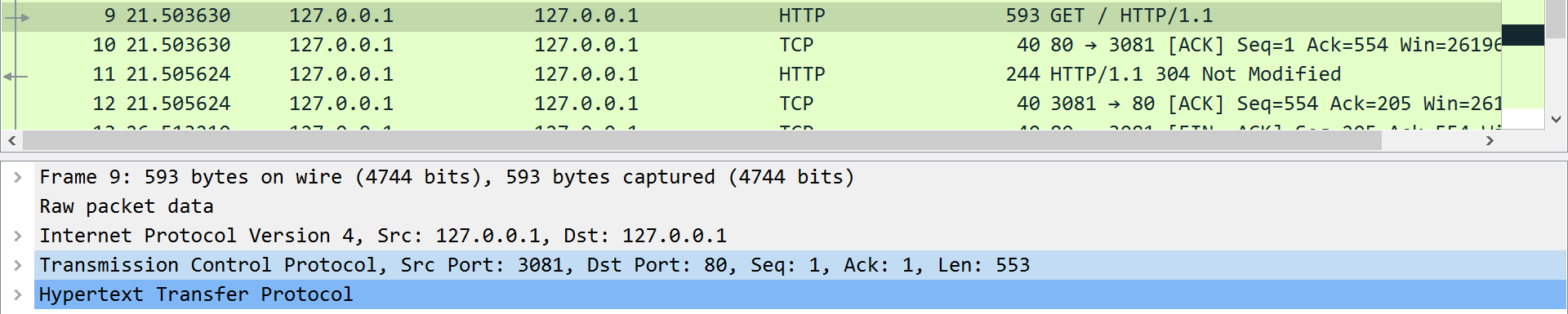
# ۱



مبدا: 3081

مقصد: 80

در بسته ی انتخابی پورت مبدا 2117 و پورت مقصد 08 است . روند برقراری ارتباط در HTTP به این صورت است که ابتدا کلاینت درخواست ارتباط TCP به سرور که بر روی پورت 08 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 کالینت 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](http://www.aut2.ac.ir/) توسط فایل hosts روی 127.0.0.1 مپ شده.

# ۲

نوع: GET

کانکشن: keep-alive

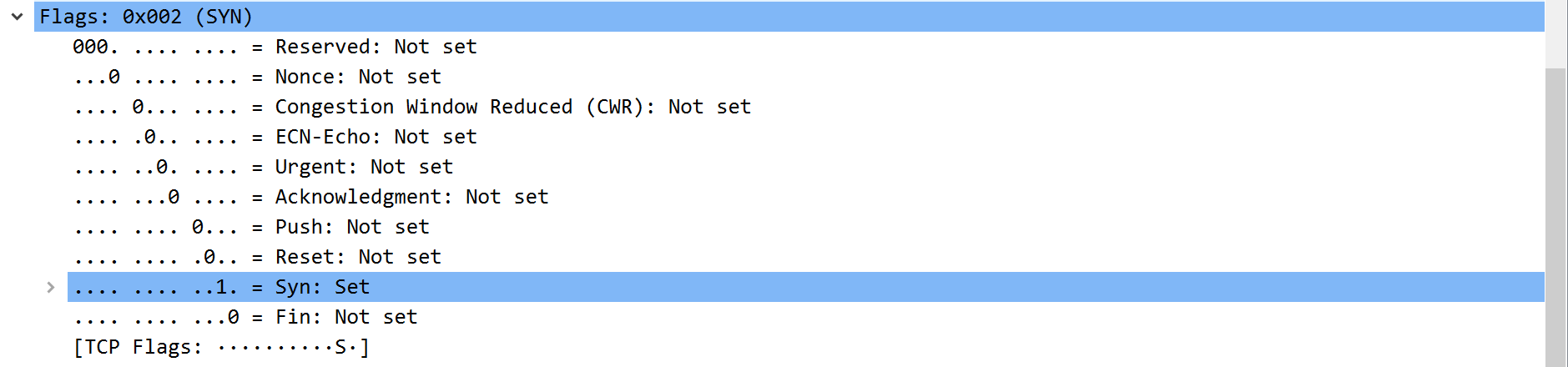
User-Agent

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 .





# ۳



# ۴

لایه انتقال:

|  |  |
| --- | --- |
|  |  |

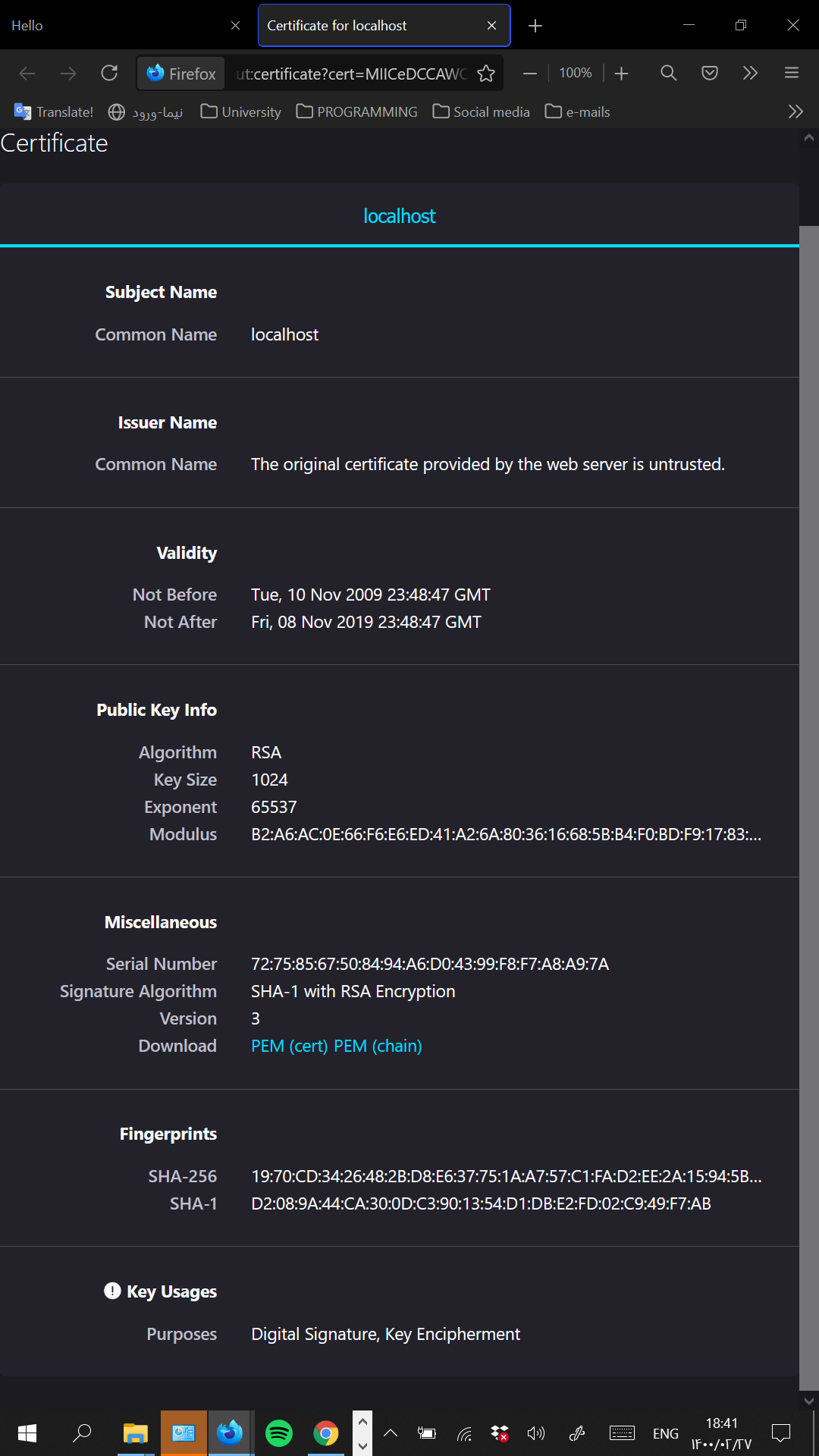
لایه شبکه:

|  |  |
| --- | --- |
|  |  |

بالاترین لایه:

|  |  |
| --- | --- |
|  |  |

# ۵



گواهی را localhost برای localhost صادر کرده است.

زمان اعتبار در عکس نشان داده شده

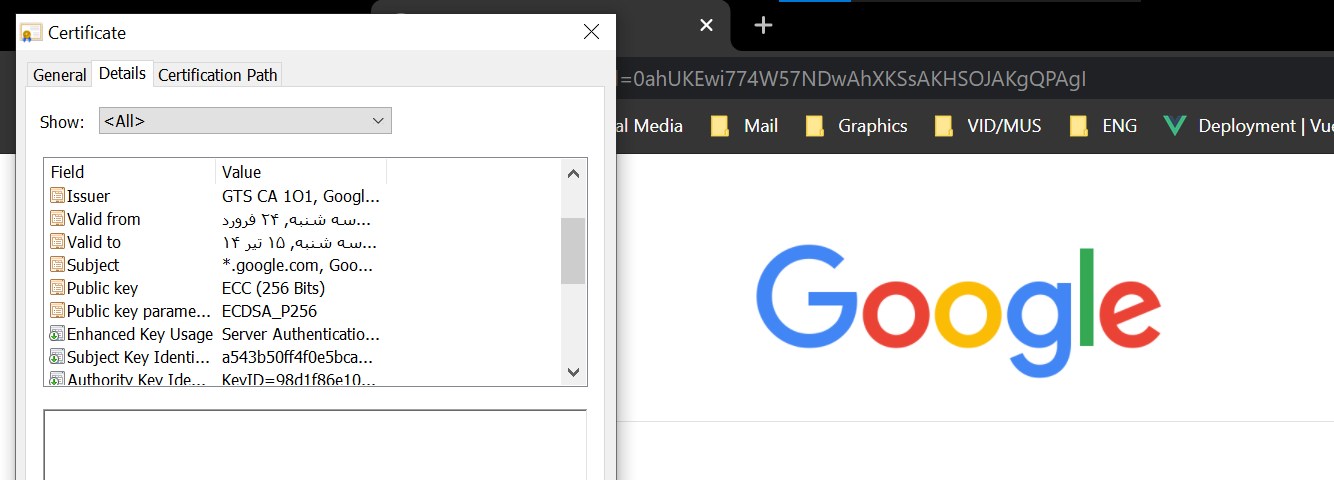
کلید عمومی الگوریتم RSA با key size = 1024 است .

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

# ۶

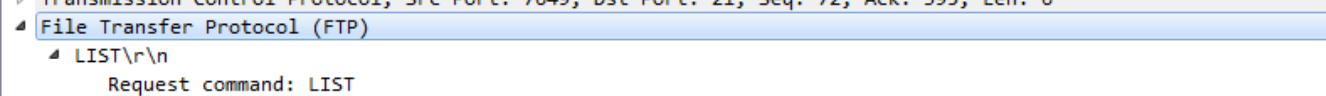
متن ارتباط دیده نمیشود چرا که گواهی آن اعتبار ندارد و wireshark نتوانسته است اطالعات session را که encrypt شده اند را decrypt کند

# ۷

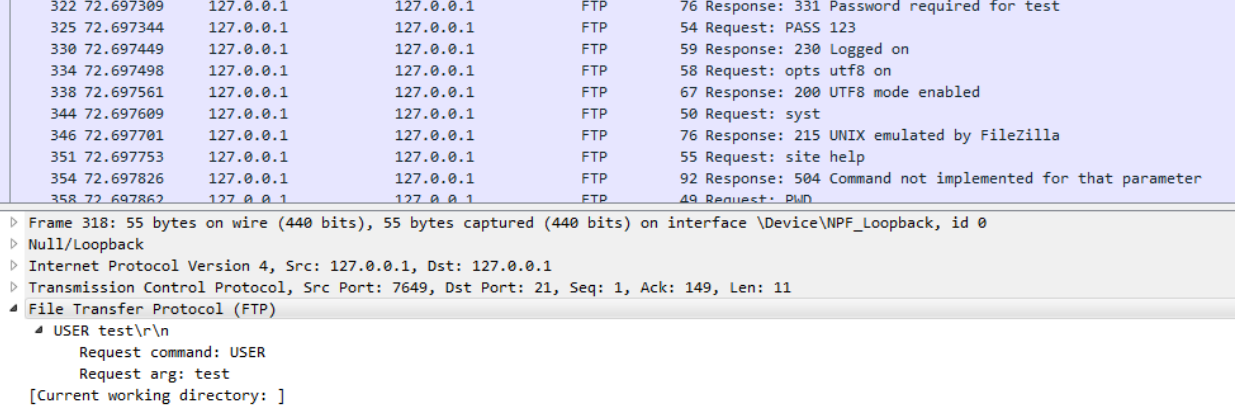


این گواهی با گواهی ما تفاووت های بسیاری دارد از جمله اینکه این گواهی معتبر است و از , 101 CA GTS Service Trust Google به Google اعطا شده است . همچنین الگوریتم امضای الکترونیکی آن و الگوریتم و سایز public key آن و تاریخ اعطای گواهی و انقضای آن نیز با گواهی ما متفاوت است .

# ۸



از دستور LIST برای لیست کردن فایل های دایرکتوری استفاده شده است . از نام کاربری test با رمز 1۲3 برای دسترسی به سایت استفاده شده است . پرتکل الیه ی transport برای این بسته ها TCP است . پورت مبدا 7649 و پورت مقصد ۲۱ است .

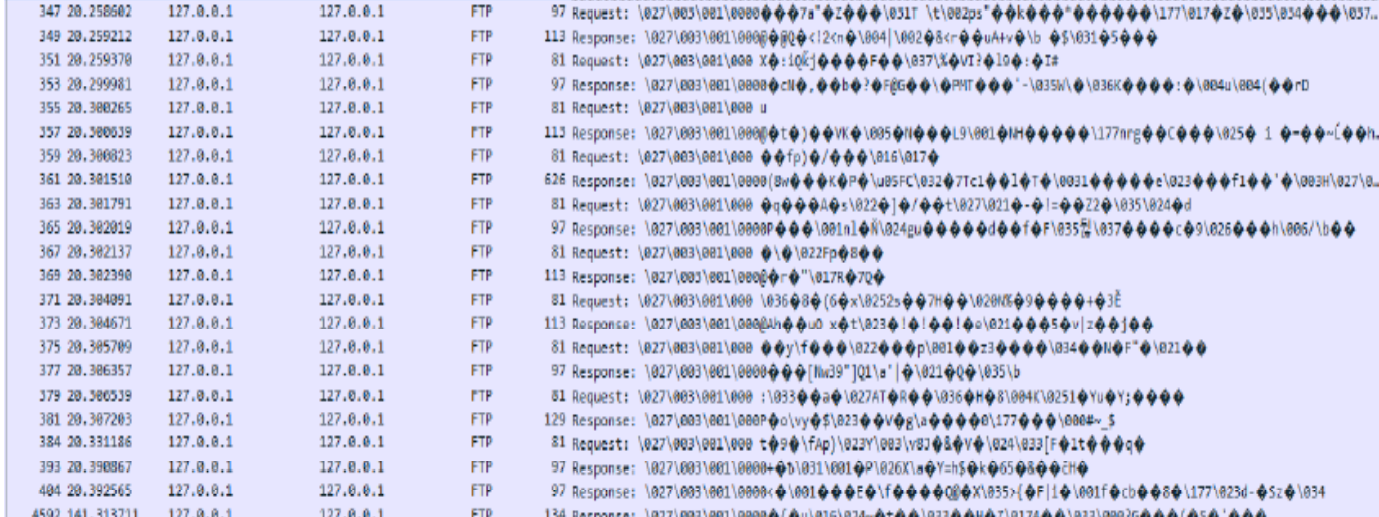


# ۹

خیر چرا که تنظیمات ssl را فعال کردیم .

# ۱۰

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



# 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>

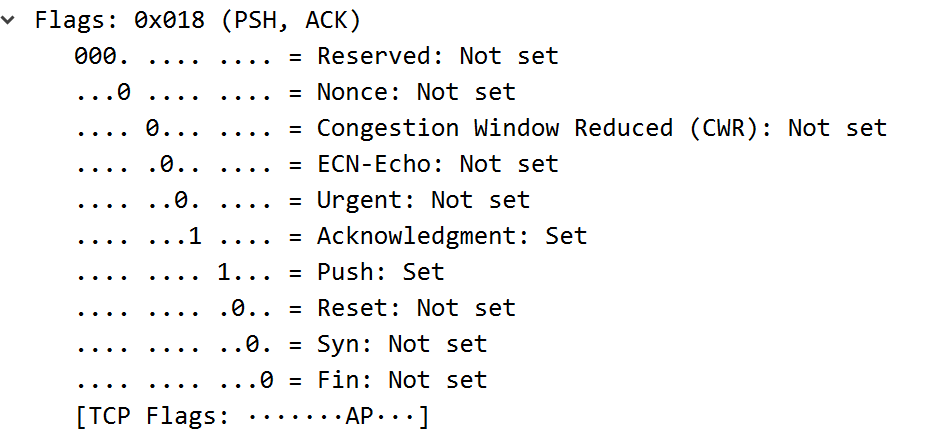
<p>The document has moved <a href="https://aut.ac.ir:443/">here</a>.</p>

</body></html>

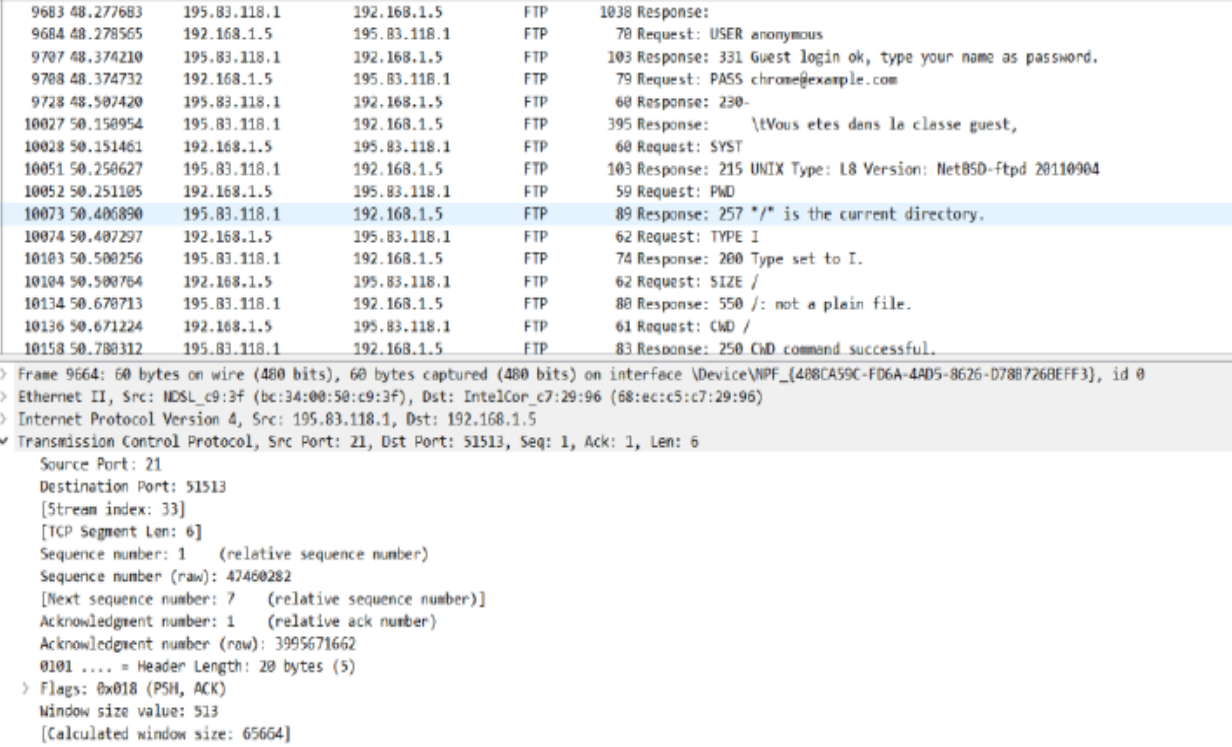
مقدار connection برابر keep-alive و درخواست GET ست. مقدار user-agent پررنگ شده.

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:



# FTP



پرتکل لابه ی transport این بسته ها TCP است .

پورت مبدا 21 و پورت مقصد 51513 می باشد . مقدار username ، anonymous است و مقدار password ، chrome@example.com می باشد که همگی در شکل قابل مشاهده می باشند .