

«باسم‌هه تعالی»



گزارش کار آزمایش چهارم
راه اندازی سرویس‌های Web و FTP



طراحی و تدوین:

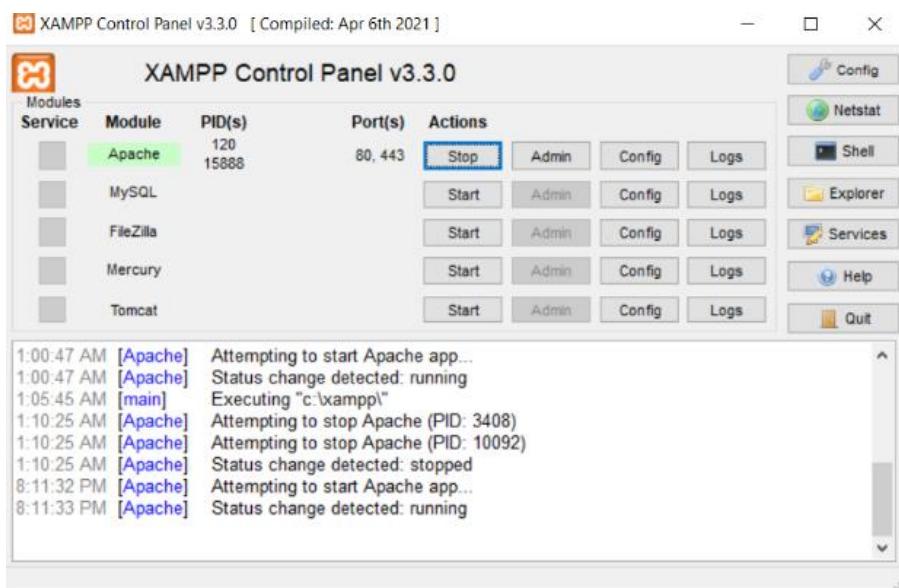
9731701 / مهدی رحمانی

هدف آزمایش

هدف این آزمایش، آشنایی با تنظیمات مقدماتی مربوط به راه اندازی سرویس‌های Web و FTP و تحلیل بسته‌های HTTP و FTP است.

فراهم کردن پیش نیاز های آزمایش

ابتدا باید برنامه XAMPP را نصب و را اندازی کنیم. پس از اینکه آن را نصب کردیم آن را باز می‌کنیم و با زدن start Apache Module مربوط به Apache باید شود :



سپس با وارد کردن 127.0.0.1 در مرورگر با این صفحه مواجه می‌شویم:

Welcome to XAMPP for Windows 8.0.6

You have successfully installed XAMPP on this system! Now you can start using Apache, MariaDB, PHP and other components. You can find more info in the FAQs section or check the HOW-TO Guides for getting started with PHP applications.

XAMPP is meant only for development purposes. It has certain configuration settings that make it easy to develop locally but that are insecure if you want to have your installation accessible to others. If you want have your XAMPP accessible from the internet, make sure you understand the implications and you checked the FAQs to learn how to protect your site. Alternatively you can use WAMP, MAMP or LAMP which are similar packages which are more suitable for production.

Start the XAMPP Control Panel to check the server status.

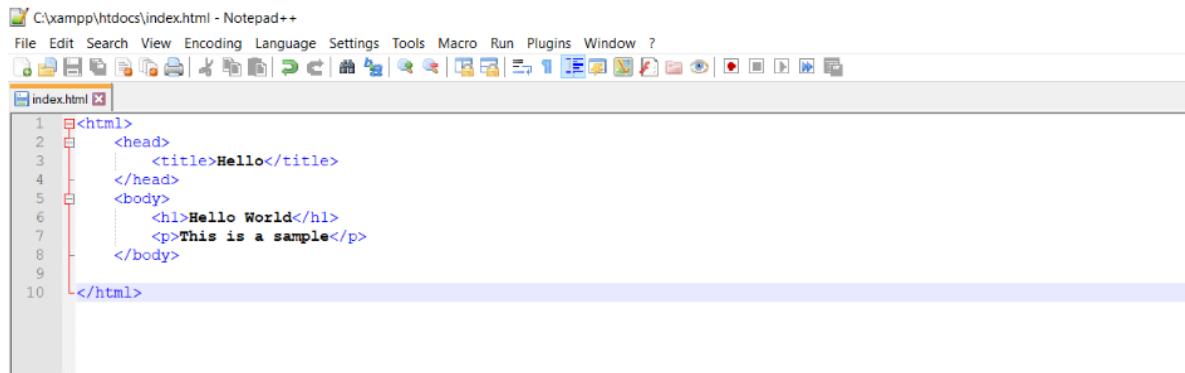
Community

XAMPP has been around for more than 10 years – there is a huge community behind it. You can get involved by joining our Forums, adding yourself to the Mailing List, and liking us on Facebook, following our exploits on Twitter, or adding us to your Google+ circles.

اطلاعات مربوط به این صفحه در فایل xampp/htdocs قرار دارد. سپس میتوانیم آن ها را حذف کنیم و فایل html مربوط به صفحه خودمان را آنجا قرار دهیم:

Name	Date modified	Type	Size
dashboard	5/13/2021 12:49 AM	File folder	
img	5/13/2021 12:49 AM	File folder	
webalizer	5/13/2021 12:49 AM	File folder	
xampp	5/13/2021 12:49 AM	File folder	
applications.html	8/27/2019 6:32 PM	Microsoft Edge HT...	4 KB
bitnami.css	8/27/2019 6:32 PM	Cascading Style Sh...	1 KB
favicon.ico	7/16/2015 8:02 PM	Icon	31 KB
index.php	7/16/2015 8:02 PM	PHP File	1 KB

سپس فایل HTML موردنظر را به صورت زیر ایجاد میکنیم و در همان مسیر ذخیره میکنیم:



```
C:\xampp\htdocs\index.html - Notepad++
File Edit Search View Encoding Language Settings Tools Macro Run Plugins Window ?
index.html
1 <html>
2   <head>
3     <title>Hello</title>
4   </head>
5   <body>
6     <h1>Hello World</h1>
7     <p>This is a sample</p>
8   </body>
9
10 </html>
```

حال اگر بار دیگر 127.0.0.1 را در مرورگر وارد کنیم با صفحه زیر روبرو میشویم:



Hello World

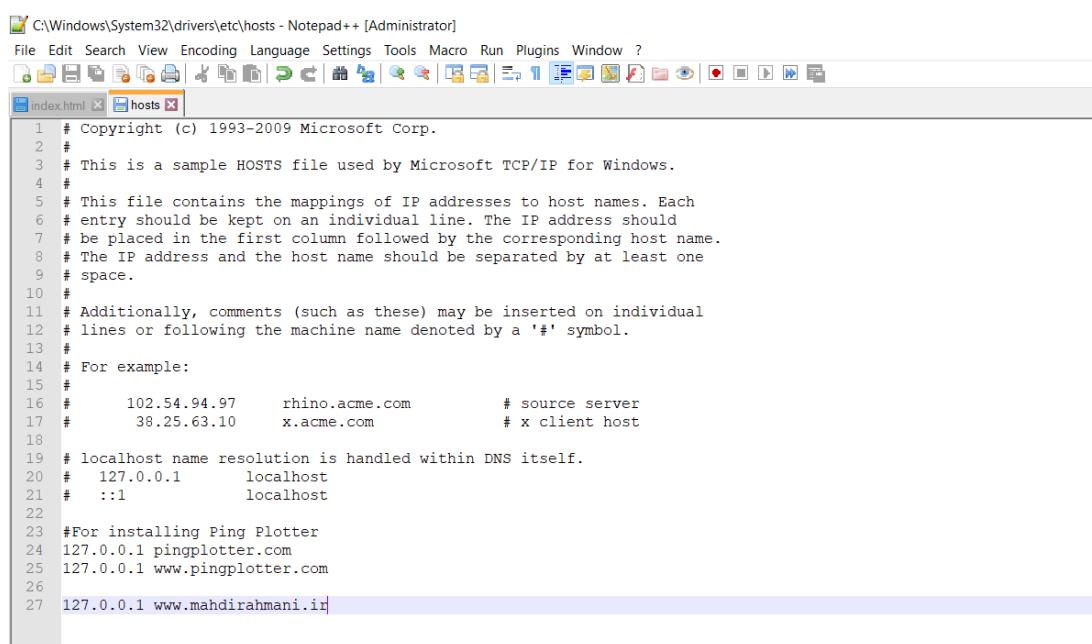
This is a sample

اگر دقت شود در مرورگر IP Address مربوط به local host خودمون را وارد میکنیم، میتوانیم این آدرس را به هر نام دامنه‌ای که میخواهیم map کنیم که هرموقع این نام را وارد کردیم به این صفحه‌ای که خودمون طراحی کردیم وارد بشیم. برای این کار به فایل hosts در مسیر زیر مرجعه میکنیم:

LocalDisk(c:)/Windows/System32/drivers/etc

برای مثال من نام دامنه را به این صورت میگذارم: www.mahdirahmani.ir

پس باید خط 27 در شکل زیر را به فایل hosts اضافه کنیم و آن را ذخیره کنیم:



```
C:\Windows\System32\drivers\etc\hosts - Notepad++ [Administrator]
File Edit Search View Encoding Language Settings Tools Macro Run Plugins Window ?
index.html hosts

1 # Copyright (c) 1993-2009 Microsoft Corp.
2 #
3 # This is a sample HOSTS file used by Microsoft TCP/IP for Windows.
4 #
5 # This file contains the mappings of IP addresses to host names. Each
6 # entry should be kept on an individual line. The IP address should
7 # be placed in the first column followed by the corresponding host name.
8 # The IP address and the host name should be separated by at least one
9 # space.
10 #
11 # Additionally, comments (such as these) may be inserted on individual
12 # lines or following the machine name denoted by a '#' symbol.
13 #
14 # For example:
15 #
16 #      102.54.94.97    rhino.acme.com        # source server
17 #              38.25.63.10    x.acme.com          # x client host
18 #
19 # localhost name resolution is handled within DNS itself.
20 #      127.0.0.1        localhost
21 #              ::1           localhost
22 #
23 #For installing Ping Plotter
24 127.0.0.1 pingplotter.com
25 127.0.0.1 www.pingplotter.com
26
27 127.0.0.1 www.mahdirahmani.ir
```

حال نام دامنه سایت خود را در مرورگر وارد میکنیم و میبینیم که همان صفحه‌ی قبلی را برای ما می‌آورد:



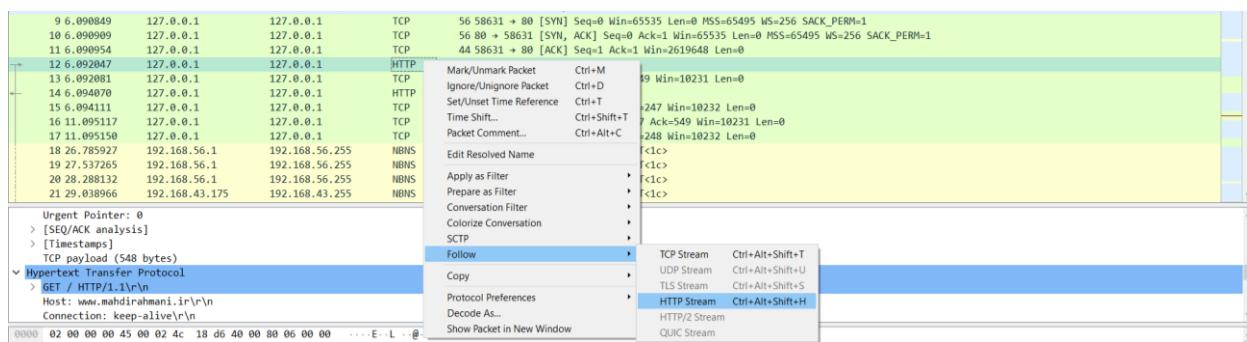
شرح آزمایش

تنظیمات سرور Web

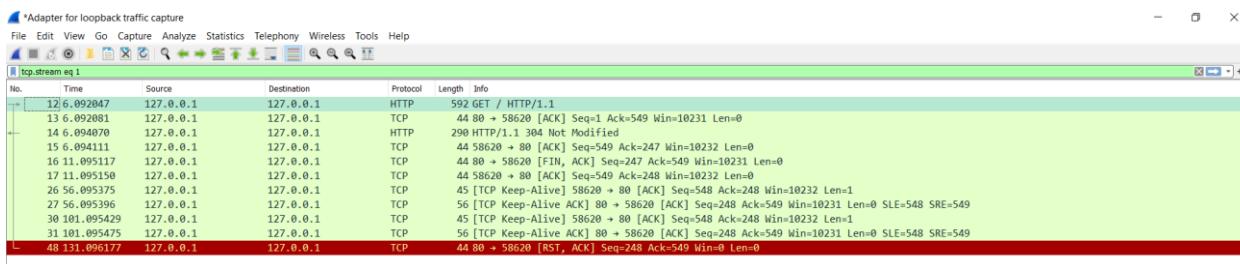
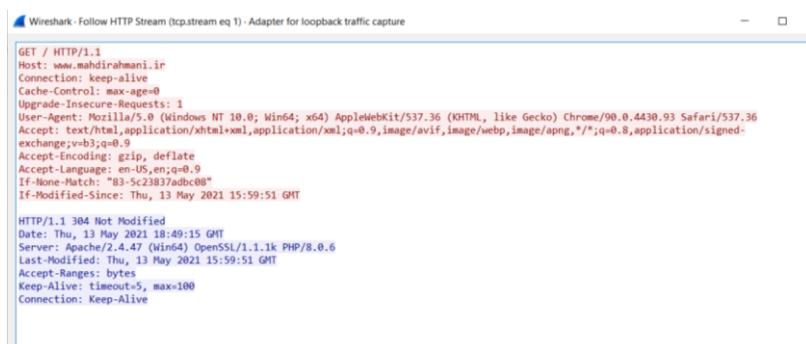
مرحله اول) آدرس سایتی که ساختیم را در مرورگر وارد میکنیم و بسته های مربوط به سایت را میابیم:

9 6.099849	127.0.0.1	127.0.0.1	TCP	56 58631 → 80 [SYN] Seq=0 Win=65535 Len=0 MSS=65495 WS=256 SACK_PERM=1
10 6.099999	127.0.0.1	127.0.0.1	TCP	56 80 + 58631 [SYN, ACK] Seq=0 Ack=1 Win=65535 Len=0 MSS=65495 WS=256 SACK_PERM=1
11 6.099954	127.0.0.1	127.0.0.1	TCP	44 58631 → 80 [ACK] Seq=1 Ack=1 Win=2619648 Len=0
12 6.092047	127.0.0.1	127.0.0.1	HTTP	592 GET / HTTP/1.1
13 6.092081	127.0.0.1	127.0.0.1	TCP	44 80 + 58620 [ACK] Seq=1 Ack=549 Win=10231 Len=0
14 6.094070	127.0.0.1	127.0.0.1	HTTP	290 HTTP/1.1 304 Not Modified
15 6.094111	127.0.0.1	127.0.0.1	TCP	44 58620 → 80 [ACK] Seq=549 Ack=247 Win=10232 Len=0
16 11.095117	127.0.0.1	127.0.0.1	TCP	44 80 + 58620 [FIN, ACK] Seq=247 Ack=549 Win=10232 Len=0
17 11.095150	127.0.0.1	127.0.0.1	TCP	44 58620 → 80 [ACK] Seq=549 Ack=248 Win=10232 Len=0
17 11.095150	127.0.0.1	127.0.0.1	TCP	44 58620 → 80 [ACK] Seq=549 Ack=248 Win=10232 Len=0

بر روی یکی از آن ها کلیک راست میکنیم و follow HTTP Stream را انتخاب میکنیم:



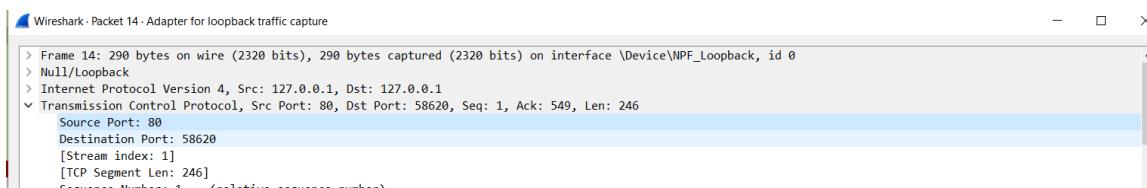
بعد از اینکه آن را انتخاب کردیم با این موارد زیر روبرو میشویم:



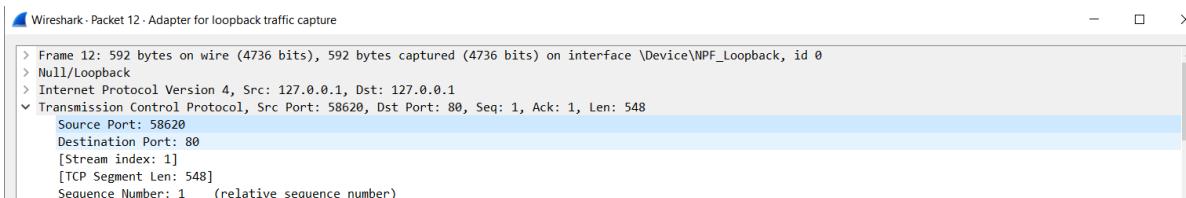
سوال 1: آدرس پورت‌های مبدأ و مقصد چیست؟ روند برقراری ارتباط در پروتکل HTTP چگونه است؟ وب سرور چگونه آدرس سایت درخواستی شما را تشخیص می‌دهد؟

چون در اینجا هم سرور و هم host روی سیستم خودمان است به خاطر همین آدرس IP مبدأ و مقصد برابر با 127.0.0.1 میباشد.

شماره پورت مبدأ برابر با 80 است و شماره پورت مقصد برابر با 58620 میباشد.



البته میدانیم که HTTP روی پورت 80 فعالیت دارد و در تصویر بالا هم پیام موردنظر پیام پاسخی است که از سمت سرور موردنظر آمده است. مثلا اگر بسته‌ی دیگری را انتخاب کنیم که بسته‌ی درخواستی است که از سمت client میرودا وقت شماره پورت مبدأ برابر با 58620 میباشد و شماره پورت مقصد برابر با 80 است.



وقتی کاربر صفحه‌ای را درخواست میکند، مرورگر چندیدن درخواست HTTP به سرور میفرستد. سرور بعد از دریافت درخواست‌ها، با برگرداندن اشیای متناظر به این درخواست‌ها پاسخ میدهد.

پروتکل HTTP از TCP به عنوان پروتکل انتقال استفاده میکند، به همین دلیل در اولین قدم باید یک اتصال TCP با سرور برقرار کند. بعد از برقراری این اتصال، فرآیندهای مرورگر و سرور از طریق سوکت‌های خود با یکدیگر حرف میزنند. فرآیند client درخواست‌های HTTP را به سوکت سمت خود میدهد و پاسخ برگشتی سرور را از طریق همین سوکت دریافت میکند. به طریق مشابه فرآیند سرور درخواست‌های کاربر را از این سوکت میگیرد و پاسخ‌های خود را به واسطه‌ی همین سوکت به مشتری برمیگرداند.

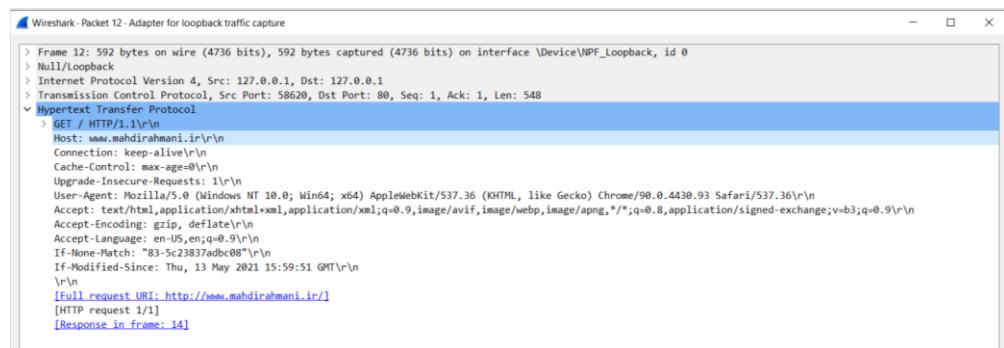
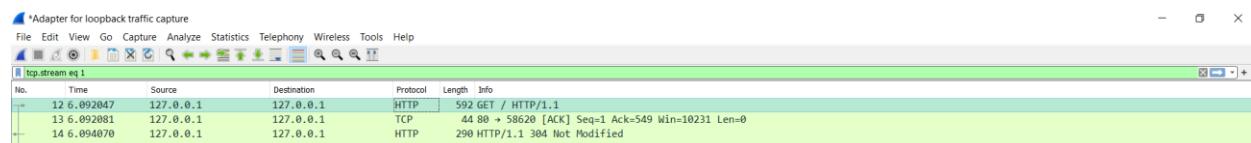
این برقراری اتصال در HTTP میتواند به دو شکل non-persistent connection و persistent connection باشد.

در حالت client اول باید درخواست برقراری اتصال TCP بدهد و بعد که برقرار شد درخواست فایل Base HTML را میدهد و در آن به چندین شیء دیگر ارجاع داده میشود. سپس روی همان اتصال TCP که اول برقرار شد بقیه object ها را هم درخواست میکند و دریافت میکند. این کار میتواند به دو صورت pipe و بدون pipe line انجام شود.

در حالت non-persistent اول باید درخواست برقراری اتصال TCP بدهد و بعد که برقرار شد درخواست فایل Base HTML را میدهد و در آن به چندین شیء دیگر ارجاع داده میشود. سپس برای دریافت هر کدام از object ها در این حالت یک اتصال TCP جدایگانه باید ایجاد شود. این کار میتواند به دو صورت موازی و غیرموازی انجام شود.

با توجه به اینکه در قسمت hosts آدرس سایت خود را وارد کردیم، وب سرور ما از آن جا آدرس سایت ما را میابد. ولی در حالت کلی وقتی نام دامنه را وارد میکنیم به کمک DNS server ها و ارسال یک پیام با رکورد A میتوانیم IP Address مربوط به آن سایت را تشخی داد. در اینجا که سرور هم روی سیستم خودمان است نقش DNS سرور را هم خود سیستم بازی میکند و در hosts که گفتیم دامنه‌ی mahdirahmani.ir را به 127.0.0.1 مپ کن این اتفاق می‌افتد و این گونه وب سرور آدرس سایت را میابد.

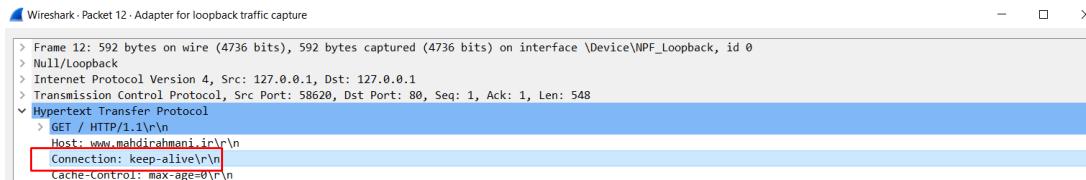
مرحله دوم) بر روی اولین بسته در پنجره باز شده کلیک کنید. بخش‌های مختلف پروتکل HTTP را مشاهده کنید.



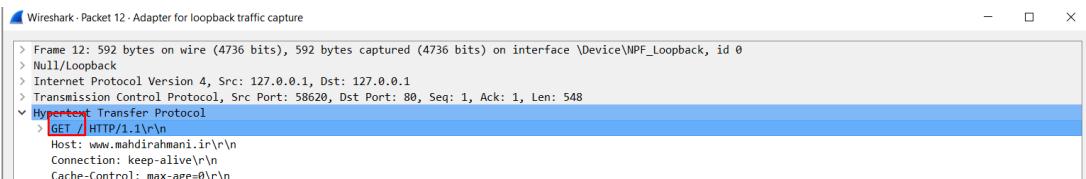
سوال 2: مقدار بخش Connection چیست؟ درخواست HTTP از نوع POST بوده است یا از نوع GET

مقدار User Agent چیست؟ به نظر شما این مقدار بیانگر چه چیزی است؟

مقدار بخش connection برابر keep-alive میباشد. درواقع میگوید بعد از اتمام این transaction درحال جریان اتصال همچنان باز است. درواقع اتصال persistent است و بسته نیست ، اجازه می دهد تا درخواستهای بعدی به همان سرور انجام شود.



درخواست HTTP از نوع GET بوده است. در خط request line که خط نخست در پیام درخواست میباشد فیلد اول که فیلد متده است میباشد این را مشخص میکند.



خط سرآیند User-agent درواقع همان مرورگر وب که از سرویس دهنده درخواست کرده، را مشخص میکند.

در اینجا User-agent ما برابر با مقدار زیر است:

Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/90.0.4430.93 Safari/537.36



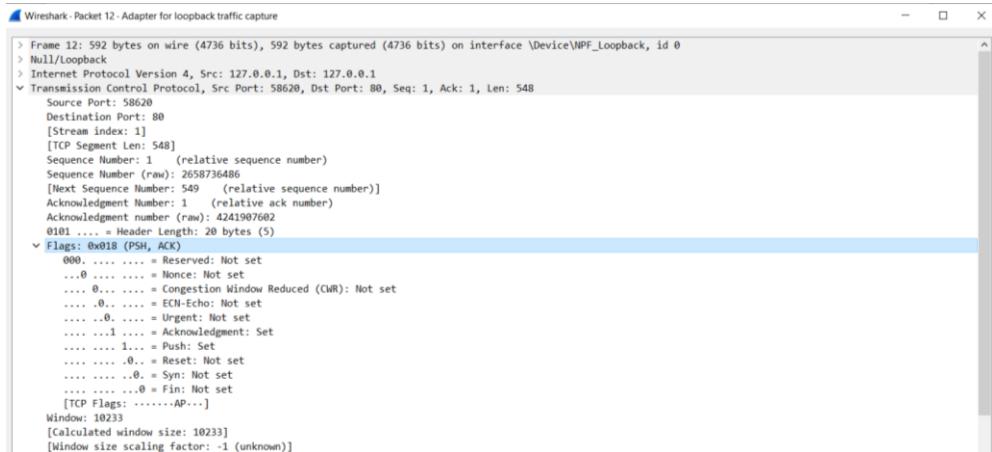
سودمندی این خط سرآیند از آن جهت است که یک سرویس دهنده میتواند ویرایش های متفاوتی از یک شیء برای هر مرورگر وب داشته باشد .

هدر درخواست User-Agent یک رشته مشخصه است که به سرورها و network peer اجازه می دهد تا application ، سیستم عامل و یا نسخه و ورژن درخواست کننده را شناسایی کنند.

سوال 3: در پنجره باز شده، اولین بسته را انتخاب کنید. سپس مقدار Flags در پروتکل TCP را مشاهده کنید.

چه مقداری برای این بسته تنظیم شده است؟

برای اولین بسته که یک بسته‌ی HTTP میباشد، مقادیر ACK و PSH برای TCP در لایه‌ی Transport تنظیم شده است.



در اتصال TCP، پرچم‌ها برای نشان دادن وضعیت خاصی از اتصال یا ارائه برخی از اطلاعات مفید اضافی مانند اهداف عیب یابی یا کنترل یک اتصال خاص استفاده می‌شوند. پرچمهایی که معمولاً استفاده می‌شوند. هر پرچم مربوط به 1 بیت اطلاعات است.

: برای تأیید بسته‌های موفقیت آمیز دریافت شده توسط host استفاده می‌شود. اگر قسمت شماره acknowledgement شامل یک شماره acknowledgement معتبر باشد، این پرچم تنظیم می‌شود و مقدارش 1 می‌شود.

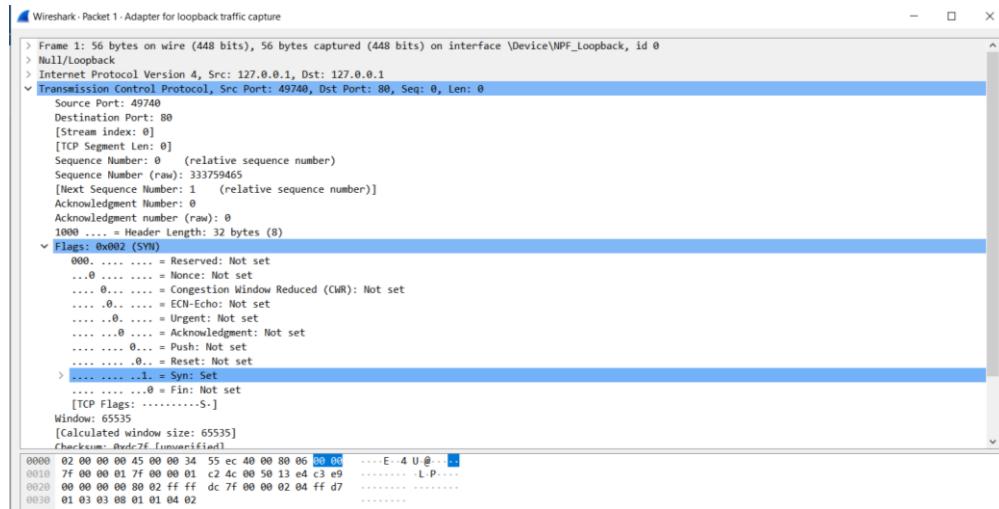
لایه transport (PSH) : به طور پیش فرض مدتی منتظر می‌ماند تا لایه application داده کافی را به اندازه حداقل اندازه یک segment ارسال کند تا تعداد بسته‌های منتقل شده در شبکه به حداقل برسد که برای برخی از برنامه‌ها مانند برنامه‌های تعاملی (چت) مطلوب نیست. به همین ترتیب لایه transport گیرنده بافر کردن بسته‌ها را تا جایی که به یه حد مشخص برسد انجام میدهد بعد به لایه‌ی application انتقال میدهد.

با استفاده از PSH این مشکل برطرف می‌شود. لایه انتقال 1 PSH = را تنظیم می‌کند و به محض دریافت سیگнал از لایه application بلافاصله قطعه را به لایه network می‌فرستد. لایه انتقال گیرنده، با دیدن PSH = 1 بلافاصله داده‌ها را به لایه application هدایت می‌کند.

به طور کلی ، به گیرنده می گوید این بسته ها را به جای بافر کردن ، همانطور که دریافت می شوند پردازش کند.

توجه شود:

اگر منظور اولین بسته‌ی TCP بوده است که دریافت شده، اطلاعات این بسته به صورت زیر است. طبق آن مقدار SYN تنظیم شده و بیت متناظر آن 1 شده است:

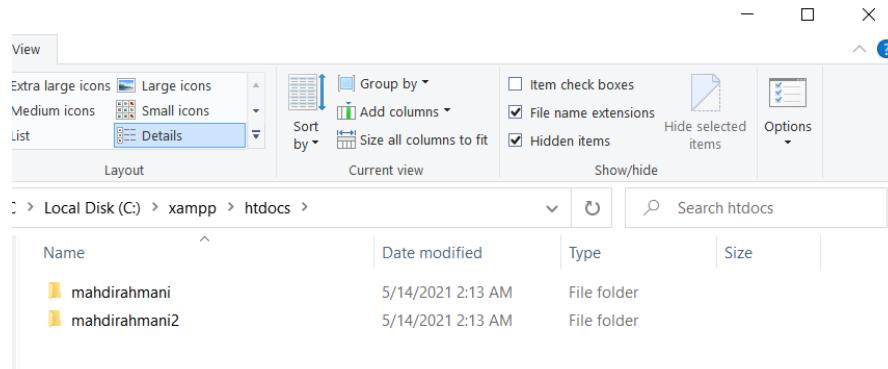


این در گام اول مرحله برقراری اتصال یا فرایند 3-way handshake (SYN) میزبان استفاده می شود. فقط بسته اول از طرف فرستنده و همچنین گیرنده باید این پرچم را تنظیم کند. این برای همگام سازی شماره توالی استفاده می شود ، یا به عبارتی برای این است که به سیستم انتهایی دیگر بگوید که باید انتظار چه شماره‌ای را در مرحله‌ی بعد داشته باشد.

سوال 4: یک سایت دیگر با نام دلخواه ایجاد کنید و بسته‌های مربوط به آن را شنود کنید. چه تفاوتی بین این دو

سایت وجود دارد؟

همانطور که در عکس زیر دیده می‌شود در مسیر xampp/htdocs دو پوشه درست کردیم که در پوشه‌ی اول سایت اول ما و در پوشه‌ی دوم سایت دوم ما می‌باشد و فایل‌های html مربوط به سایت‌ها را در آن‌ها ایجاد می‌کنیم:



فایل html مربوط به سایت دوم نیز به صورت زیر می‌باشد:

```
C:\xampp\htdocs\mahdirahmani2\index.html - Notepad++ [Administrator]
File Edit Search View Encoding Language Settings Tools Macro Run Plugins Window ?
hosts httpd-vhosts.conf index.html
1 <html>
2   <head>
3     <title>Hello</title>
4   </head>
5   <body>
6     <h1>Hello World</h1>
7     <p>This is second sample</p>
8   </body>
9
10 </html>
11
```

حال به فایل httpd-vhosts.conf در مسیر زیر می‌رویم:

LocalDisk(c:)/xampp/apache/conf/extra

سپس فایل را اصلاح می‌کنیم و به صورت زیر مینویسیم:

```
C:\xampp\apache\conf\extra\httpd-vhosts.conf - Notepad++ [Administrator]
File Edit Search View Encoding Language Settings Tools Macro Run Plugins
hosts httpd-vhosts.conf index.html
1 <VirtualHost *:80>
2   DocumentRoot "C:/xampp/htdocs/mahdirahmani"
3   ServerName www.mahdirahmani.ir
4 </VirtualHost>
5
6 <VirtualHost *:80>
7   DocumentRoot "C:/xampp/htdocs/mahdirahmani2"
8   ServerName www.mahdirahmani2.ir
9 </VirtualHost>
10
11
12
13
```

همانطور که دیده میشود در قسمت root مسیر پوشه ها را مشخص کردیم.

همچنین باید تغییرات داخل فایل hosts در مسیر etc hosts را انجام

دهیم:

```

C:\Windows\System32\drivers\etc\hosts - Notepad++ [Administrator]
File Edit Search View Encoding Language Settings Tools Macro Run Plugins Window ?
index.html hosts httpd-hosts.conf index.html

1 # Copyright (c) 1993-2009 Microsoft Corp.
2 #
3 # This is a sample HOSTS file used by Microsoft TCP/IP for Windows.
4 #
5 # This file contains the mappings of IP addresses to host names. Each
6 # entry should be kept on an individual line. The IP address should
7 # be placed in the first column followed by the corresponding host name.
8 # The IP address and the host name should be separated by at least one
9 # space.
10 #
11 # Additionally, comments (such as these) may be inserted on individual
12 # lines or following the machine name denoted by a '#' symbol.
13 #
14 # For example:
15 #
16 #       102.54.94.97    rhino.acme.com        # source server
17 #             38.25.63.10          x.acme.com       # x client host
18 #
19 # localhost resolution is handled within DNS itself.
20 #       127.0.0.1            localhost
21 #             ::1           localhost
22 #
23 #For installing Ping Plotter
24 127.0.0.1 pingplotter.com
25 127.0.0.1 www.pingplotter.com
26
27 127.0.0.1 www.mahdirahmani.ir
28 127.0.0.1 www.mahdirahmani2.ir

```

حال به کمک wireshark بسته های سایت اول و سپس بسته های سایت دوم را شنود میکنیم:

برای سایت اول بسته ها به صورت زیر است:

حال برای مثال یکی از بسته ها را انتخاب میکنیم و follow HTTP stream را انجام میدهیم:

Selected packet: 1 (HTTP/1.1 304 Not Modified)

No.	Time	Source	Destination	Protocol	Length	Info
1	0.000000	127.0.0.1	127.0.0.1	TCP	44	61858 > 80 [FIN, ACK] Seq=1 Ack=1 Win=10233 Len=0
2	0.000187	127.0.0.1	127.0.0.1	TCP	44	61858 > 61858 [ACK] Seq=2 Ack=2 Win=10233 Len=0
3	0.000318	127.0.0.1	127.0.0.1	TCP	44	61857 > 80 [FIN, ACK] Seq=1 Ack=1 Win=10231 Len=0
4	0.000429	127.0.0.1	127.0.0.1	TCP	44	88 > 61857 [ACK] Seq=3 Ack=2 Win=10233 Len=0
5	0.000551	127.0.0.1	127.0.0.1	TCP	44	88 > 61858 [FIN, ACK] Seq=1 Ack=2 Win=10233 Len=0
6	0.000719	127.0.0.1	127.0.0.1	TCP	44	61858 > 80 [ACK] Seq=2 Ack=2 Win=10233 Len=0
7	0.000893	127.0.0.1	127.0.0.1	TCP	44	61855 > 80 [FIN, ACK] Seq=1 Ack=1 Win=10233 Len=0
8	0.000979	127.0.0.1	127.0.0.1	TCP	44	88 > 61855 [SYN, ACK] Seq=0 Ack=1 Win=65535 Len=0 MSS=65495 WS=256 SACK_PERM=1
9	0.001209	127.0.0.1	127.0.0.1	TCP	44	61860 > 61855 [FIN, ACK] Seq=1 Ack=1 Win=65535 Len=0 MSS=65495 WS=256 SACK_PERM=1
10	0.001323	127.0.0.1	127.0.0.1	TCP	44	61855 > 80 [ACK] Seq=2 Ack=2 Win=10233 Len=0
11	1.926039	127.0.0.1	127.0.0.1	TCP	56	61868 > 80 [SYN] Seq=0 Win=65535 Len=0 MSS=65495 WS=256 SACK_PERM=1
12	1.926079	127.0.0.1	127.0.0.1	TCP	56	88 > 61869 [SYN, ACK] Seq=0 Ack=1 Win=65535 Len=0 MSS=65495 WS=256 SACK_PERM=1
13	1.926114	127.0.0.1	127.0.0.1	TCP	44	61860 > 80 [ACK] Seq=1 Ack=1 Win=2619648 Len=0
14	1.926381	127.0.0.1	127.0.0.1	HTTP	592	GET / HTTP/1.1

Selected packet: 1 (HTTP/1.1 304 Not Modified)

Selected bytes: 1-10233

Selected hex: 1-10233

Selected ASCII: 1-10233

Selected EBCDIC: 1-10233

Selected Unicode: 1-10233

Selected Base64: 1-10233

Selected Marked: 1-10233

Selected Unmarked: 1-10233

Selected Ignored: 1-10233

Selected Ignore/Unignore Packet: Ctrl+D

Selected Set/User Time Reference: Ctrl+T

Selected Time Shift: Ctrl+Shift+T

Selected Packet Comment...: Ctrl+Alt+C

Selected Edit Resolved Name: Ctrl+Shift+E

Selected Apply as Filter: Ctrl+F

Selected Prepare as Filter: Ctrl+Shift+F

Selected Conversation Filter: Ctrl+Shift+C

Selected Colorize Conversation: Ctrl+Shift+U

Selected SCTP: Ctrl+Shift+S

Selected Follow: Ctrl+Alt+Shift+T

Selected TCP Stream: Ctrl+Alt+Shift+T

Selected UDP Stream: Ctrl+Alt+Shift+U

Selected TLS Stream: Ctrl+Alt+Shift+S

Selected HTTP Stream: **Ctrl+Alt+Shift+H**

Selected HTTP/2 Stream: Ctrl+Alt+Shift+H

Selected QUIC Stream: Ctrl+Alt+Shift+Q

Selected Urgent Pointer: 0

> [SDO/ACK analysis]

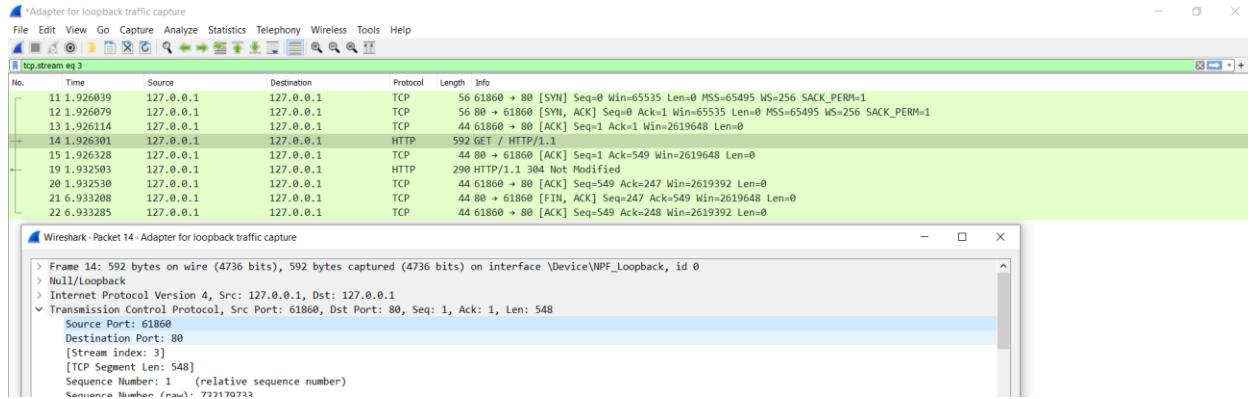
> Timestamps

TCP payload (548 bytes)

Hypertext Transfer Protocol

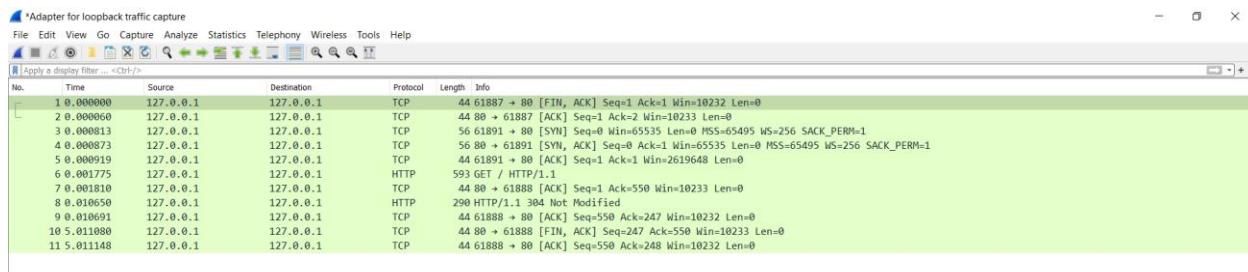
HTTP / HTTP/1.1\r\n

سپس اگر در پنجره‌ی نمایش داده شده به پورت مبدأ و مقصد نگاه کنیم و برای مثال یکی از بسته‌های را چک کنیم:

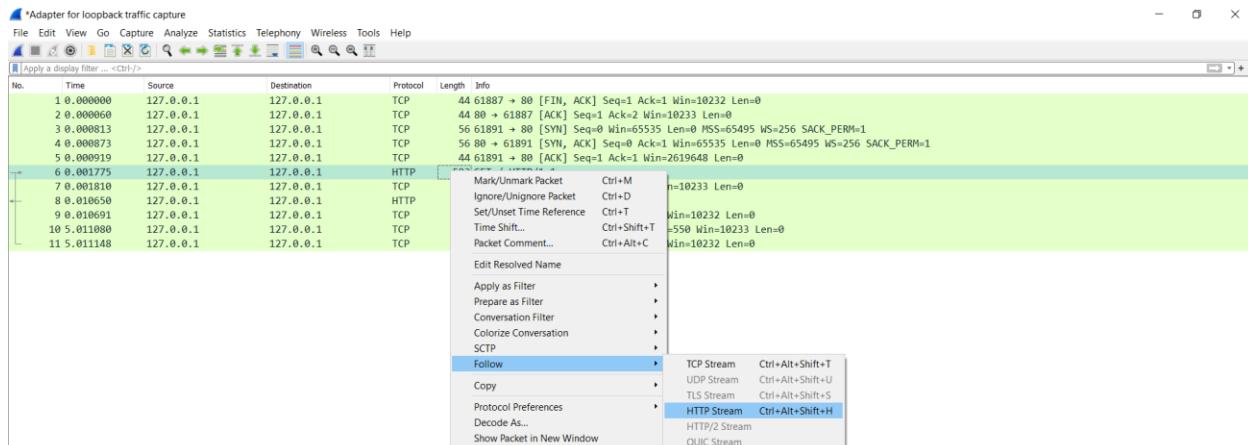


مشاهده میشود برنامه‌ی سرور روی پورت 80 و برنامه client روی پورت 61860 کار میکند.

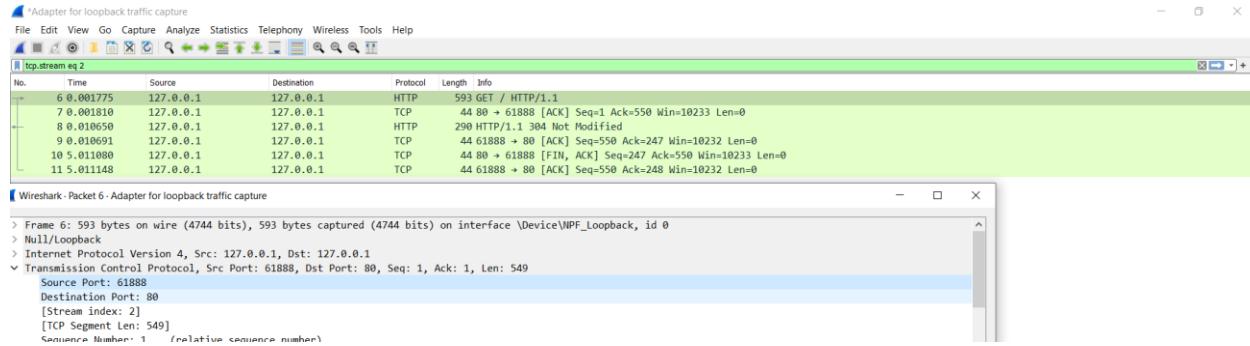
حال بسته‌های سایت دوم را دریافت میکنیم:



حال برای مثال یکی از بسته‌های را انتخاب میکنیم و follow HTTP stream را انجام میدهیم:



سپس اگر در پنجره‌ی نمایش داده شده به پورت مبدأ و مقصد نگاه کنیم و برای مثال یکی از بسته‌ها را چک کنیم:



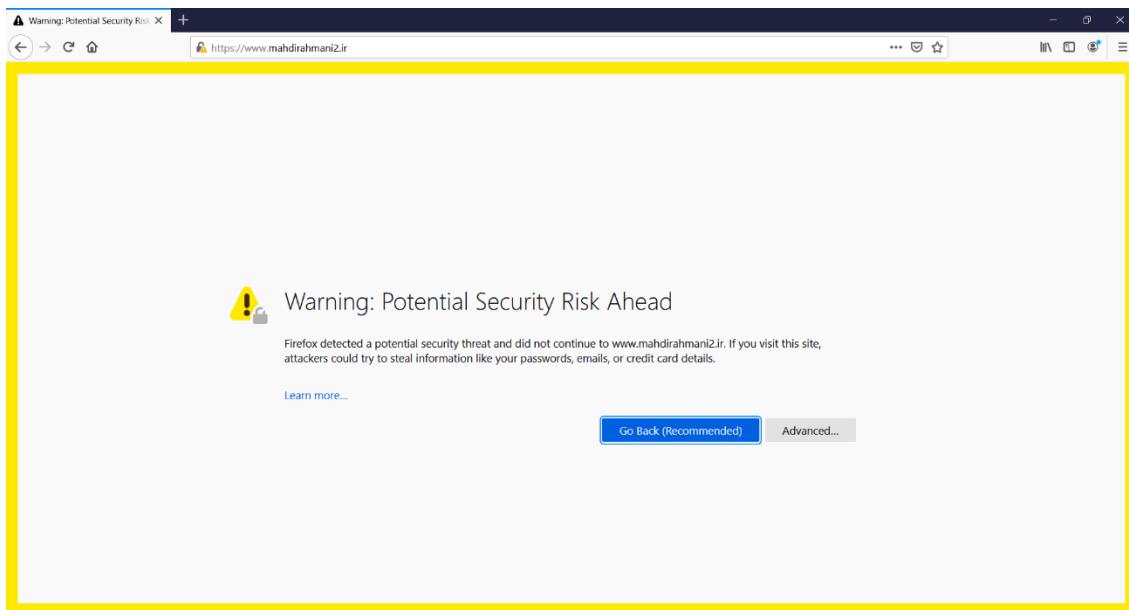
مشاهده میشود برنامه‌ی سرور روی پورت 80 و برنامه client روی پورت 61888 کار میکنند.

بنابراین یک فرق شد اینکه، پورتی که برنامه client روی آن کار میکند در این دو سایت متفاوت است.

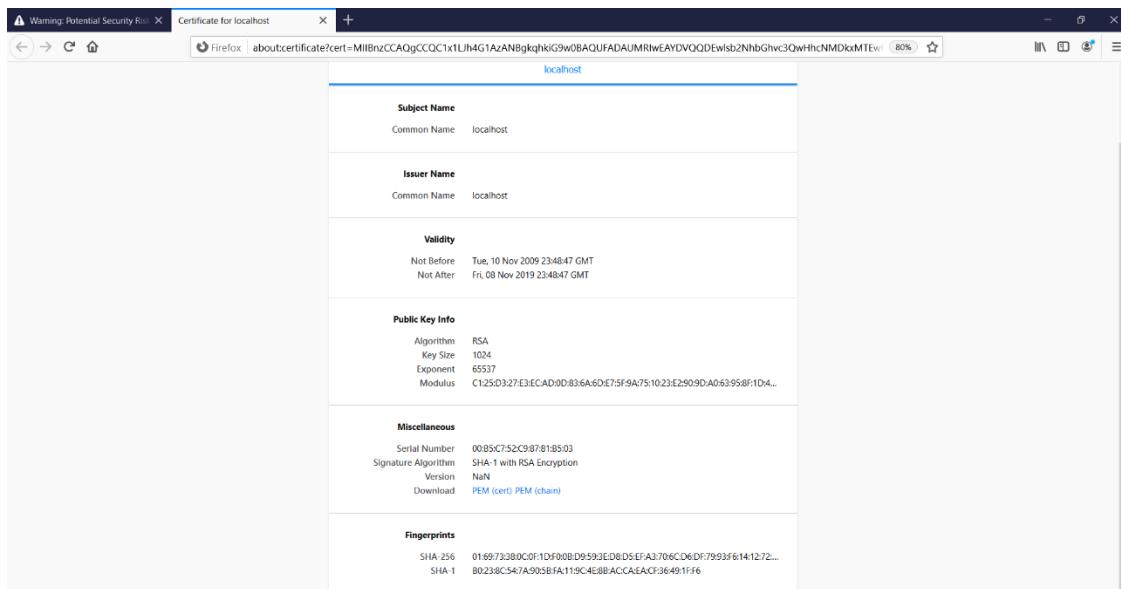
همچنین چیز دیگری که فرق دارد مقدار موجود در Host Header line مربوط به برای بسته‌های این دو سایت باهم فرق دارد. چرا که آدرس سایت‌هایی که ساختیم باهم فرق دارند.

مرحله سوم) حال آدرس <https://www.example.com> را در مرورگر خود باز کنید. دقت کنید که به جای آدرس سایت خود را قرار دهید.

مرحله چهارم) سایت را در مرورگر باز کنید. خطای نشان داده شده در شکل زیر نمایش داده میشود.



مرحله پنجم) بر روی Advanced کلیک کرده و دکمه View Certificate را فشار دهید.



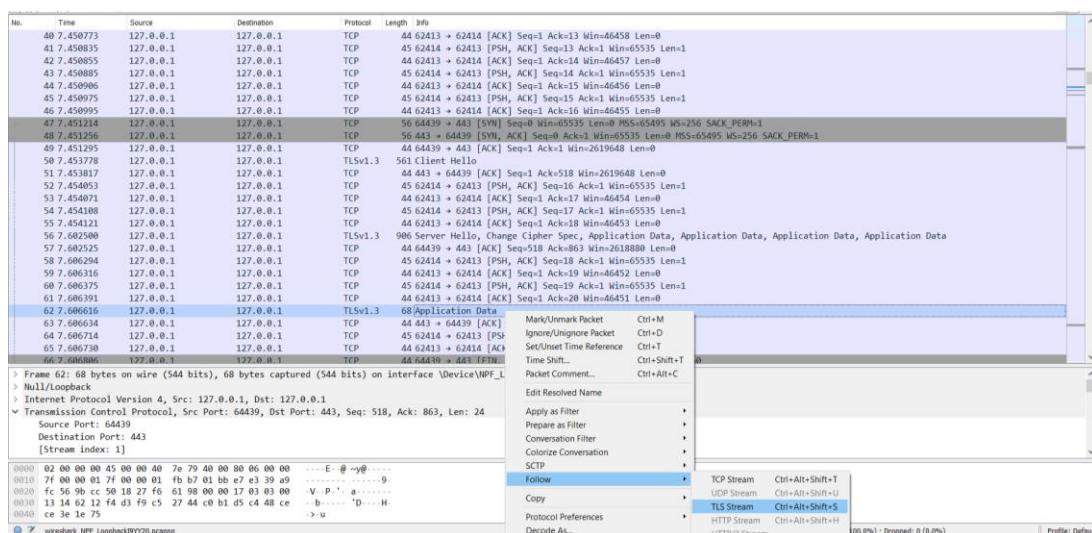
سوال 5: مشخص کنید که گواهی را چه کسی برای چه کسی صادر کرده، مدت زمان اعتبار گواهی چقدر است، کلید عمومی صادرکننده چیست و امضای دیجیتال انجام شده با چه الگوریتم‌هایی انجام شده است.

نام صادرکننده در issuer name آمده است که local host میباشد. همچنین در subject name نام کسی که گواهی برای او صادر شده است آمده که همان local host میباشد.

مدت زمان اعتبار گواهی در بخش validity آمده است که از Tue, 10 Nov 2009 23:48:47 GMT به وقت گرینویچ تا تاریخ Fri, 08 Nov 2019 23:48:47 به وقت گرینویچ اعتبار داشته است. (حدودا 10 سال)

کلید عمومی صادرکننده از دو بخش exponent و modulus تشکیل میشود. این مقادیر هم در بخش public key info آمده است.
 امضای دیجیتال انجام شده با الگوریتم‌های SHA-1 with RSA Encryption انجام شده است. این اطلاعات در قسمت Encryption Miscellaneous قابل مشاهده است.

مرحله ششم) حال ارتباط را با وايرشارک شنود کنيد. بر روی بسته TLS مربوط به اين ارتباط کليک راست کرده و انتخاب کنيد. صفحه‌اي مطابق شکل زير نمايش داده ميشود.

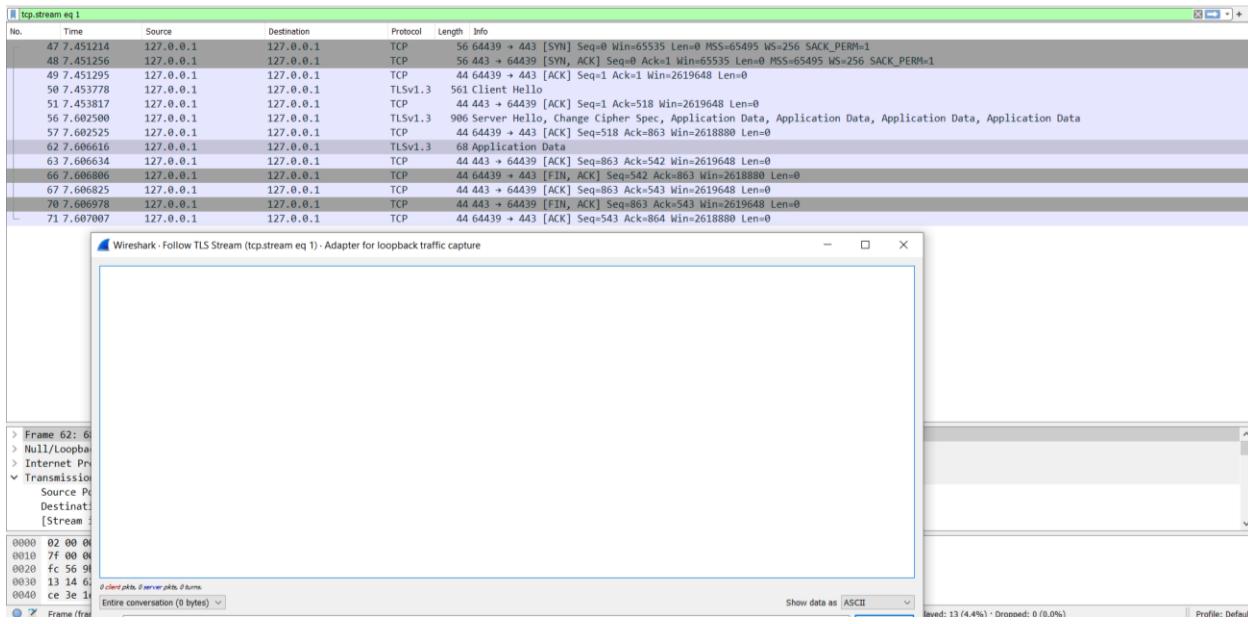


سوال 6: آیا میتوانید متن ارتباط را بخوانید؟ چرا؟

خیر نمیتوان -

زیرا بسته های TLS که با SSL امن شده اند به صورت رمز گذاری شده میباشند و قابل رویت نیستند.

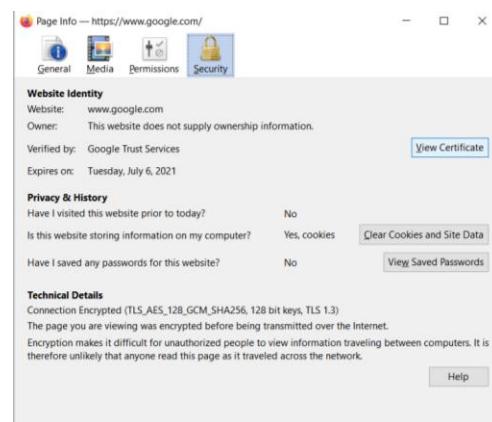
درواقع چون Encryption انجام میدهد اطلاعات منتقل شده را مخفی نگه میدارد.



به یک سایت مانند <https://google.com> وصل شده، گواهی آن را بررسی کنید. برای این کار بر روی علامت قفل در کنار آدرس سایت کلیک کنید. سپس بر روی علامت > در رو بروی عبارت Connection Secure و سپس More Information کلیک کنید.



در پنجره جدید باز شده به قسمت View Certificate مراجعه میکنیم:



اطلاعات مربوط به گواهی وبسایت <https://www.google.com> قابل مشاهده است:

Subject Name	GTS CA 101	GlobalSign
Country	US	
State/Province	California	
Locality	Mountain View	
Organization	Google LLC	
Common Name	www.google.com	
Issuer Name		
Country	US	
Organization	Google Trust Services	
Common Name	GTS CA 101	
Validity		
Not Before	Tue, 13 Apr 2021 10:17:32 GMT	
Not After	Tue, 06 Jul 2021 10:17:31 GMT	
Subject Alt Names		
DNS Name	www.google.com	
Public Key Info		
Algorithm	Elliptic Curve	
Key Size	256	
Curve	P-256	
Public Value	04:31:81:62:64:16:A0:E0:BD:C4:DB:17:B5:E7:1F:94:C3:5C:BE:3B:AF:AB:01:1...	
Miscellaneous		
Serial Number	00:ED:92:FE:51:B1:D1:8C:91:00:00:00:00:CB:F7:81	
Signature Algorithm	SHA-256 with RSA Encryption	
Version	3	
Download	PEM (cert) PEM (chain)	
Fingerprints		
SHA-256	A4:D1:0B:8B:45:46:E3:D0:39:4A:2A:F3:1F:36:22:86:09:BD:09:E0:8D:80:59:56:A...	
SHA-1	F0:4B:7A:59:65:34:33:FB:81:92:C6:CAFB:9A:CC:5A:AD:0C:83:E2	
Basic Constraints		
Extended Key Usages		
Purposes	Server Authentication	
Subject Key ID		
Key ID	3E:2B:49:7A:96:F7:51:FC:02:60:02:9E:9B:7A:16:E2:BB:8D:74:2F	
Authority Key ID		
Key ID	96:D1:F9:4E:10:E8:CF:98:EC:60:9F:1B:90:1B:00:EB:T0:9F:D:2B	
CRL Endpoints		
Distribution Point	http://crl.pki.google/GTS101/crl.crl	
Authority Info (AIA)		
Location	http://crl.pki.google/gpf101/cose	
Method	Online Certificate Status Protocol (OCSP)	
Location	http://pki.google/gr/GTS101/cf	
Method	CA Issuers	
Certificate Policies		
Policy	Certificate Type (2.23.140.1.2.2)	
Value	Organization Validation	
Policy	Statement Identifier (1.3.6.1.4.1.11129.2.5.3)	
Value	1.3.6.1.4.1.11129.2.5.3	
Embedded Scts		
Log ID	94:20:BC:1E:8E:D5:8D:6C:8B:73:1F:82:8B:22:2C:0D:D1:D4:4D:5E:8C:4F:94:3D:...	
Name	Let's Encrypt Oak 2021	
Signature Algorithm	SHA-256 ECDSA	
Version	1	
Timestamp	Tue, 13 Apr 2021 11:17:32 GMT	
Log ID	F6:5C:94:2F:D1:73:30:22:14:54:18:08:30:94:56:0E:E3:4D:13:19:33:8F:DF:0C:2F:...	
Name	Google 'Argon2021'	
Signature Algorithm	SHA-256 ECDSA	
Version	1	
Timestamp	Tue, 13 Apr 2021 11:17:32 GMT	

سوال 7: گواهی آن سایت با گواهی سایت شما چه تفاوت‌هایی دارد؟

اول از همه که تعداد فیلدھای خیلی بیشتری دارد.

در قسمت common name و subject name آن اطلاعات بیشتری آمده است و مثل سایت ما این دو قسمت یکسان نیست.

همچنین در قسمت validity مدت زمان اعتبار آن کم تر و همچنین به روزتر میباشد.

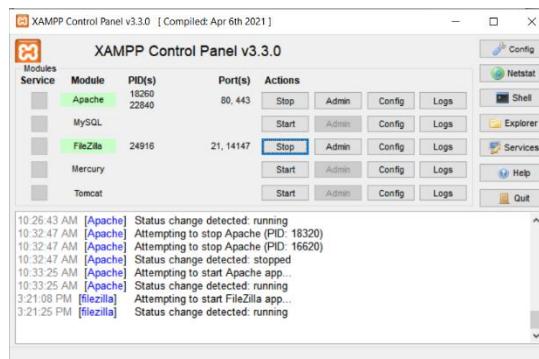
الگوریتم به کار گرفته شده برای public key سایت ما RSA بود ولی در این سایت گوگل Elliptic curve میباشد. همچنین ساز کلید نیز بسیار کوچک تر از سایز کلید سایت ما میباشد. همچنین مقدار آن public key نیز فرق دارد.

همچنین در بخش Miscellaneous برای سایت ما الگوریتم امضا به صورت SHA-1 with RSA بود ولی برای گوگل SHA-256 with RSA Encryption میباشد. همچنین شماره سریال مربوطه نیز با یک دیگر فرق دارد. ورژن آن ها نیز با یک دیگر فرق دارد و برای سایت ما NaN بود ولی برای گوگل ورژن 3 میباشد.

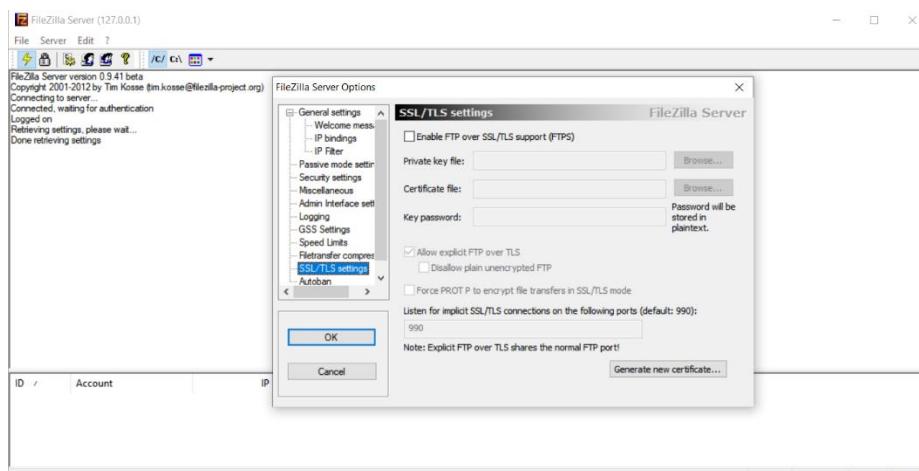
تنظیمات سرور FTP

مرحله هفتم) ابتدا از طریق XAMPP مازول FileZilla را استارت کنید. سپس طبق آموزش یک اکانت با رمز عبور دلخواه ایجاد کنید. سپس مسیر دلخواه برای به اشتراک گذاری را مشخص کنید.

ابتدا بهxampp مراجعه میکنیم و سپس استارت مربوط به FileZilla را میزنیم:

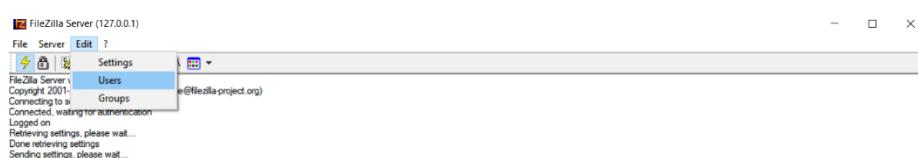


سپس به قسمت Admin مراجعه میکنیم و بعد در قسمت Edit و بعد settings میرویم و بعد در SSL/TLS میرویم و یک سری تیک ها را در صورت وجود برمیداریم تا تنظیمات به صورت زیر بشود:

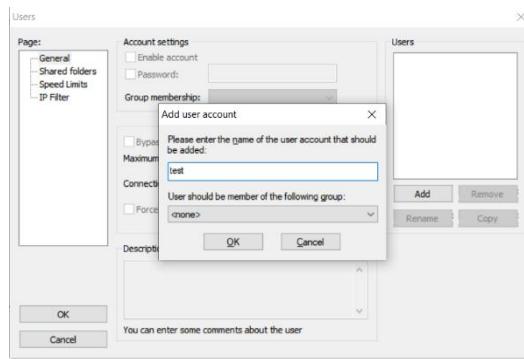


البته تنظیمات به صورت پیشفرض روی همین میباشد.

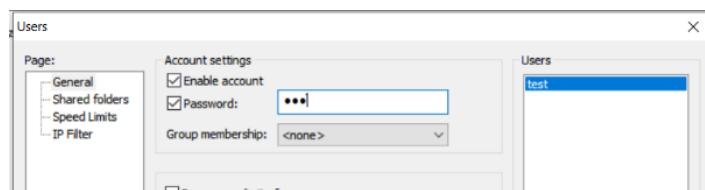
حال برای ساختن user به قسمت Users و بعد به Edit میرویم:



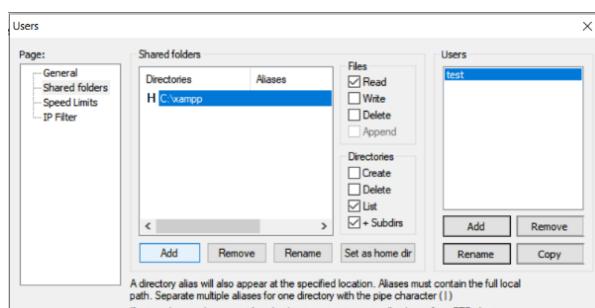
سپس گزینه‌ی Add را می‌زنیم و بعد اسم را test می‌گذاریم:



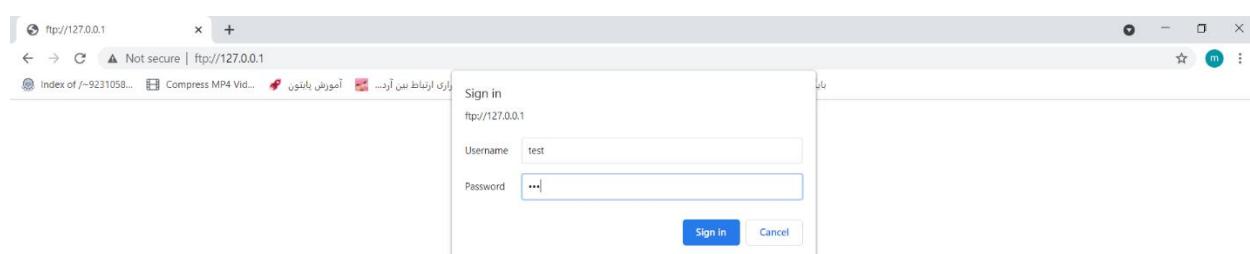
سپس قسمت password را فعال کرده و رمزی برای آن می‌گذاریم:



سپس به قسمت shared folder می‌رویم و روی دکمه Add می‌زنیم و حالا برای مثال کل پوشه‌ی xampp در درایو c را share می‌کنیم:



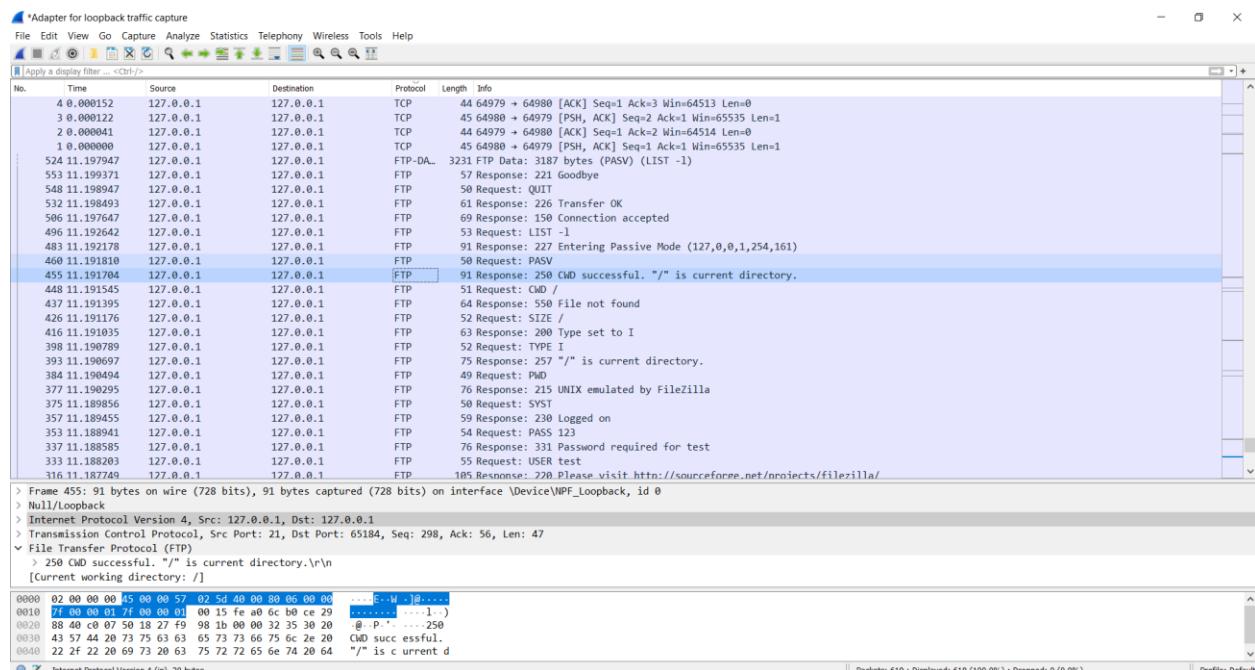
مرحله هشتم) به آدرس <ftp://127.0.0.1> بروید. ارتباط را با وايرشارك شنود کنيد.



Index of /

Name	Size	Date Modified
anonymous/		5/13/21, 5:19:00 AM
apache/		5/13/21, 5:20:00 AM
apache_start.bat	436 B	6/7/21, 4:30:00 AM
apache_stop.bat	176 B	5/13/21, 5:27:00 AM
catalina_service.bat	10.1 kB	4/5/21, 4:30:00 AM
catalina_start.bat	3.7 kB	4/5/21, 4:30:00 AM
catalina_stop.bat	3.4 kB	4/5/21, 4:30:00 AM
cgi-bin/		5/13/21, 5:27:00 AM
contrib/		5/13/21, 5:20:00 AM
cldscript.bat	2.7 kB	5/13/21, 5:19:00 AM
FileZillaFTP/		5/13/21, 5:27:00 AM
filezilla_setup.bat	78 B	3/30/13, 4:30:00 AM
filezilla_start.bat	150 B	6/7/21, 4:30:00 AM
filezilla_stop.bat	149 B	6/7/21, 4:30:00 AM
htdocs/		5/14/21, 2:53:00 PM
img/		5/13/21, 5:19:00 AM
install/		5/13/21, 5:27:00 AM
killprocess.bat	299 B	8/27/19, 4:30:00 AM
licenses/		5/13/21, 5:19:00 AM
locale/		5/13/21, 5:19:00 AM
mailoutput/		5/13/21, 5:19:00 AM
mailtdisk/		5/13/21, 5:20:00 AM
MercuryMail/		5/13/21, 5:27:00 AM
mercury_start.bat	136 B	6/7/21, 4:30:00 AM
mercury_stop.bat	60 B	6/7/21, 4:30:00 AM
mysql/		5/13/21, 5:20:00 AM
mysql_start.bat	471 B	6/3/19, 4:30:00 AM
mysql_stop.bat	256 B	5/13/21, 5:27:00 AM
passwords.txt	824 B	3/13/17, 3:30:00 AM
perl/		5/13/21, 5:22:00 AM
nhn/		5/13/21, 5:27:00 AM

حال به سراغ واپرشارک میرویم تا بسته‌های capture شده را ببینیم. برای راحت تر شدن کار بر روی protocol کلیک میکنیم تا بسته‌هایی که با یک پروتکل اند کنار هم بیوفتند. سپس به سراغ بسته‌های FTP میرویم:

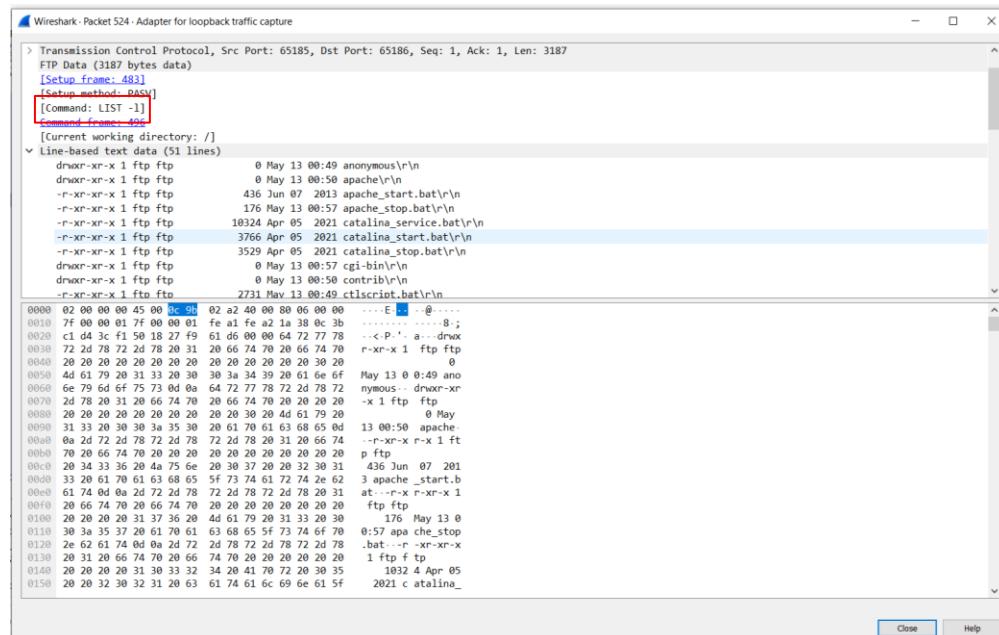


سوال 8: مشخص کنید چه دستوری برای لیست کردن فایل های دایرکتوری استفاده شده است. مشخص کنید چه نام کاربری برای دسترسی به سایت استفاده شده است. پروتکل لایه Transport استفاده شده برای این بستهها چیست؟ آدرس پورت مبدأ و مقصد ارتباط را مشخص کنید.

از دستور PWD برای لیست کردن فایل های دایرکتوری استفاده شده است. همچنین اگر در گوگل سرچ کنیم در سایت ویکی پدیا لیست تمامی دستورات مبوط به FTP را می آورد.

PASS	Authentication password.
PASV	Enter passive mode.
PBSZ	Protection Buffer Size
PORT	Specifies an address and port to which the server should connect.
PROT	Data Channel Protection Level.
PWD	Print working directory. Returns the current directory of the host.
QUIT	Disconnect.
REIN	Re initializes the connection.

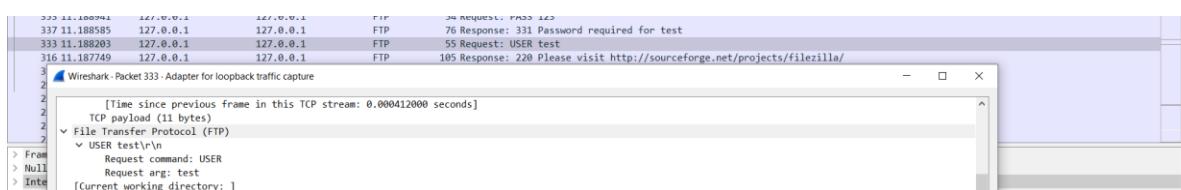
همچنین اگر به بسته‌ای که از این دستور استفاده کرده است مراجعه کنیم:



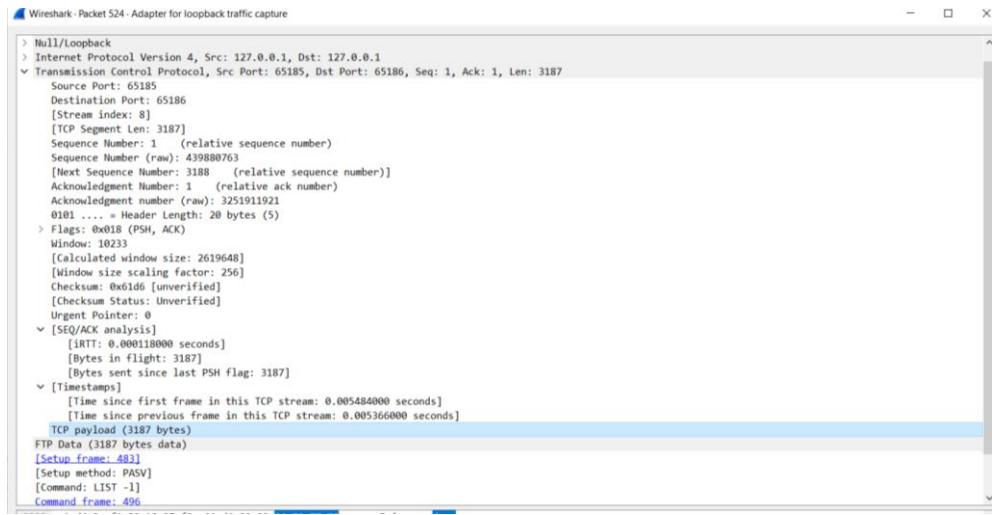
همچنین نام کاربری با دستور USER درخواست میشود.

TYPE	Sets the transfer mode (ASCII/Binary).
USER	Authentication username.
XCP	RFC 775 Change to the parent of the current working directory

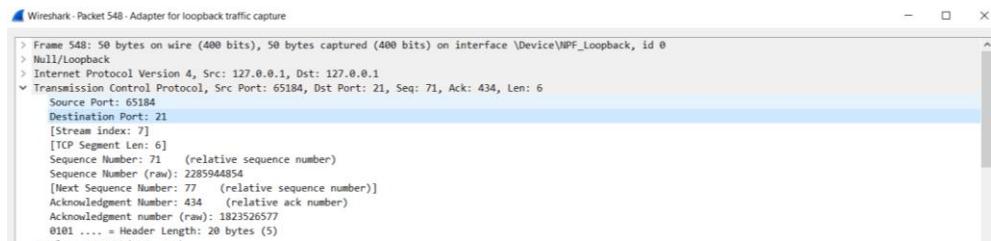
نام کاربری استفاده شده همانی هست که خودمان تنظیم کردیم که test میباشد.



پروتکل لایه‌ی Transport استفاده شده برای بسته‌ها TCP میباشد. که برای دیدن آن میتوان به لایه‌ی Transport بسته‌ها مراجعه کرد و آن را دید:



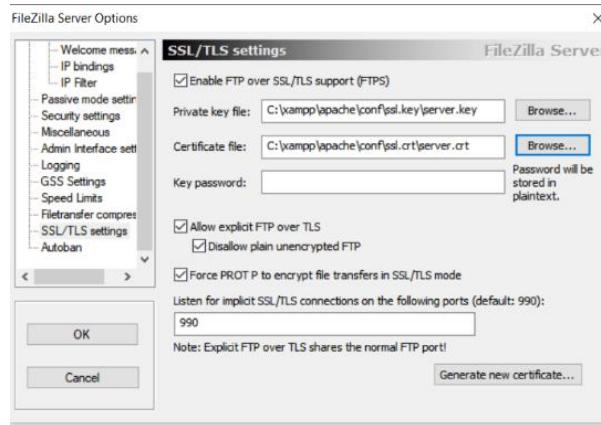
همچنین آدرس پورت مبدأ و مقصد بسته‌ها با توجه به اینکه بسته‌ها از نوع request باشد یا response یکیش شماره پورت 21 میباشد و دیگری هم شماره پورتی است که در سمت کلاینت برای این انتقال اختصاص داده شده که برای ما مقدار 65185 میباشد. برای مثال در بسته‌ی زیر که یک request میباشد پورت مبدأ برابر با 65158 و پورت مقصد برابر با 21 میباشد:



همچنین میدانیم که سرور FTP روی پورت 21 فعالیت میکند.

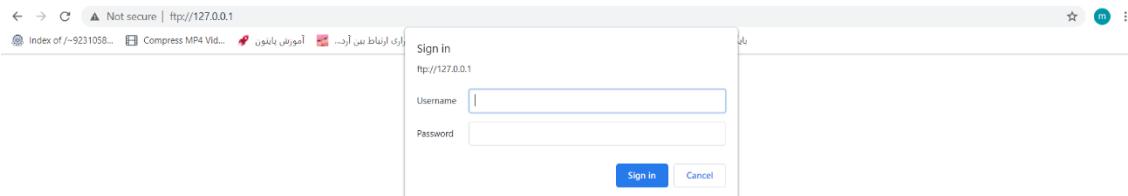
مرحله نهم) تنظیمات مربوط به استفاده از SSL برای FTP را از طریق XAMPP فعال کنید.

برای این کار پس از مراجعه به XAMPP و سپس قسمت Admin به بخش SSL/TLS settings مراجعه میکنیم و تیک Enable FTP over SSL/TLS support(FTPS) را میزنیم تا فعال شود. همچنین تیک گزینه های دیگر را نیز میزنیم و همچنین certificate file و private key file را انجام میدهیم تا نهایتاً به صورت زیر میشود:

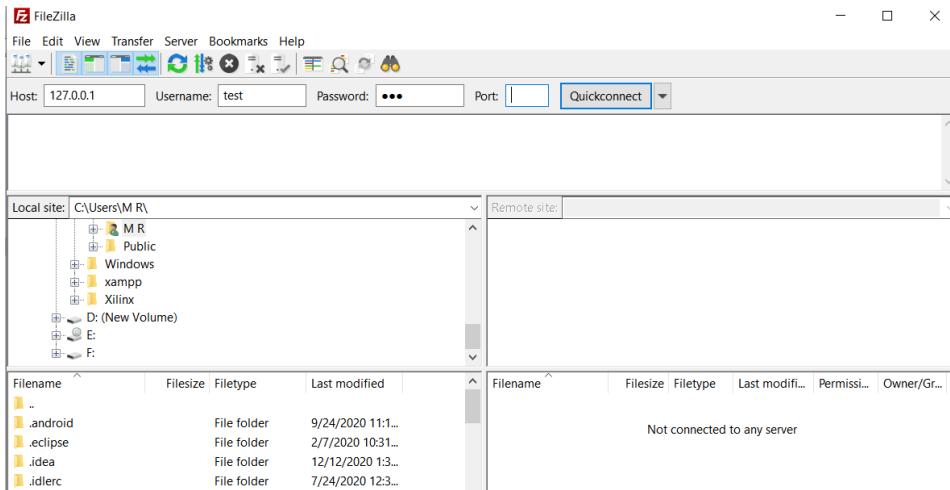


سوال 9: سعی کنید دوباره سایت را از مرورگر باز کنید. آیا میتوانید به سایت وارد شوید؟

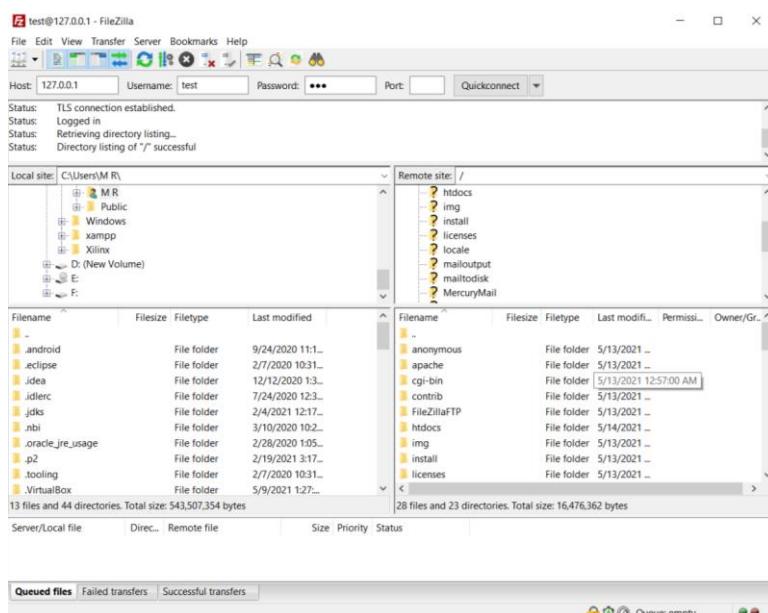
خیر نمیتوان - همانطور که مشاهده میشود بار دیگر آدرس را در مرورگر میزنیم و User name و Password را هم وارد میکنیم منتها بعد از آن اتفاقی نمیافتد و فایل ها را برای ما نمیآورد و دوباره از ما نام کاربری و رمز میخواهد:



مرحله دهم) برنامه FileZilla را از آدرس <https://filezilla-project.org/> دانلود کنید. پس از نصب، در قسمت Host 127.0.0.1 را بنویسید. نام کاربری و پسورد کاربری را که ایجاد کرده‌اید، وارد کنید و بر روی Quickconnect کلیک کنید. ارتباط را با واپرشارک شنود کنید. آیا نام کاربری و پسورد قابل خواندن است؟ پس از نصب آن را باز میکنیم و آدرس Host و همچنین Username و Password را وارد میکنیم:



حال با این نرم افزار با اینکه تنظیمات SSL و امنیتی مربوط به ftp ما فعال شده است میتوان به فایل‌ها دست یافت. اگر روی دکمه quick connect بزنیم به دایرکتوری موردنظر دسترسی پیدا میکند و فایل‌ها را برای ما می‌آورد:

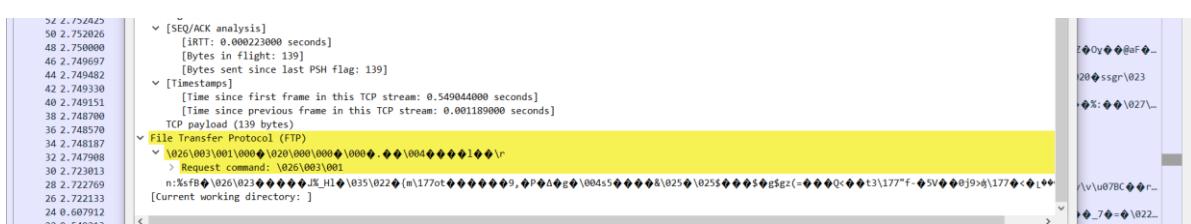


همچنین بعد از آن به سراغ وایرشارک میرویم تا بسته‌های capture شده را بینیم:

No.	Time	Source	Destination	Protocol	Length	Info
83	2.776280	127.0.0.1	127.0.0.1	TLSv1	81	Encrypted Alert
77	2.775879	127.0.0.1	127.0.0.1	TLSv1	2742	Application Data, Encrypted Alert
75	2.775561	127.0.0.1	127.0.0.1	TLSv1	97	Encrypted Handshake Message
73	2.775534	127.0.0.1	127.0.0.1	TLSv1	50	Change Cipher Spec
69	2.775261	127.0.0.1	127.0.0.1	TLSv1	189	Server Hello, Change Cipher Spec, Encrypted Handshake Message
67	2.775073	127.0.0.1	127.0.0.1	TLSv1	571	Client Hello
84	2.776307	127.0.0.1	127.0.0.1	TCP	44	49252 + 21 [ACK] Seq=952 Ack=2127 Win=2617600 Len=0
82	2.776222	127.0.0.1	127.0.0.1	TCP	44	49251 + 21 [ACK] Seq=952 Ack=2127 Win=2617600 Len=0
80	2.776055	127.0.0.1	127.0.0.1	TCP	44	49252 + 21 [ACK] Seq=957 Ack=2844 Win=4191368 Len=0
79	2.776037	127.0.0.1	127.0.0.1	TCP	44	49252 + 21 [ACK] Seq=957 Ack=2844 Win=4191368 Len=0
78	2.775904	127.0.0.1	127.0.0.1	TCP	44	49253 + 21 [ACK] Seq=957 Ack=2844 Win=4191368 Len=0
76	2.775588	127.0.0.1	127.0.0.1	TCP	44	49252 + 21 [ACK] Seq=957 Ack=2619648 Win=0
74	2.775548	127.0.0.1	127.0.0.1	TCP	44	49252 + 21 [ACK] Seq=957 Ack=2619648 Win=0
72	2.775403	127.0.0.1	127.0.0.1	TCP	44	49252 + 21 [ACK] Seq=952 Ack=2074 Win=2617600 Len=0
70	2.775283	127.0.0.1	127.0.0.1	TCP	44	49253 + 21 [ACK] Seq=952 Ack=2074 Win=2617600 Len=0
68	2.775066	127.0.0.1	127.0.0.1	TCP	44	49252 + 21 [ACK] Seq=952 Ack=2619648 Win=0
66	2.775056	127.0.0.1	127.0.0.1	TCP	44	49253 + 21 [ACK] Seq=952 Ack=1 Win=4194048 Len=0
65	2.775012	127.0.0.1	127.0.0.1	TCP	56	49252 + 21 [SYN] Seq=0 Ack=5535 Len=0 MSS=65495 WS=256 SACK_PERM=1
64	2.759962	127.0.0.1	127.0.0.1	TCP	56	49252 + 21 [SYN] Seq=0 Win=65535 Len=0 MSS=65495 WS=128 SACK_PERM=1
63	2.759686	127.0.0.1	127.0.0.1	TCP	44	21 + 49251 [ACK] Seq=2921 Ack=952 Win=2618624 Len=0
61	2.758933	127.0.0.1	127.0.0.1	TCP	44	49251 + 21 [ACK] Seq=915 Ack=2021 Win=2617600 Len=0
59	2.754380	127.0.0.1	127.0.0.1	TCP	44	21 + 49251 [ACK] Seq=1936 Ack=915 Win=2618880 Len=0
57	2.754174	127.0.0.1	127.0.0.1	TCP	44	49251 + 21 [ACK] Seq=873 Ack=1936 Win=2617856 Len=0
55	2.753440	127.0.0.1	127.0.0.1	TCP	44	21 + 49251 [ACK] Seq=1883 Ack=878 Win=2618880 Len=0
53	2.752455	127.0.0.1	127.0.0.1	TCP	44	49251 + 21 [ACK] Seq=841 Ack=1883 Win=2617856 Len=0
51	2.752050	127.0.0.1	127.0.0.1	TCP	44	21 + 49251 [ACK] Seq=1814 Ack=841 Win=2618880 Len=0
49	2.750818	127.0.0.1	127.0.0.1	TCP	44	49251 + 21 [ACK] Seq=809 Ack=1814 Win=2617856 Len=0
47	2.749715	127.0.0.1	127.0.0.1	TCP	44	21 + 49251 [ACK] Seq=1745 Ack=804 Win=2618880 Len=0
45	2.749498	127.0.0.1	127.0.0.1	TCP	44	49251 + 21 [ACK] Seq=767 Ack=1745 Win=2617856 Len=0
43	2.749348	127.0.0.1	127.0.0.1	TCP	44	21 + 49251 [ACK] Seq=1692 Ack=767 Win=2618880 Len=0
41	2.749184	127.0.0.1	127.0.0.1	TCP	44	49251 + 21 [ACK] Seq=730 Ack=1692 Win=2617856 Len=0
39	2.748727	127.0.0.1	127.0.0.1	TCP	44	21 + 49251 [ACK] Seq=1110 Ack=730 Win=2618880 Len=0
37	2.748602	127.0.0.1	127.0.0.1	TCP	44	49251 + 21 [ACK] Seq=693 Ack=1110 Win=2618624 Len=0
35	2.748278	127.0.0.1	127.0.0.1	TCP	44	21 + 49251 [ACK] Seq=1041 Ack=693 Win=2618880 Len=0
33	2.748011	127.0.0.1	127.0.0.1	TCP	44	49251 + 21 [ACK] Seq=656 Ack=1041 Win=2618624 Len=0
31	2.733830	127.0.0.1	127.0.0.1	TCP	44	21 + 49251 [ACK] Seq=889 Ack=656 Win=2618624 Len=0

No.	Time	Source	Destination	Protocol	Length	Info
3	0.000223	127.0.0.1	127.0.0.1	TCP	44	49251 + 21 [ACK] Seq=1 Ack=1 Win=2619648 Len=0
2	0.000132	127.0.0.1	127.0.0.1	TCP	56	21 + 49251 [SYN] Seq=0 Ack=1 Win=65535 Len=0 MSS=65495 WS=256 SACK_PERM=1
1	0.000000	127.0.0.1	127.0.0.1	FTP	97	Response: 21 [ACK] Seq=1 Win=2619648 Len=0
81	2.776200	127.0.0.1	127.0.0.1	FTP	97	Response: 21 [ACK] Seq=1 Win=2619648 Len=0
71	2.775356	127.0.0.1	127.0.0.1	FTP	97	Response: 21 [ACK] Seq=1 Win=2619648 Len=0
62	2.769651	127.0.0.1	127.0.0.1	FTP	81	Request: 21 [ACK] Seq=1 Win=2619648 Len=0
60	2.768867	127.0.0.1	127.0.0.1	FTP	129	Response: 21 [ACK] Seq=1 Win=2619648 Len=0
58	2.754335	127.0.0.1	127.0.0.1	FTP	81	Request: 21 [ACK] Seq=1 Win=2619648 Len=0
56	2.754136	127.0.0.1	127.0.0.1	FTP	97	Response: 21 [ACK] Seq=1 Win=2619648 Len=0
54	2.753418	127.0.0.1	127.0.0.1	FTP	81	Request: 21 [ACK] Seq=1 Win=2619648 Len=0
52	2.752425	127.0.0.1	127.0.0.1	FTP	113	Response: 21 [ACK] Seq=1 Win=2619648 Len=0
50	2.752026	127.0.0.1	127.0.0.1	FTP	81	Request: 21 [ACK] Seq=1 Win=2619648 Len=0
48	2.750800	127.0.0.1	127.0.0.1	FTP	113	Response: 21 [ACK] Seq=1 Win=2619648 Len=0
46	2.749697	127.0.0.1	127.0.0.1	FTP	81	Request: 21 [ACK] Seq=1 Win=2619648 Len=0
44	2.749482	127.0.0.1	127.0.0.1	FTP	97	Response: 21 [ACK] Seq=1 Win=2619648 Len=0
42	2.749330	127.0.0.1	127.0.0.1	FTP	81	Request: 21 [ACK] Seq=1 Win=2619648 Len=0
40	2.749151	127.0.0.1	127.0.0.1	FTP	626	Response: 21 [ACK] Seq=1 Win=2619648 Len=0
38	2.748700	127.0.0.1	127.0.0.1	FTP	81	Request: 21 [ACK] Seq=1 Win=2619648 Len=0
36	2.748570	127.0.0.1	127.0.0.1	FTP	113	Response: 21 [ACK] Seq=1 Win=2619648 Len=0
34	2.748187	127.0.0.1	127.0.0.1	FTP	81	Request: 21 [ACK] Seq=1 Win=2619648 Len=0
32	2.747908	127.0.0.1	127.0.0.1	FTP	97	Response: 21 [ACK] Seq=1 Win=2619648 Len=0
30	2.729313	127.0.0.1	127.0.0.1	FTP	81	Request: 21 [ACK] Seq=1 Win=2619648 Len=0
28	2.722769	127.0.0.1	127.0.0.1	FTP	113	Response: 21 [ACK] Seq=1 Win=2619648 Len=0
26	2.722133	127.0.0.1	127.0.0.1	FTP	81	Request: 21 [ACK] Seq=1 Win=2619648 Len=0
24	0.669712	127.0.0.1	127.0.0.1	FTP	278	Response: 21 [ACK] Seq=1 Win=2619648 Len=0
22	0.549213	127.0.0.1	127.0.0.1	FTP	97	Response: 21 [ACK] Seq=1 Win=2619648 Len=0
20	0.549142	127.0.0.1	127.0.0.1	FTP	50	Request: 21 [ACK] Seq=1 Win=2619648 Len=0
18	0.549044	127.0.0.1	127.0.0.1	FTP	182	Request: 21 [ACK] Seq=1 Win=2619648 Len=0
16	0.547810	127.0.0.1	127.0.0.1	FTP	545	Response: 21 [ACK] Seq=1 Win=2619648 Len=0
14	0.546762	127.0.0.1	127.0.0.1	FTP	417	Request: 21 [ACK] Seq=1 Win=2619648 Len=0
12	0.545995	127.0.0.1	127.0.0.1	FTP	79	Response: 21 [ACK] Seq=1 Win=2619648 Len=0
10	0.007474	127.0.0.1	127.0.0.1	FTP	54	Request: AUTH TLS
8	0.007305	127.0.0.1	127.0.0.1	FTP	105	Response: 220 Please visit http://sourceforge.net/projects/filezilla/
6	0.007077	127.0.0.1	127.0.0.1	FTP	89	Response: 220-written by Tim Kosse (Tim.Kosse@gmx.de)
4	0.006558	127.0.0.1	127.0.0.1	FTP	86	Response: 220-FileZilla Server version 0.9.41 beta

همانطور که در شکل بالا هم پیداست اصلاً نوع درخواست‌ها و دیتاهای منتقل شده قابل خواندن نیستند. همچنین اگر روی یکی از بسته‌های FTP هم کلیک کنیم میبینیم که اطلاعات قابل خواندن نیستند. بنابراین نام کاربری و پسورد قابل خواندن نمیباشد:



HTTP پروتکل

-1 عمل شنود را آغاز کنید، مرورگر را باز کرده و به آدرس <http://aut.ac.ir> بروید. شنود را متوقف کرده و بسته‌ها را بررسی کنید:

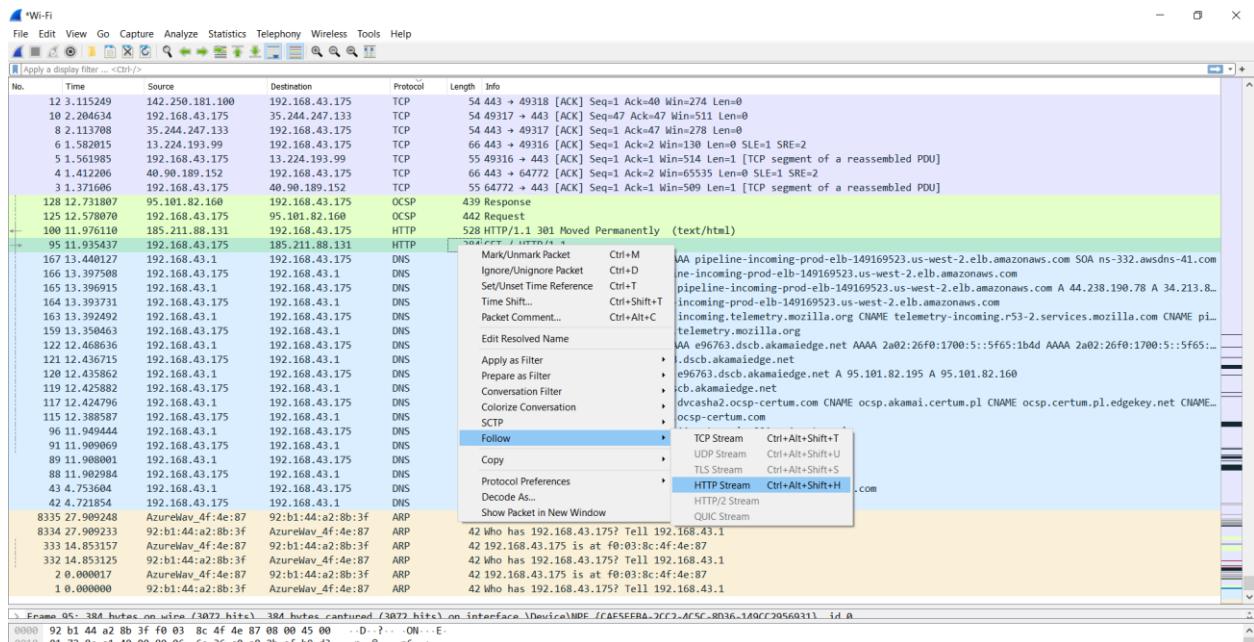
ابتدا در مرورگر آدرس سایت را میزنیم و درایم:



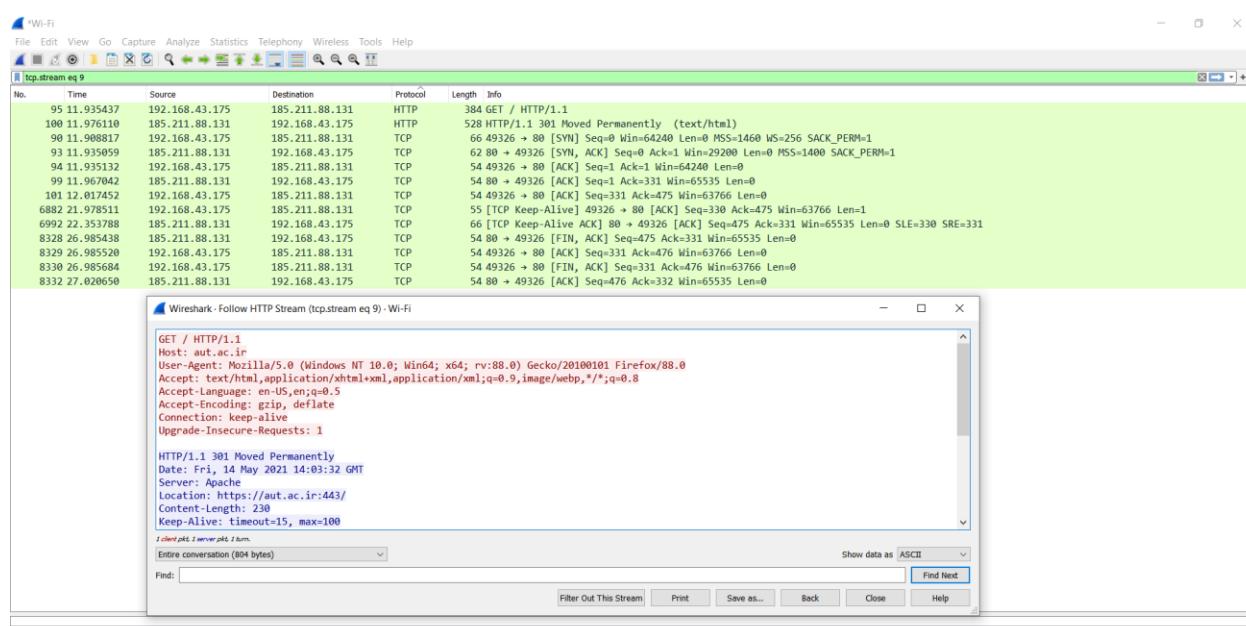
سپس به سراغ بسته‌های capture شده و ایرشارک می‌رویم. همانطور که می‌بینید بسته‌های زیادی دریافت شده است:

-2 بروی یکی از بسته‌های پروتکل HTTP کلیک راست کرده و Follow HTTP Stream را انتخاب کنید. اگر Wireshark شما این گزینه را ندارد آن را به روز کنید.

بر روی protocol کلیک میکنیم تا بسته‌ها براساس پروتکل مرتب شوند. سپس روی یکی از بسته‌های HTTP کلیک راست کرده و follow HTTP stream را میزنیم:



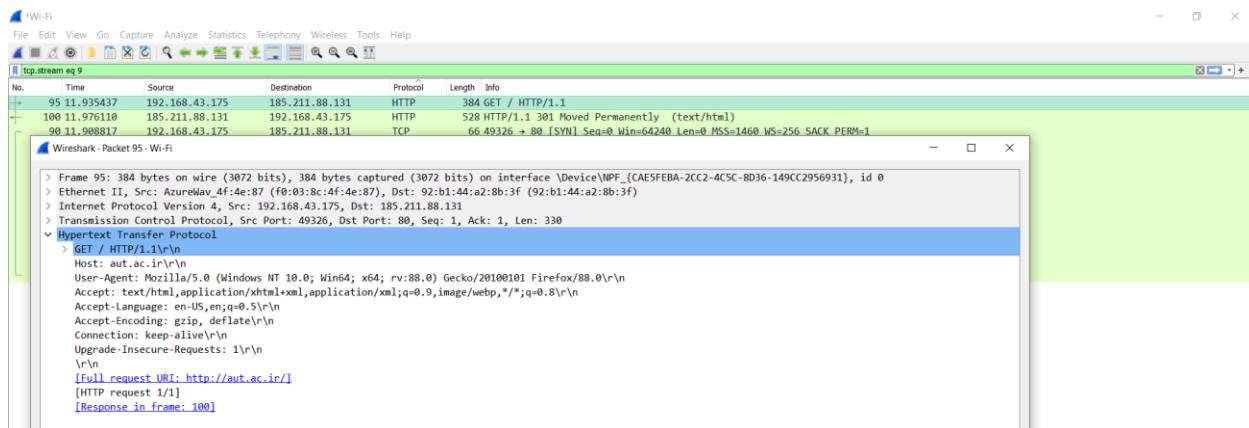
سپس صفحه‌ی زیر باز میشود:



-3 بروی اولین بسته در پنجره باز شده کلیک کنید. بخش های مختلف پروتکل HTTP را مشاهده کنید.

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

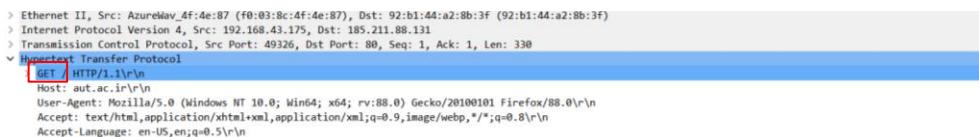
بر روی اولین بسته کلیک میکنیم:



مقدار بخش connection برابر با `keep-alive` میباشد. درواقع میگوید بعد از اتمام این transaction درحال جریان اتصال همچنان باز است. درواقع اتصال persistent است و بسته نیست ، اجازه می دهد تا درخواست های بعدی به همان سرور انجام شود:



درخواست HTTP از نوع GET بوده است. در خط request line که خط نخست در پیام درخواست میباشد فیلد اول که فیلد متده میباشد این را مشخص میکند.



خط سرآیند درواقع همان مرورگر وب که از سرویس دهنده درخواست کرده، را مشخص میکند.
در اینجا User-agent ما برابر با مقدار زیر است:

User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64; rv:88.0) Gecko/20100101 Firefox/88.0



سودمندی این خط سرآیند از آن جهت است که یک سرویس دهنده میتواند ویرایش های متفاوتی از یک شیء برای هر مرورگر وب داشته باشد.

هدر درخواست User-Agent یک رشته مشخصه است که به سرورها و network peer اجازه می دهد تا سیستم عامل و یا نسخه و ورژن درخواست کننده را شناسایی کنند.

-4 در پنجره باز شده، بسته هایی با پروتکل TCP هم مشخص شده است. اولین بسته را انتخاب کنید. سپس مقدار Flags در پروتکل TCP را مشاهده کنید. چه مقادیری برای این بسته تنظیم شده است؟

اولین بسته TCP را انتخاب میکنیم:



برای این بسته مقدار SYN تنظیم شده و بیت مربوط به آن برابر با 1 شده است.

Synchronization (SYN): این در گام اول مرحله برقراری اتصال یا فرایند 3-way handshake میزبان استفاده می شود. فقط بسته اول از طرف فرستنده و همچنین گیرنده باید این پرچم را تنظیم کند. این برای همگام سازی شماره توالی استفاده می شود ، یا به عبارتی برای این است که به سیستم انتهایی دیگر بگوید که باید انتظار چه شماره ای را در مرحله بعد داشته باشد.

پروتکل FTP

-1 عمل شنود را آغاز کرده و مرورگر را باز کرده و به آدرس <ftp://ftp.lip6.fr/> بروید. شنود را متوقف کنید. یک بسته مربوط به پروتکل FTP را انتخاب کرده، بر روی آن کلیک راست کنید و Follow TCP Stream.

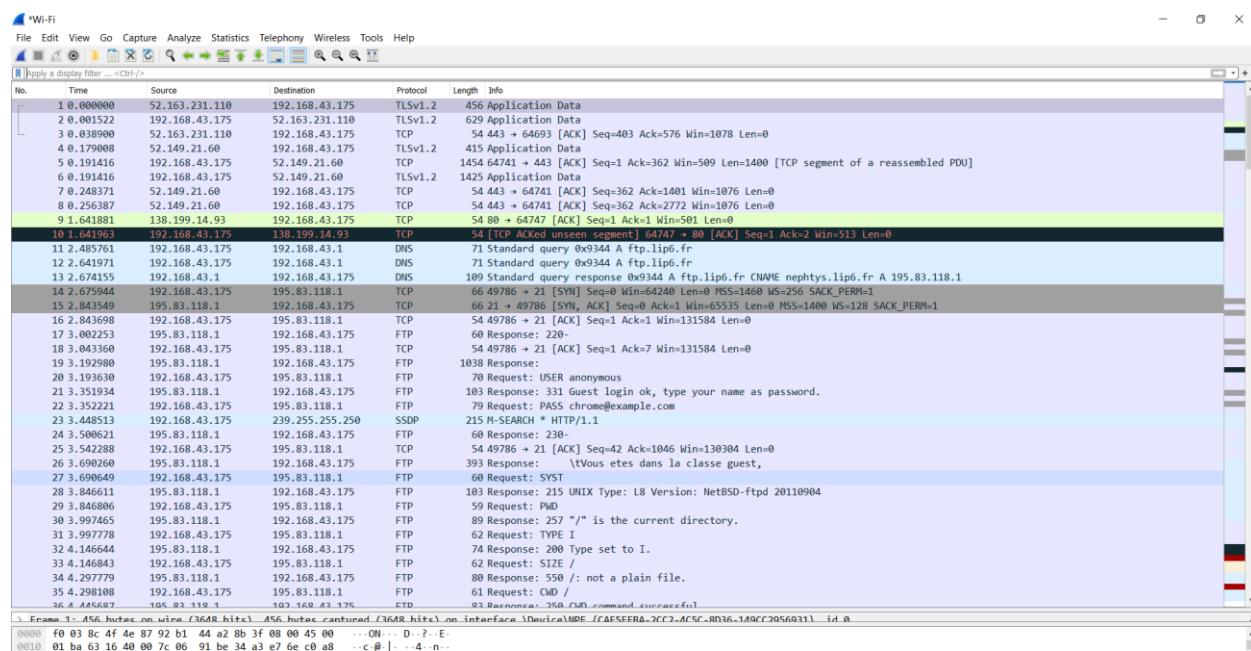
ابتدا به سایت مورد نظر میرویم:



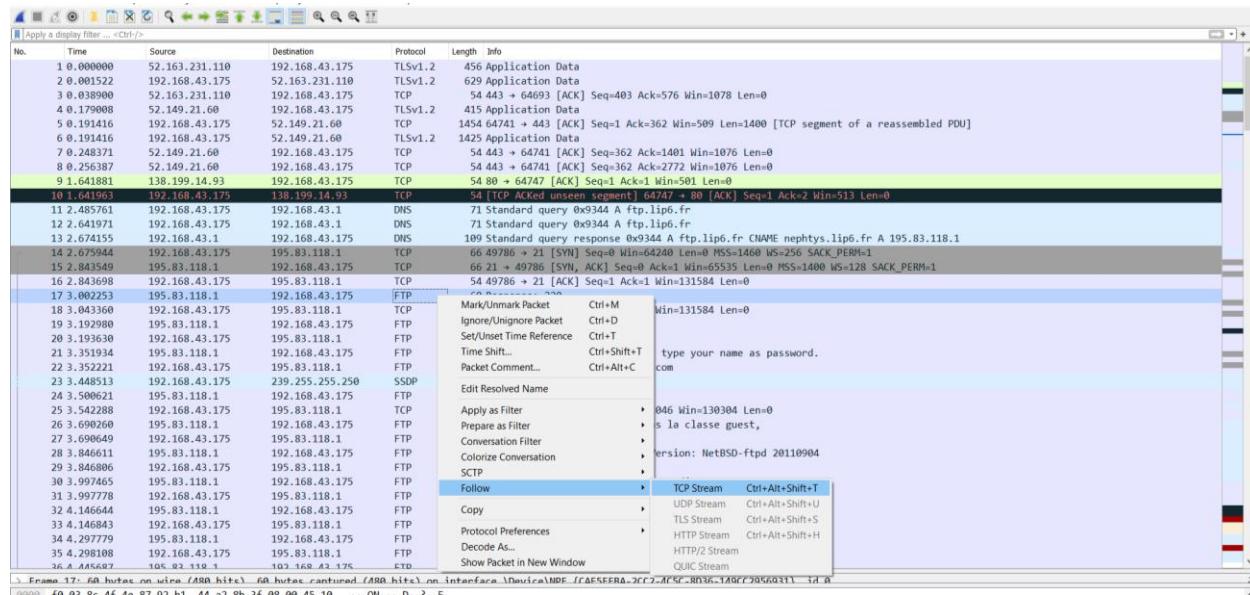
Index of /

Name	Size	Date Modified
etc/		11/30/08, 3:30:00 AM
lib/		2/16/01, 3:30:00 AM
jussieu/		6/22/00, 4:30:00 AM
lafia/		2/16/01, 3:30:00 AM
lip/		4/9/11, 4:30:00 AM
ls-IR.gz	102 MB	5/14/21, 3:16:00 PM
private/		8/16/09, 4:30:00 AM
pub/		9/20/19, 4:30:00 AM

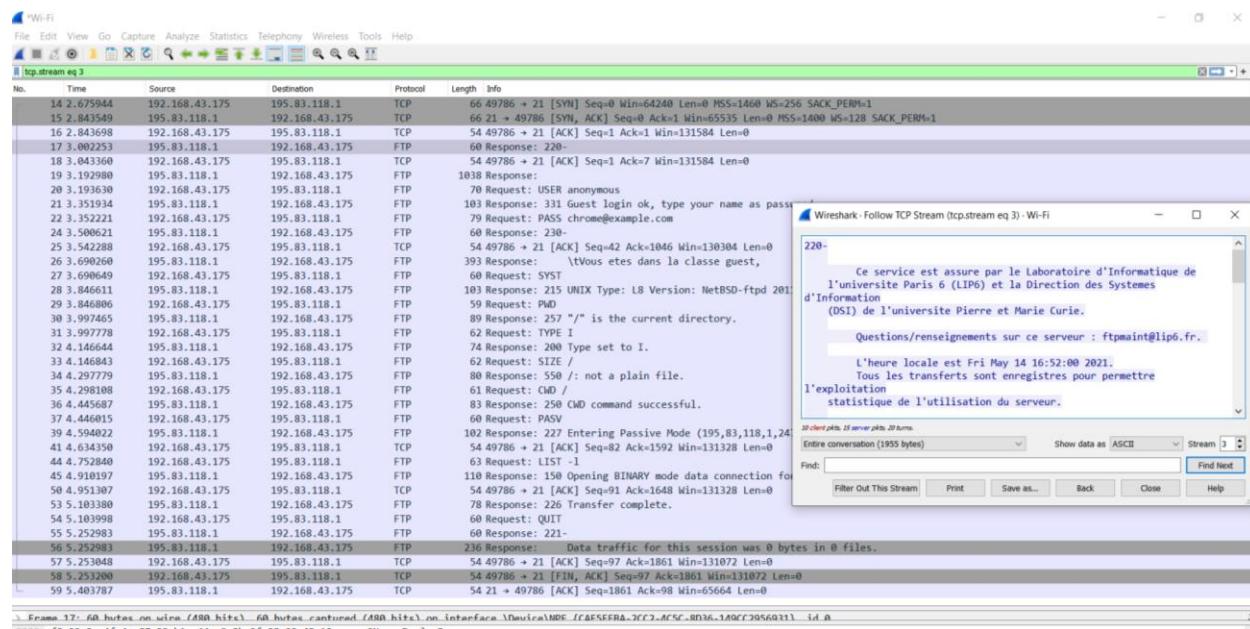
سپس شنود را متوقف میکنیم. آنگاه بسته‌های capture شده در وایرشارک به صورت زیر میباشند:



حال یکی از بسته‌های FTP را انتخاب می‌کنیم و بر روی آن کلیک راست می‌کنیم و انتخاب می‌کنیم:

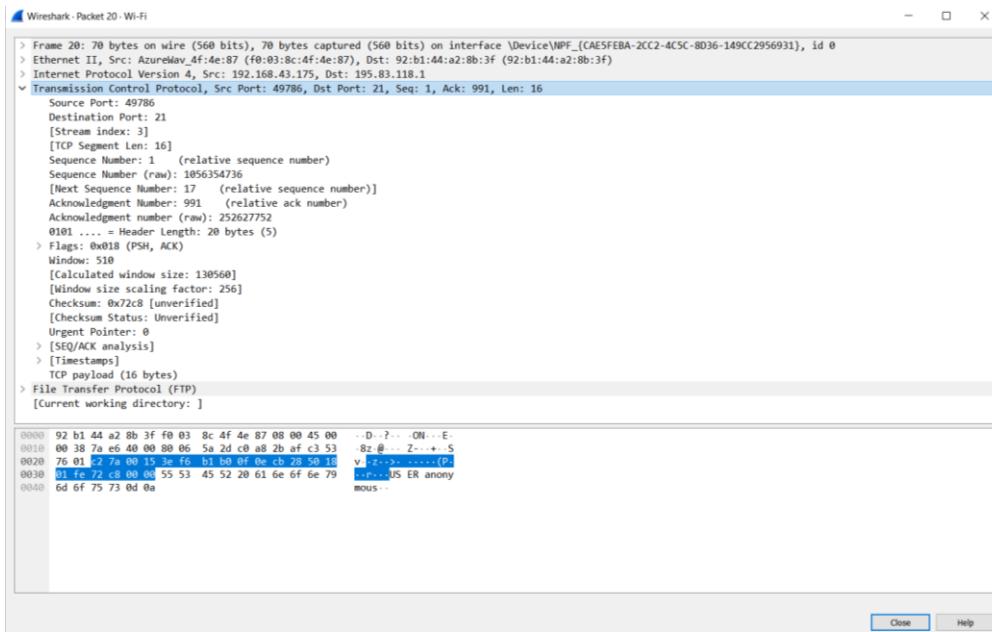


آنگاه صفحات زیر برای ما باز می‌شوند:



-2- پروتکل لایه Transport استفاده شده برای این بسته‌ها چیست؟ آدرس پورت مبدأ و مقصد ارتباط را مشخص کنید.

پروتکل لایه Transport استفاده شده برای بسته‌ها TCP میباشد. که برای دیدن آن میتوان به لایه Transport بسته‌ها مراجعه کرد و آن را دید:



همچنین آدرس پورت مبدأ و مقصد بسته‌ها با توجه به اینکه بسته از نوع request یکیش شماره پورت 21 میباشد و دیگری هم شماره پورتی است که در سمت کلاینت برای این انتقال اختصاص داده شده که برای ما مقدار 49786 میباشد. برای مثال در بسته‌ی زیر که یک request میباشد پورت مبدأ برابر با 49786 و پورت مقصد برابر با 21 میباشد:

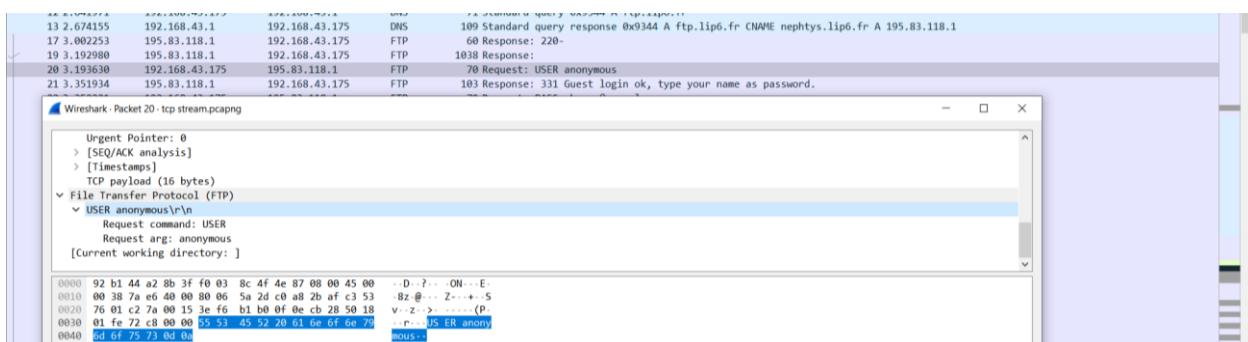


-3 در یکی از بسته‌ها مقدار Username و در بسته دیگر مقدار Password به سمت سرور ارسال شده است. این مقادیر را مشخص کنید.

نام کاربری با دستور USER درخواست می‌شود.

TYPE		Sets the transfer mode (ASCII/Binary).
USER		Authentication username
XCUP	RFC 775	Change to the parent of the current working directory

همانطور که در شکل زیر می‌بینید، نام کاربری در اینجا به صورت anonymous می‌باشد.



با دستور PASS درخواست Mی‌شود: Password

NLSI		Returns a list of file names in a specified directory.
NOOP		No operation (dummy packet; used mostly on keepalives).
OPTS	RFC 2389	Select options for a feature (for example <code>OPTS UTF8 ON</code>).
PASS		Authentication password.
PASV		Enter passive mode.
PROT	RFC 2298	Protection Different Options

همانطور که در شکل زیر می‌بینید مقدار پسورد chrome@example.com می‌باشد.

