به نام ایزد یکتا

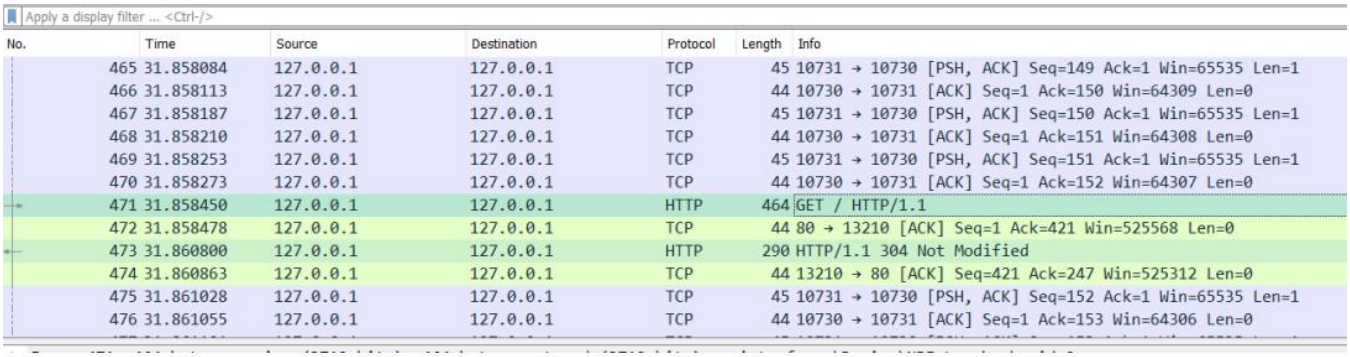


# آزمایش سوم درس آزمایشگاه شبکه‌های کامپیوتری

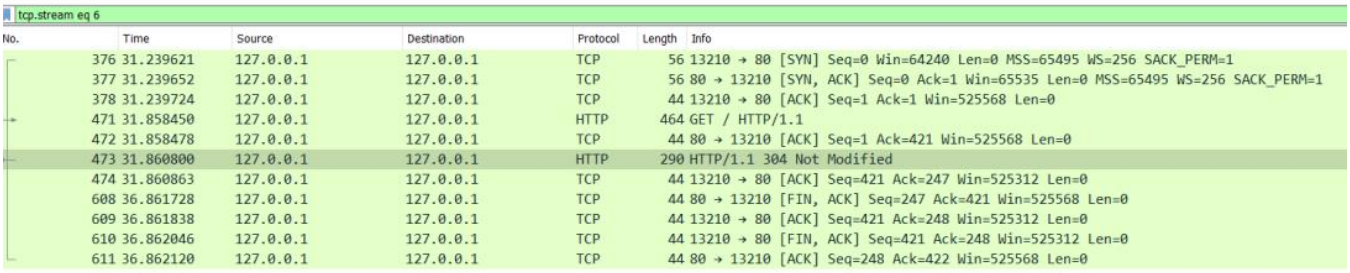
گروه دوم

تهیه کننده: بردیا اردکانیان

۹۸۳۱۰۷۲

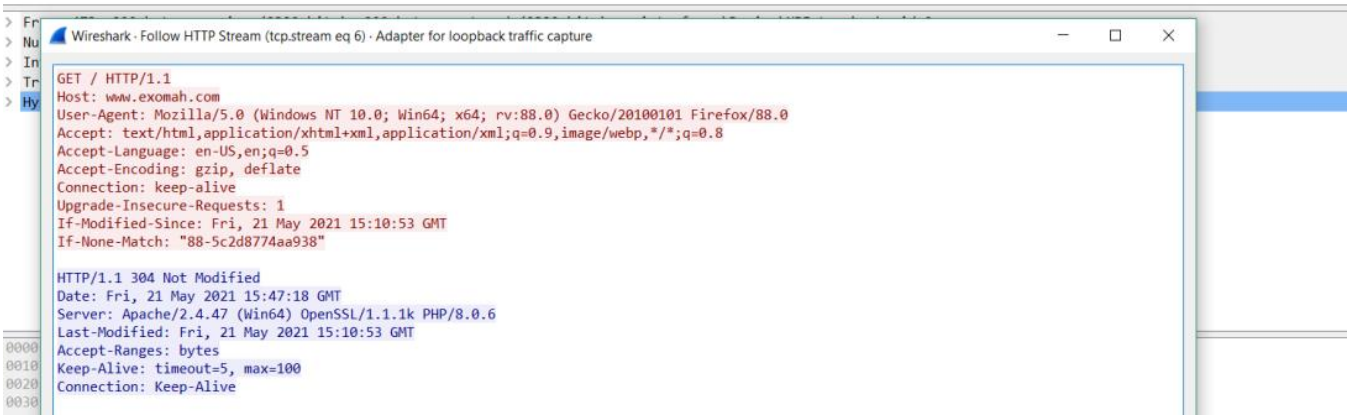


| No. | Time | Source | Destination | Protocol | Length | Info |
|---|---|---|---|---|---|---|
| 465 | 31.858084 | 127.0.0.1 | 127.0.0.1 | TCP | 45 | 10731 → 10730 [PSH, ACK] Seq=149 Ack=1 Win=65535 Len=1 |
| 466 | 31.858113 | 127.0.0.1 | 127.0.0.1 | TCP | 44 | 10730 → 10731 [ACK] Seq=1 Ack=150 Win=64309 Len=0 |
| 467 | 31.858187 | 127.0.0.1 | 127.0.0.1 | TCP | 45 | 10731 → 10730 [PSH, ACK] Seq=150 Ack=1 Win=65535 Len=1 |
| 468 | 31.858210 | 127.0.0.1 | 127.0.0.1 | TCP | 44 | 10730 → 10731 [ACK] Seq=1 Ack=151 Win=64308 Len=0 |
| 469 | 31.858253 | 127.0.0.1 | 127.0.0.1 | TCP | 45 | 10731 → 10730 [PSH, ACK] Seq=151 Ack=1 Win=65535 Len=1 |
| 470 | 31.858273 | 127.0.0.1 | 127.0.0.1 | TCP | 44 | 10730 → 10731 [ACK] Seq=1 Ack=152 Win=64307 Len=0 |
| 471 | 31.858450 | 127.0.0.1 | 127.0.0.1 | HTTP | 464 | GET / HTTP/1.1 |
| 472 | 31.858478 | 127.0.0.1 | 127.0.0.1 | TCP | 44 | 80 → 13210 [ACK] Seq=1 Ack=421 Win=525568 Len=0 |
| 473 | 31.860800 | 127.0.0.1 | 127.0.0.1 | HTTP | 290 | HTTP/1.1 304 Not Modified |
| 474 | 31.860863 | 127.0.0.1 | 127.0.0.1 | TCP | 44 | 13210 → 80 [ACK] Seq=421 Ack=247 Win=525312 Len=0 |
| 475 | 31.861028 | 127.0.0.1 | 127.0.0.1 | TCP | 45 | 10731 → 10730 [PSH, ACK] Seq=152 Ack=1 Win=65535 Len=1 |
| 476 | 31.861055 | 127.0.0.1 | 127.0.0.1 | TCP | 44 | 10730 → 10731 [ACK] Seq=1 Ack=153 Win=64306 Len=0 |



tcp.stream eq 6

| No. | Time | Source | Destination | Protocol | Length | Info |
|---|---|---|---|---|---|---|
| 376 | 31.239621 | 127.0.0.1 | 127.0.0.1 | TCP | 56 | 13210 → 80 [SYN] Seq=0 Win=64240 Len=0 MSS=65495 WS=256 SACK_PERM=1 |
| 377 | 31.239652 | 127.0.0.1 | 127.0.0.1 | TCP | 56 | 80 → 13210 [SYN, ACK] Seq=0 Ack=1 Win=65535 Len=0 MSS=65495 WS=256 SACK_PERM=1 |
| 378 | 31.239724 | 127.0.0.1 | 127.0.0.1 | TCP | 44 | 13210 → 80 [ACK] Seq=1 Ack=1 Win=525568 Len=0 |
| 471 | 31.858450 | 127.0.0.1 | 127.0.0.1 | HTTP | 464 | GET / HTTP/1.1 |
| 472 | 31.858478 | 127.0.0.1 | 127.0.0.1 | TCP | 44 | 80 → 13210 [ACK] Seq=1 Ack=421 Win=525568 Len=0 |
| 473 | 31.860800 | 127.0.0.1 | 127.0.0.1 | HTTP | 290 | HTTP/1.1 304 Not Modified |
| 474 | 31.860863 | 127.0.0.1 | 127.0.0.1 | TCP | 44 | 13210 → 80 [ACK] Seq=421 Ack=247 Win=525312 Len=0 |
| 608 | 36.861728 | 127.0.0.1 | 127.0.0.1 | TCP | 44 | 80 → 13210 [FIN, ACK] Seq=247 Ack=421 Win=525568 Len=0 |
| 609 | 36.861838 | 127.0.0.1 | 127.0.0.1 | TCP | 44 | 13210 → 80 [ACK] Seq=421 Ack=248 Win=525312 Len=0 |
| 610 | 36.862046 | 127.0.0.1 | 127.0.0.1 | TCP | 44 | 13210 → 80 [FIN, ACK] Seq=421 Ack=248 Win=525312 Len=0 |
| 611 | 36.862120 | 127.0.0.1 | 127.0.0.1 | TCP | 44 | 80 → 13210 [ACK] Seq=248 Ack=422 Win=525568 Len=0 |

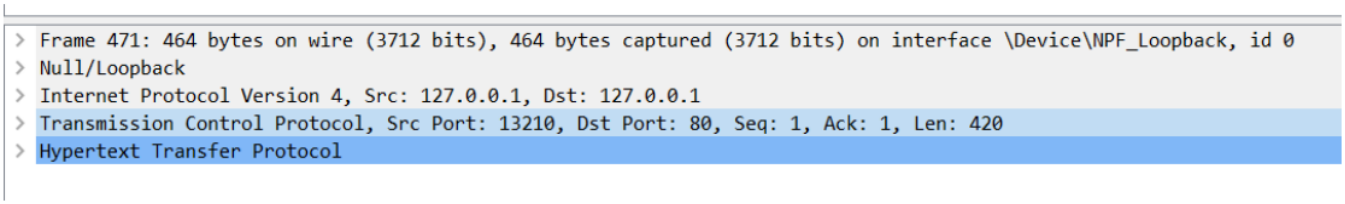


Wireshark · Follow HTTP Stream (tcp.stream eq 6) · Adapter for loopback traffic capture

```
GET / HTTP/1.1
Host: www.exomah.com
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64; rv:88.0) Gecko/20100101 Firefox/88.0
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/webp,*/*;q=0.8
Accept-Language: en-US,en;q=0.5
Accept-Encoding: gzip, deflate
Connection: keep-alive
Upgrade-Insecure-Requests: 1
If-Modified-Since: Fri, 21 May 2021 15:10:53 GMT
If-None-Match: "88-5c2d8774aa938"

HTTP/1.1 304 Not Modified
Date: Fri, 21 May 2021 15:47:18 GMT
Server: Apache/2.4.47 (Win64) OpenSSL/1.1.1k PHP/8.0.6
Last-Modified: Fri, 21 May 2021 15:10:53 GMT
Accept-Ranges: bytes
Keep-Alive: timeout=5, max=100
Connection: Keep-Alive
```

سوال ۱)



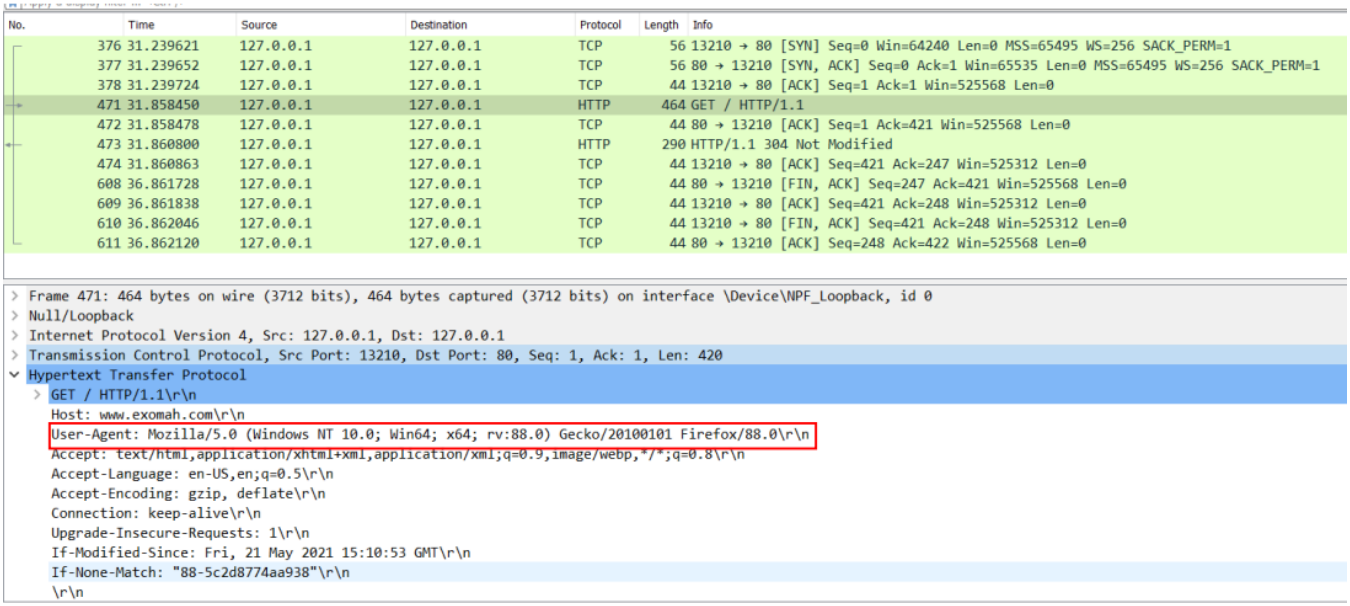
```
> Frame 471: 464 bytes on wire (3712 bits), 464 bytes captured (3712 bits) on interface \Device\NPF_Loopback, id 0
> Null/Loopback
> Internet Protocol Version 4, Src: 127.0.0.1, Dst: 127.0.0.1
> Transmission Control Protocol, Src Port: 13210, Dst Port: 80, Seq: 1, Ack: 1, Len: 420
> Hypertext Transfer Protocol
```

شماره پورت مبدا: ۱۲۳۱۰

شماره پورت مقصد: ۸۰

در ابتدای برقراری اتصال http یک کانکشن tcp ایجاد می‌شود و پس از آن html base file از سرور درخواست و دریافت می‌شود و پس از آن با توجه به فایل html، درخواستهایی برای دریافت آبجکت‌های وب فرستاده می‌شود. آدرس ip سایت درخواستی برای وب سرور فرستاده می‌شود و از این راه می‌تواند سایت درخواستی را تشخیص دهد.

سوال ۲)



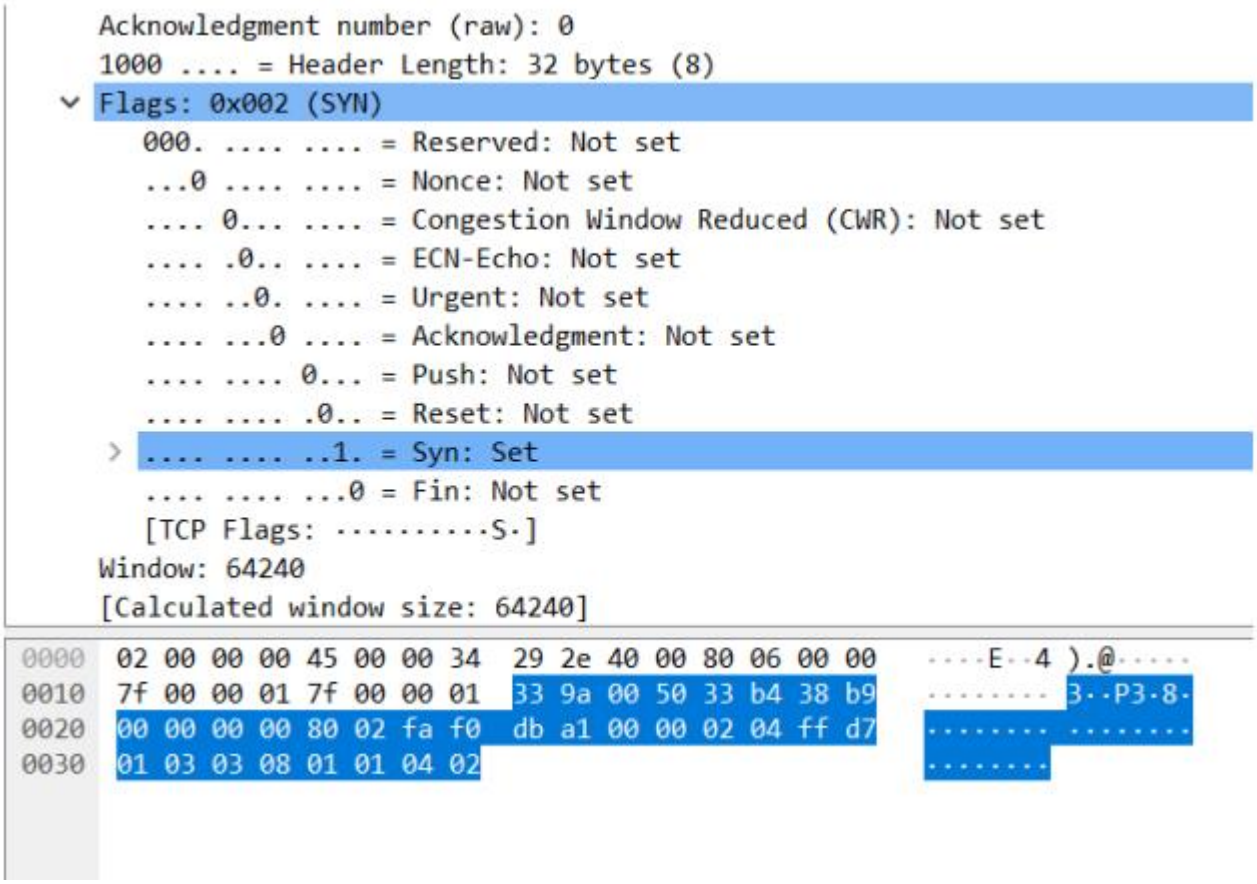
| No. | Time | Source | Destination | Protocol | Length | Info |
|---|---|---|---|---|---|---|
| 376 | 31.239621 | 127.0.0.1 | 127.0.0.1 | TCP | 56 | 13210 → 80 [SYN] Seq=0 Win=64240 Len=0 MSS=65495 WS=256 SACK_PERM=1 |
| 377 | 31.239652 | 127.0.0.1 | 127.0.0.1 | TCP | 56 | 80 → 13210 [SYN, ACK] Seq=0 Ack=1 Win=65535 Len=0 MSS=65495 WS=256 SACK_PERM=1 |
| 378 | 31.239724 | 127.0.0.1 | 127.0.0.1 | TCP | 44 | 13210 → 80 [ACK] Seq=1 Ack=1 Win=525568 Len=0 |
| 471 | 31.858450 | 127.0.0.1 | 127.0.0.1 | HTTP | 464 | GET / HTTP/1.1 |
| 472 | 31.858478 | 127.0.0.1 | 127.0.0.1 | TCP | 44 | 80 → 13210 [ACK] Seq=1 Ack=421 Win=525568 Len=0 |
| 473 | 31.860800 | 127.0.0.1 | 127.0.0.1 | HTTP | 290 | HTTP/1.1 304 Not Modified |
| 474 | 31.860863 | 127.0.0.1 | 127.0.0.1 | TCP | 44 | 13210 → 80 [ACK] Seq=421 Ack=247 Win=525312 Len=0 |
| 608 | 36.861728 | 127.0.0.1 | 127.0.0.1 | TCP | 44 | 80 → 13210 [FIN, ACK] Seq=247 Ack=421 Win=525568 Len=0 |
| 609 | 36.861838 | 127.0.0.1 | 127.0.0.1 | TCP | 44 | 13210 → 80 [ACK] Seq=421 Ack=248 Win=525312 Len=0 |
| 610 | 36.862046 | 127.0.0.1 | 127.0.0.1 | TCP | 44 | 13210 → 80 [FIN, ACK] Seq=421 Ack=248 Win=525312 Len=0 |
| 611 | 36.862120 | 127.0.0.1 | 127.0.0.1 | TCP | 44 | 80 → 13210 [ACK] Seq=248 Ack=422 Win=525568 Len=0 |

```
> Frame 471: 464 bytes on wire (3712 bits), 464 bytes captured (3712 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: 13210, Dst Port: 80, Seq: 1, Ack: 1, Len: 420
v Hypertext Transfer Protocol
  > GET / HTTP/1.1\r\n
    Host: www.exomah.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
    If-Modified-Since: Fri, 21 May 2021 15:10:53 GMT\r\n
    If-None-Match: "88-5c2d8774aa938"\r\n
    \r\n
```

مقدار بخش keep alive: connection (یعنی ارتباط tcp بسته نشود این نوع ارتباط http از نوع پایا یا persistent می‌باشد)

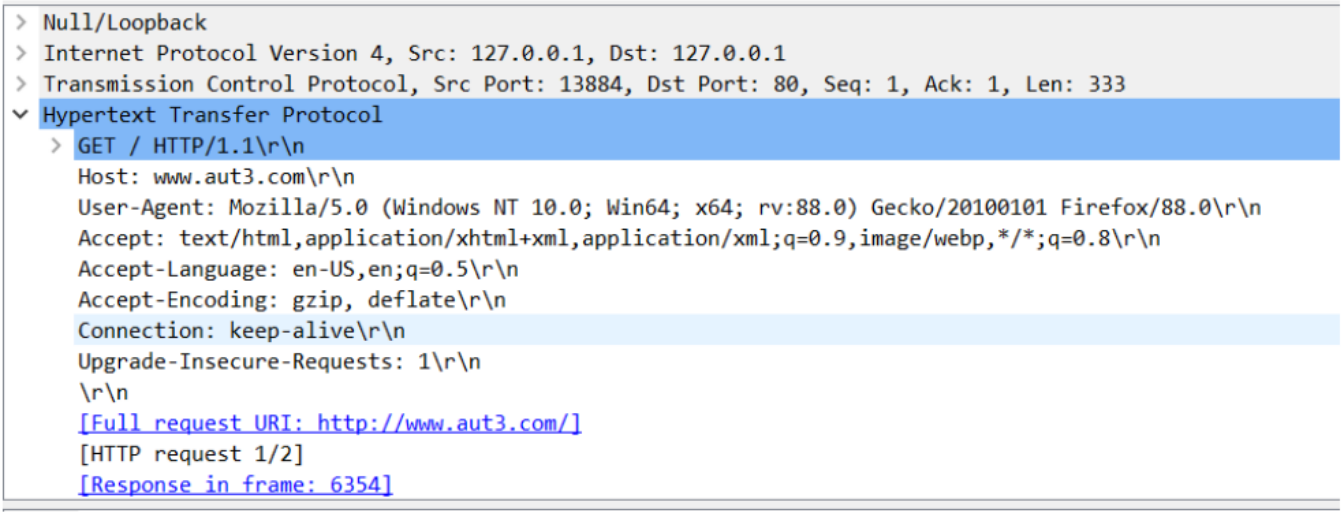
درخواست از نوع GET است. مقدار UA که در شکل نیز مشخص شده است بیانگر مشخصات مرورگر مبدا است.

سوال ۳)



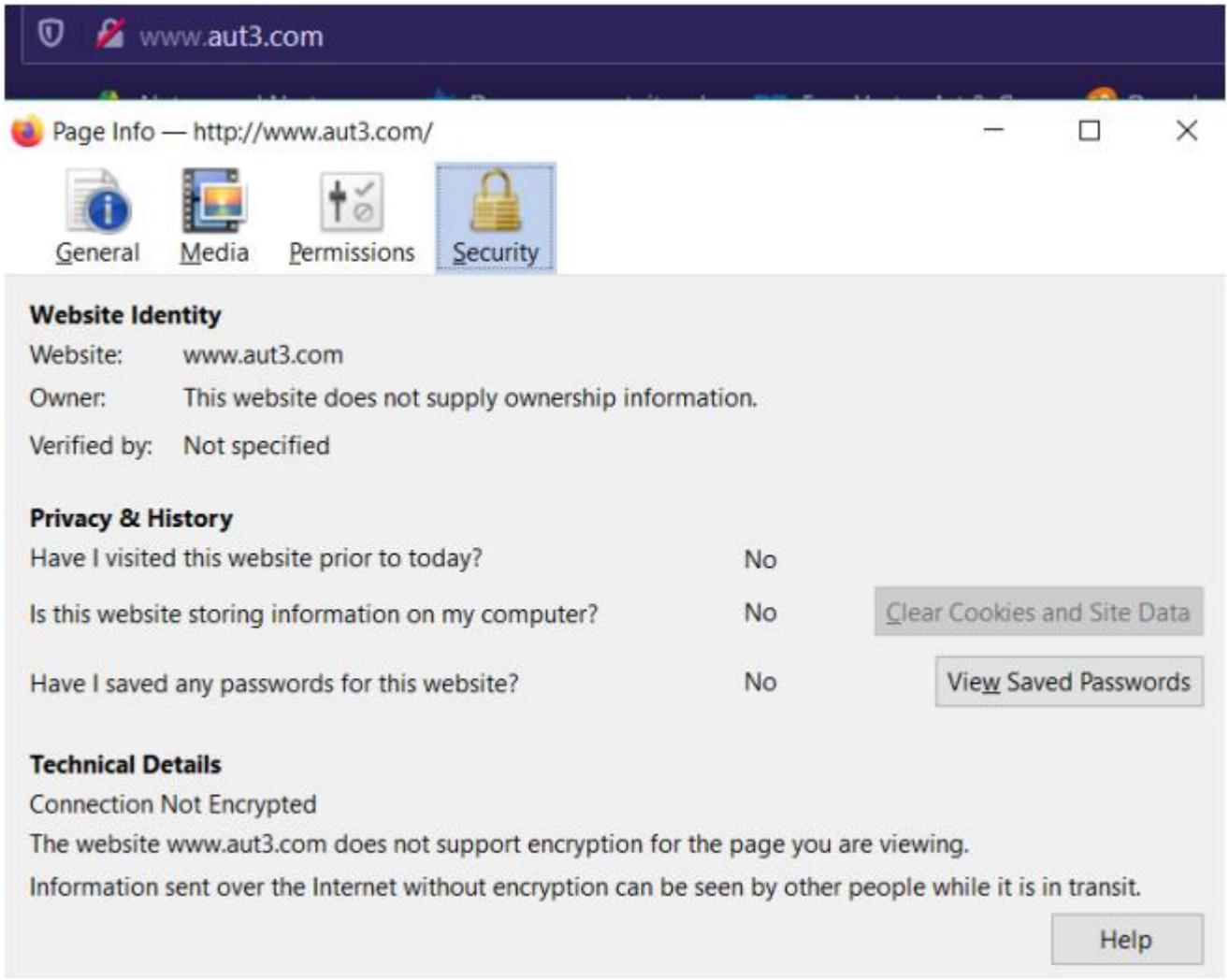

مقدارflag هایی که در اولین بستهی پروتکل TCP ست شدهاند در تصویر باال قابل مشاهده است.

سوال ۴)

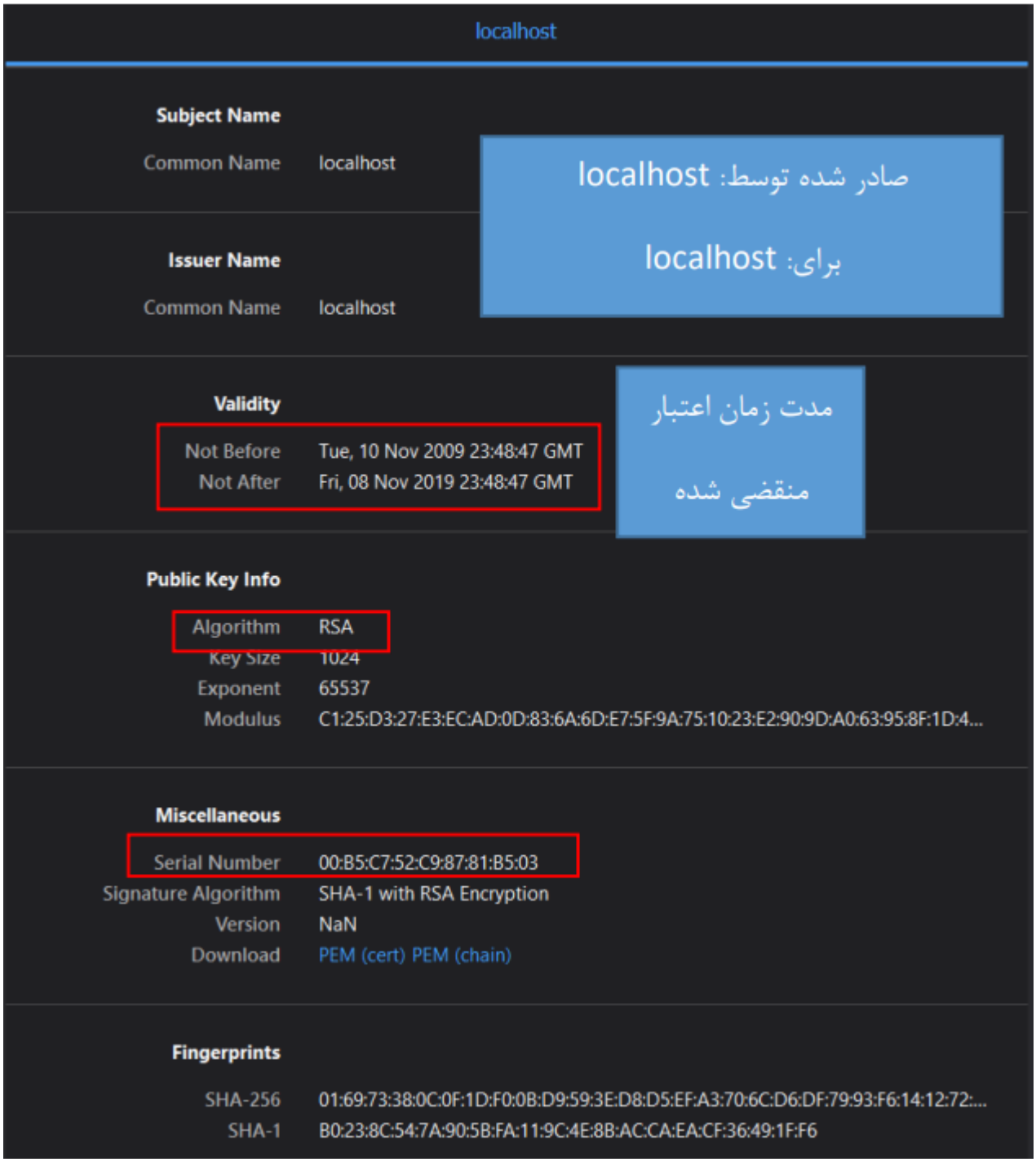



این بار از ادرس aut3.com استفاده کردیم. همانطوری که مشاهده میکنید آدرس پورت مبدا متفاوت است تا بتوان بستههای مربوط به آنها را از هم جدا کرد. طول بستههای آنها نیز متفاوت است. پارامترهای acknowledge number و sequence number هر دو که به صورت raw تنظیم شدهاست هم متفاوت است.

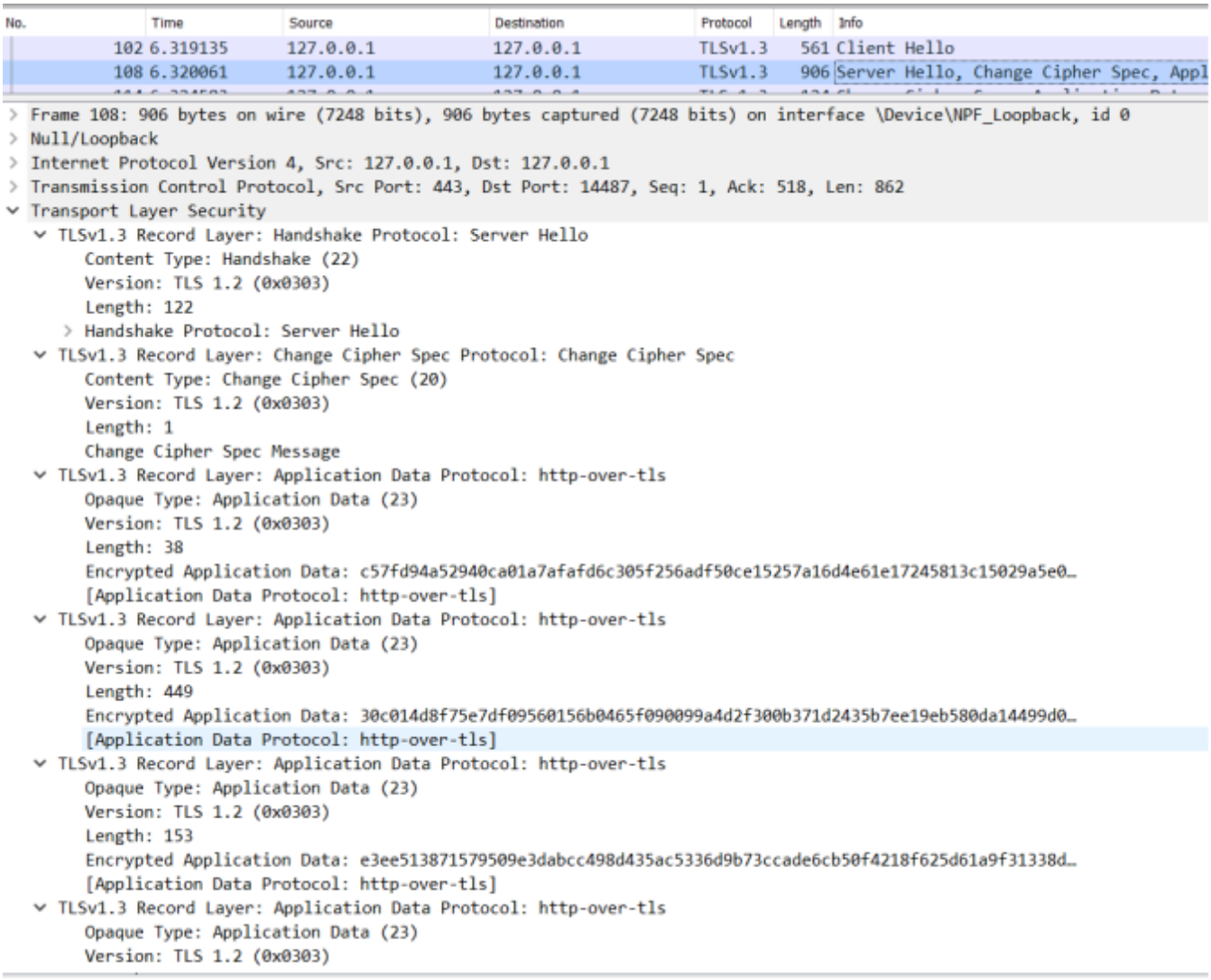
سوال ۵)


www.aut3.com
Page Info — http://www.aut3.com/
General
Media
Permissions
Security
Website Identity
Website: www.aut3.com
Owner: This website does not supply ownership information.
Verified by: Not specified
Privacy & History
Have I visited this website prior to today? No
Is this website storing information on my computer? No
Clear Cookies and Site Data
Have I saved any passwords for this website? No
View Saved Passwords
Technical Details
Connection Not Encrypted
The website www.aut3.com does not support encryption for the page you are viewing.
Information sent over the Internet without encryption can be seen by other people while it is in transit.
Help

حالا برای کانکشن https برای همین دامنه، اطلاعات مربوط به certificate :



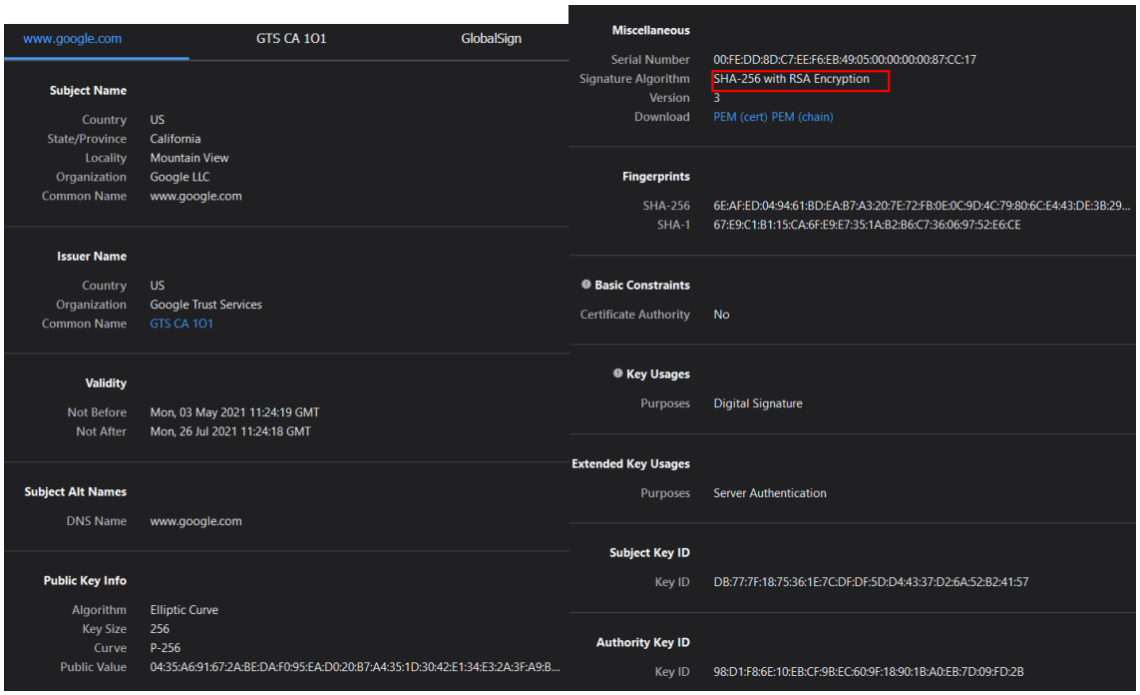
سوال ۶)

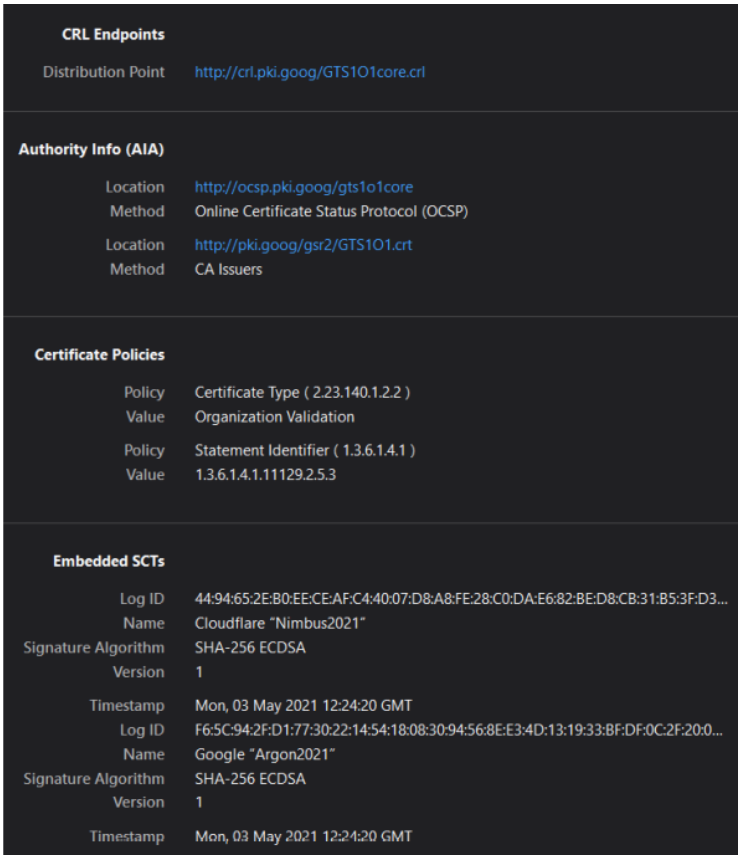



خیر. از آنجایی که از پروتکل tls استفاده شده است، متن این ارتباط قابل خواندن نیست. پروتکل tls وظیفهی رمزگذاری encryption ارتباط بین سرور و کالینت را به عهده دارد.

سوال ۷)

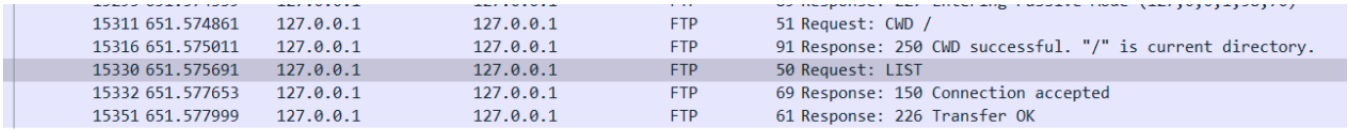
نتایج مشاهدهی certificate سایت گوگل:

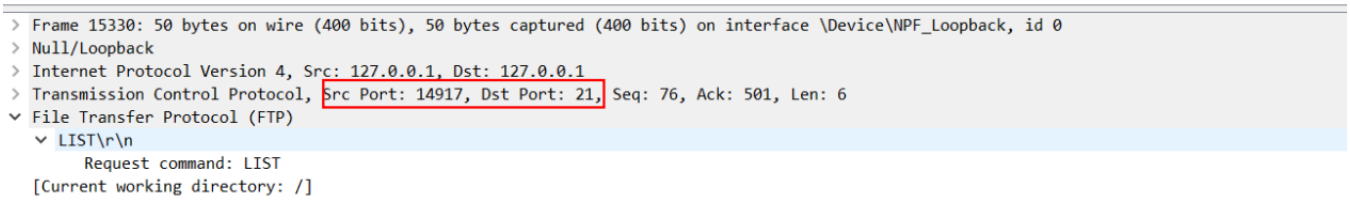


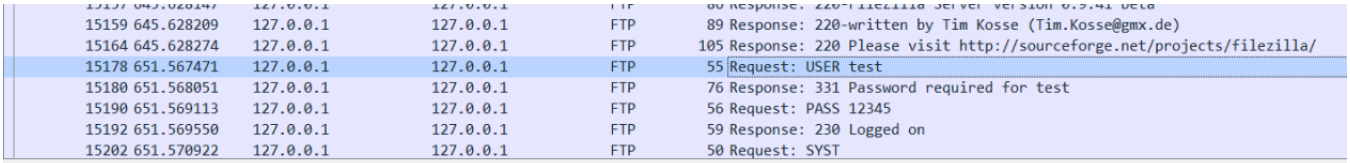
این مدرک، اطالعات بیشتری را شامل میشود. به عنوان اولین تفاوت می‌توان به تفاوت صادر کننده و دریافت‌کننده مدرک اشاره کرد و اینکه مدرک گوگل منقضی نشده است و تا تاریخ 26 جوالی 2021 اعتبار دارد. الگوریتم به کار رفته برای امضا نیز متفاوت می‌باشد.

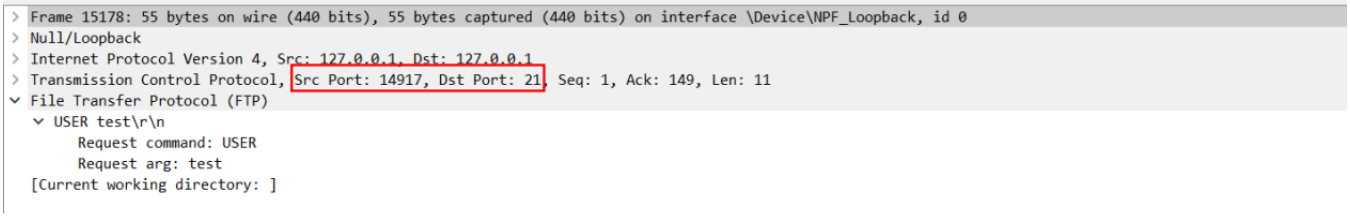
سوال ۸)




از دستور LIST برای گرفتن لیست فایلها استفاده میشود .نام کاربری استفاده شده در اینجا test است (همانطوری که در تنظیمات FileZilla ایجادش کردیم و با آن الگین کردیم)

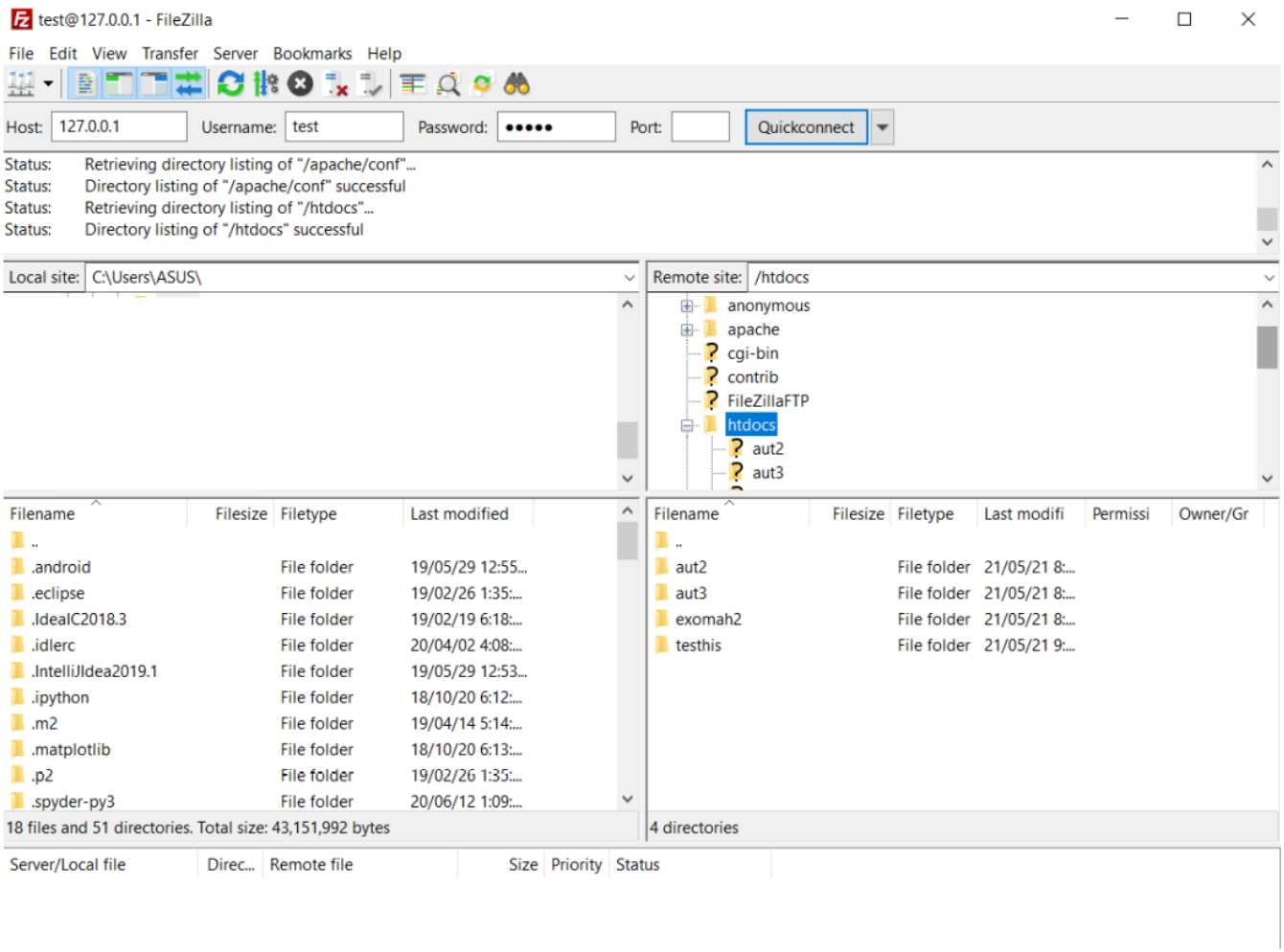


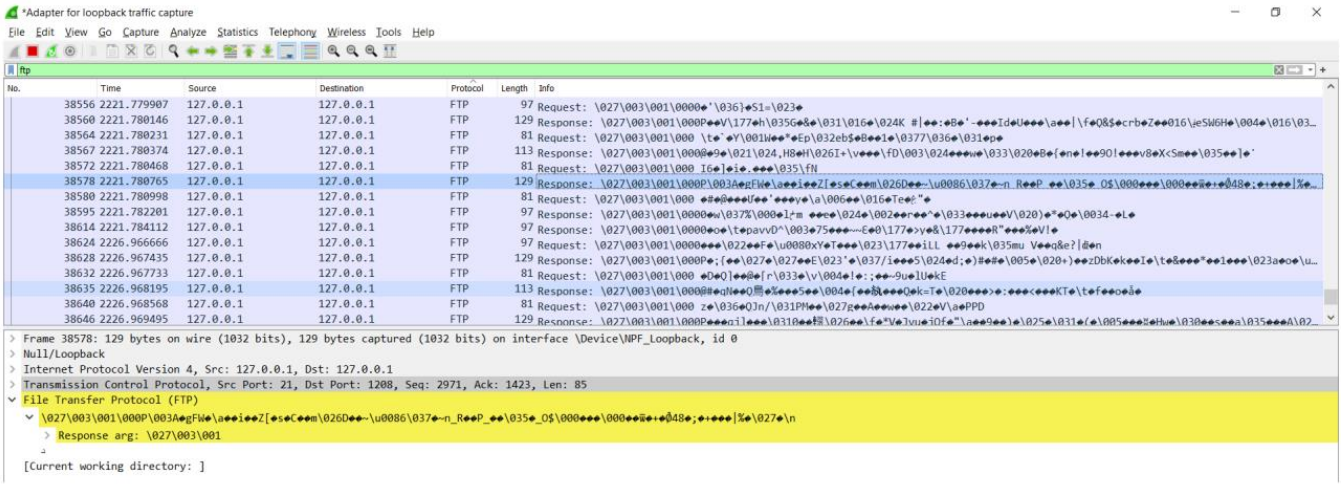

در این ارتباطات ار پروتکل TCP استفاده شده است، با شماره پورت مبدا 14917 و مقصد 21 که در تصاویر باال نیز مشخص شده است.

سوال ۹)

این بار دیگر سایت باز نمی‌شود و مرورگر پیام میدهد که برای اتصال باید از اپلیکیشن دیگری استفاده کنیم که در اینجا ما از FileZilla استفاده می‌کنیم.

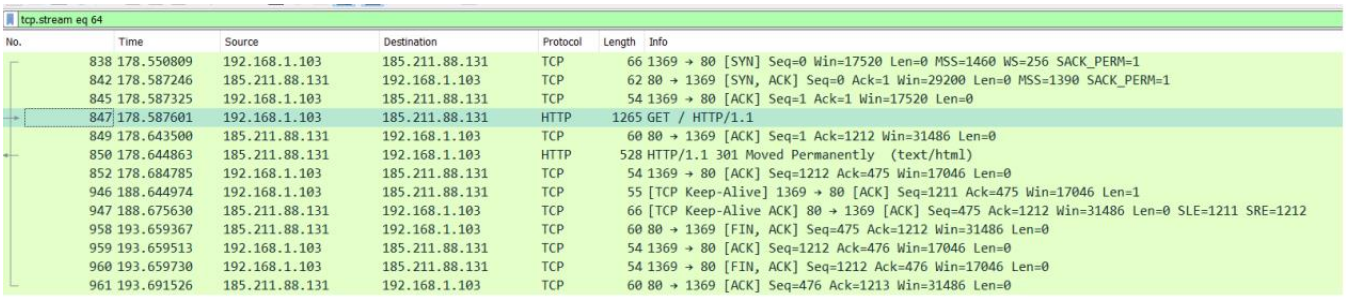


اگر بسته‌های مربوط به این ارتباطات را از وایرشارک شنود کنیم، نمیتوانیم هیچ اطلاعاتی را از آن بخوانیم.



پروتوکل HTTP:

در اینجا، بسته‌های مربوط به follow HTTP Stream را مشاهده می‌کنیم.



tcp.stream eq 64

| No. | Time | Source | Destination | Protocol | Length | Info |
|---|---|---|---|---|---|---|
| 838 | 178.550809 | 192.168.1.103 | 185.211.88.131 | TCP | 66 | 1369 → 80 [SYN] Seq=0 Win=17520 Len=0 MSS=1460 WS=256 SACK_PERM=1 |
| 842 | 178.587246 | 185.211.88.131 | 192.168.1.103 | TCP | 62 | 80 → 1369 [SYN, ACK] Seq=0 Ack=1 Win=29200 Len=0 MSS=1390 SACK_PERM=1 |
| 845 | 178.587325 | 192.168.1.103 | 185.211.88.131 | TCP | 54 | 1369 → 80 [ACK] Seq=1 Ack=1 Win=17520 Len=0 |
| 847 | 178.587601 | 192.168.1.103 | 185.211.88.131 | HTTP | 1265 | GET / HTTP/1.1 |
| 849 | 178.643500 | 185.211.88.131 | 192.168.1.103 | TCP | 60 | 80 → 1369 [ACK] Seq=1 Ack=1212 Win=31486 Len=0 |
| 850 | 178.644863 | 185.211.88.131 | 192.168.1.103 | HTTP | 528 | HTTP/1.1 301 Moved Permanently (text/html) |
| 852 | 178.684785 | 192.168.1.103 | 185.211.88.131 | TCP | 54 | 1369 → 80 [ACK] Seq=1212 Ack=475 Win=17046 Len=0 |
| 946 | 188.644974 | 192.168.1.103 | 185.211.88.131 | TCP | 55 | [TCP Keep-Alive] 1369 → 80 [ACK] Seq=1211 Ack=475 Win=17046 Len=1 |
| 947 | 188.675630 | 185.211.88.131 | 192.168.1.103 | TCP | 66 | [TCP Keep-Alive ACK] 80 → 1369 [ACK] Seq=475 Ack=1212 Win=31486 Len=0 SLE=1211 SRE=1212 |
| 958 | 193.659367 | 185.211.88.131 | 192.168.1.103 | TCP | 60 | 80 → 1369 [FIN, ACK] Seq=475 Ack=1212 Win=31486 Len=0 |
| 959 | 193.659513 | 192.168.1.103 | 185.211.88.131 | TCP | 54 | 1369 → 80 [ACK] Seq=1212 Ack=476 Win=17046 Len=0 |
| 960 | 193.659730 | 192.168.1.103 | 185.211.88.131 | TCP | 54 | 1369 → 80 [FIN, ACK] Seq=1212 Ack=476 Win=17046 Len=0 |
| 961 | 193.691526 | 185.211.88.131 | 192.168.1.103 | TCP | 60 | 80 → 1369 [ACK] Seq=476 Ack=1213 Win=31486 Len=0 |

اطلاعات مربوط به پروتکل tcp و فلگ‌ها: (در این کانکشن از این پروتکل لایه انتقال استفاده می‌شود)

```
Transmission Control Protocol, Src Port: 1369, Dst Port: 80, Seq: 1, Ack: 1, Len: 1211
    Source Port: 1369
    Destination Port: 80
    [Stream index: 64]
    [TCP Segment Len: 1211]
    Sequence Number: 1    (relative sequence number)
    Sequence Number (raw): 1380490331
    [Next Sequence Number: 1212    (relative sequence number)]
    Acknowledgment Number: 1    (relative ack number)
    Acknowledgment number (raw): 2664919712
    0101 .... = Header Length: 20 bytes (5)
```

```
  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···]
    Window: 17520
    [Calculated window size: 17520]
    [Window size scaling factor: -2 (no window scaling used)]
    Checksum: 0xafee [unverified]
    [Checksum Status: Unverified]
    Urgent Pointer: 0
```

اطلاعات مربوط به پروتکلhttp :

```
Hypertext Transfer Protocol
> GET / HTTP/1.1\r\n
  Host: aut.ac.ir\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
> [truncated]Cookie: _ga=GA1.3.234810661.1617441214; 969af8aywID_67c5c_mysid=1; HASH_969af8aywID_67c5c_mysid=9C42D581404D31E721F936995065138F04
  Upgrade-Insecure-Requests: 1\r\n
  \r\n
  [Full request URI: http://aut.ac.ir/]
  [HTTP request 1/1]
  [Response in frame: 850]
```

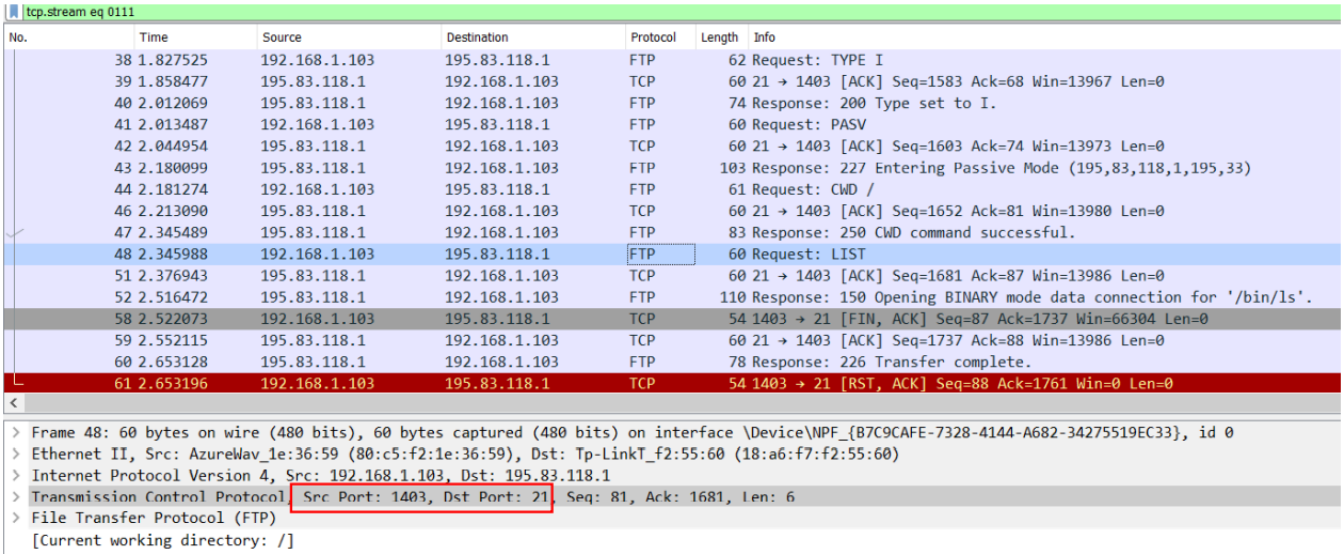
همانطور که مشاهده می‌شود، اتصال از نوعkeep-alive است که کانکشن tcp باز بماند. نوع پروتکل نیز get است.
مقدار UA در تصویر مشخص شده است که نشان دهندهی اطلاعات مرورگر مبدا است.

پروتکل :FTP در اینجا بسته‌های مربوط بهfollow HTTP Stream را مشاده می‌کنیم.

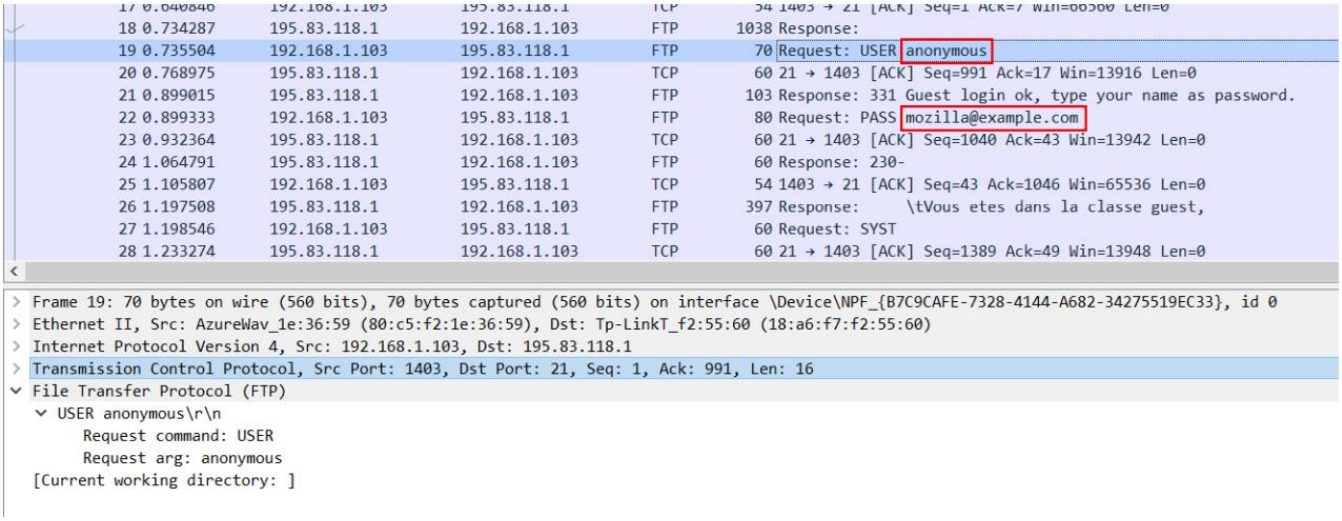
tcp.stream eq 0

| No. | Time | Source | Destination | Protocol | Length | Info |
|---|---|---|---|---|---|---|
| 8 | 0.276505 | 195.83.118.1 | 192.168.1.103 | TCP | 66 | 21 → 1403 [SYN, ACK] Seq=0 Ack=1 Win=13900 Len=0 MSS=1390 WS=1 SACK_PERM=1 |
| 9 | 0.276711 | 192.168.1.103 | 195.83.118.1 | TCP | 54 | 1403 → 21 [ACK] Seq=1 Ack=1 Win=66560 Len=0 |
| 16 | 0.600827 | 195.83.118.1 | 192.168.1.103 | FTP | 60 | Response: 220- |
| 17 | 0.640846 | 192.168.1.103 | 195.83.118.1 | TCP | 54 | 1403 → 21 [ACK] Seq=1 Ack=7 Win=66560 Len=0 |
| 18 | 0.734287 | 195.83.118.1 | 192.168.1.103 | FTP | 1038 | Response: |
| 19 | 0.735504 | 192.168.1.103 | 195.83.118.1 | FTP | 70 | Request: USER anonymous |
| 20 | 0.768975 | 195.83.118.1 | 192.168.1.103 | TCP | 60 | 21 → 1403 [ACK] Seq=991 Ack=17 Win=13916 Len=0 |
| 21 | 0.899015 | 195.83.118.1 | 192.168.1.103 | FTP | 103 | Response: 331 Guest login ok, type your name as password. |
| 22 | 0.899333 | 192.168.1.103 | 195.83.118.1 | FTP | 80 | Request: PASS mozilla@example.com |
| 23 | 0.932364 | 195.83.118.1 | 192.168.1.103 | TCP | 60 | 21 → 1403 [ACK] Seq=1040 Ack=43 Win=13942 Len=0 |
| 24 | 1.064791 | 195.83.118.1 | 192.168.1.103 | FTP | 60 | Response: 230- |
| 25 | 1.105807 | 192.168.1.103 | 195.83.118.1 | TCP | 54 | 1403 → 21 [ACK] Seq=43 Ack=1046 Win=65536 Len=0 |
| 26 | 1.197508 | 195.83.118.1 | 192.168.1.103 | FTP | 397 | Response: \tVous etes dans la classe guest, |
| 27 | 1.198546 | 192.168.1.103 | 195.83.118.1 | FTP | 60 | Request: SYST |
| 28 | 1.233274 | 195.83.118.1 | 192.168.1.103 | TCP | 60 | 21 → 1403 [ACK] Seq=1389 Ack=49 Win=13948 Len=0 |
| 29 | 1.366802 | 195.83.118.1 | 192.168.1.103 | FTP | 103 | Response: 215 UNIX Type: L8 Version: NetBSD-ftpd 20110904 |
| 30 | 1.367419 | 192.168.1.103 | 195.83.118.1 | FTP | 60 | Request: FEAT |
| 31 | 1.398702 | 195.83.118.1 | 192.168.1.103 | TCP | 60 | 21 → 1403 [ACK] Seq=1438 Ack=55 Win=13954 Len=0 |
| 32 | 1.530629 | 195.83.118.1 | 192.168.1.103 | FTP | 78 | Response: 211-Features supported |
| 33 | 1.571597 | 192.168.1.103 | 195.83.118.1 | TCP | 54 | 1403 → 21 [ACK] Seq=55 Ack=1462 Win=66560 Len=0 |
| 34 | 1.662641 | 195.83.118.1 | 192.168.1.103 | FTP | 140 | Response: MDTM |
| 35 | 1.663015 | 192.168.1.103 | 195.83.118.1 | FTP | 59 | Request: PWD |
| 36 | 1.693952 | 195.83.118.1 | 192.168.1.103 | TCP | 60 | 21 → 1403 [ACK] Seq=1548 Ack=60 Win=13959 Len=0 |
| 37 | 1.826344 | 195.83.118.1 | 192.168.1.103 | FTP | 89 | Response: 257 "/" is the current directory. |
| 38 | 1.827525 | 192.168.1.103 | 195.83.118.1 | FTP | 62 | Request: TYPE I |
| 39 | 1.858477 | 195.83.118.1 | 192.168.1.103 | TCP | 60 | 21 → 1403 [ACK] Seq=1583 Ack=68 Win=13967 Len=0 |
| 40 | 2.012069 | 195.83.118.1 | 192.168.1.103 | FTP | 74 | Response: 200 Type set to I. |
| 41 | 2.013487 | 192.168.1.103 | 195.83.118.1 | FTP | 60 | Request: PASV |
| 42 | 2.044954 | 195.83.118.1 | 192.168.1.103 | TCP | 60 | 21 → 1403 [ACK] Seq=1603 Ack=74 Win=13973 Len=0 |
| 43 | 2.180099 | 195.83.118.1 | 192.168.1.103 | FTP | 103 | Response: 227 Entering Passive Mode (195,83,118,1,195,33) |
| 44 | 2.181274 | 192.168.1.103 | 195.83.118.1 | FTP | 61 | Request: CWD / |
| 46 | 2.213090 | 195.83.118.1 | 192.168.1.103 | TCP | 60 | 21 → 1403 [ACK] Seq=1652 Ack=81 Win=13980 Len=0 |
| 47 | 2.345489 | 195.83.118.1 | 192.168.1.103 | FTP | 83 | Response: 250 CWD command successful. |
| 48 | 2.345988 | 192.168.1.103 | 195.83.118.1 | FTP | 60 | Request: LIST |
| 51 | 2.376943 | 195.83.118.1 | 192.168.1.103 | TCP | 60 | 21 → 1403 [ACK] Seq=1681 Ack=87 Win=13986 Len=0 |
| 52 | 2.516472 | 195.83.118.1 | 192.168.1.103 | FTP | 110 | Response: 150 Opening BINARY mode data connection for '/bin/ls'. |
| 58 | 2.522073 | 192.168.1.103 | 195.83.118.1 | TCP | 54 | 1403 → 21 [FIN, ACK] Seq=87 Ack=1737 Win=66304 Len=0 |

پروتکل استفاده شده در این اتصال، پروتکل TCP است. پورت مقصد 21 و پورت مبدا 1403 است.




مقدار یوزنیم و پسوورد به ترتیب anonymous و com.exmaple@mozilla می‌باشد که در تصویر بعدی نیز مشخص شده است:




اگر روی این بسته‌ها کلیک کنیم نیز همین مقادیر را به عنوان نام کاربری و رمز عبور مشاهده خواهیم کرد.