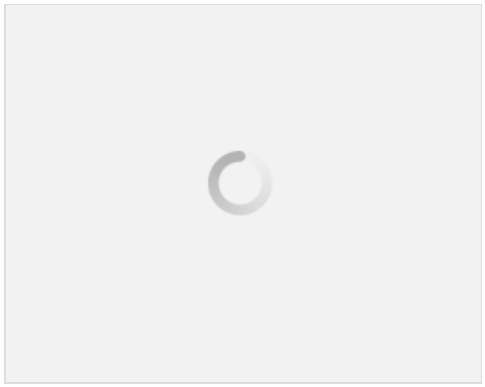
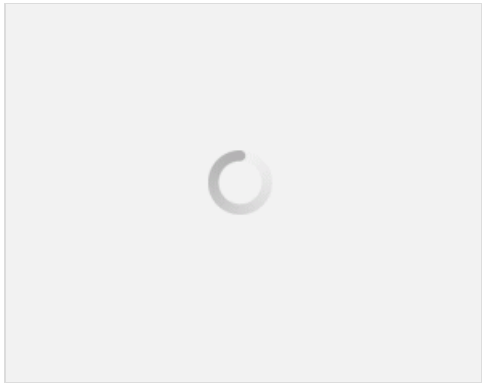
آموزش ذخیره خودکار Packet های شبکه در وایرشارک (WireShark) (نسخه PDF)

برای این کار از منوی ابزار Capture گزینه Option را انتخاب کنید تا پنچره Capture Option باز شود. در قسمت اول این پنچره لیست رابط های شبکه در دسترس را نمایش می دهد و میتوانید در صورت نصب چندین کارت شبکه در روی سیستم رابط مورد نظر را انتخاب کنید:



بعد از انتخاب رابط مورد نظر میتوانید تنظیمات زیر را اعمال کنید:

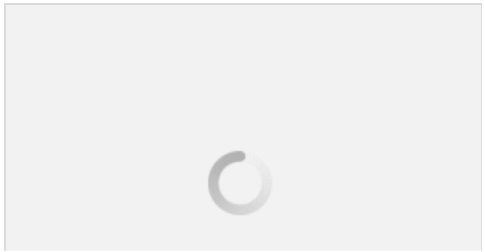


- Capture on all interfaces : با فعال کردن این گزینه برنامه قادر می شود بسته های چندین رابط را ضبط کند.
- Use promiscuous mode on all interfaces : با فعال کردن این گزینه برنامه قادر می شود به ضبط بسته ها در حالت بی قاعده.
- Capture Filter : در این قسـمت میتوانید سـربار یک شـبکه را با اعمال فیلتر حذف کنید . در این صورت فقط ترافیکی که میخواهید ضبط می شود.

نکته : به منظور انجام ضبط انتخابی باید دستور العمل های Winpcap را به WireShark عبور دهید.

- Compile selected BPFs : این گزینه پنچره کامپایل فلیتر ضبط بسته ها به صورت کد BPF نمایش می دهد.
- Manage Interfaces : برای مدیریت تنظیمات مربوط به رابط کاربری جدید استفاده می شود.

از قسمت زیر برای ذخیره سازی بسته های ضبط شده در یک پوش خاص است:

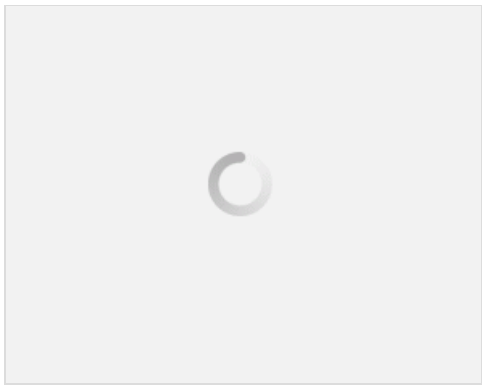


- پوشه (File): برای تعیین نام فایل و مسیر ذخیره بسته ها است . در صورت خالی گذاشتن این فیلد فایل ها بصورت موقت ذخیره خواهند شد.
- حالت استفاده از فایل های چندگانه (Use multiple files): برنامه در حالی که توسط موتور کتابخانه libpcap بسته های شبکه را در حال ضبط هست، بسته ها در بافر هم ذخیره می کند. حال برنامه این اطلاعات را می تواند به درخواست کاربر در محل مشخص ذخیره شود.در مورد فایل هایی با سایز بیشتر از ۱۰۰ مگا بایت ممکن است با سرعت کمی انجام شود. اگر قصد انجام یک ضبط طولانی مدت و یا ترافیک زیادی را دارید باید از حالت فایل های چندگانه (Multiple Files) استفاده کنید. با این کار بسته ی ضبط شده در چندین فایل کوچکتر ذخیره می شود که با گسترش ضبط این کار لذت بخش خواهد بود.
- حالت استفاده از فرمت Pcap-NG (Use pcap-ng format): این چک باکس این اجازه را به برنامه می دهد تا از فرمت پیش فرض خودش برای صرفه جویی در زمان استفاده کند. این فرمت در حال حاضر در حال توسعه است. برای اطلاعات بیشتر در مورد فرمت از به لینک زیر مراجعه کنید:

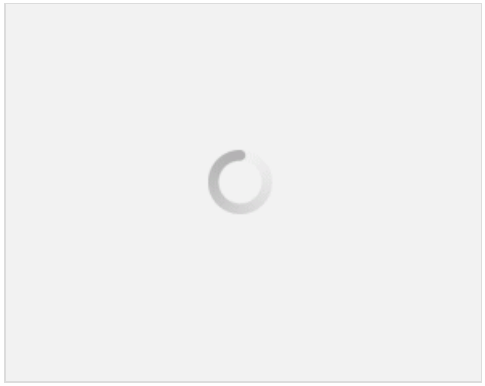
```
http://wiki.wireshark.org/Development/PcapNg
```

- Next file every n megabyte: تعیین سایز برای تغییر به فایل بعدی.
- Next file every n minute: تعیین زمان برای تغییر به فایل بعدی.
- Ring buffer with n files: تعیین تعداد فرم بافر حلقه برای تغییر به فایل بعدی.

قسمت زیر برای متوقف کردن عملیات ضبط بسته بعد از ضبط تعداد، حجم و زمان خاصی از فایل های چندگانه را امکان پذیر می کند:



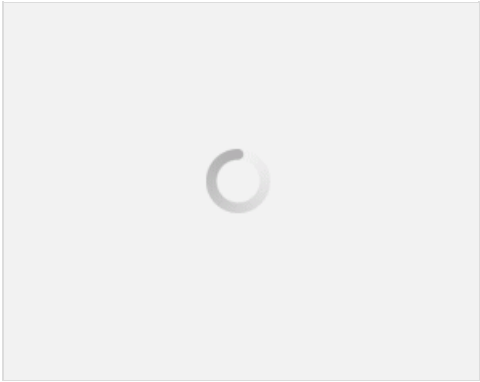
در قسمت زیر تنظیمات مربوط به نمایش فریم ها را میتوانید تعیین کنید:



- Update list of packets in real time: این گزینه برای بروز رسانی بسته ها در زمان واقعی را امکان پذیر می کند. در صورتی که این گزینه را انتخاب نکنید برنامه هیچ بسته ای را در رابط کاربری خود نمایش نخواهد داد.

- Automatic scrolling in live capture: از این گزینه برای نمایش جدید ترین بسـته های ضبط شده در رابط کاربری را امکان پذیر می کند.
- Hide capture info dialog: این گزینه نمایش اطلاعات مربوط به بسته های ضبط شده را امکانپذیر می کند.

در قسمت زیر می توانید تفکیک پذیری اسامی را در برنامه تغییر بدهید:



- Enable MAC name resolution: این گزینه ترجمه ادرس mac را برای شما امکان پذیر می کند.
- Enable network name resolution: این گزینه ترجمه ادرس شبکه را به نام شبکه امکان پذیر می کند.
- Enable transport name resolution: این گزینه ترجمه ادرس جابجایی بسته را به پروتکل ترجمه می کند.

در نهایت بعد از تعیین مقادیر بالا با انتخاب دکمه Start عملیات ضبط ها شروع خواهد شد .

منبع: ترجمه قسمت Capture Option از WireShark Users Guide .

بخاطر هر اشتباهی لطفا به بزرگواری خودتون منو ببخشین .

مصطفی عسکرنژاد

مطلب اصلی