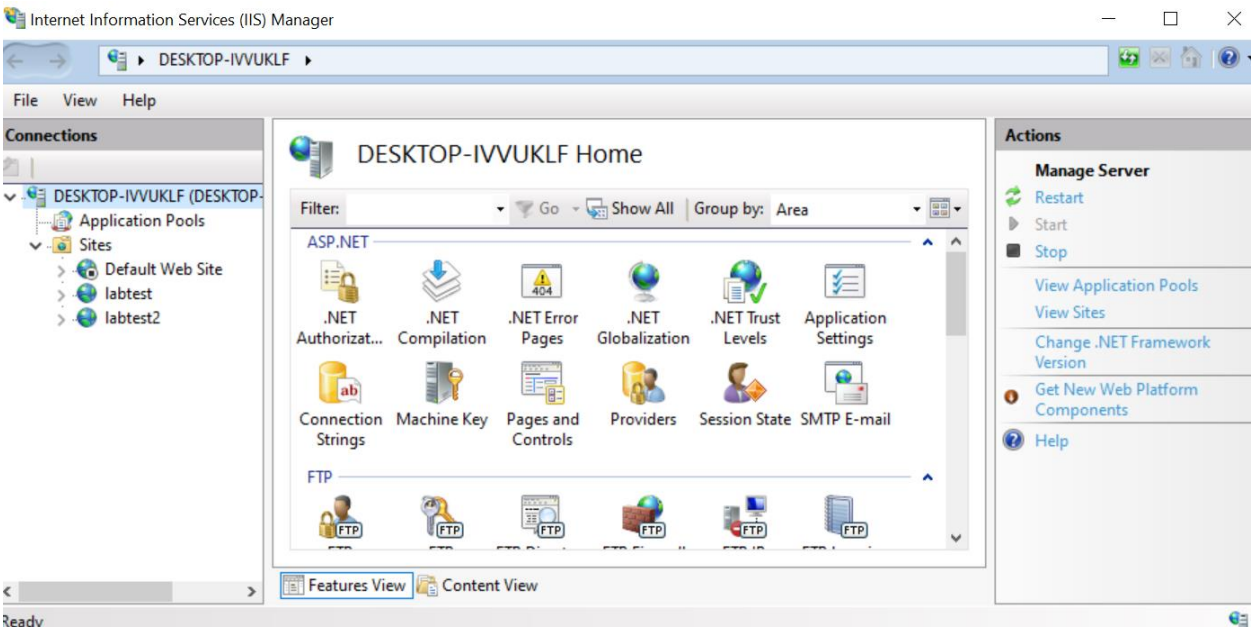
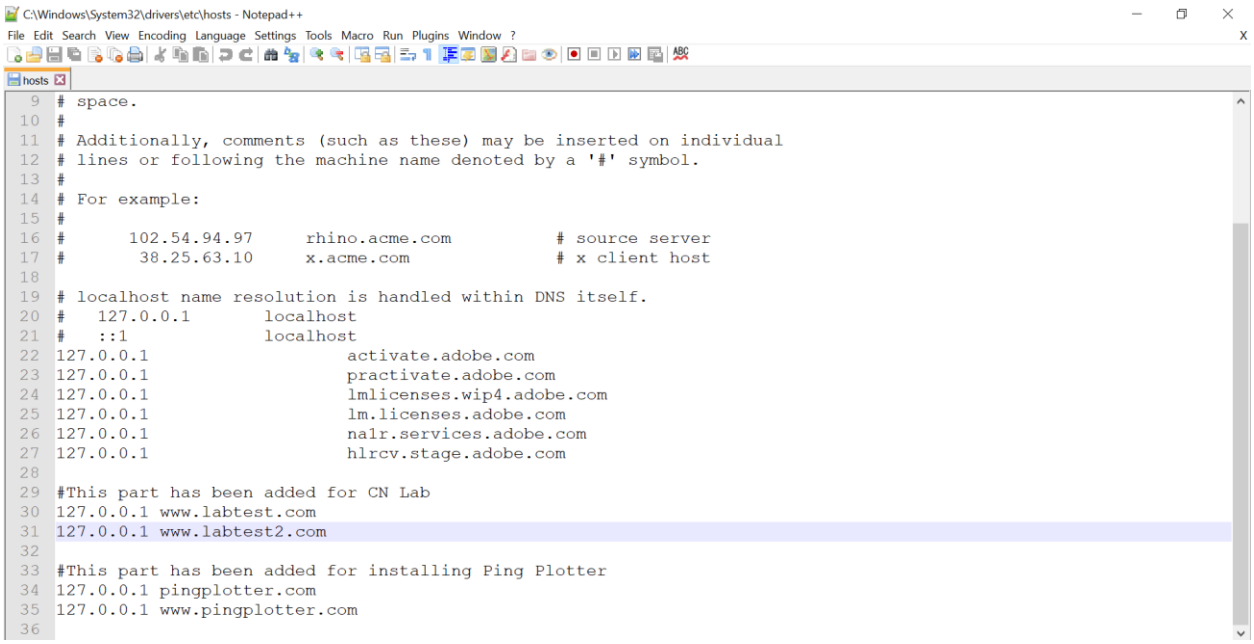
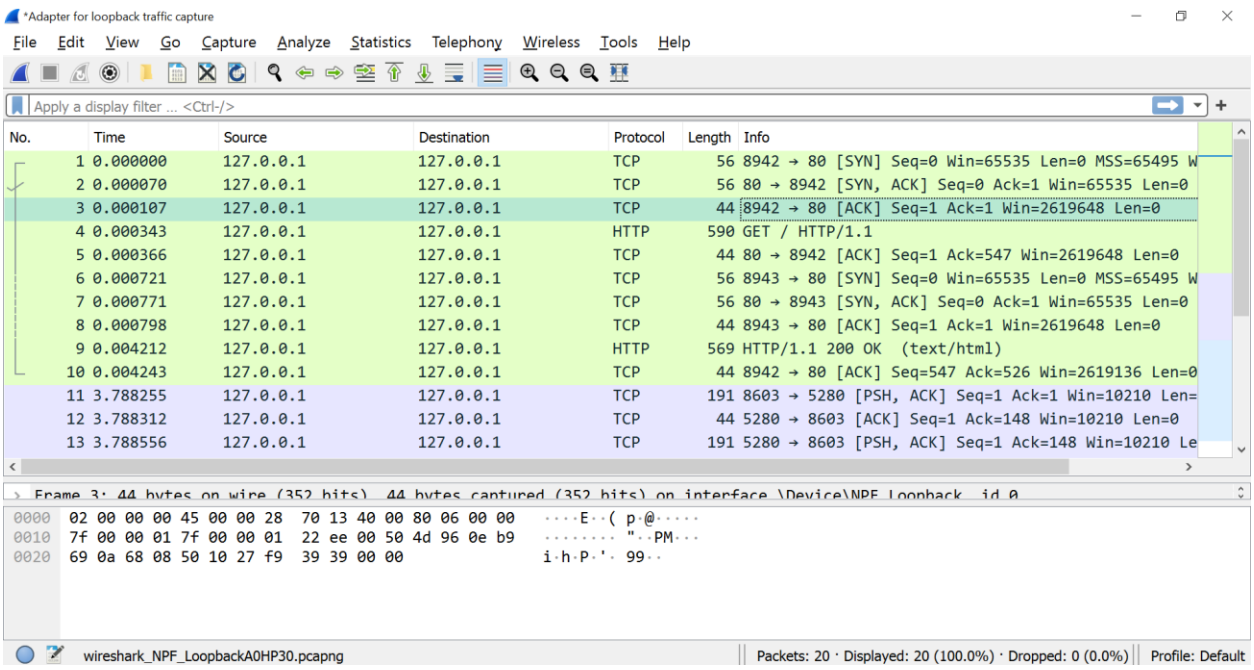
ساخت سایت‌ها


Internet Information Services (IIS) Manager
DESKTOP-IVVUKLF
File View Help
Connections
DESKTOP-IVVUKLF (DESKTOP-
Application Pools
Sites
Default Web Site
labtest
labtest2
DESKTOP-IVVUKLF Home
Filter:
Go
Show All
Group by: Area
ASP.NET
.NET Authorizat...
.NET Compilation
.NET Error Pages
.NET Globalization
.NET Trust Levels
Application Settings
Connection Strings
Machine Key
Pages and Controls
Providers
Session State
SMTP E-mail
FTP
Features View
Content View
Actions
Manage Server
Restart
Start
Stop
View Application Pools
View Sites
Change .NET Framework Version
Get New Web Platform Components
Help
Ready


C:\Windows\System32\drivers\etc\hosts - Notepad++
File Edit Search View Encoding Language Settings Tools Macro Run Plugins Window ?
hosts
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 activate.adobe.com
127.0.0.1 practivate.adobe.com
127.0.0.1 lmlicenses.wip4.adobe.com
127.0.0.1 lm.licenses.adobe.com
127.0.0.1 na1r.services.adobe.com
127.0.0.1 hlrcv.stage.adobe.com
#This part has been added for CN Lab
127.0.0.1 www.labtest.com
127.0.0.1 www.labtest2.com
#This part has been added for installing Ping Plotter
127.0.0.1 pingplotter.com
127.0.0.1 www.pingplotter.com



سوال اول

آدرس پورت‌های مبدا و مقصد چیست؟ روند کلی برقراری ارتباط در پروتکل HTTP چگونه است؟ وب‌سرور چگونه درخواست شما را تشخیص می‌دهد؟

آدرس پورت کلاینت 8942 و آدرس پورت وب‌سرور 80 است.

پروتکل HTTP در لایه‌ی انتقال از پروتکل TCP استفاده می‌کند. برای همین در ابتدای ارتباط فرایند hand shaking بین کلایت و سرور انجام می‌گیرد.

وب‌سرور با استفاده از شماره پورت، درخواست ما را تشخیص می‌دهد. در اینجا چون شماره پورت برابر 80 است، وب‌سرور متوجه می‌شود که نوع درخواست از نوع HTTP است و باید object های مربوط به سایت را انتقال دهد.

سوال دوم

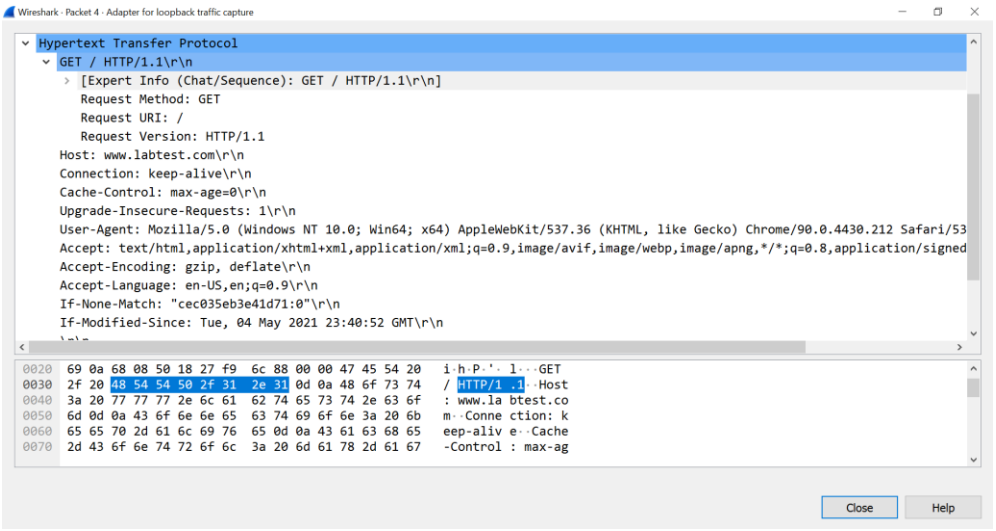
مقدار بخش connection چیست؟ درخواست HTTP از نوع GET بوده است یا از نوع POST ؟ مقدار user agent چیست؟ به نظر شما این مقدار بیانگر چه چیزی است؟

مقدار connection برابر با Keep-alive است. به این معنی که ارتباط از نوع persistent است. درخواست HTTP از نوع GET بوده است.

مقدار user agent برابر با مقدار زیر است:

```
Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/90.0.4430.212 Safari/537.36
```

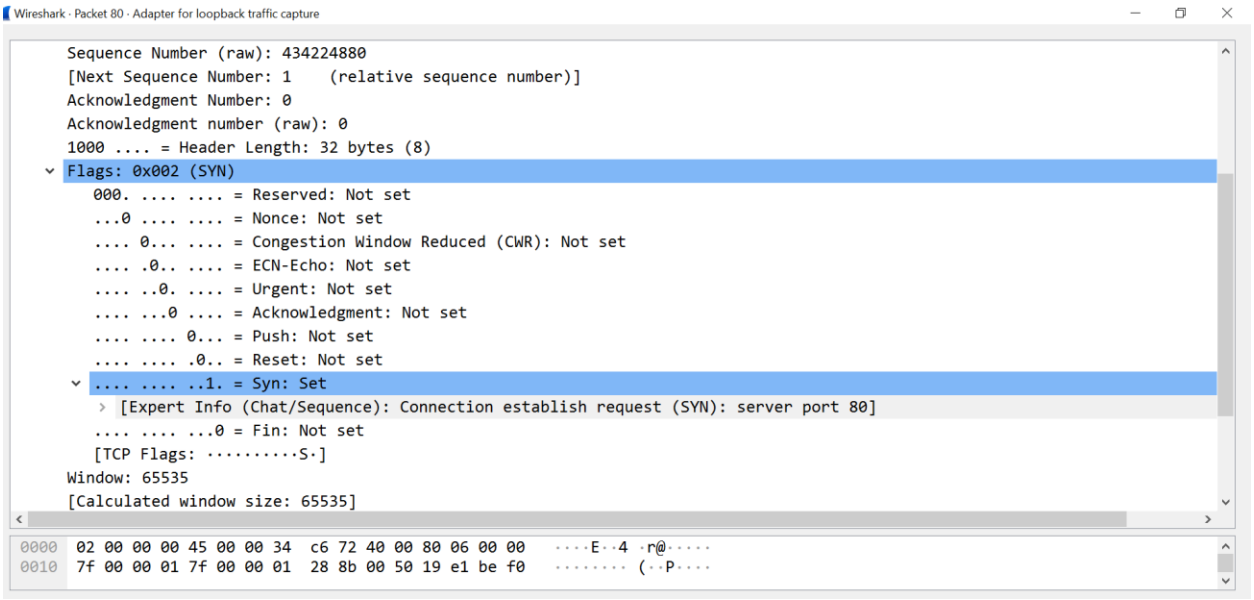
استفاده از این هدر باعث می‌شود که سرور بتواند نوع برنامه، سیستم عامل و ورژن درخواست-دهنده(در اینجا مرورگر) را پیدا کند. زیرا نوع نمایش اشیا در هرکدام از مرورگرها متفاوت است و سرور باید شی با فرمت مناسب را برگرداند.



سوال سوم

در پنجره باز شده اولین بسته را انتخاب کنید. سپس مقدار Flags در پروتکل TCP را مشاهده کنید. چه مقادیری برای این بسته تنظیم شده است؟

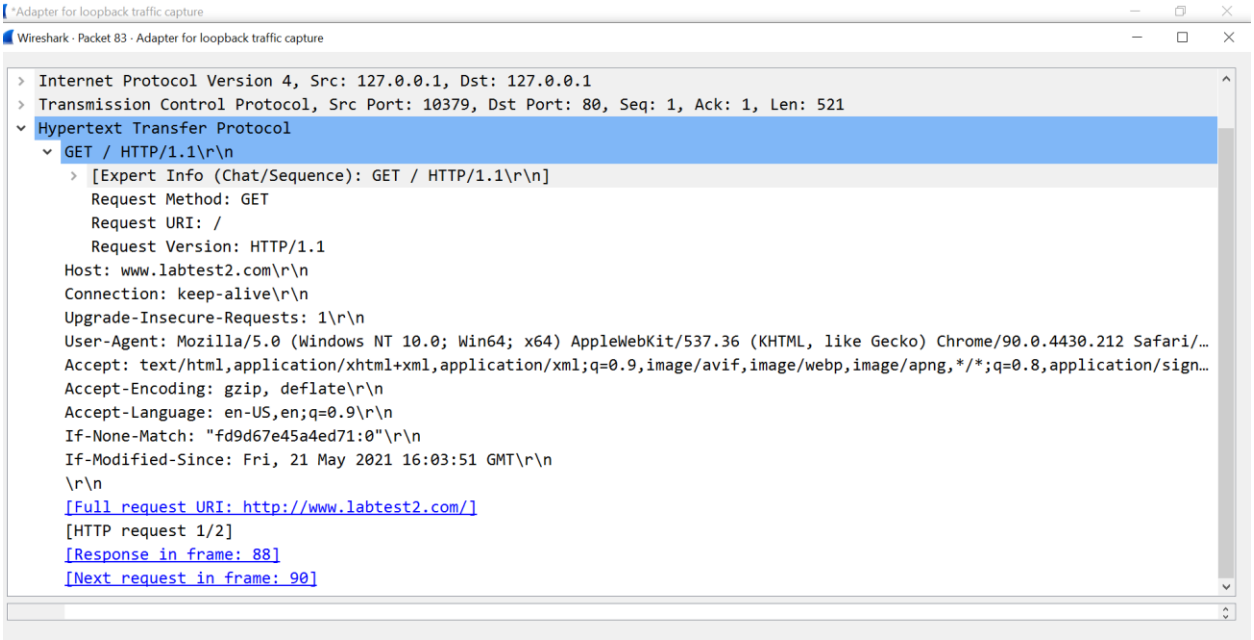
مقدار این فیلد برابر با 0x002 است. به این معنی که مقدار SYN ست شده است.



سوال چهارم

یک سایت دیگر با نام دلخواه ایجاد کنید. سپس مقدار Flags در پروتکل TCP را مشاهده کنید. چه مقادیری برای این بسته تنظیم شده است؟

در قسمت پرچم‌های این سایت هم مانند سایت قبلی فیلد SYN ست شده است. تفاوت‌های این درخواست ها را می‌توان در آدرس هاست و پورت مبدا و محتوای پیام و ... یافت.



سوال پنجم

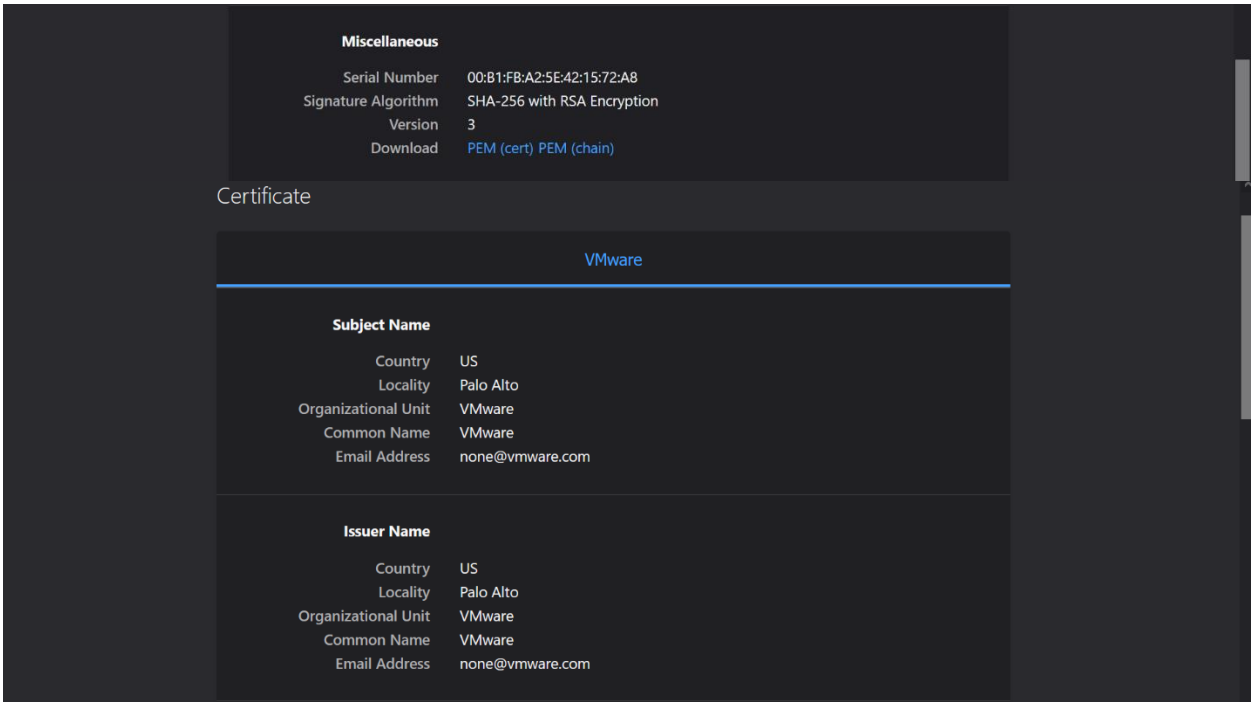
مشخص کنید که گواهی را چه کسی و برای چه کسی صادر کرده، مدت زمان اعتبار گواهی ، کلید عمومی صادر کننده و امضای دیجیتال انجام شده با چه الگوریتم‌هایی انجام شده اند؟

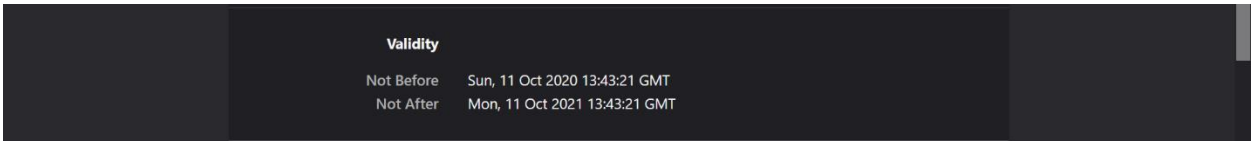
صادرکننده و دریافت‌کننده VMware است.

مدت اعتبار گواهی یک سال است. از 13:43 روز 11 اکتبر 2020 تا 13:43 روز 11 اکتبر 2021.

کلید عمومی صادرکننده یک عدد 2048 بیتی است.

امضای دیجیتال با الگوریتم SHA-256 با رمزنگاری RSA انجام شده است.

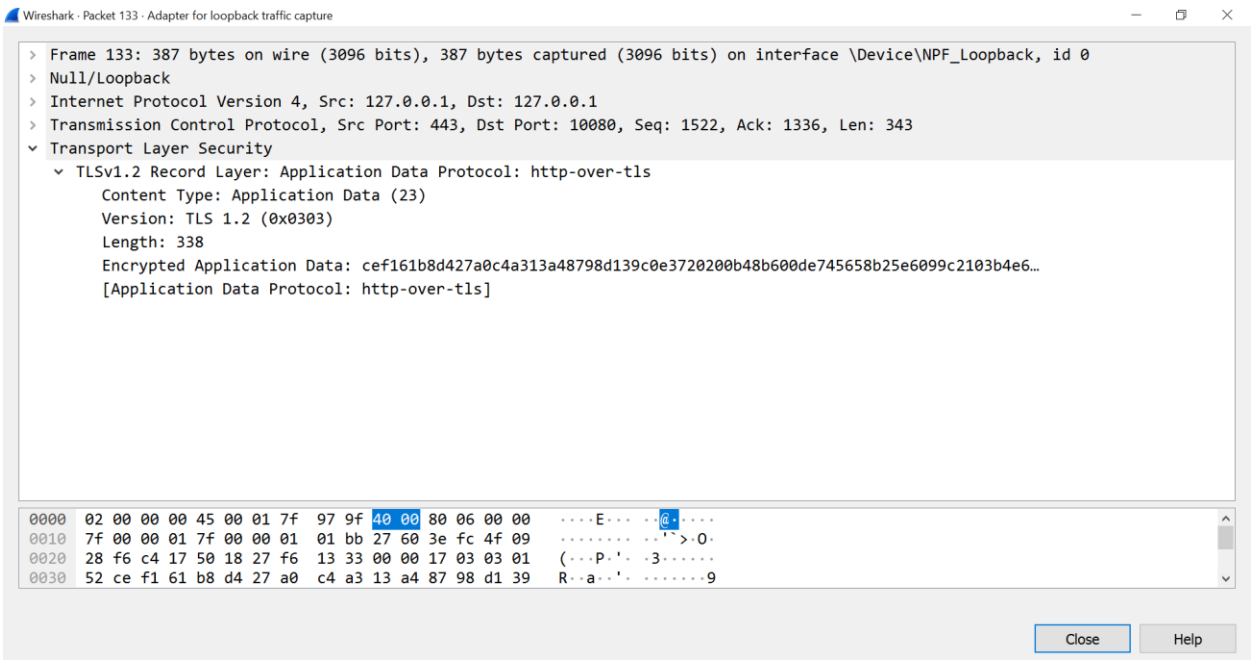




سوال ششم

آیا می‌توانید متن ارتباط را بخوانید؟

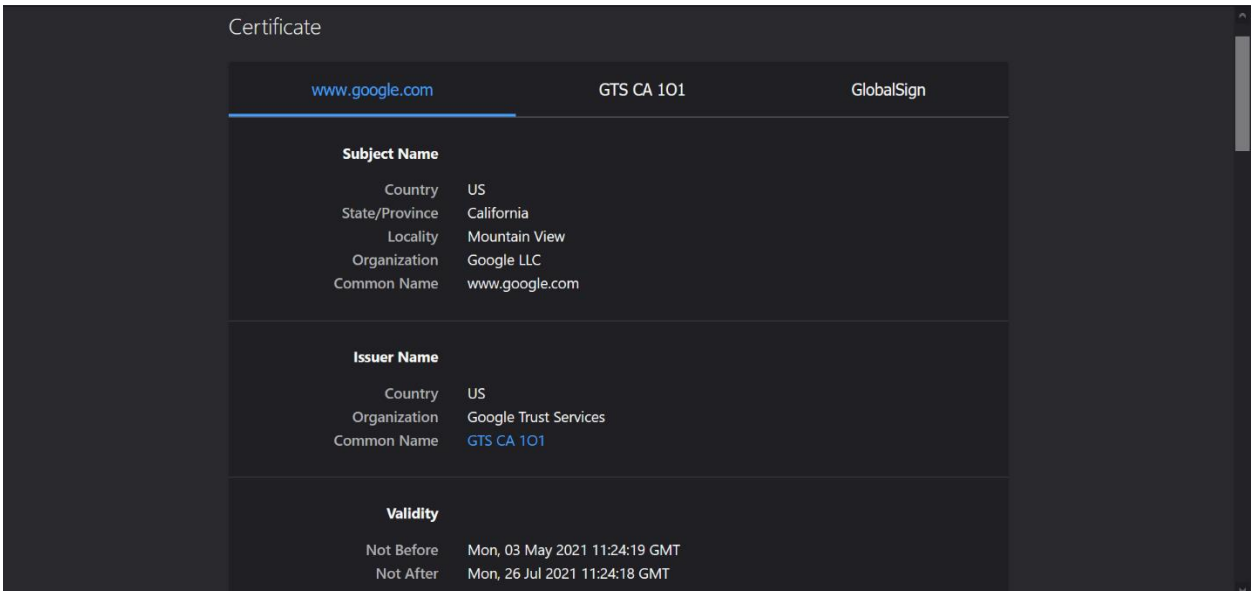
خیر. از آنجا که داده رمزگذاری شده است، نمی‌توان متن ارتباط را خواند.

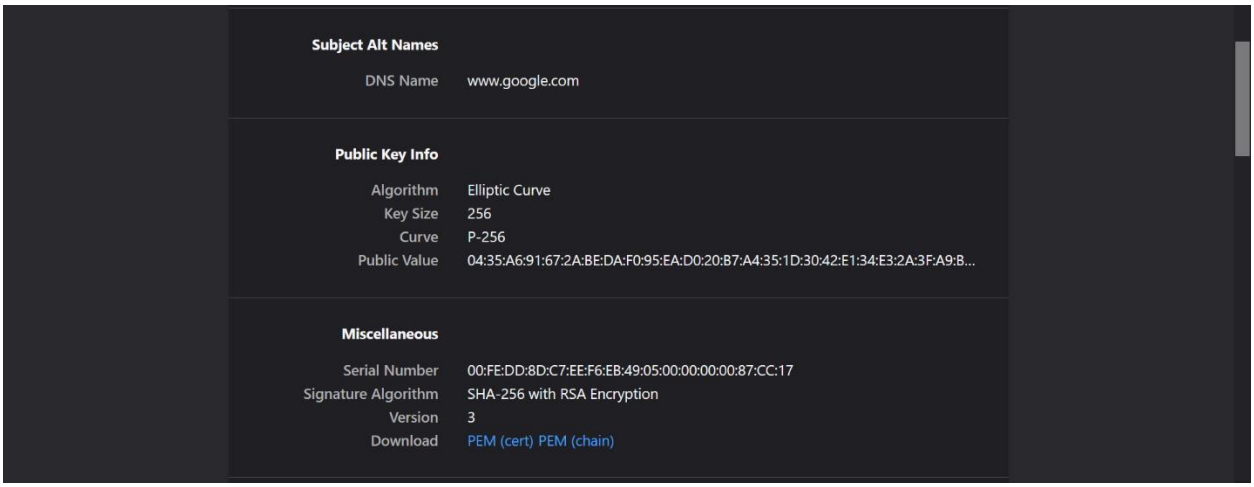


سوال هفتم

گواهی آن سایت با گواهی سایت شما چه فرقی دارد؟

صادر کننده و دریافت کننده گواهی فرق دارند. همچنین الگوریتم رمزنگاری و زمان صدور اعتبار و مدت زمان اعتبار از جمله تفاوت‌های گواهی سایت ما با `google.com` است.



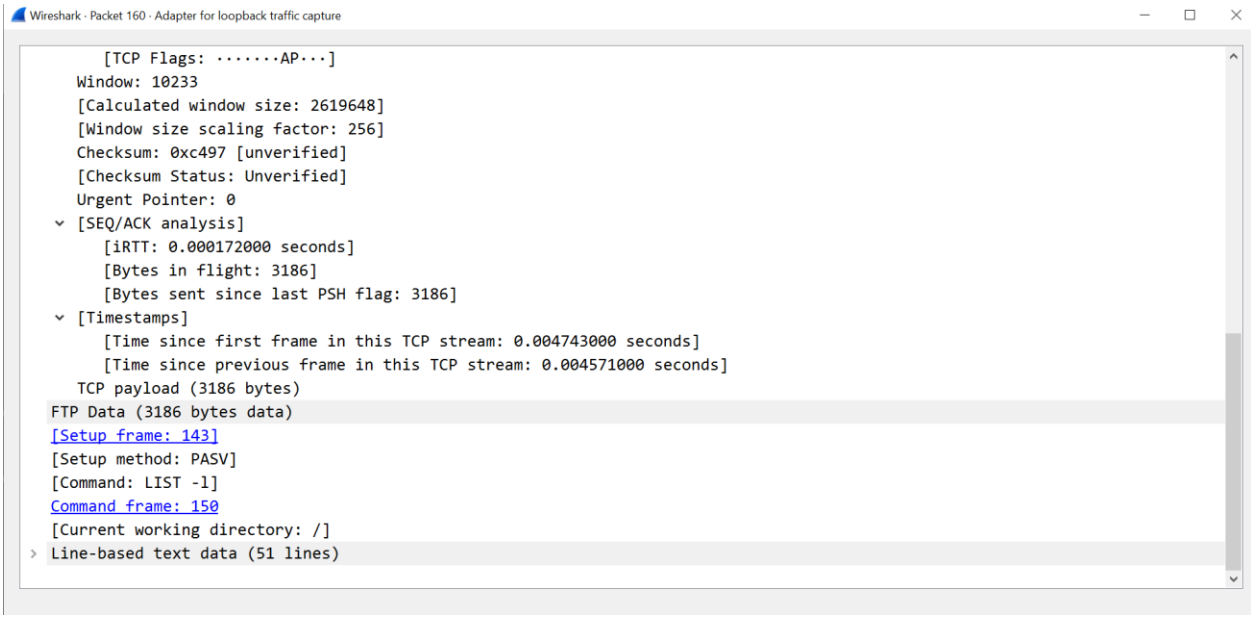


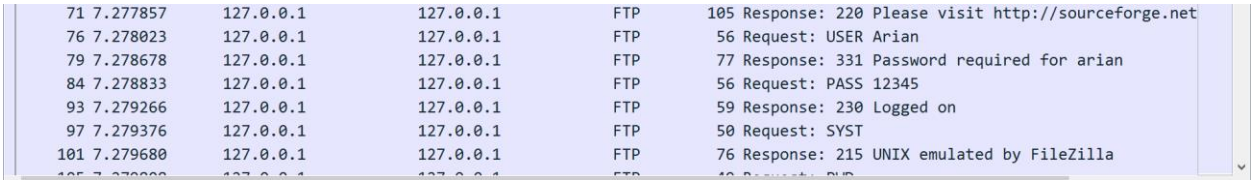
سوال هشتم

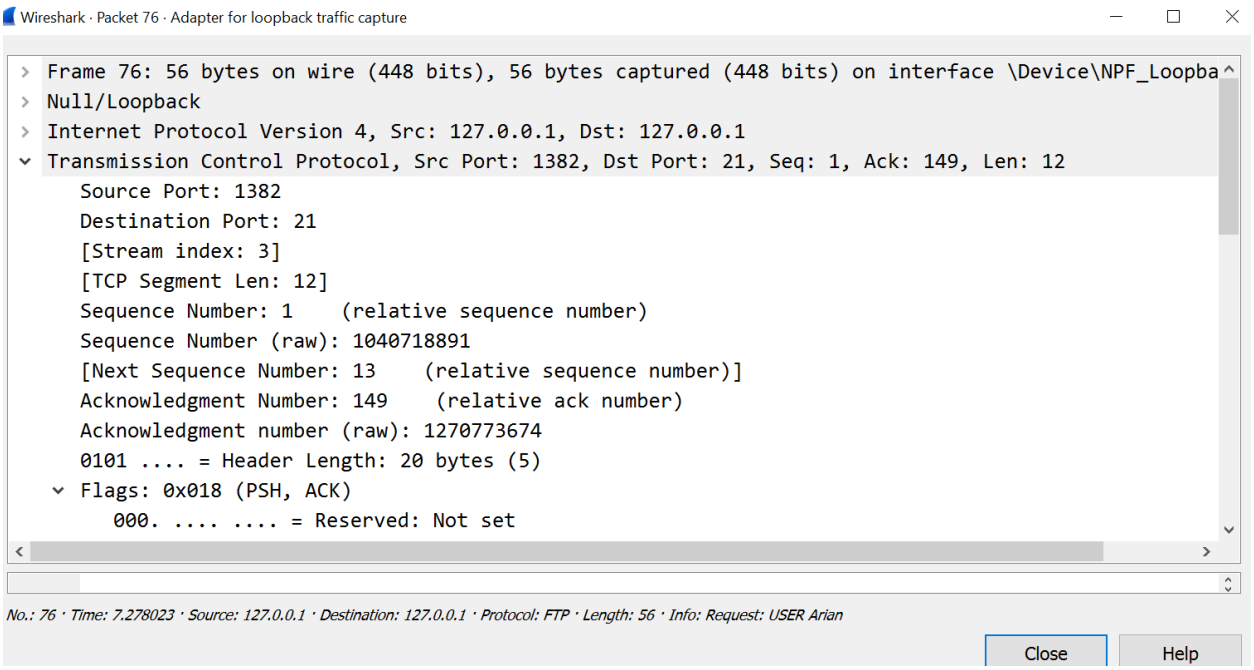
مشخص کنید از چه دستوری برای لیست کردن فایل‌های دیرکتوری استفاده شده است؟ مشخص کنید چه نام کاربری برای دسترسی به سایت استفاده شده است و پروتکل لایه‌ی Transport استفاده شده برای این بسته چیست؟ آدرس پورت مبدا و مقصد ارتباط را مشخص کنید.

از دستور `list -l` برای لیست کردن استفاده شده است.

همانطود که از شکل‌ها مشخص است، کاربر `Arian` با رمز عبور `12345` به سایت دسترسی پیدا کرده است. از پروتکل `TCP` برای انتقال استفاده شده است. پورت مبدا `1382` و پورت مقصد `21` است.







سوال نهم

سعی کنید دوباره سایت را از مرورگر باز کنید. آیا دوباره می‌توانید به سایت وارد شوید؟

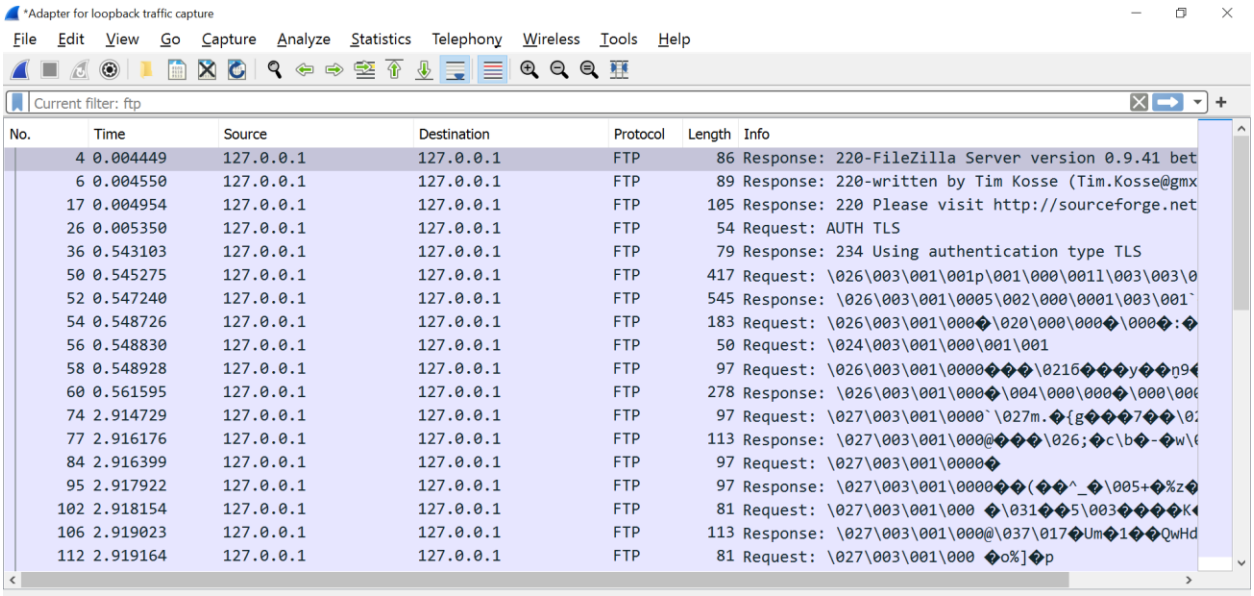
در این حالت محتوایی نشان داده نمی‌شود، زیرا تنظیمات SSL در این حالت فعال شده است.

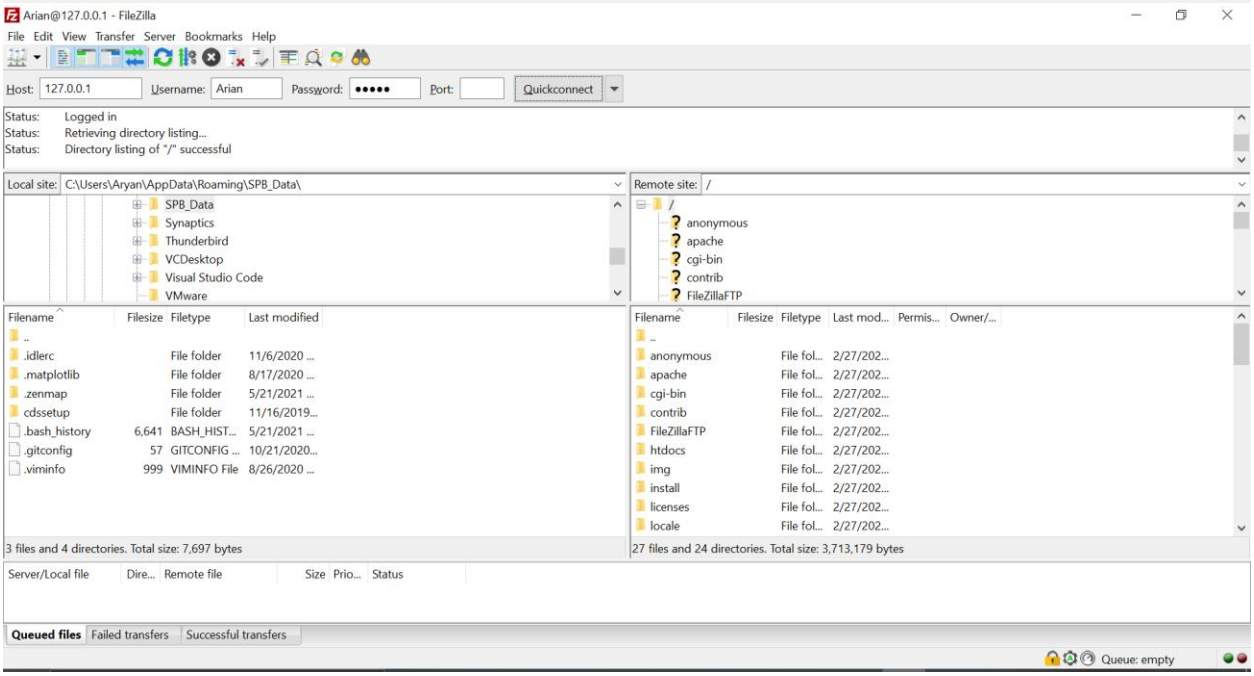
سوال دهم

برنامه `Filezilla` را دانلود کنید. ارتباط را با استفاده از وایرشارک شنود کنید. آیا نام کاربری و پسورد قابل خواندن است؟

خیر.

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


*Adapter for loopback traffic capture
File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help
Current filter: ftp
No. Time Source Destination Protocol Length Info
4 0.004449 127.0.0.1 127.0.0.1 FTP 86 Response: 220-FileZilla Server version 0.9.41 bet
6 0.004550 127.0.0.1 127.0.0.1 FTP 89 Response: 220-written by Tim Kosse (Tim.Kosse@gmx
17 0.004954 127.0.0.1 127.0.0.1 FTP 105 Response: 220 Please visit http://sourceforge.net
26 0.005350 127.0.0.1 127.0.0.1 FTP 54 Request: AUTH TLS
36 0.543103 127.0.0.1 127.0.0.1 FTP 79 Response: 234 Using authentication type TLS
50 0.545275 127.0.0.1 127.0.0.1 FTP 417 Request: \026\003\001\001p\001\000\001l\003\003\0
52 0.547240 127.0.0.1 127.0.0.1 FTP 545 Response: \026\003\001\0005\002\000\0001\003\001`
54 0.548726 127.0.0.1 127.0.0.1 FTP 183 Request: \026\003\001\000\020\000\000\000:
56 0.548830 127.0.0.1 127.0.0.1 FTP 50 Request: \024\003\001\000\001\001
58 0.548928 127.0.0.1 127.0.0.1 FTP 97 Request: \026\003\001\0000\0216y
60 0.561595 127.0.0.1 127.0.0.1 FTP 278 Response: \026\003\001\000\004\000\000\000\000
74 2.914729 127.0.0.1 127.0.0.1 FTP 97 Request: \027\003\001\0000`\027m.{g7
77 2.916176 127.0.0.1 127.0.0.1 FTP 113 Response: \027\003\001\000@\026;c\b-w
84 2.916399 127.0.0.1 127.0.0.1 FTP 97 Request: \027\003\001\0000
95 2.917922 127.0.0.1 127.0.0.1 FTP 97 Response: \027\003\001\0000(^_\005+%z
102 2.918154 127.0.0.1 127.0.0.1 FTP 81 Request: \027\003\001\000 \031\0005\003K
106 2.919023 127.0.0.1 127.0.0.1 FTP 113 Response: \027\003\001\000@\037\017Um1QwHd
112 2.919164 127.0.0.1 127.0.0.1 FTP 81 Request: \027\003\001\000 o%]p


Arian@127.0.0.1 - FileZilla
File Edit View Transfer Server Bookmarks Help
Host: 127.0.0.1 Username: Arian Password: ••••• Port: Quickconnect
Status: Logged in
Status: Retrieving directory listing...
Status: Directory listing of "/" successful
Local site: C:\Users\Aryan\AppData\Roaming\SPB_Data\
SPB_Data
Synaptics
Thunderbird
VCDesktop
Visual Studio Code
VMware
Remote site: /
anonymous
apache
cgi-bin
contrib
FileZillaFTP
Filename Filesize Filetype Last modified
.idlerc File folder 11/6/2020 ...
.matplotlib File folder 8/17/2020 ...
.zenmap File folder 5/21/2021 ...
cdssetup File folder 11/16/2019...
.bash_history 6,641 BASH_HIST... 5/21/2021 ...
.gitconfig 57 GITCONFIG ... 10/21/2020...
.viminfo 999 VIMINFO File 8/26/2020 ...
Filename Filesize Filetype Last mod... Permis... Owner/...
anonymous File fol... 2/27/202...
apache File fol... 2/27/202...
cgi-bin File fol... 2/27/202...
contrib File fol... 2/27/202...
FileZillaFTP File fol... 2/27/202...
htdocs File fol... 2/27/202...
img File fol... 2/27/202...
install File fol... 2/27/202...
licenses File fol... 2/27/202...
locale File fol... 2/27/202...
3 files and 4 directories. Total size: 7,697 bytes
27 files and 24 directories. Total size: 3,713,179 bytes
Server/Local file Dire... Remote file Size Prio... Status
Queued files Failed transfers Successful transfers
Queue: empty