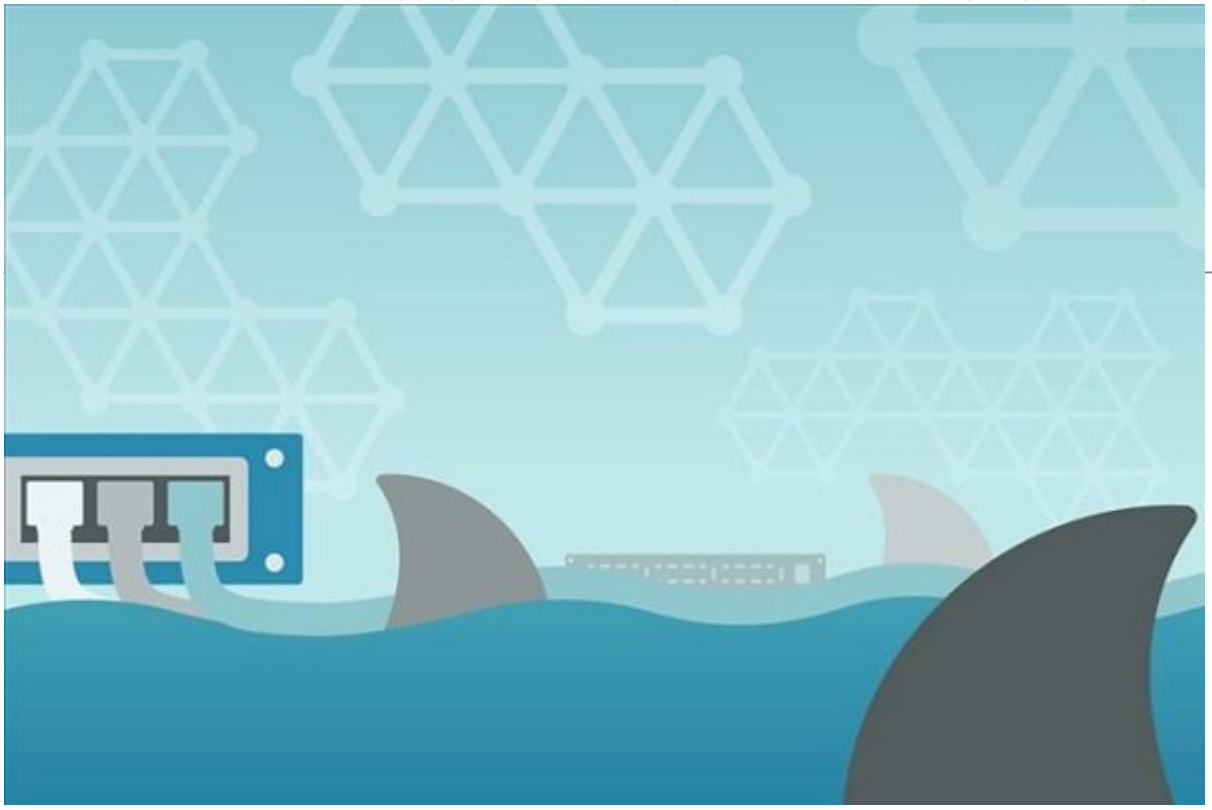
با Wireshark بر ترافیک شبکه نظارت کنید

راهنمای جامع به‌کارگیری Wireshark برای نظارت بر ترافیک شبکه‌ها



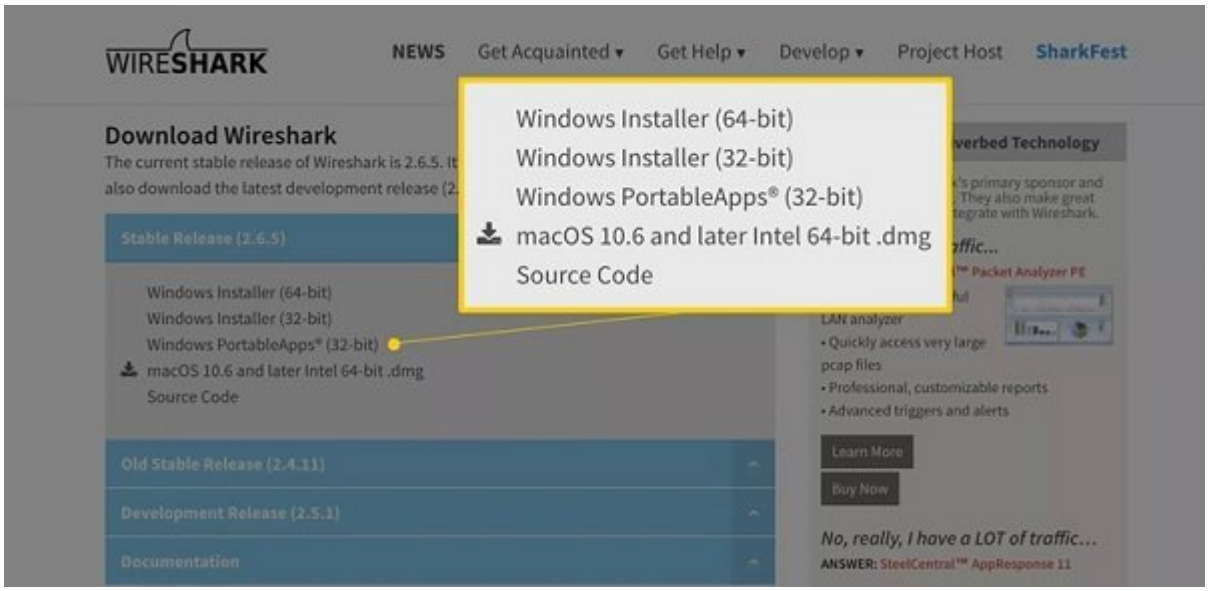
مهندس شبکه‌های کامپیوتری (بی‌سیم یا سیمی) برای پیشبرد هرچه دقیق‌تر کارهای خود مجبور است با تعدادی از نرم‌افزارهای حوزه کاری‌اش آشنایی داشته باشد. این ضرورت برای افرادی که تخصص آن‌ها طراحی و پیاده‌سازی شبکه‌های بی‌سیم است، دوچندان می‌شود، زیرا مجبورند، هرگونه تداخلی را شناسایی کرده و با نظارت روی بسته‌های اطلاعاتی مبادله شده میان دو گره نرخ انتقال داده‌ها و ضریب خطاهای موجود را شناسایی کنند. نرم‌افزار Wireshark یکی از قدرتمندترین نرم‌افزارهای رایگانی است که اجازه می‌دهد وضعیت بسته‌های اطلاعاتی ارسالی و دریافتی در یک شبکه را رصد کرده و تحلیل دقیقی از شبکه به دست آورید. نرم‌افزاری که اجازه می‌دهد محتویات هر بسته اطلاعاتی را خوانده و بنا بر نیاز خود آن‌ها را فیلتر کنید. این پروتکل متن‌باز تحلیلگر به دلیل عملکرد بسیار بالا و دقیقی که دارد، به‌عنوان یک استاندارد صنعتی پذیرفته‌شده و تا به امروز جوایز متعددی دریافت کرده است.
زمانی‌که درباره شبکه‌ها و طراحی آن‌ها صحبت می‌کنیم، ضرورت دارد که دست‌کم درباره یک ابزار پر کاربرد این حوزه سخن بگوییم. به همین دلیل در این مقاله سعی کرده‌ایم به‌طور اجمالی ابزار ذکرشده را معرفی کرده و نحوه کار با آن را تشریح کنیم.

Wireshark چیست؟

وایرشارک یک ابزار متن‌باز است که برای تحلیل ترافیک شبکه و پروتکل‌های شبکه استفاده می‌شود. این ابزار می‌تواند داده‌ها را از میان صدها پروتکل متنوعی که روی تمام شبکه‌های اصلی قرار دارند، استخراج کرده و نمایش دهد. **وایرشارك** اجازه می‌دهد، بسته‌های داده‌ای را به دو شکل برخط و آفلاین مشاهده کنید. این نرم‌افزار از ده‌ها فرمت فایلی همچون CAP و ERF که برای تحلیل اطلاعات استفاده می‌شوند، پشتیبانی می‌کند. در مجموع باید بگوییم که **وایرشارک** برای اشکال‌زدایی، آزمایش مشکلات امنیتی، تجزیه‌وتحلیل پروتکل‌ها، شناسایی رخنه‌های امنیتی و در نهایت آموزش شبکه و امنیت کاربرد دارد. لازم به توضیح است که وایرشارک زمانی به یاری‌تان خواهد آمد که شما شناخت دقیقی از شبکه، مدل مرجع OSI و پروتکل‌های شبکه داشته باشید. در نتیجه اگر در خصوص مباحث زیربنایی شبکه اطلاعاتی ندارید، پیشنهاد بر این است که کمی وقت صرف کرده و دانش خود را در خصوص مولفه‌های زیرساختی شبکه افزایش دهید. این ابزار برای آموزش مفاهیم شبکه از سوی برخی موسسات استفاده می‌شود.

دانلود و نصب نرم‌افزار

نرم‌افزار ذکرشده به شکل رایگان و بدون پرداخت هیچ‌گونه هزینه اضافی از سایت این شرکت به نشانی Wireshark Foundation website برای هر دو پلتفرم ویندوز و مک قابل دریافت است. (شکل 1)

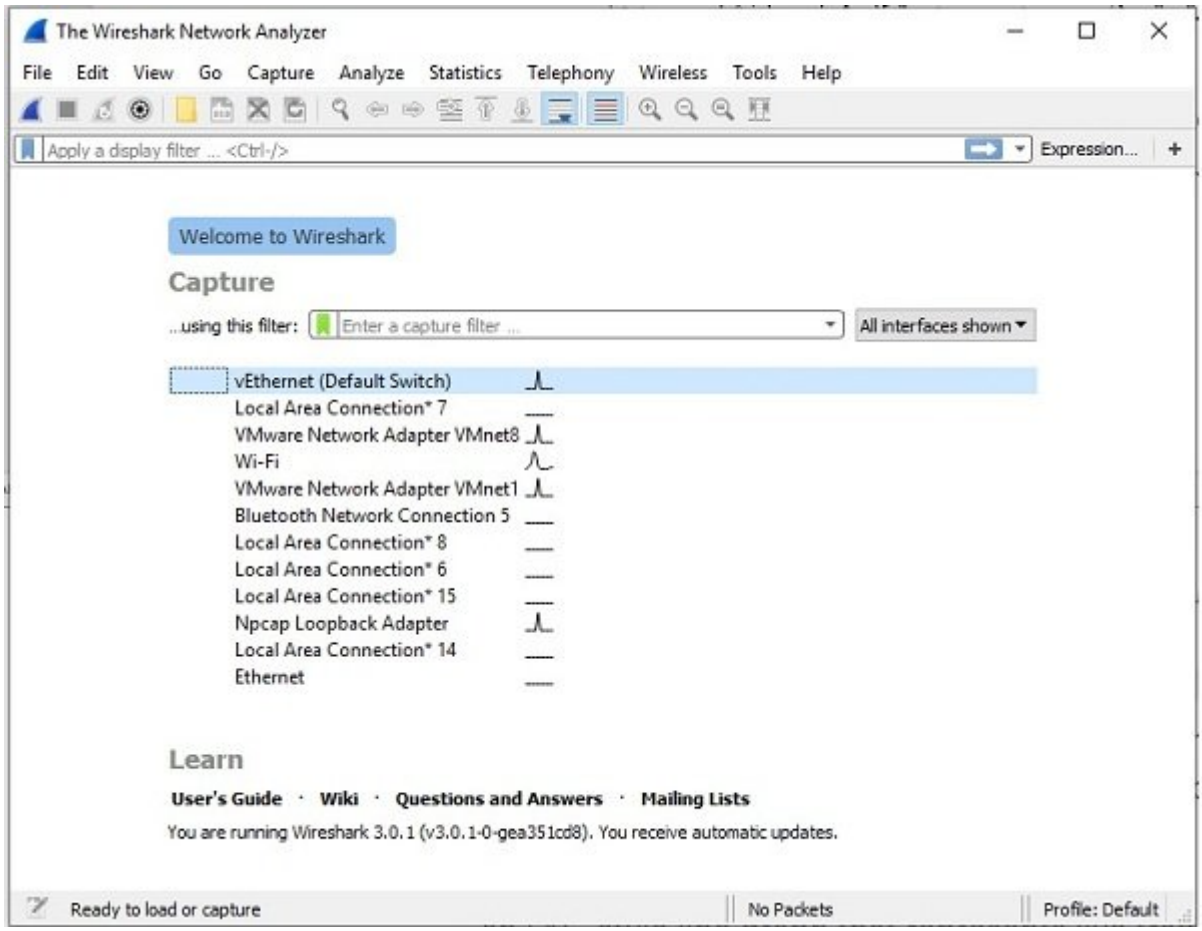


کاربرانی که از پلتفرم ویندوز استفاده می‌کنند، در زمان نصب این نرم‌افزار باید کتابخانه WinPcap را نصب کنند.

WinPcap کتابخانه‌ای است که برای ضبط داده‌های بلادرنگ به آن نیاز است. لازم به توضیح است که نسخه لینوکس و یونیکسی همچون ردهت، سولاریس و FreeBSD این نرم‌افزار در دسترس علاقه‌مندان قرار دارد. نسخه‌های باینری ویژه این پلتفرم‌ها در پایین صفحه اصلی دانلود نرم‌افزار و در بخش Third-Party Packages قرار دارد. نصب نرم‌افزار راحت است و پیچیدگی خاصی ندارد و اگر تمایل دارید در فرآیند نصب ترافیک پورت‌های USB را رصد کنید، بهتر است گزینه Install USBPcap را فعال کنید.

چگونه بسته‌های داده‌ای را ضبط کنیم؟

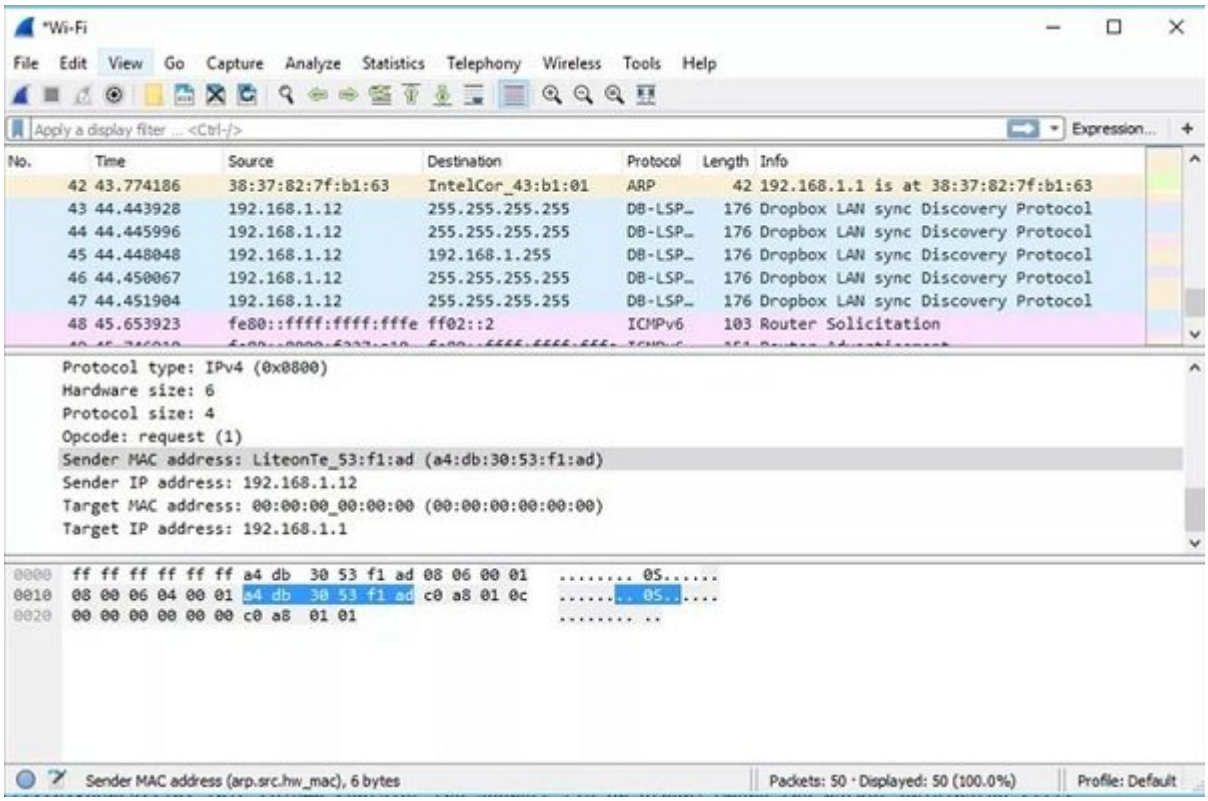
زمانی که نرم‌افزار را اجرا می‌کنید، صفحه خوشامدگویی تمامی اتصالات شبکه جاری را روی دستگاه فعلی نشان می‌دهد. (شکل 2) در شکل 2 یک اتصال بلوتوثی، اترنت، شبکه‌های مجازی، انواع اتصالات محلی و وای‌فای را مشاهده می‌کنید. اگر گزینه USBPcap را فعال کرده باشید، فهرستی از پورت‌های یواس‌بی نشان داده می‌شود. در سمت راست هر ارتباطی که فعال باشد، یک گراف خطی وضعیت ترافیک زنده را روی یک اتصال نشان می‌دهد.
برای آغاز به کار ضبط کردن بسته روی شبکه مدنظر کلیک کرده یا اگر در نظر دارید اطلاعات چند شبکه را ضبط کنید، از کلیدهای Shift یا Ctrl برای انتخاب شبکه‌های مدنظر استفاده کنید. پس از انتخاب شبکه موردنظر روی منوی Capture کلیک و گزینه Start را انتخاب کرده یا از میان‌برهای Ctrl+E برای آغاز فرآیند ضبط بسته‌ها استفاده کنید. فرآیند ضبط زنده همراه با نمایش جزییات بسته‌ها در پنجره اصلی **وایرشارک** آغاز می‌شود. برای توقف این فرآیند کافی است دومرتبه کلیدهای Ctrl+E را فشار دهید.



زمانی‌که شبکه را انتخاب کردید، روی آن دو بار کلیک کرده یا از میان‌بر فوق استفاده کنید، **وایرشارک** بسته‌هایی را که از سوی کارت شبکه ارسال یا دریافت می‌شوند، ضبط کرده و نشان می‌دهد.

مشاهده و تحلیل محتویات بسته‌ها

اکنون‌که توانستید بسته‌های داده‌ای را ضبط کنید، زمان آن رسیده تا به بسته‌های ضبط‌شده نگاهی داشته باشید. با توجه بیشتر به شکل 3 رابطی را مشاهده می‌کنید که از سه بخش اصلی پنل فهرست بسته‌ها، پنل جزییات بسته‌ها و پنل بایت‌های بسته‌ها تشکیل‌شده است.



مطلب پیشنهادی

ملزومات موردنیاز یک مسئول شبکه
10 ابزار رایگان تحلیلی و نظارتی بر شبکه‌های کامپیوتری

فهرست بسته‌ها

پنل فهرست بسته‌ها در بالای پنجره، همه بسته‌های ضبط شده را نشان می‌دهد. هر بسته ردیف خاص خود را دارد و عددی به آن تخصیص داده‌شده است. عددی که متناظر به بسته ضبط‌شده است. ستون‌های این پنل به شرح زیر هستند:
Time: در این ستون مهر زمانی ثبت بسته‌ها نشان داده می‌شود. فرمت پیش‌فرض این ستون بر حسب ثانیه است که مدت‌زمان سپری‌شده را از اولین باری که بسته‌ها ایجادشده و درون یک فایل قرار گرفته، نشان می‌دهد. برای تغییر این واحد به فرمتی که قابل‌فهم‌تر باشد (به‌طور مثال، زمان واقعی ضبط بسته‌ها) کافی است به منوی View رفته و گزینه Time Display Format را انتخاب کنید.
Source: این ستون دربرگیرنده آدرس آی‌پی یا سایر اطلاعاتی است که بسته‌ها به آن تعلق دارند.
Destination: این ستون شامل آدرسی است که بسته به آن ارسال می‌شود.
Protocol: نام پروتکل بسته همچون TCP و... را مشخص می‌کند.
Length: طول بسته‌ها بر مبنای بایت در این ستون نشان داده می‌شود.
Info: اطلاعات بیشتری در ارتباط با بسته‌ها ارائه می‌کند. محتویات نشان داده‌شده در این ستون به نوع محتوای بسته بستگی دارد.
زمانی که بسته‌ای در پنل فوق انتخاب می‌شود، ممکن است یک یا چند سمبل در ستون اول مشاهده کنید. براکت‌های باز یا بسته همراه با یک خط افقی مستقیم نشان می‌دهند که آیا بسته یا گروهی از بسته‌ها بخشی از یک نشست (Session) رفت‌وبرگشت در شبکه هستند یا خیر. یک خط افقی شکسته شده نشان می‌دهد، یک بسته بخشی از یک نشست نیست.

جزییات بسته‌ها

پنل جزییات وسط صفحه، پروتکل‌های فعلی و پروتکل‌های مرتبط با بسته‌های ضبط‌شده را در فرمتی قابل‌فهم نشان می‌دهد. در این پنل اگر روی هر یک از سطرها کلیک کنید، سطر مربوط باز شده و جزییات بیشتری نشان داده می‌شود. البته **وایرشارک** به شما اجازه می‌دهد از فیلترهای خاصی برای مشاهده جزییات استفاده کرده و استریم‌های داده‌ای را بر مبنای نوع پروتکل به شکل پالایش شده‌ای مشاهده کنید. برای این منظور کافی است در پنل میانی کلیک راست کرده و فیلتر مربوط را انتخاب کنید.

بایت‌های درون بسته‌ها

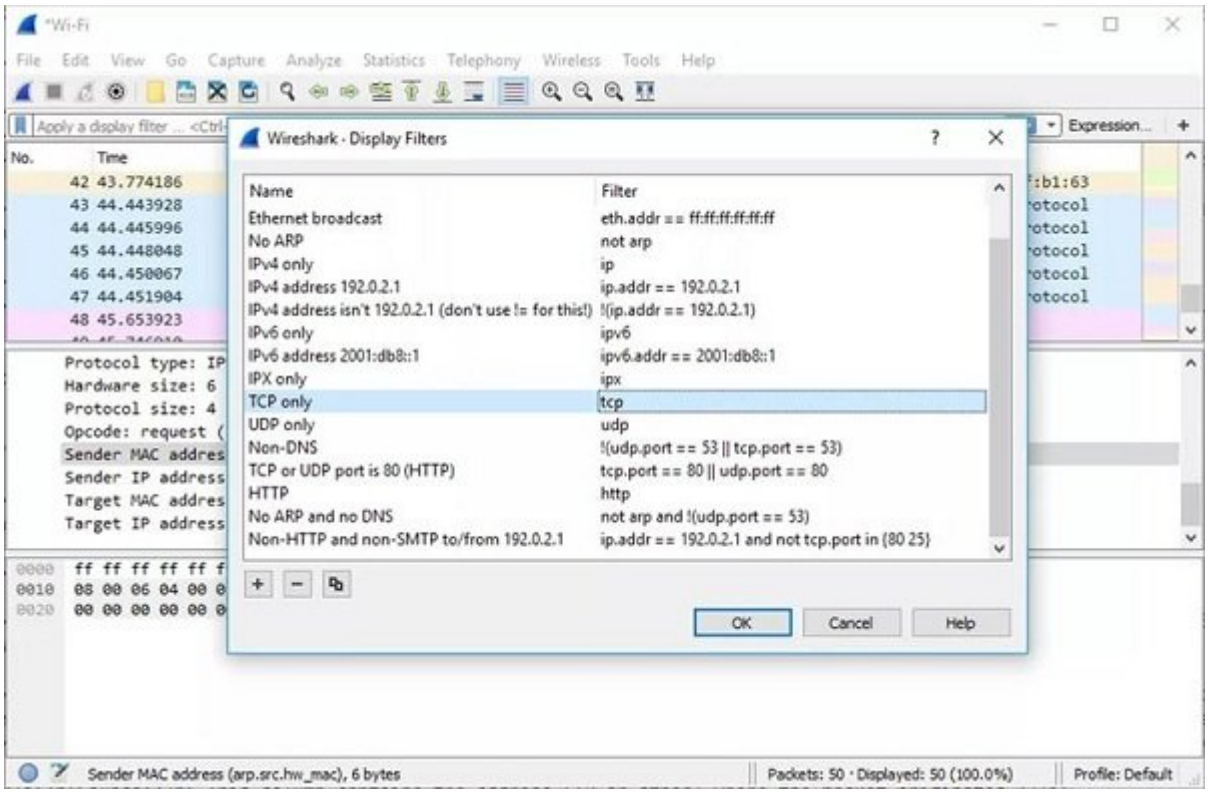
در انتهای این پنجره، پنل بایت‌ها قرار دارد که داده‌های خام بسته‌ای را که انتخاب‌شده، در مبنای هگزادسیمال نشان می‌دهد. این داده‌های هگزا شامل 16 بایت هگزادسیمال و 16 بایت اسکی هستند که در کنار داده‌های افست وضعیت یک بسته را نشان می‌دهند. اگر هر یک از مقادیر داده‌ای این بخش را انتخاب کنید، به شکل خودکار جزییات بسته در پنل میانی انتخاب‌شده و نشان داده می‌شوند. برای مشاهده داده‌ها در قالب بیتی به‌جای مبنای هگزا کافی است در همین پنل کلیک راست کرده و از منوی ظاهرشده گزینه ...as bits را انتخاب کنید. در این حالت داده‌ها در مبنای دودویی و به شکل صفر و یک نشان داده می‌شوند.

مطلب پیشنهادی

نحوه پیکربندی پیاده‌سازی دیوارآتش ویندوز
دیوارآتش از پیش ساخته شده ویندوز یک بسته امنیتی رایگان و قدرتمند

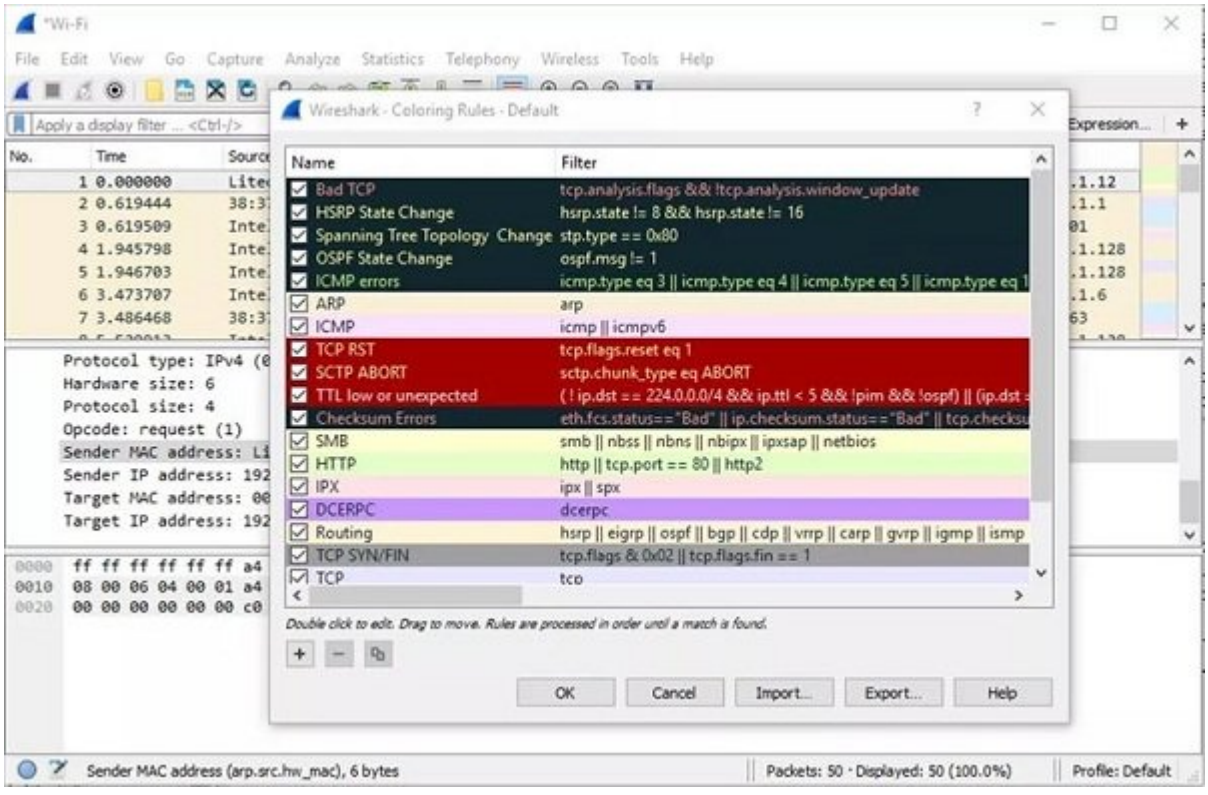
نحوه به‌کارگیری فیلترهای وایرشارک

بدون تردید یکی از مهم‌ترین قابلیت‌های برنامه **وایرشارک** فیلترها هستند، به‌ویژه مواقعی‌که بسته‌های داده‌ای درون فایل‌هایی با اندازه‌های مختلف ضبط شده‌اند. **وایرشارک** به شما اجازه می‌دهد، فیلترهای مرتبط با رکوردرها را پیش از آن‌که فرآیند ضبط بسته‌ها آغاز شود، تنظیم کنید. در چنین شرایطی وایرشارک تنها بسته‌هایی را که با معیارهای شما منطبق هستند، ثبت می‌کند. فیلترها این قابلیت را دارند که حتی روی یک فایلی که در گذشته ضبط شده‌اند، اعمال شوند. در این حالت فقط بسته‌های منطبق با معیارها نشان داده می‌شوند. این مدل فیلترها به فیلترهای صفحه‌نمایش (Display Filters) معروف هستند. وایرشارک در حالت پیش‌فرض طیف گسترده‌ای از فیلترهای از پیش‌ساخته شده را در اختیار متخصصان قرار می‌دهد تا متخصصان تنها با چند کلیک ساده تعداد بسته‌هایی را که قرار است مشاهده کنند، محدود کنند. بدون شک، این رویکرد در فرآیند تحلیل بسته‌ها کمک فراوانی می‌کند. برای آن‌که بتوانید از فیلترهای موجود در برنامه استفاده کنید، باید نام فیلتر مدنظر خود را در بخش Apply a Display Filter (بخشی که در پایین نوار ابزار **وایرشارک** قرار دارد.) یا در فیلد Enter A Capture Filter (بخشی که در صفحه اصلی برنامه وایرشارک قرار دارد.) وارد کنید. اگر به‌درستی می‌دانید که باید از چه فیلتری استفاده کنید، کافی است نام فیلتر مدنظر خود را در فیلد یاد شده وارد کنید. به‌عنوان‌مثال، اگر در نظر دارید وایرشارک تنها بسته‌های TCP را نشان دهد، باید واژه TCP را تایپ کنید. عملکرد **وایرشارک** در این زمینه هوشمند است، زمانی‌که واژه TCP را وارد کنید، وایرشارک به شکل خودکار گزینه‌های پیشنهادی را نشان می‌دهد.
روش دیگری که برای انتخاب یک فیلتر در اختیارتان قرار دارد، کلیک کردن روی آیکون سبز رنگ bookmark-like در صفحه شروع است. آیکون فوق در همان کادری قرار دارد که شما برای درج واژه TCP از آن استفاده می‌کنید. با کلیک کردن روی این گزینه منویی ظاهر می‌شود که فهرستی از فیلترهای مدنظر را نشان می‌دهد. همچنین گزینه‌ای برای مدیریت فیلترهای ضبط یا مدیریت فیلترهایی نمایش در اختیارتان قرار می‌دهد. اگر گزینه Manage Capture Filters را انتخاب کنید، پنجره‌ای ظاهرشده که اجازه اضافه، ویرایش یا حذف فیلترها را امکان‌پذیر می‌کند. (شکل 4) پس از تنظیم و اعمال فیلترها، به‌محض آغاز ثبت ترافیک شبکه فیلترها لحاظ خواهند شد. البته توجه داشته باشید، برای آن‌که فیلتر نمایش به‌درستی اعمال شود، باید روی دکمه فلشی که سمت راست فیلد ورودی قرار دارد، کلیک کنید تا فیلتر اعمال شود.



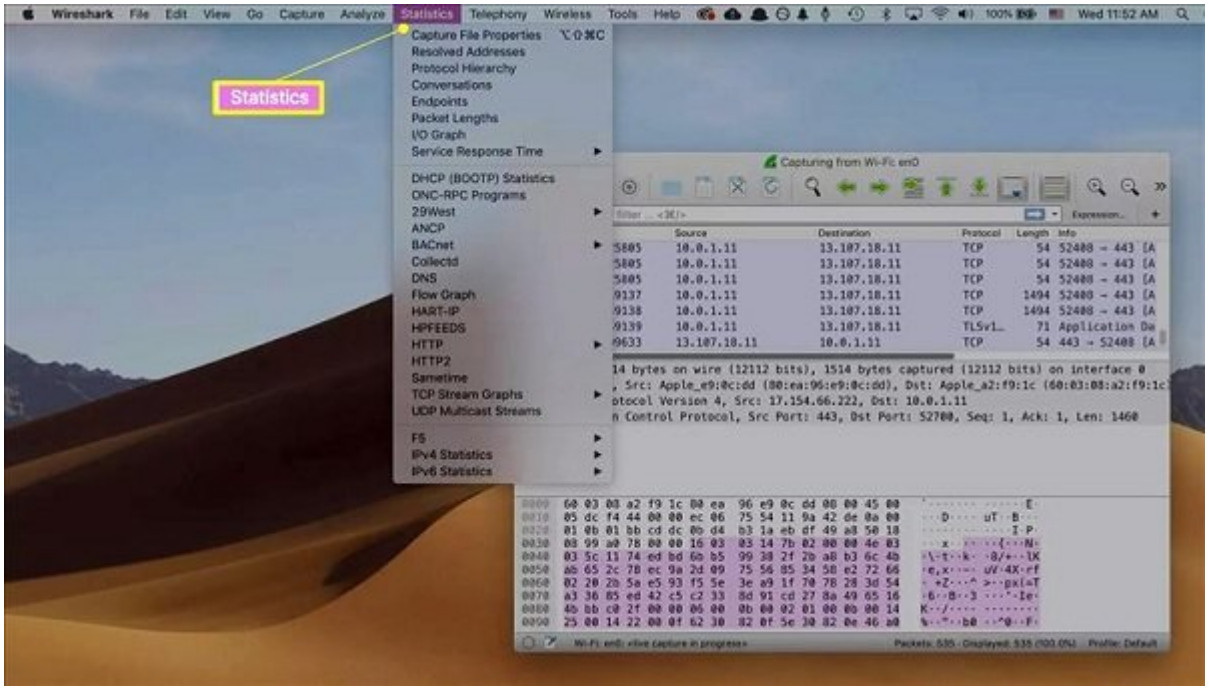
قاعده مربوط به رنگ‌ها

زمانی‌که از فیلترهای ضبط و نمایش **وایرشارک** برای محدودسازی فرآیند جمع‌آوری بسته‌ها استفاده می‌کنید، رنگ‌آمیزی ضبط و نمایش بسته‌ها متفاوت شده و معنای خاصی به خود می‌گیرند. (شکل 5) این رنگ‌آمیزی به شما اجازه می‌دهد تفاوت میان انواع مختلف بسته‌ها را به‌خوبی تشخیص دهید. ماحصل این تنوع رنگ در افزایش سرعت ذخیره‌سازی بسته‌ها در قالب یک مجموعه منحصربه‌فرد خلاصه‌شده است. **وایرشارک** نزدیک به 20 قاعده رنگ‌بندی پیش‌فرض در اختیار دارد که امکان ویرایش، حذف یا غیرفعال کردن هر یک از آن‌ها وجود دارد.



گزارش‌های آماری

علاوه بر اطلاعات بسیار دقیقی که همراه با جزییات در اختیار متخصصان قرار می‌گیرد، **وایرشارک** در پنجره اصلی خود چند معیار بیشتر برای ارائه آمارهای مفید ارائه می‌کند. این گزینه‌ها در منوی بازشونده Statistics که بالای صفحه قرار دارد، در دسترس است. (شکل 6) گزینه‌های این منو اطلاعات اندازه و زمان‌بندی ضبط بسته‌ها را درون فایل‌ها، دسترسی به ده‌ها نمودار تجزیه‌وتحلیل نشست‌ها در ارتباط با درخواست‌های توزیع بار HTTP، گزینه‌هایی برای بررسی دقیق آماری وضعیت بسته‌های رفت‌وبرگشتی در پروتکل TCP، نموداری در ارتباط با سامانه نام دامنه، نموداری برای پروتکل پیکربندی پویای میزبان و... شامل می‌شوند.



ویژگی‌های پیشرفته‌تر

در این مقاله سعی کردیم، بخشی از مهم‌ترین قابلیت‌های کاربردی **وایرشارک** را توضیح دهیم. اما در حقیقت **وایرشارک** دربرگیرنده مجموعه‌ای از قابلیت‌های اضافه و پیشرفته‌ای است که در شناسایی مشکلات شبکه کاربردی و مفید است و تنها راه تسلط بر این ابزار کار کردن با آن و مطالعه دقیق اطلاعاتی است که ارائه می‌کند و برای کار در شبکه چاره‌ای ندارید، جز این‌که با ابزارهای تخصصی این حوزه ازجمله **وایرشارک** آشنا باشید.

تاریخ انتشار:
08 مرداد 1398

نشانی منبع:
https://www.shabakeh-mag.com/cover-story/15701/%D8%B1%D8%A7%D9%87%D9%86%D9%85%D8%A7%DB%8C-%D8%AC%D8%A7%D9%85%D8%B9-%D8%A8%D9%87%E2%80%8C%DA%A9%D8%A7%D8%B1%DA%AF%DB%8C%D8%B1%DB%8C-wireshark-%D8%A8%D8%B1%D8%A7%DB%8C-%D9%86%D8%B8%D8%A7%D8%B1%D8%AA-%D8%A8%D8%B1-%D8%AA%D8%B1%D8%A7%D9%81%DB%8C%DA%A9-%D8%B4%D8%A8%DA%A9%D9%87%E2%80%8C%D9%87%D8%A7