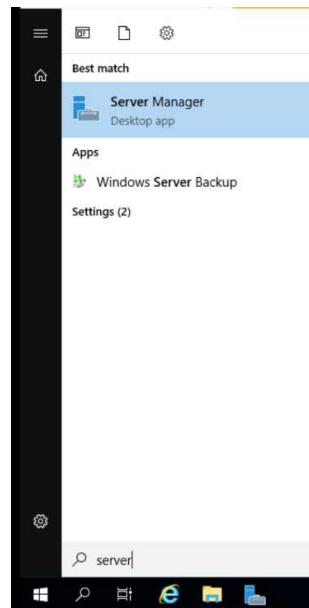


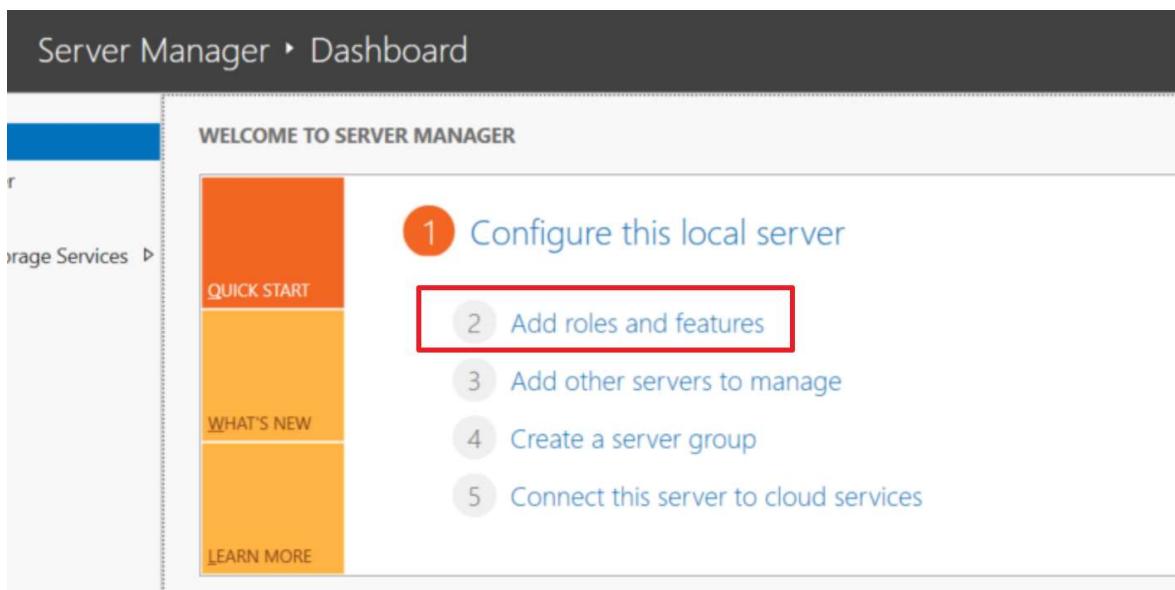
## تمرین عملی سری ۲

چگونگی نصب و راهاندازی سرویس FTP را گزارش کنید.

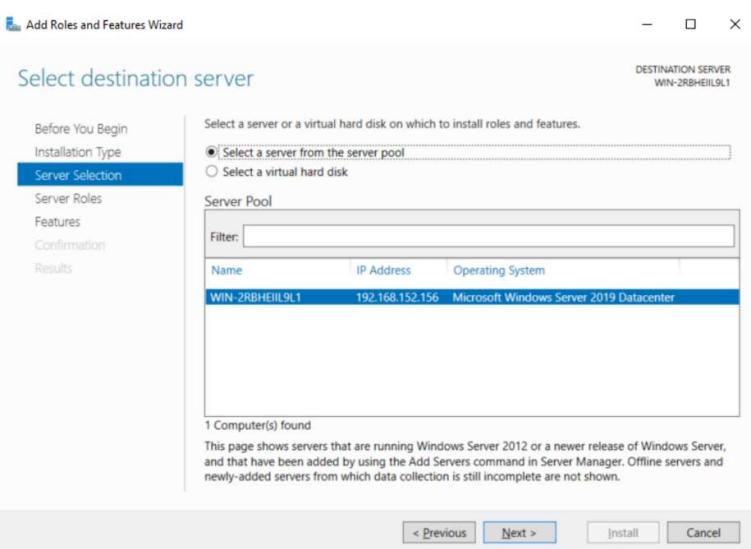
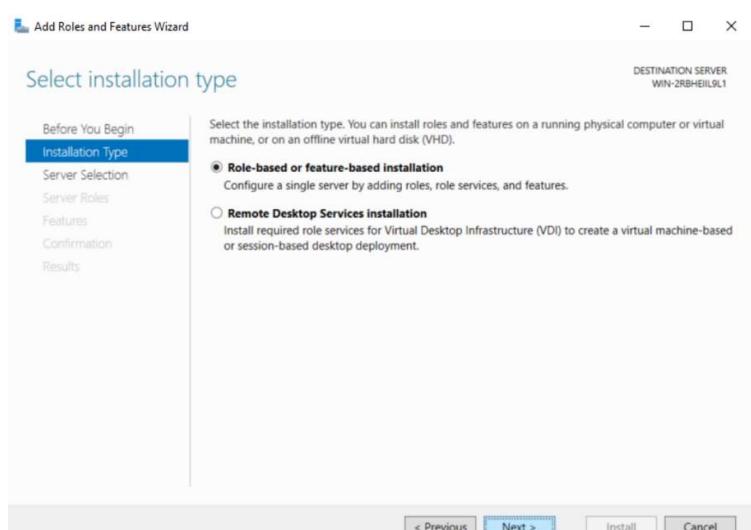
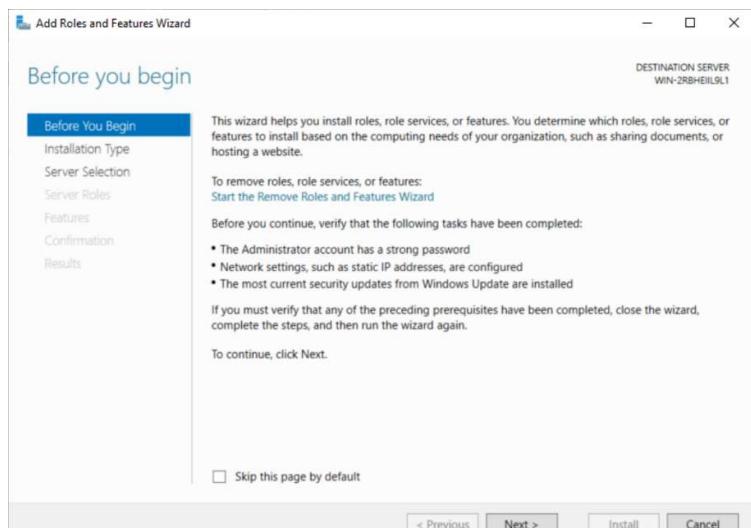
در ابتدا server manager را باز می‌کنیم.



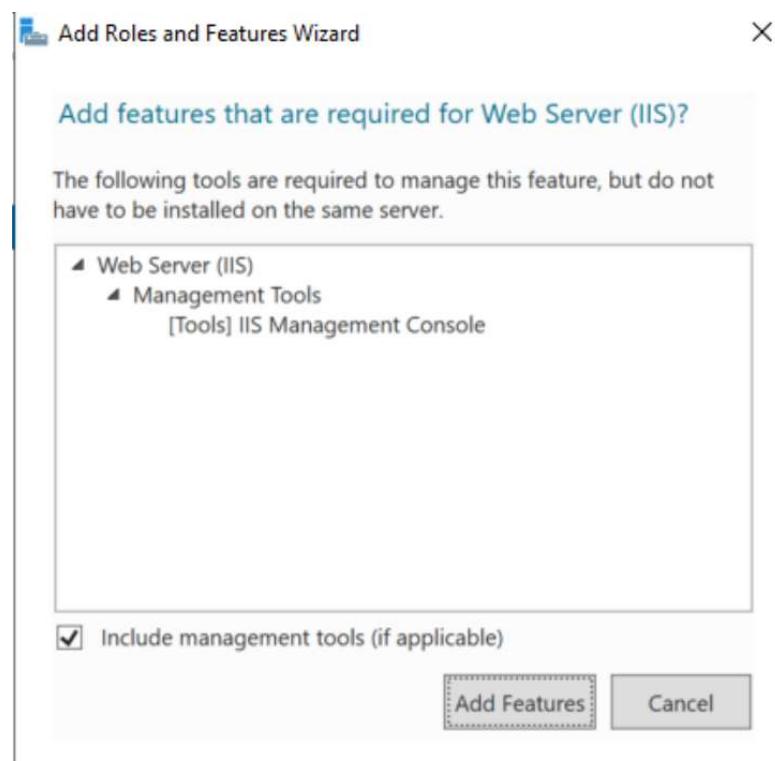
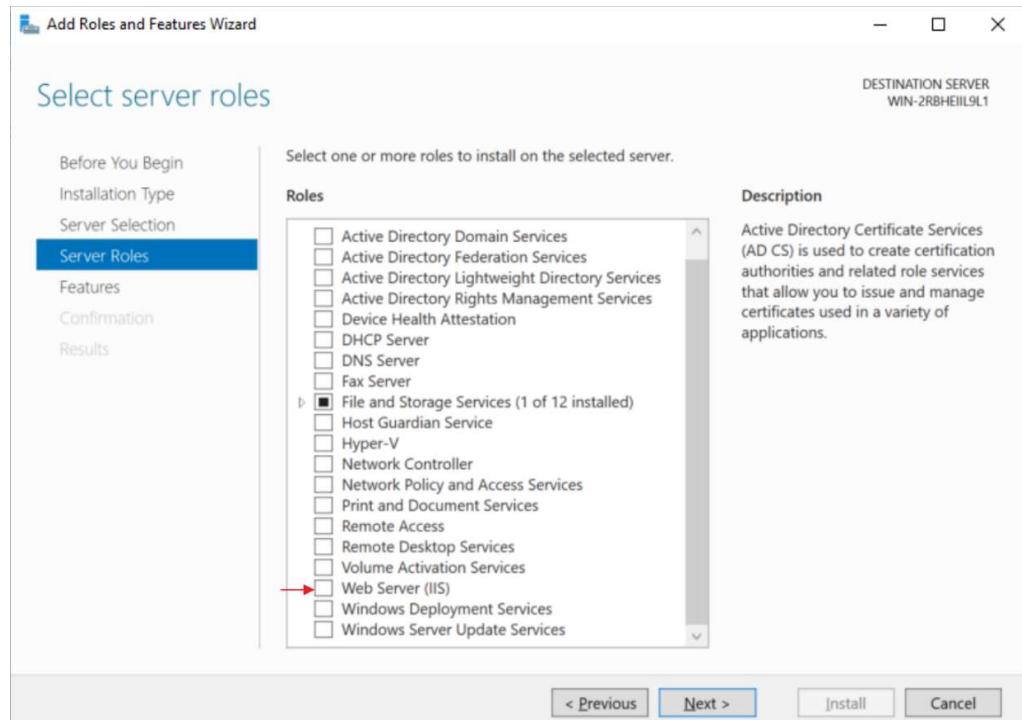
گزینه add roles and features را انتخاب می‌کنیم.



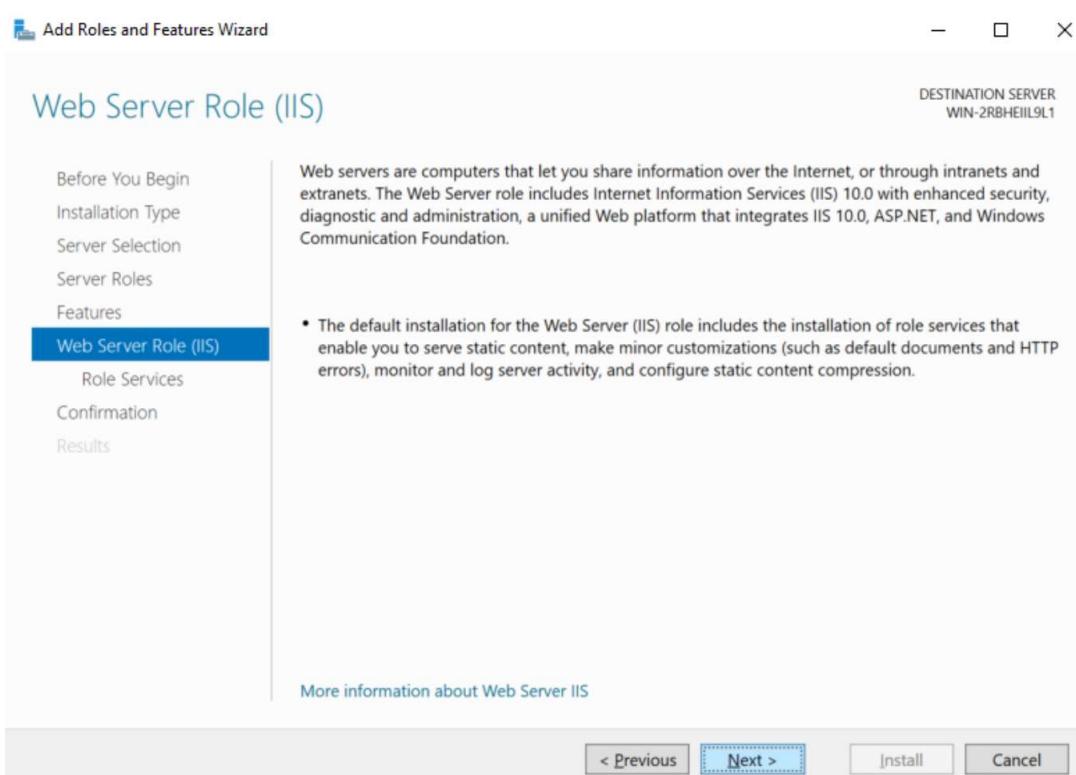
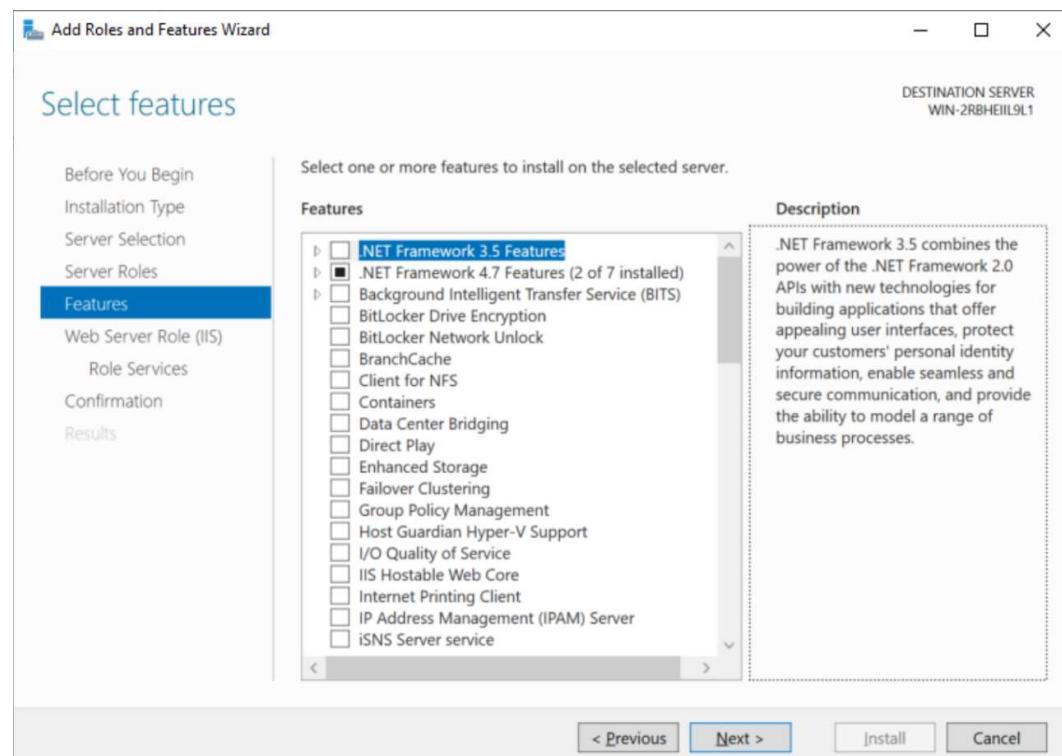
در صفحات زیر بدون اینکه چیزی را تغییر دهیم، دکمه **next** را می‌زنیم.



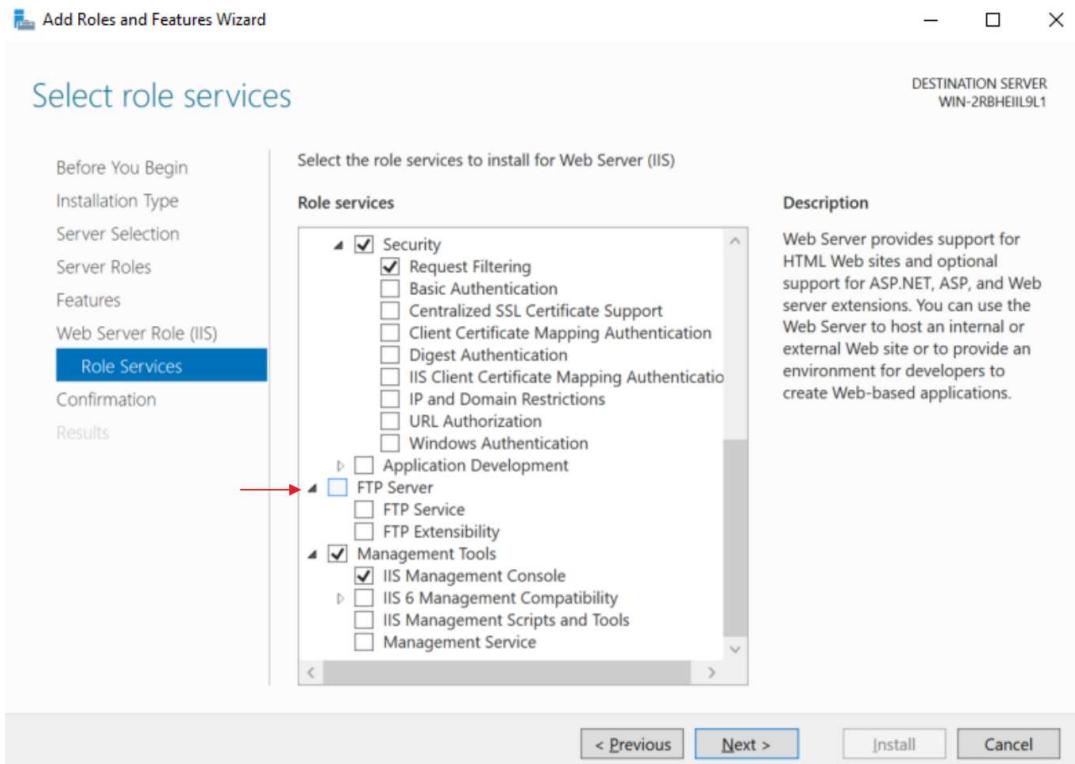
در صفحه زیر نیز Web Server (IIS) را فعال می‌کنیم.



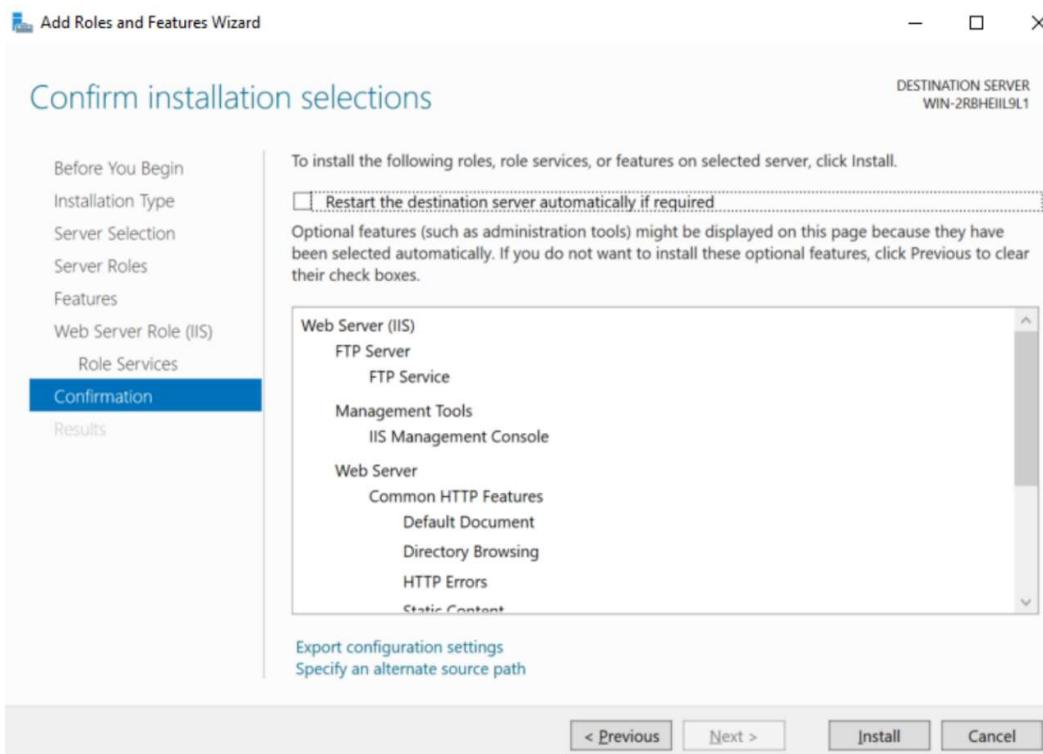
در صفحات زیر نیز next را می‌زنیم.



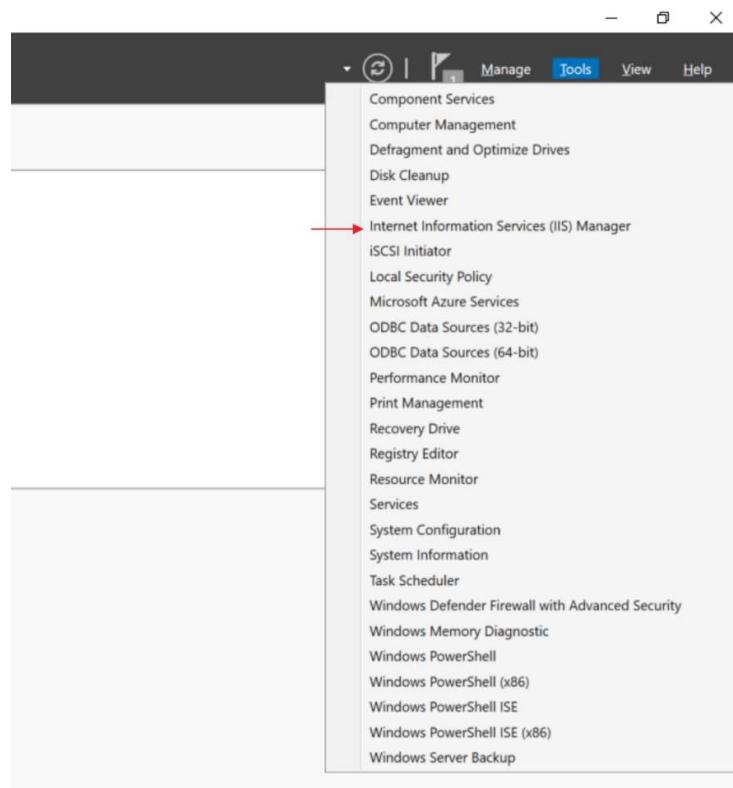
در صفحه زیر FTP Server را انتخاب می کنیم.



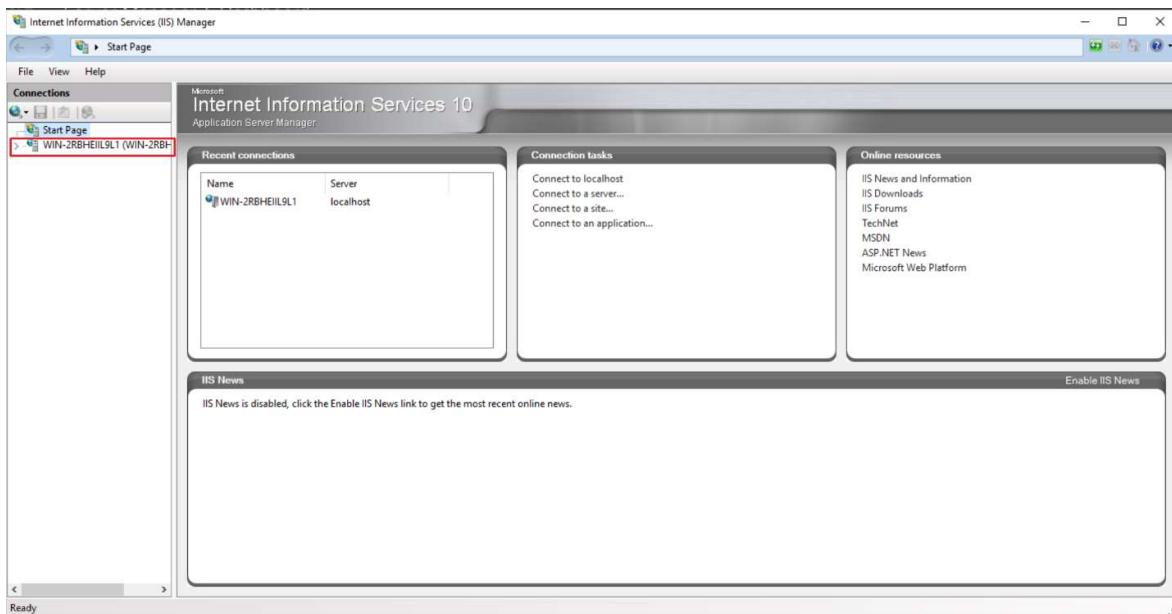
در صفحه زیر نیز install را می زنیم



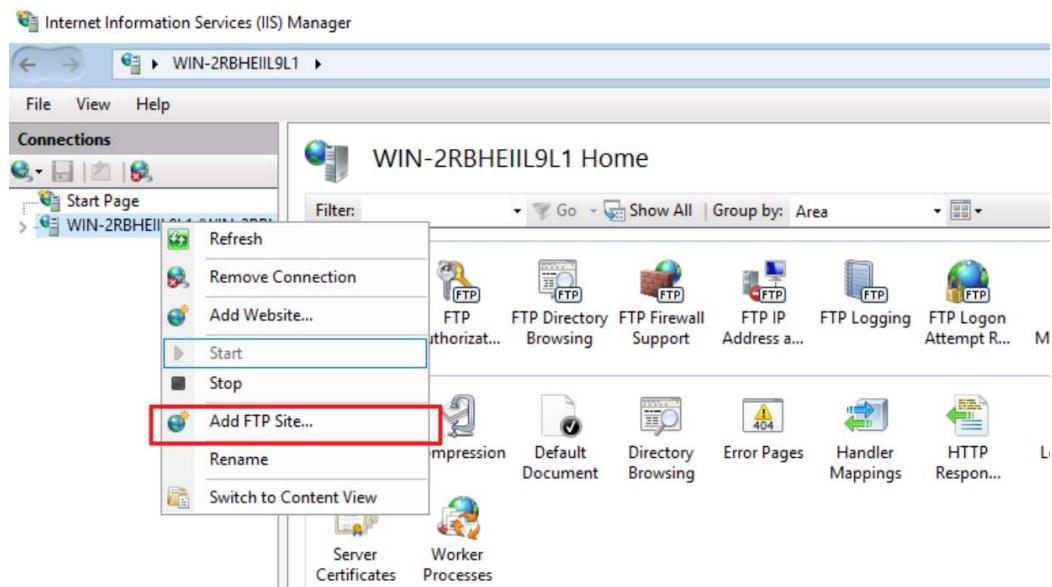
حال برای پیکربندی، از طریق منوی Tools Internet Information Services (IIS) Manager را انتخاب می‌کنیم.



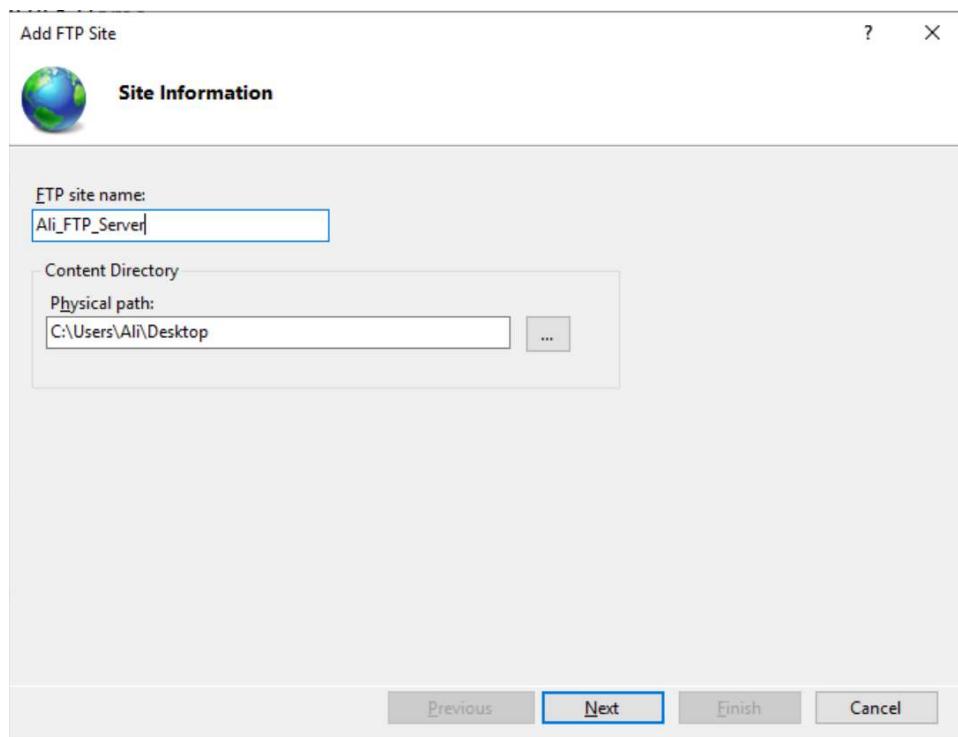
سپس در این صفحه بر روی سرور خودمان کلیک می‌کنیم.



سپس بر روی سرورمان کلیک راست کرده و بر روی ... Add FTP Site... کلیک می‌کنیم.



حال نام FTP Server و path آن را انتخاب می‌کنیم.



در این صفحه پورت مورد نظر را انتخاب می کنیم

Add FTP Site

?

X

Binding and SSL Settings

## Binding

IP Address:

All Unassigned

Port:

21

 Enable Virtual Host Names:

Virtual Host (example: ftp.contoso.com):

 Start FTP site automatically

## SSL

 No SSL Allow SSL Require SSL

## SSL Certificate:

Not Selected

Select...

View...

Previous

Next

Finish

Cancel

در این مرحله تنظیمات دسترسی به سرور توسط user ای که قبل آن را ساخته بودیم را انجام می دهیم و در نهایت finish را می زنیم.

Add FTP Site

?

X



## Authentication and Authorization Information

## Authentication

 Anonymous Basic

## Authorization

Allow access to:

Specified users

FTP\_user

## Permissions

 Read Write

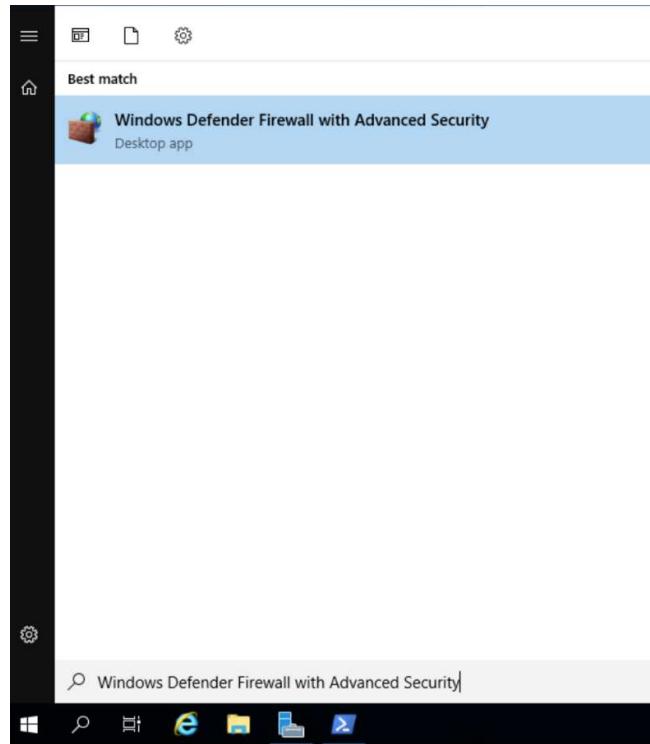
Previous

Next

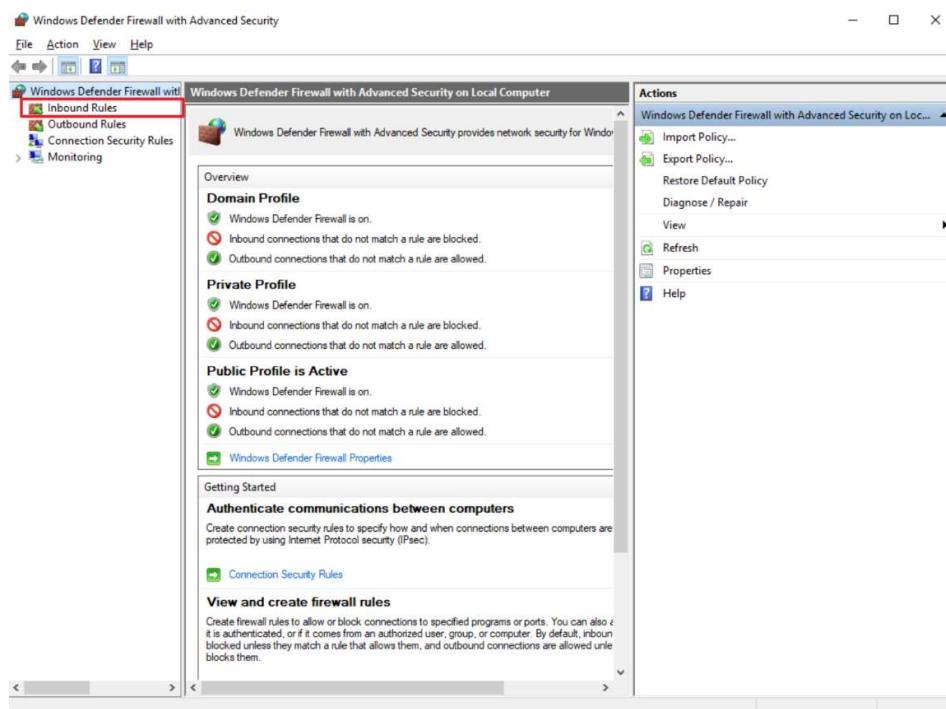
Finish

Cancel

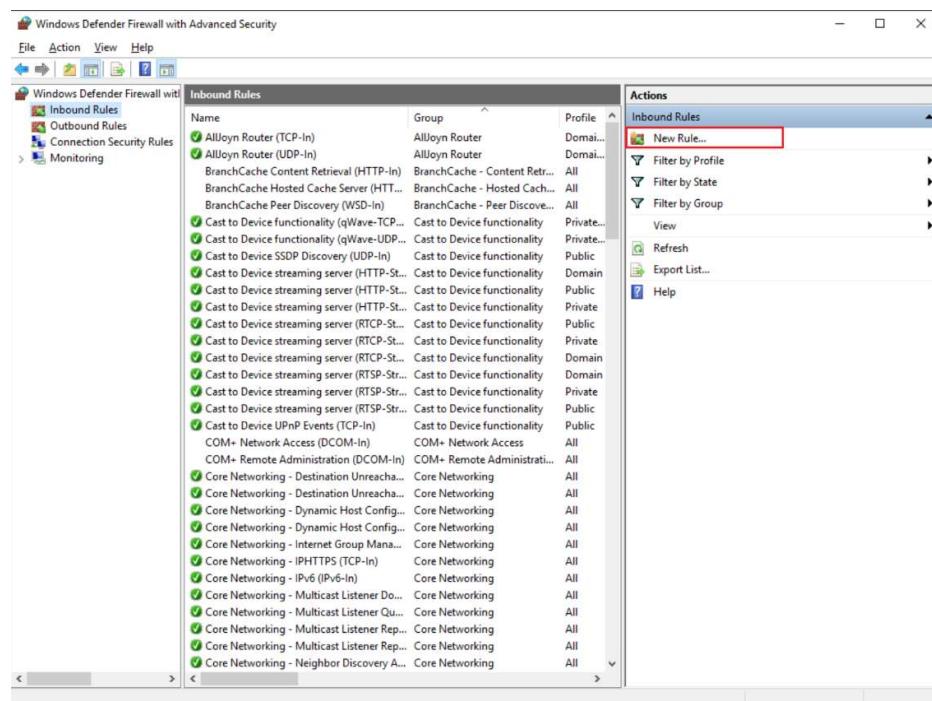
اکنون باید پورت مورد نظرمان را توسط firewall باز کنیم، پس Windows Defender Firewall with Advanced Security را باز می کنیم.



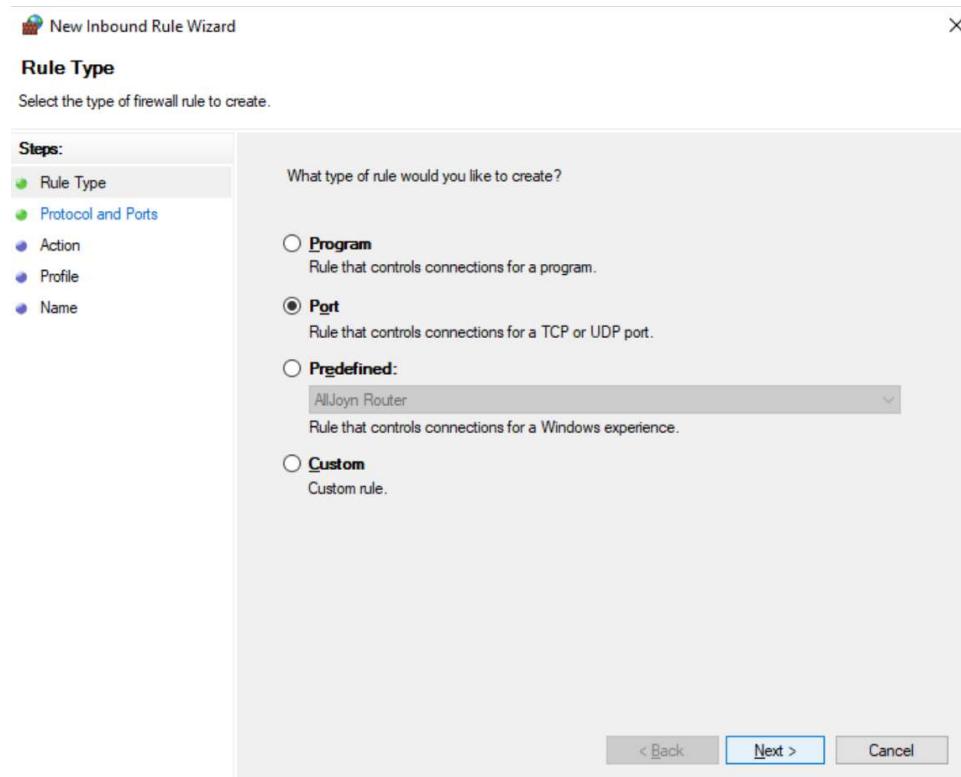
سپس inbound rules را انتخاب می کنیم



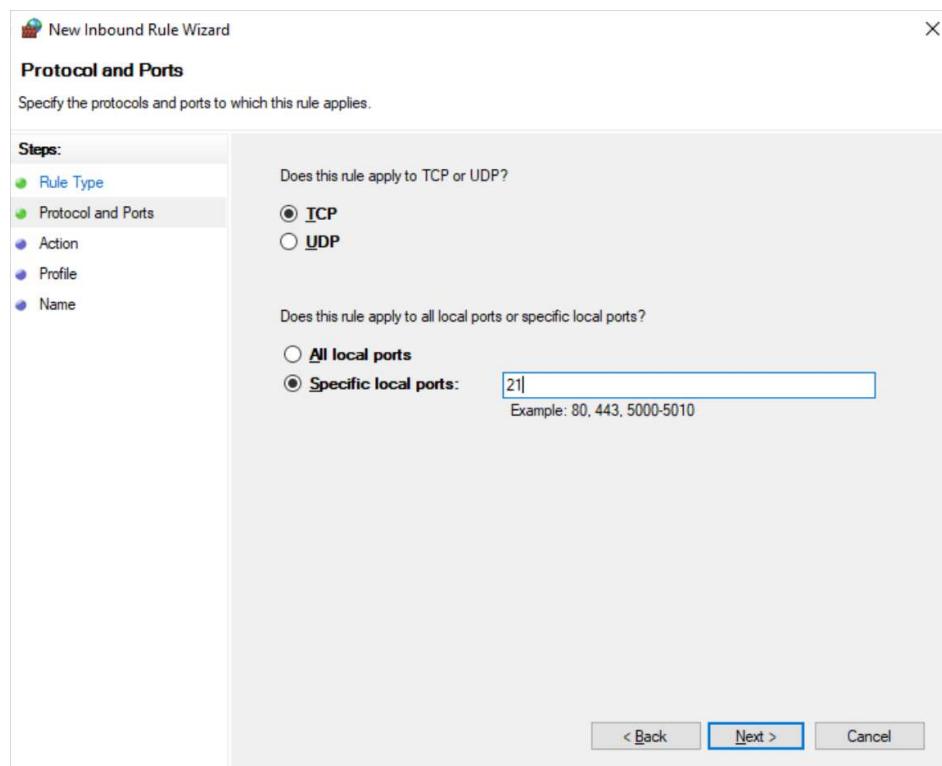
سپس new rule را انتخاب می کنیم



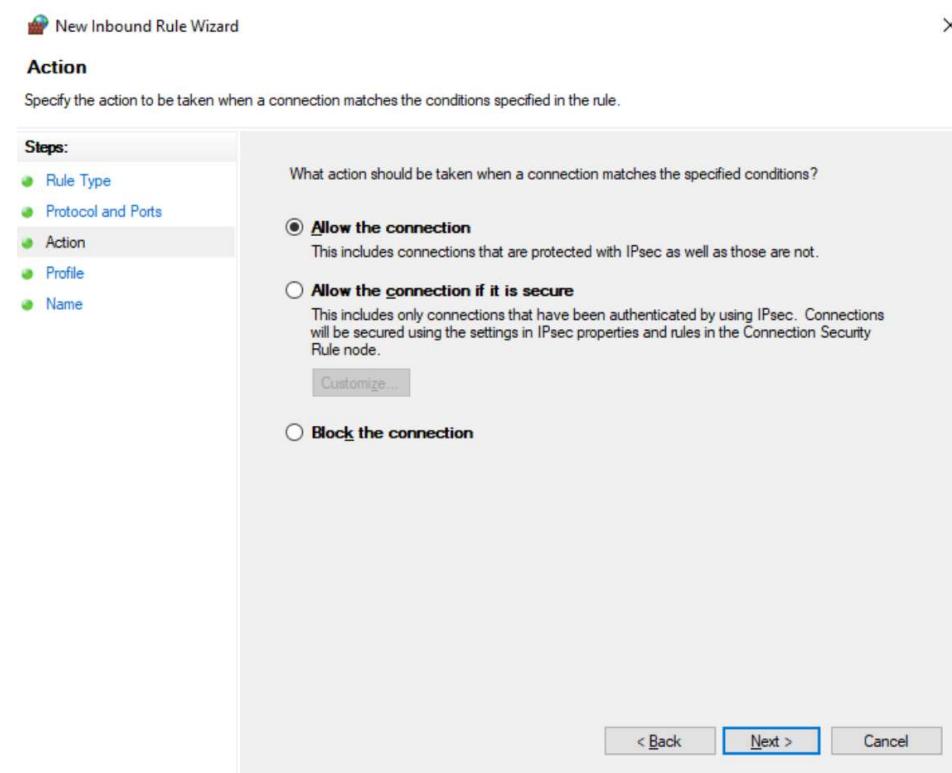
گزینه پورت را انتخاب می کنیم

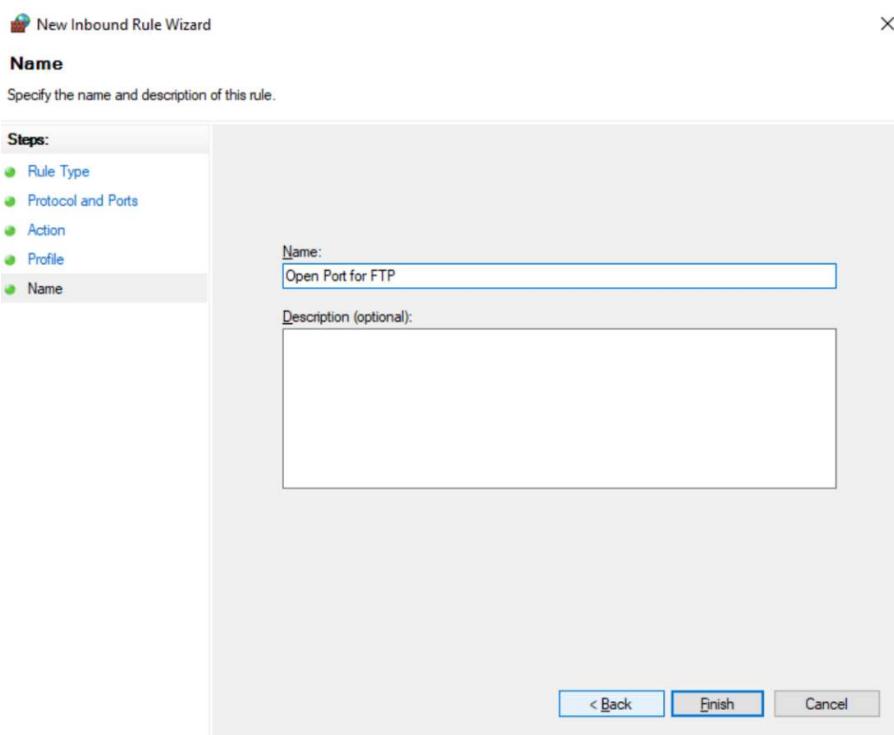
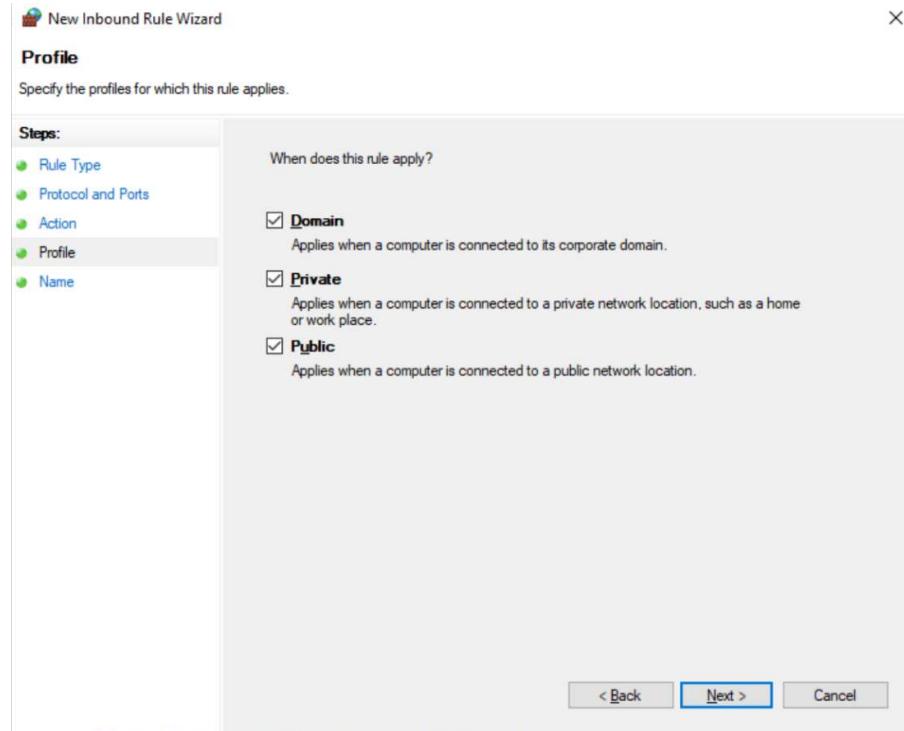


حالا پورت مورد نظرمان را وارد می کنیم



مراحل زیر را نیز با زدن next رد می کنیم





با دستور زیر میتوانیم پورت FTP را بررسی کنیم:

```
PS C:\Users\Ali> Test-NetConnection -ComputerName 192.168.152.156 -Port 21
```

```
ComputerName      : 192.168.152.156
RemoteAddress    : 192.168.152.156
RemotePort       : 21
InterfaceAlias   : VMware Network Adapter VMnet8
SourceAddress    : 192.168.152.1
TcpTestSucceeded : True
```

با دستور زیر وارد کردن مشخصات ورود بیوزر میتوانیم FTP سرور را نیز تست کنیم:

```
PS C:\Users\Ali> ftp 192.168.152.156
Connected to 192.168.152.156.
220 Microsoft FTP Service
200 OPTS UTF8 command successful - UTF8 encoding now ON.
User (192.168.152.156:(none)): FTP_user
331 Password required
Password:
230 User logged in.
ftp>
```

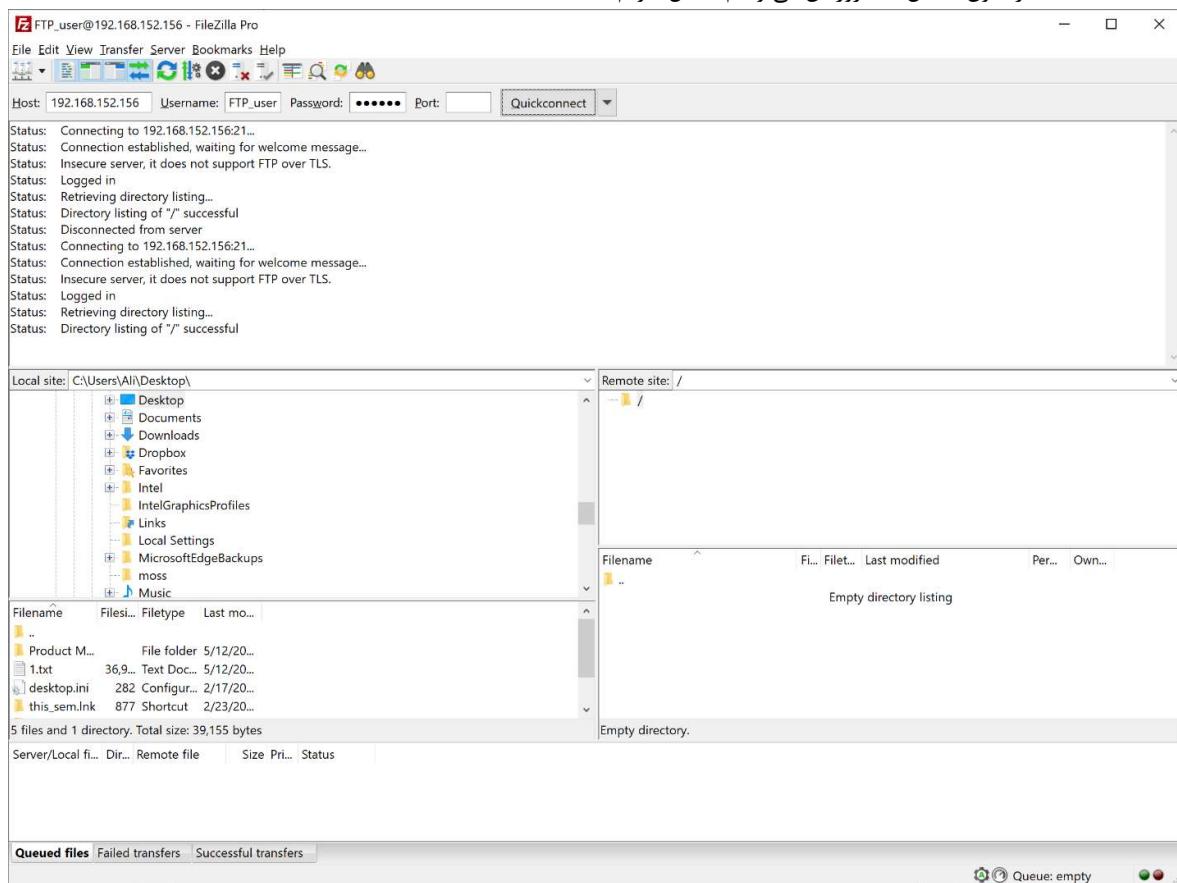
با استفاده از یک کلاینت FTP مانند مرورگر تان یا نرم افزار **Filezilla** به سروری که بالا آوریده اید متصل شوید. با استفاده از نرم افزار **Wireshark** بسته ها را جمع اوری کنید. آیا می توانید نام کاربری و رمز عبور تان را پیدا کنید؟

هنگام تست کردن FTP سرورمان اگر بسته ها را با **Wireshark** بررسی کنیم می توانیم **username** و **password** را بینیم:

124	97.498577	192.168.152.156	192.168.152.1	TCP	112 [TCP Retransmission] 21 → 6044 [PSH, ACK] Seq=28 Ack=15 Win=2...
125	97.498660	192.168.152.1	192.168.152.156	TCP	66 6044 → 21 [ACK] Seq=15 Ack=86 Win=8107 Len=0 SLE=28 SRE=86
126	107.824526	192.168.152.1	192.168.152.156	FTP	69 Request: USER FTP_user
127	107.824851	192.168.152.156	192.168.152.1	FTP	77 Response: 331 Password required
128	107.857684	192.168.152.156	192.168.152.1	TCP	77 [TCP Retransmission] 21 → 6044 [PSH, ACK] Seq=86 Ack=30 Win=2...

.Password= Ali123456 , Username= FTP\_user که می بینیم

با filezilla نیز بدون مشکل به سرورمان می توانیم متصل شویم:



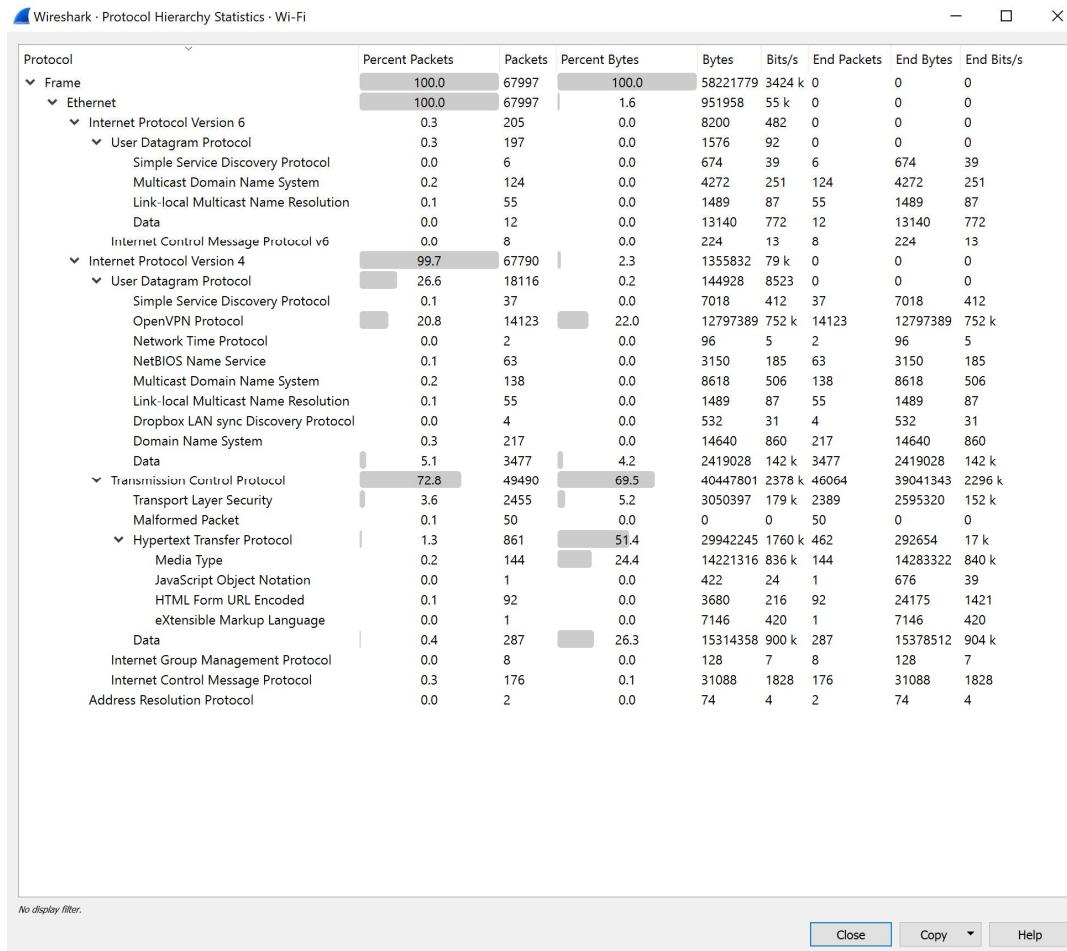
### بر روی گزینه‌ی Resolved Addresses کلیک کنید. در پنجره‌ای که باز می‌شود چه چیزی را مشاهده می‌کنید؟

در این صفحه تمامی آدرس‌های IP و DNS‌هایی که حین بررسی بسته‌ها در Wireshark از آن‌ها استفاده شده را مشاهده می‌کنیم.

Address	Name
00:1b:c5:09:40:00	reelyAct
172.217.16.170	reminders-pa.clients6.google.com
00:1b:c5:03:d0:00	rioxo
70:b3:d5:ee:80:00	robertju
a0:3e:6b:00:00:00	s&tembed
52.216.28.76	s3-1-w.amazonaws.com
e8:a7:f2	sTraffic
216.58.207.42	safebrowsing.googleapis.com
70:b3:d5:67:60:00	samwoole
172.217.22.46	sb.l.google.com
04:d1:6e:20:00:00	sdi
20:0a:0d:c0:00:00	sehwa

### بر روی گزینه‌ی protocol hierarchy کلیک کنید. در پنجره‌ای که باز می‌شود چه چیزی را مشاهده می‌کنید؟

در این صفحه پروتکل‌هایی که حین capture کردن بسته‌ها مشاهده شده را می‌بینیم هر ردیف یک پروتکل را نشان می‌دهد که به صورت سلسله مراتبی دسته بندی شده‌اند.



چند درصد بسته‌های شما به یک ارتباط TCP بر روی بستر IPv4 تعلق دارند؟

همان‌طور که در شکل نیز مشخص است 72.8 بسته‌ها از Transmission Control Protocol(TCP) برای ارتباط استفاده کرده‌اند.

## بر روی گزینه Conversations کلیک کنید. در پنجره‌ای که باز می‌شود چه چیزی را مشاهده می‌کنید؟

هر ردیف در صفحه conversations جزئیات ترافیک بین دو آدرس است.

شماره port‌ای که برای اتصال به هم استفاده کرده اند، تعداد بسته‌هایی که بینشان مبادله شده، مدت ارتباطشان و...

Wireshark - Conversations - Wi-Fi

Address A	Port A	Address B	Port B	Packets	Bytes	Packets A → B	Bytes A → B	Packets B → A	Bytes B → A	Rel Start	Duration	Bits/s A → B	Bits/s B → A
192.168.1.34	10170	40.119.211.203	443	26	3517	14	1612	12	1905	4.297200	123.5769	104	123
192.168.1.34	12324	149.154.167.92	443	1	66	1	66	0	0	24.057188	0.0000	—	—
192.168.1.34	12325	149.154.167.92	443	1	66	1	66	0	0	24.057189	0.0000	—	—
192.168.1.34	12326	149.154.167.92	80	10	845	6	599	4	246	24.070178	1.0205	4695	1928
192.168.1.34	12327	149.154.167.92	80	10	845	6	599	4	246	24.072066	1.0186	4704	1931
192.168.1.34	12328	34.98.74.57	80	13	1605	7	575	6	1030	24.280565	10.8625	423	758
192.168.1.34	12329	140.82.113.25	443	26	6791	12	2121	14	4670	24.316426	19.4884	870	1917
192.168.1.34	12334	35.190.242.34	4070	92	22 k	53	7748	39	14 k	24.630980	72.4731	855	1600
192.168.1.34	12335	78.46.14.94	443	27	8178	12	2023	15	6155	24.711318	0.7631	21 k	64 k
192.168.1.34	12336	162.125.19.131	443	22	10 k	12	9112	10	1223	25.039015	82.0833	888	119
192.168.1.34	12337	140.82.113.25	443	35	7472	18	2563	17	4909	25.052558	110.3655	185	355
192.168.1.34	12338	149.154.167.92	443	2	132	2	132	0	0	25.059543	0.9997	1056	0
192.168.1.34	12339	149.154.167.92	443	2	132	2	132	0	0	25.059544	0.9996	1056	0
192.168.1.34	12340	149.154.167.92	80	10	845	6	599	4	246	25.060925	2.0289	2361	969
192.168.1.34	12341	149.154.167.92	80	10	845	6	599	4	246	25.060928	2.0289	2361	970
192.168.1.34	12342	85.10.196.211	443	17	3437	10	2039	7	1398	25.396663	16.8814	966	662
192.168.1.34	12343	85.10.196.211	443	81	39 k	38	16 k	43	23 k	25.396802	5.0072	25 k	37 k
192.168.1.34	12344	78.46.14.94	443	42	9313	22	2739	20	6574	25.450057	76.5240	286	687
192.168.1.34	12345	74.125.206.188	443	21	6444	10	1378	11	5066	25.658634	6.8661	1605	5902
192.168.1.34	12346	162.159.130.234	443	48	8771	23	4632	25	4139	25.958370	82.6815	448	400
192.168.1.34	12347	148.251.160.242	443	3	198	3	198	0	0	25.967573	3.0088	526	0
192.168.1.34	12349	148.251.160.242	443	3	198	3	198	0	0	26.179041	3.0018	527	0
192.168.1.34	12351	192.168.1.1	80	19	8613	9	679	10	7934	26.492342	0.0999	54 k	635 k
192.168.1.34	12353	149.154.167.92	443	3	198	3	198	0	0	27.059726	3.0038	527	0
192.168.1.34	12352	149.154.167.92	443	3	198	3	198	0	0	27.059727	3.0039	527	0
192.168.1.34	12354	149.154.167.92	80	12	959	7	653	5	306	27.062295	4.4695	1168	547
192.168.1.34	12355	149.154.167.92	80	12	959	7	653	5	306	27.062352	4.4695	1168	547
192.168.1.34	12356	185.105.184.153	443	10	630	5	330	5	300	29.123873	2.3985	1100	1000
192.168.1.34	12357	148.251.160.242	443	5	330	5	330	0	0	30.303317	15.0031	175	0
192.168.1.34	12360	2.16.186.34	80	1,144	1113 k	413	25 k	731	1088 k	30.629124	6.5524	30 k	1329 k
192.168.1.34	12361	67.27.235.126	80	1,183	1121 k	447	28 k	736	1093 k	30.644568	7.2198	31 k	1211 k
192.168.1.34	12362	67.27.233.126	80	1,148	1113 k	417	24 k	731	1089 k	30.645753	8.8203	22 k	987 k
192.168.1.34	12363	52.169.82.131	443	19	4793	10	1160	9	3633	30.672667	1.8655	4974	15 k
192.168.1.34	12364	2.20.190.12	80	1,108	1110 k	378	21 k	730	1088 k	30.676816	5.3911	32 k	1615 k
192.168.1.34	12365	2.20.190.12	80	1,142	1113 k	409	24 k	733	1089 k	30.677076	4.8069	40 k	1812 k
192.168.1.34	12366	2.16.186.34	80	1,151	1113 k	422	25 k	729	1088 k	30.715843	7.4203	27 k	1173 k

Name resolution    Limit to display filter    Absolute start time   Conversation Types ▾

یک نشست TCP را مشخص کنید.

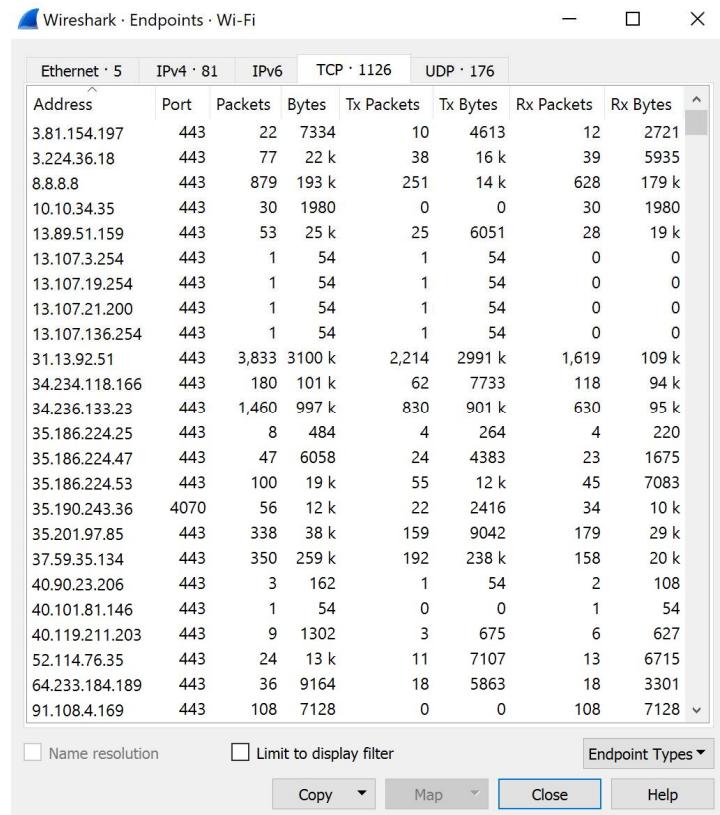
```

Frame 9060: 1444 bytes on wire (11552 bits), 1444 bytes captured (11552 bits) on interface \Device\NPF_{65CD64C8-DD26-49BD-AC9E-D489C881BB8E}, id 0
Ethernet II, Src: HuaweiTe_a4:fb:c7 (38:bc:01:a4:fb:c7), Dst: IntelCor_f2:15:d9 (00:e1:8c:f2:15:d9)
Internet Protocol Version 4, Src: 104.16.249.249, Dst: 192.168.100.10
Transmission Control Protocol, Src Port: 443, Dst Port: 13751, Seq: 1, Ack: 518, Len: 1390

```

بر روی گزینه‌ی **Endpoints** کلیک کنید. در پنجره‌ای که باز می‌شود چه چیزی را مشاهده می‌کنید؟ این صفحه شبیه صفحه **conversations** هست با این تفاوت که آمار ترافیک ورودی و خروجی یک آدرس IP را نشان می‌دهد.

چه مقصد‌هایی برای ارتباط‌های **TCP** در سیستم شما استفاده شده‌اند؟  
همان‌طور که می‌دانیم منظور از TX خروجی و منظور از RX ورودی است.



Address	Port	Packets	Bytes	Tx Packets	Tx Bytes	Rx Packets	Rx Bytes
3.81.154.197	443	22	7334	10	4613	12	2721
3.224.36.18	443	77	22 k	38	16 k	39	5935
8.8.8.8	443	879	193 k	251	14 k	628	179 k
10.10.34.35	443	30	1980	0	0	30	1980
13.89.51.159	443	53	25 k	25	6051	28	19 k
13.107.3.254	443	1	54	1	54	0	0
13.107.19.254	443	1	54	1	54	0	0
13.107.21.200	443	1	54	1	54	0	0
13.107.136.254	443	1	54	1	54	0	0
31.13.92.51	443	3,833	3100 k	2,214	2991 k	1,619	109 k
34.234.118.166	443	180	101 k	62	7733	118	94 k
34.236.133.23	443	1,460	997 k	830	901 k	630	95 k
35.186.224.25	443	8	484	4	264	4	220
35.186.224.47	443	47	6058	24	4383	23	1675
35.186.224.53	443	100	19 k	55	12 k	45	7083
35.190.243.36	4070	56	12 k	22	2416	34	10 k
35.201.97.85	443	338	38 k	159	9042	179	29 k
37.59.35.134	443	350	259 k	192	238 k	158	20 k
40.90.23.206	443	3	162	1	54	2	108
40.101.81.146	443	1	54	0	0	1	54
40.119.211.203	443	9	1302	3	675	6	627
52.114.76.35	443	24	13 k	11	7107	13	6715
64.233.184.189	443	36	9164	18	5863	18	3301
91.108.4.169	443	108	7128	0	0	108	7128

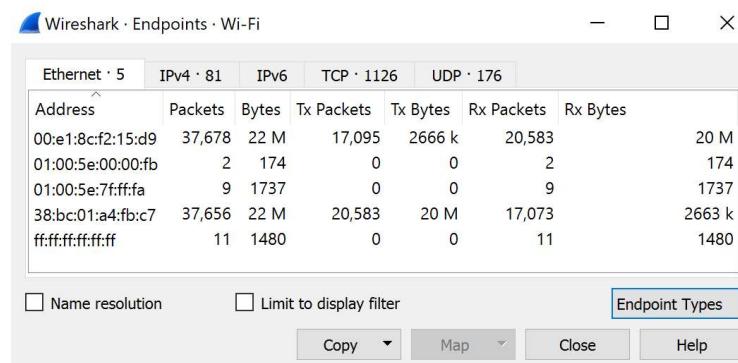
Wireshark - Endpoints - Wi-Fi

Endpoint Types

Copy Map Close Help

آیا می‌توانید از زبانه **Default Gateway** و از روی تعداد بسته‌های مبادله شده، شبکه خود را تشخیص دهید؟

همان‌طور که از شکل زیر و تعداد بسته‌های ورودی و خروجی مشخص است، بسته‌های ورودی به 00:e1:8c:f2:15:d9 آمده‌اند و بسته‌های خروجی نیز از 38:bc:01:a4:fb:c7 گذشته‌اند. پس default gateway برابر 00:e1:8c:f2:15:d9 است که مربوط به بسته‌های ورودی است.



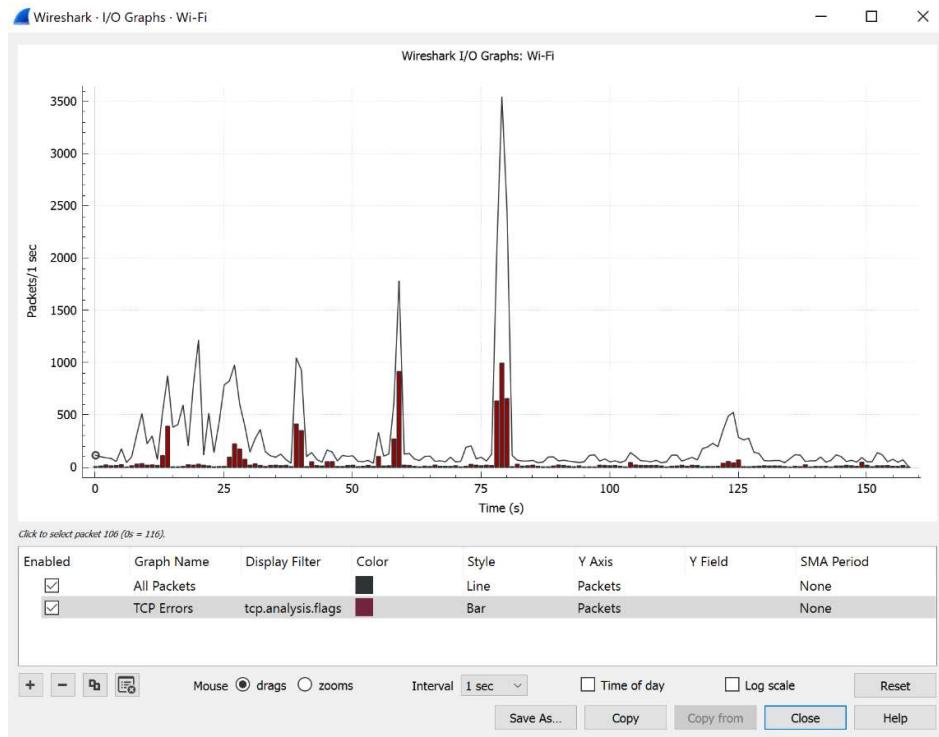
Address	Packets	Bytes	Tx Packets	Tx Bytes	Rx Packets	Rx Bytes
00:e1:8c:f2:15:d9	37,678	22 M	17,095	2666 k	20,583	20 M
01:00:5e:00:00:fb	2	174	0	0	2	174
01:00:5e:7f:ff:fa	9	1737	0	0	9	1737
38:bc:01:a4:fb:c7	37,656	22 M	20,583	20 M	17,073	2663 k
ff:ff:ff:ff:ff:ff	11	1480	0	0	11	1480

Wireshark - Endpoints - Wi-Fi

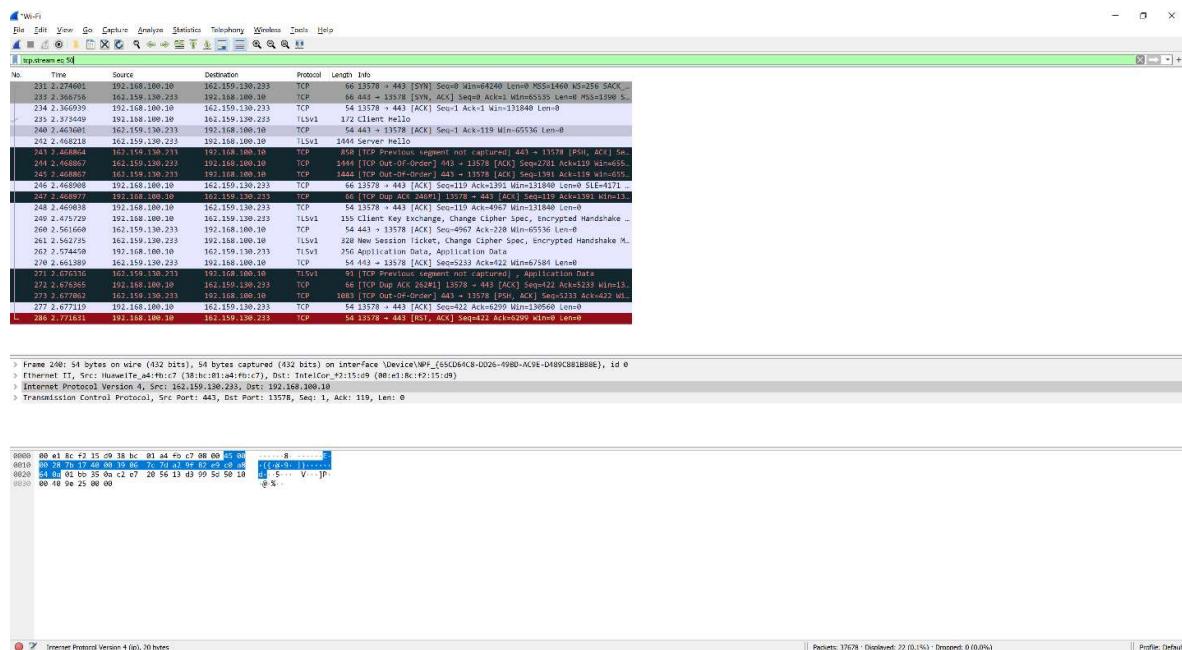
Endpoint Types

Copy Map Close Help

بر روی گزینه‌ی **I/O Graph** کلیک کنید.



بسته‌های مربوط به ارتباط با یک سایت را فیلتر کنید.



سپس بر روی گزینه‌ی **Flow Graph** کلیک کنید.  
به صورت کامل جزئیات مربوط به **Ack** و **SeqNum** و شماره پنجره را دنبال کنید.

در این صفحه نیز جزئیات ارسال‌ها و گرفتن **ack** و... مربوط به یک ارتباط **TCP** و جزئیات آن را مشاهده می‌کنیم.

