فصل



مانیتورینگ ترافیک

اهداف آموزشی

- آشنایی با امکانات ابزار Microsoft Network Monitor
- آشنایی با ویژگی‌های ابزار Wireshark
- به کارگیری ابزار Wireshark برای ضبط بسته‌های شبکه
- اعمال فیلترهای مختلف در زمان ضبط و نمایش ترافیک در Wireshark
- آشنایی با ابزار Ethereal در لینوکس
- نصب و راه‌اندازی ابزار PRTG
- به کارگیری امکانات PRTG برای مانیتور دستگاه‌های شبکه
- گزارش‌گیری با استفاده از PRTG

⊡ مقدمه

مانیتورینگ یا پایش شبکه یکی از مهمترین فعالیت‌های حساس تیم فناوری اطلاعات در یک سازمان محسوب می‌شود که به تنهایی می‌تواند باعث بالا رفتن کارایی سرویس‌ها و پرسنل، صرفه‌جویی در هزینه‌های سازمان و آرامش بخشیدن به مدیران شبکه شود. یک سیستم مانیتورینگ شبکه تمامی شبکه داخلی شما را برای پیدا کردن مشکلات پایش می‌کند، این سیستم می‌تواند به شما کمک کند میزان دانلود کاربران شبکه و استفاده آنها از اینترنت را بدانید، فضاهای اشغال شده توسط ایمیل‌های اسپم و کاربرانی که بیهوده ایمیل ارسال می‌کنند را شناسایی کنید، سرورهایی که در حال بروز مشکل هستند یا مشکل ایجاد خواهند کرد را شناسایی کنید، ترافیک شبکه را مشاهده کنید و موارد غیرعادی را در قالب گزارش ببینید و در کنار همه اینها علاوه بر نرم‌افزارها، سخت افزارهای موجود در شبکه را نیز پایش کنید. به صورت کلی شما می‌توانید با داشتن یک سیستم مانیتورینگ قوی در سازمان خود از تمامی اتفاقاتی که در شبکه خود چه از لحاظ نرم‌افزاری و چه از لحاظ سخت افزاری رخ می‌دهد آگاه شوید. یکی از مواردی که بعضاً مشاهده شده است اشتباه گرفتن سیستم‌های مانیتورینگ شبکه[1] یا NMSها با سیستم‌های تشخیص نفوذ یا IDSها و یا سیستم‌های جلوگیری از نفوذ یا IPSها است؛ توجه کنید که اینها کاملاً با هم متفاوت هستند. درست است که این سیستم‌ها نیز ترافیک شبکه را مانیتور می‌کنند اما هدف اصلی آنها شناسایی حملات هکری یا کدهای مخرب و جلوگیری از دسترسی‌های غیرمجاز است و با ذات کاری NMS تفاوت دارند. در واقع وظیفه اصلی یک سیستم جامع NMS بررسی کیفیت، وضعیت و کارایی شبکه شما در فعالیت‌های عادی و روزانه شبکه می‌باشد و هدف آن به صورت تخصصی امنیتی نیست، هر چند که بعضاً از آن به عنوان یک سیستم امنیتی نیز نام برده می‌شود.

---

1. Network Monitoring Systems

با استفاده از سیستم‌های مانیتورینگ شبکه، همه انواع شبکه‌ها را می‌توانیم مانیتور کنیم. برای یک سیستم جامع مانیتورینگ هیچ فرقی نمی‌کند که شبکه شما کابلی است یا بیسیم، شبکه شما یک LAN است یا یک WAN و یا شبکه موبایل است و یا ... همان طور که نوع شبکه در یک سیستم جامع مانیتورینگ شبکه چندان مهم نیست، نوع دستگاه‌های مورد استفاده در شبکه و همچنین نوع نرم‌افزارها و به‌ویژه سیستم‌عامل‌های مختلف به کار برده شده در شبکه نیز مهم نیستند، شما می‌توانید گوشی‌های هوشمند، سرورهای فیزیکی، سویچ‌ها، روترها، فایروال‌ها، Access Pointها، لینک‌های رادیویی، اطلاعات داخل Rack و انواع و اقسام تجهیزات سخت‌افزاری مورد استفاده در شبکه را در کنار سیستم‌عامل‌هایی مثل Android، ویندوز، لینوکس، Mac و ... مانیتور کنید. یک سیستم مانیتورینگ در یک شبکه طراحی و پیاده‌سازی می‌شود تا بر اساس معیارهایی که از طرف مدیران شبکه تعریف می‌شوند وضعیت شبکه را آنالیز کند و به شما گزارش دهد. با استفاده از این گزارش شما به عنوان مدیر شبکه می‌توانید نیازهای سازمانی خود را تخمین بزنید، مشکلات شبکه خود را متوجه شوید و قبل از بروز مشکلات حاد از آنها جلوگیری کنید؛ تهدیدات امنیتی را قبل از بروز مشکل شناسایی و رفع کنید و در نهایت روند کاری شبکه خود را به صورت گرافیکی و ملموس مشاهده نمایید.

⊡ برنامه Microsoft Network Monitor

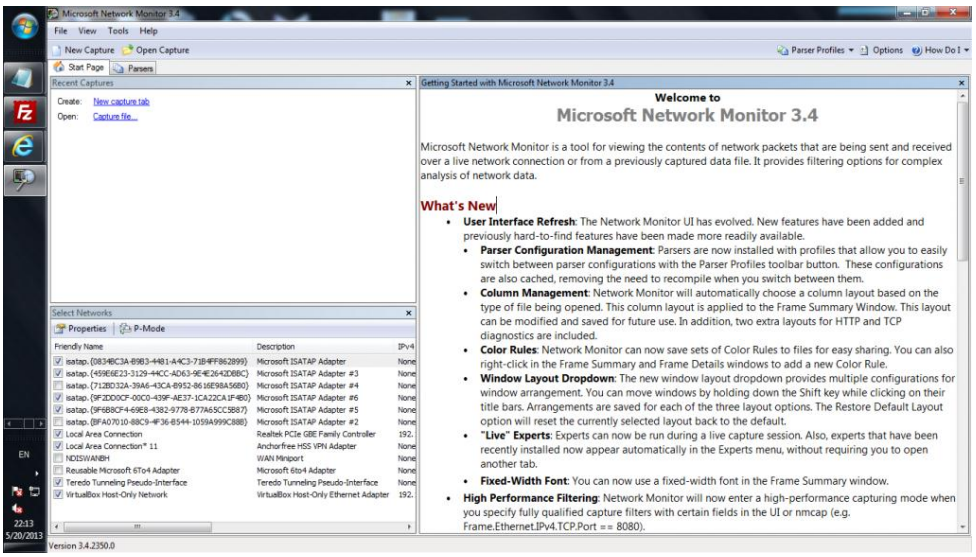
با استفاده از برنامه Microsoft Network Monitor می‌توان به رصد، آنالیز و Capture ترافیک شبکه پرداخت. این برنامه همچنین قابلیت‌های متعددی برای پروتکل‌های مختلف شبکه در خود گنجانده است؛ از جمله:

- ❖ Capture کردن داده‌های شبکه؛
- ❖ ذخیره‌سازی داده‌های Capture شده؛
- ❖ ساخت Cheat Sheet؛
- ❖ سفارشی‌سازی تنظیمات Capture؛
- ❖ نمایش فریم‌های خاصی از اطلاعات؛
- ❖ بهینه‌سازی شکل نمایش داده‌ها؛

- ❖ یافتن داده‌های مورد نظر؛
- ❖ ایجاد فیلترهای سفارشی و فیلترهای توکار؛
- ❖ افزودن رنگ مناسب به هر یک از فیلترها؛
- ❖ افزودن کامنت؛
- ❖ تنظیمات ویژه پروتکل‌های پایه شبکه مثل: ARP، DHCP، SMB؛
- ❖ قابلیت‌های پیشرفته DNS مثل: Forward کردن Queryهای DNS و Forwarding شرطی؛
- ❖ امکانات تحت خط فرمان.

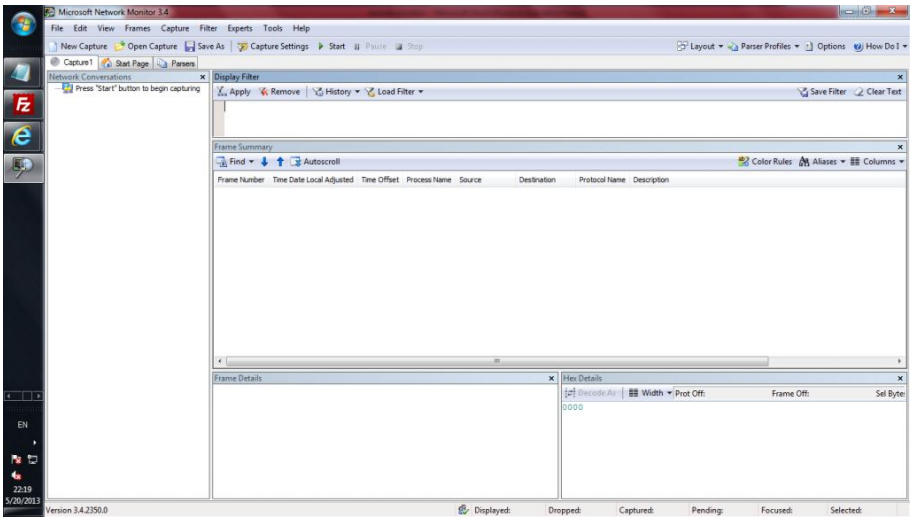
❐ روش استفاده از برنامه Microsoft Network Monitor

پس از باز نمودن برنامه، صفحه‌ای مانند شکل ۱ نمایش داده می‌شود.



شکل ۱- برنامه Microsoft Network Monitor

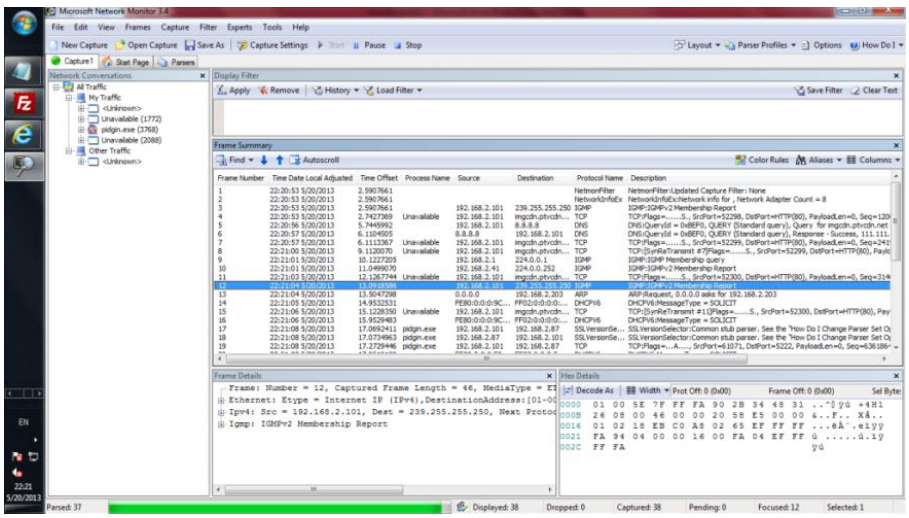
از لیست حاضر ترافیک شبکه‌هایی که نیاز به بررسی آن را دارید انتخاب، سپس از کادر بالا در سمت چپ بر روی گزینه New capture Tab کلیک نمایید؛ صفحه‌ای مانند شکل ۲ به تب‌های شما اضافه می‌گردد.



شکل ۲- برنامه Microsoft Network Monitor

با انتخاب گزینه start یا فشردن دکمه f5 کلیه ترافیک مبادله شده بر روی کارت‌های شبکه انتخاب شده در مرحله قبل به نمایش در می‌آید.

در کادر Network Conversation لیست سرویس‌های فعال که از ترافیک شبکه استفاده می‌کنند، مشاهده می‌کنید. با انتخاب هر یک از سرویس‌های موجود در کادر Summary Frame لیست Frameهای مبادله شده توسط آن سرویس را مشاهده می‌نمایید.

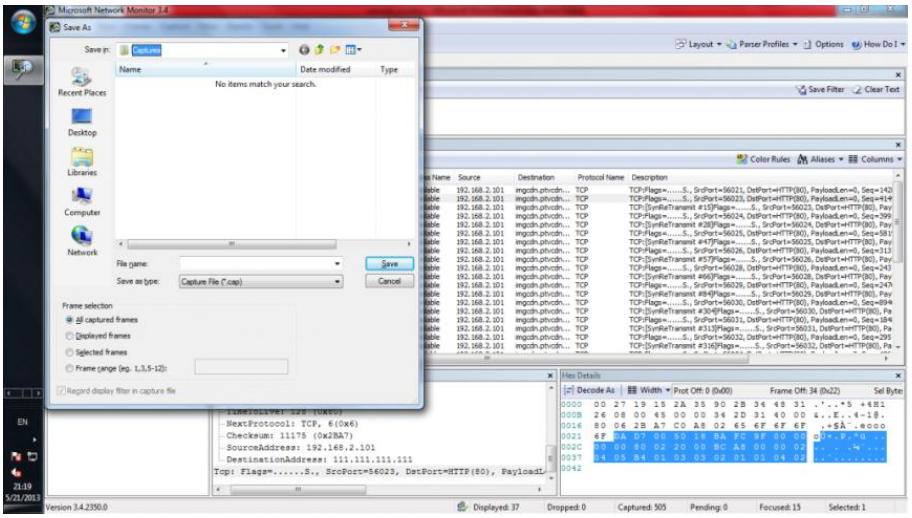


شکل ۳- برنامه Microsoft Network Monitor

با انتخاب هر یک از فریم‌ها، اطلاعاتی همچون زمان ارسال، IP مبدا، IP مقصد، پروتکل استفاده شده و همچنین توضیحاتی درباره Frame انتخاب شده نمایش داده می‌شود. از طریق کادرDisplay Filter می‌توانید فیلترهای لازم برای نمایش Frameهای موردنیاز خود را اعمال نمایید.

با انتخاب گزینه save as می‌توانید کل ترافیک مبادله شده از زمان شروع capture را در یک فایل ذخیره نمایید. این عمل برای شناسایی نقاط آسیب‌پذیر سیستم در هنگام حمله بر روی سرور بسیار مفید است، زیرا در مواقع لزوم می‌توانید ترافیک ذخیره شده در این برنامه و یا برنامه‌های مشابه را بررسی نموده و نقاط ضعف سیستم را کشف کنید.

پس از اتمام عملیات Capture، می‌توانید بر روی گزینه Stop کلیک، سپس گزینه Save as را انتخاب نمایید.



شکل ۴- برنامه Microsoft Network Monitor

می‌توانید فایل را با پسوند cap. ذخیره نمایید. این فایل را می‌توان به عنوان ورودی برنامه‌هایی مانند snort استفاده کرد، تا در صورت بروز حمله بر روی شبکه از نوع آن و IP (های) مشکل‌ساز آگاه شد.

⊡ ابزار Wireshark

برنامه Wireshark تحلیلگر بسته‌های شبکه است. یک تحلیل‌کننده بسته‌های شبکه سعی در ضبط بسته‌های شبکه دارد و تلاش می‌کند جزئیات آن بسته‌ها را تا جای ممکن به دست آورده و به ما ارائه دهد. می‌توان تحلیلگر بسته‌های شبکه را به مانند ابزار اندازه‌گیری فرض کرد که برای بازدید

کردن درون یک کابل شبکه رخ می‌دهد، به کار می‌روند. به احتمال زیاد، امروزه Wireshark یکی از بهترین تحلیلگران بسته‌های شبکه متن باز موجود است.

در اینجا مثال‌هایی از مواردی که در آنها از Wireshark استفاده می‌شود آمده است:

- مدیران شبکه از آن برای از بین بردن مشکلات به وجود آمده در شبکه استفاده می‌کنند.
- مهندسین امنیت شبکه آن را برای بازبینی مشکلات امنیتی شبکه استفاده می‌کنند.
- توسعه‌دهندگان برای اشکال زدایی پیاده‌سازی‌های پروتکل از آن استفاده می‌کنند.
- افراد از آن برای یادگیری کارکرد داخلی پروتکل استفاده می‌کنند.
- در کنار این مثال‌ها، در موقعیت‌های بسیار دیگری نیز Wireshark می‌تواند مفید واقع شود.

❐ ویژگی‌های Wireshark

موارد زیر برخی از ویژگی‌هایی است که Wireshark مجهز به آنها می‌باشد:

- ✧ قابل استفاده برای UNIX و Windows؛
- ✧ ضبط زنده بسته‌های داده از واسط شبکه؛
- ✧ نمایش بسته‌ها با جزئی‌ترین اطلاعات پروتکل؛
- ✧ باز کردن و ذخیره‌ی بسته‌های داده‌ای ضبط شده؛
- ✧ وارد کردن و صادر کردن بسته‌های داده از برنامه‌های دیگر؛
- ✧ فیلتر کردن بسته‌ها بر اساس معیارهای مختلف؛
- ✧ جستجوی بسته‌ها بر اساس معیارهای متفاوت؛
- ✧ رنگ‌آمیزی نمایش بسته‌ها براساس فیلترها؛
- ✧ ایجاد مدل‌های آماری مختلف؛
- ✧ رمزگشایی پروتکل‌های مختلف؛
- ✧ متن باز بودن نرم‌افزار؛
- ✧ و بسیاری از ویژگی‌های دیگر... .

❐ روش کار برنامه Wireshark

شنود ترافیک شبکه زمانی ممکن است که رابط شبکه (کارت شبکه) بر روی حالت انتقال بی‌قاعده قرار بگیرد. این حالت موجب می‌شود رابط شبکه تمامی ترافیک دریافتی را به جای فریمی که کنترل‌کننده برای دریافت در نظر گرفته بود، تماماً به واحد پردازش‌گر مرکزی انتقال دهد.

می‌توان شنود شبکه توسط Wireshark را به سه گام کلی تقسیم کرد که به شرح زیر هستند:

۱- جمع‌آوری: درگام اول، برنامه Wireshark رابط شبکه را به حالت بی‌قاعده انتقال می‌دهد، تا بتواند داده‌های باینری خام بر روی رسانه انتقال را دریافت کند.

۲- تبدیل: درگام دوم، داده‌های باینری جمع آوری شده، به یک قالب قابل فهم برای انسان تبدیل می‌شوند. همچنین بسته‌ها بر مبنای عدد سلسله مراتبی خود دوباره مونتاژ می‌گردند.

۳- تحلیل: گام آخر شامل تحلیل بسته‌های دریافت شده و داده‌های دوباره مونتاژ شده است. تحلیل اولیه بسته‌ها شامل شناسایی نوع پروتکل، کانال ارتباطی، شماره درگاه و... می‌شود. همچنین در یک سطح پیشرفته سرآیندهای متفاوت پروتکل می‌توانند برای یک درک عمیق‌تر مورد تحلیل قرار گیرند.

❐ نصب برنامه Wireshark

در اولین گام، نحوه نصب و راه‌اندازی محیط Wireshark را بررسی خواهیم کرد. در این قسمت ما روش نصب این برنامه بر روی لینوکس و ویندوز را نمایش خواهیم داد و در گام بعدی نحوه راه‌اندازی یک محیط Subversion برای به روزرسانی کتابخانه‌ها و اجزای مورد نیاز Wireshark را خواهیم آموخت.

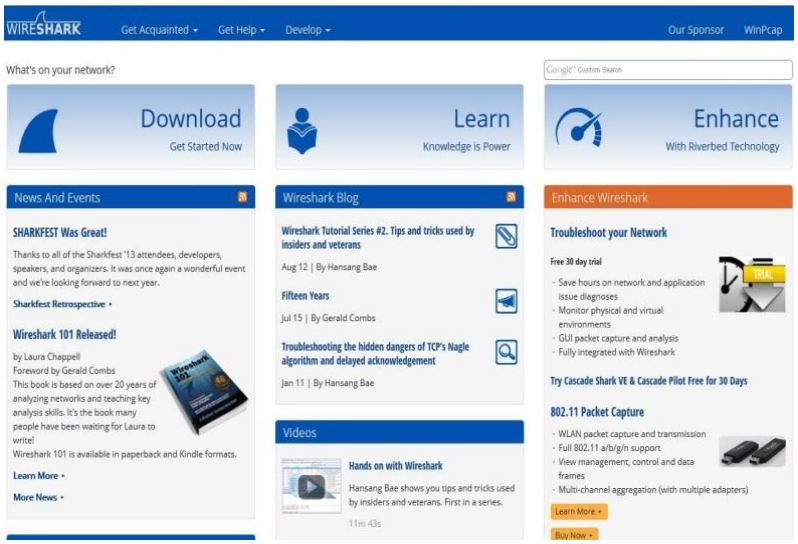
■ نصب برنامه Wireshark در ویندوز

برای نصب این برنامه نیاز به حداقل ۱۰۰ مگابایت فضای آزاد، همچنین مقداری فضا به منظور ذخیره‌سازی بسته‌های ضبط شده خواهیم داشت. علاوه بر این، به یک کارت شبکه[1] که حالت بی‌قاعده[2] را پشتیبانی کند و راه‌انداز WinPcap که در ضبط و شنود بسته‌های شبکه مورد استفاده قرار می‌گیرد، نیاز داریم.

در ابتدا بایستی این برنامه را دانلود کنیم. راحت‌ترین راه دانلود Wireshark برای سیستم عامل ویندوز، مراجعه به وب سایت http://www.wireshark.org و دریافت بسته فشرده شده آن برای سیستم عامل ویندوز، مطابق با معماری (x86 یا x64) و نسخه سیستم عامل است.

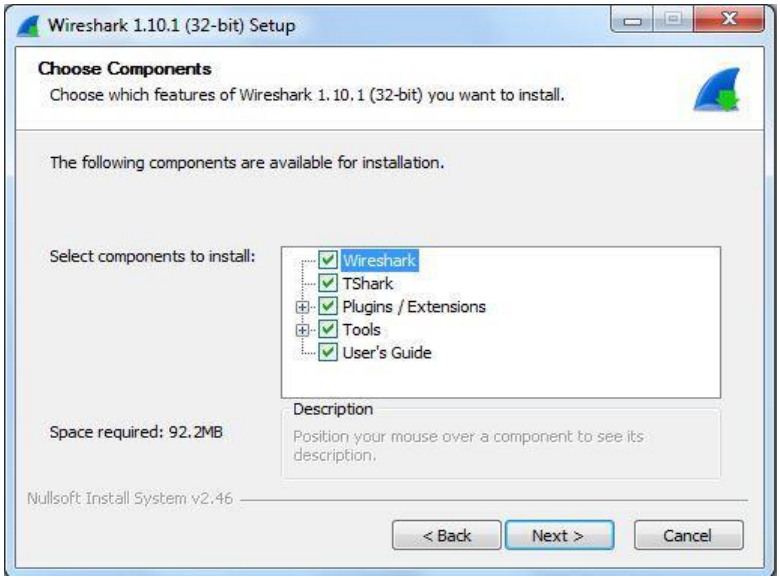
---

1. Network Interface Card
2. Promiscuous Mode



شکل ۵- سایت برنامه Wireshark

بعد از دانلود فایل برنامه، باید فایل installer برنامه Wireshark را اجرا کنید تا مراحل نصب یکی پس از دیگری انجام شود. البته در حین نصب نرم‌افزار، بسته نرم‌افزاری WinPcap نیز همراه با آن نصب می‌شود.



شکل ۶- نصب برنامه Wireshark

■ **نصب Wireshark بر روی لینوکس**

باید توجه داشت که همه توزیع‌های لینوکس از Wireshark پشتیبانی نمی‌کنند. شما می‌توانید لیست کامل توزیع‌های لینوکسی که از پروژه Wireshark پشتیبانی می‌کنند، در صفحه دانلود Wireshark که لینک آن در زیر آورده شده مشاهده کنید.

http://www.wireshark.org/download.html

■ **نصب Wireshark بر روی لینوکس از طریق کد منبع**

به منظور نصب Wireshark از طریق کد منبع آن بر روی سیستم عامل لینوکس، ابتدا بسته کد منبع برنامه را از صفحه دانلود که لینک آن در بالا ذکر شد، دانلود کنید. طبق شکل ۷ بر روی لینک Source Code کلیک کنید، تا کد منبع آن دانلود شود.



شکل ۷- نصب Wireshark در لینوکس

سپس با استفاده از دستور آورده شده در زیر، بسته wireshark با فرمت tar.gz را از حالت فشرده شده استخراج کنید.

Tar–xvf wireshark ۱.۱۰.۱-tar.bz2

بعد با دستور زیر به پوشه محتویات Wireshark بروید.

cd wireshark-۱.۱۰.۱

در این مرحله ما باید فایل‌های منبع را با استفاده از دستور make به حالت باینری تغییر بدهیم. سپس با استفاده از دستور install فایل‌های باینری را می‌توانیم بر روی سیستم نصب کنیم. به شکل زیر عمل کنید:

root:~/wireshark-/.#۱configure

root:~/wireshark-#۱make

root:~/wireshark-#۱make install

پس از اجرای فرامین بالا، برنامه Wireshark آماده استفاده در محیط لینوکس شما خواهد بود.

■ **نصب Wireshark از طریق بسته‌های نرم‌افزاری لینوکس**

شما می‌توانید با توجه به توزیع لینوکس خود فایل باینری مناسب آن را دانلود کرده و به سادگی آن را در سیستم راه‌اندازی کنید. البته در اینجا واژه باینری، فایل Exe در ویندوز نیست. منظور از فایل باینری، فایل اجرایی دودویی است که در سیستم عامل‌های گوناگون ساختار متفاوتی دارد.

■ **نصب Wireshark از طریق فایل باینری RPM**

برای نصب Wireshark بر روی سیستم عامل‌های مبتنی بر Red Hat نیاز داریم که فایل باینری rpm برنامه wireshark را از سایت آن دانلود کرده و سپس با دستور زیر آن را بر روی سیستم نصب و راه‌اندازی کنیم.

Rpm- ivh wireshark.۱.۹-i386.rpm

■ **نصب Wireshark از طریق فایل باینری DEB**

برای نصب برنامه wireshark بر روی سیستم عامل‌های مبتنی بر دبیان مانند سیستم عامل‌های Backtrack، Ubuntu، Backbox، نیاز به فایل‌های باینری DEB داریم. با دستور زیر برنامه Wireshark را بر روی این سیستم عامل‌ها نصب و راه‌اندازی کنید.

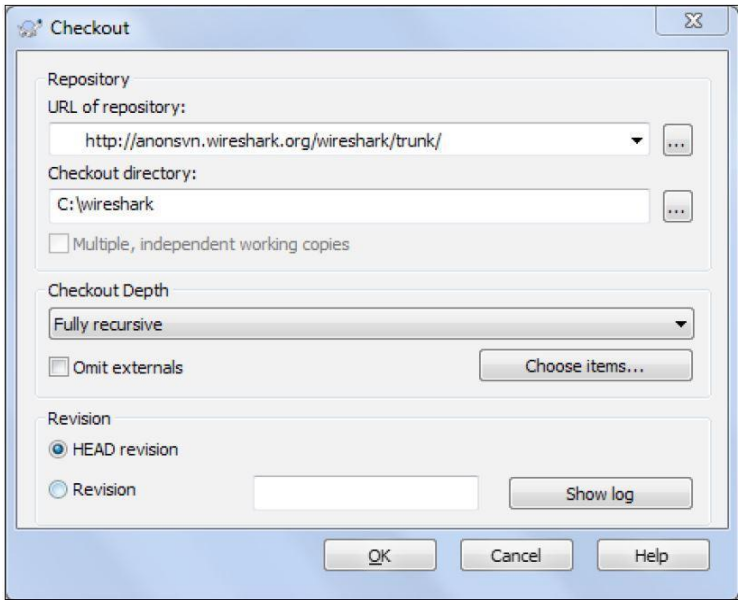
Apt-get install wireshark

```
root@bt:~/Desktop# apt-get install wireshark
Reading package lists... Done
Building dependency tree
Reading state information... Done
wireshark is already the newest version.
The following packages were automatically installed and are no longer required:
  libdmraid1.0.0.rc16 python-pyicu libdebian-installer4 cryptsetup libecryptfs0 reiserfsprogs rdate
  libdebconfclient0 dmraid keyutils
Use 'apt-get autoremove' to remove them.
0 upgraded, 0 newly installed, 0 to remove and 0 not upgraded.
root@bt:~/Desktop#
```

شکل ۸- نصب Wireshark از طریق فایل باینری DEB

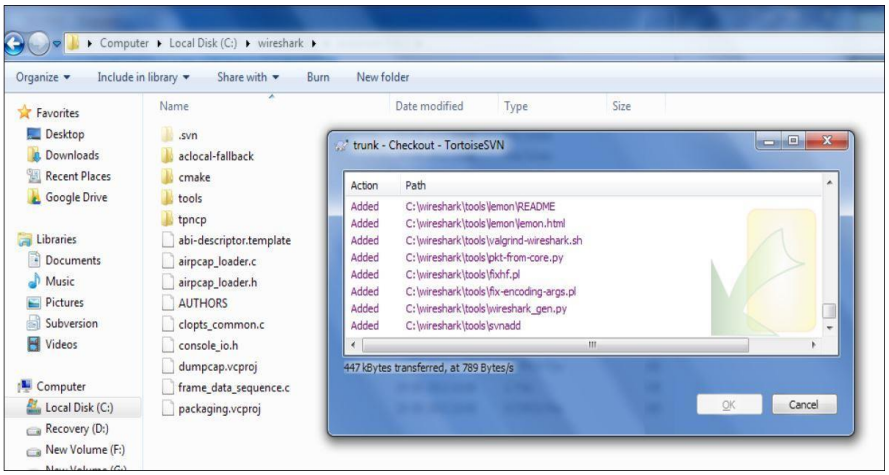
■ **نصب و راه‌اندازی Subversion**

نصب و راه‌اندازی subversion یک گزینه دلخواه برای افرادی است که قصد دارند Wireshark را از کد منبع آن نصب کنند. به این ترتیب می‌توانند در سریع‌ترین راه ممکن کتابخانه‌ها و فایل‌های برنامه را به روزرسانی کنند. بایستی ابتد راه انداز آن را از سایت http://tortoisesvn.tigris.org دانلود کنید. پس از نصب موفقیت آمیز برنامه بر روی هر پوشه‌ای که کلیک راست کنید گزینه‌های SVN را مشاهده خواهید کرد. به منظور راه‌اندزی Subversion برای Wireshark، ابتدا در سیستم پوشه‌ای با نام wireshark ایجاد کنید و سپس بر روی آن کلیک راست کرده و با کلیک کردن بر روی svn checkout آن را به svn منتقل کنید. سپس در پنجره جدید، در قسمت Url of Repository آدرس http://anonsvn.wireshark.org/wireshark/trunk را وارد کرده و در قسمت Checkout directory اطمینان حاصل کنید که مسیر درست پوشه wireshark که در مرحله قبل ایجاد کرده بوده‌اید، در این قسمت قرار دارد. سپس بر روی OK کلیک کنید تا فرایند به روزرسانی شروع گردد.



شکل ۹- نصب و راه‌اندازی subversion

هنگامی‌که Subversion شروع به پر کردن پوشه Wireshark می‌کند، مشاهده خواهید کرد که دایرکتوری‌های مختلفی ایجاد خواهند شد.

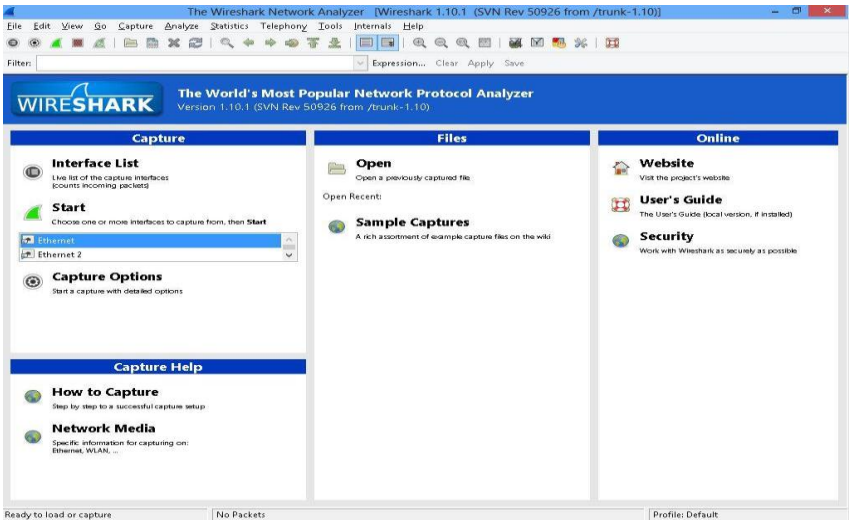


شکل ۱۰- نصب و راه‌اندازی subversion

حال کلاینت tortoise تنظیم شده است و شما می‌توانید در هر زمان با کلیک راست بر روی پوشه wireshark و انتخاب گزینه SVN update آن را به سرعت به روز رسانی کنید.

❐ شروع کار با برنامه Wireshark در ویندوز

اولین چیزی که در استفاده از Wireshark باید انجام بدهید، انتخاب رابط شبکه‌ای است که قصد دارید بسته‌های داده جاری در آن را ضبط کنید. محیط برنامه wireshark به شکل زیر است.



شکل ۱۱- برنامه wireshark در ویندوز