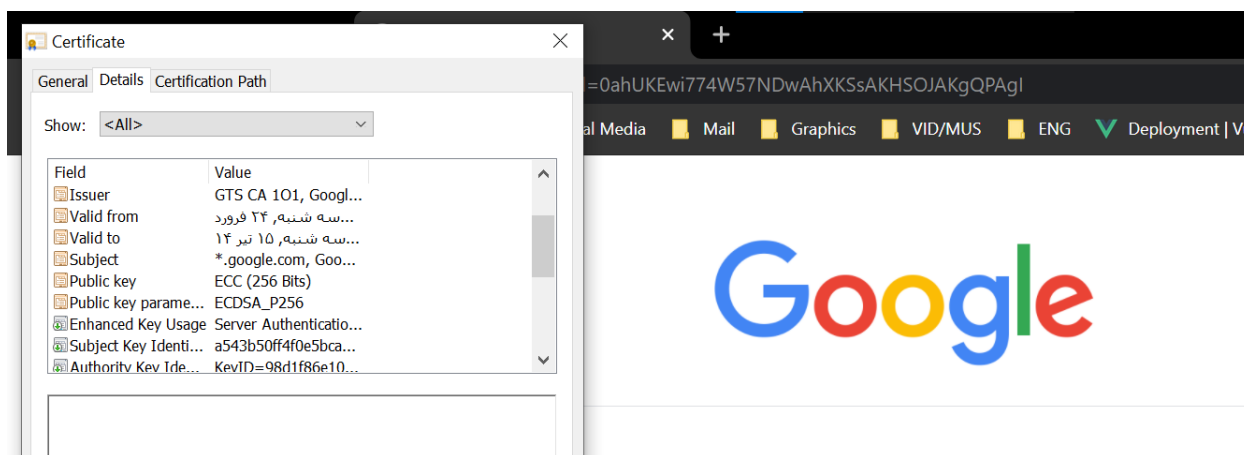
کلید عمومی الگوریتم RSA با $\text{key size} = 1024$ است .

امضای دیجیتال از الگوریتم SHA-1 with RSA Encryption استفاده میکند.

۶

متن ارتباط دیده نمیشود چرا که گواهی آن اعتبار ندارد و wireshark نتوانسته است اطلاعات session را که encrypt شده اند را decrypt کند

۷



این گواهی با گواهی ما تفاوت های بسیاری دارد از جمله اینکه این گواهی معتبر است و از ۱۰۱ CA GTS Service Trust به Google اعطا شده است . همچنین الگوریتم امضای الکترونیکی آن و الگوریتم و ساینز public key آن و تاریخ اعطای گواهی و انقضای آن نیز با گواهی ما متفاوت است.

۸

```
LIST\r\n
Request command: LIST
```

از دستور LIST برای لیست کردن فایل های دایرکتوری استفاده شده است . از نام کاربری test با رمز ۱۲۳ برای دسترسی به سایت استفاده شده است . پرتکل الیه ی transport برای این بسته ها TCP است . پورت مبدا ۷۶۴۹ و پورت مقصد ۲۱ است.

```

> Frame 318: 55 bytes on wire (440 bits), 55 bytes captured (440 bits) on interface \Device\NPF_{Loopback, id 0
> Null/Loopback
> Internet Protocol Version 4, Src: 127.0.0.1, Dst: 127.0.0.1
> Transmission Control Protocol, Src Port: 7649, Dst Port: 21, Seq: 1, Ack: 149, Len: 11
+ File Transfer Protocol (FTP)
  + USER test\r\n
    Request command: USER
    Request arg: test
    [Current working directory: ]

```

خیر چرا که تنظیمات `ssl` را فعال کردیم.

خیر، در این حالت نام کاربری و رمز عبور قابل خواندن نیست.

html

```
text/html,application/xhtml+xml,application/xml;q=0.9,image/webp,image/apng,*/*;q=0.8,application/signed-exchange;v=b3;q=0.9
```

Accept-Encoding: gzip, deflate
 Accept-Language: en-US,en;q=0.9,fa;q=0.8
 Cookie: _ga=GA1.3.1799390975.1609054157

HTTP/1.1 301 Moved Permanently
 Date: Mon, 17 May 2021 14:52:37 GMT
 Server: Apache
 Location: https://aut.ac.ir:443/
 Content-Length: 230
 Keep-Alive: timeout=15, max=100
 Connection: Keep-Alive
 Content-Type: text/html; charset=iso-8859-1

```
<!DOCTYPE HTML PUBLIC "-//IETF//DTD HTML 2.0//EN">
<html><head>
<title>301 Moved Permanently</title>
</head><body>
<h1>Moved Permanently</h1>
<p>The document has moved <a href="https://aut.ac.ir:443/">here</a>.</p>
</body></html>
```

مقدار connection برابر keep-alive و درخواست GET ست. مقدار user-agent پررنگ شده.

این مقدار اطلاعاتی را درباره ی برنامه و همچنین سیستم عاملی که درخواست را به سمت سرور ارسال کرده است و مسئول دریافت و نمایش محتوای http است را در اختیار ما قرار میدهد.

مقدار فلگ:

```
▼ 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...]
```


FTP

9683	48.277683	195.83.118.1	192.168.1.5	FTP	1038 Response:
9684	48.278565	192.168.1.5	195.83.118.1	FTP	70 Request: USER anonymous
9707	48.374210	195.83.118.1	192.168.1.5	FTP	103 Response: 331 Guest login ok, type your name as password.
9708	48.374732	192.168.1.5	195.83.118.1	FTP	79 Request: PASS chrome@example.com
9728	48.507420	195.83.118.1	192.168.1.5	FTP	60 Response: 230-
10027	50.150954	195.83.118.1	192.168.1.5	FTP	395 Response: \tVous etes dans la classe guest,
10028	50.151461	192.168.1.5	195.83.118.1	FTP	60 Request: SYST
10051	50.250627	195.83.118.1	192.168.1.5	FTP	103 Response: 215 UNIX Type: L8 Version: NetBSD-ftp 20110904
10052	50.251105	192.168.1.5	195.83.118.1	FTP	59 Request: PWD
10073	50.406890	195.83.118.1	192.168.1.5	FTP	89 Response: 257 /* is the current directory.
10074	50.407297	192.168.1.5	195.83.118.1	FTP	62 Request: TYPE I
10103	50.500256	195.83.118.1	192.168.1.5	FTP	74 Response: 200 Type set to I.
10104	50.500764	192.168.1.5	195.83.118.1	FTP	62 Request: SIZE /
10134	50.670713	195.83.118.1	192.168.1.5	FTP	80 Response: 550 /: not a plain file.
10136	50.671224	192.168.1.5	195.83.118.1	FTP	61 Request: CWD /
10158	50.780312	195.83.118.1	192.168.1.5	FTP	83 Response: 250 CWD command successful.

> Frame 9664: 60 bytes on wire (480 bits), 60 bytes captured (480 bits) on interface \Device\NPF_{408CA59C-FD6A-4AD5-8626-D7887268EFF3}, id 0

> Ethernet II, Src: MDL_c9:3f (bc:34:00:50:c9:3f), Dst: IntelCor_c7:29:96 (68:ec:c5:c7:29:96)

> Internet Protocol Version 4, Src: 195.83.118.1, Dst: 192.168.1.5

✓ Transmission Control Protocol, Src Port: 21, Dst Port: 51513, Seq: 1, Ack: 1, Len: 6

Source Port: 21

Destination Port: 51513

[Stream index: 33]

[TCP Segment Len: 6]

Sequence number: 1 (relative sequence number)

Sequence number (raw): 47460282

[Next sequence number: 7 (relative sequence number)]

Acknowledgment number: 1 (relative ack number)

Acknowledgment number (raw): 3995671662

0101 = Header Length: 20 bytes (5)

> Flags: 0x018 (PSH, ACK)

Window size value: 513

[Calculated window size: 65664]

پرتکل لایه ی transport این بسته ها TCP است.

پورت مبدا ۲۱ و پورت مقصد ۵۱۵۱۳ می باشد . مقدار username ، password و مقدار chrome@example.com می باشد که همگی در شکل قابل مشاهده می باشند.