آزمایشگاه تخصصی آپا در حوزه امنیت سرویس‌های شبکه و تجهیزات بی‌سیم

c e r t @ u m . a c . i r

معرفی ابزار Wireshark و نحوه استفاده از آن برای تحلیل ترافیک شبکه‌های محلی بی‌سیم

فاطمه دلدار

deldar@stu-mail.um.ac.ir

ویرایش اول – تیر ۱۳۸۸

شماره سند: APA_FUM_W_WIFI_0025

چکیده: گسترش استفاده از انواع مختلف شبکه‌های کامپیوتری باعث به وجود آمدن ابزارهای مختلف برای حمله به این شبکه‌ها شده است. ابزار Wireshark یکی از این ابزارهاست که کار استراق سمع و تحلیل بسته‌های شبکه را انجام می‌دهد. این ابزار به دلیل قابلیت‌هایی چون استفاده در شبکه‌های سیمی و بی‌سیم، واسط گرافیکی خیلی قوی و غیره مورد توجه زیاد قرار گرفته و به عنوان محبوب‌ترین ابزار در زمینه‌ی تحلیل بسته‌های شبکه شناخته شده است. در این مقاله به معرفی این ابزار، نحوه‌ی نصب و روش کار با واسط گرافیکی آن می‌پردازیم.

واژه‌های کلیدی: شبکه‌ی محلی بی‌سیم، استراق سمع، ضبط بسته، تحلیل ترافیک شبکه، Wireshark

۱- مقدمه

ابزار Wireshark یک استراق سمع کننده و تحلیل‌گر بسته‌های شبکه است. یک تحلیل‌گر بسته‌های شبکه تلاش می‌کند تا بسته‌ها را به دست آورده و جزئیات داده‌های آن‌ها را تا حد امکان نمایش دهد. این ابزار یکی از بهترین تحلیل‌گرهای بسته با کد منبع باز است که امروزه وجود دارد و در سطح گسترده‌ای (هم در شبکه‌های سیمی و هم در شبکه‌های بی‌سیم) از آن استفاده می‌شود. نسخه‌ی اصلی این ابزار با نام Ethereal وجود داشت که از سال ۲۰۰۶ به بعد این پروژه به Wireshark تغییر نام یافت.

Wireshark بسیار شبیه ابزار tcpdump است با این تفاوت که ابزار Wireshark واسط گرافیکی بسیار قوی داشته و اطلاعات خیلی بیشتری در زمینه‌ی مرتب‌سازی و فیلتر کردن بسته‌ها در اختیار کاربر قرار می‌دهد.

۲- خصوصیات

در این بخش برخی از ویژگی‌های ابزار Wireshark بیان می‌شود:

- نسخه‌های تحت ویندوز و یونیکس آن وجود دارد.
- بسته‌های داده‌ی دلخواه از یک واسط شبکه را ضبط می‌کند.
- بسته‌ها را با جزئیات دقیق اطلاعات پروتکلی آن‌ها نمایش می‌دهد.
- داده‌های بسته‌های گرفته شده را باز و ذخیره می‌کند.
- قابلیت وارد/خارج کردن داده‌های بسته‌ها را از/به برنامه‌های ضبط‌کننده‌ی دیگر دارد.
- می‌تواند عملیات فیلتر کردن بسته‌ها را بر اساس معیارهای زیادی انجام دهد.
- بر اساس معیارهای زیادی بر روی بسته‌ها جستجو انجام می‌دهد.
- بسته‌ها را بر مبنای نوع فیلتر آن‌ها به صورت رنگی نشان می‌دهد.
- اطلاعات آماری مختلفی را نشان می‌دهد.

در مقابل Wireshark محدودیت‌های زیر را دارد:

- Wireshark یک سیستم تشخیص نفوذ[1] نیست. این ابزار نمی‌تواند حضور شخصی غیرمجاز در شبکه را هشدار دهد و فقط می‌تواند در صورت کشف دسترسی آن چیزی را که اتفاق می‌افتد نشان دهد.
- Wireshark قابلیت دستکاری در شبکه را ندارد. این ابزار نمی‌تواند بسته‌ای روی شبکه ارسال کند یا عملیات فعال دیگری انجام دهد.

نکته: Wireshark بر روی سیستم‌عامل ویندوز (از ویندوز ۲۰۰۰ به بعد) و اکثر پلت‌فرم‌های یونیکس قابل اجراست.

نکته: Wireshark می‌تواند با یک کارت شبکه‌ی اترنت یا یک کارت شبکه‌ی محلی بی‌سیم کار کند.

[1] Intrusion Detection System (IDS)

۳- نصب

مراحل نصب ابزار Wireshark در سیستم عامل لینوکس در زیر آمده است.

تذکر: فایل منبع ابزار Wireshark از سایت آن (http://www.wireshark.org) به صورت رایگان قابل دانلود است.

۱. با استفاده از فرمان زیر فایل منبع را از حالت فشرده باز کنید.

```
tar zxvf wireshark-1.2.0-tar.gz
```

۲. مسیر خود را به پوشه‌ی منبع wireshark تغییر دهید.

۳. فایل منبع خود را پیکربندی کنید. این کار با استفاده از فرمان زیر انجام می‌گیرد:

```
./configure
```

۴. با فرمان زیر فایل‌های منبع را به صورت باینری درآورید.

```
make
```

۵. نرم‌افزار را در مقصد نهایی نصب کنید. این کار با فرمان زیر انجام می‌پذیرد:

```
make install
```

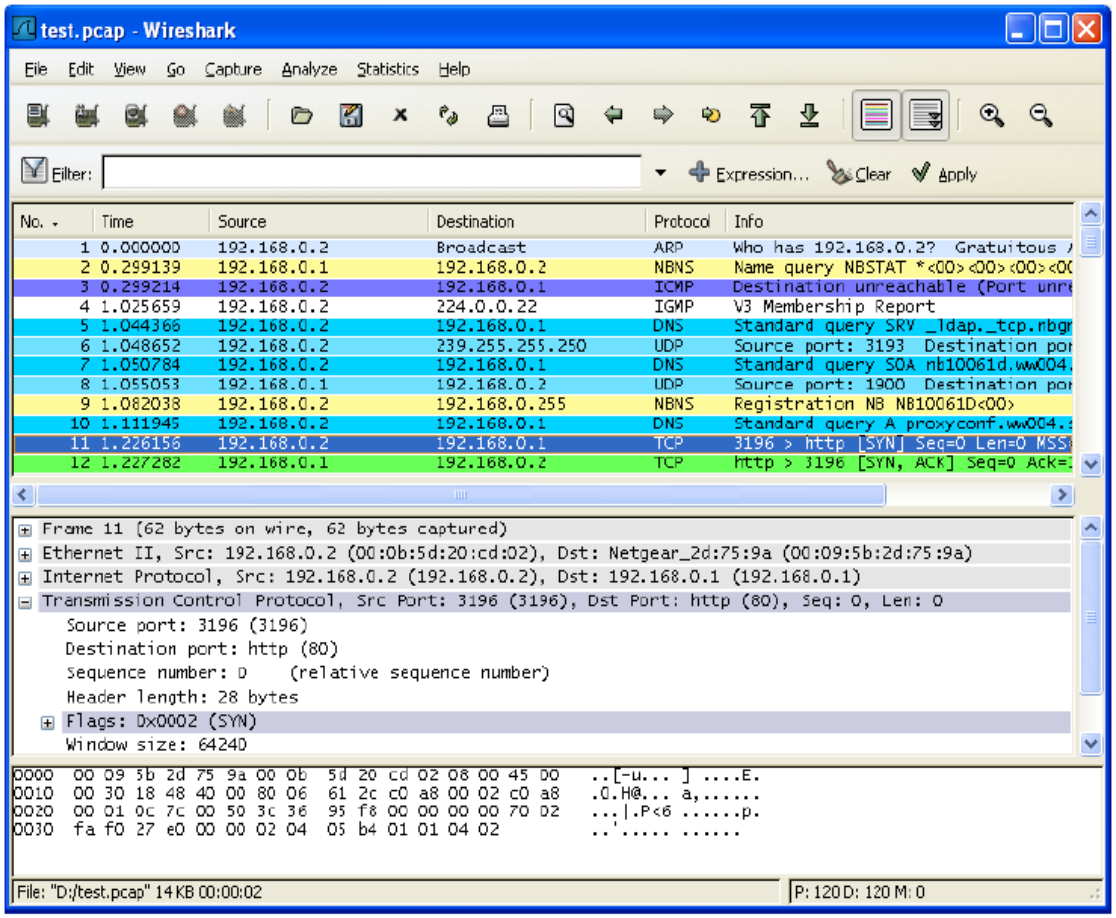
پس از نصب Wireshark می‌توان آن را با وارد کردن فرمان wireshark از طریق خط فرمان اجرا کرد.

٤- واسط کاربر

پس از اجرای Wireshark پنجره‌ی اصلی واسط کاربر آن نمایان می‌شود. این پنجره در شکل ۱ نمایش داده شده است.

صفحه‌ی اصلی Wireshark شامل قسمت‌های زیر است:

- Menu : برای شروع فعالیت‌ها استفاده می‌شود.
- Main Toolbar : امکان دسترسی سریع به آیتم‌هایی از منوها که بیشتر استفاده می‌شوند را فراهم می‌کند.
- Filter Toolbar : برای فیلتر کردن بسته‌های ضبط شده‌ی نشان داده شده در قسمت لیست بسته‌ها استفاده می‌شود.
- Packet List Pane : بسته‌های ضبط شده را به صورت خلاصه نشان می‌دهد. با کلیک کردن بر روی هر بسته در این قسمت می‌توان جزئیات آن را در دو قسمت بعد مشاهده کرد.
- Packet Details Pane : بسته‌ی انتخاب شده از قسمت قبل را با جزئیات بیشتر نشان می‌دهد.
- Packet Bytes Pane : داده‌ی بسته‌ی انتخاب شده در قسمت لیست بسته‌ها را نشان می‌دهد و فیلدهای انتخاب شده در قسمت جزئیات بسته را به صورت پررنگ‌تر نمایش می‌دهد.
- Statusbar : جزئیات اطلاعات در مورد وضعیت برنامه‌ی فعلی و داده‌های ضبط شده را نشان می‌دهد.



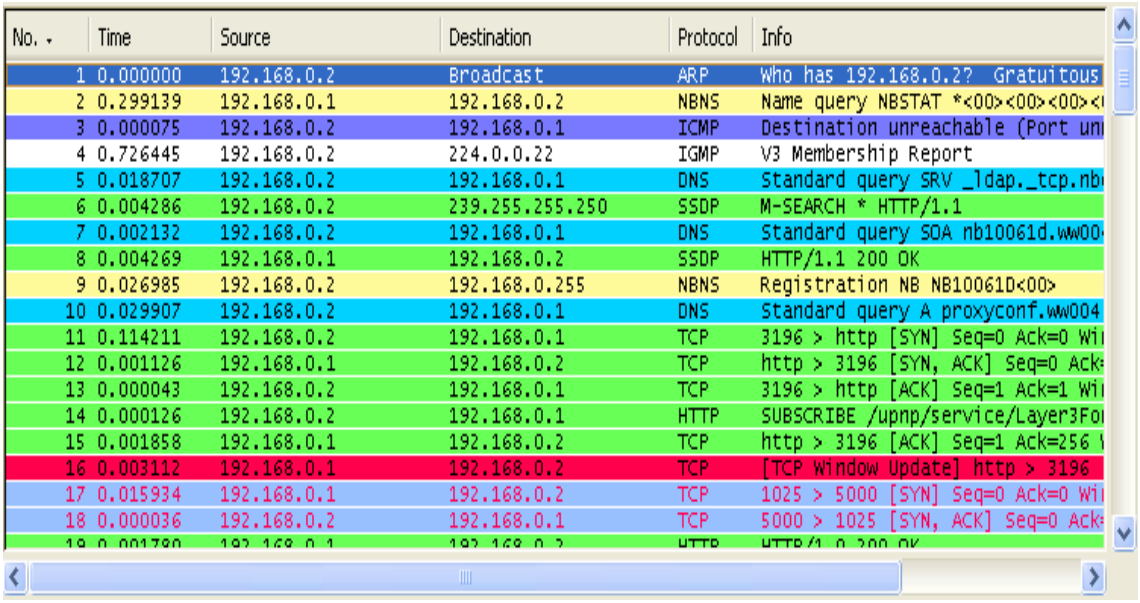
شکل ۱: صفحه اصلی Wireshark

سه قسمت اصلی این واسط در ادامه با جزئیات بیشتر آمده است.

Packet List –۱–٤

تمام بسته‌های موجود در فایل بسته‌های ضبط شده‌ی فعلی را نشان می‌دهد. جزئیات این قسمت در شکل ۲ نمایش داده شده است.

هر خط در لیست بسته‌ها یکی از بسته‌های موجود در فایل بسته‌های ضبط شده را نشان می‌دهد. اگر یک خط از این قسمت را انتخاب کنیم، جزئیات بیشتر در قسمت‌های Packet Details و Packet Bytes نشان داده می‌شود.



No.	Time	Source	Destination	Protocol	Info
1	0.000000	192.168.0.2	Broadcast	ARP	Who has 192.168.0.2? Gratuitous
2	0.299139	192.168.0.1	192.168.0.2	NBNS	Name query NBSTAT *<00><00><00><(
3	0.000075	192.168.0.2	192.168.0.1	ICMP	Destination unreachable (Port un
4	0.726445	192.168.0.2	224.0.0.22	IGMP	V3 Membership Report
5	0.018707	192.168.0.2	192.168.0.1	DNS	Standard query SRV _ldap._tcp.nb
6	0.004286	192.168.0.2	239.255.255.250	SSDP	M-SEARCH * HTTP/1.1
7	0.002132	192.168.0.2	192.168.0.1	DNS	Standard query SOA nb10061d.ww00
8	0.004269	192.168.0.1	192.168.0.2	SSDP	HTTP/1.1 200 OK
9	0.026985	192.168.0.2	192.168.0.255	NBNS	Registration NB NB10061D<00>
10	0.029907	192.168.0.2	192.168.0.1	DNS	Standard query A proxyconf.ww004
11	0.114211	192.168.0.2	192.168.0.1	TCP	3196 > http [SYN] Seq=0 Ack=0 Wi
12	0.001126	192.168.0.1	192.168.0.2	TCP	http > 3196 [SYN, ACK] Seq=0 Ack
13	0.000043	192.168.0.2	192.168.0.1	TCP	3196 > http [ACK] Seq=1 Ack=1 Wi
14	0.000126	192.168.0.2	192.168.0.1	HTTP	SUBSCRIBE /upnp/service/Layer3Fo
15	0.001858	192.168.0.1	192.168.0.2	TCP	http > 3196 [ACK] Seq=1 Ack=256
16	0.003112	192.168.0.1	192.168.0.2	TCP	[TCP Window Update] http > 3196
17	0.015934	192.168.0.1	192.168.0.2	TCP	1025 > 5000 [SYN] Seq=0 Ack=0 Wi
18	0.000036	192.168.0.2	192.168.0.1	TCP	5000 > 1025 [SYN, ACK] Seq=0 Ack

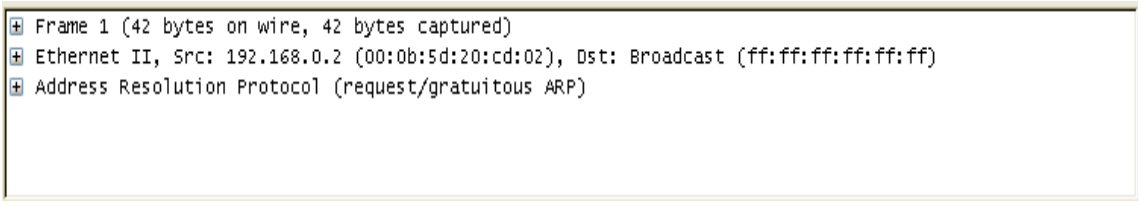
شکل ۲: قسمت Packet List از صفحه‌ی اصلی

ستون‌های پیش‌فرضی که در این قسمت نشان داده می‌شود به شرح زیر است:

- No: تعداد بسته‌های موجود در فایل بسته‌های ضبط شده.
- Time: مهر زمانی[1] هر بسته. فرمت نمایش این برچسب زمان را می‌توان تغییر داد.
- Source: آدرس منبع بسته.
- Destination: آدرس مقصد بسته.
- Protocol: نام پروتکل به صورت مخفف. چون پروتکل‌های سطح بالاتر اطلاعات پروتکل‌های سطح پایین‌تر را در بر می‌گیرند، در این ستون تنها نام سطح بالاترین پروتکل می‌آید.
- Info: اطلاعات اضافی در مورد محتوای بسته.

Packet Details -۲-٤

این بخش (شکل ۳) جزئیات بسته‌ی انتخاب شده در قسمت لیست بسته‌ها را نمایش می‌دهد.



شکل ۳: قسمت Packet Details از صفحه‌ی اصلی

[1] Timestamp

پروتکل‌ها و فیلدهای آن‌ها به ازای بسته‌ی انتخاب شده در قسمت لیست بسته‌ها در این قسمت نشان داده می‌شوند. این نمایش در یک ساختار درختی انجام می‌شود.

- Generated fields: Wireshark خود نیز فیلدهای پروتکلی اضافه‌ای را تولید خواهد کرد که این فیلدها داخل براکت قرار می‌گیرند. به عنوان مثال Wireshark یک تحلیل sequence/acknowledge از هر جریان TCP انجام می‌دهد که در فیلدهای [SEQ/ACK analysis] از پروتکل TCP نشان داده می‌شود.
- Links: اگر Wireshark رابطه‌ای بین بسته‌ی فعلی و بسته‌ی دیگری در فایل بسته‌های ضبط شده پیدا کند، یک لینک به آن بسته ایجاد می‌کند. لینک‌ها با رنگ آبی نشان داده می‌شوند که با کلیک بر روی آن‌ها Wireshark به بسته‌ی مورد نظر می‌رود.

Packet Bytes -۳-٤

این بخش (شکل ۴) داده‌ی بسته‌ی انتخاب شده در قسمت لیست بسته‌ها را در مبنای ۱۶ نشان می‌دهد.

```
0000  ff ff ff ff ff ff 00 0b  5d 20 cd 02 08 06 00 01   ........ ] ......
0010  08 00 06 04 00 01 00 0b  5d 20 cd 02 c0 a8 00 02   ........ ] ......
0020  00 00 00 00 00 00 c0 a8  00 02                    ........ ..
```

شکل ۴: قسمت Packet Bytes از صفحه‌ی اصلی

سمت چپ آفست بسته، قسمت وسط داده در مبنای ۱۶ و سمت راست کاراکترهای اسکی را نمایش می‌دهد.

۵- ضبط کردن بسته‌ها

ضبط کردن بسته‌های دلخواه، یکی از مهم‌ترین خصوصیات Wireshark است. موتور ضبط‌کننده در این ابزار دارای خصوصیات زیر است:

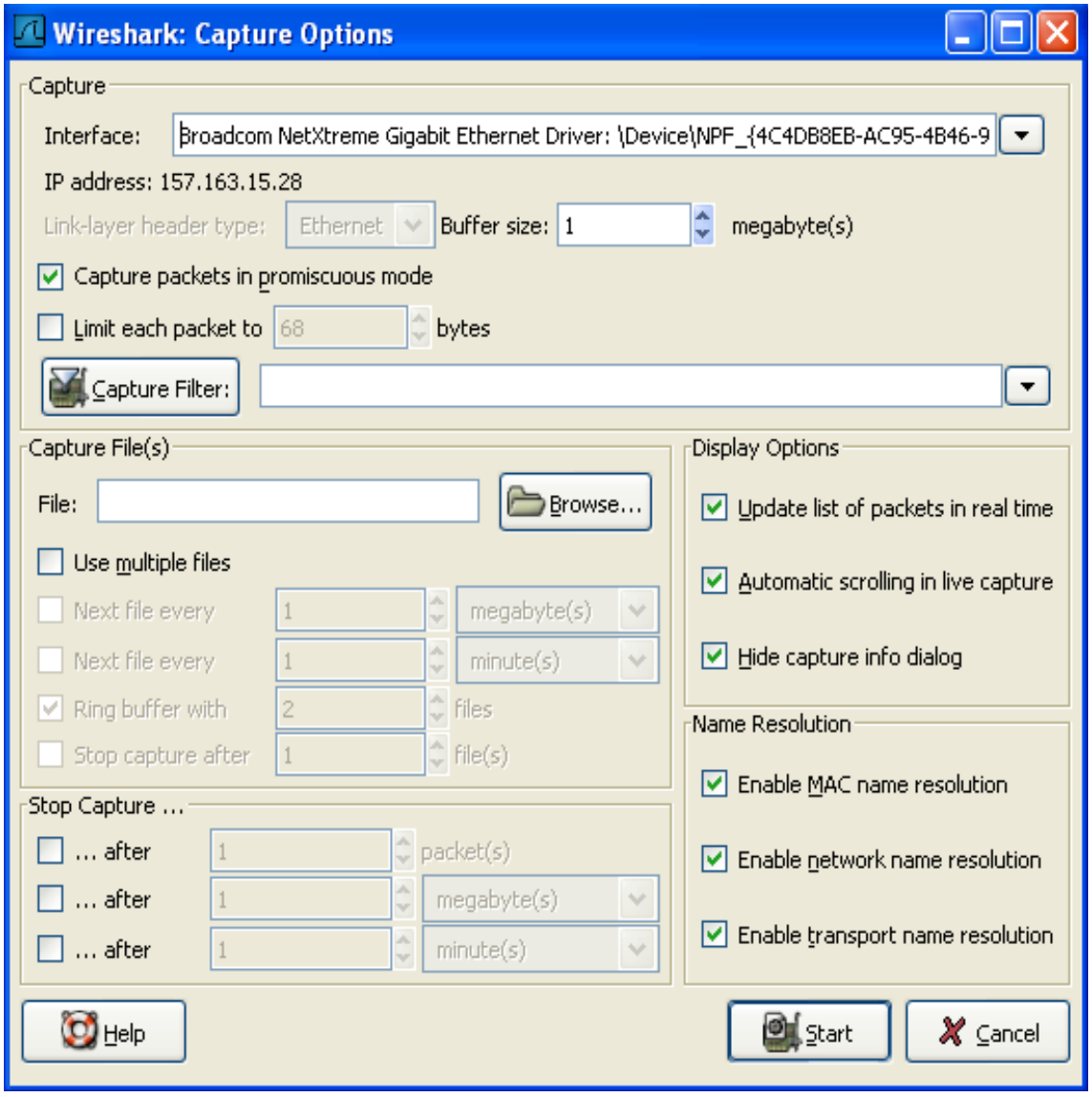
- ضبط بسته از انواع مختلف سخت‌افزارهای شبکه.
- امکان توقف ضبط با معیارهایی مانند: مقدار داده‌ی ضبط شده، زمان ضبط، تعداد بسته‌های ضبط شده.
- به طور همزمان می‌تواند بسته‌های رمزگشایی شده را در حین انجام عملیات ضبط نشان دهد.
- فیلتر کردن بسته‌ها و کاهش مقدار داده‌ی ضبط شده.
- ضبط کردن بسته‌ها در چندین فایل (وقتی عملیات ضبط به مدت زیادی طول بکشد).

با انتخاب گزینه‌ی Interfaces از منوی Capture، واسط ضبط کردن بسته‌ها باز می‌شود. این واسط (در سیستم عامل لینوکس) در شکل ۵ نمایش داده شده است.

شکل ۵: واسط ضبط کردن بسته‌ها در سیستم عامل لینوکس

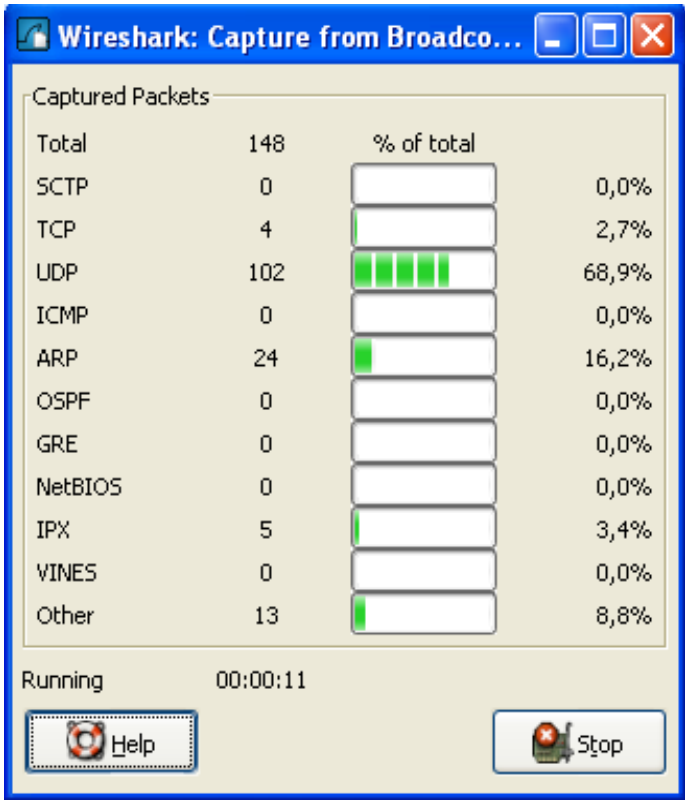
واسط ضبط کردن بسته‌ها شامل قسمت‌های زیر است:

- Device: نام وسیله‌ی واسط.
- Description: توصیف واسط که توسط سیستم عامل ایجاد می‌شود. البته کاربر می‌تواند به دلخواه این عبارت را تغییر دهد.
- IP: اولین آدرس IP که Wireshark بتواند از این واسط بگیرد. اگر Wireshark نتواند هیچ آدرس IP بگیرد (سرویس‌دهنده‌ی DHCP موجود نباشد)، عبارت unknown در این ستون نشان داده می‌شود. اگر بیشتر از یک آدرس IP نیز گرفته شود فقط آدرس اول نمایش داده می‌شود.
- Packets: تعداد بسته‌های ضبط شده از این واسط.
- Packets/s: تعداد بسته‌های ضبط شده در آخرین ثانیه.
- Stop: اجرای ضبط فعلی را متوقف می‌کند.
- Start: عملیات ضبط در این واسط را فوراً آغاز می‌کند (با استفاده از تنظیمات آخرین عملیات ضبط انجام شده).
- Options: پنجره‌ی Capture Options را باز می‌کند. این پنجره در شکل ۶ نمایش داده شده است.
- Help: صفحه‌ی help را نمایش می‌دهد.
- Close: پنجره را می‌بندد.



شکل ۶: پنجره‌ی Capture Options

در حین اجرای عملیات ضبط بسته‌ها پنجره‌ی Capture Info (شکل ۷) به کاربر نمایش داده می‌شود.



شکل ۷: پنجره‌ی Capture Info

این پنجره کاربر را از تعداد بسته‌های ضبط شده، زمان گذشته شده از آغاز ضبط بسته‌ها و غیره مطلع می‌کند.

٦- فیلتر کردن بسته‌ها

عملیات فیلتر کردن بسته‌ها در Wireshark به دو صورت قابل انجام است: یکی در هنگام انجام عملیات ضبط بسته‌ها و دیگری در هنگام مشاهده‌ی بسته‌ها (پس از اتمام عملیات ضبط).

٦-١- فیلتر کردن در هنگام ضبط بسته‌ها

به این منظور باید عبارت فیلتر را در فیلد Filter از پنجره‌ی Capture Options (نمایش داده شده در شکل ۶) وارد کرد. یک فیلتر ضبط کننده به شکل مجموعه‌ای از عبارات اولیه که با عملگرهای الحاقی (and یا or) به هم متصل شده‌اند، می‌باشد. به صورت اختیاری می‌توان از عملگر not در ابتدای عبارات اولیه استفاده کرد. شکل کلی یک فیلتر ضبط کننده به صورت زیر است:

[not] **primitive** [and|or [not] **primitive** ...]

مثالی از یک فیلتر ضبط کننده به صورت زیر می‌تواند باشد:

tcp port 23 and host 10.0.0.5

این مثال ترافیک telnet به/از میزبان 10.0.0.5 را ضبط می‌کند. مثال دیگری که در ادامه آمده است نشان می‌دهد که چگونه همه‌ی

ترافیک telnet به جز بسته‌هایی که از میزبان 10.0.0.5 می‌آیند را ضبط کنیم.

tcp port 23 and not src host 10.0.0.5

٦-٢- فیلتر کردن در هنگام نمایش بسته‌ها

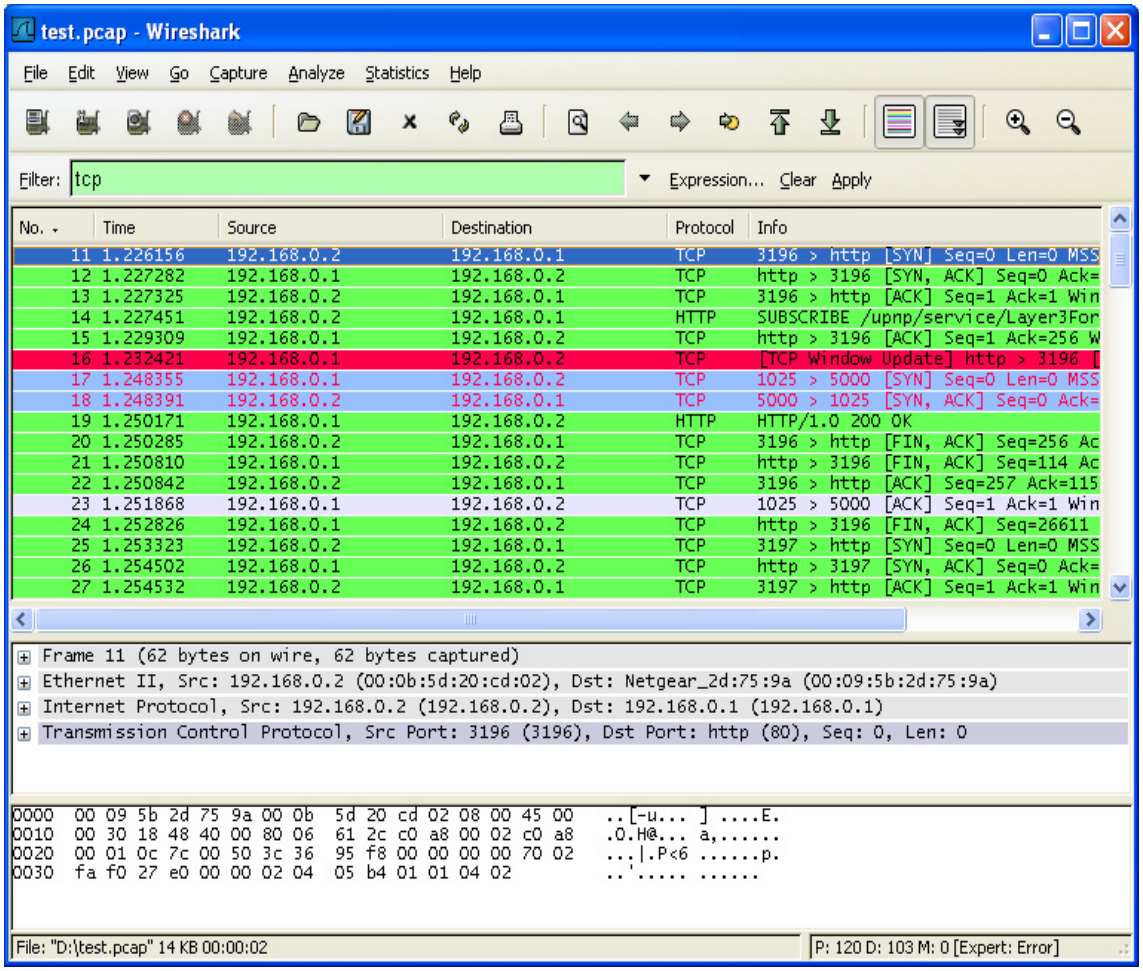
فیلتر کردن در هنگام نمایش بسته‌ها به ما این امکان را می‌دهد که روی بسته‌های مورد نظر خود متمرکز شویم و بقیه‌ی بسته‌ها غیر از بسته‌های مورد نظر از دید ما پنهان می‌شوند. در این نوع فیلتر کردن امکان انتخاب بسته‌ها به‌وسیله‌ی معیارهای زیر وجود دارد:

- پروتکل
- وجود یک فیلد خاص در بسته
- مقدار فیلدها
- مقایسه‌ی بین فیلدها
- و ...

به عنوان مثال برای انتخاب بسته‌ها بر مبنای نوع پروتکل، به سادگی می‌توان نام پروتکل مورد نظر را در قسمت Filter از نوارابزار فیلتر در پنجره‌ی اصلی Wireshark وارد کرد و پس از فشردن کلید Enter عملیات فیلتر کردن بسته‌ها بر روی آن پروتکل خاص انجام می‌شود. شکل ۸ مثالی از فیلتر کردن بسته‌ها بر روی پروتکل tcp را نمایش می‌دهد.

همان‌گونه که در شکل مشاهده می‌شود تعداد بسته‌ها تغییری نکرده و اولین بسته از شماره‌ی ۱۱ شروع می‌شود (بسته‌های ۱۰-۱ پنهان شده‌اند).

نکته: زمانی که از فیلتر کردن در هنگام نمایش بسته‌ها استفاده می‌کنیم، همه‌ی بسته‌ها در فایل بسته‌های ضبط شده باقی می‌مانند. این نوع فیلتر کردن فقط نمایش بسته‌های ضبط شده را تغییر می‌دهد نه محتوای فایل را.



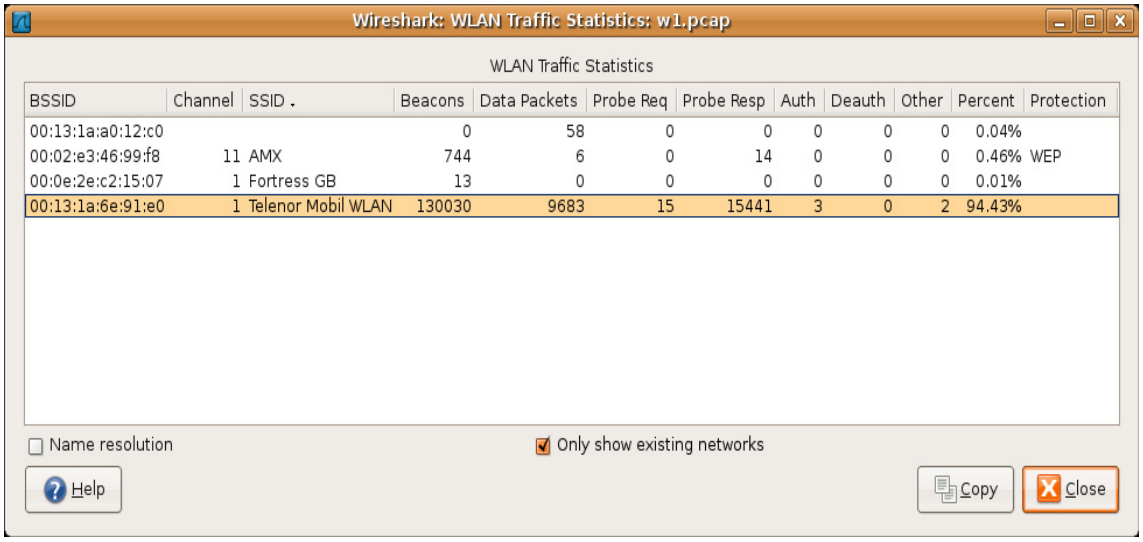
شکل ۸: فیلتر کردن بسته‌ها بر روی پروتکل tcp

Wireshark محدوده‌ی وسیعی از اطلاعات آماری شبکه را فراهم می‌کند که این اطلاعات از طریق منوی Statistics قابل دسترسی است. این اطلاعات آماری شامل اطلاعلت کلی در مورد فایل بسته‌های ضبط شده و اطلاعات در مورد پروتکل‌های خاص است. برخی از این اطلاعات در زیر آمده است:

- Summary: خلاصه‌ای در مورد فایل بسته‌های ضبط شده.
- Protocol Hierarchy: ساختار سلسله‌مراتبی پروتکل‌ها در بسته‌های ضبط شده.
- Conversations: مانند ترافیک بین آدرس‌های IP خاص.
- Endpoints: مانند ترافیک به/از یک آدرس IP خاص.
- IO Graphs: نمایش تعداد بسته‌ها (یا مقادیری از این قبیل) در واحد زمان.
- Service Response Time: زمان پاسخگویی سرویس بین درخواست و پاسخ بعضی از پروتکل‌ها.
- و ...

۶-۳- WLAN Traffic Statistics

یکی از گزینه‌های موجود در منوی Statistics از صفحه‌ی اصلی Wireshark، گزینه‌ی WLAN Traffic Statistics است. در این قسمت اطلاعات آماری ترافیک‌های شبکه‌های محلی بی‌سیم ضبط شده نشان داده می‌شود. این پنجره ترافیک شبکه‌های بی‌سیم پیدا شده در حین عملیات ضبط کردن را به صورت خلاصه نشان می‌دهد. پنجره‌ی WLAN Traffic Statistics در شکل ۹ نمایش داده شده است.



شکل ۹: پنجره‌ی WLAN Traffic Statistics

هر سطر در لیست نشان داده شده در شکل فوق، نشان دهنده‌ی مقادیر آماری برای یک شبکه‌ی بی‌سیم خاص است.

- Name resolution: در صورتی انجام خواهد شد که علاوه بر انتخاب شدن در این صفحه، در لایه‌ی MAC نیز فعال شده باشد.
- Only show existing networks: با انتخاب این گزینه درخواست‌های تفحصی که SSID آن‌ها با یکی از SSIDهای موجود در لیست منطبق نیست، نادیده گرفته می‌شوند.

۷- مراجع

[1] Ulf Lamping, Richard Sharpe, and Ed Warnicke, “Wireshark User's Guide: 29077 for Wireshark 1.2.0”, 2008.

[2] J.F. Kurose, K.W. Ross, “Wireshark Lab: Getting Started”, 2007.

[3] Wireshark, http://www.wireshark.org/