

به نام خدا

عنوان: مطالعه و بررسی دو نرم افزار مانیتورینگ و مدیریت شبکه ی Wireshark

فهرست مطالب

۱	مقدمه
۲	بخش اول
۲	معرفی ابزار Wireshark
۲	برخی از اهداف مورد نظر Wireshark
۳	ویژگی ها
۴	آنچه Wireshark پشتیبانی نمی کند
۵	نحوه ی نصب WireShark
۶	ایترفیس کاربر
۸	منو
۹	صفحه ی لیست پکت
۱۰	صفحه ی جزئیات پکت
۱۱	صفحه ی بایت های پکت
۱۲	Statusbar
۱۳	طریقه ی ضبط نمودن داده های در جریان شبکه

۱۵	آغاز ضبط اطلاعات
۱۵	پنجره ی Capture Interfaces
۱۷	پنجره ی Capture Options
۲۲	جعبه ی محاوره ی Interface Details
۲۳	ضبط فایل ها
۲۵	فیلتر کردن حین ضبط اطلاعات
۲۶	فایل ها (ورودی/خروجی) و پرینت
۳۱	صدور اطلاعات از Wireshark
۳۶	کارکردن با پکت های ضبط شده
۳۶	دیدن پکت های ضبط شده
۵۴	فیلترکردن پکت ها در حال دیدن
۵۵	ایجاد display filter expressions
۶۶	آمار
۶۷	پنجره ی Summary
۶۸	پنجره ی Protocol Hierarchy
۷۰	پنجره ی Conversations
۷۱	پنجره ی Conversation List برای پروتکل مشخص

۷۱	Endpoints پنجره‌ی
۷۳	Endpoint List برای پروتکل مشخص پنجره‌ی
۷۳	IO Graphs پنجره‌ی
۷۵	WLAN آمار ترافیک
۷۷	Service Response Time DCE-RPC پنجره‌ی
۷۸	پنجره‌ی آمارها برای یک پروتکل مشخص
Error! Bookmark not defined.	نتایج بدست آمده
Error! Bookmark not defined.	بررسی شبکه‌ی دانشگاه امیر کبیر
Error! Bookmark not defined.	بررسی شبکه‌ی شرکت پرورش داده‌ها
Error! Bookmark not defined.	Dial-up بررسی یک ارتباط
Error! Bookmark not defined.	بخش دوم
Error! Bookmark not defined.	مطالعه و بررسی نرم افزار Axence
۷۹	منابع

فهرست اشکال

- شکل ۱: Wireshark بسته ها را ضبط می کند و امکان بازدید محتوای آنها را می دهد ۴
- شکل ۲: پنجره ی اصلی ۷
- شکل ۳: منو ۸
- شکل ۴: صفحه ی لیست پکت ۹
- شکل ۵: صفحه ی جزئیات پکت ۱۱
- شکل ۶: صفحه ی بایت های پکت ۱۲
- شکل ۷: Statusbar اولیه ۱۲
- شکل ۸: statusbar با یک فایل لود شده ۱۲
- شکل ۹: Statusbar با منوی پروفایل پیکربندی ۱۳
- شکل ۱۰: Statusbar با یک پیام display filter ۱۳
- شکل ۱۱: پنجره ی واسطه های ضبط ۱۵
- شکل ۱۲: طریقه ی مخفی نمودن یک کارت شبکه از دید Wireshark ۱۷
- شکل ۱۳: پنجره ی Capture Options ۱۸
- شکل ۱۴: جعبه ی محاوره ی "Interface Details" ۲۳
- شکل ۱۵: پنجره ی باز کردن یک فایل ضبط شده ۲۶
- شکل ۱۶: پنجره ی ذخیره ی فایل ۲۸

۳۰	شکل ۱۷: پنجره ی ادغام فایل ها.....
۳۱	شکل ۱۸: نمونه ای از مجموعه فایل ها.....
۳۲	شکل ۱۹: Export as Plain Text File
۳۳	شکل ۲۰: Export as PostScript File
۳۴	شکل ۲۱: Export as PSML File
۳۵	شکل ۲۲: Export as PDML File
۳۵	شکل ۲۳: Export selected packet bytes
	شکل ۲۴: پنجره ی چاپ.....
۳۷	شکل ۲۵: Wireshark با یک پکت TCP برای دیدن.....
۳۸	شکل ۲۶: دیدن پکت در یک صفحه ی مجزا.....
۳۹	شکل ۲۷: منوی pop-up در صفحه ی لیست پکت.....
۴۵	شکل ۲۸: منوی Pop-up در صفحه ی جزئیات پکت.....
۵۵	شکل ۲۹: فیلتر کردن پکت های پروتکل TCP
۶۰	شکل ۳۰: The "Filter Expression" dialog box
۶۱	شکل ۳۱: The "Capture Filters" and "Display Filters" dialog boxes
۶۲	شکل ۳۲: The "Find Packet" dialog box
۶۳	شکل ۳۳: The "Go to Packet" dialog box

۶۵	شکل ۳۴: نمایش یک پکت با مرجع زمانی
۶۷	شکل ۳۵: پنجره‌ی Summery
۶۹	شکل ۳۶: پنجره‌ی Protocol Hierachy
۷۱	شکل ۳۷: پنجره‌ی Conversations
۷۳	شکل ۳۸: پنجره‌ی Endpoints
۷۴	شکل ۳۹: پنجره‌ی IO Graphs
۷۶	شکل ۴۰: آمار ترافیک WLAN
۷۶	شکل ۴۱: آمار ترافیک WLAN
۷۷	شکل ۴۲: پنجره‌ی "Compute DCE-RPC statistics"
	شکل ۴۳: پنجره‌ی "DCE-RPC Statistic for ..."
		شکل ۴۴: خلاصه اطلاعات ضبط شده از شبکه‌ی دانشگاه امیرکبیر Error! Bookmark not defined.
		شکل ۴۵: نمودار IO مربوط به داده‌های ضبط شده از شبکه‌ی دانشگاه امیرکبیر Error! Bookmark not defined.
		شکل ۴۶: Error! Bookmark not defined.
		شکل ۴۷: خلاصه اطلاعات ضبط شده از شبکه‌ی شرکت پرورش داده‌ها .. Error! Bookmark not defined.
		شکل ۴۸: نمودار IO مربوط به داده‌های ضبط شده از شبکه‌ی پرورش داده Error! Bookmark not defined.
		شکل ۴۹: اطلاعات ضبط شده از ارتباط Dial up Error! Bookmark not defined.

شکل ۵۰: نمودار IO مربوط به داده های ضبط شده از ارتباط Dial Up ...	Error! Bookmark not defined.
شکل ۵۱	Error! Bookmark not defined.
شکل ۵۲	Error! Bookmark not defined.
شکل ۵۳	Error! Bookmark not defined.
شکل ۵۴	Error! Bookmark not defined.
شکل ۵۵	Error! Bookmark not defined.
شکل ۵۶	Error! Bookmark not defined.
شکل ۵۷	Error! Bookmark not defined.
شکل ۵۸	Error! Bookmark not defined.
شکل ۵۹	Error! Bookmark not defined.
شکل ۶۰	Error! Bookmark not defined.
شکل ۶۱	Error! Bookmark not defined.
شکل ۶۲	Error! Bookmark not defined.
شکل ۶۳	Error! Bookmark not defined.
شکل ۶۴	Error! Bookmark not defined.
شکل ۶۵	Error! Bookmark not defined.
شکل ۶۶	Error! Bookmark not defined.

شکل ۶۷ Error! Bookmark not defined.

دانشپس نتوردی

مقدمه

در این گزارش به بررسی دو ابزار مانیتورینگ شبکه پرداخته شده است. در بخش اول ابزار Wireshark مورد بررسی قرار گرفته است. که این بررسی شامل دو قسمت مطالعه ی قابلیت ها و امکانات ابزار و روش کار با آن می باشد. در بخش دوم، ابزار Axence بررسی شده است.

بخش اول

معرفی ابزار Wireshark

Wireshark یک تحلیلگر بسته های شبکه^۱ است. یک تحلیل کننده ی بسته های شبکه سعی در ضبط بسته های شبکه دارد و تلاش می کند جزئیات آن بسته ها را تا جای ممکن به دست آورد.

می توان تحلیلگر بسته های شبکه را به مانند ابزار اندازه گیری فرض کرد که برای بازدید کردن آنچه درون یک کابل شبکه رخ می دهد به کار می رود، مانند یک ولت متر که توسط یک متخصص برای اندازه گیری آنچه داخل یک کابل برق وجود دارد استفاده می شود (البته در سطوح بالاتر).

در گذشته، اینگونه ابزارها یا بسیار گرانقیمت بوده اند یا اختصاصی یا هردو. به هر صورت، با ظهور Wireshark، تمام آن شرایط تغییر کرد. با احتمال زیاد، امروزه Wireshark یکی از بهترین تحلیلگران بسته ی منبع باز موجود است.

برخی از اهداف مورد نظر Wireshark

در اینجا مثال هایی از مواردی که در آنها از Wireshark استفاده می شود آمده است.

- مدیران شبکه از آن برای ازبین بردن مشکلات به وجود آمده در شبکه استفاده می کنند.
- مهندسين امنيت شبکه آن را برای بازبینی مشکلات امنیتی شبکه استفاده می کنند.
- توسعه دهندگان برای اشکال زدایی پیاده سازی های پروتکل از آن استفاده می کنند.
- افراد از آن برای یادگیری کارکرد داخلی پروتکل استفاده می کنند.

^۱ Packet Analyzer

- در کنار این مثال ها، در موقعیت های بسیار دیگری نیز Wireshark می تواند مفید واقع شود.

ویژگی ها

موارد زیر برخی از خیل ویژگی هایی است که Wireshark مجهز به آنها می باشد:

- قابل استفاده برای UNIX و Windows

- ضبط زنده ی بسته های داده از واسط شبکه^۱

- نمایش بسته ها با جزئی ترین اطلاعات پروتکل

- باز کردن و ذخیره ی بسته ی داده ی ضبط شده

- وارد کردن و صادر کردن بسته های داده به/از برنامه های ضبط دیگر

- فیلتر کردن بسته ها بر اساس معیارهای مختلف

- جستجو برای بسته ها بر اساس معیارهای مختلف

- رنگ آمیزی نمایش بسته ها براساس فیلترها

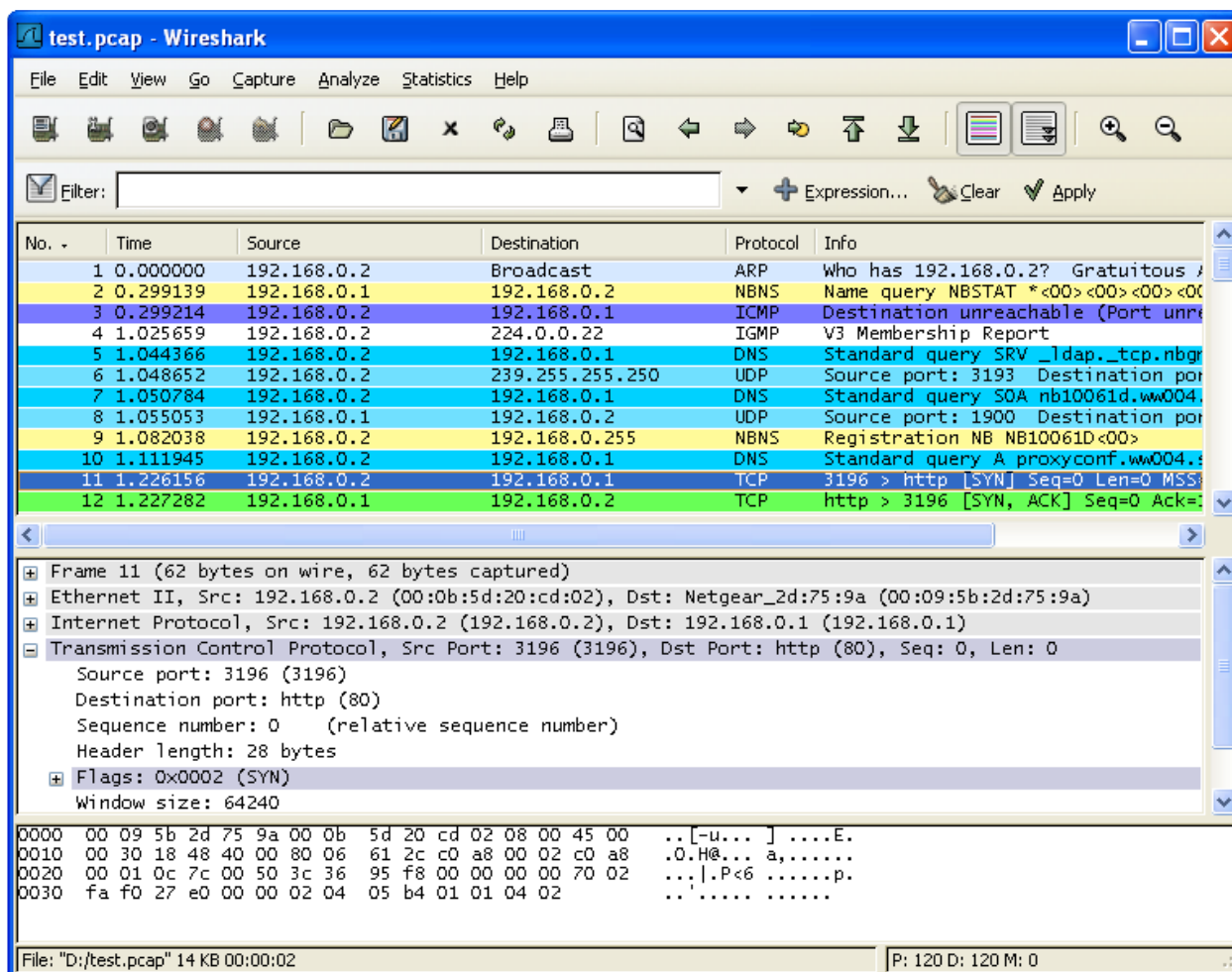
- ایجاد مدل های آماری مختلف

- دیکد کردن پروتکل های مختلف

- نرم افزار منبع باز

- و بسیاری از ویژگی های دیگر ...

^۱ Network Interface



شکل ۱: Wireshark بسته ها را ضبط می کند و امکان بازدید محتوای آنها را می دهد

آنچه *Wireshark* پشتیبانی نمی کند

در اینجا مواردی آمده است که *Wireshark* آنها را تامین نمی کند:

Wireshark سیستمی برای تشخیص نفوذها نمی باشد. این سیستم زمانی که شخصی اعمال غیرعادی - که مجاز به انجام آنها نیست - در شبکه ی شما انجام می دهد اخطار نمی دهد. در هر صورت، به هنگام رخ دادن اتفاقات عجیب، *Wireshark* در دریافتن آنچه در حال روی دادن است کمک می کند.

Wireshark هیچ چیزی را در شبکه دستکاری نمی کند، فقط در شبکه "اندازه گیری" می کند. این سیستم هیچ بسته ای را روی شبکه نمی فرستد یا فعالیت دیگری روی شبکه انجام نمی دهد. (به جز در مورد تفکیک اسامی^۱، ولی حتی آن هم می تواند غیرفعال گردد)

نحوه ی نصب WireShark

برای نصب ابتدا باید فایل installer را دانلود کنیم و سپس با اجرا ی آن مراحل نصب یکی پس از دیگری روی صفحه ظاهر می شوند که با پشت سر گذاشتن آنها می توان نرم افزار را به درستی نصب نمود. نکته ی قابل توجه حین نصب این نرم افزار این است که با نصب wireshark بسته ی نرم افزاری WinPcap نیز همراه با آن نصب می شود و بدین ترتیب نیازی به نصب جداگانه ی آن نمی باشد.

باید دقت داشت که پیش از نصب نرم افزار به حداقل نیازهای سیستمی آن توجه کنیم که این نیازها عبارتند از:

- Windows XP(All Versions) یا Windows Vista و یا Windows Server ۲۰۰۳
- سیستم پتیوم ۳۲ بیتی با قدرت پردازشی ۴۰۰۰۰۰ یا بیشتر.
- حافظه RAM بیش از ۱۲۸۰۰۰۰۰۰
- حداقل فضای دیسک ۷۵۰۰۰۰۰۰
- حداقل رزولوشن ۸۰۰*۶۰۰
- تعدادی کارت شبکه جهت ضبط نمودن ترافیک مبادله شده توسط آنها مانند Ethernet Card یا WLAN Card

^۱ Nam Resolution

اینترفیس کاربر

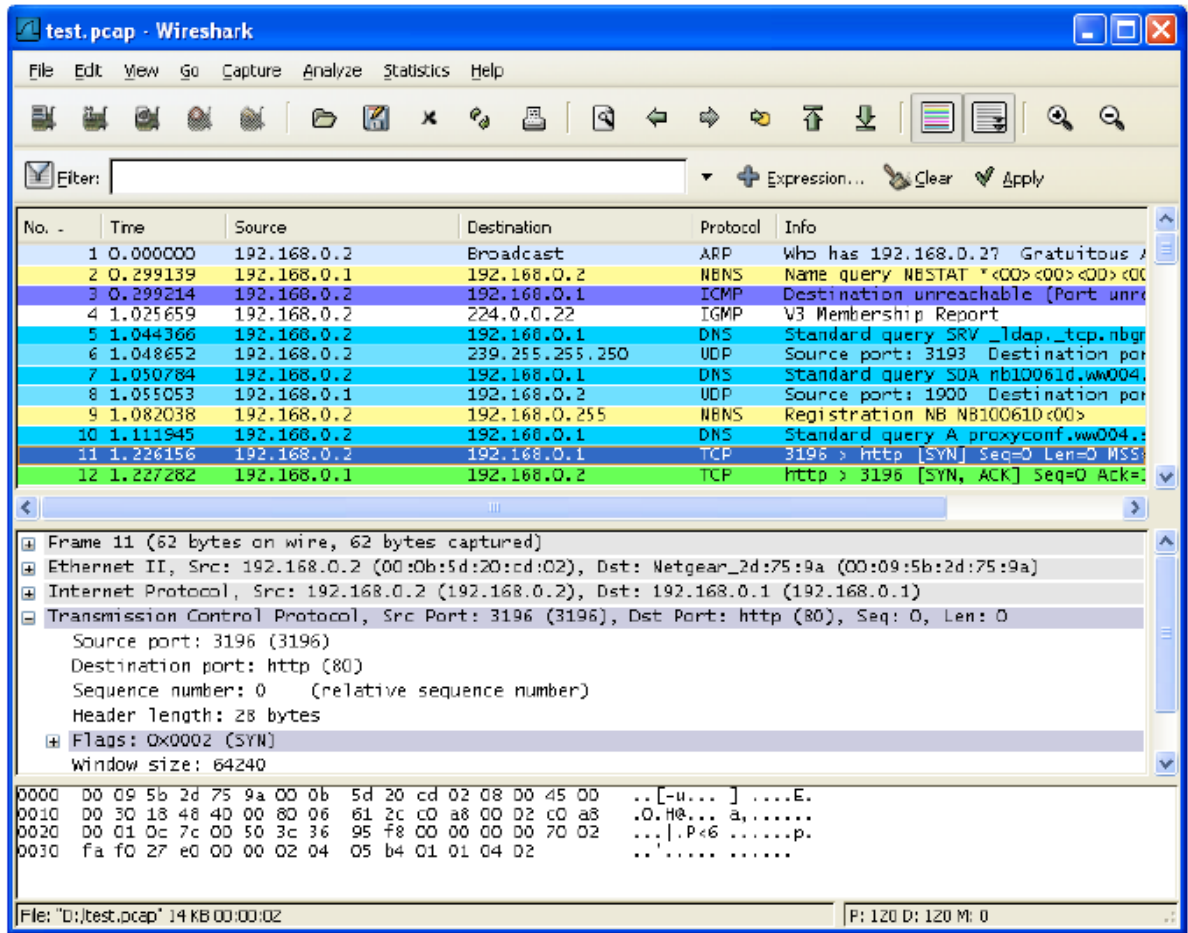
پس از نصب Wireshark می‌توان با ضبط کردن^۱ پکت‌ها کار مانیتورینگ را شروع کرد. در این قسمت در مورد مفاهیم زیر صحبت می‌کنیم:

- چگونه اینترفیس Wireshark کار می‌کند؟
- چگونه پکت‌ها را ضبط کنیم؟
- چگونه پکت‌ها را ببینیم؟
- چگونه پکت‌ها را فیلتر کنیم؟

پنجره ی اصلی^۲

نمونه ای از اینترفیس کاربر که در آن تعدادی پکت ضبط شده‌اند، در شکل زیر نشان داده شده است.

^۱ Capturing
^۲ Main Window



شکل ۲: پنجره‌ی اصلی

پنجره‌ی اصلی Wireshark شامل قسمت‌های زیر می‌باشد:

- ۱- منو که برای شروع عملیات استفاده می‌شود.
- ۲- Toolbar اصلی که اجازه‌ی دسترسی به بخش‌هایی که زیاد تکرار می‌شوند را از طریق منو می‌دهد.
- ۳- Toolbar فیلتر که امکان دستکاری مستقیم فیلتر استفاده شده را می‌دهد.
- ۴- صفحه‌ی لیست پکت^۱ که خلاصه‌ای از هر پکت ضبط شده را نمایش می‌دهد. با کلیک کردن روی پکت‌ها در این صفحه می‌توان آنچه را که در دو صفحه‌ی دیگر نمایش داده می‌شود، کنترل نمود.

^۱ item

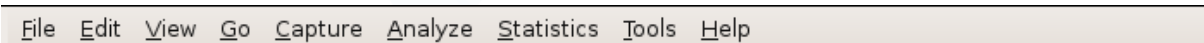
۵- صفحه‌ی جزئیات پکت^۲ که جزئیات پکت انتخاب شده را با دقت بیشتری در صفحه‌ی لیست پکت نمایش می‌دهد.

۶- صفحه‌ی بایت‌های پکت^۳ که داده‌های پکت انتخاب شده از صفحه‌ی لیست پکتها را نمایش می‌دهد و فیلد انتخاب شده در صفحه‌ی جزئیات پکت ها را هایلایت می‌کند.

۷- statusbar تعدادی اطلاعات دقیق و جزئی درباره‌ی حالت برنامه‌ی جاری و داده‌های ضبط شده، نشان می‌دهد.

منو

منوی Wireshark در بالای پنجره قرار دارد و نمونه‌ای از آن در شکل زیر نمایش داده شده است:



File Edit View Go Capture Analyze Statistics Tools Help

شکل ۳: منو

منو شامل قسمت‌های زیر می‌باشد:

File: این قسمت شما بخش‌هایی برای بازکردن، ادغام فایل‌های دریافتی، ذخیره کردن، پرینت کردن، بیرون بردن^۴ فایل‌های ضبط شده به طور جزئی یا کامل و خروج از Wireshark می‌باشد.

Edit: این قسمت شامل امکانات پیدا کردن یک بسته، مرجع زمان^۵ یا نشانه‌گذاری یک یا چند پکت، تنظیم اولویت‌ها و ... می‌باشد.

^۱ packet list pane
^۲ packet details pane
^۳ packet bytes pane
^۴ export
^۵ Time reference

View: این قسمت نمایش پکت‌های ضبط شده را کنترل می‌کند. همچنین شامل امکاناتی نظیر تعیین رنگ پکت‌ها، بزرگ کردن فونت‌ها، نمایش یک پکت در پنجره‌ی جداگانه و امکاناتی از این قبیل می‌باشد.

Go: این بخش شامل بخش‌هایی برای رفتن به یک پکت مشخص شده می‌باشد.

Capture: این قسمت امکان شروع یا متوقف کردن ضبط بسته‌ها و ویرایش فیلترهای ضبط شده را می‌دهد.

Analyze: این قسمت امکان دستکاری فیلترهای نمایش داده شده، فعال یا غیرفعال نمودن تجزیه‌ی پروتکل‌ها، پیکربندی کد برداری مشخص شده کاربر و دنبال کردن یک جریان TCP را می‌دهد.

Statistics: این قسمت شامل بخش‌هایی برای نمایش اطلاعات آماری نظیر خلاصه‌ی پکت‌های ضبط شده، نمایش آمار سلسله مراتب پروتکل و اطلاعاتی از این قبیل می‌باشد.

Tools: این قسمت شامل ابزارهای مختلف موجود در Wireshark نظیر Firewall ACL Rules می‌باشد.

صفحه‌ی لیست پکت

این صفحه تمام پکت‌ها در فایل جاری را نمایش می‌دهد.

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 Win
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 Win
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 Win
18	0.000036	192.168.0.2	192.168.0.1	TCP	5000 > 1025 [SYN, ACK] Seq=0 Ack
19	0.001780	192.168.0.1	192.168.0.2	HTTP	HTTP/1.1 200 OK

شکل ۴: صفحه‌ی لیست پکت

هر خط در لیست پکت معادل یک پکت در فایل ضبط شده می‌باشد. اگر یک خط از این صفحه انتخاب شود، اطلاعات دقیق‌تر در مورد آن در صفحه‌های جزئیات پکت و بایت‌های پکت نمایش داده می‌شوند.

در حال بررسی دقیق یک پکت، Wireshark اطلاعات را در ستون‌ها قرار می‌دهد. از آنجا که پروتکل‌های سطح بالاتر ممکن است اطلاعات سطوح پایین‌تر را overwrite کنند، تنها اطلاعات بالاترین سطح قابل مشاهده می‌باشد. به عنوان مثال یک پکت TCP داخل IP که در یک پکت Ethernet قرار دارد را در نظر بگیرید. Ethernet dissector اطلاعات خودش را می‌نویسد، IP dissector این اطلاعات را با اطلاعات خودش (نظیر آدرس‌های IP) جایگزین می‌کند، TCP dissector اطلاعات IP را جایگزین می‌کند و به همین ترتیب ادامه می‌یابد.

ستون‌های این صفحه اطلاعات زیر را نشان می‌دهند:

- No: تعداد پکت‌ها در فایل ضبط شده. این عدد حتی در صورت به کار بردن فیلتر تغییر نمی‌کند.
- Time: مهرزمانی^۱ بسته. فرمت نمایش این فیلد را می‌توان تغییر داد.
- Source: آدرس جایی که پکت از آنجا می‌آید.
- Destination: آدرس جایی که پکت می‌رود.
- Protocol: نام پروتکل به صورت مختصر.
- Info: اطلاعات اضافی در مورد محتوای پکت.

صفحه‌ی جزئیات پکت

این صفحه اطلاعات پکت را به صورت جزئی و دقیق‌تر نشان می‌دهد.

^۱ timestamp

```
[-] Frame 1 (42 bytes on wire, 42 bytes captured)
[-] Ethernet II, Src: 192.168.0.2 [00:0b:5d:20:cd:02], Dst: Broadcast (ff:ff:ff:ff:ff:ff)
[-] Address Resolution Protocol (request/gratuitous ARP)
```

شکل ۵: صفحه‌ی جزئیات پکت

هم‌چنین این صفحه پروتکل‌ها و فیلدهای پروتکل مربوط به پکت انتخاب شده در صفحه‌ی لیست پکت را نشان می‌دهد. بعضی از این فیلدها عبارتند از:

- **Generated files:** Wireshark خودش فیلدهای پروتکل اضافی تولید می‌کند که با براکت احاطه شده است. به عنوان مثال، Wireshark یک تحلیل sequence/acknowledge از هر جریان TCP انجام می‌دهد که به صورت [SEQ/ACK] در فیلدهای پروتکل TCP نشان داده می‌شود.
- **Links:** اگر Wireshark یک رابطه با پکت دیگری در فایل ضبط شده تشخیص دهد، یک لینک به آن پکت تولید می‌کند. زیر لینک‌ها خط کشیده شده و با رنگ آبی نشان داده می‌شوند. اگر روی این فیلد دوبار کلیک کنید، Wireshark به پکت مربوطه می‌رود.

صفحه‌ی بایت‌های پکت

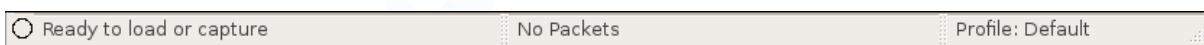
این صفحه داده‌های پکت جاری را به شیوه‌ی hexdump نمایش می‌دهد که در آن offset داده‌های پکت در سمت چپ، داده‌های پکت در وسط به صورت هگزادسیمال و کاراکترهای اسکی معادل در سمت راست نشان داده می‌شود.

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 ۶: صفحه‌ی بایت‌های پکت

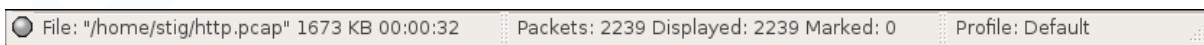
Statusbar

این قسمت پیام‌های اطلاعاتی را نمایش می‌دهند. به طور کلی در سمت چپ محتوای مربوط به اطلاعات، در وسط تعداد پکت‌های جاری و در سمت راست پروفایل پیکربندی را نمایش می‌دهد.



شکل ۷: Statusbar اولیه

این statusbar هنگامی که فایلی لود نشده باشد مانند وقتی که Wireshark کارش را آغاز می‌کند، دیده می‌شود. در شکل زیر نمونه‌ای از statusbar با فایل لود شده دیده می‌شود.



شکل ۸: statusbar با یک فایل لود شده

- The colored bullet در سمت چپ، بالاترین سطح اطلاعات ویژه که در فایل ضبط شده‌ی جاری پیدا می‌شود را نشان می‌دهد. برای بدست آوردن اطلاعات دقیق‌تر کافی است روی آن کلیک کرد.
- سمت چپ اطلاعات فایل ضبط شده، نام و اندازه‌ی آن و زمان سپری شده از شروع ضبط کردن را نشان می‌دهد.

- قسمت میانی تعداد پکت‌های فایل ضبط شده را نشان می‌دهد. همچنین اطلاعات زیر نمایش داده می‌شوند:

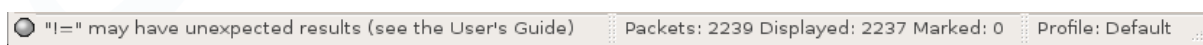
- Packets : تعداد پکت‌های ضبط شده
- Displayed : تعداد پکت‌هایی که اکنون نشان داده می‌شود
- Marked : تعداد پکت‌های علامت‌دار
- Dropped : تعداد پکت‌های drop شده

- قسمت راست پروفایل پیکربندی انتخاب‌شده را نشان می‌دهد. با کلیک کردن روی این قسمت statusbar یک منو شامل همه‌ی پروفایل‌های پیکربندی موجود باز می‌شود و می‌توان آن را تغییر داد.



شکل ۹: Statusbar با منوی پروفایل پیکربندی

در شکل زیر statusbar با یک پیام display filter دیده می‌شود.



شکل ۱۰: Statusbar با یک پیام display filter

طریقه ی ضبط نمودن داده های در جریان شبکه

موتور ضبط اطلاعات wireshark دارای قابلیت‌های زیر می‌باشد:

- ضبط اطلاعات از شبکه‌های با سخت افزارهای مختلف (Ethernet, Token Ring, ATM, ...)

- متوقف ساختن ضبط اطلاعات توسط رهاناها^۱ی مختلف
- نشان دادن بسته های دی کد شده همزمان با ادامه ی عملیات ضبط نمودن
- فیلتر کردن بسته ها و کاهش تعداد داده هایی که ضبط خواهند شد.
- ضبط کردن در چندین فایل به هنگام ضبط داده ها در فاصله ی زمانی طولانی

با وجود همه ی قابلیت هایی که برشمرده شد، Wireshark در زمینه ی ضبط بسته ها معایبی هم دارد که عبارتند از:

- نداشتن قابلیت ضبط همزمان داده های مربوط به چند کارت شبکه (گر چه می توان همزمان چند برنامه ی wireshark را به طور همزمان روی سیستم اجرا نمود و اطلاعات مربوط به هر کارت شبکه را توسط یکی از آنها ضبط کرد و در پایان آنها را ادغام نمود).

- متوقف ساختن ضبط اطلاعات و یا انجام هر عمل دیگر، بر اساس داده های ضبط شده

پیش نیازها برای ضبط زنده ی اطلاعات شبکه

- باید سطح دسترسی از نوع Administrator باشد.
- کارت شبکه ی درست برای به دست آوردن اطلاعات شبکه ی مورد نظر استفاده شود
- برای دیدن ترافیک مورد نظر باید

^۱ trigger

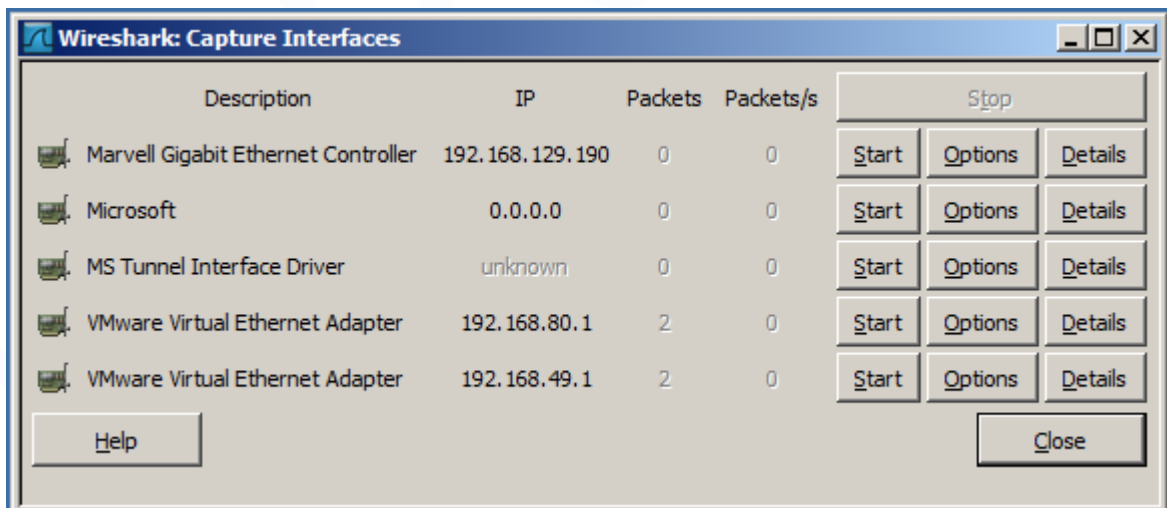
آغاز ضبط اطلاعات

برای شروع نمودن ضبط اطلاعات باید ابتدا کارت شبکه ی مورد نظر از منوی Capture را انتخاب می کنیم و سپس گزینه ی Start را از همین منو انتخاب می کنیم. در صورتیکه قبلا کارت شبکه ی مورد نظر را انتخاب کرده باشیم با انتخاب گزینه ی Start می توانیم ضبط اطلاعات را آغاز کنیم.

در صورتیکه نام کارت شبکه مورد نظر را بدانیم می توانیم از دستور `wireshark -i netInterfaceName -k` در خط فرمان عملیات را آغاز کنیم.

پنجره ی Capture Interfaces

زمانی که گزینه ی Interface را از منوی capture انتخاب می کنیم یک پنجره ی گفتگو به صورت زیر باز می شود.



شکل: ۱۱ پنجره ی واسط ها ی ضبط

Description: توصیف کارت شبکه که توسط سیستم عامل ارائه می شود.

IP: اولین آدرس IP که wireshark می تواند از روی کارت شبکه به دست آورد.

Packets: تعداد بسته هایی که از طریق کارت شبکه ی مورد نظر ضبط شده اند.

Stop: به عملیات ضبط اطلاعات پایان می دهد.

Start: عملیات ضبط را با استفاده از تنظیمات قبلی آغاز می کند.

Options: انتخابهای مربوط به کارت شبکه را نمایش می دهد.

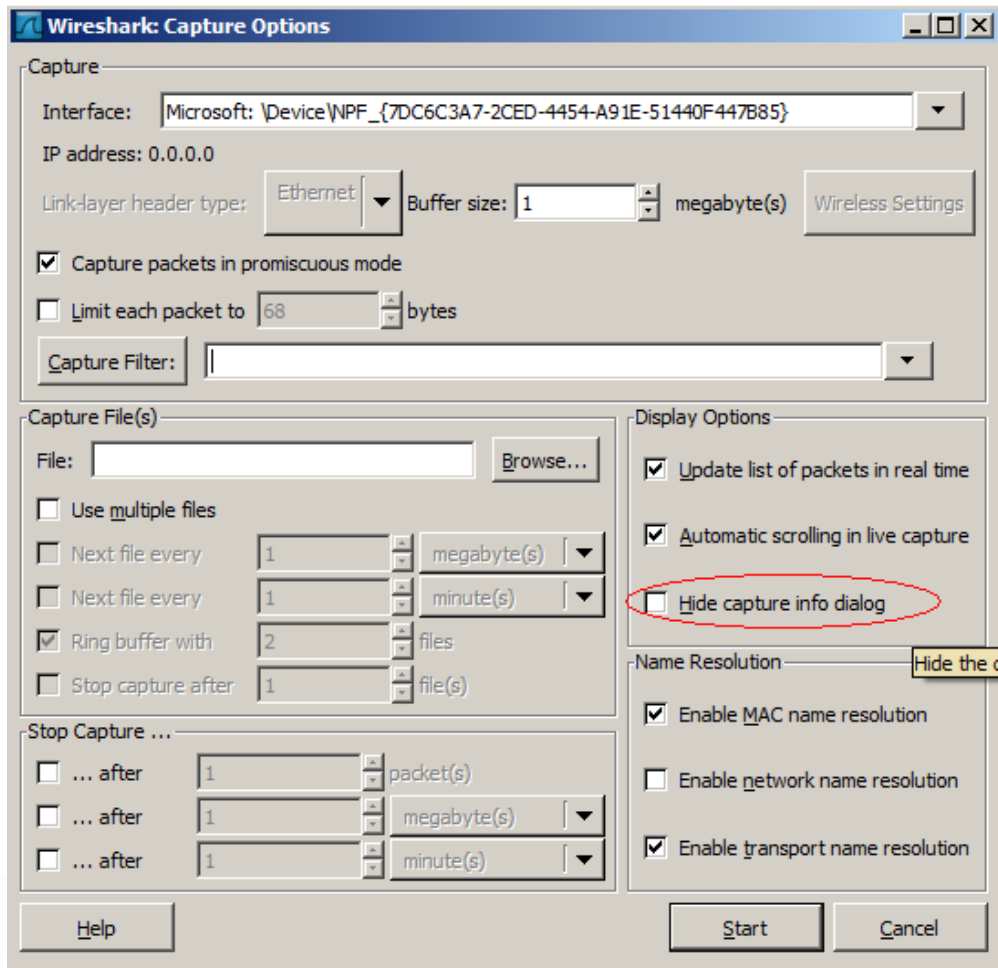
Details: جزئیات مربوط به کارت شبکه را نمایش می دهد.

Help: صفحه ی راهنمایی را باز می کند.

Close: پنجره ی دیالوگ را می بندد.

باید توجه داشت که این پنجره منابع سیستم را به مقدار زیادی مصرف می کند بنابراین باید پس از انتخاب کارت شبکه ی مناسب آن را به سرعت بست تا از سر بار اضافی سیستم جلوگیری کرد.

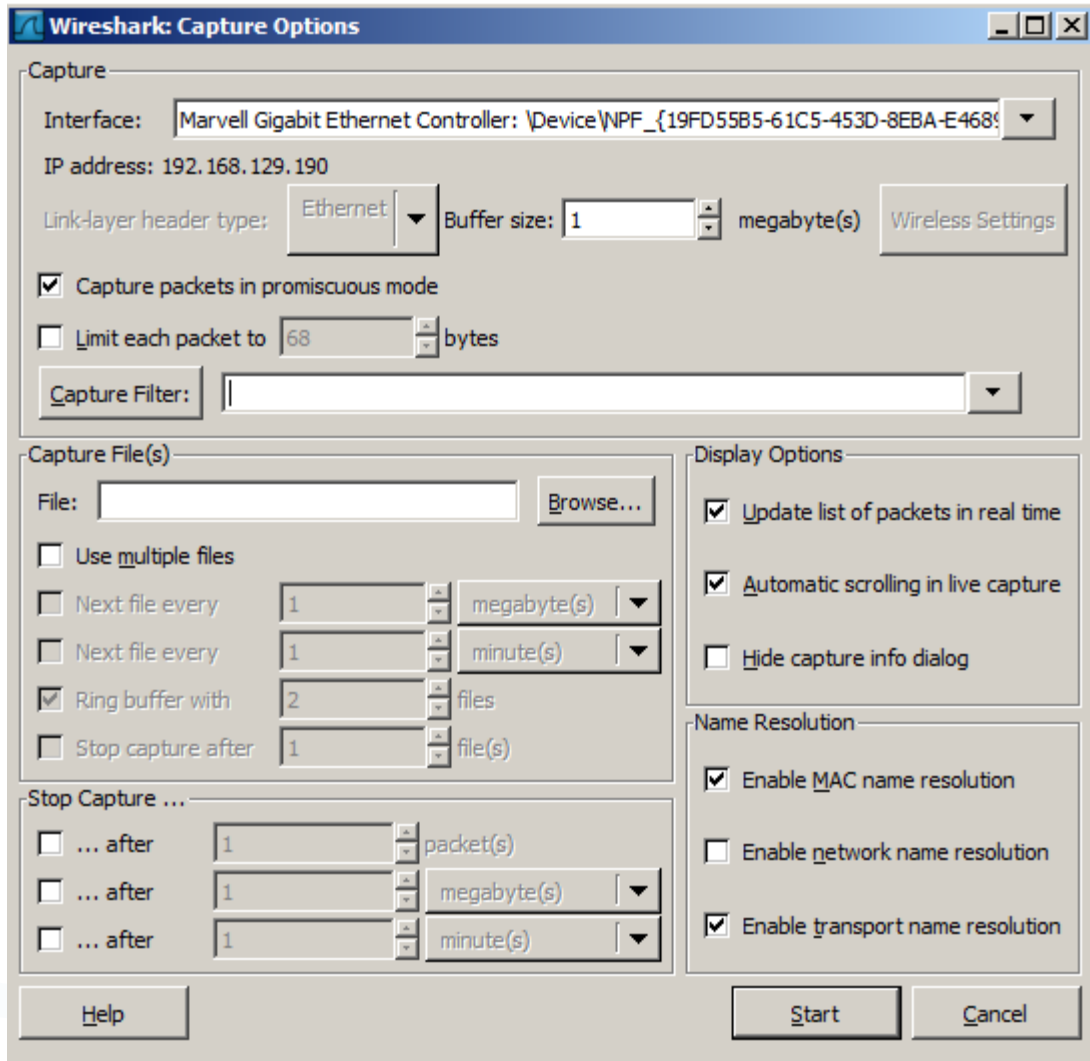
نکته ی قابل توجه دیگر این است که ممکن است تعداد کارت های شبکه ی سیستم بیشتر از تعداد لیست شده در پنجره ی Capture Interface باشد، چون wireshark کارت شبکه هایی که گزینه ی Hide Capture شده در آنها علامت خورده باشد را در پنجره ی Network Interface نمایش نمی دهد. همچنین این ابزار قابلیت نشان دادن کارت شبکه های کنترل از راه دور را ندارد.



شکل ۱۲: طریقه ی مخفی نمودن یک کارت شبکه از دید Wireshark

پنجره ی Capture Options

هنگامی که شروع به ضبط داده ها می کنیم (با فشردن دکمه ی Start) پنجره ی Capture Options باز می شود که دارای نمای زیر می باشد.



شکل ۱۳: پنجره ی Capture Options

گزینه های فریم Capture

- Interface: از این گزینه می توان کارت شبکه ی مورد نظر را انتخاب نمود.
- IP Address: آدرس IP کارت شبکه ی انتخاب شده را نشان می دهد. در صورتی که آدرس IP قابل شناسایی نباشد با عبارت Unknown مشخص می شود.

- **Link Layer header Type**: پروتکل لایه ی زیرین لایه ی شبکه را مشخص می کند که معمولا به صورت پیش فرض Ethernet می باشد.
- **Buffer Size**: سایز بافری که در طول ضبط مورد استفاده قرار می گیرد را بر حسب مگابایت نشان می دهد. در صورت مواجه شدن با Packet Drop باید سایز این بافر را افزایش داد.
- **Capture packet in promiscuous mode**: در صورتی که این گزینه انتخاب نشود، فقط بسته های ورودی و خروجی از کامپیوتری که wireshark روی آن اجرا می شود ضبط می شوند. در صورتی هم که یک سیستم دیگر روی شبکه برنامه را در promiscuous mode اجرا کرده باشد ممکن است در سیستم دیگری که این گزینه علامت نخورده هم بسته های کل شبکه ضبط شوند.
- **Limit each packet to n bytes**: امکان تعیین ماکزیمم اندازه ی اطلاعاتی که از هر بسته ضبط شود را ما می دهد. که این پارامتر به عنوان snaplen شناخته می شود و مقدار پیش فرض آن ۶۵۵۳۵ می باشد.
- **Capture filter**: برای ایجاد فیلتر هایی در اطلاعات ضبط شونده به کار می رود و مقدار پیش فرض آن خالی (بدون فیلتر) است.

گزینه های فریم Capture File(s)

- **File**: این فیلد برای مشخص کردن نام فایل که قرار است اطلاعات ضبط شده در آن قرار گیرد به کار می رود. پیش فرض این فیلد blank می باشد که در صورت عدم انتخاب نام برای فایل، اطلاعات در یک فایل موقتی ذخیره می شود.
- **Use Multiple files**: این امکان را به ما می دهد که با اجرا شدن یک رهانای خاص بقیه ی اطلاعات در یک فایل جدید ذخیره شوند.

- **Next file every n MegaByte(s)**: این گزینه در صورت علامت دار بودن **Use Multiple files** فعال می شود. این امکان را فراهم می کند که پس از حجم بایت داده ی مشخص شده (با فرمت گیگا بایت/ مگابایت/ کیلو بایت/ بایت)، ادامه ی اطلاعات را در فایل جدیدی ضبط کند.
- **Next file every n minutes**: این گزینه در صورت علامت دار بودن **Use Multiple files** فعال می شود. این امکان را فراهم می کند که پس از مدت زمان مشخص (با فرمت روز/ ساعت / دقیقه/ ثانیه)، ادامه ی اطلاعات را در فایل جدیدی ضبط کند.
- **Ring buffer with n files**: این گزینه در صورت علامت دار بودن **Use Multiple files** فعال می شود. یک بافر حلقه ای از فایل هایی که ضبط شده اند، ایجاد می کند.
- **Stop capture after n files**: این گزینه در صورت علامت دار بودن **Use Multiple files** فعال می شود. پس از ضبط اطلاعات در تعداد مشخصی فایل عملیات ضبط را متوقف می کند.
- **فرم Stop Capture...**
- **... after n packets**: پس از ضبط اطلاعات در تعداد مشخصی فایل عملیات ضبط را متوقف می کند.
- **... after n MegaBytes**: بعد از تعداد مشخصی کیلو/ مگا / گیگا بایت ضبط داده ها را متوقف می کند. زمانیکه **“Use multiple files”** انتخاب شده باشد، این گزینه غیرفعال می شود.
- **After n minute(s)**: بعد از تعداد ثانیه/دقیقه/ساعت/روز مشخصی عمل ضبط داده ها را متوقف می کند.

گزینه های فریم Display Options

- **Update list of packets in real time**: این گزینه معین می کند که آیا Wireshark باید قاب لیست بسته ها^۱ را به صورت بلادرنگ به روز رسانی کند یا خیر. در صورت نامشخص بودن وضعیت این گزینه، Wireshark تا زمانی که ضبط داده ها متوقف نشده است هیچ بسته ای نمایش نمی دهد. اگر این گزینه علامتگذاری شود، Wireshark در یک جریان جداگانه ضبط داده ها را انجام می دهد و داده های ضبط شده را برای جریان نمایش می فرستد.

- **Automatic scrolling in live capture**: این گزینه تعیین کننده ی این است که با ورود بسته های جدید به قاب لیست بسته ها Wireshark باید آن را scroll کند یا نه که در این صورت بسته هایی که اخیرا وارد قاب لیست شده اند نمایش داده می شوند. اگر وضعیت این گزینه مشخص نباشد، Wireshark بسته های جدید را به انتهای لیست اضافه می کند ولی قاب لیست بسته ها را scroll نمی کند. این گزینه در حالتیکه "Update list of packets in real time" علامتگذاری نشده باشد غیرفعال خواهد بود.

- **Hide capture info dialoge**: اگر این گزینه علامتگذاری شده باشد، جعبه ی محاوره ی اطلاعات ضبط^۲ پنهان می شود.

گزینه های فریم Name resolution

- **Enable MAC name resolution**: این گزینه امکان کنترل آن را فراهم می سازد که آیا Wireshark آدرس MAC را به اسم ترجمه کند یا خیر.

- **Enable network name resolution**: این گزینه کنترل ترجمه ی آدرس شبکه را به اسم امکانپذیر می سازد.

^۱ Packet list pane

^۲ Capture info. dialoge

- Enable transport name resolution: کنترل اینکه آیا Wireshark آدرس های Transport را به پروتکل ها ترجمه کند در اختیار این گزینه است.

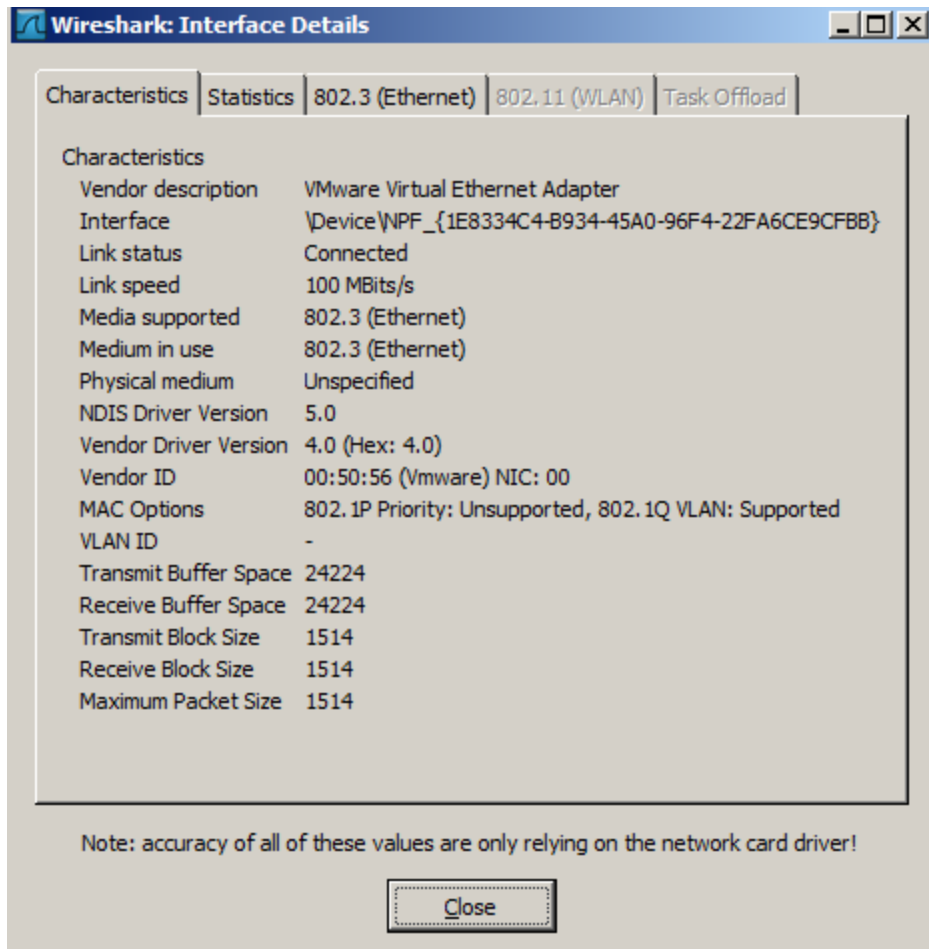
Buttons (دکمه ها)

با تنظیم مقادیر مورد نظر و انتخاب گزینه های مورد نیاز، با یک کلیک بر روی دکمه ی “start” ضبط داده ها شروع شده و با کلیک بر دکمه ی “cancel” لغو می شود.

بعد از شروع یک ضبط، Wireshark اجازه می دهد عمل ضبط را پس از ضبط تعداد کافی از بسته ها متوقف سازیم.

جعبه ی محاوره ی *Interface Details*

با انتخاب Details از منوی Capture interface، Wireshark یک جعبه ی محاوره مانند شکل زیر باز می کند. این ویژگی ها و ارقام مختلفی را برای رابط انتخاب شده نمایش می دهد. قابل توجه است که این جعبه فقط برای سیستم عامل Microsoft Windows موجود می باشد.



شکل ۱۴: جعبه ی محاوره ی “Interface Details”

ضبط فایل ها

به هنگام ضبط، موتور ضبط libcap بسته ها را از کارت شبکه ربوده و بسته ی داده را در بافر کرنل نسبتاً کوچکی نگهداری می کند. این داده توسط Wireshark خوانده می شود و در فایل (های) ضبط که کاربر تعیین کرده است ذخیره می شود.

این عملیات برای ذخیره ی داده ها در فایل های ضبط به طرق مختلف صورت می پذیرد.

باید توجه کرد که کارکردن با فایل های بزرگ مانند (بعضی از ۱۰۰ مگابایتی ها) تقریبا به کندی صورت می گیرد. زمانیکه قرار است یک عمل ضبط طولانی مدت انجام گیرد یا شبکه ای که بسته ها از آن ضبط می شوند ترافیک بالایی داشته باشد، بهتر است از گزینه ی "multiple files" استفاده شود. این عمل سبب پخش شدن بسته های ضبط شده مابین فایل های کوچکتری می شود که کار کردن با آنها بسیار آسان تر است.

توجه: استفاده از "Multiple files" ممکن است اطلاعات مربوط به مفهوم را تکه تکه کند. Wireshark اطلاعات مفهوم بسته ی داده ی بارگذاری شده را نگهداری می کند و در نتیجه می تواند مشکلات مربوط به مفهوم متن را گزارش کند (مانند خطاهای جریان)، بعلاوه اطلاعات پروتکل های مربوط به مفهوم متن را نیز نگهداری می کند (به عنوان مثال، جایی که داده در فاز برقراری ارتباط ردوبدل می شود و فقط در بسته های بعدی به آن مراجعه می شود). از آنجاییکه این اطلاعات فقط برای فایل های بارگذاری شده نگهداری می شود، استفاده از یکی از طرق فایل های چندگانه^۱ ممکن است سبب تکه تکه شدن این متون شود. اگر فاز برقراری ارتباط در یک فایل جداگانه ذخیره شود و بقیه اطلاعاتی که کاربر خواهان مشاهده ی آن است در فایل دیگری، بعضی از اطلاعات با ارزش مربوط به متن دیده نخواهد شد.

انواع مدهای ضبط فایل عبارتند از:

- Single temporary file: یک فایل موقتی ساخته و استفاده می شود (این عمل به عنوان پیش فرض صورت می گیرد). پس از توقف ضبط، این فایل می تواند تحت یک نام تعیین شده توسط کاربر ذخیره شود.
- Single named file: یک فایل ضبط تنها استفاده می شود. زمانیکه بخواهیم فایل ضبط جدید را در یک فولدر خاص ذخیره کنیم این اسلوب را انتخاب می کنیم.

^۱ Multiple file modes

- **Multiple files, continuous**: مانند اسلوب قبلی است با این تفاوت که یک فایل جدید ساخته و استفاده می شود، البته پس از حصول یکی از شرایط تعویض فایل های چندگانه (یکی از مقادیر Next “file every...”)
- **Multiple files, ring buffer**: بسیار شبیه “multiple files, continuous” عمل می کند. با برقراری یکی از شروط تعویض فایل های چندگانه به فایل های بعدی تغییر جهت می دهد. اگر مقدار Ring “buffer with n files” حاصل نشده باشد، این فایل می تواند به تازگی ساخته شده باشد. در غیر این صورت قدیمی ترین فایلی که قبلا استفاده را جایگزین می کند (و در نتیجه یک حلقه^۱ می سازد)
- این طریقه با نگهداری آخرین داده های ضبط شده ماکزیمم استفاده ی دیسک را محدود می کند، حتی برای مقدار نامحدودی از داده های ضبط شده ی ورودی.

فیلتر کردن حین ضبط اطلاعات

Wireshark که زبان فیلتر libpcap برای فیلتر کردن ضبط اطلاعات استفاده می کند. که این زبان در صفحه ی دستورالعمل TCPdump بیان شده است.

فیلترینگ خودکار ترافیک از راه دور

Whireshrak به صورت کنترل از راه دور (با استفاده از SSH و ترمینال سرور و ...) اجرا می شود و به محتوای اطلاعاتی که باید از طریق شبکه به ترمینال سرور برسد حین انتقال، بسته هایی اضافه می شود. برای اجتناب از این حالت، Wireshark به صورت خودکار یک فیلتر ضبط که با جنبه های مختلف اتصال راه دور مطابقت دارد ایجاد می کند. تشخیص پارامترهای اتصال بر اساس متغیرهای محیطی^۲ صورت می گیرد.

متغیرهای محیطی تحت بررسی عبارتند از:

SSH_CONNECTION (ssh) <remote IP> <remote port> <local IP> <local port>

^۱ ring

^۲ Environment variables

SSH_CLIENT (ssh) <remote IP> <remote port> <local port>

REMOTEHOST (tcsh, others?) <remote name>

DISPLAY (x11) [remote name]:<display num>

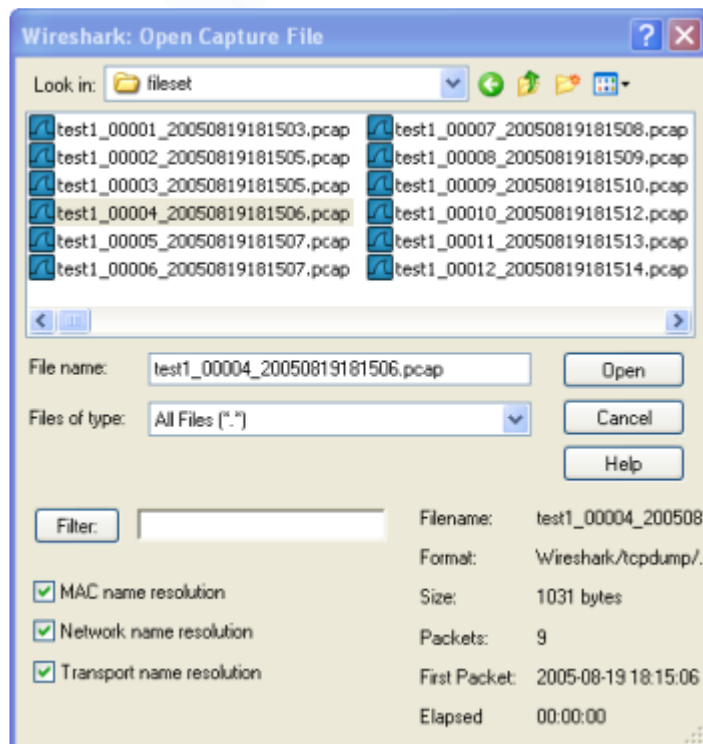
SESSIONNAME (terminal server) <remote name>

فایل ها (ورودی/خروجی) و پرینت

در این قسمت امکانات مختلفی که Wireshark برای وارد کردن و باز کردن فایل هایی که با فونت های مختلف ضبط شده اند همچنين قابليت های ذخيره و ادغام و چاپ آنها مورد بررسی قرار گرفته است.

باز کردن یک فایل ضبط شده

Wireshark قابليت باز کردن فایل هایی که از قبل ضبط شده اند را دارد. برای این کار، گزینه ی open را از منوی فایل انتخاب می کنیم و پس از انتخاب نام فایل مورد نظر روی دکمه ی open کلیک می کنیم.



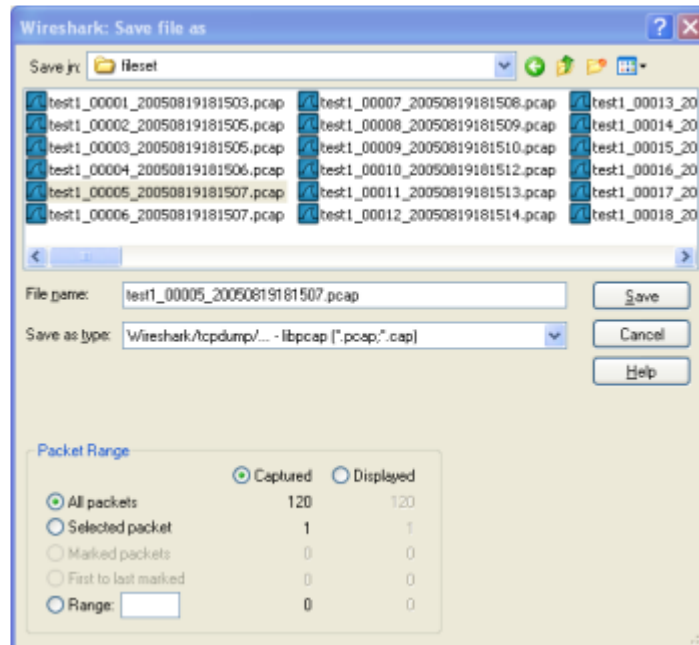
شکل ۱۵: پنجره ی باز کردن یک فایل ضبط شده

فرمت فایل هایی که برای Wireshark تعریف شده اند عبارتند از:

- libpcap, tcpdump and various other tools using tcpdump's capture format
- Sun snoop and atmsnoop
- Shomiti/Finisar *Surveyor* captures
- Novell *LANalyzer* captures
- Microsoft Network Monitor captures
- AIX's iptrace captures
- Cinco Networks NetXray captures
- Network Associates Windows-based Sniffer and Sniffer Pro captures
- Network General/Network Associates DOS-based Sniffer (compressed or uncompressed) captures
- AG Group/WildPackets EtherPeek/TokenPeek/AiroPeek/EtherHelp/PacketGrabber captures
- RADCOM's WAN/LAN Analyzer captures
- Network Instruments Observer version 9 captures
- Lucent/Ascend router debug output
- HP-UX's nettl
- Toshiba's ISDN routers dump output
- ISDN4BSD *i4btrace* utility
- traces from the EyeSDN USB S0
- IPLog format from the Cisco Secure Intrusion Detection System
- pppd logs (pppdump format)

نحوه ی ذخیره ی بسته های ضبط شده

با استفاده از گزینه ی Save As در منوی فایل به راحتی می توان اطلاعات ضبط شده را ذخیره نمود.



شکل ۱۶: پنجره ی ذخیره ی فایل

فرمت فایل های خروجی

Wireshark داده های بسته ها را در فایل های با فرمت libpcap ذخیره می کند. علاوه بر آن قابلیت ذخیره با فرمت برخی از تحلیل گره های پروتکل دیگر را هم دارد که امکان استفاده از فایل های ضبط شده با Wireshark را به دیگر ابزارهای تحلیل ترافیک می دهد. فرمت های فایل های خروجی Wireshark به صورت زیر می باشند:

- libpcap, tcpdump and various other tools using tcpdump's capture format (*.pcap,*.cap,*.dmp)
- Accellent 5Views (*.5vw)
- HP-UX's nettl (*.TRC0,*.TRC1)
- Microsoft Network Monitor - NetMon (*.cap)
- Network Associates Sniffer - DOS (*.cap,*.enc,*.trc,*.fdc,*.syc)
- Network Associates Sniffer - Windows (*.cap)
- Network Instruments Observer version 9 (*.bfr)

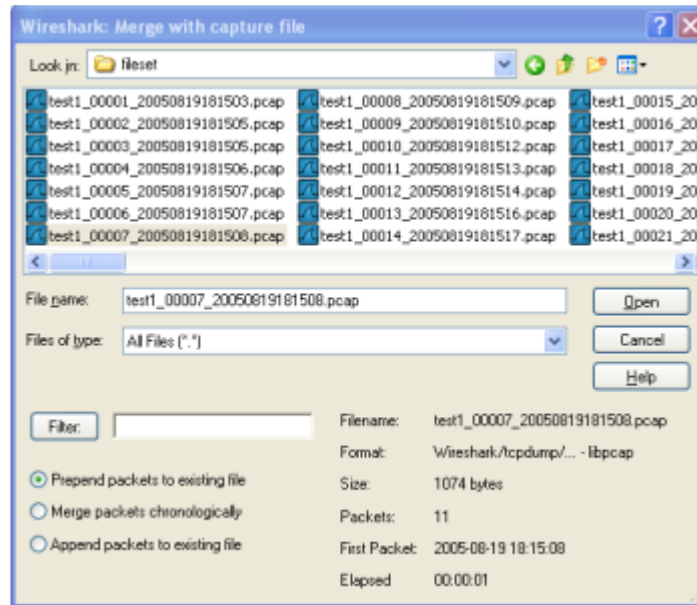
- Novell LANalyzer (*.tr1)
- Sun snoop (*.snoop,*.cap)
- Visual Networks Visual UpTime traffic (*.*)
- ... new file formats are added from time to time

ادغام فایل های ضبط شده

گاهی اوقات نیاز داریم که اطلاعات چندین فایل ذخیره شده را در هم ادغام کنیم. به طور مثال وقتی اطلاعات چند کارت شبکه مختلف را همزمان در فایل های مختلف ذخیره کرده ایم، برای بررسی ترافیک کلی می توانیم همه آنها را با هم ادغام کنیم.

ادغام سازی را می توان از طریق گزینه Merge در منوی فایل انجام داد.

- Prepend packets to existing file: اطلاعات بسته های فایل های انتخابی را به ابتدای فایل موجود اضافه می کند.
- Merge packets chronologically: داده ها را بر اساس زمان ضبط آنها ادغام می کند.
- Append packets to existing file: اطلاعات بسته های فایل های انتخابی را به انتهای فایل موجود اضافه می کند.



شکل ۱۷: پنجره ی ادغام فایل ها

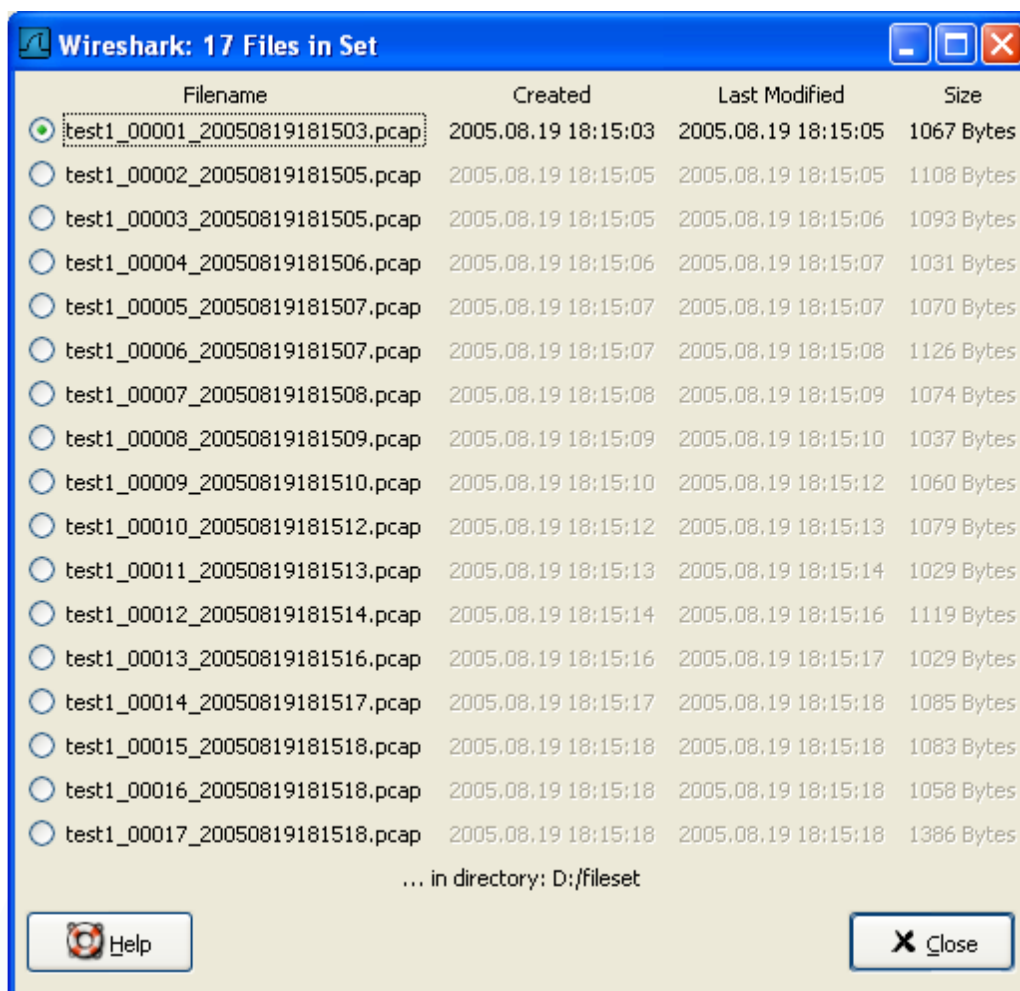
مجموعه فایل ها

وقتی داده ها را در چندین فایل ذخیره می کنیم به مجموعه ی این فایل ها، مجموعه فایل گفته می شود. از آنجاییکه کار با یک مجموعه فایل به صورت دستی عملیات ملال آور و خسته کننده ای می باشد wireshark ویژگی هایی برای کار با مجموعه داده ها فراهم می کند. این ویژگی ها در زیر منوی File Set از منوی File آورده شده اند.

List file: فایل هایی که به عنوان یک زیر مجموعه شناسایی شده اند را نشان می دهد.

Next file: فایل باز موجود را می بندد و به جای آن فایل بعدی را که به آن مجموعه فایل تعلق دارد باز می کند.

Previous file: فایل باز موجود را می بندد و به جای آن فایل قبلی را که به آن مجموعه فایل تعلق دارد باز می کند.

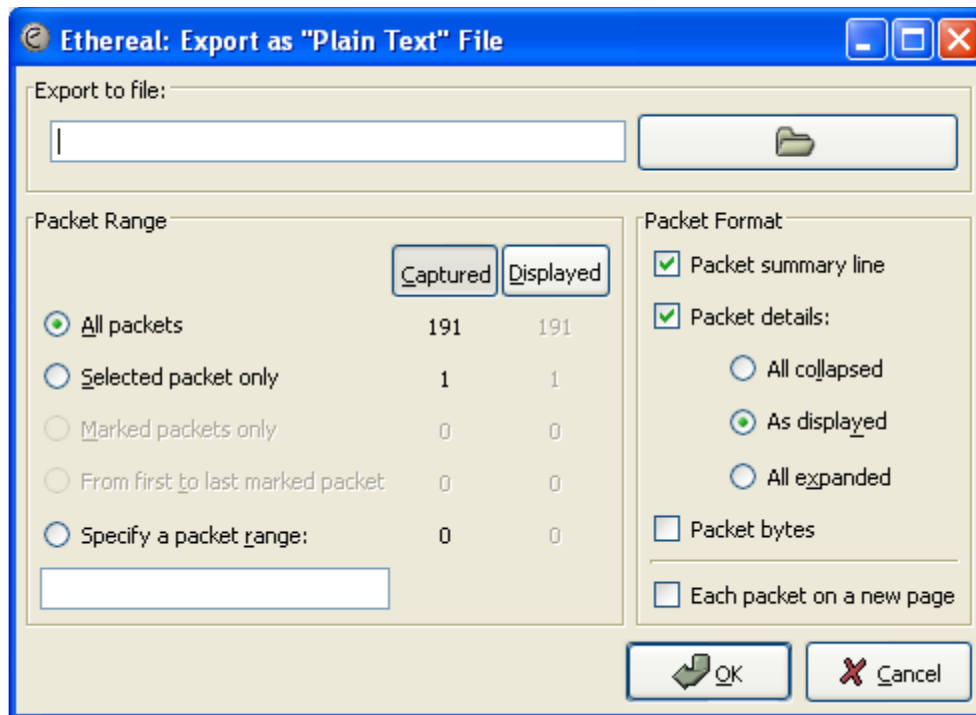


شکل ۱۸: نمونه ای از مجموعه فایل ها

صدور اطلاعات از *Wireshark*

روش های متفاوتی برای این کار وجود دارند که عبارتند از:

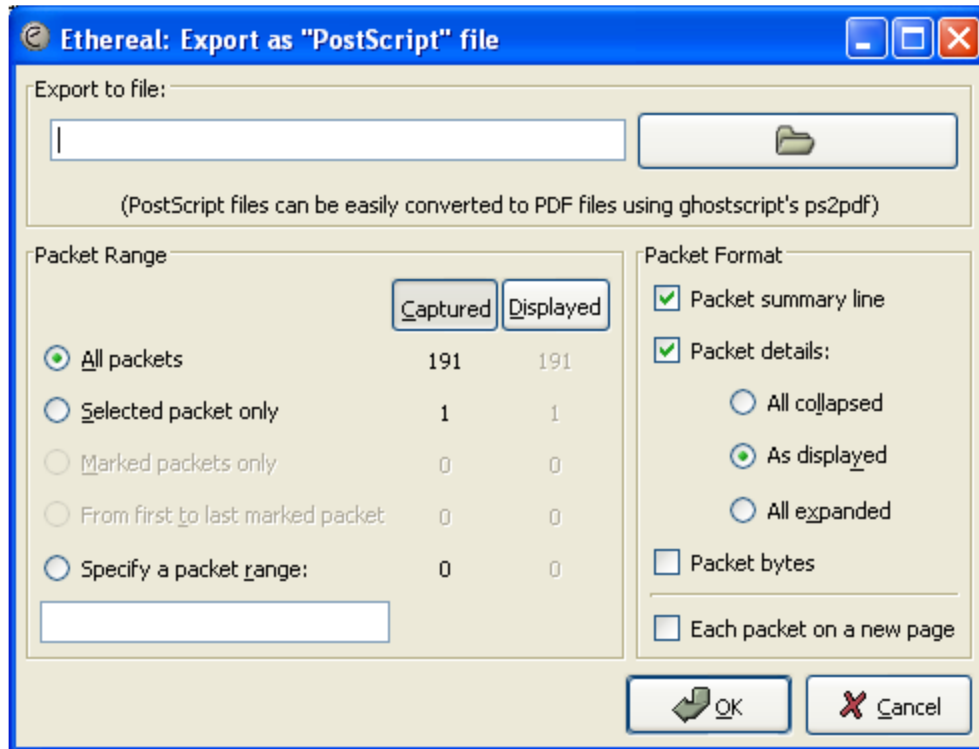
Export as Plain Text File



شکل ۱۹: Export as Plain Text File

Export as PostScript File

- این فرمت برای چاپ بسته ها مرجح است.

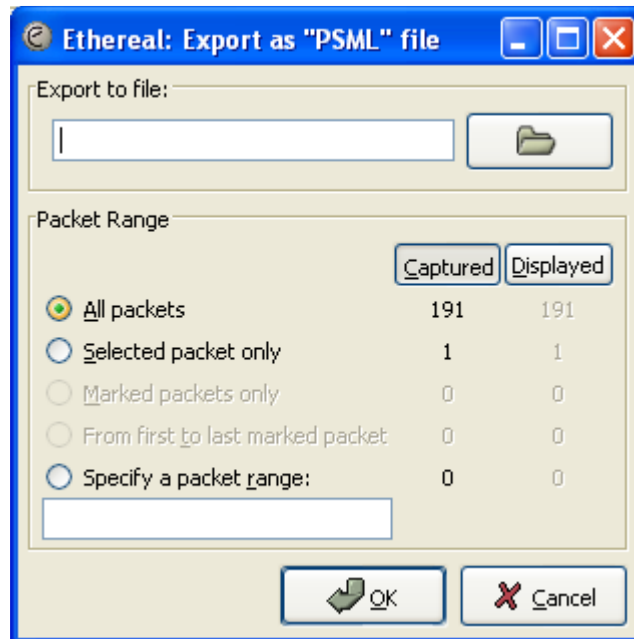


شکل ۲۰ : Export as PostScript File

Export as CSV File

خلاصه اطلاعات را به صورت CVS که برای صفحات گسترده مناسب است ایجاد می کند.

Export as PSML File

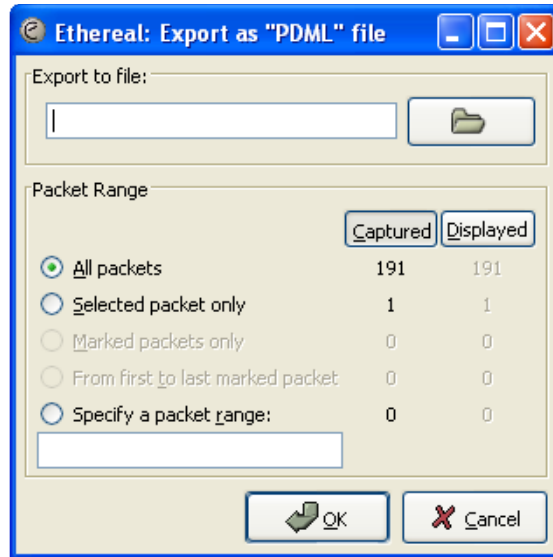


شکل ۲۱: Export as PSML File

Export as C Arrays file

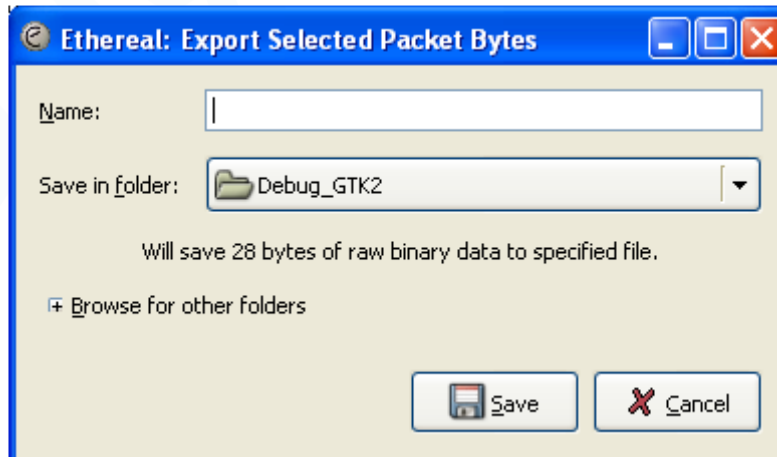
اطلاعات را در یک آرایه از نوع آرایه های C قرار می دهد که قابلیت ورود به یک برنامه ی C را دارد.

Export as PDML File



شکل ۲۲ : Export as PDML File

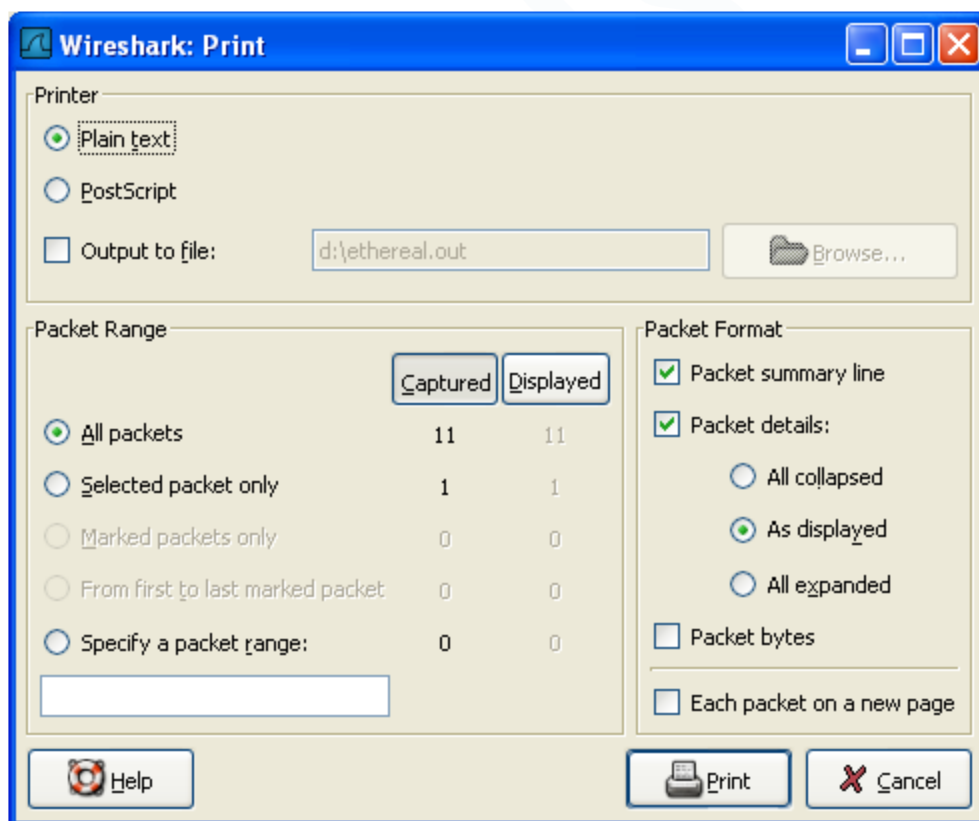
Export selected packet bytes



شکل ۲۳ : Export selected packet bytes

چاپ بسته ها

برای این کار گزینه ی Print از منوی فایل را انتخاب می کنیم به این ترتیب پنجره ای به شکل زیر ظاهر می شود. که به ما امکان اختصاصی نمودن عملیات چاپ را می دهد.



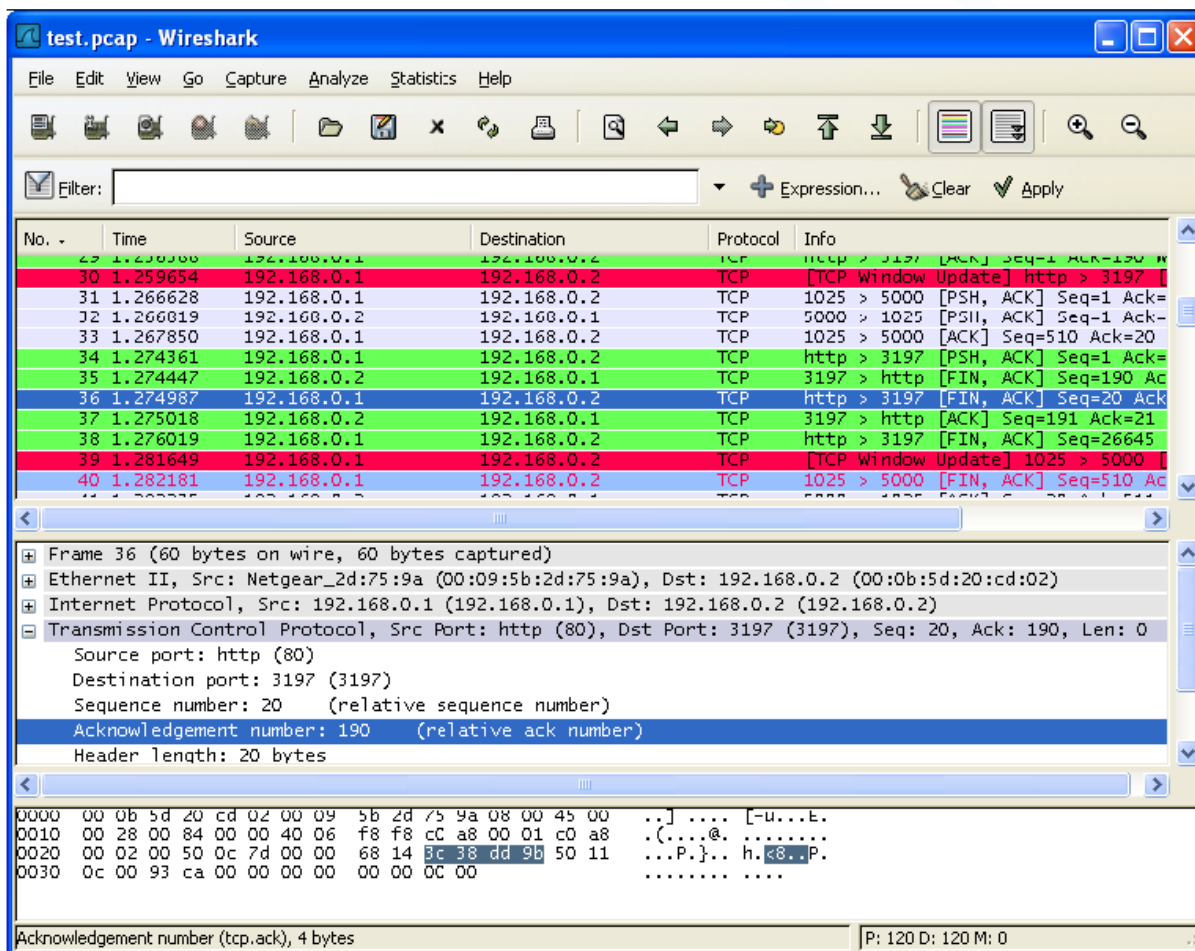
شکل: ۲۴ پنجره ی چاپ

کارکردن با پکت های ضبط شده

دیدن پکت های ضبط شده

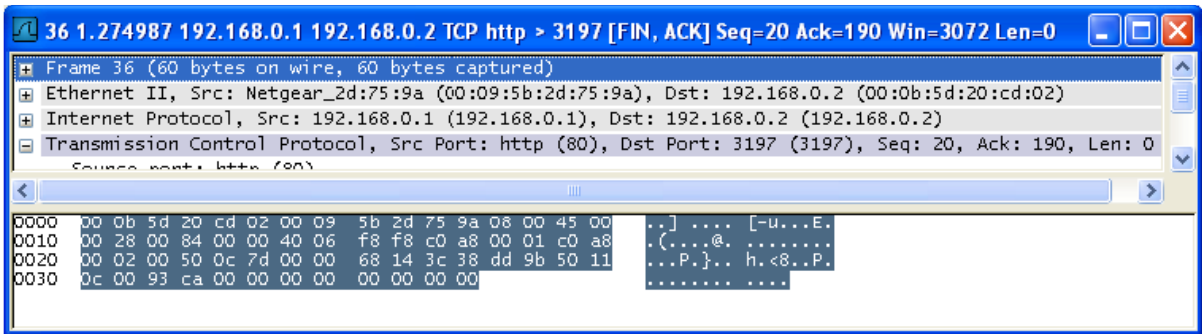
با کلیک کردن روی یک پکت در صفحه ی لیست پکت، می توان آن پکت را دید که با استفاده از گزینه ی view امکان دیدن نمایش درختی و بایتی آن پکت وجود دارد. می توان هر قسمتی از نمایش درختی را با کلیک کردن

روی نماد plus توسعه داد. یک نمونه از پکت TCP در شکل زیر نمایش داده شده است. همانطور که مشاهده می‌شود شماره‌ی Acknowledgment در هدر TCP نشان داده شده است.



شکل ۲۵: Wireshark با یک پکت TCP برای دیدن

علاوه بر این می‌توان پکت‌های مشخصی را در پنجره‌ی مجزا دید، مانند شکل زیر. بدین منظور بایستی روی پکت موردنظر کلیک راست کرد و گزینه‌ی "Show Packet in New Windows" را انتخاب نمود. بدین وسیله به راحتی می‌توان چندین پکت را با هم مقایسه کرد.

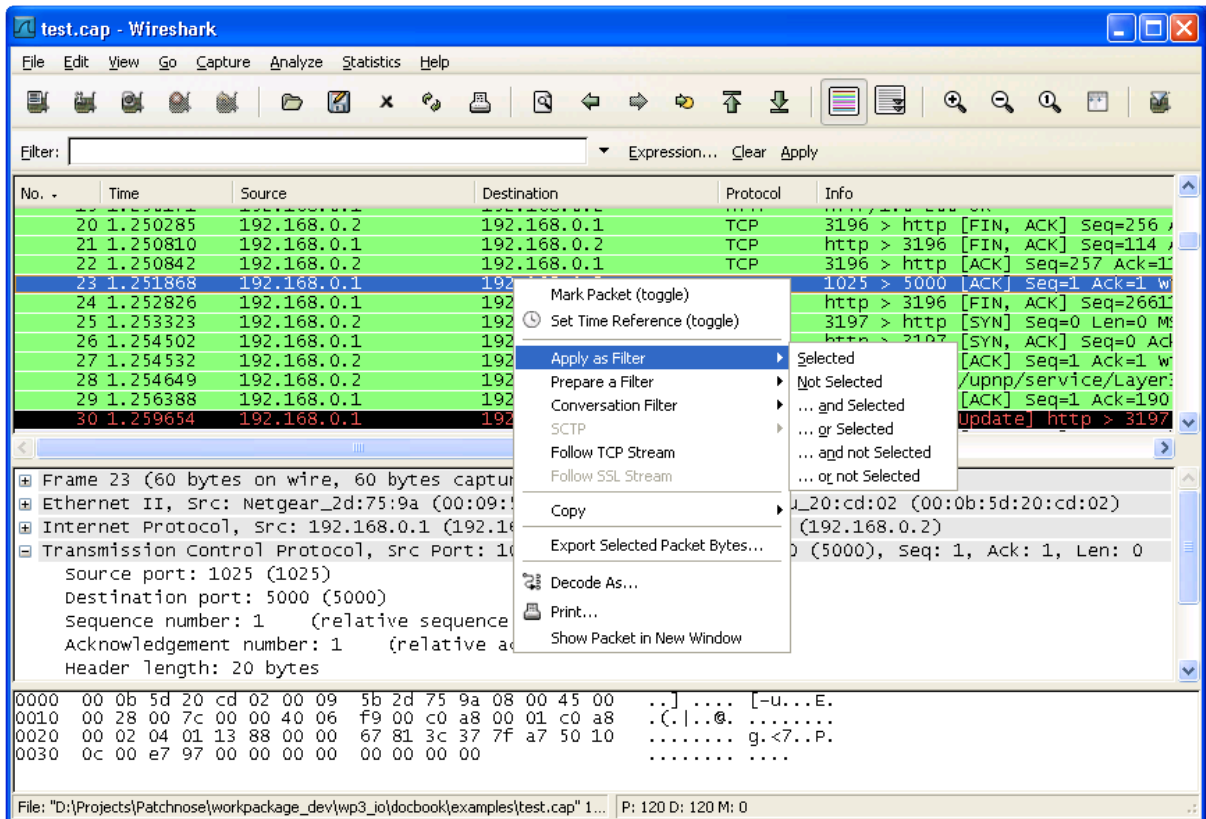


شکل ۲۶: دیدن پکت در یک صفحه‌ی مجزا

منوهای Pop-up

می‌توان یک منوی pop-up در صفحه‌های لیست پکت‌ها، جزییات پکت یا بایت‌های پکت با کلیک راست کردن در روی این صفحات، آورد.

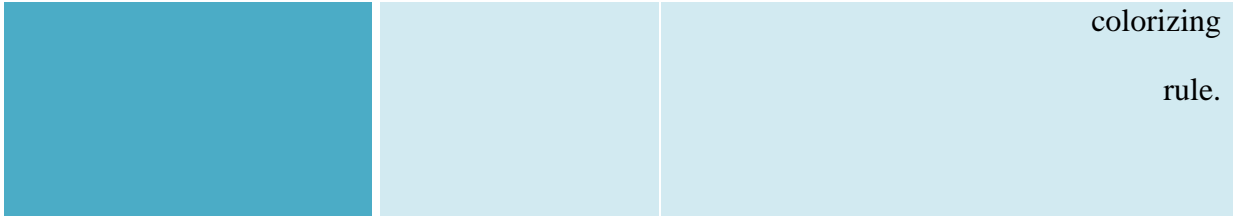
منوی Pop-up در صفحه‌ی لیست پکت



شکل ۲۷: منوی pop-up در صفحه‌ی لیست پکت

جدول زیر یک خلاصه از توابع موجود در این صفحه را نشان می‌دهد.

Item	Identical to main menu's item:	Description
Mark/unmark a packet.	Edit	Mark/unmark a packet.
Set Time Reference (toggle)	Edit	Set/reset a time reference.
.....		
Apply as Filter	Analyze	Prepare a display filter based on the currently selected item.
Conversation Filter		This menu item applies a display filter with the address information from the selected packet. E.g. the IP menu entry will set a filter to show the traffic between the two IP addresses of the current packet. XXX - add a new section describing this better.
Colorize Conversation	-	This menu item uses a display filter with the address information from the selected packet to build a new



دانشگاه تهران

SCTP	-	XXX - add an explanation of this.
Follow TCP Stream	Analyze	Allows you to view all the data on a TCP stream between a pair of nodes.
Follow SSL Stream	Analyze	Same as "Follow TCP Stream" but for SSL. XXX - add a new section describing this better.

Copy/ Summary (Text)	-	Copy the summary fields as displayed to the clipboard, as tab-separated text.
Copy/ Summary (CSV)	-	Copy the summary fields as displayed to the clipboard, as comma-separated text.
Copy/ As Filter		Prepare a display filter based on the currently selected item and copy that filter to the clipboard.
Copy/ Bytes (Offset)	-	Copy the packet bytes to the clipboard in

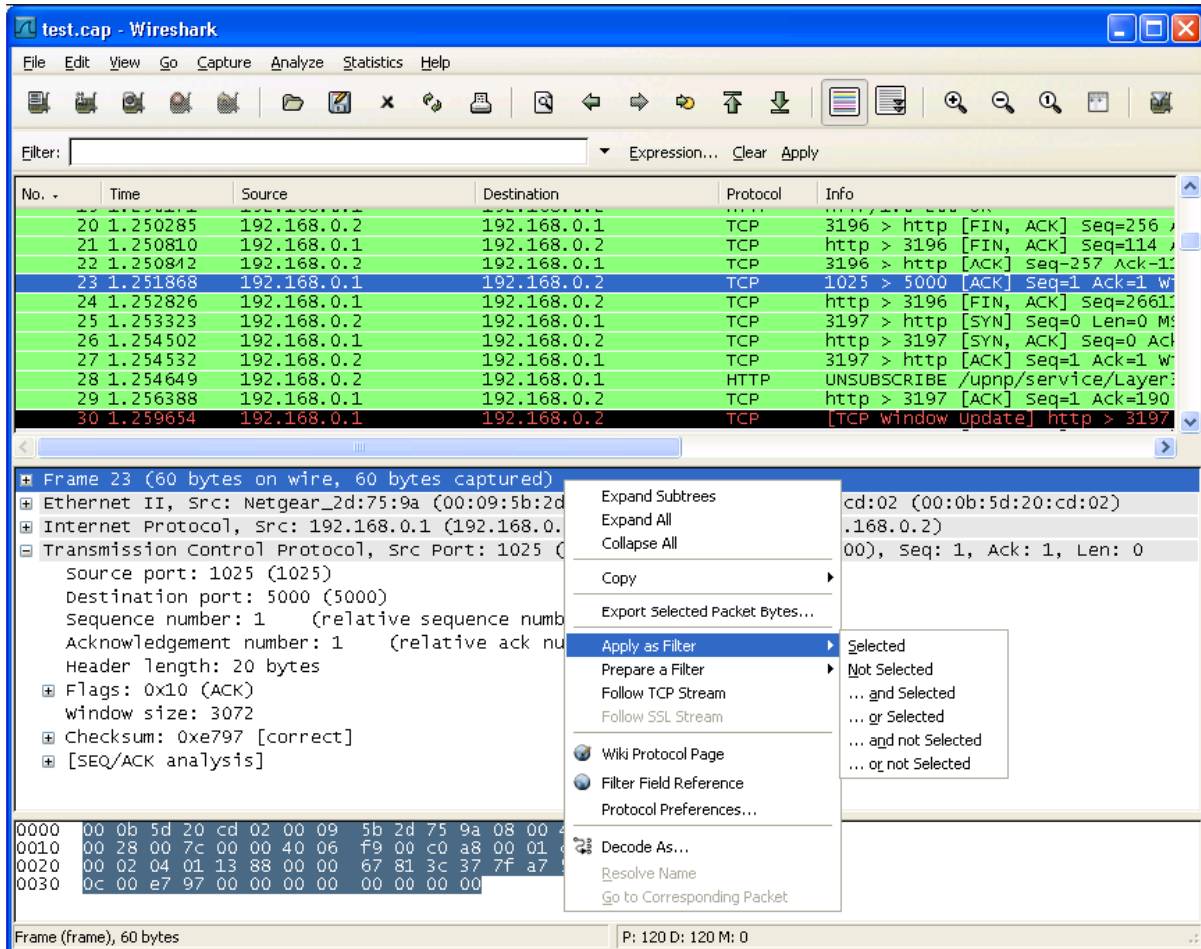
Hex Text)		hexdump-like format.
Copy/ Bytes (Offset Hex)	-	Copy the packet bytes to the clipboard in hexdump-like format, but without the text portion.
Copy/ Bytes (Printable Text Only)	-	Copy the packet bytes to the clipboard as ASCII text, excluding non-printable characters.
Copy/ Bytes (Hex Stream)	-	Copy the packet bytes to the clipboard as an unpunctuated list of hex digits.
Copy/ Bytes (Binary Stream)	-	Copy the packet bytes to the clipboard as raw binary. The data is stored in the clipboard as MIME-type "application/octet-stream". This option is not available in versions of Wireshark built using GTK+ 1.x.
Export Selected	File	This menu item is the same as the File menu item of the

Packet Bytes...		same name. It allows you to export raw packet bytes to a binary file.

Decode As...	Analyze	Change or apply a new relation between two dissectors.
Print...	File	Print packets.
Show Packet in New Window	View	Display the selected packet in a new window.

جدول ۱

منوی Pop-up در صفحه‌ی جزئیات پکت

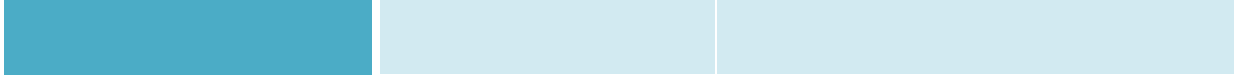


شکل ۲۸: منوی Pop-up در صفحه‌ی جزئیات پکت

جدول زیر یک خلاصه از توابع موجود در این صفحه را نشان می‌دهد.

Item	Identical to main menu's item:	Description
Expand Subtrees	View	Expand the currently selected subtree.
Expand All	View	Expand all subtrees in all packets in the capture.
Collapse All	View	Wireshark keeps a list of all the protocol subtrees that are expanded, and uses it to ensure that the correct subtrees are expanded when you display a packet. This menu item collapses the tree view of all packets in the capture list.

Copy/ Description	-	Copy the displayed text of the selected field to the system clipboard.
Copy/ As Filter	Edit	Prepare a display filter based on the currently selected item and copy it to the clipboard.



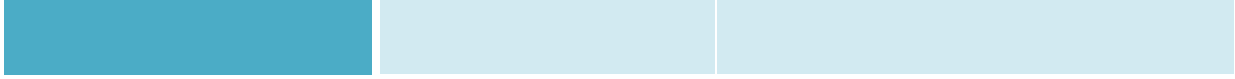
دانشپس پژوهشی

Copy/ Bytes (Offset Hex Text)		<ul style="list-style-type: none"> - Copy the packet bytes to the clipboard in hexdump-like format; similar to the Packet List Pane command, but copies only the bytes relevant to the selected part of the tree (the bytes selected in the Packet Bytes Pane).
Copy/ Bytes (Offset Hex)		<ul style="list-style-type: none"> - Copy the packet bytes to the clipboard in hexdump-like format, but without the text portion; similar to the Packet List Pane command, but copies only the bytes relevant to the selected part of the tree (the bytes selected in the Packet Bytes Pane).
Copy/ Bytes (Printable Text Only)		<ul style="list-style-type: none"> - Copy the packet bytes to the clipboard as ASCII text, excluding non-printable characters; similar to the Packet List Pane command, but copies only the bytes relevant to the selected part of the tree (the bytes selected in the Packet Bytes Pane).



دائیتیس نئوادی

Copy/ Bytes (Hex Stream)		<ul style="list-style-type: none"> - Copy the packet bytes to the clipboard as an unpunctuated list of hex digits; similar to the Packet List Pane command, but copies only the bytes relevant to the selected part of the tree (the bytes selected in the Packet Bytes Pane).
Copy/ Bytes (Binary Stream)		<ul style="list-style-type: none"> - Copy the packet bytes to the clipboard as raw binary; similar to the Packet List Pane command, but copies only the bytes relevant to the selected part of the tree (the bytes selected in the Packet Bytes Pane). The data is stored in the clipboard as MIME-type "application/octet-stream". This option is not available in versions of Wireshark built using GTK+ 1.x.
Export Selected Packet Bytes...	File	<p>This menu item is the same as the File menu item of the same name. It allows you to export raw packet bytes to a binary file.</p>



دانشگاه تهران
دانشکده مهندسی

Apply as Filter	Analyze	Prepare and apply a display filter based on the currently selected item
Prepare a Filter	Analyze	Prepare a display filter based on the currently selected item.
Colorize with Filter	-	Prepare a display filter based on the currently selected item and use it to prepare a new colorize rule.
Follow TCP Stream	Analyze	Allows you to view all the data on a TCP stream between a pair of nodes.
Follow SSL	Analyze	
Stream		Same as "Follow TCP Stream" but for SSL. XXX - add a new section describing this better.

Wiki Protocol Page		- Show the wiki page corresponding to the currently selected protocol in your web browser.
Filter Field Reference		- Show the filter field reference web page corresponding to the currently selected protocol in your web browser.
Protocol Preferences...		- The menu item takes you to the properties dialog and selects the page corresponding to the protocol if there are properties associated with the highlighted field.

Decode As...	Analyze	Change or apply a new relation between two dissectors.
Resolve Name	View	Causes a name resolution to be performed for the selected packet, but NOT every packet in the capture.

Go to Corresponding Packet	Go	If the selected field has a corresponding packet, go to it. Corresponding packets will usually be a request/response packet pair or such.
----------------------------	----	--

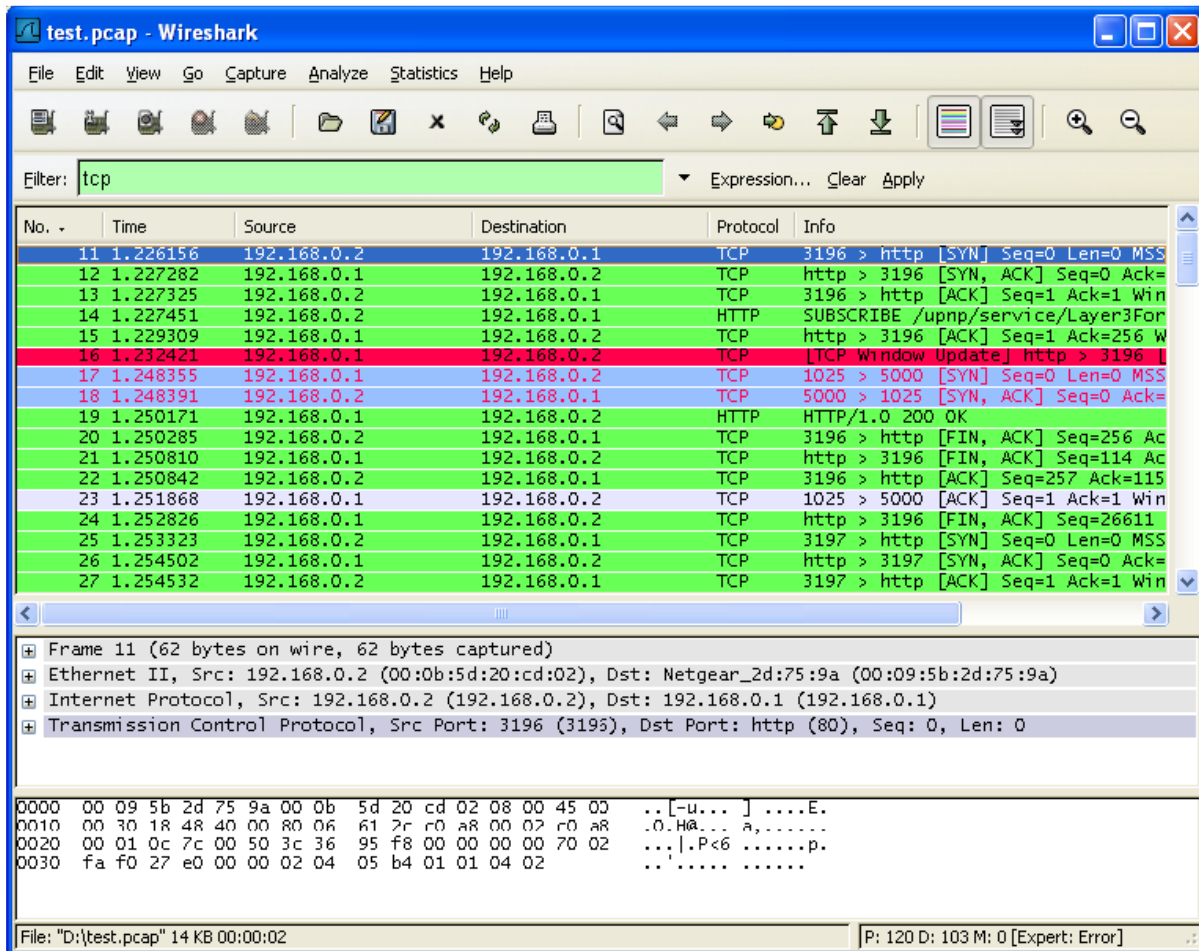
جدول ۲

فیلترکردن پکت‌ها در حال دیدن

Wireshark دو زبان برای فیلترکردن دارد: یکی در زمان ضبط پکت‌ها استفاده می‌شود و دیگری در زمان دیدن پکت‌ها. Display filter سبب می‌شود که بتوان روی پکت‌های دلخواه تمرکز کرد و بقیه را مخفی نمود. می‌توان پکت‌ها را با یک از موارد زیر انتخاب نمود:

- پروتکل
- حضور یک فیلد
- مقادیر فیلدها
- مقایسه بین فیلدها
- و ...

در شکل زیر پکت‌ها براساس پروتکل TCP فیلتر شده‌اند (پکت‌های ۱ تا ۱۰ پنهان شده‌اند). تعداد پکت‌ها همانند قبل باقی می‌ماند، بنابراین اولین پکت نشان داده شده دارای شماره‌ی ۱۱ می‌باشد.



شکل ۲۹: فیلتر کردن پکت‌های پروتکل TCP

ایجاد *display filter expressions*

Wireshark یک زبان ساده اما قوی برای *display filter* در اختیار می‌گذارد که با استفاده از آن می‌توان عبارات فیلتری پیچیده‌تری ساخت. می‌توان مقادیر پکت‌ها را با ترکیب این عبارات با هم مقایسه کرد.

فیلدهای *display filter*

هر فیلد در صفحه‌ی جزئیات پکت می‌تواند به عنوان یک رشته فیلتر استفاده شود، در نتیجه می‌توان تنها پکت‌هایی را که شامل این فیلد هستند نمایش داد. به عنوان مثال رشته‌ی *tcp* اگر به عنوان فیلتر باشد، تمام پکت‌های شامل پروتکل *tcp* دیده می‌شوند.

یک لیست کامل از فیلدهای فیلتر موجود در منوی "Help/Supported Protocols" از صفحه‌ی "Display Filter Field" موجود می‌باشد.

مقایسه‌ی مقادیر

می‌توان فیلترهایی ساخت که مقادیر را با استفاده از اپراتورهای مقایسه‌ای مقایسه می‌کنند.

English	C-like	Description and example
eq	==	Equal ip.src==10.0.0.5
ne	!=	Not equal ip.src!=10.0.0.5
gt	>	Greater than frame.len > 10
lt	<	Less than frame.len < 128
ge	>=	Greater than or equal to frame.len ge 0x100
le	<=	Less than or equal to frame.len <= 0x20

جدول ۳

علاوه بر این تمام فیلدهای پروتکل دارای نوع هستند. در جدول زیر انواع و نمونه‌ای از کاربرد آن‌ها نشان داده شده است.

Type	Example
Unsigned integer (8-bit, 16-bit, 24-bit, 32-bit)	You can express integers in decimal, octal, or hexadecimal. The following display filters are equivalent: ip.len le 1500 ip.len le 02734 ip.len le 0x436
Signed integer (8-bit, 16-bit, 24-bit, 32-bit)	
Boolean	A boolean field is present in the protocol decode only if its value is true. For example, tcp.flags.syn is present, and thus true, only if the SYN flag is present in a TCP segment header. Thus the filter expression tcp.flags.syn will select only those packets for which this flag exists, that is, TCP segments where the segment header contains the SYN flag. Similarly, to find sourcerouted token ring packets, use a filter expression of tr.sr.
Ethernet address (6 bytes)	Separators can be a colon (:), dot (.) or dash (-) and can have one or two bytes between separators: eth.dst == ff:ff:ff:ff:ff:ff eth.dst == ff-ff-ff-ff-ff-ff eth.dst == ffff.ffff.ffff
IPv4 address	ip.addr == 192.168.0.1 Classless InterDomain Routing (CIDR) notation can be used to test if an IPv4 address is in a certain subnet. For example, this display filter will find all packets in the 129.111 Class-B network: ip.addr == 129.111.0.0/16
IPv6 address	ipv6.addr == ::1
IPX address	ipx.addr == 00000000.ffffffffffff

String (text)	http.request.uri == "http://www.wireshark.org/"
---------------	---

جدول ۴: انواع فیلدهای display filter

ترکیب کردن عبارات

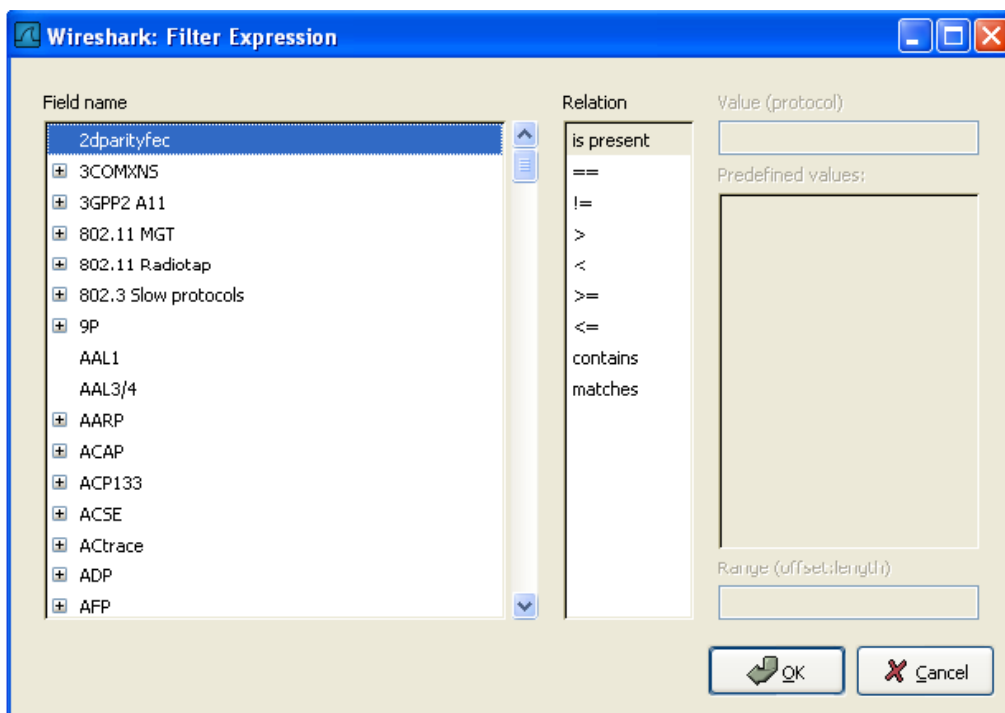
با استفاده از اپراتورهای منطقی زیر می توان عبارات فیلتر را با هم ترکیب کرد.

English	C-like	Description and example
and	&&	Logical AND ip.src==10.0.0.5 and tcp.flags.fin
or		Logical OR ip.src==10.0.0.5 or ip.src==192.1.1.1
xor	^^	Logical XOR tr.dst[0:3] == 0.6.29 xor tr.src[0:3] == 0.6.29
not	!	Logical NOT not llc
[...]		Substring Operator Wireshark allows you to select subsequences of a sequence in rather elaborate ways. After a label you can place a pair of brackets [] containing a comma separated list of range specifiers. eth.src[0:3] == 00:00:83 The example above uses the n:m format to specify a single range. In this case n is the beginning offset and m is the length of the range being specified. eth.src[1-2] == 00:83 The example above uses the n-m format to specify a single range. In this case n is the beginning offset and m is the ending offset. eth.src[:4] == 00:00:83:00

		<p>The example above uses the :m format, which takes everything from the beginning of a sequence to offset m. It is equivalent to 0:m eth.src[4:] == 20:20</p> <p>The example above uses the n: format, which takes everything from offset n to the end of the sequence. eth.src[2] == 83</p> <p>The example above uses the n format to specify a single range. In this case the element in the sequence at offset n is selected. This is equivalent to n:1. eth.src[0:3,1-2,:4,4:,2] == 00:00:83:00:83:00:00:83:00:20:20:83</p> <p>Wireshark allows you to string together single ranges in a comma separated list to form compound ranges as shown above.</p>
--	--	---

جدول ۵: اپراتورهای منطقی display filter

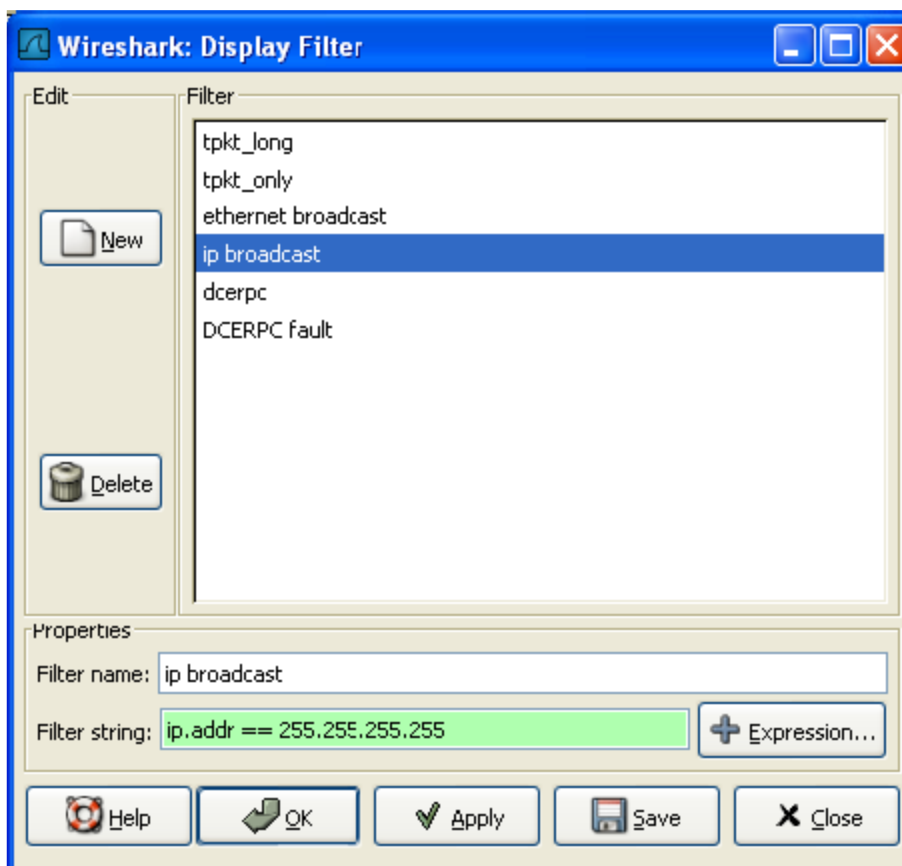
اگر با سیستم فیلترینگ Wireshark آشنا باشیم و بدانیم چه برچسب‌هایی برای فیلترهایمان استفاده کنیم، به سرعت می‌توان این کار را انجام داد. اگرچه می‌توان با استفاده از Filter Expression dialog box نیز فیلترینگ را انجام داد.



شکل ۳۰: The "Filter Expression" dialog box

تعریف و ذخیره کردن فیلترها

با Wireshark می‌توان فیلتر تعریف کرد و برای استفاده‌ی مجدد به آن برچسب زد. برای تعریف یک فیلتر جدید یا ویرایش کردن آن، گزینه‌ی Capture Filter از منوی Capture یا گزینه‌ی Display Filter از منوی Analyze را انتخاب می‌کنیم. dialog box زیر ظاهر می‌شود که می‌توان فیلتر جدید را تعریف نمود.



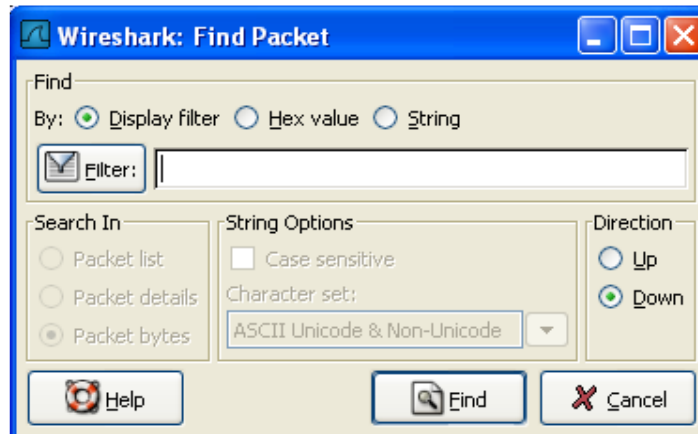
شکل ۳۱: The "Capture Filters" and "Display Filters" dialog boxes

تعریف و ذخیره کردن ماکروهای فیلتر

با استفاده از Wireshark می‌توان ماکروهای فیلتر تعریف نمود و برای استفاده‌ی مجدد به آن برچسب زد.

پیدا کردن پکت‌ها

می‌توان به سادگی پکت‌هایی را در فایل ضبط شده پیدا کرد. بدین منظور از منوی Edit، گزینه‌ی Find packet را انتخاب می‌کنیم



شکل ۳۲: The "Find Packet" dialog box

رفتن به یک پکت مشخص

با استفاده از منوی Go می‌توان به سادگی به یک پکت مشخص رفت.

دستور "Go Back"

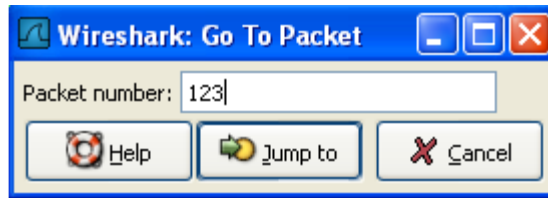
از این گزینه برای برگشتن به packet history استفاده می‌شود، همانند page history در مرورگرهای وب جاری.

دستور "Go Forward"

از این گزینه برای رفتن به جلو به packet history استفاده می‌شود، همانند page history در مرورگرهای وب جاری.

The "Go to Packet" dialog box

با استفاده از این گزینه، می‌توان شماره‌ی پکت را وارد کرد. با فشردن دکمه‌ی Jump to می‌توان به پکت موردنظر رفت.



شکل ۳۳: The "Go to Packet" dialog box

دستور "Go to Corresponding packet"

اگر یک فیلد پروتکل که به یک پکت در فایل ضبط شده اشاره می‌کند، انتخاب شده باشد با استفاده از این دستور می‌توان به آن پرش کرد.

دستور "Go to First Packet"

با استفاده از این دستور می‌توان به اولین پکت پرش کرد.

دستور "Go to Last Packet"

با استفاده از این دستور می‌توان به آخرین پکت پرش کرد.

نشانه‌گذاری پکت‌ها

می‌توان پکت‌ها در صفحه‌ی لیست پکت‌ها نشانه‌گذاری کرد. در اینصورت پکت موردنظر با زمینه‌ی سیاه نشان داده خواهد شد. نشانه‌گذاری پکت برای پیدا کردن آن در زمان تحلیل یک فایل بزرگ ضبط شده می‌تواند مفید باشد.

فرمت‌های نمایش زمان و مراجع زمان

هنگامی که پکت‌ها ضبط می‌شوند، هر پکت دارای مهرزمانی است. این زمان‌ها در فایل ضبط شده ذخیره می‌شوند، بنابراین برای تحلیل‌های آتی در دسترس هستند.

فرمت‌هایی نمایش زمان به صورت‌های زیر می‌باشند:

- **Date and Time of Day**: ۱۹۷۰-۰۱-۰۱ ۰۱:۰۲:۰۳,۱۲۳۴۵۶ تاریخ مطلق و زمان روزی که پکت ضبط شده است.

- **Time of Day**: ۰۱:۰۲:۰۳,۱۲۳۴۵۶ زمان مطلق روزی که پکت ضبط شده است.

- **Seconds Since Beginning of Capture**: ۱۲۳,۱۲۳۴۵۶ زمان نسبی از زمان شروع ضبط فایل یا اولین زمان مرجع قبل از این پکت.

- **Seconds Since Previous Captured Packet**: ۱,۱۲۳۴۵۶ زمان نسبت به پکت قبلی ضبط شده

- **Seconds Since Previous Displayed Packet**: ۱,۱۲۳۴۵۶ زمان نسبت به پکت قبلی نمایش داده شده

- **Seconds Since Epoch** (۱۹۷۰-۰۱-۱۰) : ۱۲۳۴۵۶۷۸۹۰,۱۲۳۴۵۶ زمان نسبت به مبدا تاریخ (نیمه شب UTC ماه ژانویه ۱۹۷۰)

دقت‌های موجود در Wireshark عبارتند از:

- **Automatic**: این دقت به صورت پیش فرض در Wireshark استفاده می‌شود.

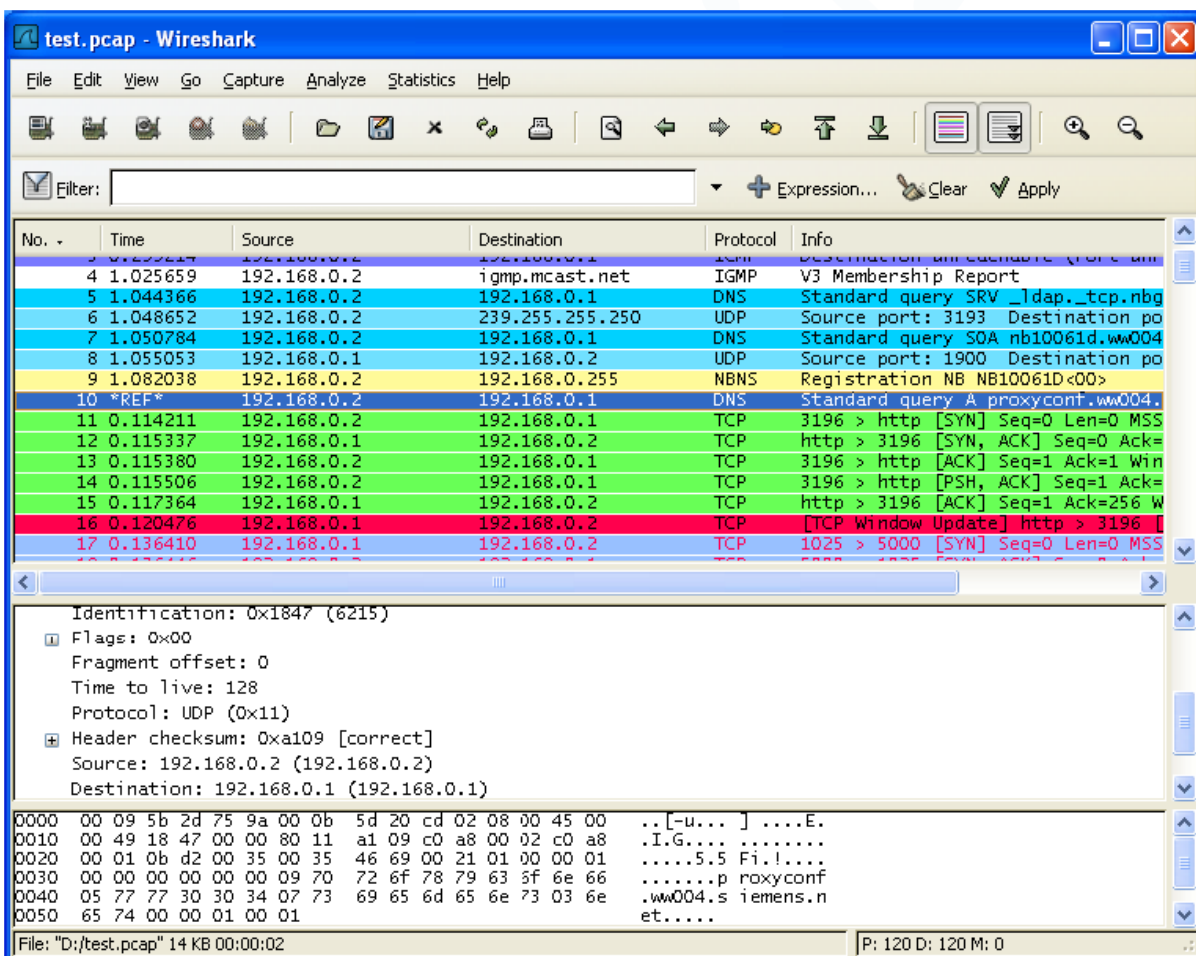
Seconds, Deciseconds, Centiseconds, Milliseconds یا Nanoseconds :

مثالی از دقت: اگر یک زمان داشته باشیم که دارای فرمت "Seconds Since Previous Packet" باشد، ممکن است دارای مقدار ۱,۱۲۳۴۵۶ باشد. این فرمت دارای دقت اوماتیک می‌باشد، اگر از روش دوم استفاده شود با دقت Seconds مقدار ۱ و با دقت Nanoseconds مقدار ۱,۱۲۳۴۵۶۰۰۰ نشان داده می‌شود.

Packet time referencing

کاربر می‌تواند مراجع زمانی پکت‌ها را تغییر دهد. منظور از مرجع زمانی نقطه‌ی شروع برای تمام محاسبات زمانی پکت‌ها می‌باشد. دیدن مقادیر زمان مربوط به پکت‌ها (به عنوان مثال زمان شروع یک درخواست جدید) می‌تواند مفید باشد. می‌توان چندین مرجع زمانی در فیل ضبط شده تنظیم کرد.

برای کارکردن با مرجع زمانی، از منوی "Edit" گزینه‌ی "Time Reference" را انتخاب کنید.



شکل ۳۴: نمایش یک پکت با مرجع زمانی

مرجع زمانی یک پکت با رشته‌ی "REF" در ستون زمان نشانه‌گذاری شده است (به پکت شماره‌ی ۱۰ نگاه کنید).

آمار

Wireshark یک محدوده ی وسیعی از آمارهای شبکه را از طریق گزینه ی Statistics فراهم می آورد. این آمارها از اطلاعات کلی درباره ی فایل ضبط شده نظیر تعداد پکت های عبوری از شبکه تا آمار پروتکل های شبکه نظیر تعداد درخواست ها^۱ و پاسخ های^۲ HTTP را شامل می شود.

بعضی از آمارهای کلی عبارتند از:

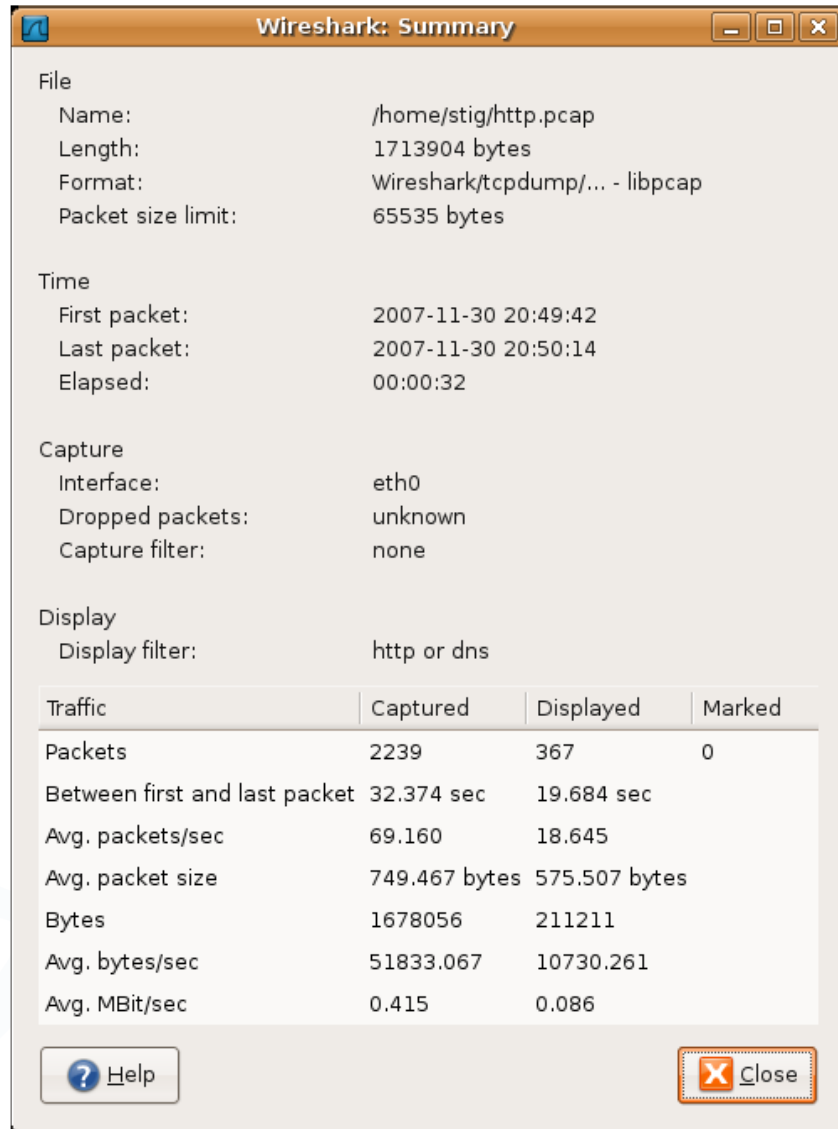
- Summary درباره ی فایل ضبط شده.
- Protocol Hierarchy از پکت های ضبط شده.
- Conversations نظیر ترافیک بین آدرس های IP مشخص.
- Endpoints نظیر ترافیک ورودی یا خروجی یک آدرس IP.
- IO Graphs برای متصور ساختن تعداد پکت ها در زمان.

آمارهای خاص پروتکل عبارتند از:

- Service Response Time بین درخواست و پاسخ برخی پروتکل ها.
- Various other برای آمارهای مشخص پروتکل.

^۱ requests

^۲ responses



شکل ۳۵: پنجره‌ی Summary

همانطور که در بالا ذکر شد این گزینه آمار کلی درباره‌ی فایل ضبط شده بدست می‌دهد. این آمارها عبارتند از:

File: اطلاعات کلی درباره‌ی فایل ضبط شده.

Time: زمان اولین و آخرین بسته‌ی ضبط شده و همچنین مدت زمان بین آنها.

Capture: اطلاعات در مدت زمان ضبط بسته‌ها را نشان می‌دهد.

Display: بعضی از اطلاعات (نظیر `display filter`) را نمایش می‌دهد.

Traffic: بعضی از آمارها از دید ترافیک شبکه را بدست می‌دهد. اگر یک `display filter` برای جریان شبکه تنظیم شده باشد، می‌توان مقادیر را در ستون `Captured` مشاهده کرد و اگر پکت‌ها نشانه‌گذاری شده باشند می‌توان مقادیر را در ستون `Marked` مشاهده نمود. مقادیر در ستون `Captured` همانند قبل باقی می‌مانند درحالی‌که مقادیر در ستون `Displayed`، مقادیر معادل پکت‌های نشان داده شده در فیلد `display` را نمایش می‌دهند. مقادیر ستون `Marked` نیز مقادیر معادل در پکت‌های نشانه‌گذاری شده را نشان می‌دهند.

پنجره‌ی Protocol Hierarchy

این قسمت سلسله مراتب پروتکل را نمایش می‌دهد.

Wireshark: Protocol Hierarchy Statistics

Display filter: http or dns

Protocol	% Packets	Packets	Bytes	Mbit/s	End Packets	End Bytes	End Mbit/s
▼ Frame	100.00%	367	211211	0.086	0	0	0.000
▼ Ethernet	100.00%	367	211211	0.086	0	0	0.000
▼ Internet Protocol	100.00%	367	211211	0.086	0	0	0.000
▼ Transmission Control Protocol	93.46%	343	207029	0.084	113	82553	0.034
▼ Hypertext Transfer Protocol	62.67%	230	124476	0.051	189	93393	0.038
Compuserve GIF	7.36%	27	17114	0.007	27	17114	0.007
Line-based text data	3.27%	12	12265	0.005	12	12265	0.005
JPEG File Interchange Format	0.27%	1	990	0.000	1	990	0.000
eXtensible Markup Language	0.27%	1	714	0.000	1	714	0.000
▼ User Datagram Protocol	6.54%	24	4182	0.002	0	0	0.000
Domain Name Service	6.54%	24	4182	0.002	24	4182	0.002

Help Close

شکل ۳۶: پنجره‌ی Protocol Hierarchy

همانطور که در شکل بالا مشاهده می‌شود، این گزینه درخت تمام پروتکل‌های ضبط شده را نمایش می‌دهد. می‌توان زیر درخت‌ها را با کلیک کردن روی آیکون‌های plus/minus توسعه و یا کاهش داد.

هر سطر شامل مقادیر آماری یک پروتکل می‌باشد. Display filter فیلتر نمایش جاری را نشان می‌دهد.

ستون‌های زیر شامل مقادیر آماری موجود می‌باشند:

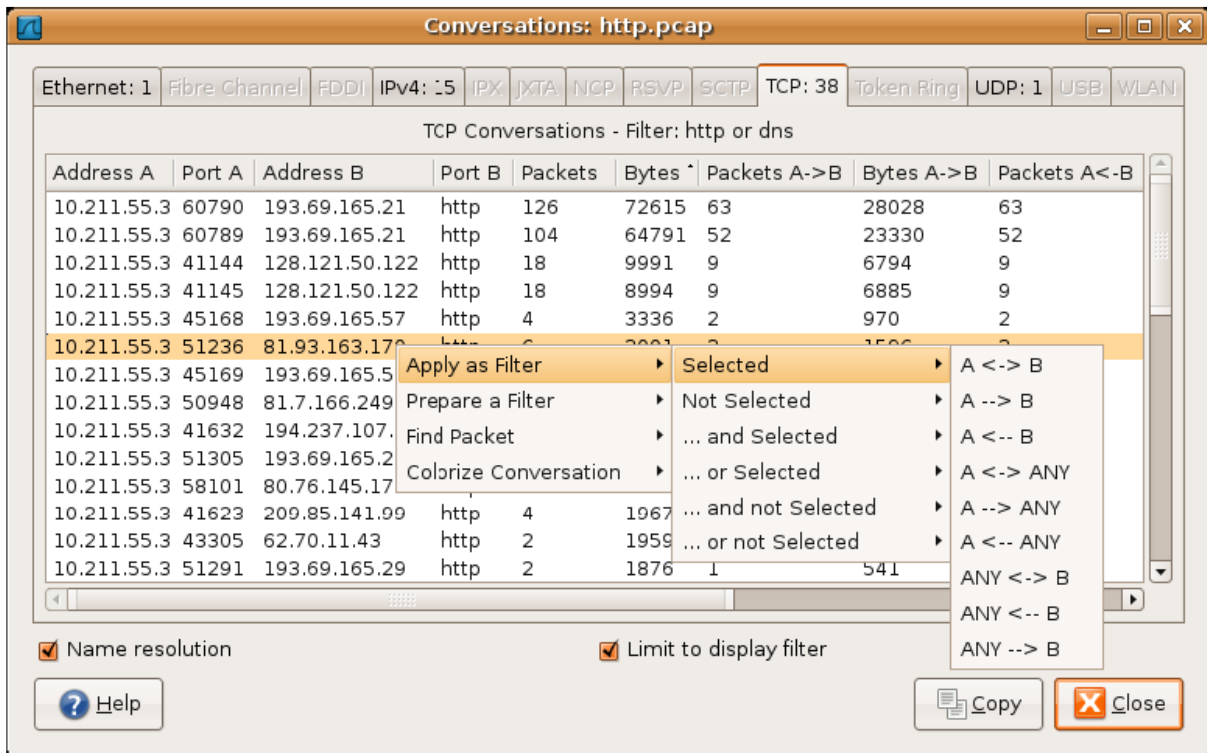
- Protocol: نام پروتکل
- %Packets: درصد پکت‌های پروتکل در فایل ضبط شده

- Bytes: تعداد مطلق بایت‌های پروتکل
- Mbit/s: پهنای باند پروتکل در مدت زمان ضبط بسته‌ها
- End Packets: تعداد مطلق پکت‌های پروتکل (درحالی‌که این پروتکل بالاترین پروتکل برای دیکد شدن بوده است)
- End Bytes: تعداد مطلق بایت‌های پروتکل (درحالی‌که این پروتکل بالاترین پروتکل برای دیکد شدن بوده است)
- End Mbit/s: پهنای باند پروتکل در مدت زمان ضبط بسته‌ها (درحالی‌که این پروتکل بالاترین پروتکل برای دیکد شدن بوده است)

پنجره‌ی *Conversations*

منظور از مکالمه یا Conversation در شبکه، ترافیک بین دو نقطه‌ی انتهایی مشخص می‌باشد. به عنوان مثال یک IP conversation عبارتست از تمام ترافیک‌ها بین دو آدرس IP.

این پنجره شبیه پنجره‌ی Endpoints که در ادامه توضیح خواهیم داد. علاوه بر فیلدهای آدرس، شمارنده‌های پکت و شمارنده‌های بایت پنجره‌ی مکالمه چهار ستون دیگر نیز اضافه می‌کند که عبارتند از: زمان بین شروع ضبط و شروع مکالمه بر حسب ثانیه (Rel Start)، زمان مکالمه بر حسب ثانیه و میانگین بیت‌ها (نه بایت‌ها) در هر ثانیه در تمام جهات.



شکل ۳۷: پنجره‌ی Conversations

هر سطر در لیست مقادیر آماری را برای دقیقاً یک مکالمه نمایش می‌دهد.

پنجره‌ی Conversation List برای پروتکل مشخص

قبل از اینکه پنجره‌ی بالا که شامل پروتکل‌های مختلف می‌باشد، در دسترس باشد هر کدام از صفحه‌های آن به عنوان یک پنجره‌ی مجزا نمایش داده شده‌اند. اگرچه پنجره‌ی مرکب برای استفاده آسانتر است، اما هر کدام از آنها از طریق این پنجره به صورت جدا قابل رویت هستند. دلیل اصلی این است که برای فایل‌های ضبط شده‌ی خیلی بزرگ دسترسی از این طریق سریعتر است.

پنجره‌ی Endpoints

منظور از endpoint در شبکه، نقطه‌ی انتهایی منطقی جداکننده‌ی ترافیک پروتکل از یک لایه‌ی پوتکل مشخص می‌باشد.

آمار endpoint در Wireshark، نقاط انتهایی زیر را برای محاسبه به کار می‌برد:

Ethernet: یک نقطه‌ی انتهایی Ethernet معادل آدرس MAC مربوط به Ethernet می‌باشد.

Fibre Channel: XXX – اطلاعات را در اینجا وارد کنید.

FDDI: یک نقطه‌ی انتهایی FDDI معادل آدرس MAC مربوط به FDDI می‌باشد.

IPv4: یک نقطه‌ی انتهایی IP معادل آدرس IP مربوط به آن می‌باشد.

IPX: XXX – اطلاعات را اینجا وارد کنید.

TCP: یک نقطه‌ی انتهایی TCP ترکیب یک آدرس IP و پورت TCP استفاده شده می‌باشد. بنابراین پورت‌های متفاوت TCP با آدرس‌های IP یکسان، نقاط انتهایی متفاوت می‌باشند.

Token Ring: یک نقطه‌ی انتهایی Token Ring معادل آدرس MAC مربوط به Token Ring می‌باشد.

UDP: یک نقطه‌ی انتهایی UDP ترکیب یک آدرس IP و پورت UDP استفاده شده می‌باشد. بنابراین پورت‌های متفاوت UDP با آدرس‌های IP یکسان، نقاط انتهایی متفاوت می‌باشند.

پنجره‌ی Endpoints آمار مربوط به نقاط انتهایی ضبط شده را نشان می‌دهد.

Endpoints: http.pcap

Ethernet: 2 | Fibre Channel | FDDI | IPv4: 16 | IPX | JXTA | NCP | RSVP | SCTP | TCP: 51 | Token Ring | UDP: 2 | USB | WLAN

IPv4 Endpoints - Filter: http or dns

Address	Packets	Bytes	Tx Packets	Tx Bytes	Rx Packets	Rx Bytes
10.211.55.3	367	211211	184	91005	183	120206
193.69.165.21	230	137406	115	86048	115	51358
128.121.50.122	36	18985	18	5306	18	13679
193.69.165.29	28	18580	14	10235	14	8345
10.211.55.1	24	4182	12	3275	12	907
193.69.165.57	8	5824	4	3855	4	1000
62.70.11.43	6	3596	3	2075	3	1980
81.7.166.249	6	5165	3	1880	3	1150
81.93.163.170	7	3581	3	1400	4	2181
209.85.141.99	4	1967	2	580	2	1000
81.93.172.130	4	1610	2	520	2	1000
194.237.107.53	4	3817	2	1830	2	1980
193.88.71.150	4	2193	2	1037	2	1150
66.102.9.99	2	1060	1	425	1	635
194.237.107.154	2	1252	1	277	1	975

Name resolution Limit to display filter

Buttons: Help, Copy, Close

شکل ۳۸: پنجره ی Endpoints

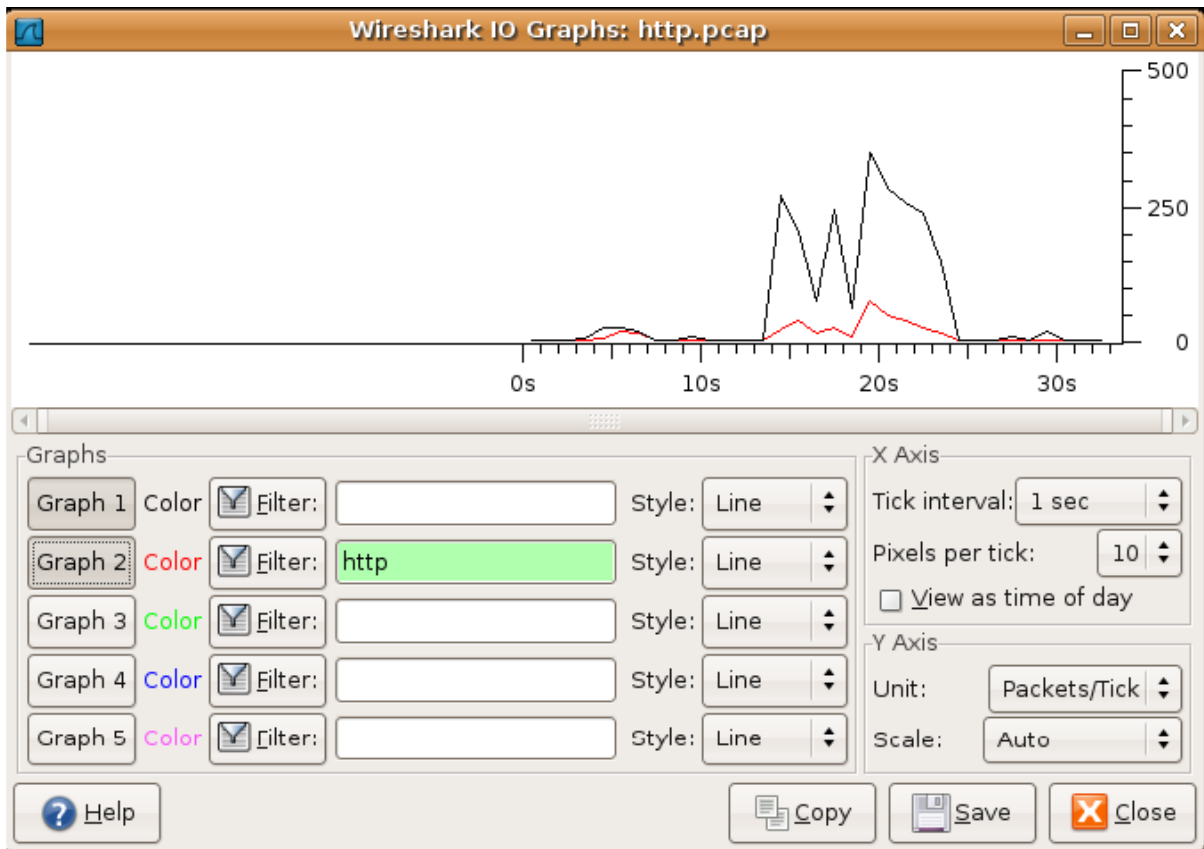
برای هر پروتکل پشتیبانی شده، یک tab در پنجره نشان داده شده است. برچسب هر tab تعداد نقاط انتهایی ضبط شده را نشان می‌دهد (به عنوان مثال برچسب "Ethernet: ۵" می‌گوید که پنج نقطه‌ی انتهایی ضبط شده است). هر سطر در لیست مقادیر آماری برای دقیقاً یک نقطه‌ی انتهایی را نشان می‌دهد.

پنجره ی Endpoint List برای پروتکل مشخص

این پنجره نقاط انتهایی مربوط به هر پروتکل را در پنجره مجزایی نشان می‌دهد..

پنجره ی IO Graphs

این پنجره گراف‌های قابل پیکربندی توسط کاربر از پکت‌های شبکه را نشان می‌دهد. می‌توان تا پنج گراف رنگی متفاوت تعریف نمود.



شکل ۳۹: پنجره‌ی IO Graphs

کاربر می‌تواند پارامترهای زیر را تنظیم کند:

• گراف‌ها

- گراف ۱-۵: یکی از گراف‌های نوع ۱ تا ۵ را فعال می‌کند (تنها گراف ۱ به صورت پیش فرض فعال است)
- رنگ گراف
- فیلتر: یک display filter برای این گراف (تنها پکت‌هایی که از این فیلتر عبور می‌کنند، برای این گراف به حساب می‌آیند)

▪ مدل گراف: که می‌تواند یک از انواع Line, Impulse, Fbar یا Dot باشد.

• محور X

▪ فاصله‌ی علامت^۱

▪ تعداد پیکسل‌های هر علامت: می‌توان از ۱۰/۵/۲/۱ پیکسل برای هر علامت استفاده کرد.

▪ مشاهده به صورت زمان روز: می‌توان محور X را به صورت روز به جای ثانیه یا دقیقه برچسب گذاری کرد.

• محور Y

▪ واحد محور y که می‌تواند به صورت Packets/Tick, Bytes/Tick, Bits/Tick و Advanced .. باشد.

▪ مقیاس محور y (۱۰، ۲۰، ۵۰، ۱۰۰، ۲۰۰ و ...)

آمار ترافیک WLAN

این گزینه آمار ترافیک WLAN ضبط شده را نشان می‌دهد و ترافیک شبکه‌ی بی‌سیم را خلاصه می‌کند. درخواست‌های Probe در صورتیکه با SSID مطابقت کنند، در یک شبکه‌ی موجود ادغام می‌شوند.

^۱ Tick interval

Wireshark: WLAN Traffic Statistics: w1.pcap

WLAN Traffic Statistics

BSSID	Channel	SSID .	Beacons	Data Packets	Probe Req	Probe Resp	Auth	Deauth	Other	Percent	Protection
00:13:1a:a0:12:c0			0	58	0	0	0	0	0	0.04%	
00:02:e3:46:99:f8	11	AMX	744	6	0	14	0	0	0	0.46%	WEP
00:0e:2e:c2:15:07	1	Fortress GB	13	0	0	0	0	0	0	0.01%	
00:13:1a:6e:91:e0	1	Telenor Mobil WLAN	130030	9683	15	15441	3	0	2	94.43%	

Name resolution Only show existing networks

[Help](#) [Copy](#) [Close](#)

شکل ۴۰: آمار ترافیک WLAN

هر سطر در این لیست مقادیر آماری برای دقیقاً یک شبکه‌ی بی‌سیم را نشان می‌دهند.

این گزینه آمار ترافیک WLAN ضبط شده را نشان می‌دهد و ترافیک شبکه‌ی بی‌سیم را خلاصه می‌کند. درخواست‌های Probe در صورتیکه با SSID مطابقت کنند، در یک شبکه‌ی موجود ادغام می‌شوند.

Wireshark: WLAN Traffic Statistics: w1.pcap

WLAN Traffic Statistics

BSSID	Channel	SSID .	Beacons	Data Packets	Probe Req	Probe Resp	Auth	Deauth	Other	Percent	Protection
00:13:1a:a0:12:c0			0	58	0	0	0	0	0	0.04%	
00:02:e3:46:99:f8	11	AMX	744	6	0	14	0	0	0	0.46%	WEP
00:0e:2e:c2:15:07	1	Fortress GB	13	0	0	0	0	0	0	0.01%	
00:13:1a:6e:91:e0	1	Telenor Mobil WLAN	130030	9683	15	15441	3	0	2	94.43%	

Name resolution Only show existing networks

[Help](#) [Copy](#) [Close](#)

شکل ۴۱: آمار ترافیک WLAN

هر سطر در این لیست مقادیر آماری برای دقیقاً یک شبکه‌ی بی‌سیم را نشان می‌دهند.

Service Response Time

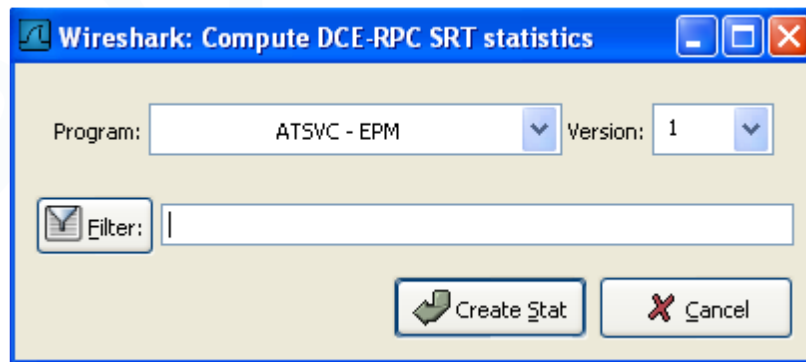
زمان پاسخ سرویس برابر زمان بین یک درخواست و پاسخ معادل آن می‌باشد. این مقدار برای بیشتر پروتکل‌ها در دسترس است و اکنون برای پروتکل‌های زیر در Wireshark موجود می‌باشند:

- DCE-RPC
- Fiber Channel
- H.225 RAS
- LDAP
- MGCP
- SMB

به عنوان مثال زمان پاسخ سرویس برای پروتکل DCE-RPC در زیر شرح داده شده است:

پنجره‌ی *Service Response Time DCE-RPC*

ابتدا اینترفیس پروتکل DCE-RPC را انتخاب می‌کنیم.



شکل ۴۲: پنجره‌ی "Compute DCE-RPC statistics"

به منظور کاهش تعداد پکت‌ها می‌توان به دلخواه یک display filter را انتخاب کرد.

Index	Procedure	Calls	Min SRT	Max SRT	Avg SRT

شکل ۴۳: پنجره‌ی "DCE-RPC Statistic for ..."

هر سطر معادل یک متد از اینترنتیس انتخاب شده می‌باشد (بنابراین اینترنتیس EPM در ورژن ۳، هفت تا متد دارد). برای هر متد، تعداد احضارها^۱ و آمارهای زمان SRT محاسبه شده است.

پنجره‌ی آمارها برای یک پروتکل مشخص

این پنجره اطلاعات جزئی پروتکل‌ها را نشان می‌دهد.

^۱ calls

- ۱) www.wireshark.org
- ۲) Ulf Lamping, Richard Sharpe, and Ed Warnicke, '*Wireshark User's Guide*,' NS Computer Software and Services P/L, 2008.