۳ - آشنایی با نرم‌افزارWireshark

۳-۱ - هدف آزمایش

در این آزمایش با نرم‌افزار Wireshark آشنا می‌شویم تا بتوانیم با کمک این ابزار، ترافیک شبکه را ضبط، تحلیل و پروتکل‌های مختلف را در لایه‌های گوناگون شناسایی کنیم.

۳-۲ - قطعات و ابزارهای موردنیاز

- نرم‌افزار Wireshark نسخه ۲ به بعد
- سیستم‌عامل ویندوز ۷ به بعد
- دسترسی به اینترنت

۳-۳ - مطالب مقدماتی

نرم‌افزار Wireshark یک تحلیلگر بسته‌های شبکه است که امکان مشاهده و بررسی ترافیک شبکه در سیستم‌عامل‌های ویندوز و لینوکس را به کاربران می‌دهد. این نرم‌افزار در سال ۱۹۹۸ با نام Ethereal توسط Gerald Combs آغاز شد و در سال ۲۰۰۶ به Wireshark تغییر نام داد. این ابزار با استفاده از چارچوب Qt و به زبان‌های C/C++ توسعه یافته و قادر به تحلیل آنلاین بیش از ۱۰۰۰ پروتکل در نسخه‌های مختلف خود می‌باشد. همچنین این برنامه می‌تواند اطلاعات خروجی از ابزارهایی مانند، TCPdumpو Microsoft Network Monitor را خوانده و در فرمت‌هایXML ، CSV، PostScriptیا Plaintext ذخیره کند.

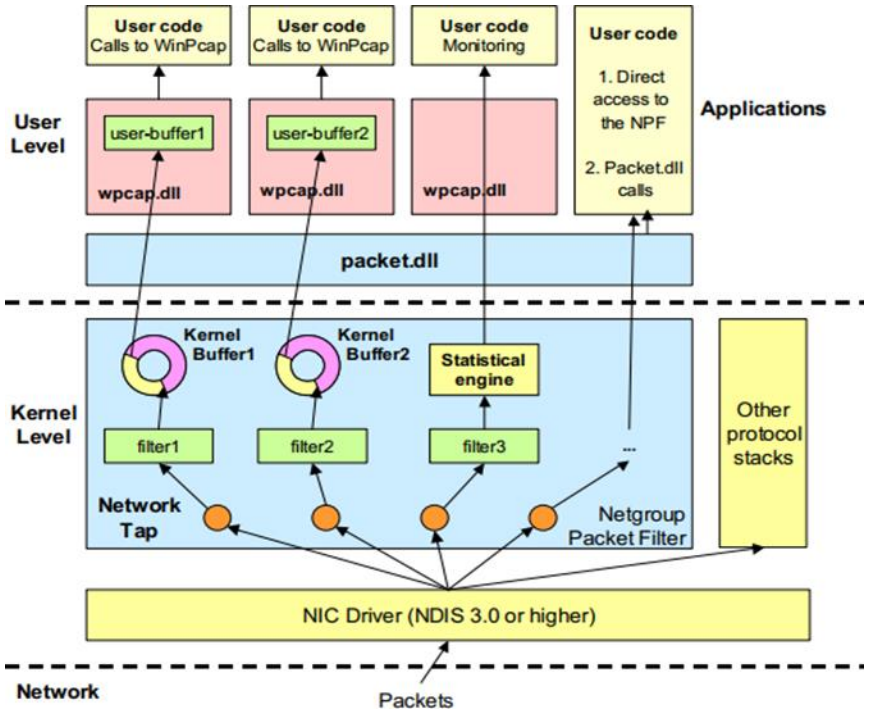
اسنیفر (Sniffer) ابزاری است که ترافیک شبکه را به صورت زنده دریافت و تحلیل می‌کند. به کمک اسنیفر، می‌توان بسته‌های ارسالی و دریافتی در شبکه را ضبط کرده و جزئیات پروتکل‌ها و داده‌ها را بررسی نمود. نرم‌افزار Wireshark به عنوان یک اسنیفر پیشرفته، امکان بررسی دقیق و تحلیل عمیق ترافیک شبکه را فراهم می‌آورد.

در سیستم‌عامل ویندوز، Wiresharkاز کتابخانه دریافت بسته (WinPcap) برای کار با ترافیک شبکه استفاده می‌کند. معماری WinPcapشامل دو بخش اصلی است(در تصویر ۱-۱ معماری کلی آن را مشاهده می‌کنید.):

- بافرهای کرنل و کاربر: برای ذخیره و مدیریت داده‌های دریافت شده از شبکه.
- ماشین فیلترکننده: که فیلترهایی را به بسته‌های دریافتی اعمال می‌کند. همچنین، فایل‌های wpcap.dll و packet.dllبه عنوان رابط‌های نرم‌افزاری بین Wireshark و WinPcap عمل می‌کنند تا دسترسی به بسته‌های شبکه فراهم شود.

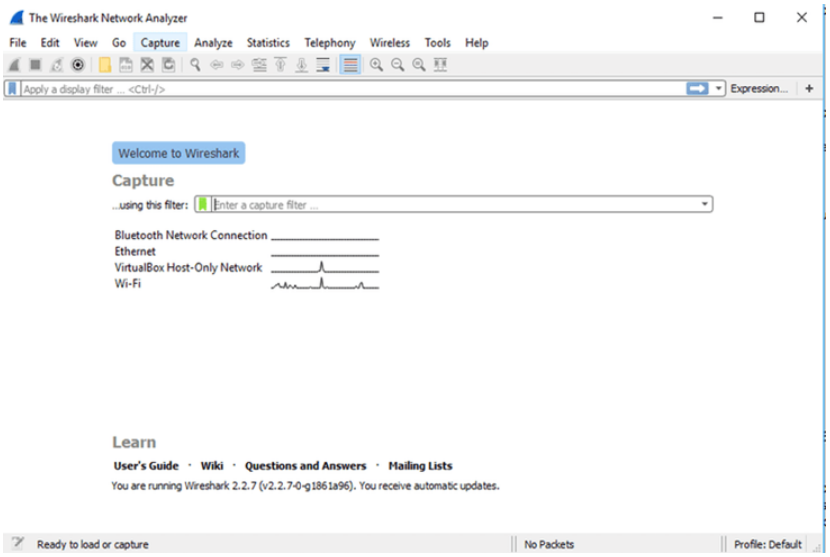
کاربر می‌تواند با استفاده از ابزارهای فیلترینگ ارائه‌شده توسطWinPcap ، بسته‌های مورد نظر را از میان ترافیک کلی شبکه انتخاب کند. به عنوان مثال، با تعریف یک فیلتر از طریق(Packet Netgroup Filter (NPF ، می‌توان بسته‌های مربوط به پروتکل UDPیا سایر پروتکل‌ها را انتخاب و دریافت نمود WinPcap .به صورت خودکار یک کپی از بسته‌های دریافت شده تهیه می‌کند

و این بسته‌ها پس از پردازش، به سایر لایه‌های پروتکل‌های موجود در سیستم‌عامل نیز ارسال می‌شوند. این فرآیند تضمین می‌کند که تحلیل ترافیک شبکه با دقت و کارایی بالایی انجام شود.



تصویر ۱- ۱) معماری نرم‌افزار wireshark

برای شروع ابتدا واسط شبکه‌ای که قصد بررسی بسته‌های آن را داریم، مشخص می‌کنیم. همان‌طور که در تصویر زیر (۱-۲) مشاهده می‌کنید چهار واسط وجود دارد که بسته به سیستم شما ممکن است تعداد آن‌ها متفاوت باشد (توجه داشته باشید که واسط شبکه انتخابی شما باید به اینترنت متصل باشد.).



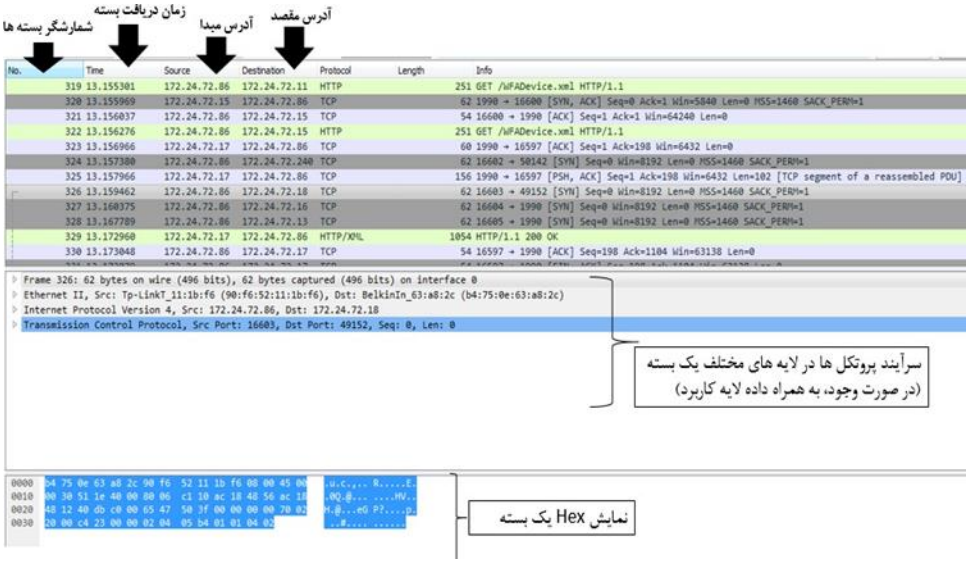
تصویر ۱- ۲) صفحه اولیه و انتخاب واسط شبکه در نرم‌افزار wireshark

حال پس از انتخاب واسط شبکه عملیات شنود و دریافت بسته‌ها را آغاز کنید و پس از مدتی عملیات را متوقف کنید (مانند تصویر ۱-۳) همچنین می‌توانید با دکمه‌های ترکیبی CTRL+E عملیات شنود را آغاز و متوقف کنید .

تصویر ۱- ۳) عملیات آغاز دریافت بسته‌ها از واسط شبکه مشخص شده

در ادامه برنامه شروع به دریافت بسته‌ها از واسط انتخابی 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 rulesقابل دسترس است. همان‌طور که در تصویر زیر مشاهده می‌کنید(تصویر ۱-۴)، هر بسته در هر سطر به همراه توضیحاتی مانند نوع پروتکل، آدرس مبدا و زمان دریافت بسته مشخص شده است همچنین توضیحات بیشتری را در مورد بسته می‌توانید در زیر مشاهده کنید.



تصویر ۱- ۴) بسته‌های دریافت شده توسط نرم‌افزار و توضیحات مرتبط با هر بسته

۳-۴ -شرح آزمایش

*در تمام بخش‌های آزمایش، واسطی که با آن دسترسی به اینترنت دارید را برای شنود بسته انتخاب کنید.

۳-۴-۱ -لایه‌بندی پروتکل‌ها

شروع به شنود بسته‌ها کنید. به اینترنت وارد شوید، شروع به وب گردی کنید و پس از گذشت سه دقیق شنود را متوقف کنید.

سوال ۱: به یک بخش دلخواه از بسته‌های شنود شده مراجعه کنید. چه پروتکل‌هایی را مشاهده می‌کنید. لیست آنها را یادداشت کنید.

سوال ۲: یک بسته را به دلخواه انتخاب کنید. مشخص کنید که چه پروتکل‌هایی در لایه‌های مختلف آن استفاده شده است. ترتیب قرارگیری بیت‌ها داخل بسته چه ارتباطی با لایه‌های مختلف دارد؟ اندازه فریم لایه دو این بسته چقدر است؟ اندازه بسته لایه ۳ چقدر است؟

سوال ۳: آیا می‌توانید بسته‌هایی را پیدا کنید که بدون پروتکل‌های لایه‌هایNetwork، Transportو Application باشند؟

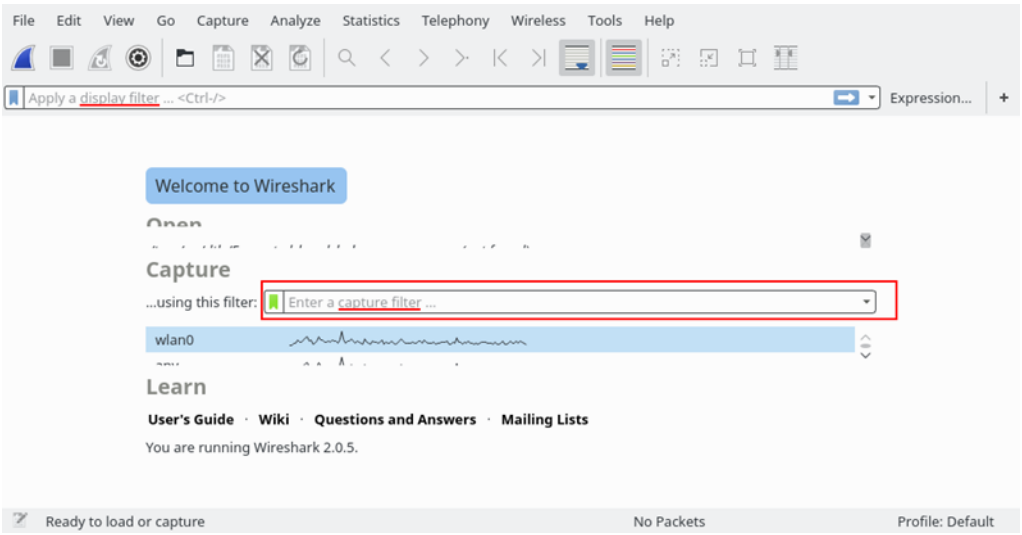
سوال۴: این بسته‌ها از چه پروتکلی استفاده کرده‌اند؟

سوال ۵: از یکی از بسته‌ها بخش مربوط به پروتکل Protocol(IP) Internet را پیدا کنید Checksum .پروتکل IP را پیدا کنید و آن را یادداشت کنید.

سوال ۶: از یکی از بسته‌ها بخش مربوط به پروتکل Protocol(TCP) Control Transport و یا Protocol(UDP) Datagram Userرا پیدا کنید. عدد مربوط به Port مبدا و مقصد را یادداشت کنید. به نظر شما این اعداد در مبدا و مقصد چه چیزی را مشخص میکند؟ Checksum مربوط به پروتکلهای TCP و UDP را مشخص کنید.

۳-۴-۲ -کار با فیلترکننده بسته‌ها

برنامه Wireshark دو نوع فیلتر کننده بسته دارد. یک نوع Filter Capture است و نوع دیگر Filter .Display Filter Captureقبل از شروع به شنود بسته مقداردهی می‌شود و در حقیقت همان فیلتری است که توسط NPF بر روی بسته‌های دریافت شده از گرداننده شبکه اعمال میگردد. بنابراین این فیلتر بر جمع‌آوری بسته‌ها تاثیر می‌گذارد. در مقابل Filter Display صرفا مربوط به فیلتر کردن بسته‌های جمع‌آوری شده است. با استفاده از Filter Display می‌توان تعدادی از بسته‌های جمع‌آوری شده را مشخص کرد که در پنجره Wireshark نمایش داده شوند. این تفاوت در تصویر ۱-۵ نیز نمایش داده شده است.



تصویر ۱- ۵) انواع فیلتر بسته‌ها

۱-۲-۴-۳- کار با capture filter

۱. به صفحه اول برنامه بروید و در قسمتFilter Capture ، مقدار port 53 را وارد کنید .
۲. حال واسط شبکه موردنظر خود را انتخاب کنید.
۳. در command prompt دستور ping google.com را وارد کنید.
٤. سپس دستور nslookup 1.1.1.1 را وارد کنید.
۵. حال شنود بسته‌ها را متوقف کرده و شما باید صرفا پروتکل‌های DNS را در wireshark مشاهده کنید .

سوال ۷: یکی از بسته‌ها که از سیستم شما ارسال شده است را انتخاب کنید. پروتکل لایه Transport چیست؟ آدرس IP مقصد چیست؟ سرایند (header) لایه دوم را انتخاب کنید. آدرس مبدا و مقصد را یادداشت کنید.

سوال ۸: کدامیک از آدرس‌های پیدا کرده در بخش قبل را می‌توانید در خروبی دستور ipconfig /allمشاهده کنید؟

سوال ۹: یک بسته مربوط به دستور Ping را انتخاب کنید و به بخش مربوط به پروتکدل DNS در آن بروید. به بخش Queriesبروید. چه type ای انتخاب شده است؟ به نظر شما این درخواست DNS برای چه کاری استفاده شده است؟

سوال ۱۰: یک بسته مربوط به دستور nslookup را انتخداب کنید و به بخش مربوط به پروتکل DNS در آن بروید. به بخش Queriesبروید. چه type ای انتخاب شده است؟ بده نظر شما این درخواست DNS برای چه کاری استفاده شده است؟

سوال ۱۱: به نظر شما چه type های دیگری ممکن است وجود داشته باشد؟ سه مورد را یادداشت کنید.

۲-۲-۴-۳- کار با display filter

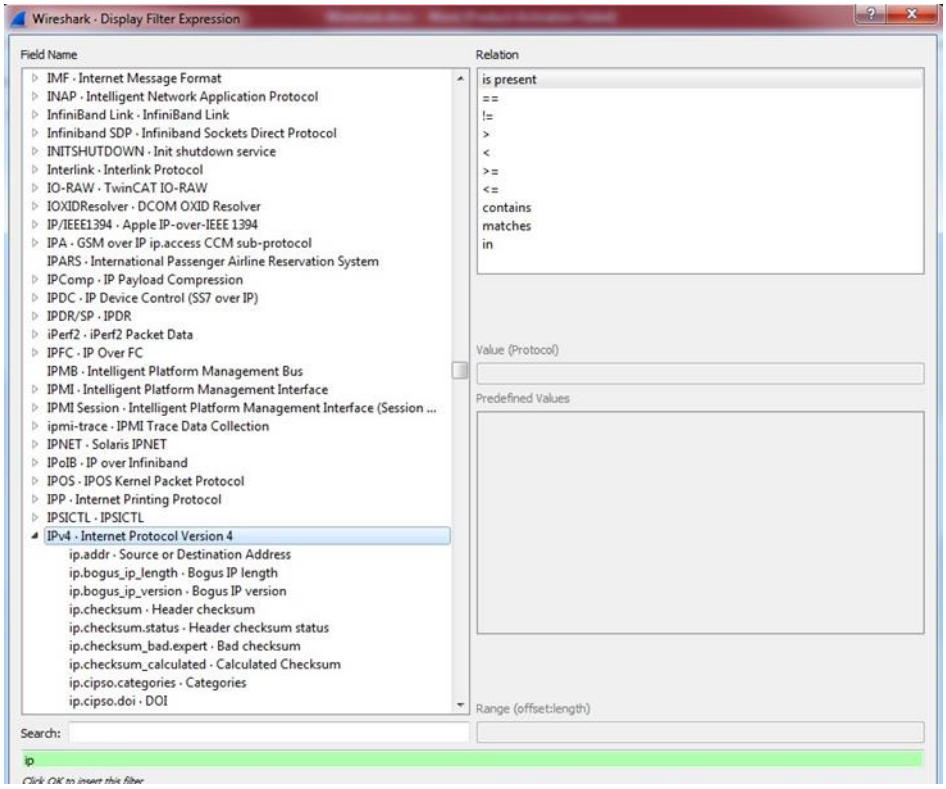
۱. دوباره به صفحه اول برنامه بروید. این بار واسط شبکه را بدون هیچ Filter Capture ای انتخاب کنید.

۲. در command prompt دستور tracert p30download.com را وارد کنید. منتظر بمانید تا کار دستور به اتمام برسد.

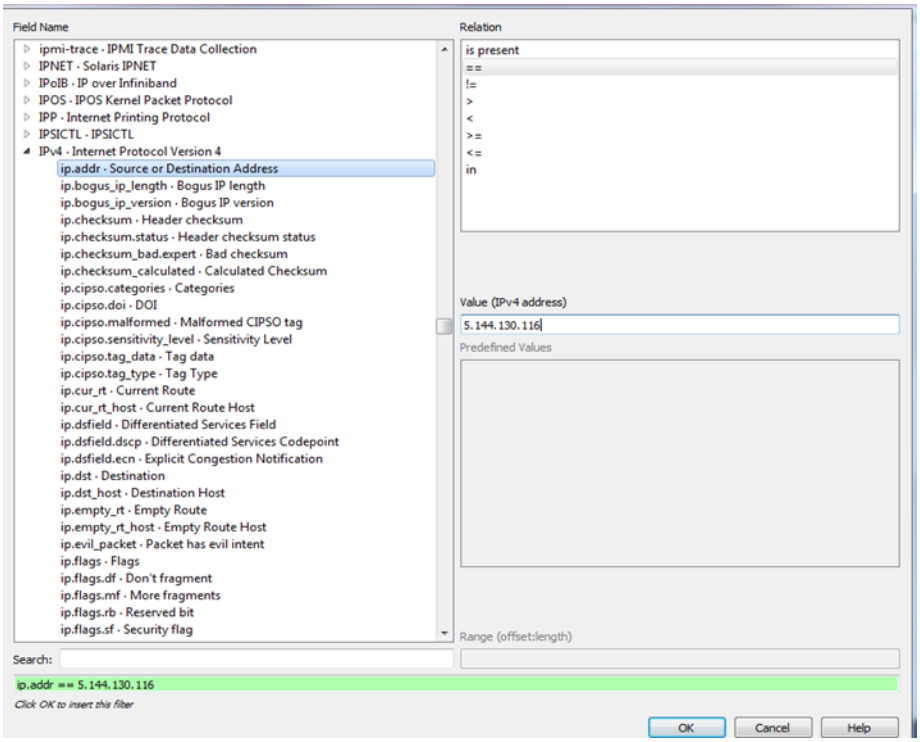
۳. بدون اینکه شنود بسته را متوقف کنید در قسمت filter display مقدار dns را تایپ کنید و اینتر را بزنید. مشاهده میکنید که صرفا بسته‌های مربوط به پروتکل DNS انتخاب شدند در حالی که سایر بسته‌ها نیز در حال دریافت شدن از گرداننده کارت شبکه هستند.

٤. در قسمتdisplay filter ، کلیک راست کنید و بر روی display filter expression کلیک کنید. مانند تصویر ۱-۶ صفحه‌ای باز شده و واژه ip را جستجو کنید و مقدار ipv4 را انتخاب کنید .

٥. از زیر بخشهایIPv4 ، بخش ip.addr را انتخاب کنید. سپس از بخشrelation ، مقدار == را انتخاب کرده و در بخش Value آدرس IP که از دستور tracert به شما گزارش شده است را وارد کنید. به عنوان مثال برای آدرس p30download.comبه تصویر ۱-۷ مراجعه کنید .



تصویر ۱- ٦) انتخاب display filter



تصویر ۱- ۷) مقادیر برای p30download.com

سوال ۱۲: بعد از کلیک کردن بر روی OK چه اتفاقی میافتد؟ در بسته‌هایی که مشخص شده‌اند چه پروتکل‌هایی را مشاهده می‌کنید؟

سوال ۱۳: اولین بسته را انتخاب کنید. به بخش پروتکل Internet Control Message Protocolبروید. مقدار type را مشخص کنید. به بخش مربوط به پروتکل IP بروید و مقدار TTL را یادداشت کنید.

٦. برای بسته‌هایی که مبدا آنها ماشین شماست مقدار TTL را یادداشت کنید. این مقدار در حدال تغییر است.

سوال ۱۴: به نظر شما هدف از تغییر این مقدار چیست؟ می‌توانید با مراجعه به هدف دستور tracert آن را شرح دهید.

۷. از بخش فیلتر، مقدار فیلتر را به دستور ip.proto == ۶ تغییر دهید .

سوال ۱۵: این فیلتر چه کاری انجام می‌دهد؟