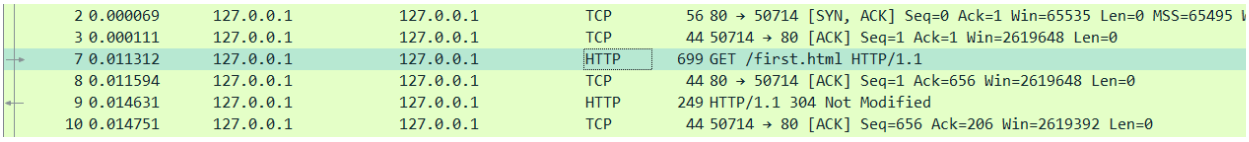
بسمه تعالی

گزارشکار آزمایش سوم شبکه‌های کامپیوتری

راه اندازی سرویس‌های Web و FTP

هلیاسادات هاشمی پور- ۹۸۳۱۱۰۶

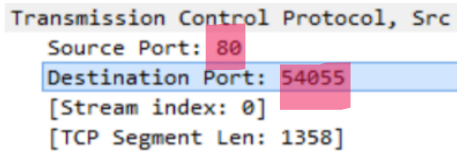
سوال اول: آدرس پورت‌های مبدا و مقصد چیست؟ روند برقراری ارتباط در پروتکل HTTP چگونه است؟ وب سرور چگونه آدرس سایت درخواستی شما را تشخیص می دهد؟



- آدرس هر دو ۱۲۷.۰.۰.۱ می‌باشد.(زیرا چون هم سرور و هم هاست روی سیستم خودمان می باشد)همچنین:

Source Poer: 80

Destination Port: 54055



- این پروتکل از پروتکل‌های لایه‌ی Application (کاربرد) می باشد که این لایه بالاترین لایه در TCP/IP است. همچنین مرورگرهای وب و سرورهای اینترنتی برای برقراری ارتباط از این پروتکل استفاده می‌کنند.روند ارتباط در این پروتکل ارتباط بین کلاینت و سرور که از طریق پورت ۸۰ انجام می‌شود در اصل چون می دانیم پروتکل HTTP بر پایه TCP است با استفاده از handshaking یک ارتباط صورت می گیرد و کلاینت یک به پورت ۸۰ فرستاده و یک آبجکت دریافت می کند.(درواقع کلاینت درخواست خود را برای دریافت آبجکت به سرور می دهد) و سرور پاسخ داده و و پاسخ آن آبجکت درخواست یا اگر موجود بود برای کاربر ارسال می شود و نتایج درخواستی روی وب نشان داده می شوند.
- به صورت کلی با استفاده از پروتکل DNS آدرس صفحات وب را تشخیص داد.(اما در اینجا سیستم کلاینت به وسیله فایل host که در آن IP معادل را پیدا می کند)

سوال دوم: مقدار بخش Connection چیست؟ درخواست HTTP از نوع GET بوده است یا از نوع POST؟ مقدار User Agent چیست؟ به نظر شما این مقدار بیانگر چه چیزی است؟

- مقدار بخش Connection از نوع keep-alive است.
- درخواست از نوع GET می باشد.

- User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/86.0.4240.198 Safari/537.36\r\n

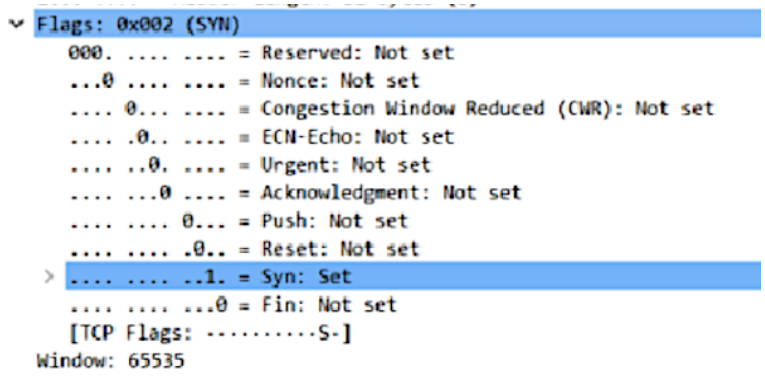
- **رشته‌ای که داریم به بخش‌های مختلفی تقسیم شود که هر کدام معنای اختصاصی خودشان را دارند.**

User-Agent شامل مشخصاتی است که درخواست را صادر کرده است. که در اسن بخش مرورگر ما هست که درخواست را صادر کرده است.

- **User-Agent برابر Mozilla 5 می باشد که تقریبا بین تمام browserها مشترک است.**
- **(Windows NT 10.0; Win64; x64)مشخص می‌کند درخواست توسط چه platformای اتفاق افتاده است**
- **AppleWebKit/537.36 (KHTML, like Gecko) مربوط به Webkit engine build را نشان داده است.**
- **Chrome/86.0.4240.198 ورژن chromای که request را فرستاده مشخص می‌کند**
- **در آخر هم Safari build number را مشخص کرده‌است.**

سوال سوم: در پنجره‌ی باز شده، اولین بسته را انتخاب کنید. سپس مقدار Flags در پروتکل TCP را مشاهده کنید. چه مقادیری برای این بسته تنظیم شده است؟

مقادیر تنظیم شده برای Flags مختلف مشخص شده است. (این مقدار براب با0x002 است)



سوال چهارم: یک سایت دیگر با نام دلخواه ایجاد کنید و بسته‌های مربوط به آن را شنود کنید. چه تفاوتی بین این دو سایت وجود دارد؟

```
<html>
    <head>
        <title>helooooo</title>
    </head>
    <body>
        <p> second sample </p>
    </body>
</html>
```

File Edit Search View Encoding Language Settings Tools Macro Run Plugins Window ?

change.log | hosts | new 1.html

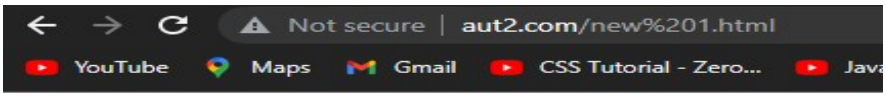
```
# Copyright (c) 1993-2009 Microsoft Corp.
#
# This is a sample HOSTS file used by Microsoft TCP/IP for Windows.
#
# This file contains the mappings of IP addresses to host names. Each
# entry should be kept on an individual line. The IP address should
# be placed in the first column followed by the corresponding host name.
# The IP address and the host name should be separated by at least one
# space.
#
# Additionally, comments (such as these) may be inserted on individual
# lines or following the machine name denoted by a '#' symbol.
#
# For example:
#
#      102.54.94.97     rhino.acme.com          # source server
#       38.25.63.10     x.acme.com              # x client host

# localhost name resolution is handled within DNS itself.
#   127.0.0.1       localhost
#   ::1             localhost


127.0.0.1 www.aut2.com
127.0.0.1 www.aut3.com
```

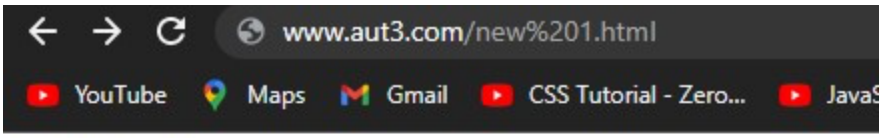
دو تا سایت به این شکل هستند:

۱-



first sample

۲-



second sample

بسته های مربوط به سایت ها در وایرشایرک شنود می کنیم و سپس یکی از بسته ها را انتخاب کرده و follow HTTP stream را میزنیم:

۱-

```
Frame 34: 376 bytes on wire (3008 bits), 376 bytes captured (3008 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: 52103, Dst Port: 80, Seq: 1, Ack: 1, Len: 332
Hypertext Transfer Protocol
  GET / HTTP/1.1\r\n
    [Expert Info (Chat/Sequence): GET / HTTP/1.1\r\n]
        [GET / HTTP/1.1\r\n]
        [Severity level: Chat]
        [Group: Sequence]
      Request Method: GET
      Request URI: /
      Request Version: HTTP/1.1
  Host: www.aut2.com\r\n
  User-Agent: Mozilla/5.0 (Windows NT 6.3; Win64; x64; rv:82.0) Gecko/20100101 Firefox/82.0\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
```

۲-

```
Frame 298: 376 bytes on wire (3008 bits), 376 bytes captured (3008 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: 52109, Dst Port: 80, Seq: 1, Ack: 1, Len: 332
Hypertext Transfer Protocol
  GET / HTTP/1.1\r\n
    [Expert Info (Chat/Sequence): GET / HTTP/1.1\r\n]
        [GET / HTTP/1.1\r\n]
        [Severity level: Chat]
        [Group: Sequence]
      Request Method: GET
      Request URI: /
      Request Version: HTTP/1.1
  Host: www.aut3.com\r\n
  User-Agent: Mozilla/5.0 (Windows NT 6.3; Win64; x64; rv:82.0) Gecko/20100101 Firefox/82.0\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
```

- پورتی که برنامه کلاینت روی آن کار می کند متفاوت است. (اولی ۵۲۱۰۳ و دومی ۵۲۱۰۹ است)
- شماره frameمتفاوت است.
- مقدار موجود در hedear line، host متفاوت می باشد.

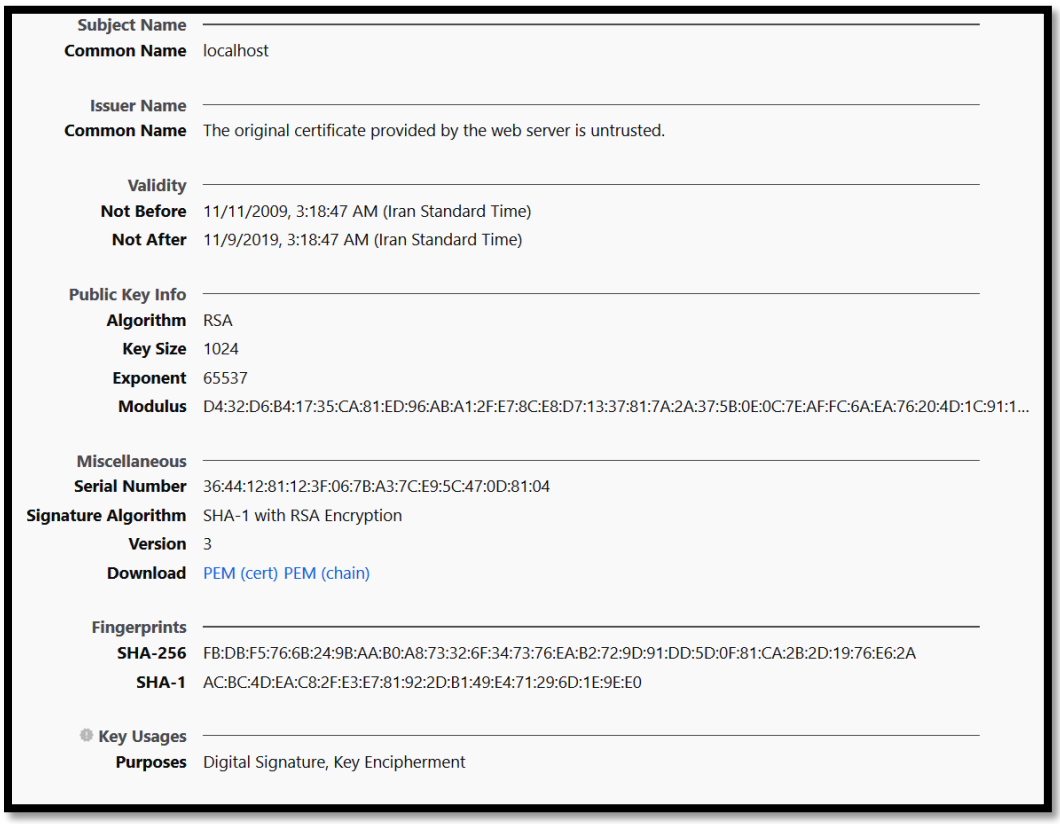
سوال پنجم: مشخص کنید که گواهی را چه کسی برای چه کسی صادر کرده، مدت زمان اعتبار گواهی چقدر است، کلید عمومی صادرکننده چیست و امضای دیجیتال انجام شده با چه الگوریتم‌هایی انجام شده است.

گواهی را وب‌سرور برای localhost صادر کرده است.

مدت زمان اعتبار این گواهی که در بخش Validity مشخص شده است تقریبا برابر با ده سال است.

کلید عمومی یک Cryptographic key است که مرتبط با الگوریتم‌های ریاضی می‌باشد. الگوریتم استفاده شده در این گواهی RSA است که در گواهی‌های SSL/TLS برای رمزنگاری و رمز گشایی استفاده می‌شود.

امضای دیجیتال با استفاده از الگوریتم SHA-۱ انجام شده است.



سوال ششم: آیا می‌توانید متن ارتباط را بخوانید؟ چرا؟

خیر نمی‌توان آن را خواند زیرا به شکل رمزنگاری شده هستند و برای ما قابل رویت نیست.

```
Content Type: Application Data (23)
Version: TLS 1.2 (0x0303)
Length: 34
Encrypted Application Data: 04ee52046bf1af9da098b1430f78d61c5b2fe72d0d1caade…
```

سوال هفتم: گواهی سایت google با گواهی سایت شما چه تفاوت‌هایی دارد؟

این گواهی فیلدهای بیشتری نسبت به گواهی سایت قبلی دارد. بخش Subject Alt Names که در آن نام DNS سایت نوشته شده است و بخش Basic Constrains، Key Usage ، Extended Key Usage و Authority Key ID اضافه تر هستند.

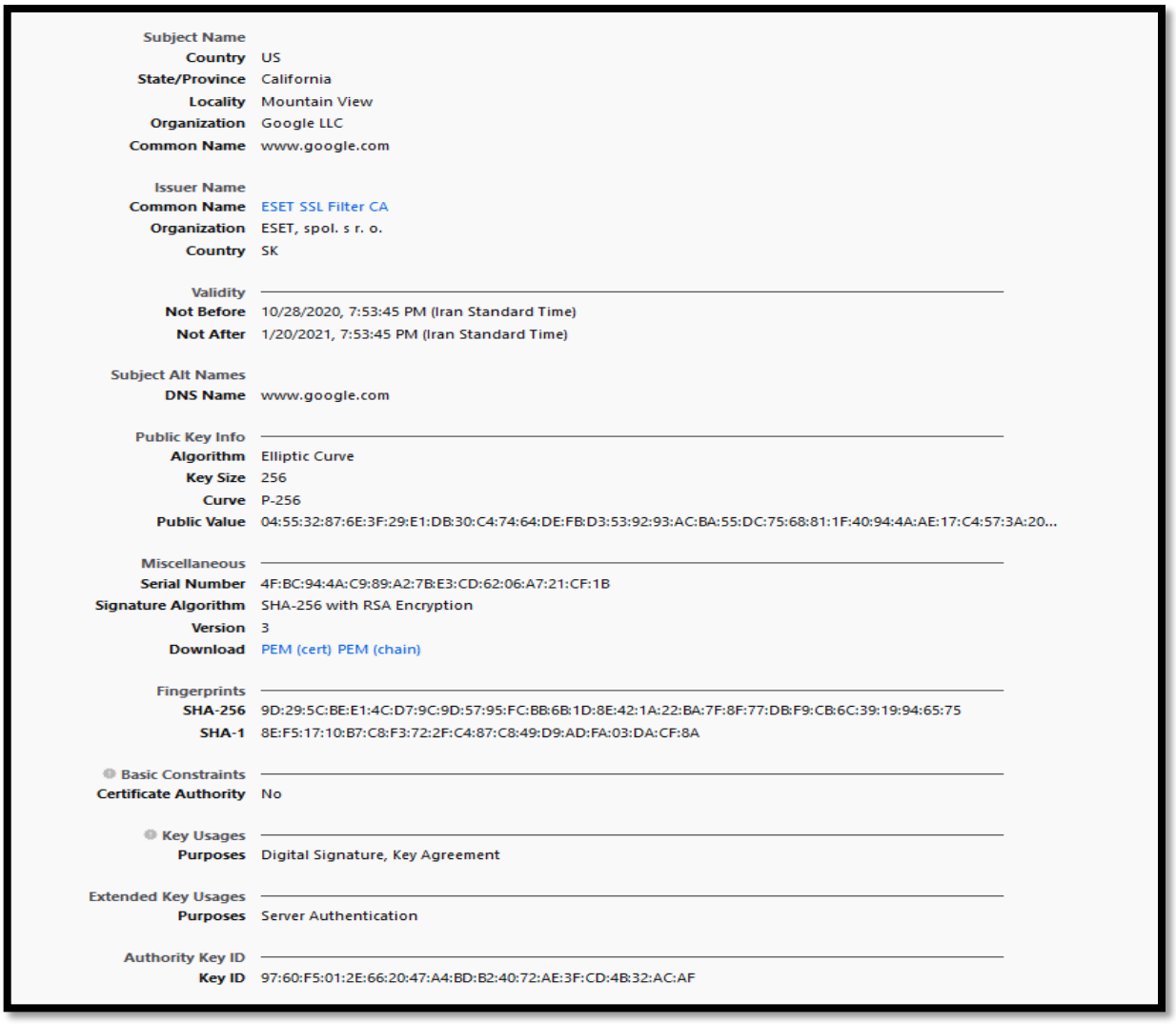
Certificate گوگل valid می باشد.

در بخش valiityهم مدت زمان اعتبار آن کمتر و به روز تر است.

امضای دیجیتال در این سایت SHA–256 است.

الگوریتم رمز نگاری این سایت Elliptic Curve ماست در حالیکه الگوریتم سایت قبل RSA بود.

در حالت قبلی سایز کلید برابر با ۱۰۲۴ بود و در سایت گوگل برابر ۲۵۶ است.



Subject Name
Country US
State/Province California
Locality Mountain View
Organization Google LLC
Common Name www.google.com

Issuer Name
Common Name ESET SSL Filter CA
Organization ESET, spol. s r. o.
Country SK

Validity
Not Before 10/28/2020, 7:53:45 PM (Iran Standard Time)
Not After 1/20/2021, 7:53:45 PM (Iran Standard Time)

Subject Alt Names
DNS Name www.google.com

Public Key Info
Algorithm Elliptic Curve
Key Size 256
Curve P-256
Public Value 04:55:32:87:6E:3F:29:E1:DB:30:C4:74:64:DE:FB:D3:53:92:93:AC:BA:55:DC:75:68:81:1F:40:94:4A:AE:17:C4:57:3A:20...

Miscellaneous
Serial Number 4F:BC:94:4A:C9:89:A2:7B:E3:CD:62:06:A7:21:CF:1B
Signature Algorithm SHA-256 with RSA Encryption
Version 3
Download PEM (cert) PEM (chain)

Fingerprints
SHA-256 9D:29:5C:BE:E1:4C:D7:9C:9D:57:95:FC:BB:6B:1D:8E:42:1A:22:BA:7F:8F:77:DB:F9:CB:6C:39:19:94:65:75
SHA-1 8E:F5:17:10:B7:C8:F3:72:2F:C4:87:C8:49:D9:AD:FA:03:DA:CF:8A

Basic Constraints
Certificate Authority No

Key Usages
Purposes Digital Signature, Key Agreement

Extended Key Usages
Purposes Server Authentication

Authority Key ID
Key ID 97:60:F5:01:2E:66:20:47:A4:BD:B2:40:72:AE:3F:CD:4B:32:AC:AF

سوال هشتم: مشخص کنید چه دستوری برای لیست کردن فایل‌های دایرکتوری استفاده شده است. مشخص کنید چه نام کاربری برای دسترسی به سایت استفاده شده است. پروتکل لایه‌ی Transport استفاده شده برای بسته‌ها چیست؟ آدرس پورت مبدا و مقصد ارتباط را مشخص کنید.

- دستور LIST-l برای لیست کردن فایل های دایرکتوری استفاده شده است.
- نام کاربری که برای دسترسی به سایت استفاده شده است همان test است.
- پروتکل لایه‌ی Transport استفاده شده برای بسته‌ها، TCP می باشد.
- آدرس پورت مبدا و مقصد هر دو 127.0.0.1 هستند. و اینکه

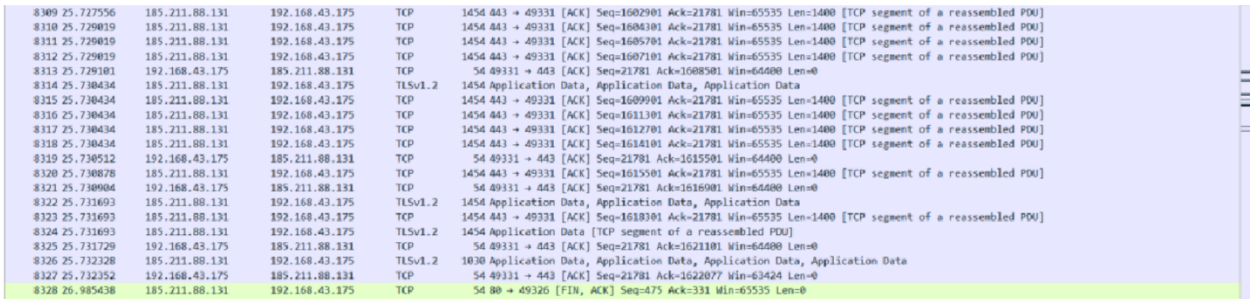
Src port = 65184

Dst port = 21

```
Transmission Control Protocol, Src Port: 65184, Dst Port: 21, Seq: 71, Ack: 434, Len: 6
```

۱-۳-۳- پروتکل HTTP

.۱



8309 25.727556	185.211.88.131	192.168.43.175	TCP	1454 443 → 49331 [ACK] Seq=1602901 Ack=21781 Win=65535 Len=1400 [TCP segment of a reassembled PDU]
8310 25.729019	185.211.88.131	192.168.43.175	TCP	1454 443 → 49331 [ACK] Seq=1604301 Ack=21781 Win=65535 Len=1400 [TCP segment of a reassembled PDU]
8311 25.729019	185.211.88.131	192.168.43.175	TCP	1454 443 → 49331 [ACK] Seq=1605701 Ack=21781 Win=65535 Len=1400 [TCP segment of a reassembled PDU]
8312 25.729019	185.211.88.131	192.168.43.175	TCP	1454 443 → 49331 [ACK] Seq=1607101 Ack=21781 Win=65535 Len=1400 [TCP segment of a reassembled PDU]
8313 25.729101	192.168.43.175	185.211.88.131	TCP	54 49331 → 443 [ACK] Seq=21781 Ack=1608501 Win=64400 Len=0
8314 25.730434	185.211.88.131	192.168.43.175	TLSv1.2	1454 Application Data, Application Data, Application Data
8315 25.730434	185.211.88.131	192.168.43.175	TCP	1454 443 → 49331 [ACK] Seq=1609901 Ack=21781 Win=65535 Len=1400 [TCP segment of a reassembled PDU]
8316 25.730434	185.211.88.131	192.168.43.175	TCP	1454 443 → 49331 [ACK] Seq=1611301 Ack=21781 Win=65535 Len=1400 [TCP segment of a reassembled PDU]
8317 25.730434	185.211.88.131	192.168.43.175	TCP	1454 443 → 49331 [ACK] Seq=1612701 Ack=21781 Win=65535 Len=1400 [TCP segment of a reassembled PDU]
8318 25.730434	185.211.88.131	192.168.43.175	TCP	1454 443 → 49331 [ACK] Seq=1614101 Ack=21781 Win=65535 Len=1400 [TCP segment of a reassembled PDU]
8319 25.730512	192.168.43.175	185.211.88.131	TCP	54 49331 → 443 [ACK] Seq=21781 Ack=1615501 Win=64400 Len=0
8320 25.730878	185.211.88.131	192.168.43.175	TCP	1454 443 → 49331 [ACK] Seq=1615501 Ack=21781 Win=65535 Len=1400 [TCP segment of a reassembled PDU]
8321 25.730904	192.168.43.175	185.211.88.131	TCP	54 49331 → 443 [ACK] Seq=21781 Ack=1616901 Win=64400 Len=0
8322 25.731693	185.211.88.131	192.168.43.175	TLSv1.2	1454 Application Data, Application Data, Application Data
8323 25.731693	185.211.88.131	192.168.43.175	TCP	1454 443 → 49331 [ACK] Seq=1618301 Ack=21781 Win=65535 Len=1400 [TCP segment of a reassembled PDU]
8324 25.731693	185.211.88.131	192.168.43.175	TLSv1.2	1454 Application Data [TCP segment of a reassembled PDU]
8325 25.731729	192.168.43.175	185.211.88.131	TCP	54 49331 → 443 [ACK] Seq=21781 Ack=1621101 Win=64400 Len=0
8326 25.732328	185.211.88.131	192.168.43.175	TLSv1.2	1030 Application Data, Application Data, Application Data, Application Data
8327 25.732352	192.168.43.175	185.211.88.131	TCP	54 49331 → 443 [ACK] Seq=21781 Ack=1622077 Win=63424 Len=0
8328 26.985438	185.211.88.131	192.168.43.175	TCP	54 80 → 49326 [FIN, ACK] Seq=475 Ack=331 Win=65535 Len=0

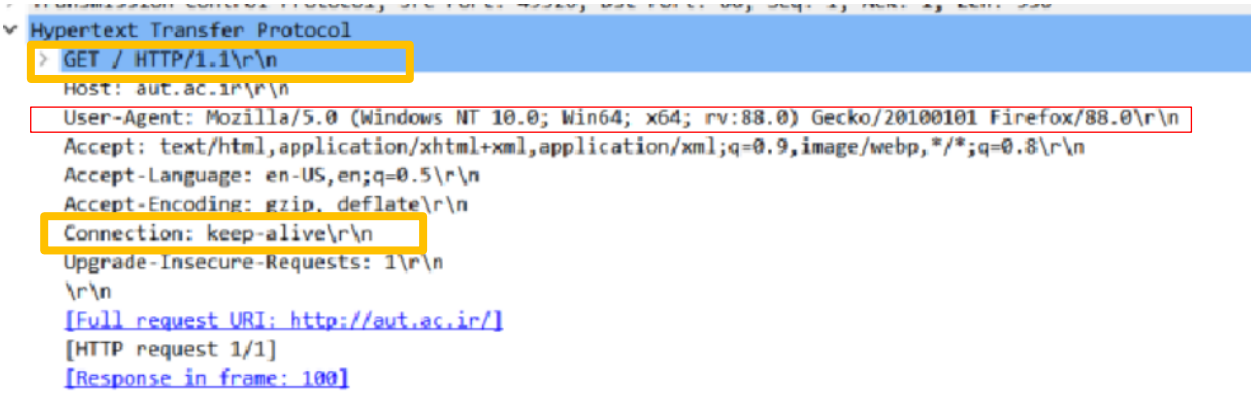
.۲

```
GET / HTTP/1.1
Host: aut.ac.ir
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

HTTP/1.1 301 Moved Permanently
Date: Fri, 14 May 2021 14:03:32 GMT
Server: Apache
Location: https://aut.ac.ir:443/
Content-Length: 230
Keep-Alive: timeout=15, max=100
```

۳.

- **مقدار بخش Connection** ، Keep-Alive می باشد.



- درخواست داده شده از نوع GET می‌باشد.
- این مقدار بیانگر این است که کاربر درخواست کننده از چه پلتفرمی استفاده می‌کرده است.(در اصل همان مرورگر وب که از سرویس دهنده درخواست کرده را مشخص می کند)
- همانطور که مشاهده می‌شود به Syn تنظیم شده است.