

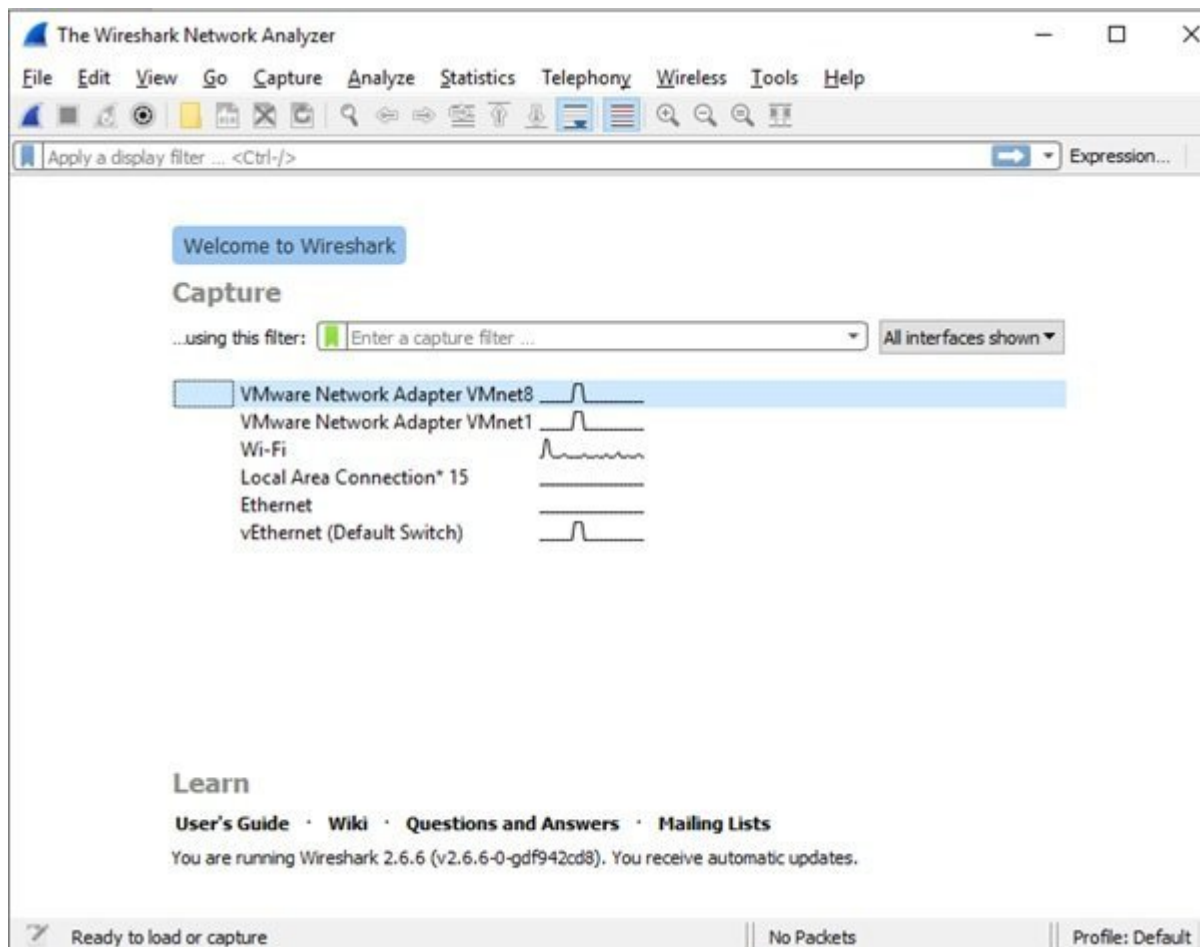


زمانی که داده‌های شبکه را با Wireshark و بر مبنای تنظیمات پیش‌فرض جمع‌آوری می‌کنید، اطلاعاتی در ارتباط با تولیدکننده کارت شبکه نیز جمع‌آوری شده و به شما اجازه می‌دهد اطلاعاتی درباره هر دستگاه به دست آورید.

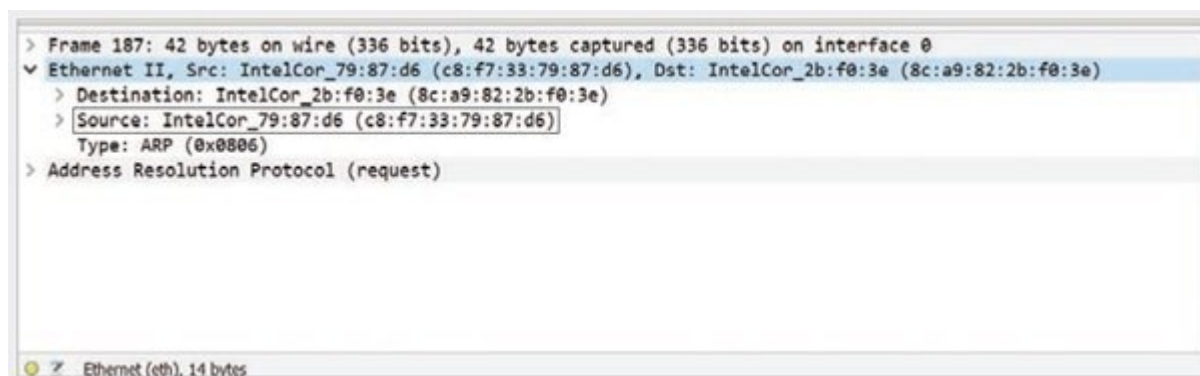
این مطلب بخشی از [سری آموزش‌های نتورک پلاس](#) است که بیشتر در سایت شبکه منتشر شده است. برای مشاهده فهرست و خرید کتاب Network+ راهنمای شبکه‌ها [اینجا](#) کلیک کنید.

شناسایی سازنده یک کارت شبکه

[Wireshark](#) یک ابزار تحلیل‌گر متن‌باز رایگان شبکه است که برای شناسایی پیام‌های شبکه و پیاده‌سازی یک مدل مبتنی بر OSI به کارشناسان شبکه کمک می‌کند. بیشتر بسته‌هایی که روی یک شبکه ارسال می‌شوند مک آدرس دریافت‌کننده، ارسال‌کننده یا هر دو را دارند. زمانی که داده‌های شبکه را با Wireshark و بر مبنای تنظیمات پیش‌فرض جمع‌آوری می‌کنید، اطلاعاتی در ارتباط با تولیدکننده کارت شبکه نیز جمع‌آوری شده و به شما اجازه می‌دهد اطلاعاتی درباره هر دستگاه به دست آورید. زمانی که ابزار فوق را دانلود کرده و اجرا کردید تصویری همانند شکل زیر مشاهده می‌کنید.



در شکل بالا برای مشاهده مک آدرس کافی است روی ارتباط فعال خود (وای فای یا سیمی) در تصویر بالا وای فای کلیک کنید. با کلیک روی این گزینه پنجره‌ای ظاهر می‌شود که فعالیت‌های انجام شده در شبکه را نشان می‌دهد. در پنل میانی این پنجره اطلاعاتی در ارتباط با وضعیت ارتباطات و پروتکل‌های استفاده شده نشان داده می‌شود. در این پنل اگر روی گزینه Ethernet II دوبار کلیک کنید تا باز شود، Wireshark مک آدرس کارت شبکه را مقابل فیلد Source همانند تصویر زیر نشان می‌دهد.



گاهی اوقات، مجبور هستید با آدرس‌های فیزیکی ارائه شده توسط یک فرمان خروجی کار کرده یا به اطلاعاتی فراتر از آنچه Wireshark ارائه می‌کند دسترسی داشته باشید. در چنین شرایطی بهتر است از جداول مک آدرس‌های آنلاین شبیه به Wireshark's OUI Lookup Tool استفاده کنید.

1. در شکل بالا مشاهده می‌کنید که آدرس MAC در فیلد source مشخص شده است. سه بایت اول این آدرس، c8:f7:33، OUI سازنده دستگاه را مشخص می‌کنند. اگر به سایت wireshark.org/tools/oui-lookup مراجعه کرده، این مقادیر را درون فیلد OUI search وارد کرده و دکمه Find را کلیک کنید، ابزار OUI Lookup Wireshark اطلاعات جالبی در اختیارتان قرار می‌دهد.

دسترسی به اطلاعات مک‌آدرس از طریق خط فرمان

2. برای مشاهده اطلاعات مک‌آدرس از طریق خط فرمان، پنجره Command Prompt را باز کرده و دستور ipconfig / all را برای شناسایی آدرس فیزیکی کارت شبکه وارد کنید.

3. برای انتخاب و کپی اطلاعات موردنیاز در کلیپ‌بورد، ابتدا Ctrl+M را برای فعال کردن علامت‌گذاری فشار دهید، سپس سه بایت اول از آدرس فیزیکی اتصال فعال شبکه را با ماوس انتخاب کرده و کلیدهای Ctrl+C را فشار دهید. (در پنجره خط فرمان سه بایت اول مک‌آدرس را کپی کنید.)

4. به فیلد جست‌وجوی وب‌سایت Wireshark (که در پاراگراف قبل با آن آشنا شدید) رفته و Ctrl+V را فشار دهید تا اطلاعات درون فیلد Wireshark Lookup Tool قرار گیرند، سپس روی Find کلیک کنید. چه شرکتی تولیدکننده کارت شبکه شما است؟

تاریخ انتشار:

18 دی 1398

نشانی منبع:

<https://www.shabakeh-mag.com/networking-technology/16170/%DA%86%DA%AF%D9%88%D9%86%D9%87-%D8%A8%D8%A7-wireshark-%D8%B3%D8%A7%D8%B2%D9%86%D8%AF%D9%87-%DB%8C%DA%A9-%DA%A9%D8%A7%D8%B1%D8%AA-%D8%B4%D8%A8%DA%A9%D9%87-%D8%B1%D8%A7-%D8%B4%D9%86%D8%A7%D8%B3%D8%A7%DB%8C%DB%8C-%DA%A9%D9%86%DB%8C%D9%85>