



دانشگاه مهندسی کامپیوتر
و فناوری اطلاعات



بسمه تعالی

دانشگاه صنعتی امیرکبیر (پلی تکنیک تهران)

دانشگاه مهندسی کامپیوتر و فناوری اطلاعات



دانشگاه صنعتی امیرکبیر
(پلی تکنیک تهران)

نمره

مسئله

درس شبکه های کامپیوتری، نیم سال دوم سال تحصیلی ۹۸-۹۹

تمرین علمی سری دوم (تاریخ ۱۳۹۹/۰۲/۱۶، موعده تحویل: ۱۳۹۹/۰۲/۲۸)

نام و نام خانوادگی:

شماره دانشجویی:

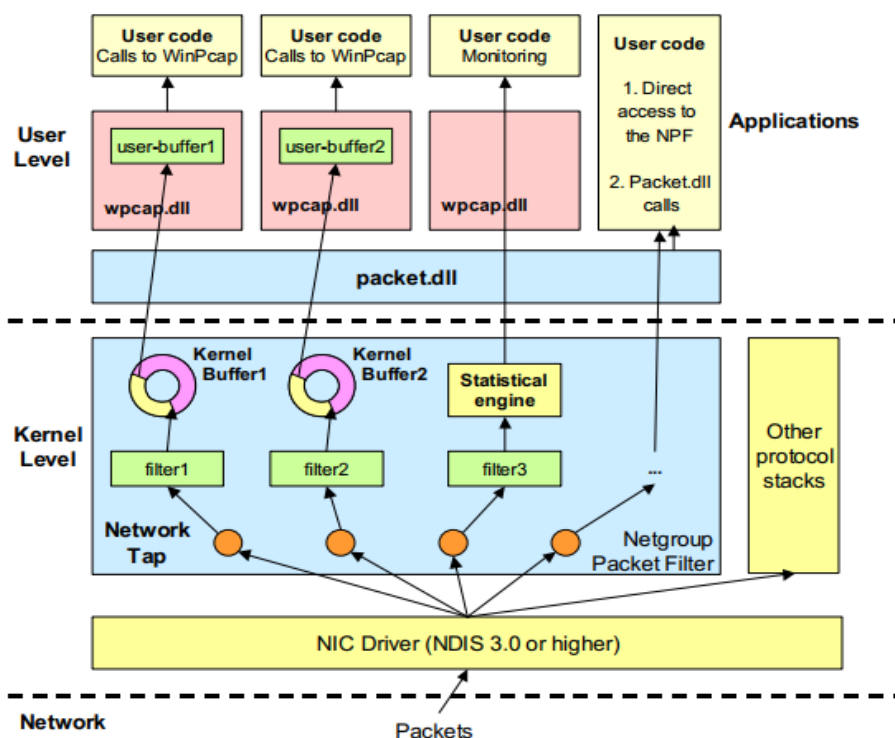
نمره:

مطالب مقدماتی

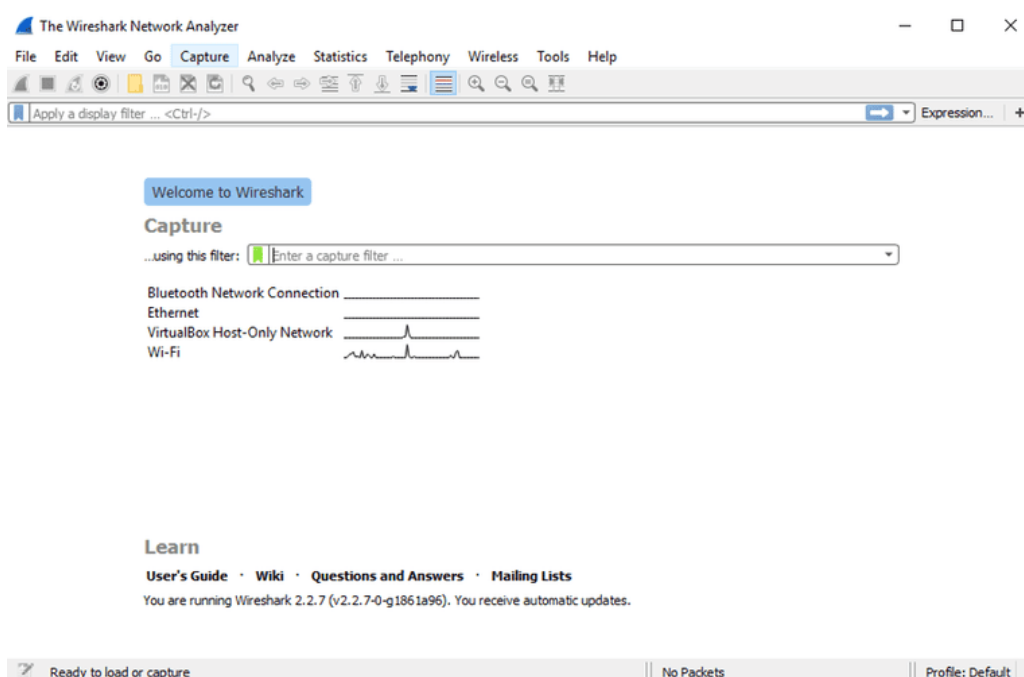
برنامه Wireshark تحلیل کننده پروتکل و شنود کننده ارتباط متن باز بر روی سیستم عامل های خانواده ویندوز و لینوکس است که به شما اجازه می دهد ترافیک شبکه خود را تحلیل کنید. پروژه های Wireshark در سال ۱۹۹۸ با نام Ethereal توسط Gerald Combs آغاز شد. این پروژه در سال ۲۰۰۶ به Wireshark تغییر نام داد. این نرم افزار توسط چهارچوب Qt و با زبان ++C/C نوشته شده است. این برنامه قادر به تحلیل برخط بیش از ۱۰۰۰ پروتکل در نسخه ۱.۱۰.۶ است. همچنین قادر به خواندن اطلاعات خروجی انواع برنامه های شنود و تحلیل دیگر مانند TCPdump، Microsoft Network Monitor است. خروجی این برنامه می تواند به صورت XML، CSV، PostScript یا Plaintext باشد.

در سیستم عامل خانواده ویندوز، برنامه Wireshark شنود بسته ها با استفاده از کتابخانه Winpcap انجام می دهد. معماری نرم افزار Winpcap در شکل زیر نمایش داده شده است. همان گونه 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 بسته ها اعمال می کند و همچنین دو فایل wpcap.dll و packet.dll که اینترفیس های این برنامه را ارائه می کنند تشکیل شده است.

در ابتدا کاربر می تواند فیلترهایی را مشخص کند که این فیلترها توسط Netgroup Packet Filter (NPF) به دستوراتی ترجمه می شوند که توسط فیلترها بر روی بسته ها اعمال می شوند. به عنوان مثال کاربر می تواند یک فیلتر را به صورت «صرفا بسته های پروتکل UDP دریافت شوند» تعریف کند. بسته ها پس از اینکه توسط گرداننده شبکه، از واسط شبکه خوانده شدند جمع آوری می شوند؛ بنابراین کارایی Winpcap وابسته به گرداننده شبکه است. همچنین مشخص است که صرفا یک کپی از بسته ها توسط Winpcap دریافت می شود و بسته ها هم زمان می توانند پشته پروتکلی سیستم عامل 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.

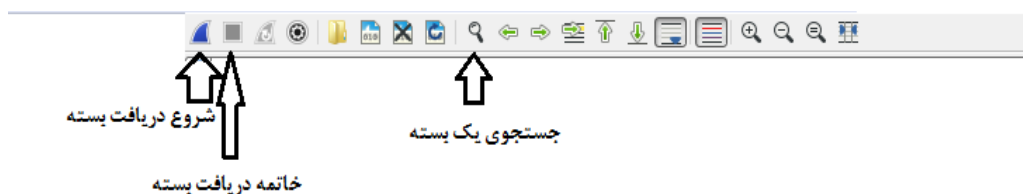


درس شبکه‌های کامپیوتری، نیم سال دوم تحصیلی ۹۸-۹۹

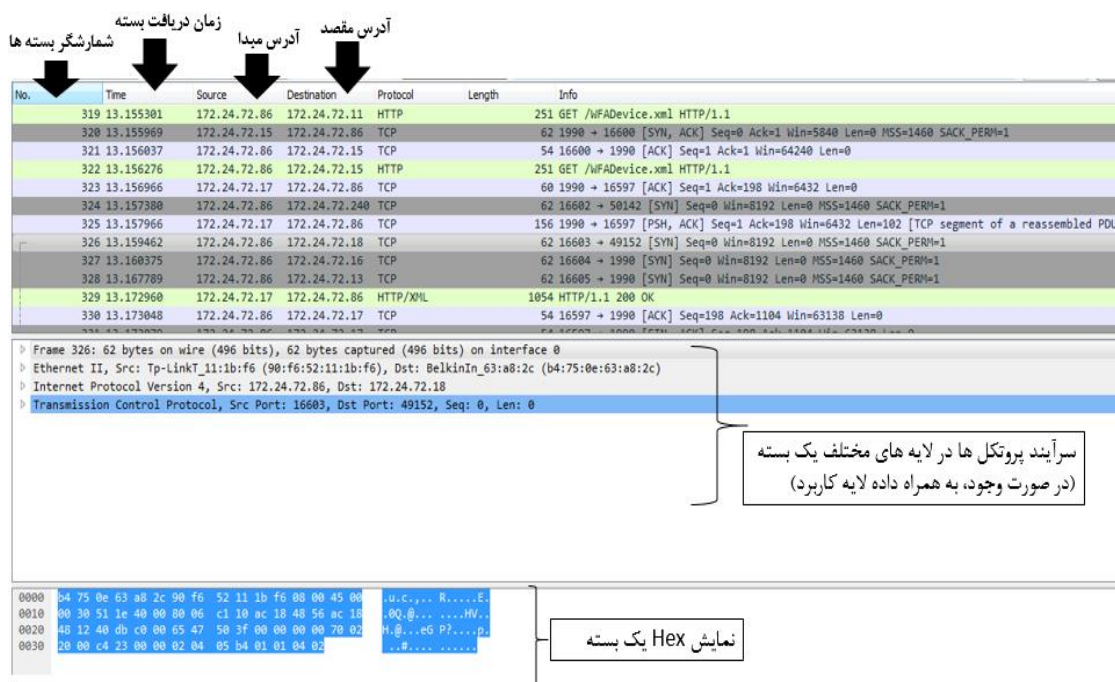
تمرین عملی سری دوم (موعد تحویل: ۱۳۹۹/۰۲/۲۸)

صفحه: 3 از 5

واسط شبکه‌ای که به اینترنت متصل است را انتخاب کنید. در ادامه برنامه شروع به دریافت بسته‌ها از کارت شبکه می‌کند. معمولاً 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، شهود بسته‌ها را متوقف کنید. با دوباره فشردن CTRL+E، Wireshark دوباره شروع به شهود 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.



شهود 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 شهود 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 مرورگر یا نرم‌افزار Filezilla به سروری که بالا آورده‌اید متصل شوید. با استفاده از نرم‌افزار Wireshark بسته‌ها را جمع‌آوری کنید. آیا می‌توانید نام کاربری و رمز عبورتان را پیدا کنید؟



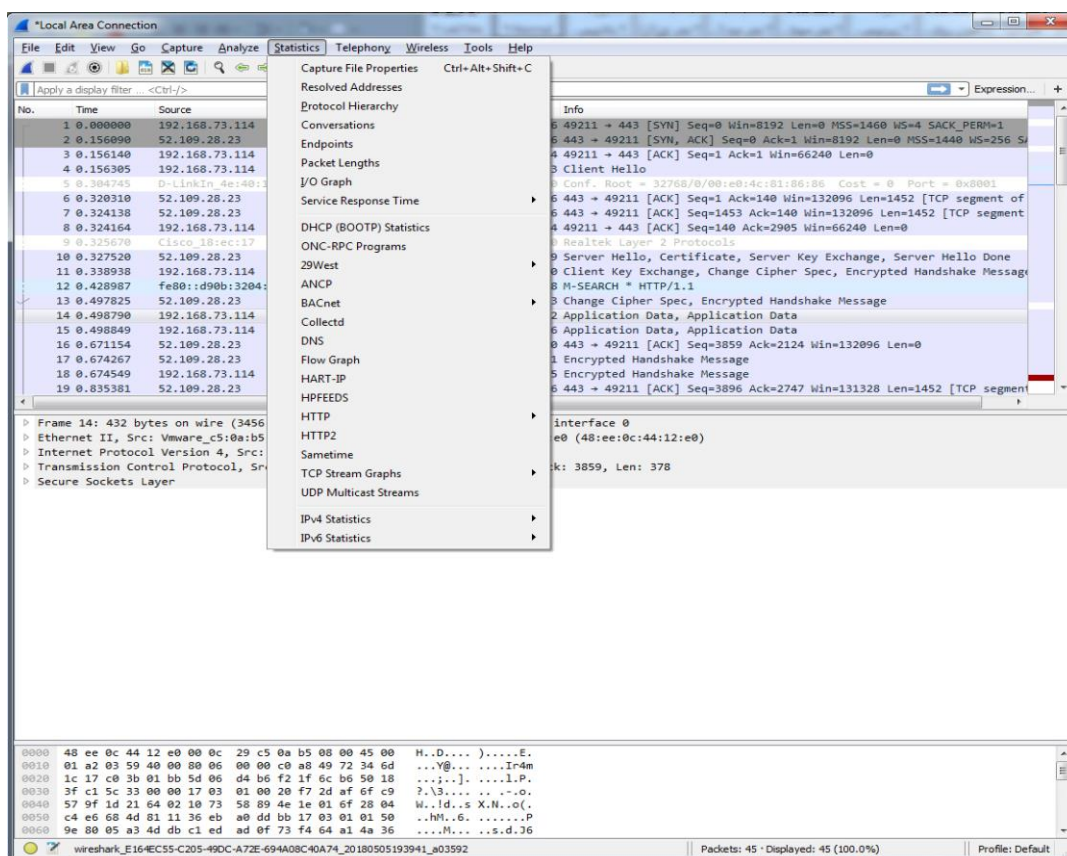
درس شبکه‌های کامپیوتری، نیم سال دوم تحصیلی ۹۹-۹۸

تمرین عملی سری دوم (موعد تحویل: ۱۳۹۹/۰۲/۲۸)

صفحه: 4 از 5

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 گزینه Statistics کلیک کنید. در ادامه قصد داریم مواردی که در این زبانه وجود دارند را بررسی کنیم.



1. بر روی گزینه Resolved Addresses کلیک کنید.

در پنجره‌ای که باز می‌شود چه چیزی را مشاهده می‌کنید؟

2. بر روی گزینه 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 IP4 تعلق دارند؟

3. بر روی گزینه Conversations کلیک کنید.

در پنجره‌ای که باز می‌شود چه چیزی را مشاهده می‌کنید؟

4. 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.

5. بر روی گزینه endpoints کلیک کنید.

درس شبکه‌های کامپیوتری، نیم سال دوم تحصیلی ۹۸-۹۹

تمرین عملی سری دوم (موعد تحویل: ۱۳۹۹/۰۲/۲۸)

صفحه: 5 از 5

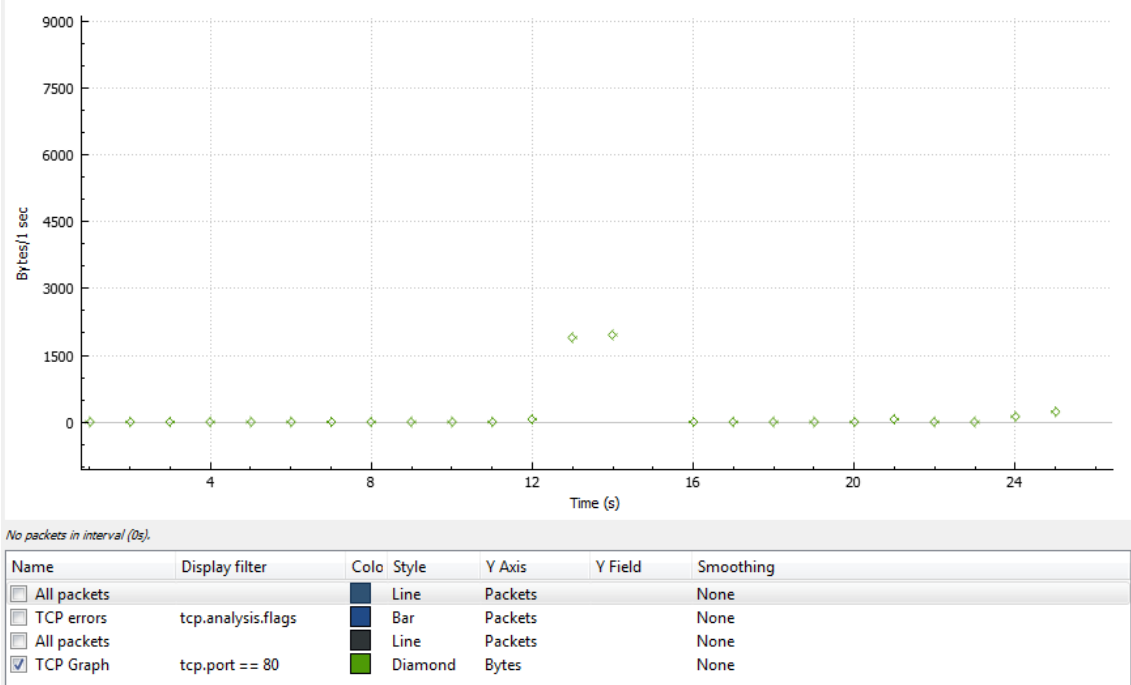
در پنجره‌ای که باز می‌شود چه چیزی را مشاهده می‌کنید؟

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؟

6. 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.

Wireshark IO Graphs: wireshark_682549B6-C51A-4159-A889-131B89D481D8_20180506001244_a06656



7. 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. به صورت کامل جزئیات مربوط به SeqNum و Ack و شماره پنجره را دنبال کنید و آن‌ها را توضیح دهید.