-	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=2619€			
4	11 21.505624 127.0.0.1 127.0.		127.0.0.1	HTTP	244 HTTP/1.1 304 Not Modified			
	12 21.505624	127.0.0.1	127.0.0.1	TCP 46	40 3081 → 80 [ACK] Seq=554 Ack=205 Win=261			
<	12 26 512210	107 0 0 1	107 0 0 1	TCD	40 00 3004 FETN 46K3 5 30F 4-1/ FF4 112			
> F	Frame 9: 593 bytes on wire (4744 bits), 593 bytes captured (4744 bits)							
R	Raw packet data							
> I	Internet Protocol Version 4, Src: 127.0.0.1, Dst: 127.0.0.1							
> T	Transmission Control Protocol, Src Port: 3081, Dst Port: 80, Seq: 1, Ack: 1, Len: 553							
> H	Hypertext Transfer Protocol							

مبدا: ۳۰۸۱

مقصد: ۸۰

در بسته ی انتخابی پورت مبدا 117 و پورت مقصد 10 است . روند برقراری ارتباط در HTTP به این صورت است که ابتدا کلاینت درخواست ارتباط TCP به سرور که بر روی پورت 10 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 seep alive باشد برای ارسال تمامی اشیا درخواست شده تنها یک بار بین سرور و کالینت ارتباط 10 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، header request میبندد و برای شی جدید به connection جدید نیاز است . آدرس وب سایت درخواستی در beader request ای که کلاینت به سرور میفرستد موجود است .

نام وبسايت يعني <u>www.aut2.ac.ir</u> توسط فايل hosts روى 127.0.0.1 مي شده.



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"

```
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
```

[TCP Flags: ······S·]



لايه انتقال:

```
Source Port: 20340

Destination Port: 80

[Stream index: 0]

[TCP Segment Len: 348]

Sequence number: 1 (relative sequence number)

Sequence number: 28083739529

[Next sequence number: 349 (relative sequence number)]

Acknowledgment number: 1 (relative ack number)

Acknowledgment number (raw): 4170156556

Source Port: 2015

Destination Port: 80

[Stream index: 0]

[TCP Segment Len: 348]

Sequence number: 1 (relative sequence number)

Sequence number: 1 (relative sequence number)

Sequence number: 3706744083

[Next sequence number: 349 (relative sequence number)]

Acknowledgment number: 1 (relative ack number)

Acknowledgment number: 1 (relative ack number)

Acknowledgment number (raw): 4170156556
```

لايه شبكه:

Total Length: 388	Total Length: 388
Identification: 0x1c0a (7178)	Identification: 0x1bf8 (7160)
▶ Flags: 0x4000, Don't fragment	▶ Flags: 0x4000, Don't fragment
Format officer o	Formula official A

بالاترين لايه:

```
[Time shift for this packet: 0.000000000 seconds]

Epoch Time: 1606657888.165341000 seconds

[Time delta from previous captured frame: 0.058875000 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: 0.0000000000 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
```

۵

Certificate				
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 Exponent	1024 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 Download	3 PEM (cert) PEM (chain)			
Fingerprints				
SHA-256 SHA-1	19:70:CD:34:26:48:2B:D8:E6:37:75:1A:A7:57:C1:FA:D2:EE:2A:15:94:5B 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

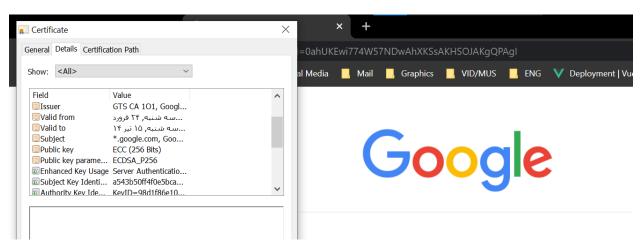
كليد عمومي الگوريتم RSA با key size = 1024 است .

امضاى ديجيتال از الگوربتم SHA-1 with RSA Encryption استفاده ميكند.

٦

متن ارتباط دیده نمیشود چرا که گواهی آن اعتبار ندارد و wireshark نتوانسته است اطالعات session را که encrypt شده اند را decryptکند





این گواهی با گواهی ما تفاووت های بسیاری دارد از جمله اینکه این گواهی معتبر است و از , ۲۰۱ CA GTS Service Trust (باین گواهی معتبر است و ان پستان و تاریخ Google اعطا شده است . همچنین الگوریتم امضای الکترونیکی آن و الگوریتم و سایز public key آن و تاریخ اعطای گواهی و انقضای آن نیز با گواهی ما متفاوت است.



▲ 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 . پورت مبدا ۷۶۴۹ و پورت مقصد ۲۱ سایت استفاده شده است . پرتکل الیه ی transport برای این بسته ها TCP است . پورت مبدا ۷۶۴۹ و پورت مقصد ۲۱ است.

322 72.697309	127.0.0.1	127.0.0.1	FTP	76 Response: 331 Password required for test
325 72.697344	127.0.0.1	127.0.0.1	FTP	54 Request: PASS 123
330 72.697449	127.0.0.1	127.0.0.1	FTP	59 Response: 230 Logged on
334 72.697498	127.0.0.1	127.0.0.1	FTP	58 Request: opts utf8 on
338 72.697561	127.0.0.1	127.0.0.1	FTP	67 Response: 200 UTF8 mode enabled
344 72.697609	127.0.0.1	127.0.0.1	FTP	50 Request: syst
346 72.697701	127.0.0.1	127.0.0.1	FTP	76 Response: 215 UNIX emulated by FileZilla
351 72.697753	127.0.0.1	127.0.0.1	FTP	55 Request: site help
354 72.697826	127.0.0.1	127.0.0.1	FTP	92 Response: 504 Command not implemented for that parameter
358 72 697862	127 0 0 1	127 0 0 1	FTP	49 Request PMD

- 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:]

9

خير چرا كه تنظيمات ادا و فعال كرديم.

1.

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

347 20.258602	127.0.0.1	127.0.0.1	FTP	97 Request: \027\003\001\0000���7a"�Z��\031T \t\002ps"��k���*���\177\017�Z�\035\034��\057
349 20.259212	127.0.0.1	127.0.0.1	FTP	113 Response: \027\093\091\090@\$@\@\$ 2<n\$\004\\002\$&<r\$\$uA+v\$\b \$\$\031\$5\$\$\$</td
351 20.259370	127.0.0.1	127.0.0.1	FTP	81 Request: \027\003\001\000 X�:10Kj���F��\037\X�VI}�10�:�I#
353 20,299981	127.0.0.1	127.0.0.1	FTP	97 Response: \827\883\881\8888\cil\chi,\chi\chi\chi\chi\chi\chi\chi\chi\chi\chi
355 20.300265	127.0.0.1	127.0.0.1	FTP	81 Request: \027\003\0031\000 u
357 20.300639	127.0.0.1	127.0.0.1	PTP	113 Response: \027\003\001\0000\01\0000\01\0000\01\0000\01\01\
359 29,300823	127.0.0.1	127.0.0.1	FTP	81 Request: \027\003\001\000 ��fp)�/��\016\017�
361 20.301510	127.0.0.1	127.0.0.1	FTP	626 Response: \827\883\881\8808(8% \ \ \ \ \ \ \ \ \ \ \ \ \ \ \ \ \ \ \
363 20.301791	127.0.0.1	127.0.0.1	FTP	81 Request; \027\003\001\000 \q\\\\\\\\\\\\\\\\\\\\\\\\\\\\\
365 20.302019	127.0.0.1	127.0.0.1	FTP	97 Response: \827\883\881\8808P���\881nl�N\824gu����d��f�F\835\\837����c�9\826���h\886/\b��
367 29.302137	127.0.0.1	127.0.0.1	FTP	81 Request: \027\003\001\000 \0\022Fp\05\0
369 20.302390	127.0.0.1	127.0.0.1	FTP	113 Response: \027\001\000@�r�"\017R�7Q�
371 20.304091	127.0.0.1	127.0.0.1	FTP	81 Request: \027\003\001\000 \036\08\0(6\0000x\0252s\000000007H\000000000000000000000000000
373 20.304671	127.0.0.1	127.0.0.1	FTP	113 Response: \027\003\001\0000\0000\0000\0000\0000\0000\
375 20.385709	127.0.0.1	127.0.0.1	FTP	81 Request: \827\883\881\898 \\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\
377 20.306357	127.0.0.1	127.0.0.1	FTP	97 Response: \027\003\001\0000\000\000\000\000\000\000\00
379 20.386539	127.0.0.1	127.0.0.1	PTP	51 Request: \027\003\001\000 :\033��a�\027AT�R��\036�H�8\004K\0251�Yu�Y;����
381 29.307203	127.0.0.1	127.0.0.1	FTP	129 Response: \@27\@83\@81\@80P�o\vy∳\$\823♦♦V∲g\a∳♦\\$\177♦♦♦\@80#~_5
384 20.331186	127.0.0.1	127.0.0.1	FTP	81 Request: \027\003\001\000 t\09\fap)\023Y\003\V8J\08\024\033[F\01t\000]t\000]
393 20.390867	127.0.0.1	127.0.0.1	FTP	97 Response: \027\093\001\0908+\pa\031\091\P\026X\a\rightarrowY=h\$\phi\rightarrow65\phi\rightarrow\chi\rightarrow
404 20.392565	127.0.0.1	127.0.0.1	FTP	97 Response: \027\003\001\0000< \001\0000 \0000
4592 141 313711	127 0 0 1	127 8 8 1	FTP	13d Secondar 1977 1997 1997 1999 A. () 1975 1974 A. () 1974 A. () 1974 A. () 1975 A. () 1

html

GET / HTTP/1.1

Host: aut.ac.ir

Connection: keep-alive

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 Edg/90.0.818.62

Accept:

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>
The document has moved <a href="https://aut.ac.ir:443/">here</a>.
```

</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 ... = Reset: Not set
    .....0 = Syn: Not set
    .....0 = Fin: Not set
    .....0 = Fin: Not set
```

FTP

```
9683 48.277683
                     195.83.118.1
                                         192.168.1.5
                                                                       1038 Response:
   9684 48.278565
                    192,168,1,5
                                         195.83.118.1
                                                             FTP
                                                                        70 Request: USER anonymous
   9797 48.374210
                    195.83.118.1
                                         192.168.1.5
                                                             FTP
                                                                        103 Response: 331 Guest login ok, type your name as password.
   9798 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-
                                                             FTP
                                                                                       \tVous etes dans la classe guest,
  10027 50.150954
                    195.83.118.1
                                         192, 168, 1, 5
                                                                        395 Response:
                                                             FTP
                                                                        60 Request: SYST
  10028 50.151461
                    192.168.1.5
                                         195.83.118.1
  10051 50.250627
                    195.83.118.1
                                         192.168.1.5
                                                             FTP
                                                                        103 Response: 215 UNIX Type: L8 Version: NetBSD-ftpd 20110904
   10052 50.251105
                                                              FTP
                     192.168.1.5
                                          195.83.118.1
                                                                       89 Response: 257 */* is the current directory.
  10073 50.406890 195.83.118.1
                                        192.168.1.5
                                                             FTP
  10074 50 407297
                     192.168.1.5
                                         195.83.118.1
                                                             ETP
                                                                         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
                                         195.83.118.1
                                                              FTP
                                                                         62 Request: SIZE /
                    192.168.1.5
  10134 50.670713
                     195.83.118.1
                                         192.168.1.5
                                                             FTP
                                                                        80 Response: 550 /: not a plain file.
                                                             FTP
                                                                        61 Request: CWD /
  10136 50.671224
                    192.168.1.5
                                         195.83.118.1
  10158 50.780312
                   195.83.118.1
                                         192.168.1.5
                                                             FTP
                                                                         83 Response: 250 CMD command successful.
Frame 9664: 60 bytes on wire (480 bits), 60 bytes captured (480 bits) on interface \Device\NPF_4488CA59C-FD6A-4AD5-8626-D788726BEFF3], id 0
> Ethernet II, Src: NDSL_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
v 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]
                        (relative sequence number)
    Sequence number: 1
    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
```

پرتکل لابه ی transport این بسته ها TCP است.

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

[Calculated window size: 65664]