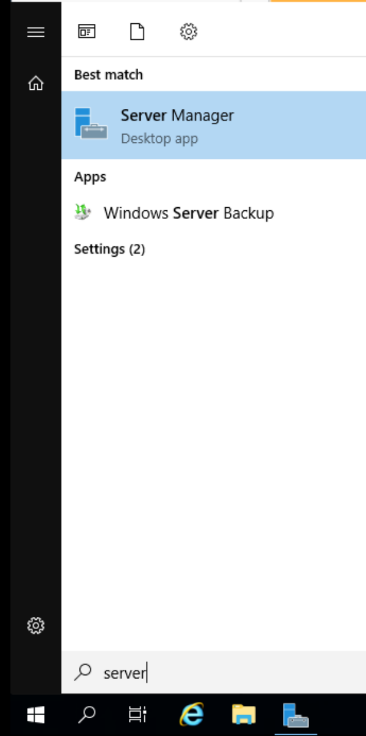
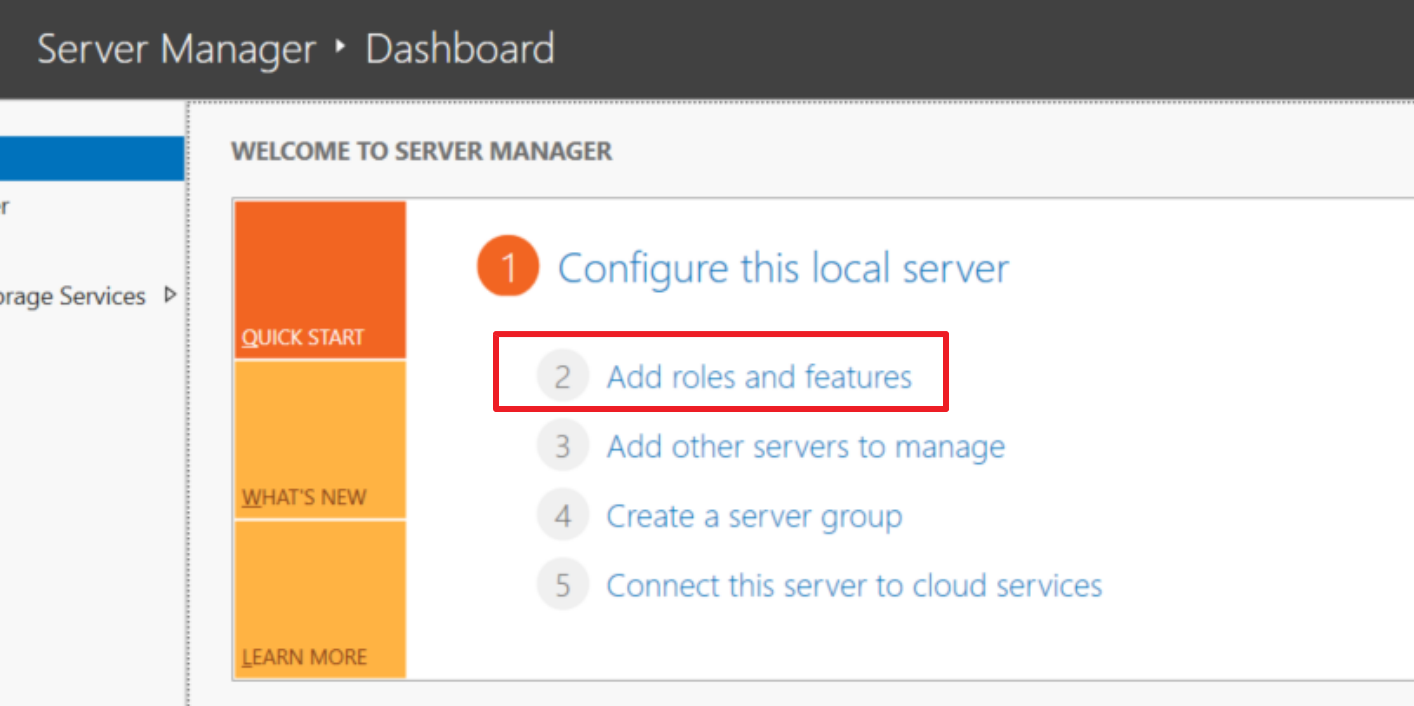
**تمرین عملی سری ۲**

**چگونگی نصب و راه‌اندازی سرویس FTP را گزارش کنید.**

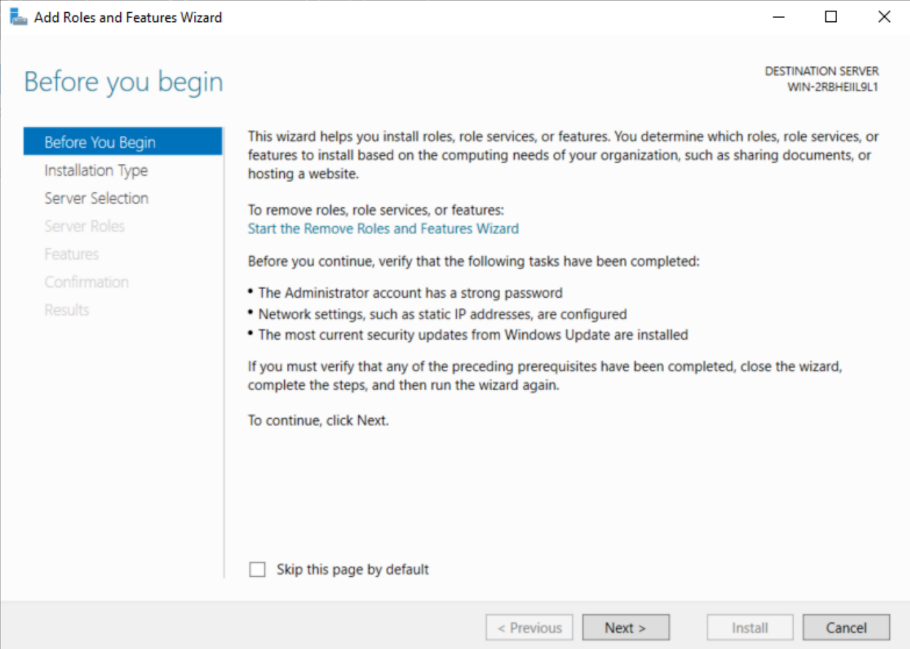
در windows server، ابتدا server manager را باز می‌کنیم.

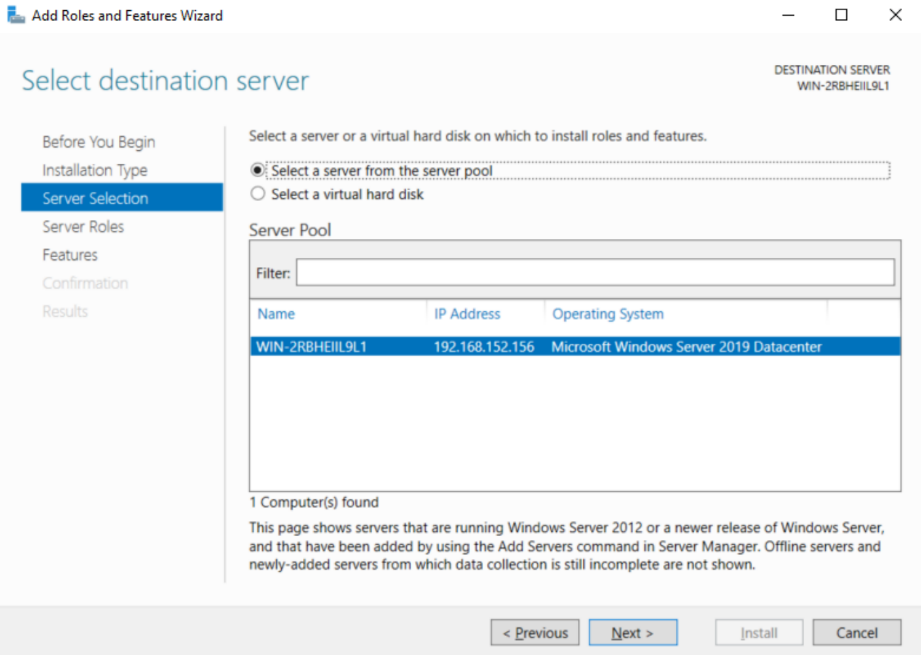


گزینه add roles and features را انتخاب می‌کنیم.

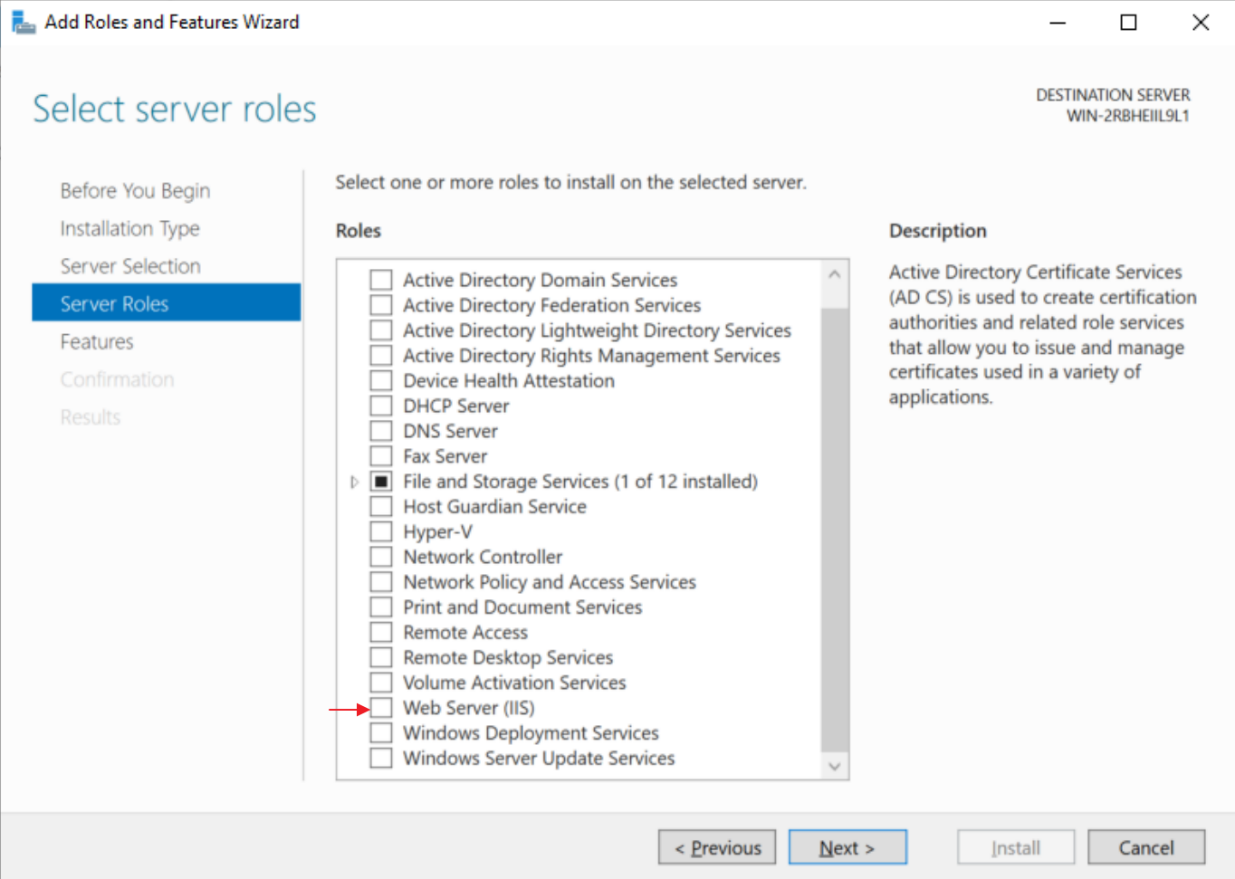


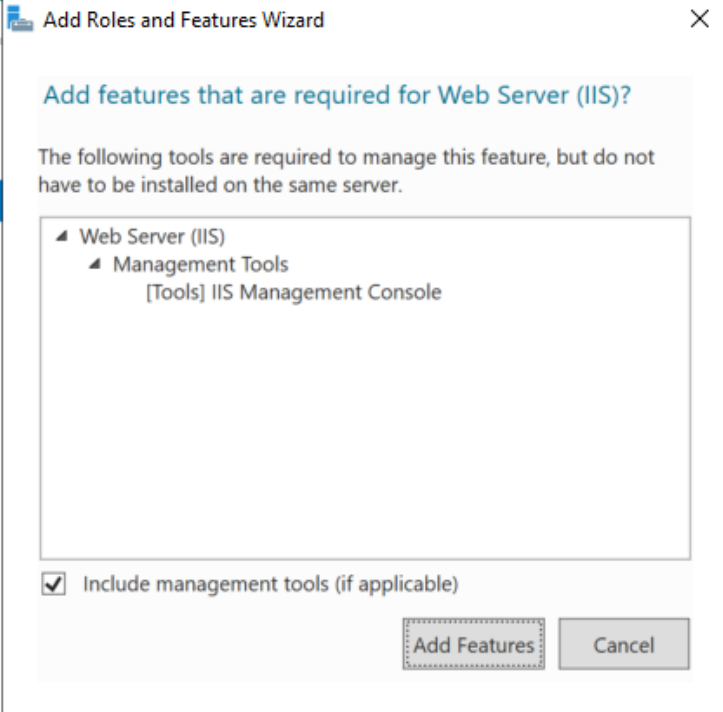
در صفحات زیر بدون اینکه چیزی را تغییر دهیم، دکمه next را می‌زنیم.



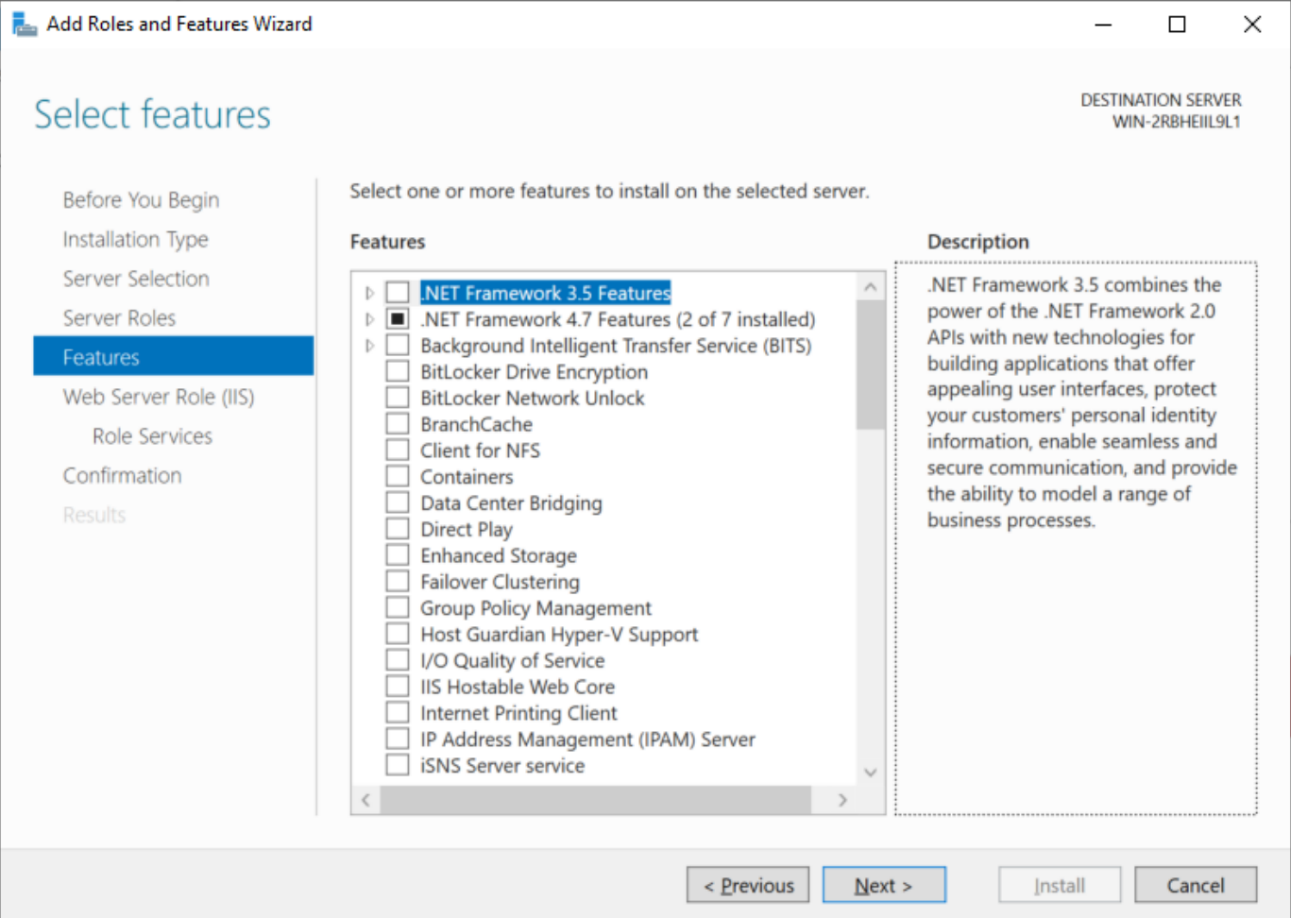


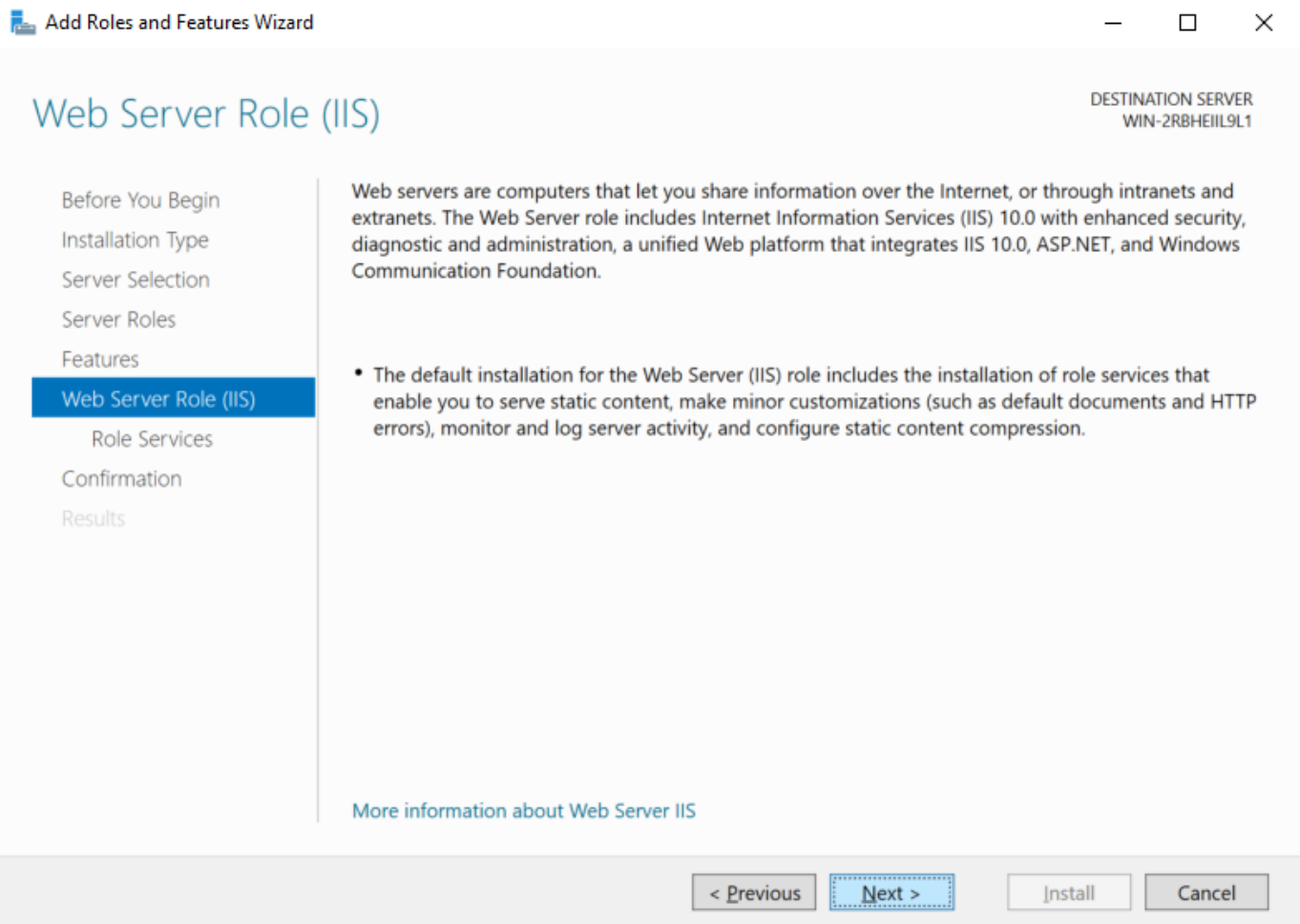
در صفحه زیر نیز Web Server (IIS) را فعال می‌کنیم.



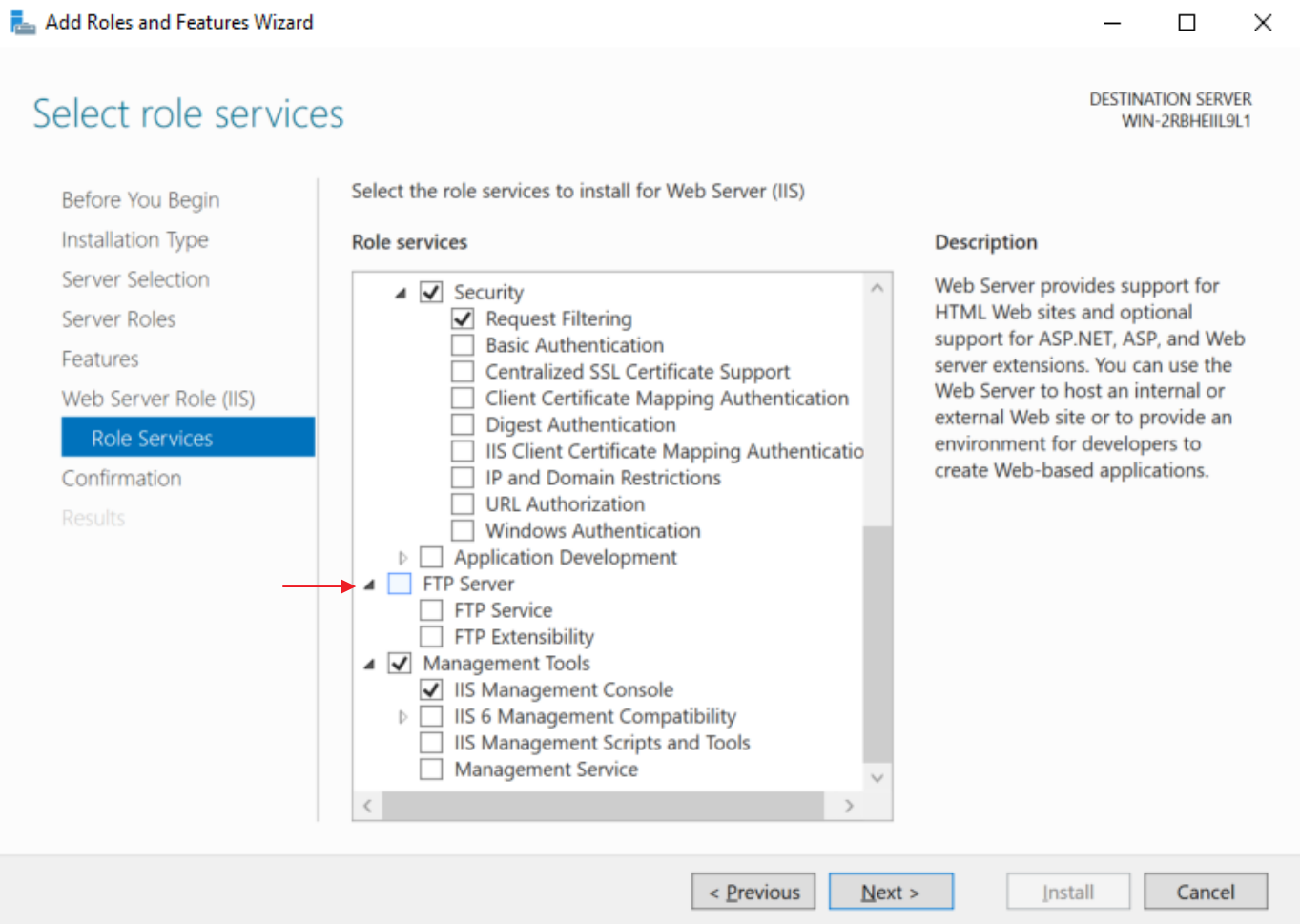


در صفحات زیر نیز next را می‌زنیم.

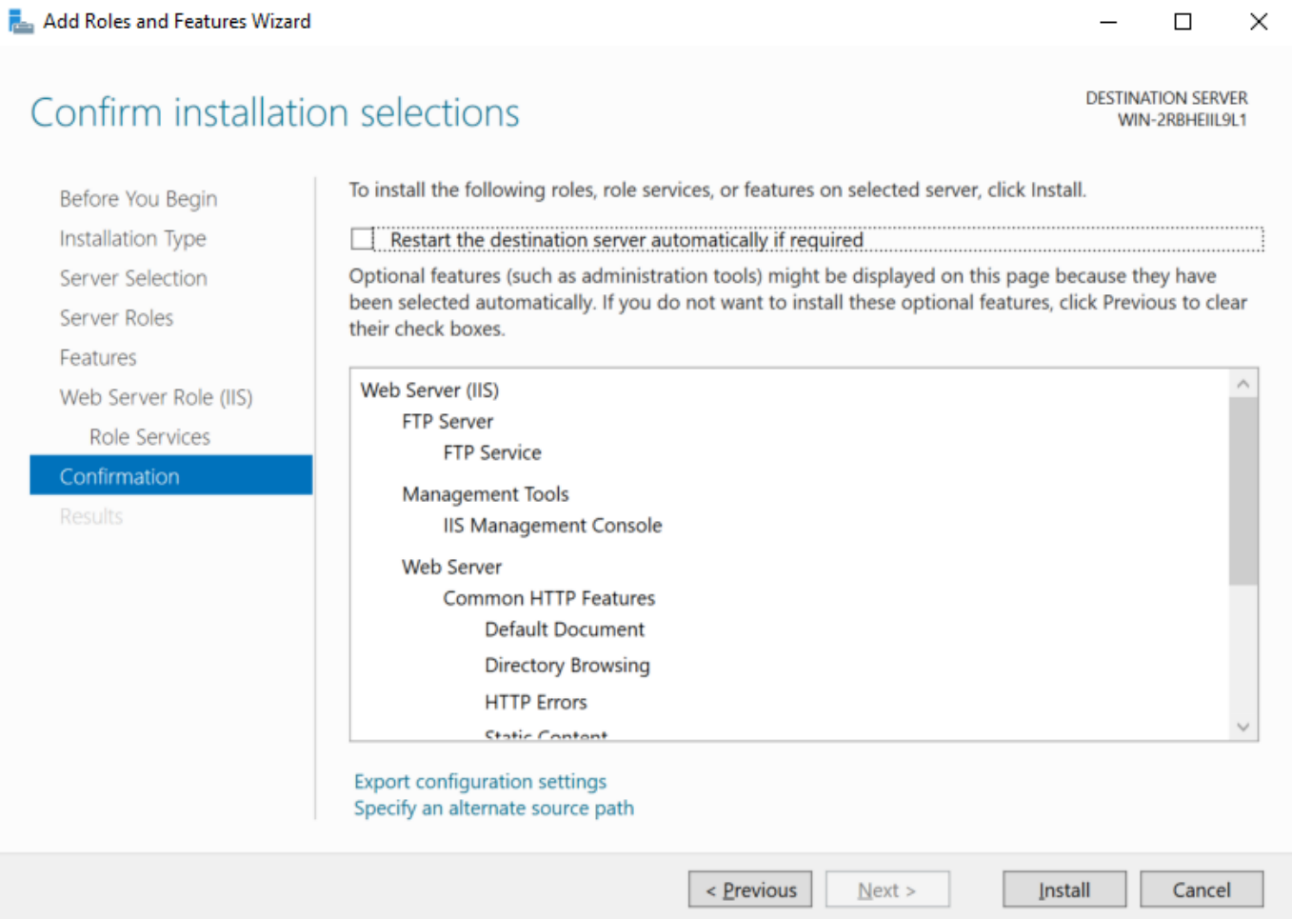




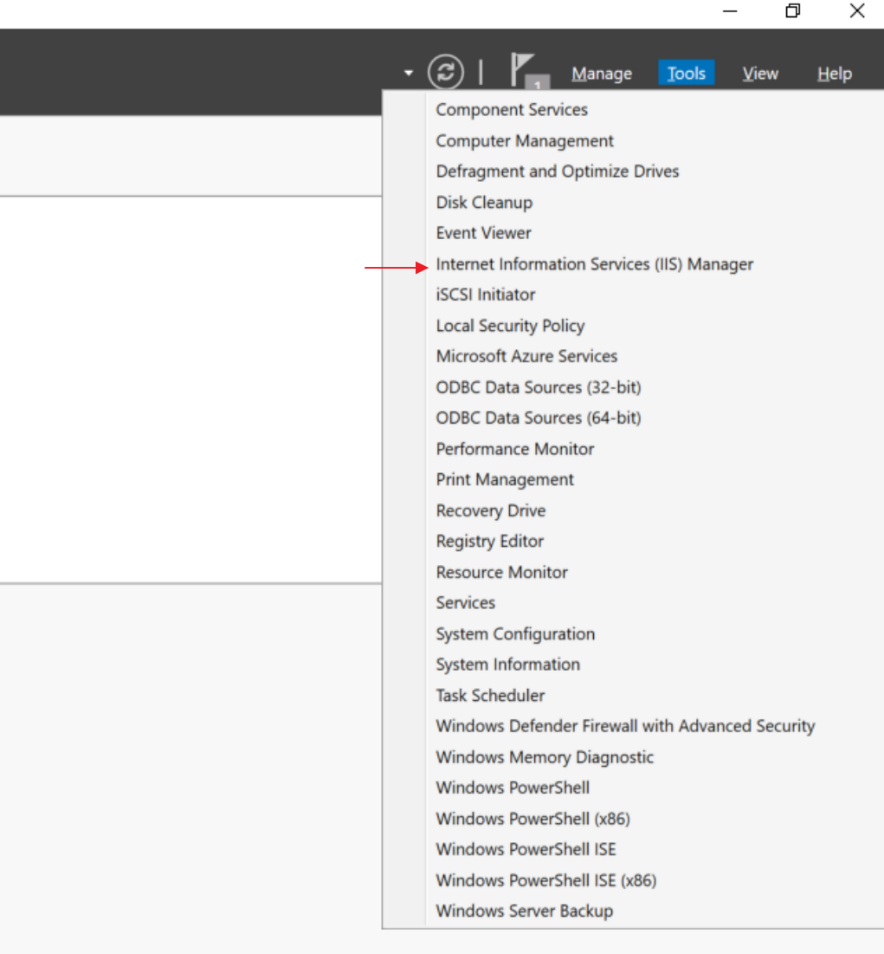
در صفحه زیر FTP Server را انتخاب می‌کنیم.

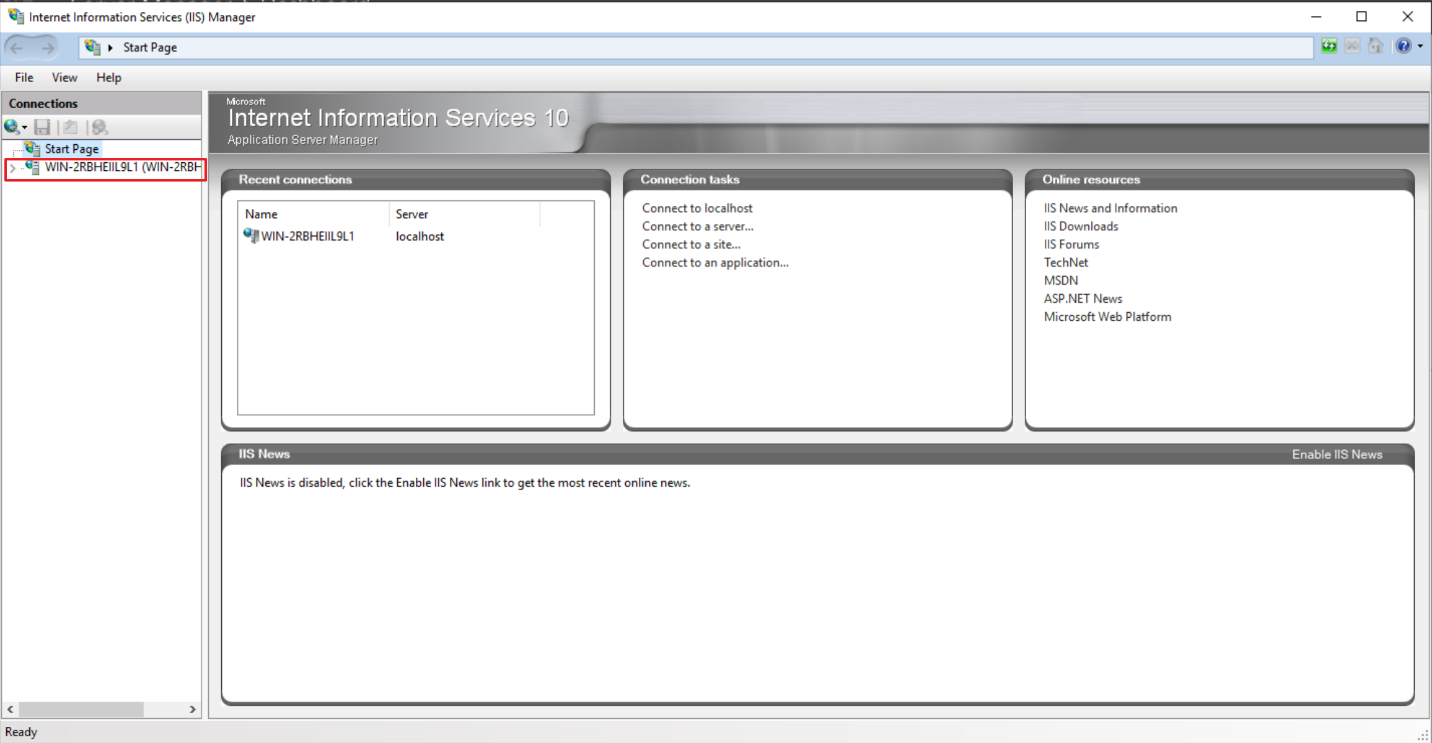


در صفحه زیر نیز install را می‌زنیم

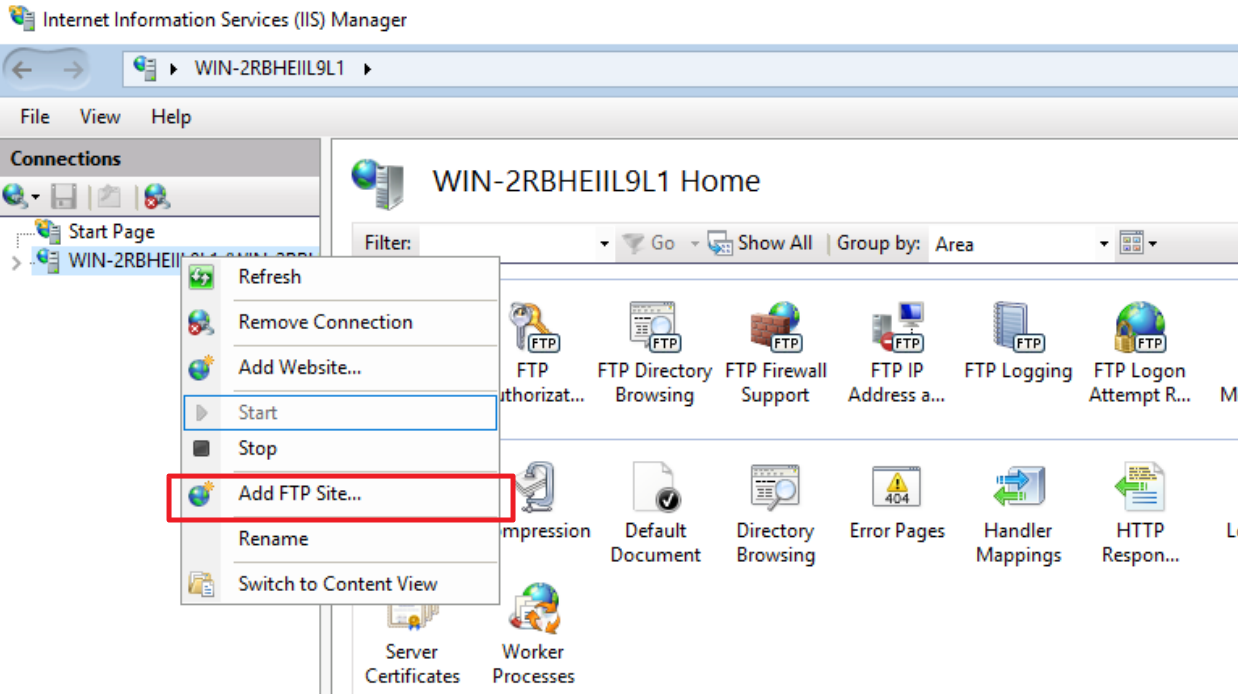


حال برای پیکربندی، از طریق منوی Tools، Internet Information Services (IIS) Manager را انتخاب می‌کنیم.

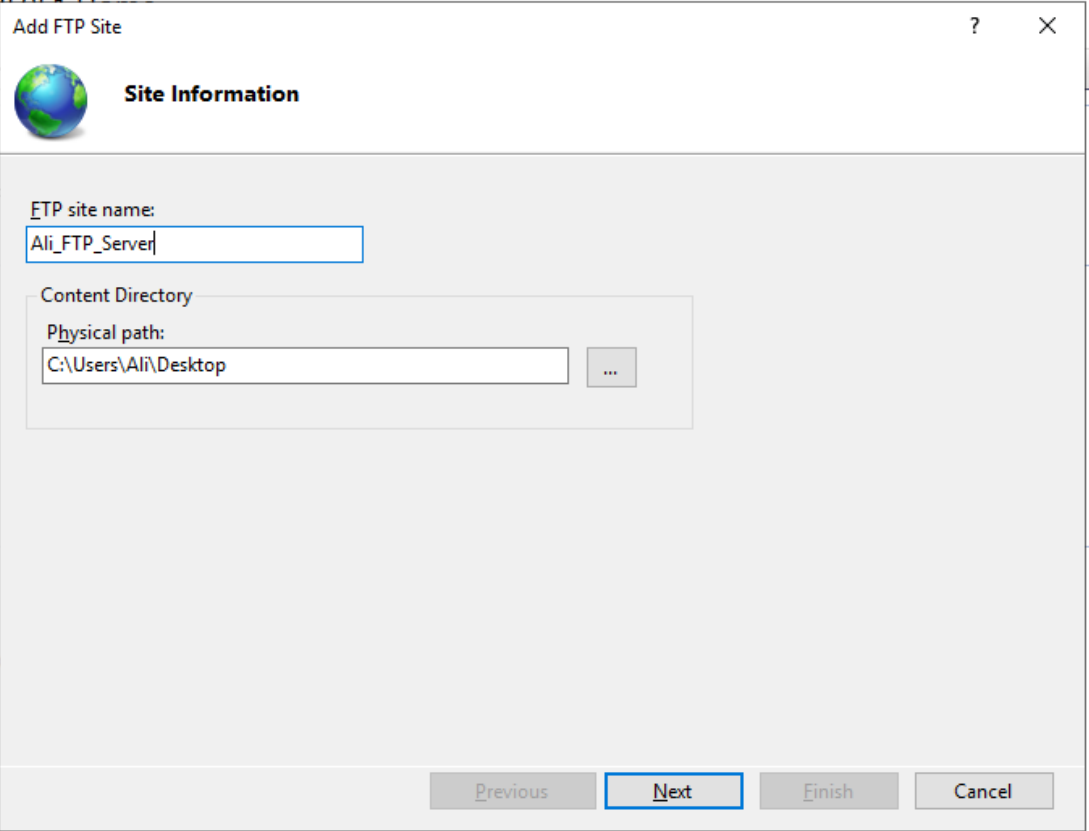


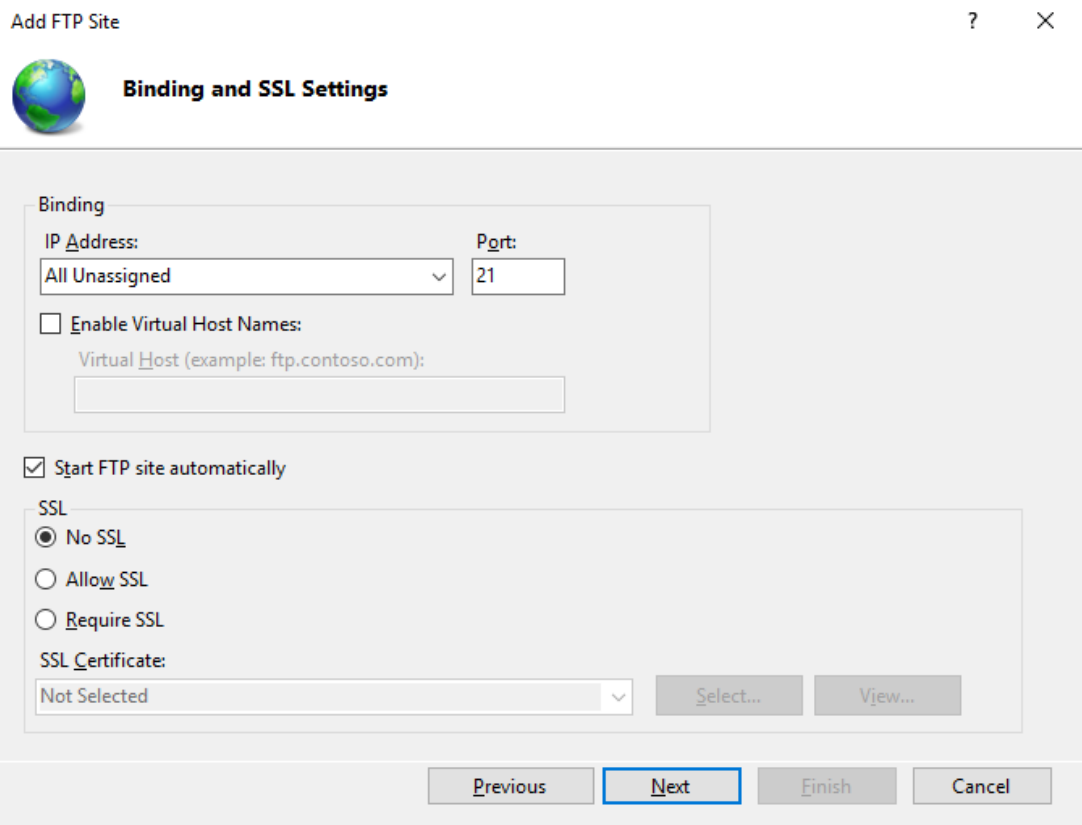
سپس در این صفحه بر روی سرور خودمان کلیک می‌کنیم.

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

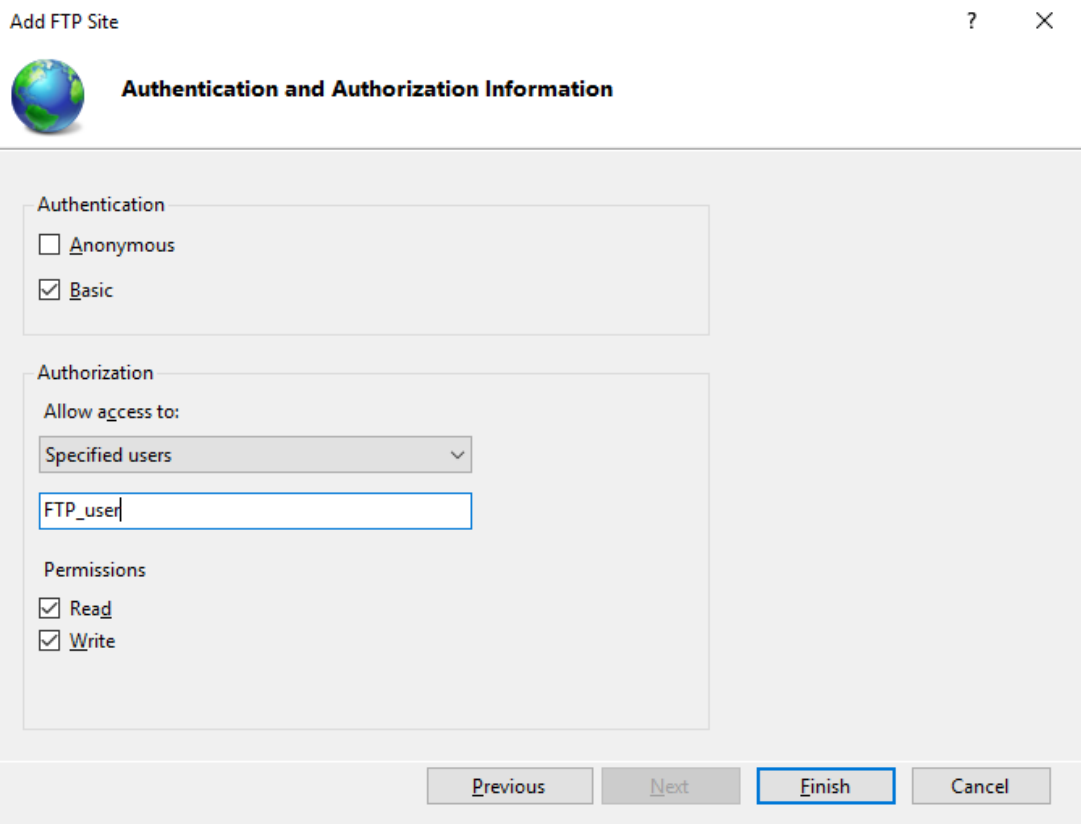


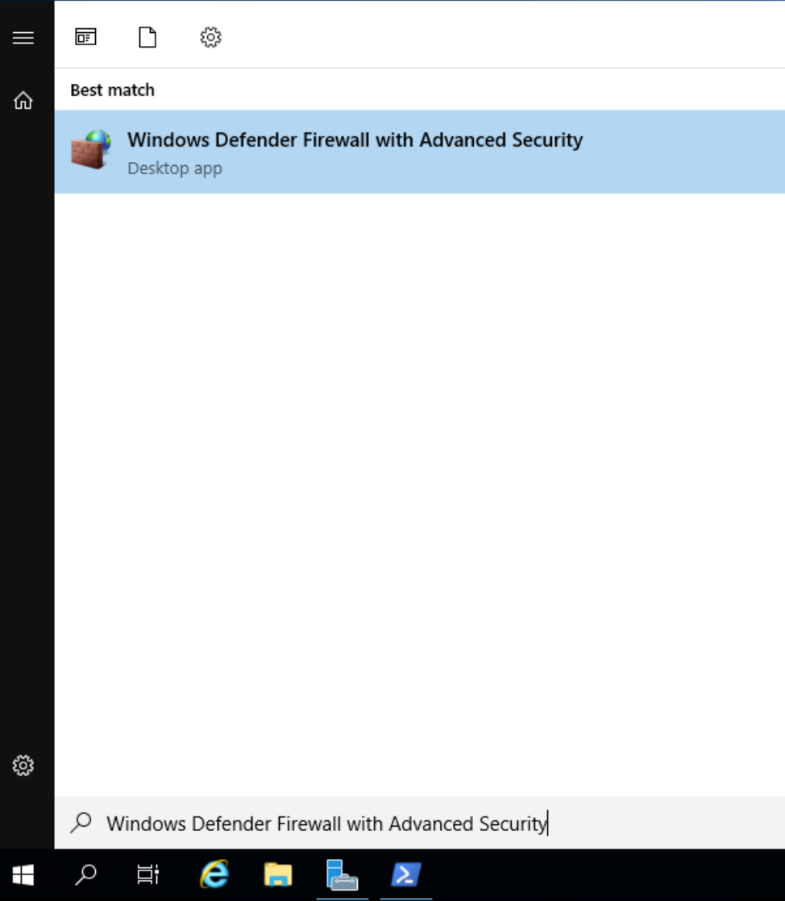
حال نام FTP Server و path آن را انتخاب می‌کنیم.



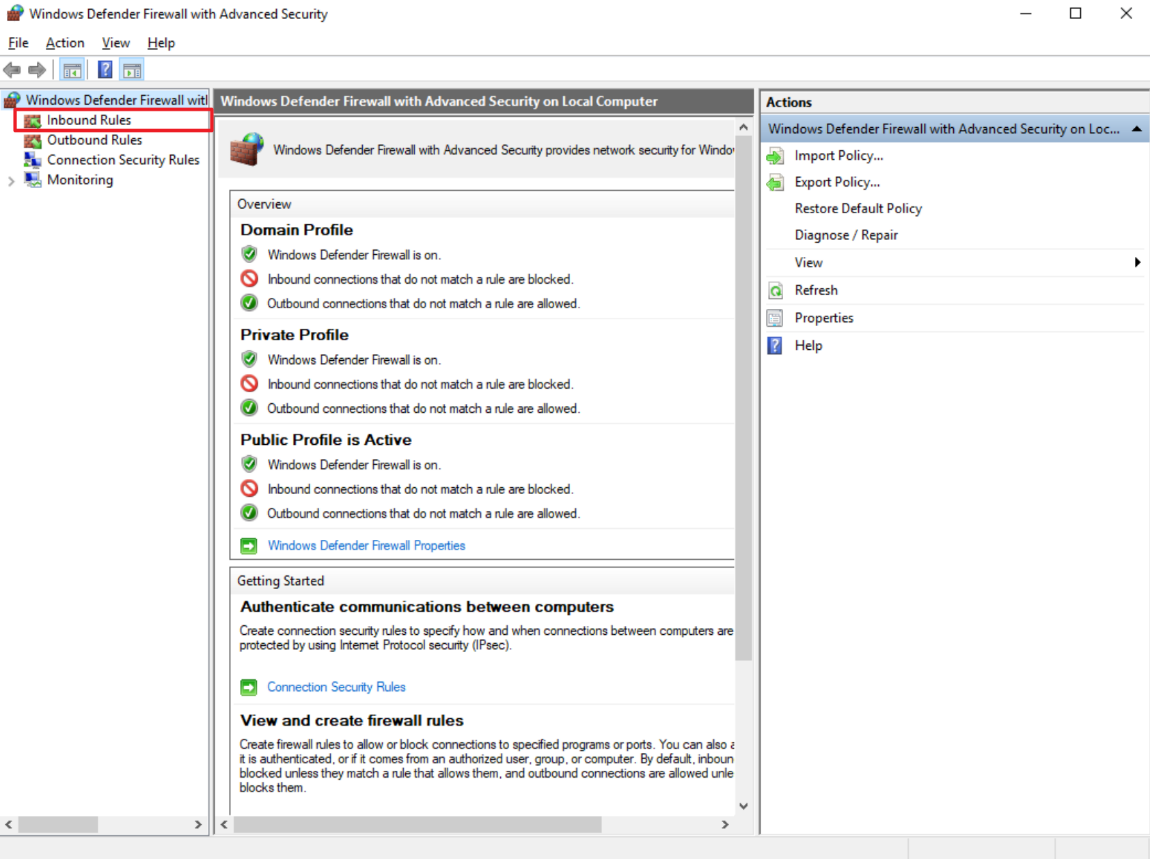
در این صفحه پورت مورد نظر را انتخاب می‌کنیم

در این مرحله تنظیمات دسترسی به سرور توسط userای که قبلا آن را ساخته بودیم را انجام می‌دهیم و در نهایت finish را می‌زنیم.

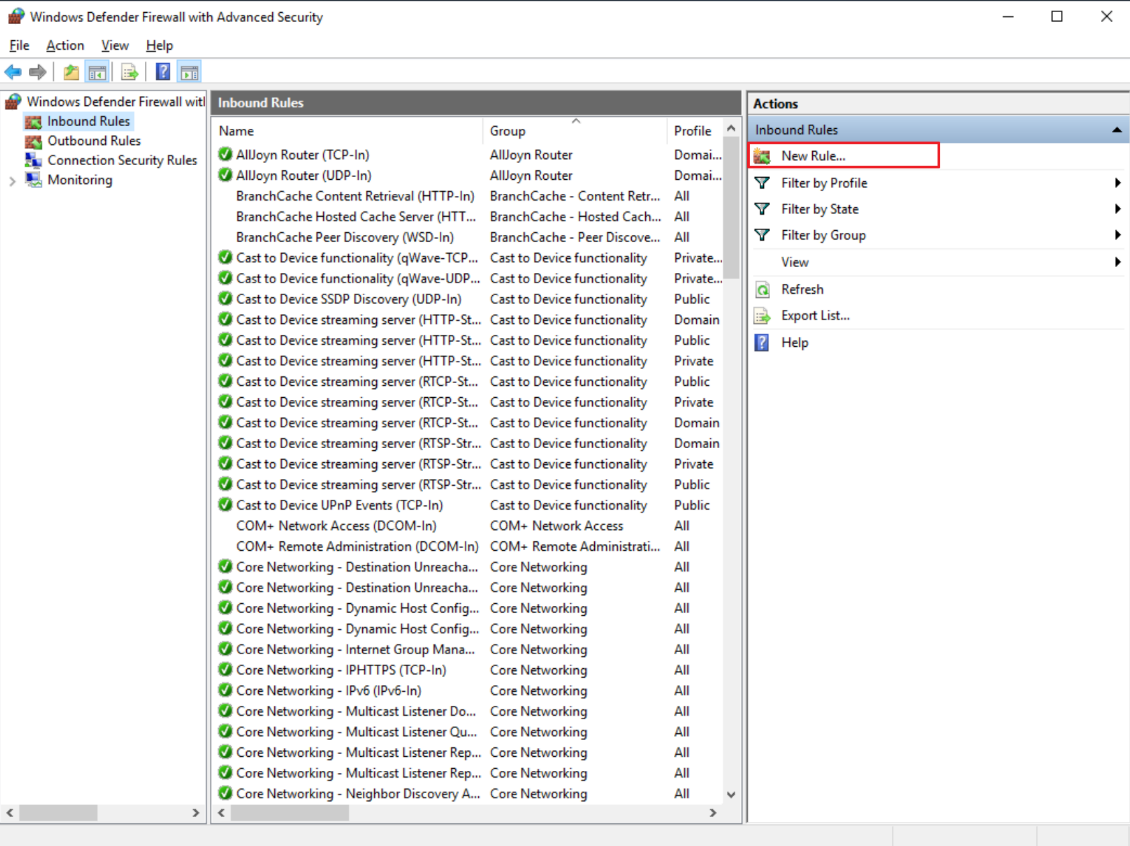


اکنون باید پورت مورد نظرمان را توسط firewall باز کنیم، پس Windows Defender Firewall with Advanced Security را باز می‌کنیم.

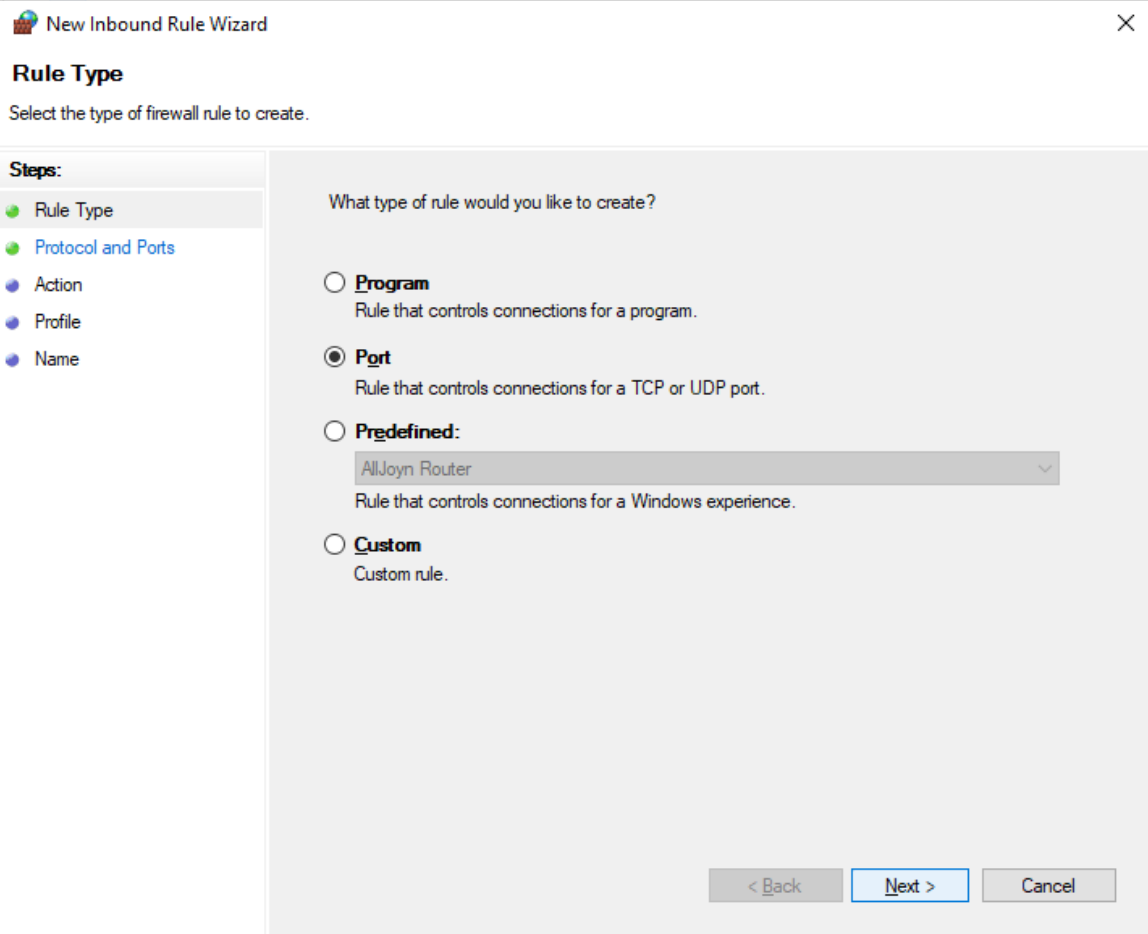
سپس inbound rules را انتخاب می‌کنیم



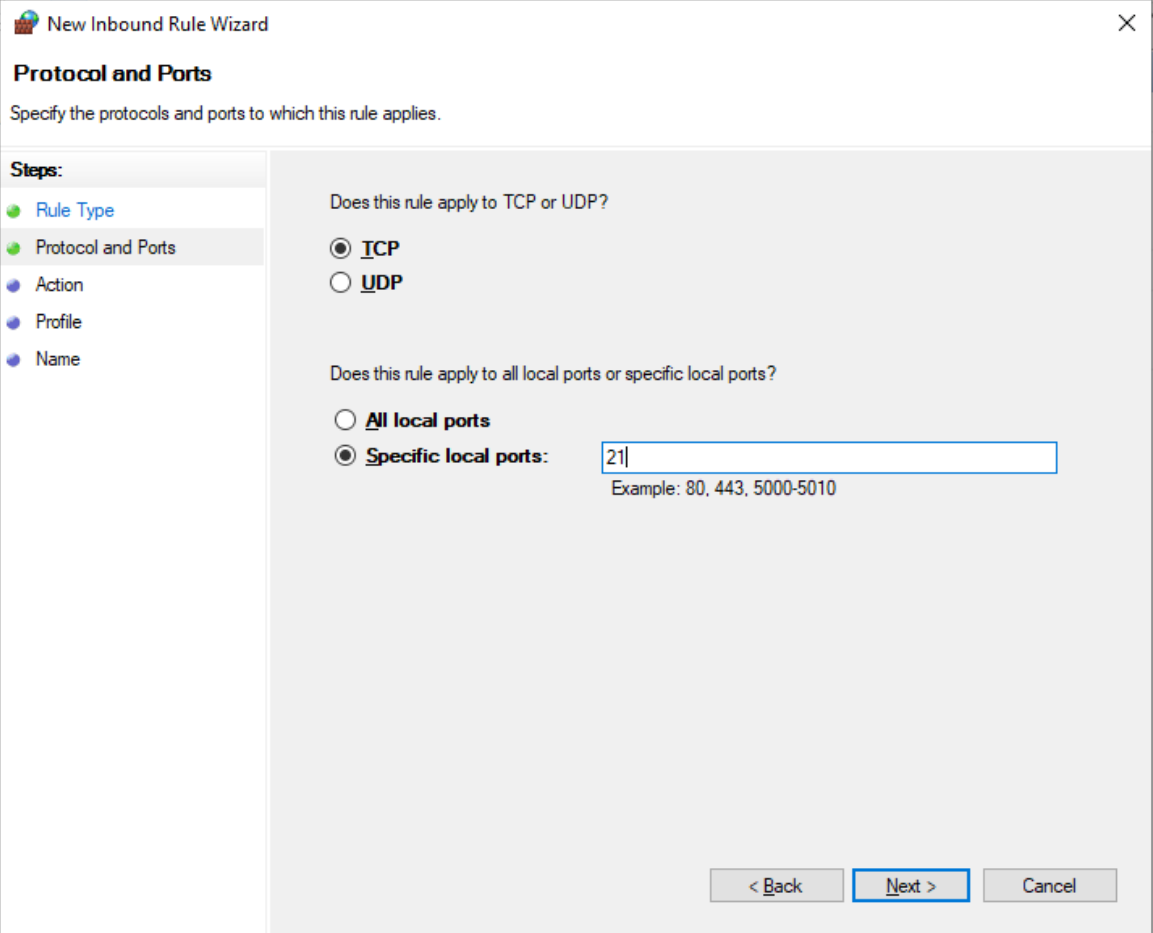
سپس new rule را انتخاب می‌کنیم



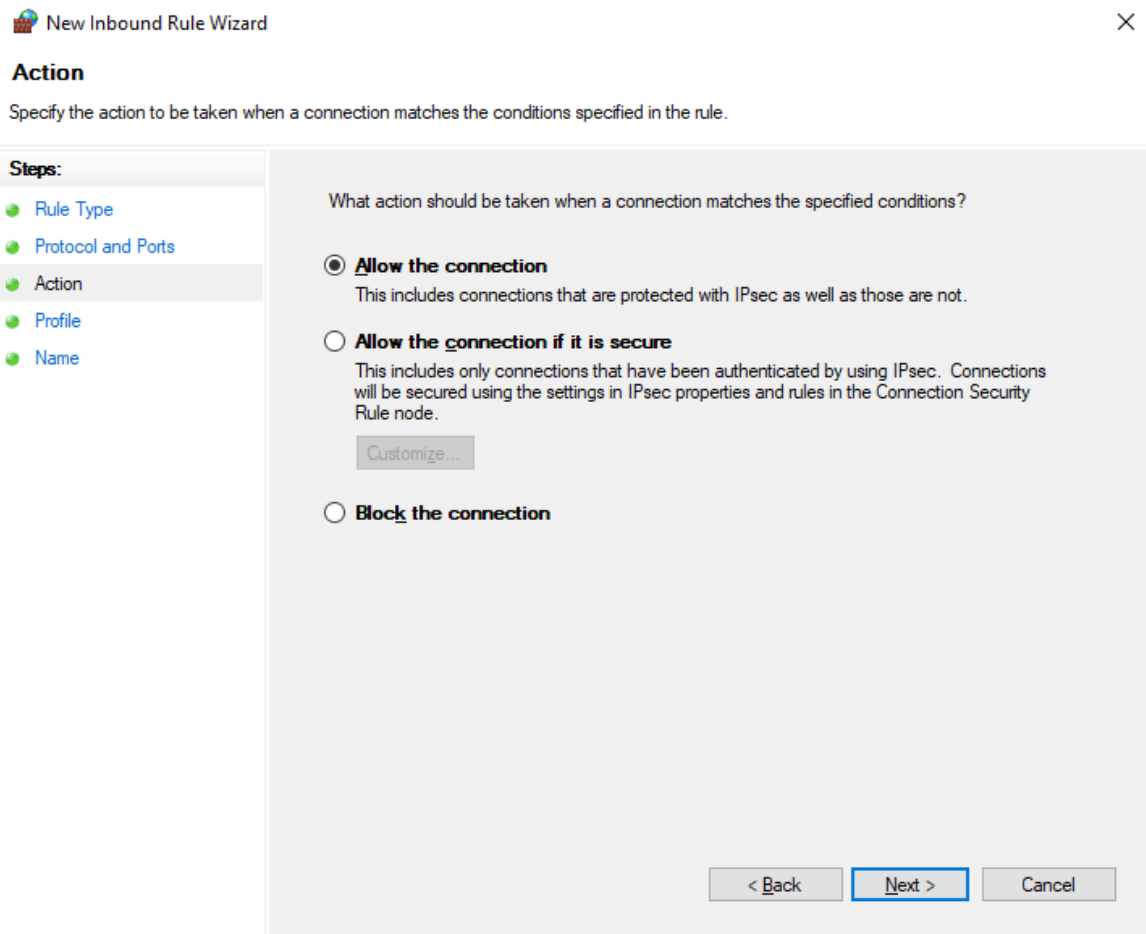
گزینه پورت را انتخاب می‌کنیم

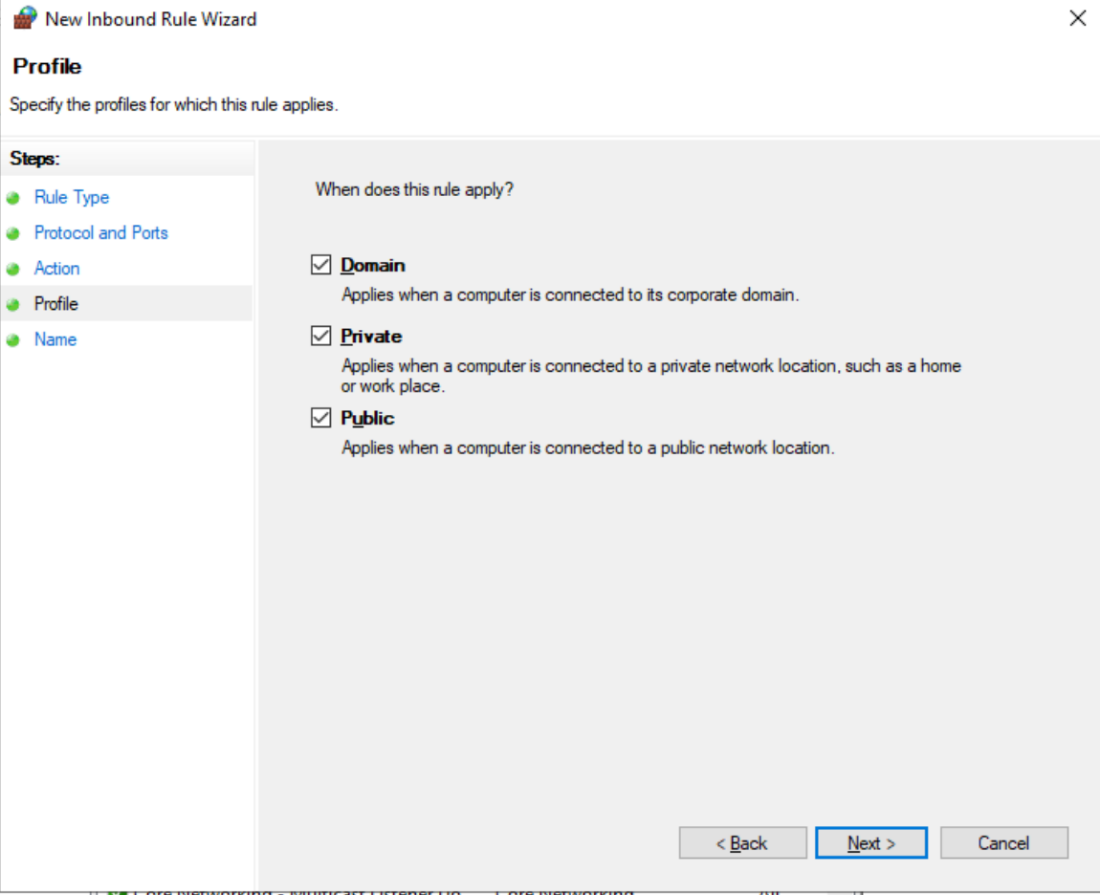


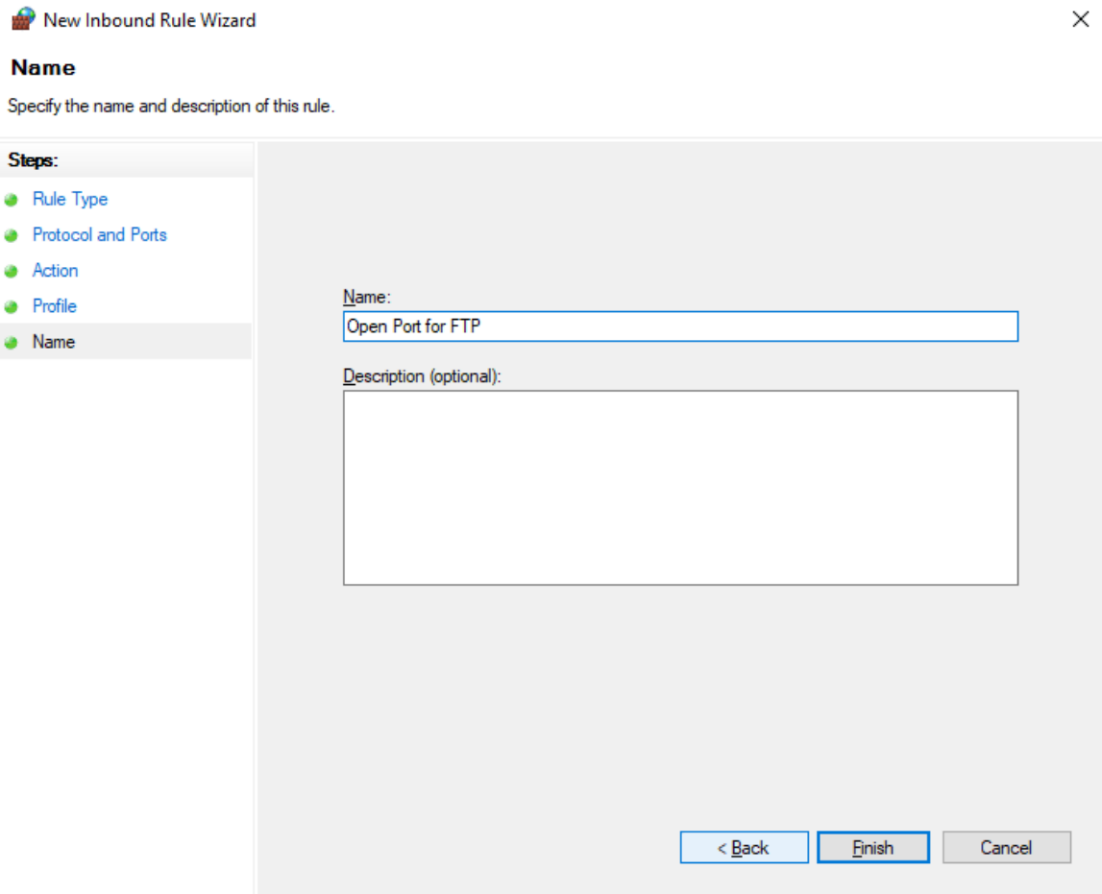
حالا پورت مورد نظرمان را وارد می‌کنیم

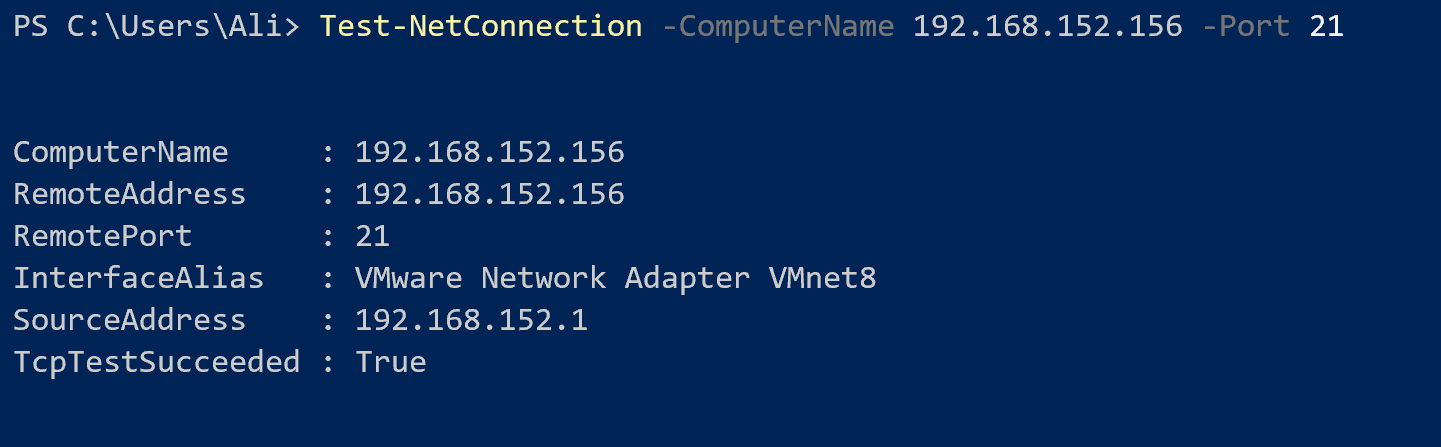


مراحل زیر را نیز با زدن next رد می‌کنیم

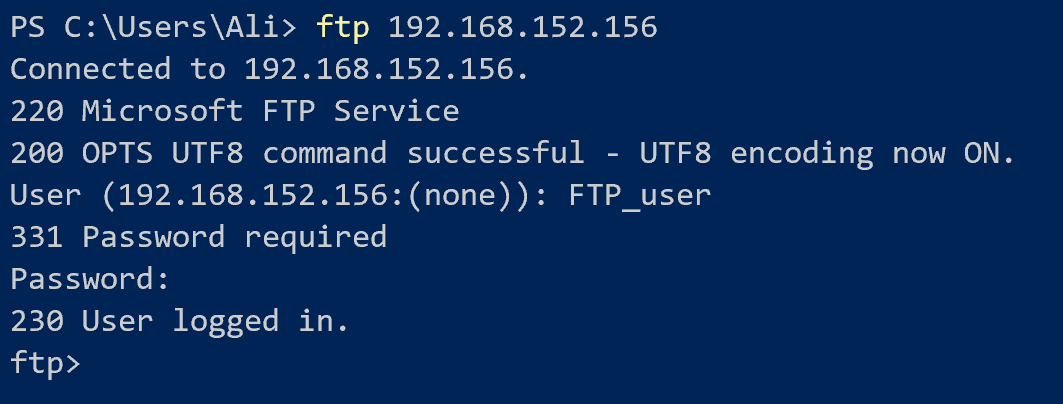






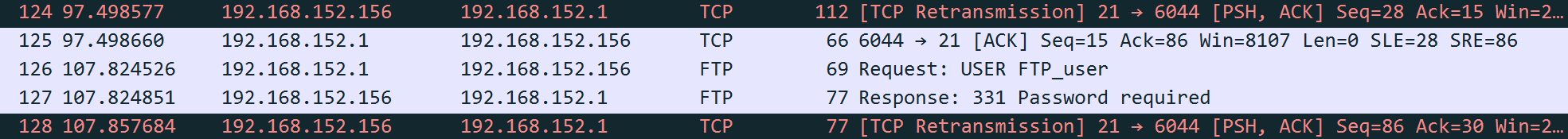
با دستور زیر می‌توانیم پورت FTP را بررسی کنیم:

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



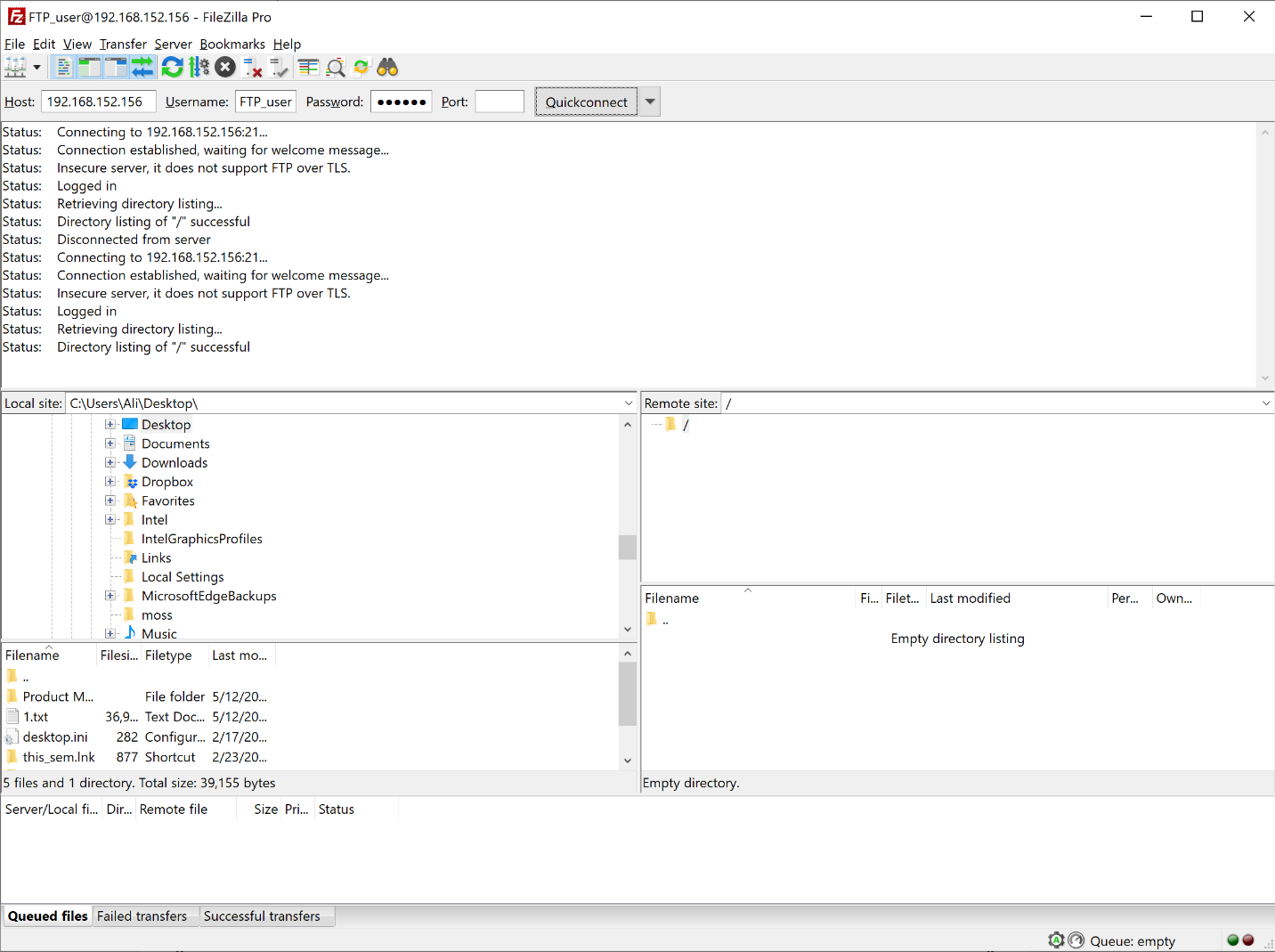
**با استفاده از یک کلاینت FTP مانند مرورگرتان یا نرم‌افزار Filezilla به سروری که بالا آوریده‌اید متصل شوید. با استفاده از نرم‌افزار Wireshark بسته‌ها را جمع‌اوری کنید. آیا می‌توانید نام کاربری و رمز عبورتان را پیدا کنید؟**

هنگام تست کردن FTP سرورمان اگر بسته‌ها را با wireshark بررسی کنیمُ می‌توانیم username و passwordمان را ببینیم:



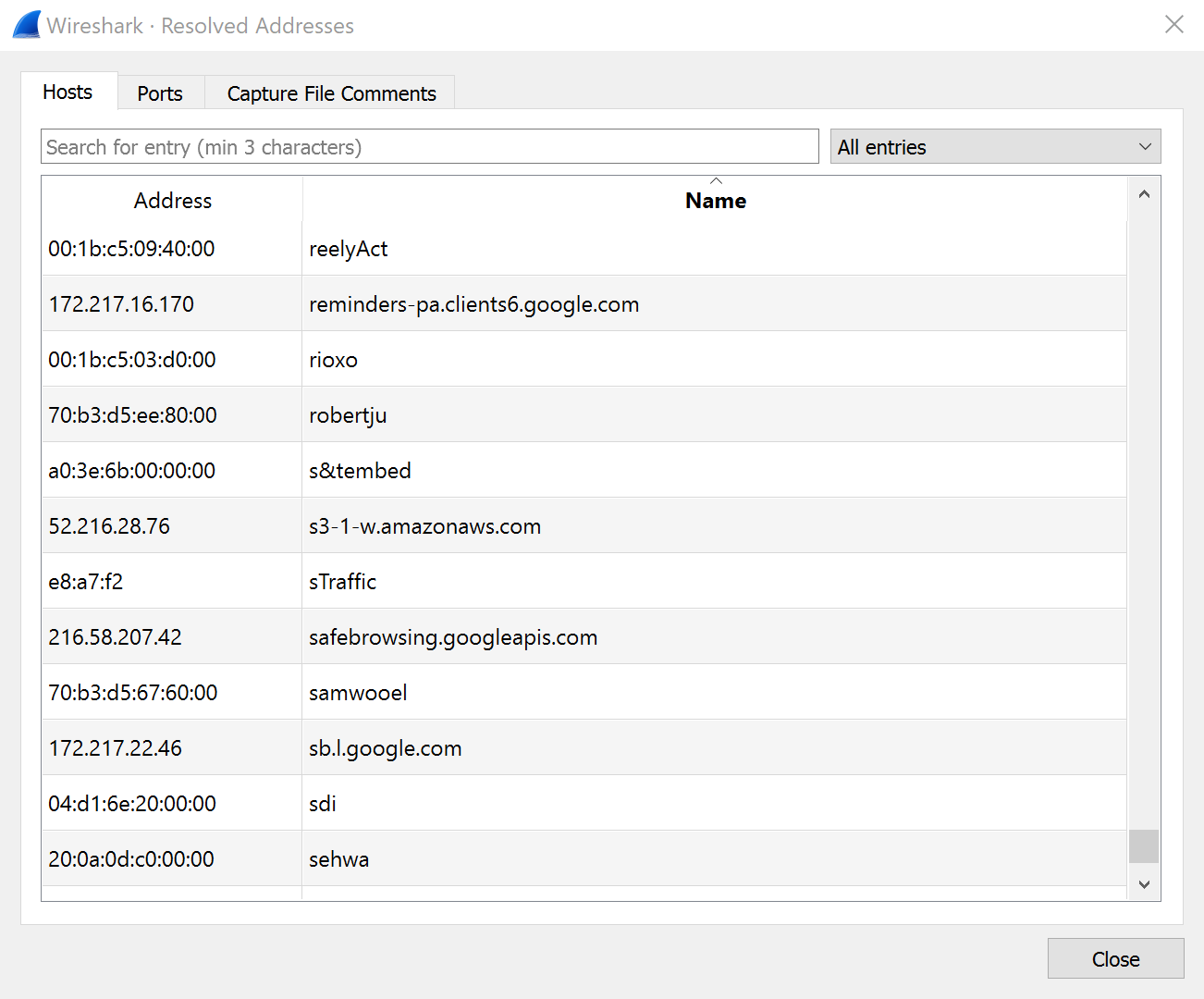
می‌بینیم که Username= FTP\_user و Password= Ali123456.

با filezilla نیز بدون مشکل به سرورمان می‌توانیم متصل شویم:



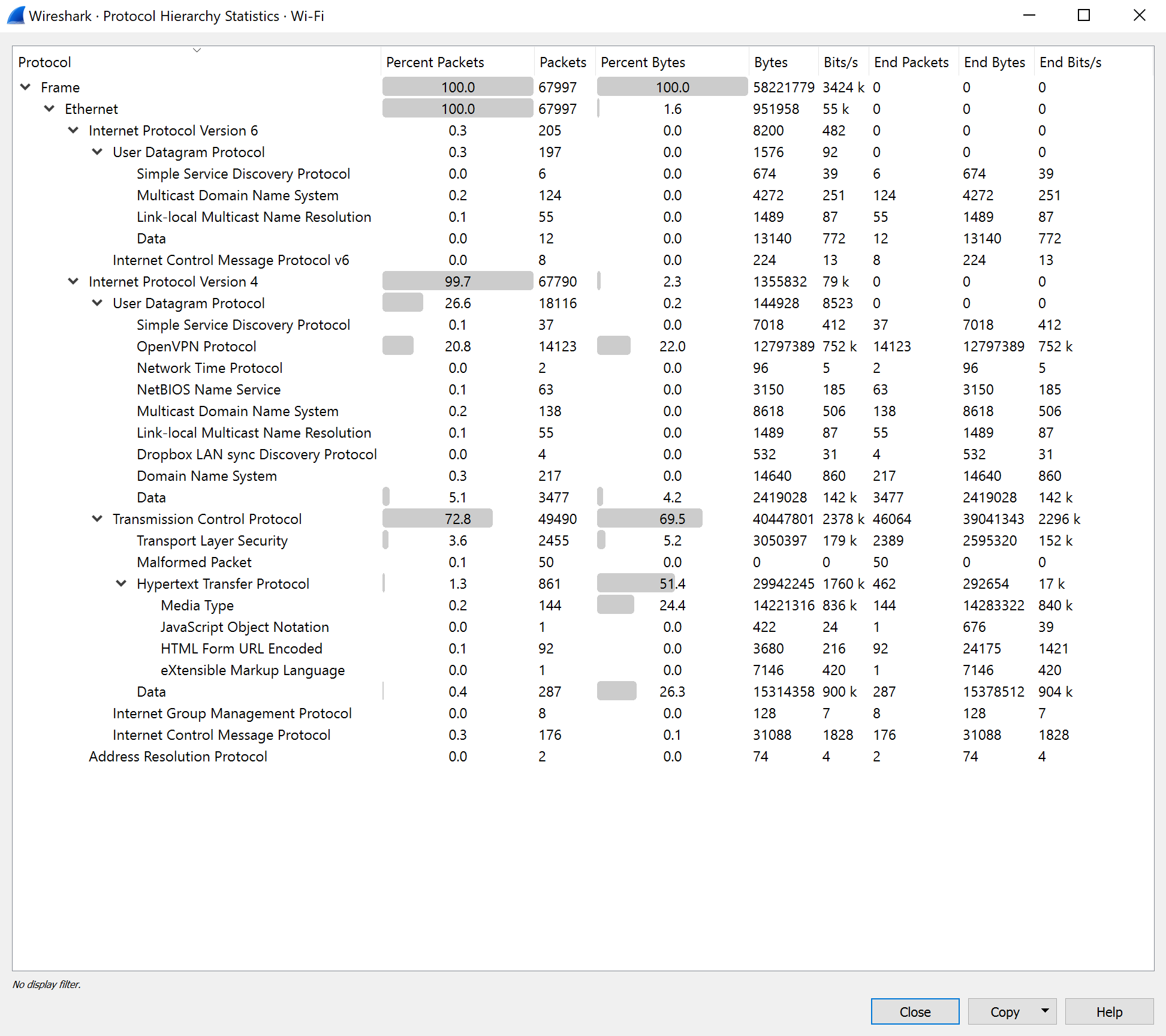
**بر روی گزینه‌ی Resolved Addresses کلیک کنید. در پنجره‌ای که باز می‌شود چه چیزی را مشاهده می‌کنید؟**

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



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

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



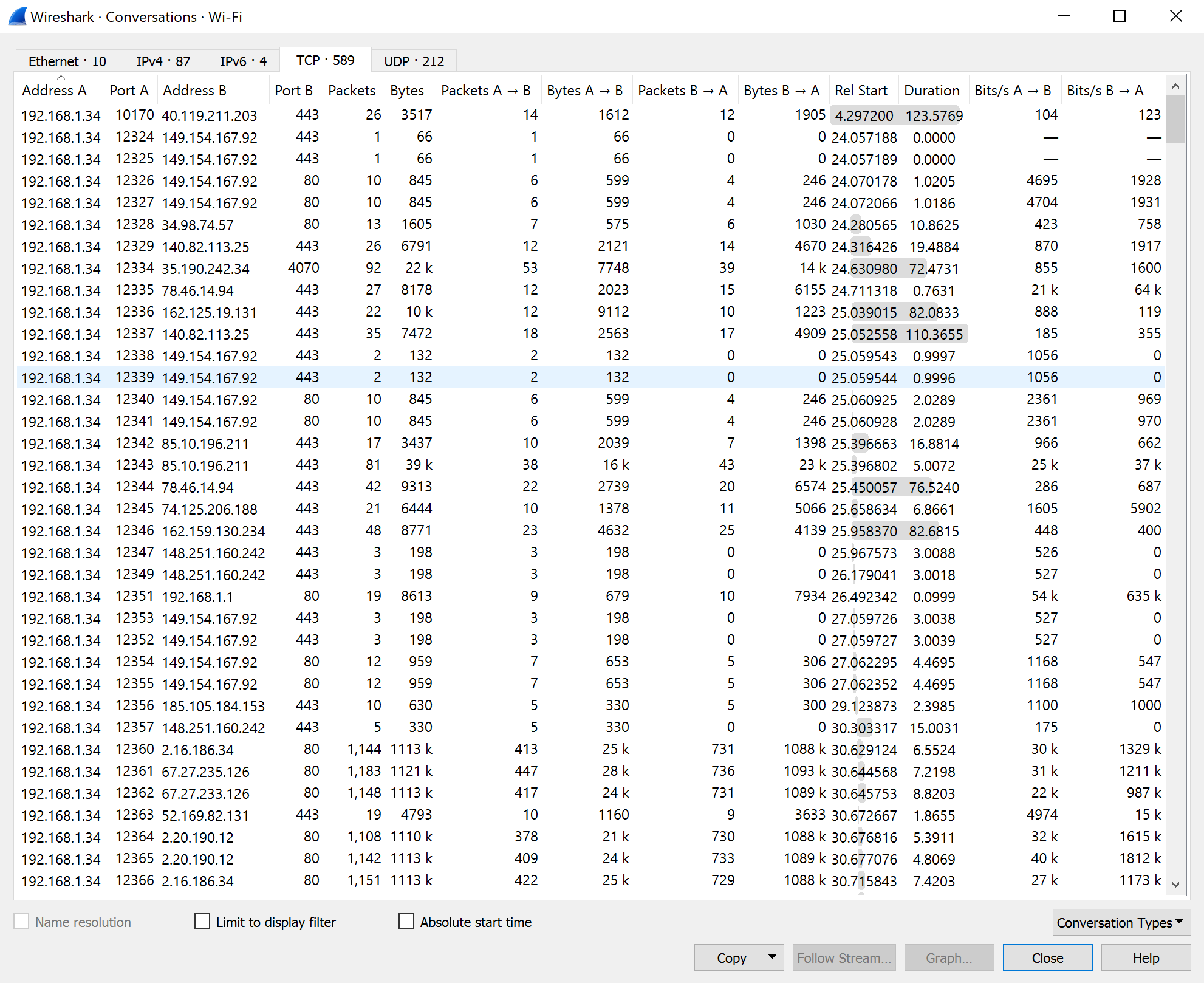
**چند درصد بسته‌های شما به یک ارتباط TCP بر روی بستر IPv4 تعلق دارند؟**

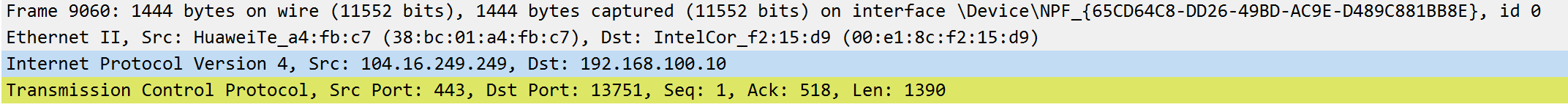
همان‌طور که در شکل نیز مشخص است 72.8 بسته‌ها از Transmission Control Protocol(TCP) برای ارتباط استفاده کرده‌اند.

**بر روی گزینه‌ی 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...



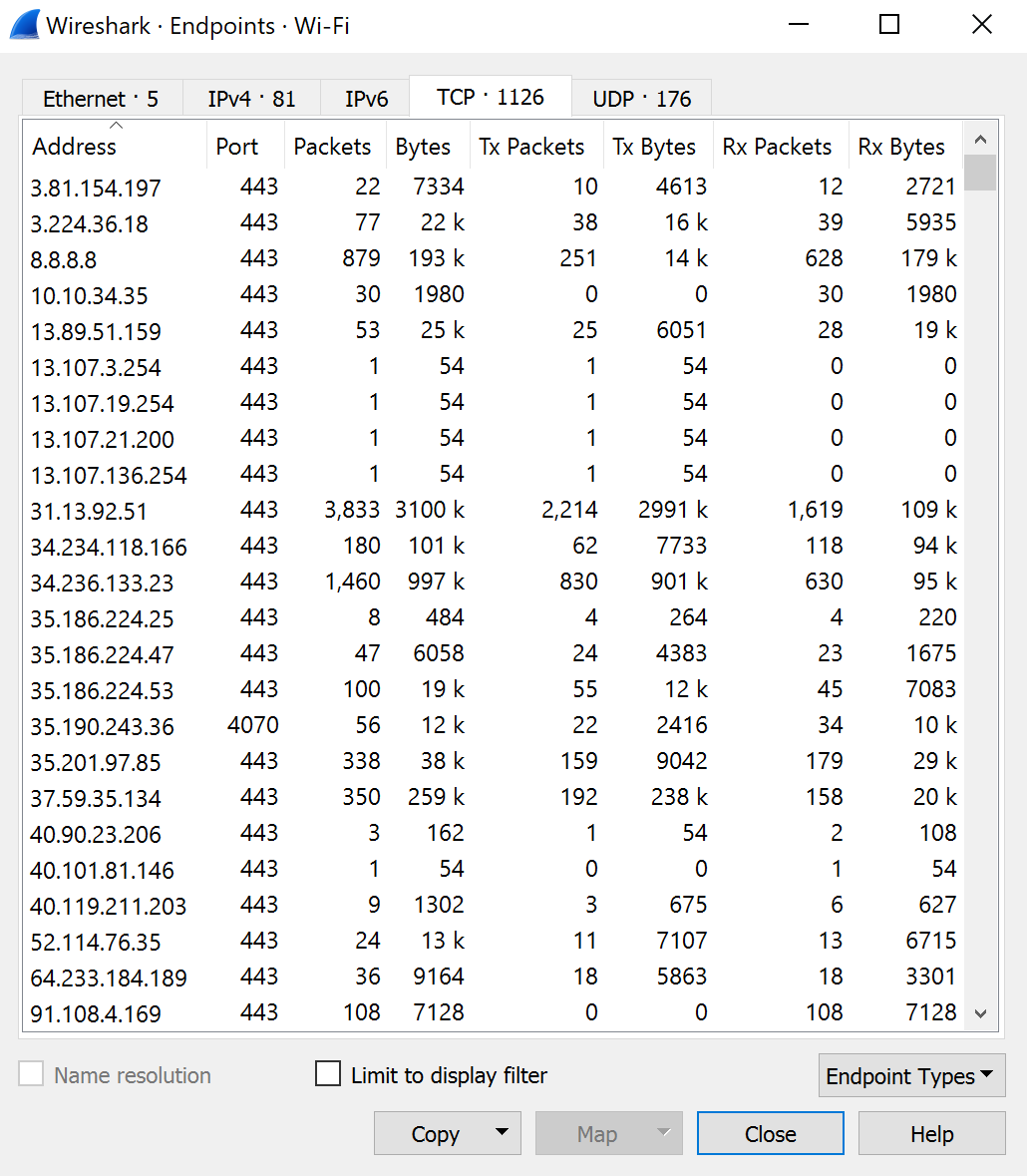
**یک نشست TCP را مشخص کنید.**

**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.

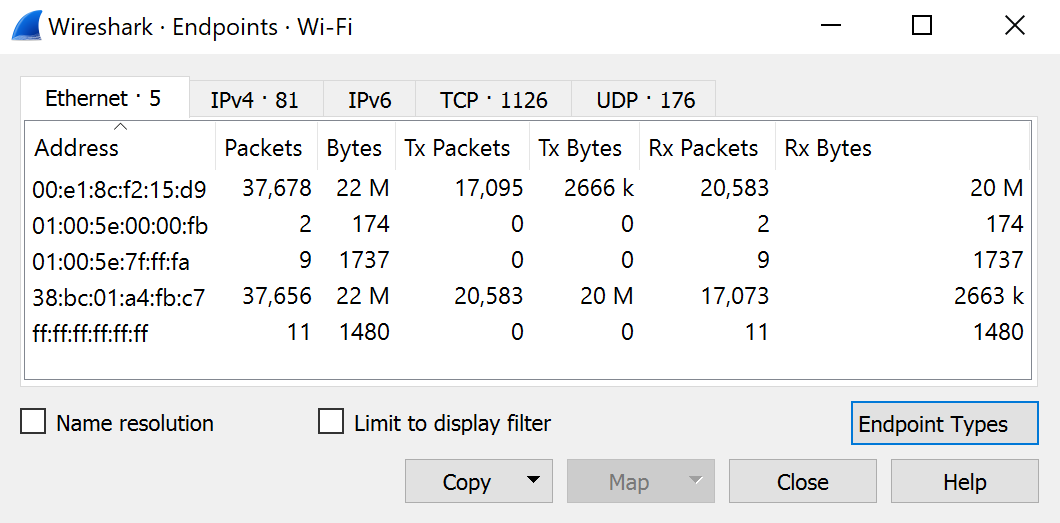
**چه مقصدهایی برای ارتباط‌های TCP در سیستم شما استفاده شده‌اند؟**

همان‌طور که می‌دانیم منظور از TX خروجی و منظور از RX ورودی است.

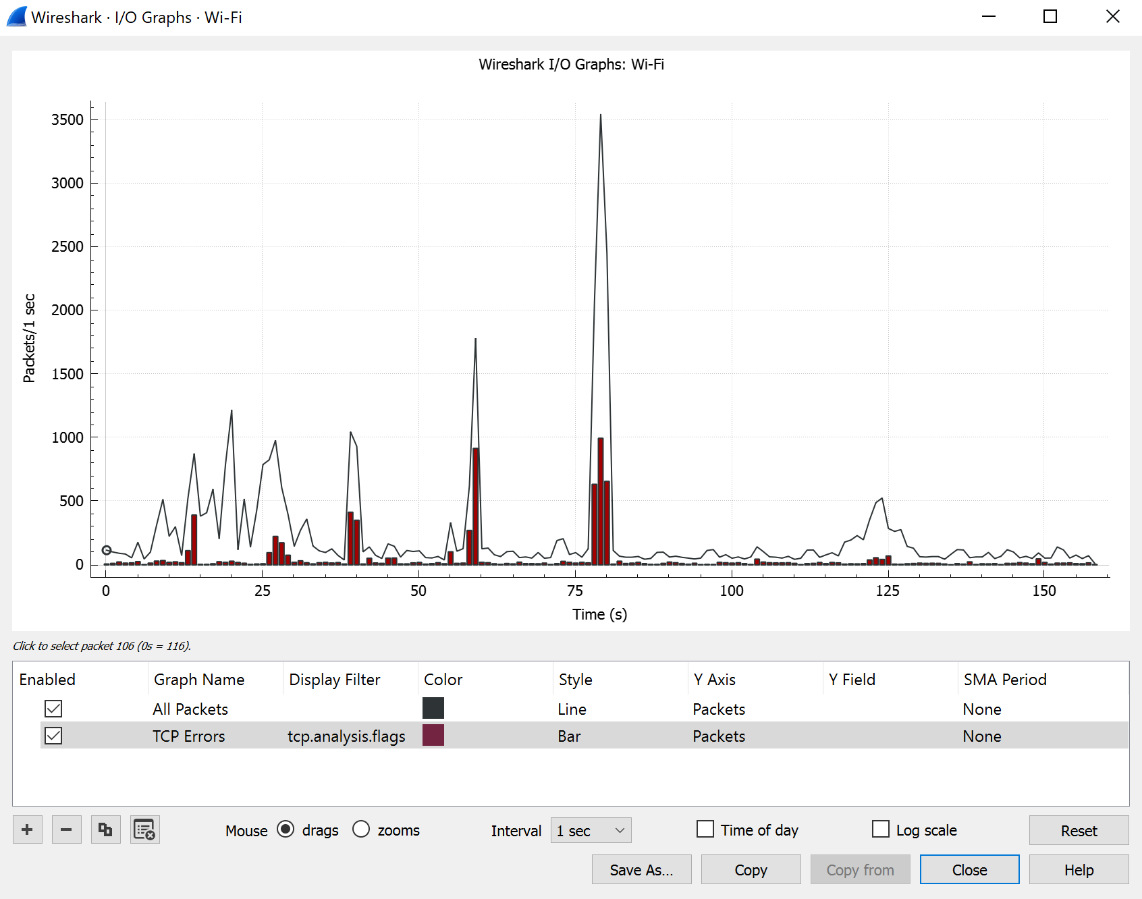


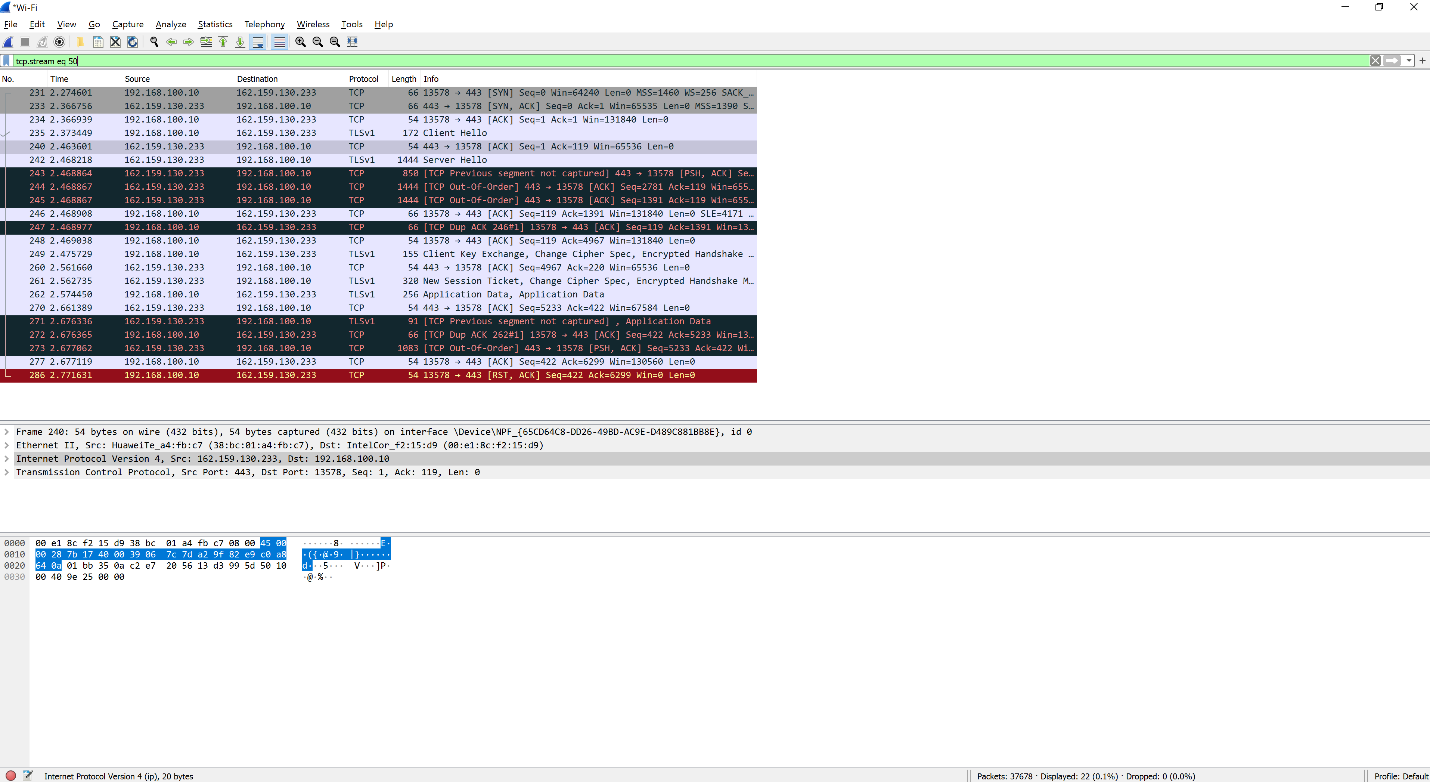
**آیا می‌توانید از زبانه Ethernet و از روی تعداد بسته‌های مبادله شده، Default Gateway شبکه خود را تشخیص دهید؟**

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



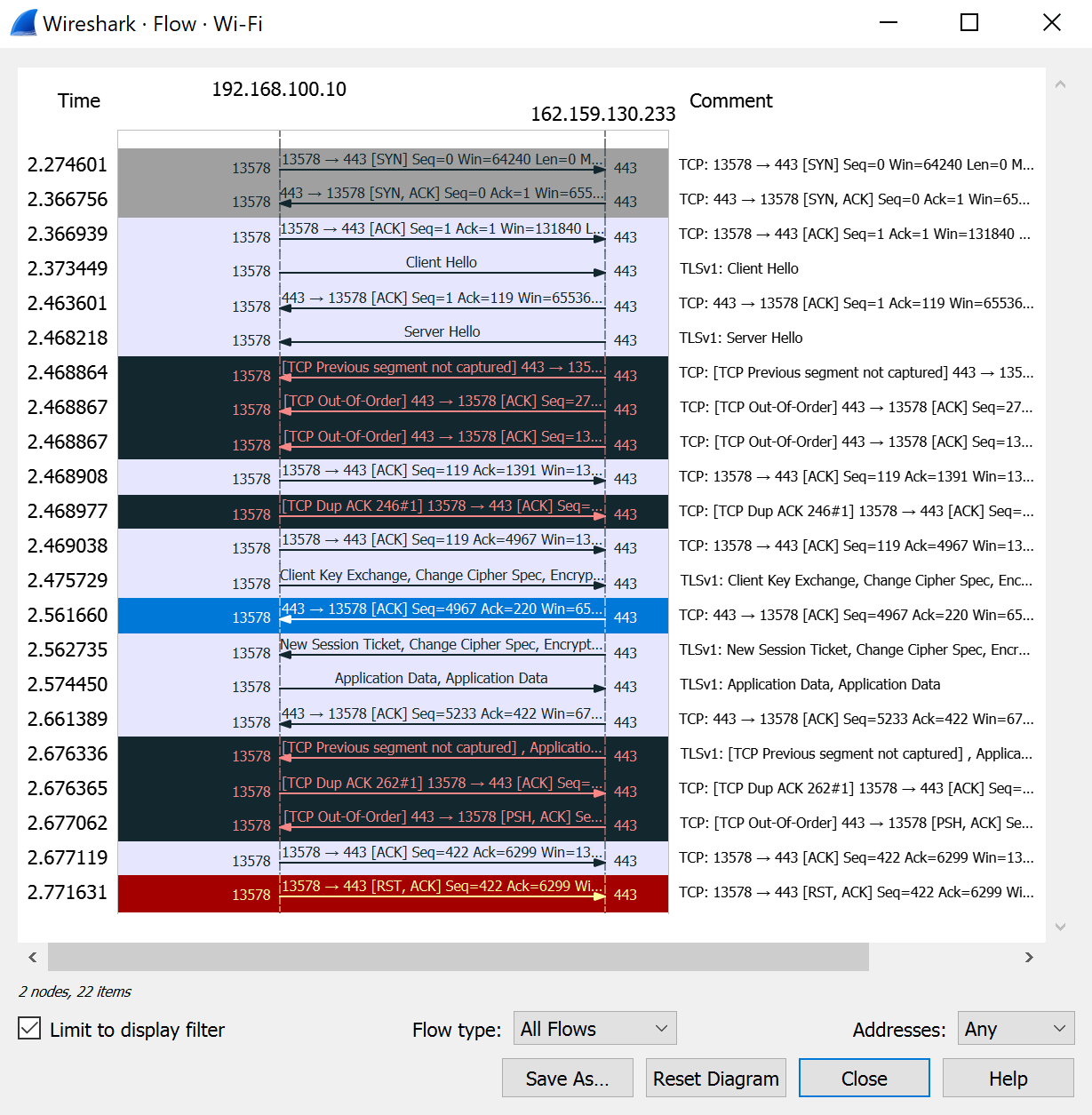
**بر روی گزینه‌ی I/O Graph کلیک کنید.**



**بسته‌های مربوط به ارتباط با یک سایت را فیلتر کنید.**

**سپس بر روی گزینه‌ی Flow Graph کلیک کنید.**

**به‌صورت کامل جزئیات مربوط به SeqNum و Ack و شماره پنجره را دنبال کنید.**

در این صفحه نیز جزئیات ارسال‌ها و گرفتن ack و... مربوط به یک ارتباط TCP و جریانی که طی می‌کند را مشاهده می‌کنیم.