۳- آشنایی با نرم‌افزار Wireshark

۳-۱- هدف آزمایش

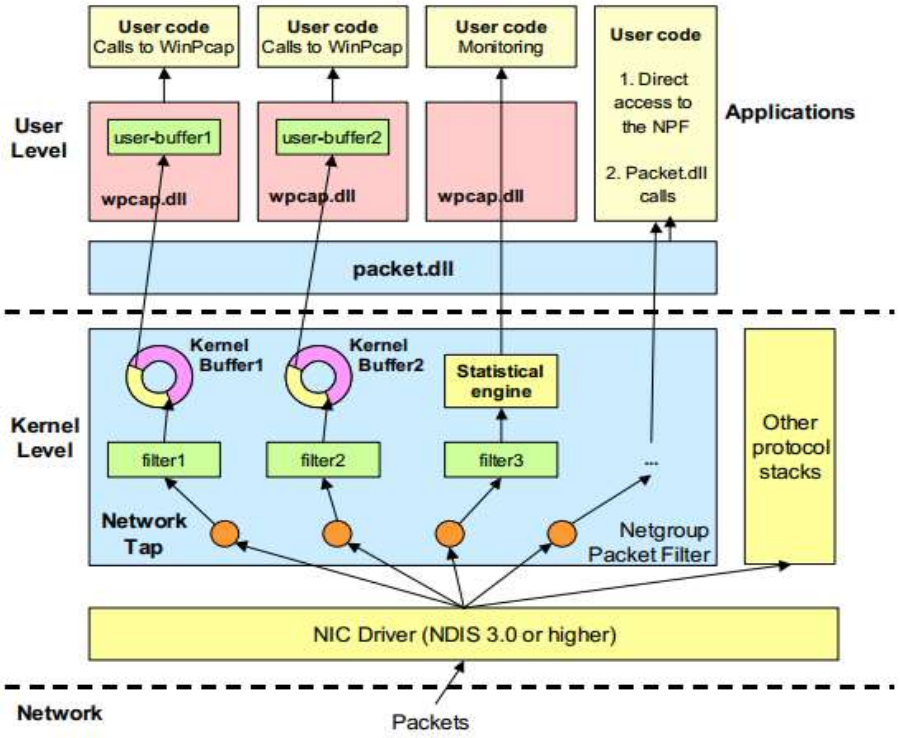
هدف از این آزمایش آشنایی با نرم‌افزار Wireshark و بررسی پروتکل‌ها در لایه مختلف معماری TCP/IP است.

۳-۲- 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 ۱۰۰۰ پروتکل در نسخه ۱.۱۰.۶ 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.

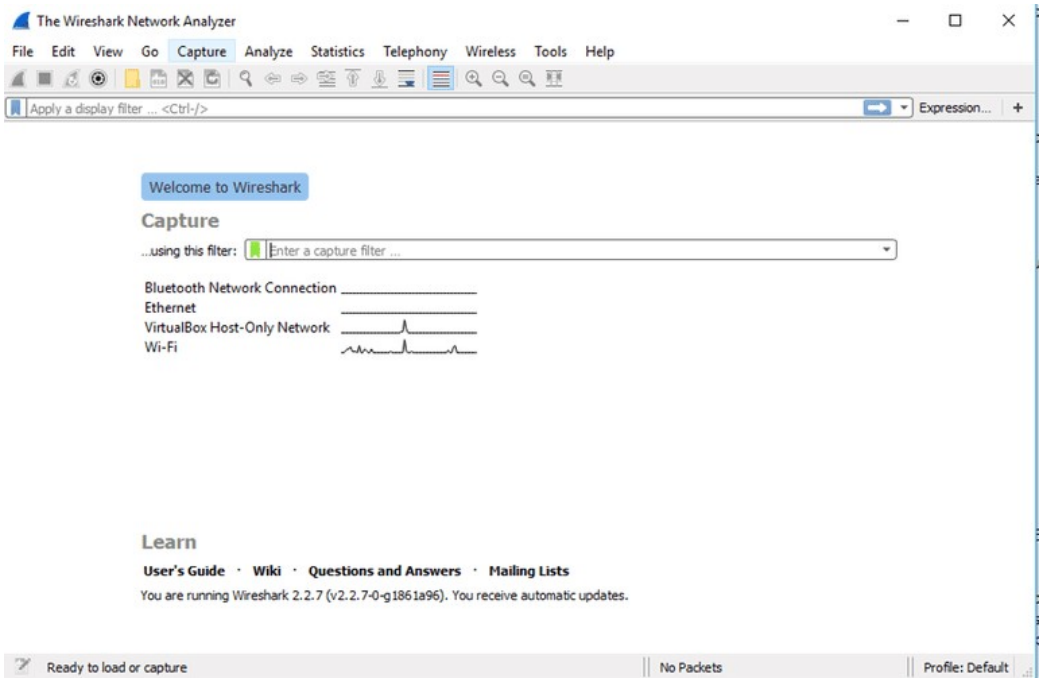
در سیستم‌عامل خانواده ویندوز، برنامه Wireshark شنود بسته‌ها با استفاده از کتابخانه Winpcap انجام می‌دهد. معماری نرم‌افزار Winpcap در شکل (۱-۳۵) نمایش داده شده است. همان‌گونه که در این شکل مشخص است، برنامه Winpcap از دو بافر یکی در سطح کرنل و دیگری در سطح کاربر، یک ماشین فیلتر کننده که فیلترهایی را به 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.



شکل (۳۵-۱) معماری نرم‌افزار Wireshark

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 (۱-۳۶) نمایش داده می‌شود.

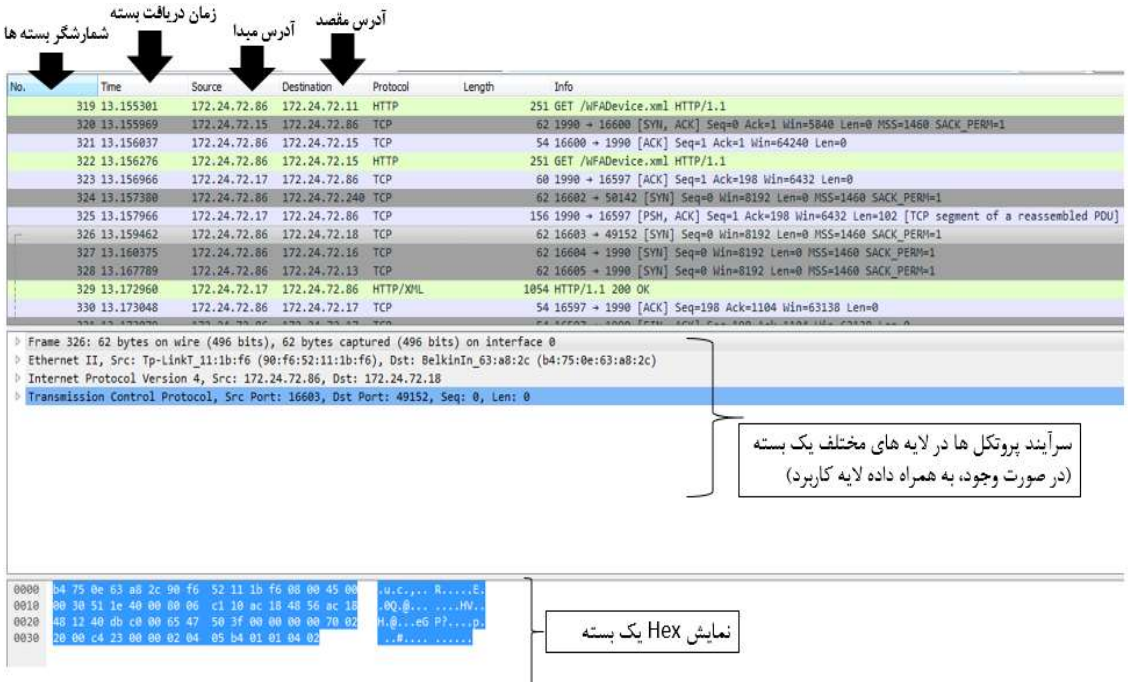


شکل (۳۶-۱) صفحه اول برنامه

واسط شبکه‌ای که به اینترنت متصل است را انتخاب کنید. در ادامه برنامه شروع بـه دریافـت بسته‌ها از کارت شبکه می‌کند. معمولا هر سطر یک بسته را نشان می‌دهـد. همان‌گونـه کـه مشـاهده می‌کنید بسته‌ها با رنگ‌های مختلف نمایش داده شده‌اند. قوانین رنـگ گـذاری Wireshark از بخـش View->Coloring rules قابل دسترس است. اجزای مختلف منـوی ابـزار Wireshark در شـکل (۱-۳۷) نمایش داده شده است.

شکل (۳۷-۱) منوی ابزار

هر زمان که خواستید می‌توانید با استفاده از کلیدهای CTRL+E یا دکمه قرمز رنگ در نـوار ابزار، شنود بسته‌ها را متوقف کنید. با دوباره فشردن CTRL+E، Wireshark دوباره شـروع بـه شـنود 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 اصـلی Wireshark در شکل (۱-۳۸) نمایش داده شده است.



شکل (۳۸-۱) بخش‌های مهم نرم‌افزار wireshark

۳-۳- قطعات و ابزارهای موردنیاز

ابزارهای موردنیاز در این آزمایش عبارت‌اند از:

- برنامه Wireshark نسخه ۲ به بعد
- یک کامپیوتر با سیستم‌عامل ویندوز 7 به بعد با دسترسی به اینترنت

۴-۳- شرح آزمایش

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

۱-۴-۳- 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 به‌دلخواه 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؟

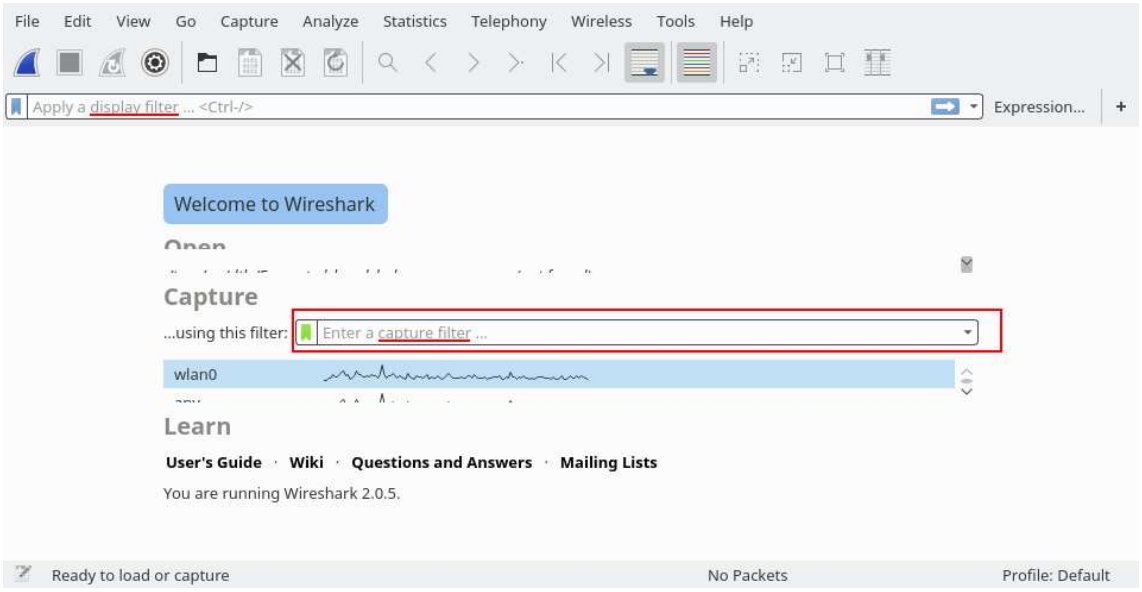
سوال ۳: آیا می‌توانید بسته‌هایی را پیدا کنید که بدون پروتکل‌های لایه‌های Network، Transportو Application باشند؟ این بسته‌ها از چه پروتکلی استفاده کرده‌اند؟

سوال ۴: از یکی از بسته‌ها بخش مربوط به پروتکل Internet Protocol(IP) را پیدا کنید. Checksum پروتکل IP را پیدا کنید و آن را یادداشت کنید.

سوال ۵: از یکی از بسته‌ها بخش مربوط به پروتکل Transport Control Protocol(TCP) و یا User Datagram Protocol(UDP) را 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.

۲-۴-۳- کار با فیلتر کننده بسته‌ها

برنامه Wireshark دو نوع فیلتر کننده بسته دارد. یک نوع Capture Filter است و نوع دیگر Display Filter. Capture Filter قبل 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 Display Filter صرفا مربوط به فیلتر کردن بسته‌های جمع‌آوری شده است. با استفاده از Display Filter می‌توان تعدادی از بسته‌های جمع‌آوری شده را مشخص کرد که در پنجره Wireshark نمایش داده شوند. این تفاوت در شکل (۱-۳۹) نیز نمایش داده شده است.



شکل (۳۹-۱) انواع فیلتر بسته

۱-۲-۴-۳- کار با Capture Filter

۱. به صفحه اول برنامه بروید و در قسمت Capture Filter، مقدار

port 53

۲. را وارد کنید. درنهایت اینترفیسی که به اینترنت دسترسی دارد را انتخاب کنید.

۳. CMD را باز کرده و دستور

ping google.com

را وارد کنید. سپس دستور

nslookup 1.1.1.1

را نیز وارد کنید. اکنون شنود بسته‌ها را متوقف کنید. شما باید صرفا بسته‌های پروتکل DNS را در Wireshark مشاهده کنید.

سوال ۶: یکی از بسته‌ها که از سیستم شما ارسال شده است را انتخاب کنید. پروتکل لایه Transport چیست؟ آدرس IP مقصد چیست؟ سرایند لایه دوم را انتخاب کنید. آدرس مبدا و مقصد را یادداشت کنید.

سوال ۷: کدام‌یک از آدرس‌های پیدا کرده در بخش قبل را می‌توانید در خروجی دستورall/ ipconfig مشاهده کنید؟

سوال ۸: یک بسته مربوط به دستور Ping را انتخاب کنید و به بخش مربوط به پروتکل DNS در آن بروید. به بخش Queries بروید. چه type ای انتخاب شده است؟ به نظر شما این درخواست DNS برای چه کاری استفاده شده است؟

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

سوال ۱۰: 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 اینترفیس را بدون هیچ Capture Filter ای انتخاب کنید.

۲. در CMD دستور زیر را وارد کنید.

tracert p30download.com

منتظر بمانید تا کار دستور به اتمام برسد.

۳. بدون اینکه شنود بسته را متوقف کنید در قسمت display filter 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 گردانده کارت شبکه هستند.

۴. در قسمت Display Filter، کلیک راست کرده و بر روی Display Filter Expression کلیک کنید. صفحه مطابق شکل (۱-۴۰) باز می‌شود. IP را جستجو کنید و IPv4 را از ستون سمت چپ انتخاب کنید.

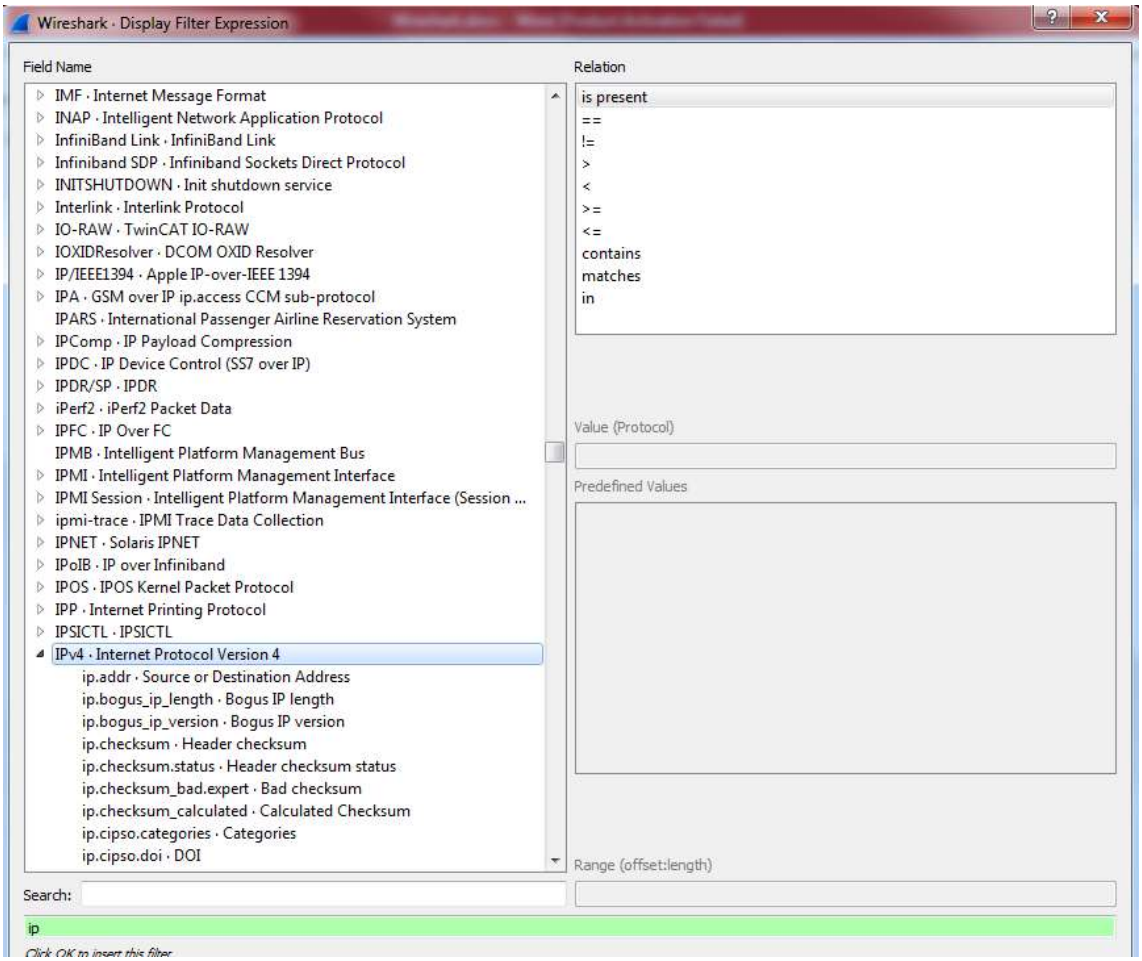
۵. از زیر بخش‌های IPv4، بخش ip.addr را انتخاب کنید. سپس از بخش relation، مقدار == را انتخاب کرده و در بخش Value آدرس IP که از دستور tracert به شما گزارش شده است را وارد کنید. به عنوان مثال برای آدرس p30download.com مشابه شکل (۱-۴۱) است.

سوال ۱۱: بعد از کلیک کردن بر روی OK چه اتفاقی می‌افتد؟ در بسته‌هایی که مشخص شده‌اند چه پروتکل‌هایی را مشاهده می‌کنید؟

سوال ۱۲: اولین بسته را انتخاب کنید. به بخش پروتکل Internet Control Message Protocol بروید. مقدار type را مشخص کنید. به بخش مربوط به پروتکل IP بروید و مقدار TTL را یادداشت کنید.

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

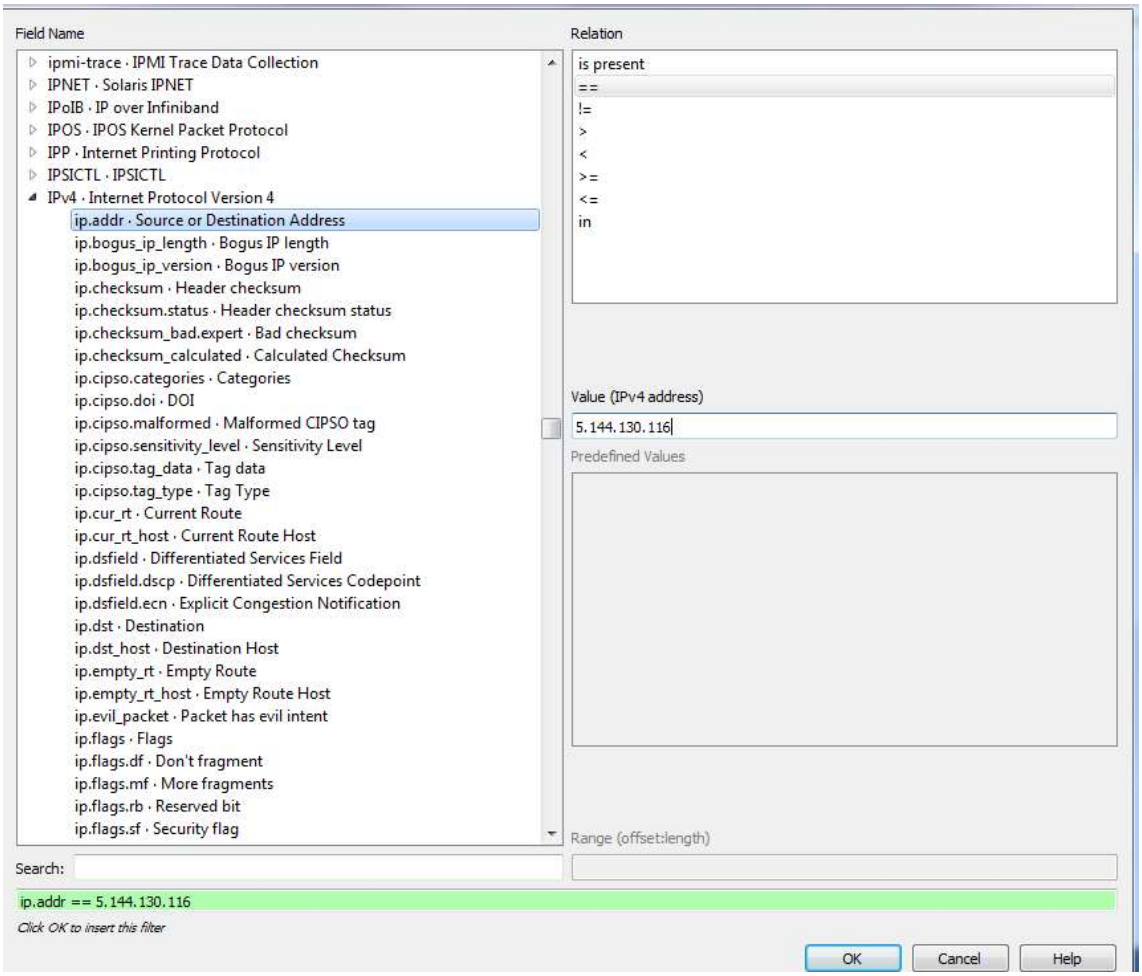
سوال ۱۳: به نظر شما هدف از تغییر این مقدار چیست؟ می‌توانید با مراجعه به هدف دستور tracert آن را شرح دهید.



شکل (۴۰-۱) انتخاب Display Filter

۷. از بخش فیلتر، مقدار فیلتر را به دستور ip.proto == 6 تغییر دهید.

سوال ۱۴: این فیلتر چه کاری انجام می‌دهد؟



شکل (۴۱-۱) مقادیر برای p30download.com