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

به نام خدا

۱	مقادمه
۲	بخش اول
۲	معرفی ابزار Wireshark
۲	برخی از اهداف مورد نظر Wireshark
۳	ويژگى ها
٤	آنچه Wireshark پشتیبانی نمی کن <i>د</i>
٥	نحوه ی نصب WireShark
٦	اينترفيس كاربر
Λ	منو
۹	صفحەي ليست پكت
۱۰	صفحەي جزييات پكت
11	صفحەي بايتھاي پکت
١٢	Statusbar
۱۳	طریقه ی ضبط نمودن داده های در جریان شبکه

١٥		أغاز ضبط اطلاعات
١٥		پنجرہ ی Capture Interfaces
١٧		پنجرہ ی Capture Options
22		جعبه ی محاوره ی Interface Details
۲٣		ضبط فایل ها
۲٥		فیلتر کردن حین ضبط اطلاعات
۲٦		فایل ها (ورودی/خروجی) و پرینت
۳۱		صدور اطلاعات از Wireshark
٣٦		کارکردن با پکت های ضبط شده
٣٦		دیدن پکتهای ضبط شده
٥٤		فیلترکردن پکتها در حال دیدن
00		ایجاد display filter expressions
77	_	آمار
٦٧		پنجرهی Summary
٦٨		پنجرمی Protocol Hierarchy
٧.		پنجرهی Conversations
۷١	شخص	پنجرہی Conversation List برای پروتکل م

V1	پنجرهی Endpoints
٧٣	پنجرهی Endpoint List برای پروتکل مشخص
٧٣	پنجرهی IO Graphs
۷۵	آمار ترافیک WLAN
VV	پنجرهی Service Response Time DCE-RPC
VA	پنجرهی آمارها برای یک پروتکل مشخص
Error! Bookmark not defined	نتايج بدست آمده
Error! Bookmark not defined	بررسی شبکهی دانشگاه امیر کبیر
Error! Bookmark not defined	بررسی شبکهی شرکت پروش دادهها
Error! Bookmark not defined.	بررسی یک ارتباط Dial-up
Error! Bookmark not defined	بخش دوم
Error! Bookmark not defined	مطالعه و بررسی نرم افزار Axence
٧٩	منابع

# فهرست اشكال

٤	شکل۱ : Wireshark بسته ها را ضبط می کند و امکان بازدید محتوای آنها را می دهد
۷	نىكل۲ : پنجرەي اصلى
۸	ئىكل:٣ منو
۹	لىكل٤ : صفحەي ليست پكت
۱۱	نىكلە : صفحەي جزييات پكت
۱۲	نیکل۲ : صفحهی بایتهای پکت
	نىكلv : Statusbar اوليە
۱۲	شکل:۸ statusbar با یک فایل لود شده
۱۳	شکل۹ : Statusbar با منوی پروفایل پیکربندی
۱۳	ئىكل.۱۰ : Statusbar با يك پيام display filter
۱٥	نیکل:۱۱ پنجره ی واسط ها ی ضبط
۱۷	شکل ۱۲: طریقه ی مخفی نمودن یک کارت شبکه از دید Wireshark
۱۸	ئىكل1۳ : پنجرە ى Capture Options
۲۳	نیکل ۱٤: جعبه ی محاوره ی "Interface Details"
77	شکل ۱۵: پنجره ی باز کردن یک فایل ضبط شده
۲۸	شکل ۱۶: پنجره ی ذخیره ی فایل

۳.	شکل۱۷ : پنجره ی ادغام فایل ها
۳۱	شکل:۱۸ نمونه ای از مجموعه فایل ها
٣٢	شکل :Export as Plain Text File ۱۹
٣٣	شکل .۲۰ : Export as PostScript File
٣٤	شکل:۲۱ Export as PSML File
٣٥	شکل Export as PDML File : ۲۲
٣٥	شکل۳۲ : Export selected packet bytes : ۳۳
	شکل:۲٤ پنجره ی چاپ
٣٧	شکل ۲۵: Wireshark با یک پکت TCP برای دی <i>د</i> ن
٣٨	شکل ۲٦: دیدن پکت در یک صفحهی مجزا
٣٩	شکل ۲۷: منوی pop-up در صفحهی لیست پکت
٤٥	شکل ۲۸: <b>منوی Pop-up در صفحهی جزییات پکت</b>
00	شکل ۲۹: فیلترکردن پکتهای پروتکل TCP
٦٠	شکل ۳۰: The "Filter Expression" dialog box
٦١	شکل The "Capture Filters" and "Display Filters" dialog boxes:۳۱
٦٢	The "Find Packet" dialog boxشکل ۳۳:
٦٣	شکار ۳۳: The "Go to Packet" dialog box

٦٥		شکل ۳٤: نمایش یک پکت با مرجع زمانی
77		شکل ۳۵: پنجرهی Summery
٦٩		شکل ۳۶: پنجرهی Protocol Hierachy
۷١		شکل ۳۷: پنجرهی Conversations
۷٣		شکل ۳۸: پـنـجـرهي Endpoints
٧٤		شکل ۳۹: پنجرهی IO Graphs
٧٦		شکل ٤٠: آمار ترافیک WLAN
٧٦		شکل ٤١: آمار ترافیک WLAN
vv		شکل ٤٢: پنجرهي "ompute DCE-RPC statistics
		شکل ٤٣: پنجرهي " DCE-RPC Statistic for"
Er	.انشگاه امیرکبیر Bookmark not defined.	شکل ٤٤: خلاصه اطلاعات ضبط شده از شبکه ی د
Er	از شبکه ی دانشگاه امیرکبیر ror! Bookmark not	شکل ٤٥: نمودار IO مربوط به داده های ضبط شده
		defined.
Er	ror! Bookmark not defined	شکل ٤٦
Er	رکت پرورش داده هاFor! Bookmark not defined	شکل ٤٧:خلاصه اطلاعات ضبط شده از شبکه ی ش
Er	از شبکه ی پرورش داده ror! Bookmark not	شکل ٤٨: نمودار IO مربوط به داده های ضبط شده
		defined.
Er	ror! Bookmark not defined.	شکل ٤٩: 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.	شكل٢٥
Error! Bookmark not defined.	شکل <b>۵۳</b>
Error! Bookmark not defined.	شكل ٤٥
Error! Bookmark not defined.	شكل ٥٥
Error! Bookmark not defined.	شکل ٥٦
Error! Bookmark not defined.	شکل ۵۷
Error! Bookmark not defined.	شکل ۸۵
Error! Bookmark not defined.	شکل ۵۹
Error! Bookmark not defined.	شکل ٦٠
Error! Bookmark not defined.	شکل ٦١
Error! Bookmark not defined.	شکل ٦٢
Error! Bookmark not defined.	شکل ۲۳
Error! Bookmark not defined.	شکل ۶۶
Error! Bookmark not defined.	شکل ٦٥
Error! Bookmark not defined.	شکل ٦٦

Error! Bookmark not defined.	 77	شكل
Error! Bookmark not defined.	 77	ىكل

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.

۱

مقدمه

# معرفی ابزار Wireshark

Wireshark یک تحلیلگر بسته های شبکه <sup>۱</sup> 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.
  - مهندسین امنیت 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.

<sup>&</sup>lt;sup>\</sup> 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 <sup>۱</sup>
- 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 ...

<sup>&#</sup>x27; Network Interface

🖸 test. pcap - Wireshark			X
<u>File E</u> dit <u>V</u> iew <u>Go C</u> apture <u>A</u> nalyza	e Statistics Help		
	A <      A <      A <      A <      A <      A <      A <      A <      A <      A <      A <      A <      A <      A <      A <      A <      A <      A <      A <      A <      A <      A <      A <      A <      A <      A <      A <      A <      A <      A <      A <      A <      A <      A <      A <      A <      A <      A <      A <      A <      A <      A <      A <      A <      A <      A <      A <      A <      A <      A <      A <      A <      A <      A <      A <      A <      A <      A <      A <      A <      A <      A <      A <      A <      A <      A <      A <      A <      A <      A <      A <      A <      A <      A <      A <      A <      A <      A <      A <      A <      A <      A <      A <      A <      A <      A <      A <      A <      A <      A <      A <      A <      A <      A <      A <      A <      A <      A <      A <      A <      A <      A <      A <      A <      A <      A <      A <      A <      A <      A <      A <      A <      A <      A <      A <      A <      A <      A <      A <      A <      A <      A <      A <      A <      A <      A <      A <      A <      A <      A <      A <      A <      A <      A <      A <      A <      A <      A <      A <      A <      A <      A <      A <      A <      A <      A <      A <      A <      A <      A <      A <      A <      A <      A <      A <      A <      A <      A <      A <      A <      A <      A <      A <      A <      A <      A <      A <      A <      A <      A <      A <      A <      A <      A <      A <      A <      A <      A <      A <      A <      A <      A <      A <      A <      A <      A <      A <      A <      A <      A <      A <      A <      A <      A <      A <      A <      A <      A <      A <      A <      A <      A <      A <      A <      A <      A <      A <      A <      A <      A <      A <      A <      A <      A <      A <      A <      A <      A <      A <      A <      A <      A <      A <      A <      A <      A <      A <	♦ ♥ 주 보 [] ] ♥ ♥	
Eilter:		▼ ♣ Expression ‰ ⊆lear ♥ Apply	
No Time Source	Destination	Protocol Info	^
1 0.000000 192.168.0.2	Broadcast	ARP Who has 192.168.0.2? Gratuitous /	
3 0.299214 192.168.0.2	192.168.0.1	TCMP Destination unreachable (Port unre	
4 1.025659 192.168.0.2	224.0.0.22	IGMP V3 Membership Report	
5 1.044366 192.168.0.2	192.168.0.1	DNS Standard query SRV _ldaptcp.nbgr	
6 1.048652 192.168.0.2	239.255.255.250	UDP Source port: 3193 Destination por	
8 1.055053 192.168.0.1	192.168.0.2	UDP Source port: 1900 Destination por	
9 1.082038 192.168.0.2	192.168.0.255	NBNS Registration NB NB10061D<00>	
10 1.111945 192.168.0.2	192.168.0.1	DNS Standard query A proxyconf.ww004.	
11 1.226156 192.168.0.2	192.168.0.1	TCP 3196 > http [SYN] Seq=0 Len=0 MSS:	-
12 1.22/282 192.188.0.1	192.168.0.2	TCP TTCP > 5196 [STN, ACK] SEQ=0 ACK=.	<b>×</b>
<		>	
⊞ Frame 11 (62 bytes on wire, 6	2 bytes captured)		^
Ethernet II, Src: 192.168.0.2	(00:0b:5d:20:cd:02), Dst: Net	tgear_2d:75:9a (00:09:5b:2d:75:9a)	
∃ Internet Protocol, Src: 192.1	.68.0.2 (192.168.0.2), Dst: 192	2.168.0.1 (192.168.0.1)	
🖃 Transmission Control Protocol	, Src Port: 3196 (3196), Dst F	Port: http (80), Seq: O, Len: O	
Source port: 3196 (3196)			Ξ
Destination port: http (80)	)		
Sequence number: 0 (rela	ative sequence number)		
Header length: 28 bytes			_
Window size: 64240			~
0000 00 09 5b 2d 75 9a 00 0b 5	id 20 cd 02 08 00 45 00	u]E.	_
0010 00 30 18 48 40 00 80 06 6	51 Zc c0 a8 00 02 c0 a8 .0.H@	e a,	
0020 00 01 0c 7c 00 50 3c 36 9 0030 fa fo 37 a0 00 00 02 04 0	95 †8 00 00 00 00 70 02 .	.P<6p.	
File: "D:/test.pcap" 14 KB 00:00:02		P: 120 D: 120 M: 0	

شکل Wireshark : ۱ 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 نفوذ ها نمی باشد. این سیستم زمانی که شخصی اعمال غیرعادی -که مجاز به انجا م 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'، 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 Server ۲۰۰۳ یا Windows Vista و یا ۲۰۰۴ Windows XP
  - سیستم پنتیوم ۳۲ بیتی با قدرت پردازشی ۵۵۵ یا بیشتر.
    - حافظه RAM بیش از ۵۵۵۵۵۵۱
      - حداقل فضای دیسک ۵۵۵۵۵۷
        - حداقل رزولوشن ۲۰۰\*۸۰۰
- تعدادی کارت شبکه جهت ضبط نمودن ترافیک مبادله شده توسط آنها مانند Ethernet Card یا
   WLAN Card

**Nam Resolution** 

**ایـنـتـرفـیس کـاربـر** پس از نصب Wireshark می توان با ضبط کردن<sup>۱</sup> پکتها کار مانیتورینگ را شروع کرد. در این قسمت در مورد مفاهیم زیر صحبت می کنیم:

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

پنجره ی اصلی ٔ

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

<sup>&</sup>lt;sup>`</sup>Capturing

<sup>&</sup>lt;sup>\*</sup> Main Window

🗹 test. pcap - Wireshark			
File Edit Mew Go Capture Analyze Statistic	s Help		
	% 🖪 🔄 🗢		
Eiter:		• 💠 Expression	‱⊆lear ¥ дрріу
No Time Source	Destination	Protocal Info	<u>^</u>
1 0.000000 192.168.0.2	Broadcast	ARP Who has 1	92.168.D.27 Gratuitous / 📃
3 0.299214 192.168.0.2	192.168.0.1	ICMP Destinati	on unreachable (Port unre
4 1.025659 192.168.0.2	224.0.0.22	IGMP V3 Member	ship Report
5 1.044366 192.168.0.2	192.168.0.1	DNS Standard	query SRV _ldaptcp.nbgr
6 1.048652 192.168.0.2 7 1.050784 197.168.0.2	239.255.255.250	DNS Standard	nuery SDA nh10061d.ww004.
8 1.055053 192.168.0.1	192.168.0.2	UDP Source po	rt: 1900 Destination por
9 1.082038 192.168.0.2	192.168.0.255	NBNS Registrat	ion NB NB10061D<00>
10 1.111945 192.168.0.2	192.168.0.1	DNS Standard	query A proxycont.ww004.: to ISMAT Secto Lendo MSS:
12 1.227282 192.168.0.1	192.168.0.2	TCP http://dl	96 [SYN, ACK] Seg=0 Ack=: V
<			>
Enome 11 (52 butter on wine 62 butter	conturad)		
$\square$ Frame II (52 bytes on wire, 52 bytes $\square$ Ethernet II Spc: 192 168 0.2 (00:0b)	Sd:20:rd:02) Det: Net:		19 ·5h · 2d · 25 · 9a 1
■ Internet Protocol Src: 192,168,0.2 (	197 168 0 2) Dst 197	168.0.1 (192.168.)	11)
Transmission Control Protocol. Src Po	ort: 3196 (3196), Dst P	rt: http (RO). Se	n: O. Len: O
Source port: 3196 (3196)			,
Destination nort: http (80)			
Sequence number: 0 (relative se	quence number)		
Header length: ZB bytes			
Window size: 64240			×
10000 D0 09 55 2d 75 9a 00 05 5d 20 cd	02 08 D0 45 OD	]E.	
0010 D0 30 18 48 4D 00 8D 06 61 2c cO	a8 00 D2 c0 a8 .0. He	a,	
0020 D0 01 0c 7c 0D 50 3c 36 95 †8 00 0030 fa fa 27 a0 00 00 03 04 05 b4 01	00 00 00 70 02	°<6p.	
	VI 04 0C		
File: "D:)test.pcap" 14 KB 00:00:02		P: 1	ZO D: 120 M: 0 .:

شکل۲ : پنجرهی اصلی

پنجره ی اصلی Wireshark شامل قسمتهای زیر می باشد:

منو که برای شروع عملیات استفاده می شود.

- ۲- Toolbar اصلی که اجازه دسترسی به بخش هایی که زیاد تکرار می شوند را از طریق منو می دهد.
  - ۳- Toolbar فیلتر که امکان دستکاری مستقیم فیلتر استفاده شده را میدهد.
- ٤- صفحه ی لیست پکت که خلاصه ای از هر پکت ضبط شده را نمایش میدهد. با کلیک کردن روی پکت ها در این صفحه می توان آنچه را که در دو صفحه ی دیگر نمایش داده می شود، کنترل نمود.

' item

- ۰۰ صفحه ی جزییات پکت<sup>۲</sup> که جزییات پکت انتخاب شده را با دقت بیشتری در صفحه ی لیست پکت نمایش می دهد.
- ۲- صفحه یایت های پکت<sup>۳</sup> که داده های پکت انتخاب شده از صفحه ی لیست پکتها را نمایش می دهد و فیلد انتخاب شده در صفحه ی جزییات پکت ها را هایلایت می کند.
- -۷ statusbar تعدادی اطلاعات دقیق و جزیی درباره ی حالت برنامهی جاری و دادههای ضبط شده، نشان می دهد.

#### 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 بخش هایی برای بازکردن، ادغام فایل های دریافتی، ذخیره کردن، پرینت کردن، بیرون بردن<sup>٤</sup> فایل های ضبط شده به طور جزیی یا کامل و خروج از Wireshark میباشد.

Edit: این قسمت شامل امکانات پیداکردن یک بسته، مرجع زمان<sup>°</sup> یا نشانه گذاری یک یا چند پکت، تنظیم اولویتها و ... میباشد.

<sup>export</sup>

<sup>&#</sup>x27; packet list pane

<sup>&</sup>lt;sup>v</sup> packet details pane

<sup>&</sup>lt;sup>r</sup> packet bytes pane

<sup>°</sup> Time reference

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 بخش هایی 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 می باشد.

صفحهی لیست یکت

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><	
	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 _ldaptcp.nb	1
	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>	
1	0 0.029907	192.168.0.2	192.168.0.1	DNS	Standard query A proxyconf.ww004	
1:	1 0.114211	192.168.0.2	192.168.0.1	TCP	3196 > http [SYN] Seq=0 Ack=0 Wi	1
1	2 0.001126	192.168.0.1	192.168.0.2	TCP	http > 3196 [SYN, ACK] Seq=0 Ack	
1	3 0.000043	192.168.0.2	192.168.0.1	TCP	3196 > http [ACK] Seq=1 Ack=1 Wi	1
1	4 0.000126	192.168.0.2	192.168.0.1	HTTP	SUBSCRIBE /upnp/service/Layer3Fo	1
1	5 0.001858	192.168.0.1	192.168.0.2	TCP	<pre>http &gt; 3196 [ACK] Seq=1 Ack=256 '</pre>	1
1	6 0.003112	192.168.0.1	192.168.0.2	TCP	[TCP Window Update] http > 3196	
1	7 0.015934	192.168.0.1	192.168.0.2	TCP	1025 > 5000 [SYN] Seq=0 Ack=0 Wi	1
1	8 0.000036	192.168.0.2	192.168.0.1	TCP	5000 > 1025 [SYN, ACK] Seq=0 Ack	
1 1	0 0 001700	107 160 0 1	107 160 0 7	иттр	UTTD/1 0 200 ОК	1 🗹
<					>	

این صفحه تمام پکتها در فایل جاری را نمایش میدهد.

شکل٤: صفحهي ليست 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 جزییات پکت و بایتهای پکت نمایش داده می شوند.

در حال بررسی دقیق یک پکت، Wireshark اطلاعات را در ستونها قرار می دهد. از آنجا که پروتکلهای سطح بالاتر ممکن است اطلاعات سطوح پایین تر را overwrite کنند، تنها اطلاعات بالاترین سطح قابل مشاهده می باشد. به عنوان مثال یک پکت TCP داخل IP که در یک پکت Ethernet قرار دارد را در نظر بگیرید. می باشد. به عنوان مثال یک پکت TCP داخل IP که در یک پکت Ethernet قرار دارد را در نظر بگیرید. آدرسهای Ethrenet dissector اطلاعات خودش را می نویسد، IP dissector این اطلاعات را با اطلاعات خودش (نظیر می یابد.

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 نمی کند.
  - Time: مهرزمانی ' بسته. فرمت نمایش این فیلد را می توان 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 جزییات پکت

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

<sup>&#</sup>x27; timestamp

شکل ٥ : صفحهي جزيبات 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:

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

## صفحهی بایت های 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	Ob	5 d	20	cd	02	08	06	00	01	 ]
0010	08	00	06	04	00	01	00	Оb	5 d	20	cd	02	с0	a8	00	02	 ]
0020	00	00	00	00	00	00	с0	a8	00	02							 ••

شکل 7 : صفحه ی بایت های 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.

O Ready to load or capture	No Packets	Profile: Default

### شكل Statusbar : v اوليه

این statusbar هنگامیکه 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.

File: "/home/stig/http.pcap" 1673 KB 00:00:32 Packets: 2239 Displayed: 2239 Marked: 0 Profile: Default

شکل:۸ statusbar با یک فایل لود شده

- The colorized bullet در سمت چپ، بالاترین سطح اطلاعات ویژه که در فایل ضبط شده ی جاری
   پیدا می شود را نشان می دهد. برای بدست آوردن اطلاعات دقیق تر 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 می دهد.

- قسمت میانی تعداد پکتهای فایل ضبط شده را نشان میدهد. همچنین اطلاعات زیر نمایش داده می شوند:
  - Packets : تعداد پکتهای ضبط شده
  - Displayed : تعداد پکتهایی که اکنون نشان داده می شود
    - Marked : تعداد پکتهای علامتدار
    - Dropped: تعداد یکتهای drop شده
- قسمت راست پروفایل پیکربندی انتخاب شده را نشان میدهد. با کلیک کردن روی این قسمت statusbar یک منو شامل همهی پروفایل های پیکربندی موجود باز می شود و می توان آن را تغییر داد.



در شکل زیر statusbar با یک پیام display filter دیده می شود.

🔘 "I=" may have unexpected results (see the User's Guide) 🔋 Packets: 2239 Displayed: 2237 Marked: 0 🛛 Profile: Default

شکل ۲۰ : Statusbar با یک پیام display filter

طریقه ی ضبط نمودن داده های در جریان شبکه موتور ضبط اطلاعات wireshark دارای قابلیت های زیر می باشد:

• ضبط اطلاعات از شبکه های با سخت افزارهای مختلف ( ... Ethernet, Token Ring, ATM)

- متوقف ساختن ضبط اطلاعات توسط رهاناها ی 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

<sup>&#</sup>x27; 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 با دستور wireshark -i netInterfaceName –k در صورتیکه نام کارت شبکه مورد نظر را بدانیم می توانیم از با دستور

## ینجره 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.

Wireshark: Capture Interfaces							
	Description	IP	Packets	Packets/s	Stop		
<b>.</b>	Marvell Gigabit Ethernet Controller	192.168.129.190	0	0	<u>S</u> tart	Options	<u>D</u> etails
<b>.</b>	Microsoft	0.0.0.0	0	0	<u>S</u> tart	Options	<u>D</u> etails
<b>.</b>	MS Tunnel Interface Driver	unknown	0	0	<u>S</u> tart	Options	<u>D</u> etails
🛒. VMware Virtual Ethernet Adapter		192.168.80.1	2	0	<u>S</u> tart	Options	<u>D</u> etails
<b>.</b>	VMware Virtual Ethernet Adapter	192.168.49.1	2	0	<u>S</u> tart	Options	<u>D</u> etails
	Help					9	lose

شکل:۱۱ ینجره ی واسط ها ی ضبط

Description : توصيف كارت شبكه كه توسط سيستم عامل ارائه مي 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: عمليات ضبط را با استفاده از تنظيمات قبلي آغاز مي كند.

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 سربار 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 Info Dialog 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.

Wireshark: Capture Options					
Capture					
Interface: Microsoft: \Device\NPF_{7DC6C3A7-2CED-4454-A	A91E-51440F447B85}				
IP address: 0.0.0.0					
Link-layer header type: Ethernet <b>Buffer size:</b> 1	megabyte(s) Wireless Settings				
Capture packets in promiscuous mode					
Limit each packet to 68					
Capture Filter:	•				
Capture File(s)	Display Options				
File: Browse	Update list of packets in real time				
Use <u>m</u> ultiple files					
Next file every 1 megabyte(s)	Automatic scrolling in live capture				
Next file every 1 minute(s) V	Hide capture info dialog				
✓ Ring buffer with 2 ★ files					
Stop capture after 1 file(s)	Name Resolution Hide the c				
Stop Capture	Enable MAC name resolution				
after 1packet(s)	Enable network name resolution				
after 1 megabyte(s)					
□ after 1 minute(s) ▼	Enable transport name resolution				
Help	<u>S</u> tart <u>C</u> ancel				

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.

Wireshark: Capture Options					
Capture					
Interface: Marvell Gigabit Ethernet Controller: \Device\WPF_{19FD55B5-61C5-453D-8EBA-E468					
IP address: 192.168.129.190					
Link-Jayer header type: Ethernet  Buffer size: 1	megabyte(s) Wireless Settings				
Capture packets in promiscuous mode					
Limit each packet to 68 y bytes					
Capture Filter:	•				
Capture File(s)	Display Options				
File: Browse	Update list of packets in real time				
Use <u>m</u> ultiple files	_				
▶ Next file every 1 megabyte(s) ▼	<u>A</u> utomatic scrolling in live capture				
Next file every     1     minute(s)     ▼	Hide capture info dialog				
Ring buffer with 2	Name Resolution				
Stop capture after 1 file(s)					
Stop Capture	Enable MAC name resolution				
I after 1 packet(s)	Enable network name resolution				
□ after 1 megabyte(s) ▼					
□ after 1 ★ minute(s) ▼	Enable transport name resolution				
Help	<u>S</u> tart <u>C</u> ancel				

شکل ۲۳ : پنجره ی Capture Options

# گزینه های فریم Capture

- Interface از این گزینه می توان کارت شبکه ی مورد نظر را انتخاب نمود.
- IP Address ادرس 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 ۲۵۵۳۵ 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 فایلی 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.

- (s) Next file every n MegaByte: 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 باید قاب لیست بسته ها<sup>۱</sup> را به صورت بلادرنگ به روز رسانی کند یا خیر. در صورت نامشخص بودن وضعیت این گزینه، Wireshark تا زمانیکه 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 که 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<sup>۲</sup> 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.

<sup>&</sup>lt;sup>\</sup> Packet list pane

<sup>&</sup>lt;sup>r</sup> Capture info. dialoge

Transport name resolution آدرس های Transport را به
 پروتکل ها ترجمه کند در اختیار این گزینه است.

### (دكمه ها) Buttons

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.

1	Wireshark: Interface Details				
			·		
	Characteristics	Statistics	802.3 (Ethernet) 802.11 (WLAN) Task Offload		
	Characteristics	S			
	Vendor desc	ription	VMware Virtual Ethernet Adapter		
	Interface		\Device\WPF_{1E8334C4-B934-45A0-96F4-22FA6CE9CFBB}		
	Link status		Connected		
	Link speed		100 MBits/s		
	Media suppo	rted	802.3 (Ethernet)		
	Medium in us	se 🛛	802.3 (Ethernet)		
	Physical med	lium	Unspecified		
	NDIS Driver	Version	5.0		
	Vendor Driver Version		4.0 (Hex: 4.0)		
	Vendor ID		00:50:56 (Vmware) NIC: 00		
	MAC Options	s	802. 1P Priority: Unsupported, 802. 1Q VLAN: Supported		
	VLAN ID				
	Transmit Buf	ffer Space	24224		
	Receive Buff	fer Space	24224		
	Transmit Blo	ck Size	1514		
	Receive Bloc	k Size	1514		
	Maximum Pa	cket Size	1514		
	Note: accura	acy of all of	f these values are only relying on the network card driver!		
			Close		

شکل ۱٤: جعبه ی محاوره ی "Interface Details"

ضبط فايل ها

به هنگام ضبط، موتور ضبط libcap بسته ها را از کارت شبکه ربوده و بسته ی داده را در بافر کرنل نسبتا 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 نیز مفهوم متن را گزارش کند (مانند خطاهای جریان)، بعلاوه اطلاعات پروتکل های مربوط به مفهوم متن را نیز نگهداری می کند و در نتیجه می شود به مفهوم متن را نیز نگهداری می کند و در بسته ای مربوط به مفهوم متن را نیز مفهوم متن را گزارش کند (مانند خطاهای جریان)، بعلاوه اطلاعات پروتکل های مربوط به مفهوم متن را نیز نگهداری می کند و در بسته ی مربوط به مفهوم متن را نیز 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 بارگذلری شده نگهداری می شود، استفاده از یکی از طرق فایل های چندگانه 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 فایلی دیگر، ارتباط در یک فایل جداگانه ذخیره شود و بقیه اطلاعاتی که کاربر خواهان مشاهده ی آن است در فایلی دیگر، ارتباط در یک فایل جداگانه ذخیره شود و بقیه اطلاعاتی که کاربر خواهان مشاهده ی آن است در فایلی دیگر، ارتباط در یک فایل جداگانه ذخیره شود و بقیه اطلاعاتی که کاربر خواهان مشاهده ی آن است در فایلی دیگر، ارتباط در یک فایل جداگانه ذخیره شود و بقیه اطلاعاتی که کاربر خواهان مشاهده ی آن است در فایلی دیگر، ارتباط در یک فایل جاری 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.

<sup>&</sup>lt;sup>\</sup> 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"
   "....
- Multiple files, ring buffer عمل می کند. با برقراری :Multiple files, ring buffer active in a start active i
- 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.

### فيلتر كردن حين 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

هنگامی که 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<sup>۲</sup> صورت می گیرد.

متغیرهای محیطی تحت بررسی عبارتند از:

SSH\_CONNECTION (ssh) <remote IP> <remote port> <local IP> <local port>

<sup>`</sup> ring

<sup>&</sup>lt;sup>\*</sup> 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 همچنین قابلیت های ذخیره و ادغام و چاپ آنها مورد بررسی قرار گرفته است.

باز کردن یک فایل ضبط شده

Wireshark قابلیت 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.

Wireshark:	Open Capture File		? 🗙		
Look in: 🗀	fileset	💌 🔇 🕻	• 🖽 对		
<pre>// test1_0000 // test1_0000 // test1_0000 // test1_0000 // test1_0000 // test1_0000</pre>	01_20050819181503.pcap 02_20050819181505.pcap 03_20050819181505.pcap 04_20050819181506.pcap 05_20050819181507.pcap 06_20050819181507.pcap	Lest1_00007_20           Lest1_00008_20           Lest1_00009_20           Lest1_00010_20           Lest1_00011_20           Lest1_00011_20           Lest1_00012_20	test1_00007_20050819181508.pcap test1_00008_20050819181509.pcap test1_00009_20050819181510.pcap test1_00010_20050819181512.pcap test1_00011_20050819181513.pcap test1_00012_20050819181514.pcap		
<	<				
File name:	test1_00004_200508191815	506.pcap	Open		
Files of type:	All Files (".")	~	Cancel Help		
Filter:		Filename:	test1_00004_200508		
		Format:	Wireshark/tcpdump/.		
MAC name resolution  Network name resolution  Transport name resolution		Size:	1031 bytes		
		Packets:	9		
		First Packet:	2005-08-19 18:15:06		
		Elapsed	00:00:00		

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.
				? 🛿
Savejn: 🗀 fileset			🚽 🔾 💋	) 🗈 🗔 •
<pre> test1_00001_20050819 test1_00002_20050819 test1_00003_20050819 test1_00004_20050819 test1_00006_20050819 test1_0006_20050819 test1_0006_000608 test1_000608 test1_000608 test1_000</pre>	181503.pcap 2 181505.pcap 2 181505.pcap 2 181506.pcap 2 181507.pcap 2 181507.pcap 2	<pre>best1_00007_20050 best1_00008_20050 best1_00009_20050 best1_00010_20050 best1_00011_20050 best1_00012_20050</pre>	819181508.pcap 819181509.pcap 819181510.pcap 819181512.pcap 819181513.pcap 819181514.pcap	test1_00013_20 test1_00014_20 test1_00015_20 test1_00016_20 test1_00017_20 test1_00018_20
rite game: test1_00005	_2005081918150/	(.pcap		Save
Save as type: Wireshark/topdump/ libpcap (".pcap;".cap)			Cancel	
				Help
Packet Range				
	<ul> <li>Captured</li> </ul>	<ul> <li>Displayed</li> </ul>		
	120			
<ul> <li>All packets</li> </ul>	120			
<ul> <li>All packets</li> <li>Selected packet</li> </ul>	120	1		
All packets     Selected packet     Marked packets	1	1		
All packets     Selected packet     Marked packets     First to last marked	1 0	1 0 0		

شکل ۱٦: 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 گرهای 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.

Wireshark: Merge with capture fik			? 🗙
Look jn: 🇀 fileset		💌 🔮 🖻	• 🖽 •
test1_00001_20050819181503.pcap           test1_00002_20050819181505.pcap           test1_00003_20050819181505.pcap           test1_00004_20050819181505.pcap           test1_00005_20050819181507.pcap           test1_00006_20050819181507.pcap           test1_00007_20050819181508.pcap           test1_00007_20050819181508.pcap           test1_00007_20050819181508.pcap           test1_00007_20050819181508.pcap           test1_00007_20050819181508.pcap           test1_00007_20050819181508.pcap	<pre>     test1_00008_20     test1_00009_20     test1_00010_20     test1_00011_20     test1_00012_20     test1_00013_20     test1_00014_20     test1_00014_20     508.pcap </pre>	050819181509,pcap 050819181510,pcap 050819181512,pcap 050819181513,pcap 050819181514,pcap 050819181516,pcap 050819181516,pcap 050819181517,pcap	est1_00015_20 est1_00016_20 est1_00017_20 est1_00018_20 est1_00019_20 est1_00020_20 est1_00020_20 est1_00020_20
Filter: Prepend packets to existing file Merge packets chronologically Append packets to existing file	Filename: Format: Size: Packets: First Packet: Elapsed	Lest1_00007_2005081918 Wireshark/tcpdump/ lib 1074 bytes 11 2005-08-19 18:15:08 00:00:01	1508.pcap pcap

شکل۱۷ : پنجره ی ادغام فایل ها

مجموعه فايل 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 آور ده 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.

🛽 Wireshark: 17 Files in Set		(	
Filename	Created	Last Modified	Size
test1_00001_20050819181503.pcap	2005.08.19 18:15:03	2005.08.19 18:15:05	1067 Bytes
🔘 test1_00002_20050819181505.pcap	2005,08,19 18(15)05	2005,08,19 18(15)05	1108 Bytes
🔘 test1_00003_20050819181505.pcap	2005,08,19 18(15)05	2005.08.19 18:15:06	1093 Bytes
🔘 test1_00004_20050819181506.pcap	2005.08.19 18:15:06	2005.08.19 18:15:07	1031 Bytes
🔘 test1_00005_20050819181507.pcap	2005.08.19 18:15:07	2005.08.19 18:15:07	1070 Bytes
🔘 test1_00006_20050819181507.pcap	2005.08.19 18:15:07	2005.08.19 18:15:08	1126 Bytes
🔘 test1_00007_20050819181508.pcap	2005.08.19 18:15:08	2005.08.19 18:15:09	1074 Bytes
🔘 test1_00008_20050819181509.pcap	2005.08.19 18:15:09	2005.08.19 18:15:10	1037 Bytes
🔘 test1_00009_20050819181510.pcap	2005.08.19 18:15:10	2005.08.19 18:15:12	1060 Bytes
🔘 test1_00010_20050819181512.pcap	2005.08.19 18:15:12	2005.08.19 18:15:13	1079 Bytes
🔘 test1_00011_20050819181513.pcap	2005.08.19 18:15:13	2005.08.19 18:15:14	1029 Bytes
🔘 test1_00012_20050819181514.pcap	2005.08.19 18:15:14	2005.08.19 18:15:16	1119 Bytes
🔘 test1_00013_20050819181516.pcap	2005.08.19 18:15:16	2005.08.19 18:15:17	1029 Bytes
🔘 test1_00014_20050819181517.pcap	2005.08.19 18:15:17	2005.08.19 18:15:18	1085 Bytes
🔘 test1_00015_20050819181518.pcap	2005.08.19 18:15:18	2005.08.19 18:15:18	1083 Bytes
🔘 test1_00016_20050819181518.pcap	2005.08.19 18:15:18	2005.08.19 18:15:18	1058 Bytes
🔘 test1_00017_20050819181518.pcap	2005.08.19 18:15:18	2005.08.19 18:15:18	1386 Bytes
i	n directory: D:/fileset		
			<b>X</b> <u>⊂</u> lose

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

Content of the second secon	Fext" File	9	
Export to file:			
			6
- Darket Dange			-Dacket Format
ratket Kalige		[Diselaward]	Packet summary line
<b>O</b>		Displayed	Packet details:
• <u>A</u> ll packets	191	191	
Selected packet only	1	1	All collapsed
O Marked packets only	0	0	<ul> <li>As displayed</li> </ul>
O From first <u>to</u> last marked packet	0	0	O All expanded
O Specify a packet <u>r</u> ange:	0	0	Packet bytes
			Each packet on a new page
			QK X Cancel

شکل :Export as Plain Text File ۱۹

Export as PostScript File

این فرمت برای چاپ بسته ها مرجح است.

🕄 Ethereal: Export as "PostScript" file					
Export to file:					
(PostScript files can be easi	ly converted	d to PDF files	using ghostscript's ps2pdf)		
Packet Range			Packet Format		
	<u>⊂</u> aptured	Displayed	Packet summary line		
<u>A</u> II packets     ■	191	191	Packet details:		
O Selected packet only	1	1	<ul> <li>All collapsed</li> </ul>		
O Marked packets only	0	0	⊙ As displa <u>y</u> ed		
O From first <u>t</u> o last marked packet	0	0	O All expanded		
O Specify a packet <u>r</u> ange:	0	0	Packet bytes		
	]		Each packet on a new page		
			<u>₩QK</u> X <u>C</u> ancel		

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

Content of the second secon	file	
Export to file:		
		6
Packet Range		
	<u>C</u> aptured	Displayed
All packets	191	191
O Selected packet only	1	1
Marked packets only	0	0
O From first <u>t</u> o last marked packet	0	0
Specify a packet range:	0	0
		🗙 <u>C</u> ancel

شکل:Export as PSML File ۱۱

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

C Ethereal: Export as "PDML"	file	
Export to file:		
Packet Range		
	<u>C</u> aptured	Displayed
<ul> <li><u>All packets</u></li> </ul>	191	191
Selected packet only	1	1
Marked packets only	0	0
<ul> <li>From first to last marked packet</li> </ul>	0	0
O Specify a packet <u>r</u> ange:	0	0
		🗙 <u>C</u> ancel

شکل **Export as PDML File** : ۲۲

## Export selected packet bytes

🍘 Ethereal: Export Selected Packet Bytes 🛛 🗖 🔀				
<u>N</u> ame:				
Save in <u>f</u> older:	Debug_GTK2			
Will save 28 bytes of raw binary data to specified file.				
<b>∓</b> <u>B</u> rowse for o	ther folders			
	Save 🗶 Cancel			

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.

💿 Plain <u>t</u> ext			
O PostScript			
Output to file: d:\ethere	eal.out		Browse
Packet Range			Packet Format
	⊆aptured	Displayed	Packet summary line
<ul> <li>All packets</li> </ul>	11	11	Packet details:
O Selected packet only	1	1	🔘 All coļlapsed
O Marked packets only	0	0	<ul> <li>As displaye</li> </ul>
🔘 From first to last marked packet	0	0	◯ All e⊻pande
O Specify a packet range:	0	0	Packet bytes
			Each packet on a pr

شکل:۲٤ پنجره ی چاپ

# كاركردن با پكت هاي ضبط شده

### دیدن پکتهای ضبط شده

با کلیک کردن روی یک پکت در صفحهی لیست پکت، میتوان آن پکت را دید که با استفاده از گزینهی view امکان دیدن نمایش درختی و بایتی آن پکت وجود دارد. میتوان 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 می شود شمارهی Acknowledgment در هدر TCP نشان داده شده است.

🖪 test. pcap - Wireshark				. 🗆 🗙
<u> Eile Edit V</u> iew <u>G</u> o <u>C</u> apture <u>A</u> nalyze <u>S</u> tatisti	cs <u>H</u> elp			
	°, 🖪 🖸 🗢	🔿 🗢 奋	₹ III SI S	Q,
Eilter:			n 🏷⊆lear 🖋 Apply	
No Time Source	Destination	Protocol Info		^
	192.100.0.2	TCP HCCP	A DISK FRONT SOUTH MON-	100 1
30 1.259654 192.168.0.1	192.168.0.2	TCP LICP	Window updatej nttp > 3	
31 1.266619 192.166.0.2	192.168.0.1	TCP 1025	> 5000 [PSH, ACK] Seq=1 -> 1025 [PSH, ACK] Seq=1	ACK=
33 1.267850 192.168.0.1	192.168.0.2	TCP 1025	> 5000 [ACK] Seg=510 Ac	k=20
34 1.274361 192.168.0.1	192.168.0.2	TCP http	> 3197 [PSH. ACK] Seg=1	Ack=
35 1.274447 192.168.0.2	192.168.0.1	TCP 3197	> http [FIN, ACK] Seg=1	.90 Ac
36 1.274987 192.168.0.1	192.168.0.2	TCP http	> 3197 [FIN. ACK] Seg=2	O Ack
37 1.275018 192.168.0.2	192.168.0.1	TCP 3197	> http [ACK] Seg=191 Ac	:k=21
38 1.276019 192.168.0.1	192.168.0.2	TCP http	> 3197 [FIN, ACK] Seq=2	6645
39 1.281649 192.168.0.1	192.168.0.2	TCP [TCP	Window Update] 1025 > 5	000 [
40 1.282181 192.168.0.1	192.168.0.2	TCP 1025	> 5000 [FIN, ACK] Seq=5	10 Ac 🧹
	100 100 8 1	TCD 0000	ABDE FACEL OF AL	
<u>&lt;</u>				>
Frame 36 (60 bytes on wire, 60 bytes	captured)			~
Ethernet II Src: Netgear 20:75:9a (	00.00.5h.2d.75.9a) Det	· 192 168 0 2	(00.0h.5d.20.cd.02)	
Totanat Distance Constant 102 100 0 1	(100, 100, 200, 200, 100, 200, 200, 200,	100 0 0 0 (100	(00.00.50.20.00.02)	
Internet Protocol, Src: 192.168.0.1	(192.168.0.1), DST: 192	.168.0.2 (192.	168.0.2)	
Transmission Control Protocol, Src P	ort: http (80), Dst Por	t: 3197 (3197)	, Seq: 20, Ack: 190, Ler	1:0
Source port: http (80)				
Destination port: 3197 (3197)				
Sequence number: 20 (relative s	equence number)			_
Acknowledgement number: 190 (re	lative ack number)			
Header length: 20 bytes				~
<				
0000 00 0b 5d 20 cd 02 00 09 5b 2d 75	9a 08 00 45 00].	[-uE.		
0010  00 28 00 84 00 00 40 06  f8 f8 cC	a8 00 01 c0 a8 .(	.@		
0020 00 02 00 50 0c 7d 00 00 68 14 🔢	38 dd 9b 50 11P.	} h.<8₽.		
0030   0c   00   93   ca   00   00   00   00   00   00   00	00			
			[	
Acknowledgement number (tcp.ack), 4 bytes			JP: 120 D: 120 M: 0	

شکل ۲۵: Wireshark با یک پکت TCP برای دیدن

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

Л	🛿 36 1.274987 192.168.0.1 192.168.0.2 TCP http > 3197 [FIN, ACK] Seq=20 Ack=190 Win=3072 Len=0		×
E	Frame 36 (60 bytes on wire, 60 bytes captured)		^
Đ	Ethernet II, Src: Netgear_2d:75:9a (00:09:5b:2d:75:9a), Dst: 192.168.0.2 (00:0b:5d:20:cd:02)		
Ð	Internet Protocol, Src: 192.168.0.1 (192.168.0.1), Dst: 192.168.0.2 (192.168.0.2)		-
	🗉 Transmission Control Protocol, Src Port: http (80), Dst Port: 3197 (3197), Seq: 20, Ack: 190, L	.en: O	
L	Course mant, bttp (00)		$\mathbf{\Sigma}$
<			ļ
	000 00 0b 5d 20 cd 02 00 09 5b 2d 75 9a 08 00 45 00] [-uE. 010 00 28 00 84 00 00 40 06 f8 f8 c0 a8 00 01 c0 a8 .(@ 020 00 02 00 50 0c 7d 00 00 68 14 3c 38 dd 9b 50 11P.} h.<8P. 030 0c 00 93 ca 00 00 00 00 00 00 00 00		

شکل ۲۶: دیدن پکت در یک صفحهی مجزا

منوهای Pop-up

می توان یک منوی pop-up در صفحه های لیست پکت ها، جزییات پکت یا بایت های پکت با کلیک راست

کردن در روی این صفحات، آورد.

منوی Pop-up در صفحهی لیست پکت

🗖 test.cap - Wireshark	
<u> Edit View Go Capture Analyze Statistics Help</u>	
	◙ ⇔ ⇒ ∞ ₮ ⊻   🗐 📑   ◎, ○, ○, 🖻   🛎
Eilter:	▼ Expression Clear Apply
No Time Source Des	stination Protocol Info
20 1.250285 192.168.0.2 193 21 1.250810 192.168.0.1 193 22 1.250842 192.168.0.2 193	22.168.0.1 TCP 3196 > http [FIN, ACK] seq=256 / 22.168.0.2 TCP http > 3196 [FIN, ACK] seq=114 / 22.168.0.1 TCP 3196 > http [ACK] seq=257 Ack=11
23         1.251868         192.168.0.1         19           24         1.252826         192.168.0.1         19           25         1.253323         192.168.0.2         19           26         1.254502         192.168.0.1         19	1025         5000         LACK         Seq=1         Ack=1         w           102         Mark Packet (toggle)         http<>3196         [FIN, ACK]         Seq=26611           102         Set Time Reference (toggle)         3197         http         SYN]         Seq=0         Len=0         Mttp
27         1.254532         192.168.0.2         192           28         1.254649         192.168.0.2         192           29         1.256388         192.168.0.1         192	Z         Apply as Filter         Selected         [ACK] seq=1         Ack=1         w           2         Prepare a Filter         Not Selected         /upnp/service/Layen:           2         Conversation Filter         and Selected         [ACK] seq=1         Ack=1.90
SU1.259634 192.168.0.1 19. SU1.259634 192.168.0.1 19. ■ ■ ■ ■ ■ ■ ■ ■ ■ ■ ■ ■ ■	Z     SCTP     →     or Selected     □0001CE     10007CF     >
<ul> <li>■ Ethernet II, Src: Netgear_2d:75:9a (00:09:</li> <li>■ Internet Protocol, Src: 192.168.0.1 (192.1</li> <li>■ Transmission Control Protocol, Src Port: 1</li> </ul>	Copy L Export Selected Packet Bytes L Export Selected Packet Bytes L Export Selected Packet Bytes
Source port: 1025 (1025) Destination port: 5000 (5000) Sequence number: 1 (relative sequence Acknowledgement number: 1 (relative a Header length: 20 bytes	Image: Show Packet in New Window
0000 00 0b 5d 20 cd 02 00 09 5b 2d 75 9a 08 0010 00 28 00 7c 00 00 40 06 f9 00 c0 a8 00 0020 00 02 04 01 13 88 00 00 67 81 3c 37 71 0030 0c 00 e7 97 00 00 00 00 00 00 00 00	8 00 45 00] [-uE. 0 01 c0 a8 .(. @ f a7 50 10 g.<7P. 
File: "D:\Projects\Patchnose\workpackage_dev\wp3_io\docbook\example:	es\test.cap" 1   P: 120 D: 120 M: 0 .:

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

colorizing
rule.

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.
	Analyze	Same as "Follow TCP Stream" but for
Follow SSL Stream		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.
5	ول ۱	جا

منوی Pop-up در صفحهی جزییات پکت

🕂 test.cap - Wireshark	
File Edit View Go Capture Analyze Statistics Help	
Eilter:	▼ Expression <u>C</u> lear Apply
No Time Source Destination	Protocol Info
20 1.250285 192.168.0.2 192.168.	0.1 TCP 3196 > http [FIN, ACK] Seq=256 /
21 1.250810 192.168.0.1 192.168.	.0.2 TCP http > 3196 [FIN, ACK] Seq=114
22 1.250842 192.168.0.2 192.168.	0.1 TCP 3196 > http [ACK] Seq-257 Ack-11 0.2 TCP 1025 > 5000 [ACK] Seq-1 Ack-1 W
24 1.252826 192.168.0.1 192.168.	0.2 TCP http > 3196 [FIN, ACK] Seg=2661
25 1.253323 192.168.0.2 192.168.	0.1 TCP 3197 > http [SYN] Seq=0 Len=0 M:
26 1.254502 192.168.0.1 192.168.	0.2 TCP http > 3197 [SYN, ACK] Seq=0 Ack
27 1.254532 192.168.0.2 192.168 28 1 254649 192 168 0 2 192 168	0.1 TCP 3197 > NTTP [ACK] SEQ=1 ACK=1 W 0.1 HTTP UNSUBSCRIBE /uppn/service/laver:
29 1.256388 192.168.0.1 192.168.	0.2 TCP http > 3197 [ACK] Seg=1 Ack=190
30 1.259654 192.168.0.1 192.168.	0.2 TCP [TCP Window Update] http > 3197 🗸
<ul> <li>Frame 23 (60 bytes on wire, 60 bytes captured)</li> <li>Ethernet II, Src: Netgear_2d:75:9a (00:09:5b:2d</li> <li>Internet Protocol, Src: 192.168.0.1 (192.168.0.</li> <li>Transmission Control Protocol, Src Port: 1025 ( Source port: 1025 (1025)</li> </ul>	Expand Subtrees         cd:02 (00:0b:5d:20:cd:02)           Expand All         .168.0.2)           Collapse All         00), Seq: 1, Ack: 1, Len: 0           Copy         •
Sequence number: 1 (relative sequence numb	Export Selected Packet Bytes
Acknowledgement number: 1 (relative ack nu	Apply as Filter
Header length: 20 bytes	Prepare a Filter    Not Selected
⊞ Flags: 0x10 (ACK)	Follow TCP Stream <u>a</u> nd Selected
Window size: 3072	Follow SSL Stream <u>o</u> r Selected
⊞ Checksum: 0xe797 [correct] ⊞ [SEQ/ACK analysis]	Wiki Protocol Page and not Selected or not Selected
	Silter Field Reference
	Protocol Preferences
0000 00 0b 5d 20 cd 02 00 09 5b 2d 75 9a 08 00 4 0010 00 28 00 7c 00 00 40 06 f9 00 c0 a8 00 01 4 0020 00 02 04 01 13 88 00 00 67 81 3c 37 7f a7 9 0030 0c 00 e7 97 00 00 00 00 00 00 00 00	Image: Solve Name         Go to Corresponding Packet
Frame (frame), 60 bytes	P: 120 D: 120 M: 0

شکل ۲۸: **منوی Pop-up در صفحهی جزییات 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.

Copy/ Bytes (Offset Hex Text)	-	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)	-	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)	-	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).

Copy/ Bytes (Hex Stream)	-	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)	-	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	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.

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

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	If the selected field has a
Go to Corresponding		corresponding packet, go to it.
Packet		
		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 می شود و دیگری در زمان دیدن پکتها. Display filter سبب می شود که بتوان روی پکتهای دلخواه تمرکز کرد و بقیه را مخفی نمود. می توان پکتها را با یک از موارد زیر انتخاب نمود:

- پروتکل
- حضور یک فیلد
  - مقادير فيلدها
- مقايسه بين فيلدها
  - 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.

Elle Edit View Go Capture Analyze Statistics Help         Image: Construction of the statistics of the statis of the statistics of the statistics of the	🛯 te	st.pc	ap - W	iresh	ark																×
Image: Source       Destination       Protocol       Info         11       1.227282       192.168.0.1       192.168.0.2       192.168.0.2       192.168.0.1       192.168.0.2       192.168.0.1       192.168.0.2       102.168.0.2	Eile	⊑dit	⊻iew	Go	⊆apture	e <u>A</u> naly	yze ;	Statistics	Help												
Eller: <pre> Eller: <pre> Eller: </pre> Eller: <pre> Eller: <pre> Eller: </pre> Eller: <pre> Eller: <pre> Eller: </pre> Eller: <pre> Eller</pre></pre></pre></pre></pre></pre></pre></pre></pre></pre></pre></pre></pre></pre></pre></pre></pre></pre></pre></pre></pre></pre></pre></pre></pre></pre></pre></pre></pre></pre></pre></pre></pre></pre></pre></pre></pre></pre></pre></pre></pre></pre></pre></pre></pre></pre></pre></pre></pre></pre></pre></pre></pre></pre></pre></pre></pre></pre></pre></pre></pre></pre></pre></pre></pre></pre></pre></pre></pre></pre></pre></pre></pre></pre></pre></pre></pre></pre></pre></pre></pre></pre></pre></pre></pre></pre></pre></pre></pre></pre></pre></pre></pre></pre></pre></pre></pre></pre></pre></pre></pre></pre></pre></pre></pre></pre></pre></pre></pre></pre></pre></pre></pre></pre></pre></pre></pre></pre></pre></pre></pre></pre></pre></pre></pre></pre></pre></pre></pre></pre>		4	0	<b>M</b>	<b></b>	D	8	) ×	¢ø	8	6	<b>1</b> (**	\$	¢	Ŧ	⊉ [		3	€,	Q,	
No     Time     Source     Destination     Protocol     Info       11     1.226156     192.168.0.1     192.168.0.2     TCP     3196 > http     SYNJ Seq=0 Lene 0 #55       12     1.227282     192.168.0.1     192.168.0.2     TCP     http > 3196     SYN, ACKJ Seq=1 Ack=1 win       14     1.227325     192.168.0.2     192.168.0.1     TCP     http > 3196     SYNJ Seq=0 Ack=2 for       15     1.229309     192.168.0.1     192.168.0.2     TCP     http > 3196     Seq=1 Ack=1 win       14     1.227325     192.168.0.1     192.168.0.2     TCP     http SUBSCRIBE /upnp/service/Layer3For       15     1.229309     192.168.0.1     192.168.0.2     TCP     ICP     Window Update]       17     1.248355     192.168.0.1     192.168.0.2     TCP     ICP     Window Update]       19     1.250171     192.168.0.2     192.168.0.1     TCP     Seq=0 Ack=       19     1.250171     192.168.0.2     192.168.0.2     TCP     http FIN, ACKJ Seq=1Ack=1 win       20     1.250842     192.168.0.1     TCP     3196     FIN, ACKJ Seq=27 Ack=115       21     1.250840     192.168.0.2     TCP     http FIN, ACKJ Seq=266 Ack       21     1.250842     192.168.0.2     TCP <td< td=""><td><u>F</u>ilter:</td><td>tcp</td><td></td><td></td><td></td><td></td><td></td><td></td><td></td><td></td><td></td><td></td><td>▼ <u>E</u>xpr</td><td>ession.</td><td> ⊆lea</td><td>ar <u>A</u>pply</td><td></td><td></td><td></td><td></td><td></td></td<>	<u>F</u> ilter:	tcp											▼ <u>E</u> xpr	ession.	⊆lea	ar <u>A</u> pply					
11       1.221168.0.1       192.168.0.2       192.168.0.2       TCP       http [SYN] Seq=0 Len=0 MSS         12       1.227282       192.168.0.2       192.168.0.1       TCP       http 3196       SYN, ACK] Seq=0 Ack=         13       1.227325       192.168.0.2       192.168.0.1       TCP       3196 > http [ACK] Seq=1 Ack=1 Win         14       1.227325       192.168.0.2       192.168.0.1       TCP       http 3196 [ACK] Seq=1 Ack=1 Win         14       1.227325       192.168.0.1       192.168.0.2       TCP       http 3196 [ACK] Seq=1 Ack=256 W         16       1.229309       192.168.0.1       192.168.0.2       TCP       http S196 [ACK] Seq=1 Ack=256 W         16       1.229309       192.168.0.1       192.168.0.2       TCP       http [ACK] Seq=2 Ack=256 W         17       1.248355       192.168.0.1       192.168.0.2       TCP       http S106 [ACK] Seq=256 Ack=1 Win         19       1.250171       192.168.0.1       192.168.0.2       TCP       http S106 [ACK] Seq=1 Ack=1 Win         20       1.250840       192.168.0.1       TCP       http S106 [ACK] Seq=27 Ack=115         23       1.251868       192.168.0.2       TCP       http S106 [ACK] Seq=27 Ack=115         23       1.251868       192.168.0.2 <t< td=""><td>No. +</td><td>1</td><td>ſime</td><td></td><td>Sourc</td><td>e</td><td></td><td></td><td>Desti</td><td>inatior</td><td>ı</td><td></td><td>Pro</td><td>tocol</td><td>Info</td><td></td><td></td><td></td><td></td><td></td><td>^</td></t<>	No. +	1	ſime		Sourc	e			Desti	inatior	ı		Pro	tocol	Info						^
12       1.227325       192.168.0.1       192.168.0.1       TCP       110(p) 2139 [2116, Xet] Seq=0 Ack=1       Win         14       1.227325       192.168.0.1       TCP       1105       1.229309       192.168.0.1       192.168.0.2       TCP       http [Ack] Seq=1 Ack=1 Win         15       1.229309       192.168.0.1       192.168.0.2       TCP       http [Ack] Seq=1 Ack=3 & Win         16       1.232421       192.168.0.1       192.168.0.2       TCP       http [Ack] Seq=1 Ack=3 & Win         17       1.248355       192.168.0.1       192.168.0.2       TCP       http [Ack] Seq=0 Ack=3         18       1.248391       192.168.0.1       TCP       5000 [StN] Seq=0 Len=0 MSS         18       1.248391       192.168.0.2       TCP       http [Ack] Seq=266 Ack=3         19       1.250171       192.168.0.1       TCP       http [Ack] Seq=266 Ack=3         20       1.250285       192.168.0.2       TCP       http [Ack] Seq=27 Ack=115         23       1.250810       192.168.0.2       TCP       http [Ack] Seq=266 Ack=3         21       1.250842       192.168.0.2       TCP       http [Ack] Seq=27 Ack=115         23       1.251868       192.168.0.2       TCP       http [Ack] Seq=26611 <t< td=""><td></td><td>11 1</td><td>.2261</td><td>.56</td><td>192.</td><td>168.0</td><td>.2</td><td></td><td>192.</td><td>168.</td><td>.0.1</td><td></td><td>TCF</td><td>)</td><td>3196</td><td>&gt; http &gt; 2106</td><td>[SYN]</td><td>Seq=(</td><td>) Len=</td><td>⊧O MSS</td><td>≣</td></t<>		11 1	.2261	.56	192.	168.0	.2		192.	168.	.0.1		TCF	)	3196	> http > 2106	[SYN]	Seq=(	) Len=	⊧O MSS	≣
14       1.227451       192.168.0.2       192.168.0.1       HTTP       SUBSCRIBE /upnp/service/Layer3For         15       1.229309       192.168.0.1       192.168.0.2       TCP       Http > 3196       [ACK] Seq=1 Ack=256 W         16       1.229421       192.168.0.1       192.168.0.2       TCP       Http > 3196       [ACK] Seq=1 Ack=256 W         17       1.248355       192.168.0.1       192.168.0.2       TCP       1025 > 5000       [SYN] Seq=0 Len=0 MSS         18       1.248391       192.168.0.2       192.168.0.1       TCP       5000 S 1025       [SYN, ACK] Seq=1 Ack=1         19       1.250171       192.168.0.2       192.168.0.1       TCP       5000 S 1025       [SYN, ACK] Seq=256 Ac         20       1.250285       192.168.0.2       192.168.0.1       TCP       http > 3196       [FIN, ACK] Seq=14 Ac         22       1.250842       192.168.0.1       192.168.0.2       TCP       http > 3196       [FIN, ACK] Seq=256 Ac         23       1.251868       192.168.0.1       192.168.0.2       TCP       http > 3196       [FIN, ACK] Seq=26611         24       1.252826       192.168.0.1       192.168.0.2       TCP       http > 3197       [SNH ACK] Seq=26611         25       1.253323       192.168.0		13 1	. 2273	25	192.	168.0	.1 .2		192.	.168.	.0.2		TCF	, ,	3196	> 5196	FACK1	Seg=1	i Ack=u	1 Win	
15       1.223009       192.168.0.1       192.168.0.2       TCP       http > 3196       [ACK] Seq=1 Ack=256 W         16       1.232421       192.168.0.1       192.168.0.2       TCP       [ICP Window Update]       http > 3196         17       1.248355       192.168.0.1       192.168.0.2       TCP       1025 > 5000       [SYN] Seq=0 Len=0 MSS         18       1.248391       192.168.0.2       192.168.0.2       HTP       TTP /1.0 200 0K         20       1.250171       192.168.0.2       192.168.0.2       HTP HTP/1.0 200 0K         20       1.250285       192.168.0.1       192.168.0.2       HTP HTP/1.0 200 0K         21       1.250810       192.168.0.1       192.168.0.2       TCP 3196 > http [FIN, ACK] Seq=256 Ac         21       1.250810       192.168.0.1       192.168.0.2       TCP 1025 > 5000 [ACK] Seq=14 Ac         23       1.251868       192.168.0.1       192.168.0.2       TCP 1025 > 5000 [ACK] Seq=1 Ack=1 Win         24       1.252826       192.168.0.1       192.168.0.2       TCP 1025 > 5000 [ACK] Seq=1 Ack=1 Win         25       1.254532       192.168.0.2       192.168.0.1       TCP 3197 > http [SVN, ACK] Seq=0 Ack=         27       1.254532       192.168.0.2       192.168.0.1       TCP 3197 > http [SVN, ACK] Se		14 1	.2274	51	192.	168.0	.2		192.	.168.	.0.1		HTT	ΓP	SUBSC	RIBE /	upnp/s	envíce	e/Laye	en3For	
10       1.22.102.0.1       1.22.102.0.2       10.1       10.1       10.1       10.2		15 1	.2293	09	192.	168.0	.1		192.	.168.	.0.2		TCF		http	> 3196	[ACK]	Seq=1	1 Ack=	-256 W	
18       1.248391       192.168.0.2       192.168.0.1       TCP       5000 > 1025       [SYN, ACK] Seq=0 Acke         19       1.250171       192.168.0.1       192.168.0.2       HTTP       HTTP/1.0.200 0K         20       1.250285       192.168.0.2       192.168.0.1       TCP       3196 > http [FIN, ACK] Seq=256 Ac         21       1.250840       192.168.0.1       192.168.0.2       TCP       http > 3196 [FIN, ACK] Seq=257 Ack=115         23       1.251866       192.168.0.1       192.168.0.2       TCP       http > 3196 [FIN, ACK] Seq=26611         24       1.252826       192.168.0.1       192.168.0.2       TCP       http > 3196 [FIN, ACK] Seq=26611         25       1.254323       192.168.0.2       192.168.0.2       TCP       http > 3197 Stry, ACK] Seq=26611         25       1.254502       192.168.0.1       192.168.0.2       TCP       http > 3197 Stry, ACK] Seq=26611         25       1.254532       192.168.0.2       192.168.0.1       TCP       3197 Stry, ACK] Seq=26611         26       1.254502       192.168.0.2       192.168.0.2       TCP       http > 3197 [Stry, ACK] Seq=0 Ack=         27       1.254532       192.168.0.2       192.168.0.1       TCP       3197 Stry, ACK] Seq=1 Ack=1 Win         4		17 1	. 2483	55	192.	168.0	.1		192.	.168.	.0.2		TCF	0	1025	> 5000	[SYN]	Sea=0	) Len=	=O MSS	
19 1.250171 192.168.0.1 192.168.0.2 HTTP HTTP/1.0 200 0K 20 1.250285 192.168.0.2 192.168.0.1 TCP 3196 > http [FIN, ACK] Seq=256 Ac 21 1.250810 192.168.0.1 192.168.0.2 TCP http > 3196 [FIN, ACK] Seq=257 Ack=115 23 1.251868 192.168.0.1 192.168.0.2 TCP 1025 > 5000 [ACK] Seq=1 Ack=1 Win 24 1.252826 192.168.0.1 192.168.0.2 TCP http > 3196 [FIN, ACK] Seq=26611 25 1.253323 192.168.0.1 192.168.0.2 TCP http > 3196 [FIN, ACK] Seq=26611 25 1.253323 192.168.0.1 192.168.0.2 TCP http > 3197 [SYN Seq=0 Len=0 MSS 26 1.254502 192.168.0.1 192.168.0.2 TCP http > 3197 [SYN, ACK] Seq=0 Ack= 27 1.254532 192.168.0.2 192.168.0.1 TCP 3197 > http [ACK] Seq=1 Ack=1 Win F Frame 11 (62 bytes on wire, 62 bytes captured) F Frame 11 (62 bytes on wire, 62 bytes captured) F Transmission Control Protocol, Src 192.168.0.2 (192.168.0.2), Dst: Netgear_2d:75:9a (00:09:5b:2d:75:9a) T Transmission Control Protocol, Src Port: 3196 (3195), Dst Port: http (80), Seq: 0, Len: 0 00000 00 09 5b 2d 75 9a 00 0b 5d 20 cd 02 08 00 45 00[-u]E. 0010 00 30 1R 48 40 00 80 06 61 2r r0 a8 00 02 r0 a8[-u]E. 0010 00 30 1R 48 40 00 80 06 61 2r r0 a8 00 02 r0 a8[-u]E. 0010 00 30 1R 48 40 00 80 06 61 2r r0 a8 00 02 r0 a8[-u]E. 0010 00 30 c7 c 00 50 3c 36 95 f8 00 00 00 07 00 2].Pc6p. 0030 fa f0 27 e0 00 00 02 04 05 b4 01 01 04 02].Pc6p.		18 1	.248	91	192.	168.0	.2		192.	168	0.1		TCF		5000	> 1025	ESYN,	ACK]	Seq=0	Ack=	
20 1.250285 192.168.0.2 192.168.0.1 1CP 3196 > http [-N, Ack] Seq=256 Ac 21 1.250810 192.168.0.1 192.168.0.2 TCP http > 3196 > http [ACK] Seq=14 Ac 22 1.250842 192.168.0.1 192.168.0.2 TCP 1025 > 5000 [ACK] Seq=1 Ack=1 Win 24 1.252826 192.168.0.1 192.168.0.2 TCP http > 3197 [FN, ACK] Seq=26611 25 1.253323 192.168.0.2 192.168.0.1 TCP 3197 > http [SYN] Seq=0 Len=0 MSS 26 1.254502 192.168.0.1 192.168.0.2 TCP http > 3197 [SYN, ACK] Seq=0 Ack= 27 1.254532 192.168.0.2 192.168.0.1 TCP 3197 > http [ACK] Seq=1 Ack=1 Win Frame 11 (62 bytes on wire, 62 bytes captured) Frame 11 (62 bytes o		19 1	.2501	.71	192.	168.0	.1		192.	.168.	.0.2		HT	ΓP	HTTP/	1.0 20	O OK				
2111230010       132.100.011       132.100.011       102.100.011		20 1	2502	285	192.	168.0	.2		192.	168.	.0.1			, ,	3196 http	> http > 3106	LEIN,	ACK	Seq=2	156 AC	
23 1.251868 192.168.0.1 192.168.0.2 TCP 1025 > 5000 [ACK] Seq=1 Ack=1 Win 24 1.252826 192.168.0.1 192.168.0.2 TCP http > 3196 [FIN, ACK] Seq=26611 25 1.253323 192.168.0.2 192.168.0.1 TCP 3197 > http [SYN] Seq=0 Len=0 MSS 26 1.254502 192.168.0.1 192.168.0.2 TCP http > 3197 [SYN, ACK] Seq=0 Ack= 27 1.254532 192.168.0.2 192.168.0.1 TCP 3197 > http [ACK] Seq=1 Ack=1 Win Frame 11 (62 bytes on wire, 62 bytes captured) Frame 11 (62 bytes on wire, 62 bytes captured) Finternet Protocol, Src: 192.168.0.2 (192.168.0.2), Dst: Netgear_2d:75:9a (00:09:5b:2d:75:9a) Transmission Control Protocol, Src Port: 3196 (3196), Dst Port: http (80), Seq: 0, Len: 0 00000 00 09 5b 2d 75 9a 00 0b 5d 20 cd 02 08 00 45 00[-u]E. 0010 00 30 18 48 40 00 80 06 61 2c r0 a8 00 02 r0 a8 .0.HA a, 0020 00 01 0c 7c 00 50 3c 36 95 f8 00 00 00 00 70 02[P<6p. 0030 fa f0 27 e0 00 00 02 04 05 b4 01 01 04 02		22 1	.2508	342	192.	168.0	.2		192.	.168.	.0.1		TCF		3196	> http	FACK1	Seg=2	257 Ac	:k=115	
24 1.252826 192.168.0.1 192.168.0.2 TCP http > 3196 [FIN, ACK] Seq=26611 25 1.253323 192.168.0.2 192.168.0.1 TCP 3197 > http [SYN] Seq=0 Len=0 MSS 26 1.254502 192.168.0.1 192.168.0.2 TCP http > 3197 [SYN, ACK] Seq=0 Ack= 27 1.254532 192.168.0.2 192.168.0.1 TCP 3197 > http [ACK] Seq=1 Ack=1 Win Frame 11 (62 bytes on wire, 62 bytes captured) Frame 11 (62 bytes on wire, 62 bytes captured) Finternet Protocol, Src: 192.168.0.2 (192.168.0.2), Dst: Netgear_2d:75:9a (00:09:5b:2d:75:9a) Finternet Protocol, Src: 192.168.0.2 (192.168.0.2), Dst: 192.168.0.1 (192.168.0.1) Framsmission Control Protocol, Src Port: 3196 (3196), Dst Port: http (80), Seq: 0, Len: 0 00000 00 09 5b 2d 75 9a 00 0b 5d 20 cd 02 08 00 45 00[-u]E. 0010 00 30 18 48 40 00 80 06 61 2c r0 a8 00 02 r0 a8 .0.Ha a, 0020 00 01 0c 7c 00 50 3c 36 95 f8 00 00 00 00 70 02[-P<6p. 0030 fa f0 27 e0 00 00 02 04 05 b4 01 01 04 02'		23 1	.2518	868	192.	168.0	.1		192.	.168.	.0.2		TCF	, ,	1025	> 5000	[ACK]	Seq=1	1 Ack=	∶1 Win	
25 1.253323       192.168.0.2       192.168.0.1       102		24 1	.2528	326	192.	168.0	.1		192.	.168.	.0.2		TCF	, ,	http	> 3196	[FIN,	ACK]	Seq=2	26611	
27 1.254532       192.168.0.2       192.168.0.1       TCP       3197 > http       [ACK] Seq=1 Ack=1 Win		25 1	2533	23	192.	168.0	.2		192.	168.	.0.1			, ,	3197 http	> http > 3107	ESYNJ ESVN	Seq=0	) Len= Sea=0	:O MSS \ A∈k=	
<ul> <li>Frame 11 (62 bytes on wire, 62 bytes captured)</li> <li>Ethernet II, Src: 192.168.0.2 (00:0b:5d:20:cd:02), Dst: Netgear_2d:75:9a (00:09:5b:2d:75:9a)</li> <li>Internet Protocol, Src: 192.168.0.2 (192.168.0.2), Dst: 192.168.0.1 (192.168.0.1)</li> <li>Transmission Control Protocol, Src Port: 3196 (3196), Dst Port: http (80), Seq: 0, Len: 0</li> </ul>		27 1	.2545	32	192.	168.0	.2		192.	.168.	.0.1		TCF		3197	> http	FACK1	Seg=1	1 Ack=	1 Win	~
<ul> <li>         Frame 11 (62 bytes on wire, 62 bytes captured)         ■ Ethernet II, Src: 192.168.0.2 (00:0b:5d:20:cd:02), Dst: Netgear_2d:75:9a (00:09:5b:2d:75:9a)         ■ Internet Protocol, Src: 192.168.0.2 (192.168.0.2), Dst: 192.168.0.1 (192.168.0.1)         ■ Transmission Control Protocol, Src Port: 3196 (3195), Dst Port: http (80), Seq: 0, Len: 0         00000 00 09 5b 2d 75 9a 00 0b 5d 20 cd 02 08 00 45 00[-u]E.         0010 00 30 18 48 40 00 80 06 61 2r r0 a8 00 02 r0 a8 .0.H@ a,         0020 00 01 0c 7c 00 50 3c 36 95 f8 00 00 00 00 70 02 .P&lt;6p.         0030 fa f0 27 e0 00 00 02 04 05 b4 01 01 04 02'</li></ul>	<																			>	
<ul> <li>              Ethernet II, Src: 192.168.0.2 (00:0b:5d:20:cd:02), Dst: Netgear_2d:75:9a (00:09:5b:2d:75:9a)               Internet Protocol, Src: 192.168.0.2 (192.168.0.2), Dst: 192.168.0.1 (192.168.0.1)               Transmission Control Protocol, Src Port: 3196 (3195), Dst Port: http (80), Seq: 0, Len: 0                  00000 00 09 5b 2d 75 9a 00 0b 5d 20 cd 02 08 00 45 00[-u]E.             0010 00 30 18 48 40 00 80 06 61 2c r0 a8 00 02 r0 a8 .0.Hã a,             0020 00 01 0c 7c 00 50 3c 36 95 f8 00 00 00 00 70 02 .P&lt;6p.             0030 fa f0 27 e0 00 00 02 04 05 b4 01 01 04 02'         </li></ul>	🛨 Fr	ame :	11 (6)	2 byt	es on	wire,	62	bytes c	aptur	ed)											
<ul> <li>              Internet Protocol, Src: 192.168.0.2 (192.168.0.2), Dst: 192.168.0.1 (192.168.0.1)      </li> <li>             Transmission Control Protocol, Src Port: 3196 (3196), Dst Port: http (80), Seq: 0, Len: 0      </li> <li>             00000 00 09 5b 2d 75 9a 00 0b 5d 20 cd 02 08 00 45 00[-u]E.             0010 00 30 18 48 40 00 80 06 61 2r r0 a8 00 02 r0 a8 .0.Ha a,             0020 00 01 0c 7c 00 50 3c 36 95 f8 00 00 00 00 70 02 .P&lt;6p.             0030 fa f0 27 e0 00 00 02 04 05 b4 01 01 04 02'  </li> </ul>	🕀 Et	hern	et II	, Src	: 192	.168.0	.2 ((	00:0b:5	d:20:	cd:C	)2), C	ost: N	etgear_	_2d:7	5:9a (	(00:09:	5b:2d:	75:9a	)		
Transmission Control Protocol, Src Port: 3196 (3195), Dst Port: http (80), Seq: 0, Len: 0     0000 00 09 5b 2d 75 9a 00 0b 5d 20 cd 02 08 00 45 00[-u]E.     0010 00 30 18 48 40 00 80 06 61 2r r0 a8 00 02 r0 a8 .0.H@ a,     0020 00 01 0c 7c 00 50 3c 36 95 f8 00 00 00 00 70 02 .P<6p.     0030 fa f0 27 e0 00 00 02 04 05 b4 01 01 04 02'	🕀 In	itern	et Pro	otoco	l, Sre	: 192	.168	.0.2 (1	.92.16	8.0.	2), D	)st: 1	92.168.	.0.1	(192.1	168.0.1	)				
0000 00 09 5b 2d 75 9a 00 0b 5d 20 cd 02 08 00 45 00[-u]E. 0010 00 30 18 48 40 00 80 06 61 2c c0 a8 00 02 c0 a8 .0.H@ a, 0020 00 01 0c 7c 00 50 3c 36 95 f8 00 00 00 00 70 02 .P<6p. 0030 fa f0 27 e0 00 00 02 04 05 b4 01 01 04 02'	🕀 Tr	ansm	issio	1 Con	trol	Protoc	ol, :	Src Por	rt: 31	.96 (	(3195)	), Dst	Port:	http	(80),	, Seq:	0, Ler	1:0			
0000 00 09 5b 2d 75 9a 00 0b 5d 20 cd 02 08 00 45 00[-u]E. 0010 00 30 18 48 40 00 80 06 61 2c c0 a8 00 02 c0 a8 .0.H& a, 0020 00 01 0c 7c 00 50 3c 36 95 f8 00 00 00 00 70 02 .P<6p. 0030 fa f0 27 e0 00 00 02 04 05 b4 01 01 04 02'																					
0010 00 30 18 48 40 00 80 06 61 2c c0 a8 00 02 c0 a8 .0.H@ a, 0020 00 01 0c 7c 00 50 3c 36 95 f8 00 00 00 00 70 02 .P<6p. 0030 fa f0 27 e0 00 00 02 04 05 b4 01 01 04 02'	0000	00	09 5b	2d 7	5 9a -	00 Ob	5d	20 cd 0	2 08	00 4	45 00	••[	-u	· · · ·	.E.						
boso fa fo zz eo oo oo oo oo oo ba oo ba oo oo oo ba oo oo oo oo ba oo oo oo ba oo oo oo ba oo ba oo oo oo ba oo	0010	00	30 18 01 0⊂	48 4 7c 0	0 00 -	KO OA 3c 36	61 95 -	76 60 8 f8 00 0	NO 00	02 n 00 7	-0 a8 20 02	.0.	на I.Р<б	a,	 .n.						
	0030	fa	f0 27	e0 0	0 00	02 04	05	b4 01 0	1 04	02 Í											
File: "D:\test.pcap" 14 KB 00:00:02 P: 120 D: 103 M: 0 [Expert: Error]	File: "D	D:\test	.pcap"	14 KB C	0:00:02	2										P: 120 D	): 103 M	: 0 [Expe	ert: Erro	or]	.:

شکل ۲۹: فیلترکردن پکتهای پروتکل TCP

ايجاد display filter expressions

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

فیلدهای display filter

هر فیلد در صفحهی جزییات پکت می تواند به عنوان یک رشته فیلتر استفاده شود، در نتیجه می توان تنها پکتهایی را که شامل این فیلد هستند رنمایش داد. به عنوان مثال رشتهی tcp اگر به عنوان فیلتر باشد، تمام پکتهای شامل پروتکل tcp دیده می شوند. یک لیست کامل از فیلدهای فیلتر موجود در منوی "Help/Supported Protocols" از صفحهی "Display" از صفحه Filter Field"

مقايسەي مقادير

می توان فیلترهایی ساخت که که مقادیر را با استفاده از اپراتورهای مقایسهای مقایسه می کنند.

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 <b>frame.len &lt; 128</b>
ge	>=	Greater than or equal to <b>frame.len ge 0x100</b>
le	<=	Less than or equal to <b>frame.len &lt;= 0x20</b>

جدول ۳

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

Туре	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 eth.dst == 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.fffffffffff

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

جدول ٤: انواع فیلدهای display filter

تركيب كردن 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.scr==10.0.0.5 or ip.src==192.1.1.1
xor	٨٨	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

	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
	The example above uses the n: format, which takes
	everything from offset
	n to the end of the sequence.
	eth.src[2] == 83
	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
	Wireshark allows you to string together single
	ranges in a comma separated
	list to form compound ranges as shown above.

جدول ٥: : اپراتورهای منطقی display filter

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

Л	Wireshark: Filter Expression			
I	Field name		Relation	Value (protocol)
	2dparityfec		is present	
	E 3COMXNS		==	Predefined values:
	3GPP2 A11		!=	
	802.11 MGT     802.11 MGT     1		>	
	🗷 802.11 Radiotap		<	
	🗄 802.3 Slow protocols		>=	
	⊞ 9P		<=	
	AAL1		contains	
	AAL3/4		matches	
	I AARP			
	I ACAP			
	ACSE			
	ACtrace			
	I ADP			Range (offsetslength)
	I ■ AFP	*	1	
				<u>₩</u> <u>O</u> K X <u>C</u> ancel

شکل ۳۰: The "Filter Expression" dialog box

تعريف و ذخيره كردن فيلترها

با Wireshark می توان 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 را انتخاب می کنیم. dialog box زیر ظاهر می شود که می توان فیلتر جدید را تعریف نمود.

🗖 Wireshark	: Display Filter						
Edit	Filter						
	tpkt_long						
	tpkt_only						
New	ethernet broadcast						
	ip broadcast						
	DCERPC fault						
Delete							
Properties							
Filter name: in	broadcast						
Filter string:       ip.addr == 255.255.255.255							
🔯 <u>H</u> elp	QK ✔ Apply 🕞 Save 🗙 Close						

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

تعریف و ذخیره کردن ماکروهای فیلتر

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

پيداكردن پكتها

می توان به سادگی پکت هایی را در فایل ضبط شده پیدا کرد. بدین منظور از منوی Edit، گزینهی Find packet را انتخاب می کنیم

Wireshark: Fi	🛽 Wireshark: Find Packet								
Find	Find								
By: 💿 Display filte	By:      Display filter      Hex value      String								
Ellter:	Filter:								
Search In String Options									
🔿 Packet list	Case sensitive	◯ Up							
🔿 Packet details	Character set:	💿 <u>D</u> own							
<ul> <li>Packet bytes</li> </ul>	ASCII Unicode & Non-Unicode 💌								
	Eind	🗶 <u>C</u> ancel							

شکل ۲۳: The "Find Packet" dialog box

رفتن به یک پکت مشخص

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

دستور "Go Back"

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

#### دستور "Go Forward"

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

#### The "Go to Packet" dialog box

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

Wireshark:		
Packet number: 1		
🔯 <u>H</u> elp	💫 Jump to	🗶 Cancel

شکل ۳۳: The "Go to Packet" dialog box

#### "Go to Corresponding packet" دستور

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" دستور

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

"Go to Last Packet" دستور

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

نشانه گذاری پکتها

می توان پکتها در صفحهی لیست پکتها نشانه گذاری کرد. در اینصورت پکت موردنظر با زمینهی سیاه نشان داده خواهد شد. نشانه گذاری پکت برای پیداکردن آن در زمان تحلیل یک فایل بزرگ ضبط شده می تواند مفید باشد.

فرمتهای نمایش زمان و مراجع زمان
هنگامیکه 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 : ۱۹۷۰-۱۰-۱۰۱۰۰۱:۰۲:۰۳,۱۲۳٤٥٦ :Date and Time of Day شده است.
  - Time of Day: ۰۱:۰۲:۰۳,۱۲۳٤٥٦ زمان مطلق روزی که پکت ضبط شده است.
- seconds Since Beginning of Capture : ۶۹۲,۱۲۳٤۵٦ زمان نسبی از زمان شروع ضبط فایل یا اولین زمان مرجع قبل از این پکت.
  - Seconds Since Previous Captured Packet : زمان نسبت به یکت قبلی ضبط شده
- Seconds Since Previous Displayed Packet : ۲۵۱،۱۲۳٤۵۲ زمان نسبت به پکت قبلی نمایش داده شده
- (۱۹۷۰-۰۱-۱۰) (نیمه شب ۱۲۳٤۵۲۷۸۹۰,۱۲۳٤۵۲ : Seconds Since Epoch (۱۹۷۰-۰۱-۱۰)
  UTC ماه ژانویه ۱۹۷۰)

دقتهای موجود در Wireshark عبارتند از:

• Automatic : این دقت به صورت پیش فرض در Wireshark استفاده می شود.

: Nanoseconds الع المعالي المعامي المعامي المعامي Nanoseconds :

مثالی از دقت: اگر یک زمان داشته باشیم که دارای فرمت "Seconds Since Previous Packet" باشد، ممکن است دارای مقدار ۱٫۱۲۳٤٥٦ باشد. این فرمت دارای دقت اوماتیک می باشد، اگر از روش دوم استفاده شود با دقت Seconds مقدار ۱ و با دقت Nanoseconds مقدار ۱٫۱۲۳٤٥٦۰۰۰ نشان داده می شود.

#### Packet time referencing

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

🗖 test. p	cap - Wire	shark														(		×
<u> Eile Edit</u>	⊻iew <u>G</u> o	⊆apture	Analyze	Statistics	Help													
			c (	×	e,	8	٩	\$	•	÷	Ŧ	⊉	[		Ţ	€,	Q,	
Filter:									• •	🕈 Exp	ressio	n	8	⊆lear	√ Арр	bly		
No. +	Time	Source			Destin	ation			Proto	ocol I	info							^
4	1.025659	192.1	68.0.2		igmp.	mcast	t.net		IGMP	۰ ۱	/3 Me	embe	rshi	p Rep	ort		C MIII	
5	1.044366	192.1	68.0.2		192.1	168.0.	.1		DNS		Stand	dand	que	ny SR	v _1d	apto	p.nbg	
6	1.048652	192.1	68.0.2 68.0.2		239.2	255.25	1		DNS	2	Stand	te p	ort:	3193 rv SO	Des A nh1i	tinati DO61d	on po	
8	1.055053	192.1	68.0.1		192.1	168.0.	.2		UDP	2	Sourc	ie p	ort:	1900	Des	tinati	on po	
9	1.082038	192.1	68.0.2		192.1	168.0.	.255		NBNS	5 F	Regis	stra	tion	NB N	B1006	1D<00>	,	
10	*REF*	192.1	68.0.2		192.1	168.0.	.1		DNS	-	stano 2106	lard	que	ny A Esvel	proxy	cont.v	w004.	
12	0.115337	192.1	68.0.1		192.1	168.0.	.2		TCP	Ē	ittp	$\frac{2}{3}$	196	ESYN,	ACK]	Seg=0	) Ack=	
13	0.115380	192.1	68.0.2		192.1	168.0.	.1		TCP	3	3196	> h	ttp	[ACK]	Seq=	1 Ack=	⊧1 Win	
14	0.115506	192.1	68.0.2		192.1	168.0.	.1		TCP		3196	> h	ttp 106	[PSH,	ACK]	Seq=1	L Ack=	
16	0.120476	192.1	68.0.1		192.1	168.0.	.2		TCP		ТСР	Win	dow	Updat	e] ht	tp > 3	196 W	
17	0.136410	192.1	68.0.1		192.1	168.0.	.2		TCP	1	1025	> 5	000	[SYN]	Seq=	0 Len=	O MSS	V
<																	>	1
Ide	ntificati	on: 0×184	47 (6215	,														~
🔲 Fla	igs: 0×00																	
Fra	gment off	set: O																
Tim	ne to live	: 128																
Pro	tocol: UD	P (0×11)	_	_														
🕀 Hea	der check	sum: Oxal	109 [cor	rect]														
Sou D	irce: 192.	168.0.2 (	(192.168	.0.2)														
Ues	tination:	192.168.	.0.1 (19	2.168.0.	1)													<u> </u>
0000 00	09 5b 2d	75 9a 00	)0b5d )11 =1	20 cd 0	2 08 0	)0 45 )2 c0	00 a8	[-u. тс	]		Ε.							^
0020 00	01 Ob d2	00 35 00	35 46	69 00 2	1010		01	5	.5 Fi	i.!								
0030 00	00 00 00	00 00 09	70 72	6f 78 7	9 63 8 5 60 3	of 6e	66 60		.p ro	oxyco	nf							
0050 65	74 00 00	01 00 01	73 69 L	00 OU O	, ee (	5 05	0e	et		emens	• 11							~
File: "D:/te:	st.pcap" 14 K	B 00:00:02										P: 1	120 D:	120 M:	0			.:

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

شکل ۳٤: نمایش یک پکت با مرجع زمانی

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

# آمار

Wireshark یک محدوده ی وسیعی از آمارهای شبکه را از طریق گزینهی Statistics فراهم می آورد. این آمارها از اطلاعات کلی دربارهی فایل ضبط شده نظیر تعداد پکتهای عبوری از شبکه تا آمار پروتکلهای شبکه نظیر تعداد درخواستها و پاسخها ی HTTP را شامل می شود.

بعضی از آمارهای کلی عبارتند از:

- Summary دربارهی فایل ضبط شده.
- Protocol Hierarchy از یکتهای 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 پکتها در زمان.

آمارهای خاص پروتکل عبارتند از:

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

<sup>&#</sup>x27; requests

<sup>&</sup>lt;sup>r</sup> responses

🔽 Wiresha	rk: Summary		_ • ×					
File Name: Length: Format: Packet size limit:	/home/stig/http.pcap 1713904 bytes Wireshark/tcpdump/ libpcap 65535 bytes							
Time First packet: Last packet: Elapsed:	2007-11-30 20 2007-11-30 20 00:00:32	1:49:42 1:50:14						
Capture Interface: Dropped packets: Capture filter:	eth0 unknown none							
Display Display filter:	http or dns							
Traffic	Captured	Displayed	Marked					
Packets	2239	367	0					
Between first and last packet	32.374 sec	19.684 sec						
Avg. packets/sec	69.160	18.645						
Avg. packet size	749.467 bytes	575.507 bytes						
Bytes	1678056	211211						
Avg. bytes/sec	51833.067	10730.261						
Avg. MBit/sec	0.415	0.086						
elp			Close					

شکل ۳۵: پنجرهی Summery

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

File: اطلاعات کلی دربارہی فایل ضبط شدہ.

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

Capture: اطلاعات در مدت زمان ضبط بسته ها را نشان می دهد.

Display: بعضى از اطلاعات (نظير display filter) را نمايش مىدهد.

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 H	ierarchy	Statist	ics			_ • ×
	Display filt	er: http o	r 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	υ	υ	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
2 Help						[	Close



همانطور که در شکل بالا مشاهده می شود، این گزینه درخت تمام پروتکل های ضبط شده را نمایش میدهد. می توان زیر درخت ها را با کلیک کردن روی آیکون های 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 Byted: تعداد مطلق بایت های پروتکل (درحالیکه این پروتکل بالاترین پروتکل برای دیکد شدن بوده است)
- End Mbit/s پهنای باند پروتکل در مدت زمان ضبط بسته ها (درحالیکه این پروتکل بالاترین پروتکل برای دیکد شدن بوده است)

#### پنجرهی Conversations

منظور از مکالمه یا Conversaion در شبکه، ترافیک بین دو نقطهی انتهایی مشخص میباشد. به عنوان مثال یک IP conversaion 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 ضبظ و شروع مکالمه بر حسب ثانیه (Rel Start)، زمان مکالمه بر حسب ثانیه و میانگین بیتها (نه بایتها) در هر ثانیه در تمام جهات.

			Convers	ations: I	http.po	sap			
Ethernet: 1	ibre Cha	annel FDDI <b>IPv</b>	4: 15 IPX	JXTA NC		SCTP TCP	: 38 Token Rin	ING UDP: 1 USE	B WLAN
			TCP Conv	ersations	- Filter	http or dns			
Address A	Port A	Address B	Port B	Packets	Bytes	Packets A	->B Bytes A	->B   Packets A	<-B
10.211.55.3	60790	193.69.165.21	http	126	7261	5 63	28028	63	
10.211.55.3	60789	193.69.165.21	http	104	6479	1 52	23330	52	
10.211.55.3	41144	128.121.50.12	2 http	18	9991	9	6794	9	
10.211.55.3	41145	128.121.50.12	2 http	18	8994	9	6885	9	
10.211.55.3	45168	193.69.165.57	http	4	3336	2	970	2	
10.211.55.3	51236	81.93.163.17	منطقها المناطقة المناطقة	~	2001		1500	2 -	
10.211.55.3	45169	193.69.165.5	Apply as Fil	ter	•	Selected	,	A <-> B	
10.211.55.3	50948	81.7.166.249	Prepare a f	Filter	•	Not Selected	• k	A> B	
10.211.55.3	41632	194.237.107. p	Find Packet		•	and Selec	ted 🕨	A < B	
10.211.55.3	51305	193.69.165.2	Colorizo Co	nvorentia		or Selecte	d b		
10.211.55.3	58101	80.76.145.17		niversatio	// ·	of Selecte	, u , r		
10.211.55.3	41623	209.85.141.99	http	4	1967	and not S	elected 🕨	A> ANY	
10.211.55.3	43305	62.70.11.43	http	2	1959	or not Sel	ected 🕨	A < ANY	
10.211.55.3	51291	193.69.165.29	http	2	1876	Ţ	541	ANY <-> B	
4								ANY < B	
🛿 Name reso	lution			0	🗹 Limit	to display filt	er	ANY> B	
? <u>H</u> elp								Eopy	<u>C</u> lose

شکل ۳۷: پنجرهی Conversations

هر سطر در لیست مقادیر آماری را برای دقیقا 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 نقطه ی انتهایی Ethernet معادل آدرس MAC مربوط به Ethernet می باشد.

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

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

IPv٤ : یک نقطهی انتهایی IP معادل آدرس IP مربوط به آن می باشد.

XXX : IPX– اطلاعات را اينجا وارد كنيد.

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

Token Ring : یک نقطهی انتهایی Token Ring معادل آدرس MAC مربوط به Toekn Ring می باشد.

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

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

thernet: 2 Fibre (	Channel	FDDI <b>IP</b> v	4:16 (PX )X	TA NCP F	RSVP SCTP	TCP:	51 Token Ring UDP: 2 USB	WLA
			IP∨4 Endp	oints - Filte	er: http or dn	IS		
Address	Packets	Bytes	T× Packets	Tx Bytes	Rx Packets	R× E	Bytes	
10.211.55.3	367	211211	184	91005	183	120	206	
193.69.165.21	230	137406	115	86048	115	513	58	
128.121.50.122	36	18985	18	5306	18	136	79	
193.69.165.29	28	18580	14	10235	14	834	5	
10.211.55.1	24	4182	12	3275	12	907		
193.69.165.57	8	5824	4	388	a Tila an	100	Coloritoria	
62.70.11.43	6	3596	3	201 Apply	as Hiter	•	Selected	
81.7.166.249	6	5165	3	188 Prepa	are a Filter	•	Not Selected	
81.93.163.170	7	3581	3	14 Find F	rame	•	and Selected	
209.85.141.99	4	1967	2	58( Color	ize Hest Traff	i.c.	or Selected	
81.93.172.130	4	1610	2	524			of Selected	
194.237.107.53	4	3817	2	1830	2	198	and not Selected	
193.88.71.150	4	2193	2	1037	2	115	or not Selected	
66.102.9.99	2	1060	1	425	1	635		
194.237.107.154	2	1252	1	277	1	975		
/ Name resolution	٦			🗹 L	imit to displa	ay filt	er	

شكل ۳۸: پنجرەي 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 "<sup>o</sup> Ethernet" می گوید که پنج نقطهی انتهایی ضبط شده است). هر سطر در لیست مقادیر آماری برای دقیقا یک نقطهی انتهایی را نشان میدهد.

# پنجرهی Endpoint List برای پروتکل مشخص

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

#### پنجرهی IO Graphs

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

	Wireshark IO Graphs: h	nttp.pcap			_ <b> </b>
					- 250
	Os	10s	20s	6	30s
					Þ
Graphs				Axis	
Graph 1 Color <u>Filter:</u>	st	tyle: Line	<b>≑</b> Tio	ck interval:	l sec 🛟
Graph 2 Color 🛐 <u>F</u> ilter:	http St	tyle: Line	🗧 Pi	xels per tick	:: 10 🗘
Graph 3 Color <u>Filter</u> :	st	tyle: Line	÷,	] <u>V</u> iew as tir Axis	me of day
Graph 4 Color 😰 <u>F</u> ilter:	st	tyle: Line	+ Ur	nit: Pa	ackets/Tick 💲
Graph 5 Color I	st	tyle: Line	¢ so	ale: Au	ito 🔶
elp Help			ору	<u>S</u> ave	Close

شکل ۳۹: پنجرهی IO Graphs

کاربر میتواند پارامترهای زیر را تنظیم کند:

- گراف،ا
- گراف ٥-۱: یکی از گراف های نوع ۱ تا ٥ 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 می تواند یک از انواع Fbar ،Impulse ،Line یا Dot باشد.

• محور X

- فاصلەي علامت
- تعداد پیکسل های هر علامت: می توان از ۱۰/۵/۲/۱ پیکسل برای هر علانت استفاده کرد.
- مشاهده به صورت زمان روز: می توان محور x را به صورت روز به جای ثانیه یا دقیقه برچسب
  گذاری کرد.
  - محور Y
- واحد محور y که می تواند به صورت Advanced ،Bits/Tick ،Bytes/Tick ،Packets/Tick و ..
  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 می شوند.

**Tick interval** 

		Wire	shark: WL	AN Traffic St	atistics: w	L.pcap					_ <b>-</b> ×
				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	ı			🗹 Only	r show existi	ng networks				Copy	Close

شکل ٤٠: آمار ترافیک WLAN

هر سطر در این لیست مقادیر آماری برای دقیقا یک شبکهی بی سیم را نشان می دهند.

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 می شوند.

2	1		Wire	shark: WL	AN Traffic St	atistics: w	1.pcap					_ <b>-</b> ×
					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 resolutior	٦			🗹 Only	<sup>,</sup> show existi	ng networks					
	Pelp										Copy	Close

شکل ٤١: آمار ترافيک WLAN

هر سطر در این لیست مقادیر آماری برای دقیقا 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.

🖸 Wiresha	ark: Compute DCE-RPC SRT st	atistics 📃 🗖 🔀	
Program:	ATSVC - EPM	Version: 1	
	1		
Eilter:			
	Creat	te Stat 🗶 Cancel	

شکل ٤٢: پنجرهی "Compute DCE-RPC statistics"

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

DCE-	RPC Service Response Ti DCE-RPC Service Resp	i <mark>me statistics</mark> onse Time statis Filt	tics for EPM n	najor versio najor version 3	on 3: test	
ndex	Procedure	Calls *	Min SRT	Max SRT	Avg SRT	

شکل ٤٣: پنجرهي "... DCE-RPC Statistic for"

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

پنجرهی آمارها برای یک پروتکل مشخص

این پنجره اطلاعات جزیی پروتکلها را نشان میدهد.

' calls

- 1) <u>www.wireshark.org</u>
- (\*) Ulf Lamping, Richard Sharpe, and Ed Warnicke, '*Wireshark User's Guide*,' NS Computer Software and Services P/L, 2008.

منابع