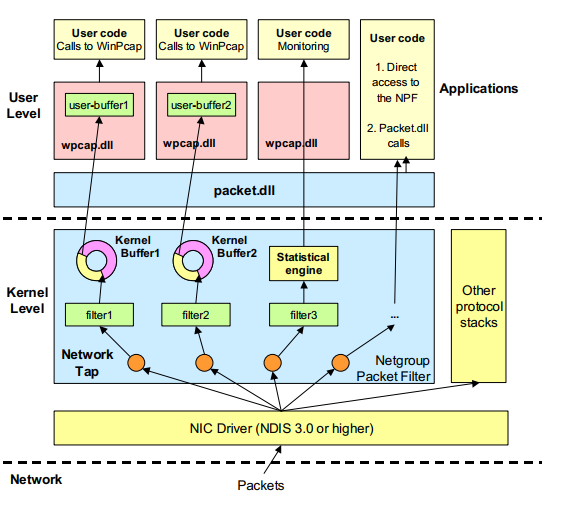
مطالب مقدماتی

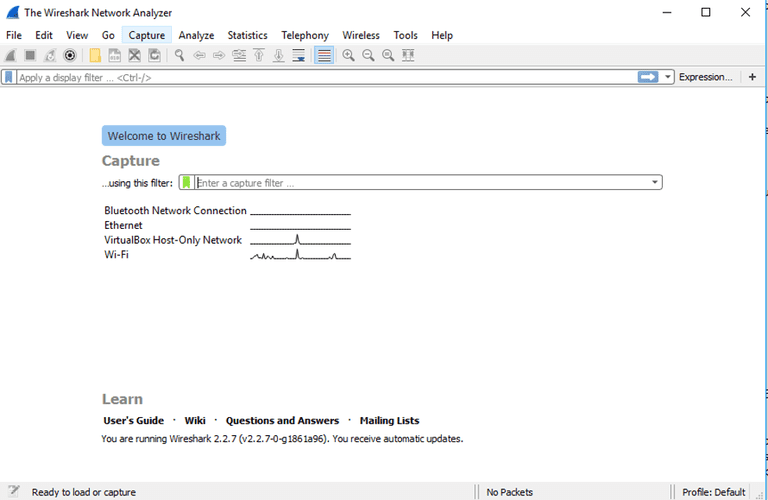
برنامه Wireshark تحلیل‌کننده پروتکل و شنود کننده ارتباط متن‌باز بر روی سیستم‌عامل‌های خانواده ویندوز و لینوکس است که به شما اجازه می‌دهید ترافیک شبکه خود را تحلیل کنید. پروژه‌ی Wireshark در سال ۱۹۹۸ با نام Ethereal توسط Gerald Combs آغاز شد. این پروژه در سال ۲۰۰۶ به Wireshark تغییر نام داد. این نرم‌افزار توسط چهارچوب Qt و با زبان C/C++ نوشته شده است. این برنامه قادر به تحلیل برخط بیش از 1000 پروتکل در نسخه 1.10.6 است. همچنین قادر به خواندن اطلاعات خروجی انواع برنامه‌های شنود و تحلیل دیگر مانند TCPdump، Microsoft Network Monitor است. خروجی این برنامه می‌تواند به‌صورت XML،CSV،PostScript یا Plaintext باشد.

در سیستم‌عامل خانواده ویندوز، برنامه Wireshark شنود بسته‌ها با استفاده از کتابخانه‌ Winpcap انجام می‌دهد. معماری نرم‌افزار Winpcap در ‏شکل زیر نمایش داده شده است. همان‌گونه که در این شکل مشخص است، برنامه Winpcap از دو بافر یکی در سطح کرنل و دیگری در سطح کاربر، یک ماشین فیلتر کننده که فیلترهایی را به بسته‌ها اعمال می‌کند و همچنین دو فایل wpcap.dll و packet.dll که اینتفریس‌های این برنامه را ارائه می‌کنند تشکیل شده است.

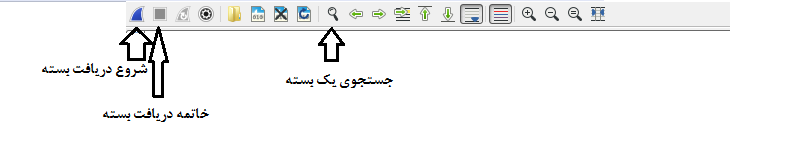
در ابتدا کاربر می‌تواند فیلترهایی را مشخص کند که این فیلترها توسط Netgroup Packet Filter(NPF) به دستوراتی ترجمه می‌شوند که توسط فیلترها بر روی بسته‌ها اعمال می‌شوند. به عنوان مثال کاربر می‌تواند یک فیلتر را به صورت «صرفا بسته‌های پروتکل UDP دریافت شوند» تعریف کند. بسته‌ها پس از اینکه توسط گرداننده شبکه، از واسط شبکه خوانده شدند جمع‌آوری می‌شوند؛ بنابراین کارایی Winpcap وابسته به گرداننده شبکه است. همچنین مشخص است که صرفا یک کپی از بسته‌ها توسط Winpcap دریافت می‌شود و بسته‌ها هم‌زمان می‌توانند پشته پروتکلی سیستم‌عامل که در شکل با نام Other protocol stack مشخص شده است را طی کنند.



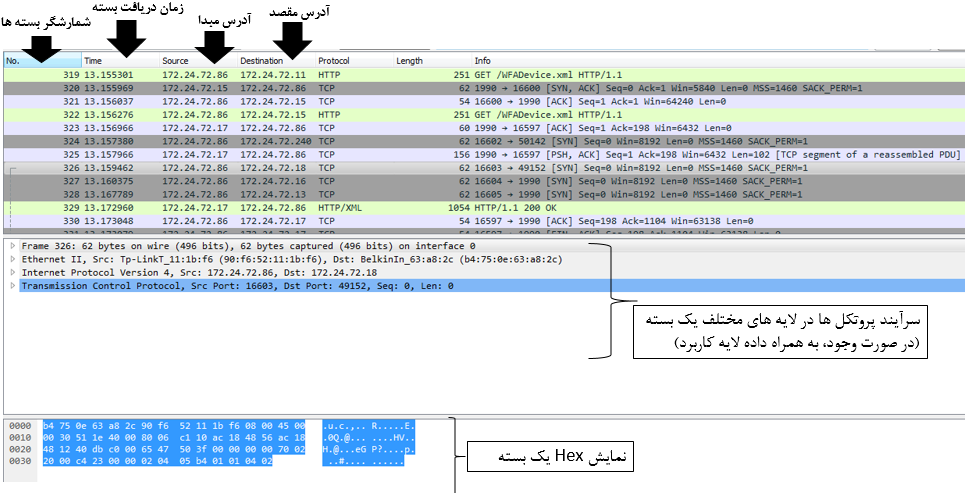
برای کار با برنامه Wireshark ابتدا باید واسط شبکه‌ای که قرار است بسته‌ها از آن دریافت شوند مشخص شود. پس از باز کردن برنامه صفحه‌ای مشابه ‏شکل زیر نمایش داده می‌شود.



واسط شبکه‌ای که به اینترنت متصل است را انتخاب کنید. در ادامه برنامه شروع به دریافت بسته‌ها از کارت شبکه می‌کند. معمولا هر سطر یک بسته را نشان می‌دهد. همان‌گونه که مشاهده می‌کنید بسته‌ها با رنگ‌های مختلف نمایش داده شده‌اند. قوانین رنگ گذاری Wireshark از بخش View->Coloring rules قابل دسترس است. اجزای مختلف منوی ابزار Wireshark در ‏شکل زیر نمایش داده شده است.



هر زمان که خواستید می‌توانید با استفاده از کلیدهای CTRL+E یا دکمه قرمز رنگ در نوار ابزار، شنود بسته‌ها را متوقف کنید. با دوباره فشردن CTRL+E، Wireshark دوباره شروع به شنود بسته‌ها می‌کند. همچنین این کار می‌تواند با استفاده از دکمه آبی رنگ در نوار ابزار نیز انجام شود. در نوار وضعیت نیز می‌توانید تعداد بسته‌های دریافت شده را مشاهده کنید. بخش‌های مهم محیط اصلی Wireshark در ‏شکل زیر نمایش داده شده است.



شنود محتوای بسته‌های FTP

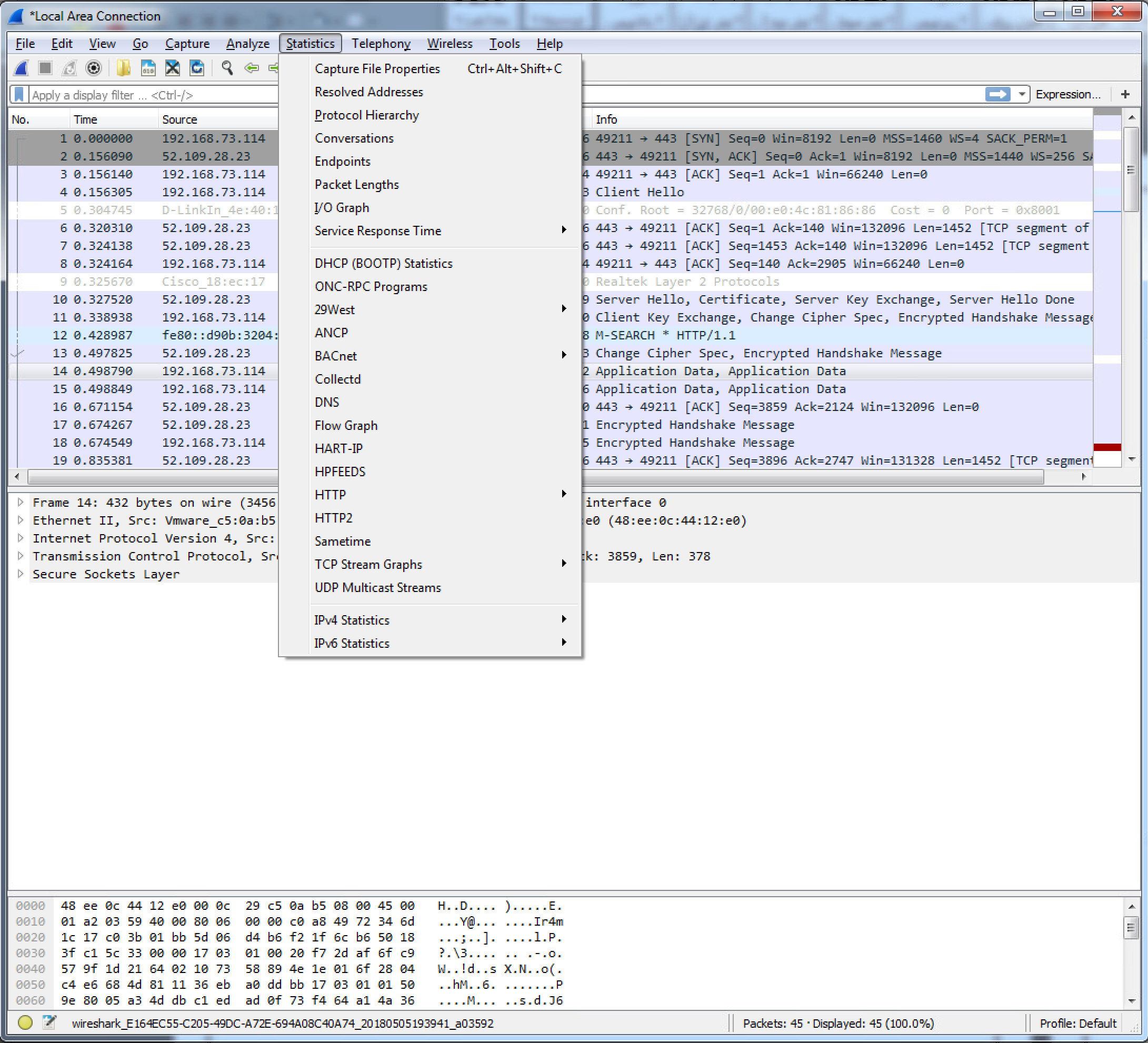
پروتکل FTP یک پروتکل ساده در جهت انتقال فایل می‌باشد. این پروتکل محتوای خود را بدون رمزنگاری و به صورت متنی منتقل می‌کند. در این قسمت قصد داریم با شنود بسته‌های FTP نام کاربری و رمز عبور کاربران را بدست بیاوریم. برای این منظور در اولین گام نیاز است یک سرور FTP را راه‌اندازی کنیم. برای این منظور می‌توانید از ویندوز سرور استفاده کنید. در پیوست تمرین ویدیو نصب ویندوز سرور روی VMWare آمده است. بعد از نصب سرویس FTP را راه‌اندازی کنید.

چگونگی نصب و راه‌اندازی سرویس FTP را گزارش کنید.

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؟

کار با منو Analyze

نرم‌افزار wireshark را باز کرده، چند دقیقه به وب گردی بپردازید و بسته‌ها را جمع‌آوری کنید. سپس مطابق جمع‌آوری بسته را متوقف کرده و از منوی بالا بر روی گزینه‌ی Statistics کلیک کنید. در ادامه قصد داریم مواردی که در این زبانه وجود دارند را بررسی کنیم.



1. بر روی گزینه‌ی Resolved Addresses کلیک کنید.

در پنجره‌ای که باز می‌شود چه چیزی را مشاهده می‌کنید؟

1. بر روی گزینه‌ی protocol hierarchy کلیک کنید.

در پنجره‌ای که باز می‌شود چه چیزی را مشاهده می‌کنید؟

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

1. بر روی گزینه‌ی Conversations کلیک کنید.

در پنجره‌ای که باز می‌شود چه چیزی را مشاهده می‌کنید؟

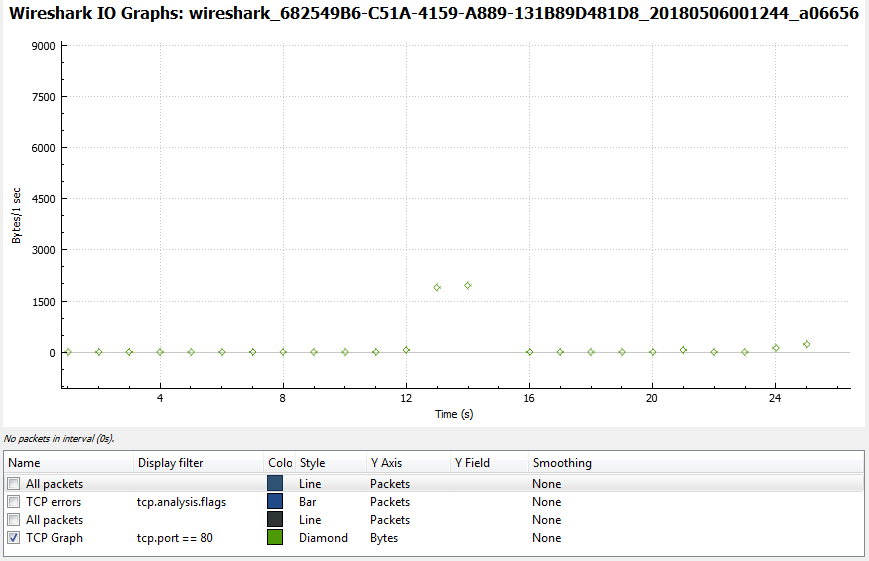
1. یک نشست TCP را مشخص کنید. (برای مشخص کردن یک نشست TCP نیاز است که آدرس و پورت مبدا و مقصد را مشخص کنید.) توجه داشته باشید مفهومی که Wireshark از نشست برداشت می‌کند با مفهومی که در کلاس آموخته‌اید تفاوت دارد.
2. بر روی گزینه‌ی endpoints کلیک کنید.

در پنجره‌ای که باز می‌شود چه چیزی را مشاهده می‌کنید؟

چه مقصدهایی برای ارتباط‌های TCP در سیستم شما استفاده شده‌اند؟

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

1. بر روی گزینه‌ی I/O Graph کلیک کنید. در پنجره‌ای که باز می‌شود می‌توانید نرخ I/O‌ را مشاهده کنید. شما می‌توانید در این صفحه نمودارهای مختلفی بسازید. بر روی دکمه + در پایین پنجره باز شده کلیک کنید، سپس یک فیلتر به آن اضافه کنید تا نمودار تعداد بسته‌ها در ثانیه را مشاهده کنید. مشاهده می‌کنید که با کلیک بر روی نمودار، بسته‌ها در پنجره اصلی مشخص خواهند شد.



1. بسته‌های مربوط به ارتباط با یک سایت را فیلتر کنید (با استفاده از Follow TCP Stream). سپس بر روی گزینه‌ی Flow Graph کلیک کنید. از منوی پایین، در بخش Show، Displayed packets را انتخاب کنید. به‌صورت کامل جزئیات مربوط به SeqNum و Ack و شماره پنجره را دنبال کنید و آن‌ها را توضیح دهید.