



Yellow Way; Wireshark, Penetration Testers Guide

By Milad Kahsari Alhadi(C3phalex1n)

What is wireshark, Capturing packet of network with wireshark, Features you need to know about wireshark, Wireshark Activity and so on.



درباره نویسنده کتاب

نام و نام خانوادگی: میلاد کهساری الهادی (سفالکسین)

تاریخ تولد: 1373 - اردیبهشت 14

مقطع تحصیلی: کاردانی، نرم افزار، شهید چمران گرگان (فعلا)

علاقه مندی ها : از سن 15 سالگی وارد عرصه امنیت و شبکه های کامپیوتری شده و تو این سال ها توانسته ام با موفقیت مدارک Linux Plus و Network Plus را دریافت کنم و هم اکنون در حال مطالعه و ادامه راه علم آموزی خود در زمینه شبکه، مهندسی معکوس و تکنولوژی های نوین کامپیوتر هستم.

علاوه بر نکات فوق الذکر در این مدتی که در عرصه امنیت رایانه ها فعالیت داشته ام، کتاب هایی از جمله؛ راهنمای استفاده از فریمورک متاسپلویت، راهنمای راه اندازی آزمایشگاه امنیت، تجزیه و تحلیل بدافزار را به انتشار رسانده ام و همچنین در مجلات امنیتی چندین مقاله پژوهشی به انتشار عموم گذاشته ام که از آنها می توان به عنوان سابقه پژوهشی خود در زمینه امنیت و اطلاعات یاد کنم.

Twitter: https://twitter.com/C3phalex1n_0x

Facebook: <https://facebook.com/Milad.kahsari>

Linkedin : <https://ir.linkedin.com/in/miladkahsari>

Milad Kahsari Alhadi (0xc3phalex1n[AT]gmail.com)

SECURITY IS LOVE

همراه بسیار است، اما همدمی نیست
مثل تمام غصه ها، این هم غمی نیست
دل بسته اندوه دامن گیر خود باش
از عالم غم دلربا تر عالمی نیست
کار بزرگ خویش را کوچک مپندار
از دوست دشمن ساختن کار کمی نیست
چشمی حقیقت بین کنار کعبه می گفت
«انسان» فراوان است، اما «آدمی» نیست.

فاضل نظری

موضوع	صفحه
فصل اول : معرفی ابزار Wireshark	7
برخی از اهداف مورد نظر Wireshark	7
ویژگی ها	7
آنچه Wireshark پشتیبانی نمی کند	8
برنامه Wireshark با جزئیات دقیق تر؟	9
برنامه Wireshark چگونه کار می کند؟	10
فصل دوم : نصب برنامه Wireshark	11
گام اول : چه چیزی ما نیاز داریم؟!	11
گام دوم : دانلود برنامه Wireshark	11
گام سوم : نصب کردن Wireshark	12
نصب کردن Wireshark از طریق کد منبع آن	13
نصب از طریق بسته های نرم افزاری لینوکس	15
نصب Wireshark از طریق فایل باینری RPM	15
نصب Wireshark از طریق فایل باینری DEB	16
نصب و راه اندازی Subversion	17
فصل سوم : ضبط اولین بسته شبکه با Wireshark	18
انتخاب رابط شبکه	18
نگاهی سریع به رابط گرافیکی کاربر برنامه Wireshark	20
پانل های گرافیکی Wireshark	21
پانل ضبط	22
پانل مشخصات بسته	22
پانل بایت های بسته	23
پانل وضعیت	23
تنظیم فیلتر ها	30
کار با جعبه محاوره ای Filter Expression	32
ضبط زنده اطلاعات	32
آشنایی با رنگ آمیزی بسته ها توسط Wireshark	33
کار با بسته های اطلاعاتی ضبط شده	34
جستجو برای بسته ها	35
علامت گذاری بسته ها	35
ذخیره سازی داده های ضبط شده	35
صدور و ادغام بسته ها	37
چاپ بسته های	38

39	پنجره گراف ورودی و خروجی
41	اطلاعات تخصصی
43	استفاده از پنجره Preferences
44	فصل چهارم : 5 ویژگی مهمی که شما باید درباره آن ها بدانید
45	کار با جریان های بسته
47	رمز گشایی بسته و صادرات اشیاء
48	آمارگیری بسته های ضبط شده
51	نمایش سلسله مراتبی پروتکل
54	تفکیک اسامی و مونتاژ دوباره بسته ها
55	مونتاژ دوباره بسته ها
55	ابزار های تحت خط فرمان Wireshark
57	برنامه Terminal Wireshark یا Tshark
59	Rawshark، انباشت و تجزیه و تحلیل ترافیک

بِسْمِ اللَّهِ الرَّحْمَنِ الرَّحِيمِ

اللَّهُمَّ عَجِّلْ لَوْلِيكَ الْفَرَجَ وَالْعَافِيَةَ وَالنَّصْرَ

و اجعلنا من خَيْرِ أَنْصَارِهِ وَاعْوَانِهِ وَ الْمُسْتَشْهَدِينَ بَيْنَ يَدَيْهِ

خدایا، ولیّ ات حضرت حجّه بن الحسن که دروذهای تو بر او و بر پدرانش باد. در این لحظه و در تمام لحظات سرپرست و نگاهدار و راهبر و یاری گر و راهنما و دیدبانش باش، تا او را به صورتی که خوشایند اوست ساکن زمین گردانی، و مدّت زمان طولانی در آن بهره‌مند سازی. به امید ظهور پایان دهنده تمامی تاریکی ها و ترس ها امام بزرگوار شیعیان مهدی (ع).

فصل اول : معرفی ابزار Wireshark

برنامه Wireshark تحلیلگر بسته های شبکه¹ است. یک تحلیل کننده بسته های شبکه سعی در ضبط² بسته های شبکه دارد و تلاش می کند جزئیات آن بسته ها را تا جای ممکن به دست آورده و به ما ارائه بدهد. 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 روند، 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 گران قیمت یا اختصاصی یا هردو گزینه ذکر شده بوده اند. به هر صورت، با ظهور Wireshark، تمام آن شرایط تغییر کرد. به احتمال زیاد، امروزه Wireshark یکی از بهترین تحلیلگران بسته های شبکه متن 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 از بین بردن مشکلات به وجود آمده در شبکه استفاده می کنند.
- مهندسين امنيت شبکه آن را برای بازبینی مشکلات امنیتی شبکه استفاده می کنند.
- توسعه دهندگان برای اشکال زدایی پیاده سازی های پروتکل از آن استفاده می کنند.
- افراد از آن برای یادگیری کارکرد داخلی پروتکل استفاده می کنند.
- در کنار این مثال ها، در موقعیت های بسیار دیگری نیز Wireshark می تواند مفید واقع شود.

ویژگی ها

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

- قابل استفاده برای UNIX و Windows
- ضبط زنده بسته های داده از واسط شبکه³
- نمایش بسته ها با جزئی ترین اطلاعات پروتکل
- باز کردن و ذخیره ی بسته های داده ای ضبط شده
- وارد کردن و صادر کردن بسته های داده از برنامه های دیگر
- فیلتر کردن بسته ها بر اساس معیارهای مختلف

¹ Packet Analyzer

² Capture

³ Network Interface

- 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 متن باز
- و بسیاری از ویژگی های دیگر ...

آنچه Wireshark پشتیبانی نمی کند

در اینجا مواردی را آورده ایم که متاسفانه Wireshark آنها را نمی تواند برای ما تامین کند:

- Wireshark برنامه ای برای تشخیص نفوذ به سیستم نیست. با استناد به همین موضوع، این برنامه زمانیکه شخصی عملیات غیرعادی که مجاز به انجام آنها نیست در شبکه انجام بدهد، هیچ خطاری برای ما در خروجی صادر نخواهد کرد. در هر صورت، به هنگام رخ دادن اتفاقات عجیب، Wireshark در دریافتن آنچه در حال روی دادن است فقط می تواند به متخصصین کمک 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 اسامی¹، ولی حتی آن هم می تواند غیرفعال گردد)

برنامه Wireshark با جزئیات دقیق تر؟

Wireshark یک ابزار متن باز برای تحلیل شبکه های رایانه ای است که جریان داده های در حال عبور از سیم (رسانه انتقال شبکه) را دریافت می کند و در یک قالب قابل فهم برای انسان به نمایش می گذارد. می توان برنامه Wireshark را مانند یک چاقوی سوئیسی همه کاره در نظر گرفت، زیرا از این برنامه می توان برای اهداف گوناگونی؛ مانند تحلیل شبکه، عملیات های امنیتی، اشکال یابی شبکه و اعمال مهندسی معکوس بر روی پروتکل ها و فهمیدن جزئیات درون آنها و... این برنامه را مورد استفاده قرار داد. برنامه Wireshark تنها ابزاری است که تمامی این قابلیت ها را به سادگی به ما ارائه می دهد. برخی از مزئیت های مهم استفاده از Wireshark به شرح زیر است:

1. پشتیبانی از چندین پروتکل²: برنامه Wireshark یک محدوده بسیار گسترده ای از پروتکل های شبکه، مانند پروتکل های TCP، UDP و Http تا پروتکل های پیشرفته مانند AppleTalk را پشتیبانی می کند.

¹ Name Resolution

² Multiple protocol support

2. **رابط کاربر پسند¹** : برنامه Wireshark یک رابط کاربر گرافیکی (GUI) بسیار قدرتمند دارد که این رابط به متخصصین اجازه می دهد، بسته های ضبط شده خود را به ساده ترین شکل ممکن تحلیل کنند. همچنین چندین گزینه پیشرفته از قبیل فیلتر کردن بسته ها²، صادر کردن بسته ها³ و تفکیک کننده اسامی⁴ هم به ما ارائه می دهد.
 3. **تحلیل زنده ترافیک⁵** : برنامه Wireshark می تواند به صورت زنده جریان شاری در رسانه انتقال را دریافت کرده و به سرعت اطلاعات پروتکل، جریان رسانه، کانال های ارتباطی و ... آن را در خروجی برای ما تولید کند.
 4. **پروژه متن باز⁶** : برنامه Wireshark یک پروژه متن باز است و بیشتر توسعه دهندگان آن در قالب 500 نفر از قسمت های گوناگون جهان می باشند. حتی شما هم می توانید یکی از توسعه دهندگان این برنامه باشید.
- این چند ویژگی باعث شده است برنامه Wireshark مشهورترین برنامه متن باز در حوزه تحلیل شبکه گردد. با این حال در قسمت بعدی، درباره این عملیات ها با جزئیات بیشتر بحث خواهیم کرد.

برنامه Wireshark چگونه کار می کند؟

اجازه دهید یک مقدمه بسیار کوتاه درباره نحوه عملکرد برنامه Wireshark ارائه بدهیم. شنود ترافیک شبکه زمانی ممکن است که رابط شبکه (کارت شبکه) بر روی حالت انتقال بی قاعده⁷ قرار بگیرد. این حالت موجب می شود، رابط شبکه تمامی ترافیک دریافتی را به جای آن فریم ای که کنترل کننده برای دریافت در نظر گرفته بوده است را تماماً به واحد پردازشگر مرکزی انتقال دهد. حالت بی قاعده برای شبکه های Bridged شده در مجازی سازی توسعه اولیه داده شده بود. با این حال می توان شنود شبکه توسط Wireshark را به سه گام کلی تقسیم کرد، که به شرح زیر هستند :

1. **جمع آوری⁸** : در گام اول، برنامه Wireshark ابتدا رابط شبکه را به حالت بی قاعده انتقال می دهد، تا بتواند داده های باینری خام بر روی رسانه انتقال را دریافت کند.
2. **تبدیل⁹** : در گام دوم، داده های باینری جمع آوری شده به یک قالب قابل فهم برای انسان تبدیل می شوند. همچنین بسته ها بر مبنای عدد سلسله مراتبی خود دوباره مونتاز می گردند.

¹ User friendly interface

² Filtering the packets

³ Exporting packets

⁴ Name resolution

⁵ Live traffic analysis

⁶ Open source project

⁷ Promiscuous mode

⁸ Collection

⁹ Conversion

3. **تحلیل**¹: گام آخری شامل تحلیل بسته های دریافت شده و داده های دوباره مونتاژ شده می گردد. تحلیل اولیه بسته ها شامل شناسایی نوع پروتکل، کانال ارتباطی، شماره درگاه و... می شود. همچنین در یک سطح پیشرفته سرآیند های متفاوت پروتکل می توانند برای یک درک عمیق تر نیز مورد تحلیل قرار گیرند. این یک مقدمه بسیار ساده درباره Wireshark و روش های عملیاتی آن بود. در قسمت بعدی ما فرآیند نصب کردن آن را با جزئیات دقیقی نشان خواهیم داد.

¹ Analysis:

فصل دوم : نصب برنامه Wireshark

اجازه بدهید سفر خود به تجزیه و تحلیل شبکه با استفاده از Wireshark را آغاز کنیم. در اولین گام، نحوه نصب و راه اندازی محیط Wireshark را بررسی خواهیم کرد. در این قسمت ما روش نصب این برنامه بر روی لینوکس و ویندوز را نمایش خواهیم داد و در گام بعدی نحوه راه اندازی یک محیط Subversion برای به روز رسانی کتابخانه ها و اجزای مورد نیاز Wireshark را به شما خواهیم آموخت. بنابراین بگذارید کار خود را با نصب Wireshark بر روی ویندوز آغاز کنیم. شما می توانید در طی سه گام تشریح شده زیر Wireshark را بر روی ویندوز نصب و راه اندازی کنید.


گام اول : چه چیزی ما نیاز داریم؟!

لیست زیر نیازمندی های این برنامه است :


1. **فضای آزاد :** برای نصب برنامه Wireshark حداقل 100 مگابایت فضای آزاد نیاز است، شایان ذکر است، به منظور ذخیره سازی بسته های ضبط شده توسط Wireshark به فضای بیشتری نیاز خواهید داشت.
2. **حافظه :** برنامه Wireshark حداقل به 256 مگابایت حافظه نیاز دارد، اما برای کارایی بهتر 1 گیگابایت فضای حافظه توصیه می شود.
3. **نیازمندی های :** برنامه Wireshark نیاز به یک کارت شبکه (network interface card) دارد که حالت بی قاعده (promiscuous mode) را پشتیبانی کند. همچنین برنامه Wireshark به راه انداز WinPcap نیاز دارد که در ضبط و شنود بسته های شبکه مورد استفاده قرار می گیرد.

گام دوم : دانلود برنامه Wireshark

راحت ترین راه دانلود Wireshark برای سیستم عامل ویندوز، رفتن به وب سایت <http://www.wireshark.org> و دریافت بسته فشرده شده آن برای سیستم عامل ویندوز است. در این وب سایت شما می توانید آخرین نسخه پایدار (Stable) برنامه Wireshark را مطابق با معماری (x86 یا x64) و نسخه سیستم عامل خود دانلود کنید. کاربران سیستم عامل ویندوز می توانند با کلیک راست کردن بر روی My Computer معماری سیستم عامل خود را مشخص سازند و کاربران سیستم عامل لینوکس برای شناسایی معماری سیستم خود می توانند دستور `uname -i` را در ترمینال اجرا کنند.



[Get Acquainted ▾](#)
[Get Help ▾](#)
[Develop ▾](#)
[Our Sponsor](#)
[WinPcap](#)

What's on your network?




Download

Get Started Now



Learn

Knowledge is Power



Enhance

With Riverbed Technology

News And Events

SHARKFEST Was Great!

Thanks to all of the Sharkfest '13 attendees, developers, speakers, and organizers. It was once again a wonderful event and we're looking forward to next year.

[Sharkfest Retrospective ▸](#)

Wireshark 101 Released!

by Laura Chappell
Foreword by Gerald Combs

This book is based on over 20 years of analyzing networks and teaching key analysis skills. It's the book many people have been waiting for Laura to write!

Wireshark 101 is available in paperback and Kindle formats.

[Learn More ▸](#)

[More News ▸](#)

Wireshark Blog

Wireshark Tutorial Series #2. Tips and tricks used by insiders and veterans

Aug 12 | By Hansang Bae

Fifteen Years

Jul 15 | By Gerald Combs

Troubleshooting the hidden dangers of TCP's Nagle algorithm and delayed acknowledgement

Jan 11 | By Hansang Bae

Videos

Hands on with Wireshark

Hansang Bae shows you tips and tricks used by insiders and veterans. First in a series.

11m 43s

Enhance Wireshark

Troubleshoot your Network

Free 30 day trial

- Save hours on network and application issue diagnoses
- Monitor physical and virtual environments
- GUI packet capture and analysis
- Fully integrated with Wireshark

Try Cascade Shark VE & Cascade Pilot Free for 30 Days

802.11 Packet Capture

- WLAN packet capture and transmission
- Full 802.11 a/b/g/n support
- View management, control and data frames
- Multi-channel aggregation (with multiple adapters)

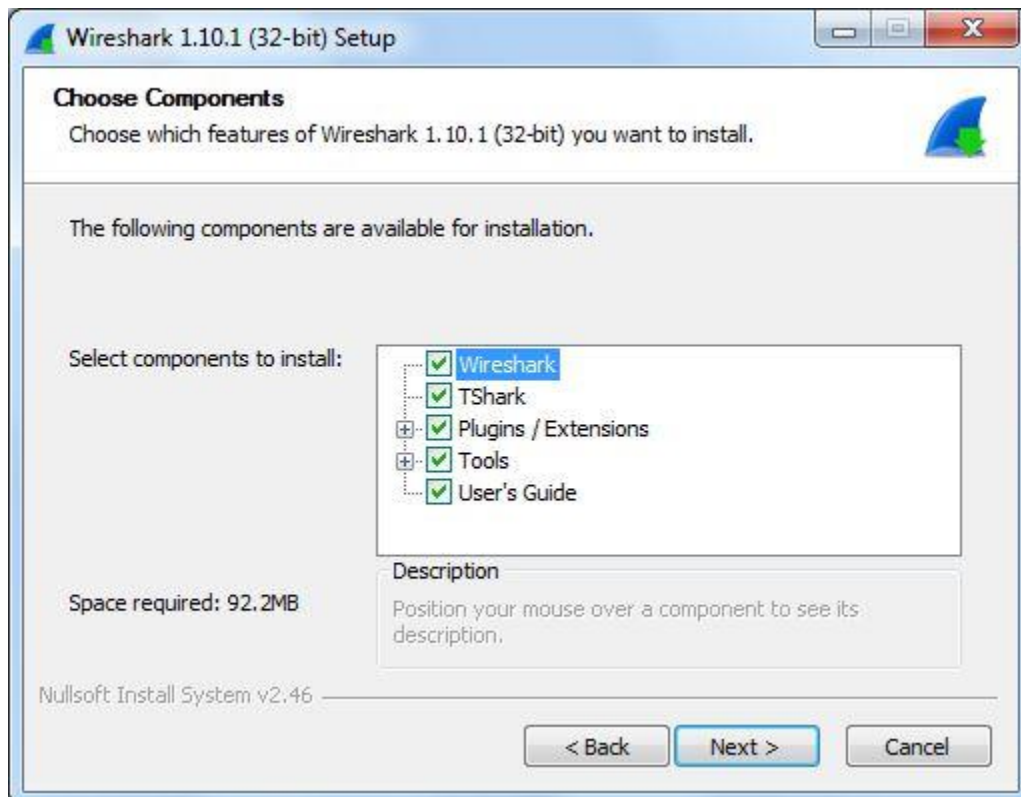
[Learn More ▸](#)

[Buy Now ▸](#)

تصویر 1-1 : صفحه وب سایت wireshark.org

گام سوم : نصب کردن Wireshark

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



حال بگذارید یک گام به جلو برداریم و در مورد نصب و راه اندازی Wireshark بر روی محیط لینوکس بحث و گفتگو کنیم. دلیل اینکه ما نصب و راه اندازی Wireshark بر روی لینوکس را مجزا مورد بررسی قرار دادیم، این است که همه توزیع های لینوکس از پروژه Wireshark پشتیبانی نمی کنند. شما می توانید لیست کامل توزیع های لینوکسی که از پروژه Wireshark پشتیبانی می کنند را در صفحه دانلود Wireshark که لینک آن در زیر آورده شده مشاهده کنید.

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

نصب کردن Wireshark از طریق کد منبع آن

به منظور نصب Wireshark از طریق کد منبع آن بر روی سیستم عامل لینوکس، چهار گام آورده شده در زیر را به دقت دنبال کنید.

گام اول : دریافت فایل های منبع

بسته کد منبع برنامه Wireshark را می توانید از صفحه دانلود wireshark که در قسمت بالا آورده شد، دانلود کنید. بدین منظور کافیست به سادگی بر روی Source Code کلیک کنید، تا کد منبع آن شروع به دانلود شود.



گام دوم : استخراج محتوای فایل فشرده

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

```
Tar -xvf wireshark-1.10.1.tar.bz2
```

گام سوم : تغییر پوشه

در این قسمت به پوشه محتویات Wireshark بروید. با دستور زیر :

```
cd wireshark-1.10.1
```

گام چهارم : نصب کردن wireshark

حال در این گام ما باید فایل های منبع را با استفاده از دستور make به حالت باینری تغییر بدهیم. سپس با استفاده از دستور install فایل های باینری را می توانیم بر روی سیستم نصب کنیم. به شکل زیر عمل کنید :

```
root:~/wireshark-1# ./configure
```

```
root:~/wireshark-1#make
```

```
root:~/wireshark-1#make install
```

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

نصب از طریق بسته های نرم افزاری لینوکس

نصب کردن برنامه Wireshark از طریق فایل باینری آن یک فرآیند بسیار ساده است. شما می توانید با استناد به توزیع لینوکس خود فایل باینری مناسب آن را دانلود کنید و به سادگی آن را در سیستم خود راه اندازی کنید. شایان ذکر است، در اینجا واژه باینری، فایل Exe در ویندوز نیست. منظور از فایل باینری، فایل اجرایی دودویی است که در سیستم عامل های گوناگون ساختار متفاوتی دارد. در این قسمت برخی از آنها را مورد بررسی قرار خواهیم داد.

نصب Wireshark از طریق فایل باینری RPM

در این قسمت ما می خواهیم Wireshark را بر روی سیستم عامل های مبتنی بر رد هت نصب و راه اندازی کنیم. بدین منظور ما نیاز خواهیم داشت فایل باینری rpm برنامه wireshark را از سایت آن دانلود کرده و سپس با دستور زیر آن را بر روی سیستم نصب و راه اندازی کنیم. این فرآیند به سادگی انجام می گیرد و شما دیگر نیاز نخواهید داشت که بسته های نرم افزاری مورد نیاز این برنامه را به صورت مجزا نصب کنید.

```
rpm -ivh wireshark-1.9.i386.rpm
```

نصب Wireshark از طریق فایل باینری DEB

برای نصب برنامه wireshark از طریق فایل های باینری DEB که مخصوص سیستم عامل های مبتنی بر دیبیا است، کفایت دستور نمایش داده شده در تصویر 2-2 را در ترمینال سیستم عامل خود اجرا کنید تا برنامه wireshark برای شما نصب شود. سیستم عامل های Backtrack، Ubuntu، Backbox از سیستم عامل هایی هستند که بر پایه دیبیا می باشند. شما می توانید متشابه با اجرا دستور زیر این برنامه را بر روی این سیستم عامل ها نصب و راه اندازی کنید.

apt-get install wireshark

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

نصب و راه اندازی Subversion

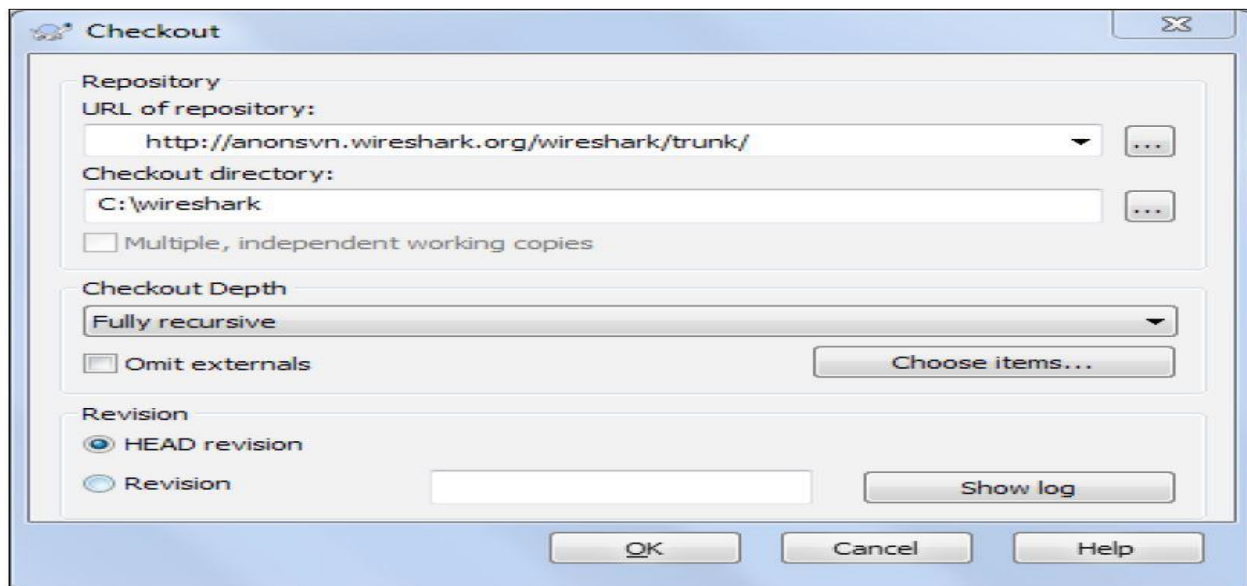
نصب و راه اندازی subversion یک گزینه دلخواه برای افرادی است که قصد دارند Wireshark را از کد منبع آن نصب کنند. Subversion کمک می کند که در سریع ترین راه ممکن کتابخانه ها و فایل های برنامه را به روز رسانی کنید. در این قسمت ما از SVN که جزء مشهورترین کلاینت های Subversion می باشد، استفاده خواهیم کرد. شما می توانید راه انداز آن را از سایت <http://tortoisesvn.tigris.org> دانلود کنید. پس از نصب موفقیت آمیز برنامه بر روی هر پوشه ای که کلیک راست کنید گزینه های SVN را مشاهده خواهید کرد. به منظور راه اندازی Subversion برای Wireshark مراحل زیر را دنبال کنید :

گام اول : ایجاد یک پوشه

در سیستم یک پوشه با نام wireshark ایجاد کنید و سپس بر روی آن کلیک راست کرده و با کلیک کردن بر روی svn checkout آن را به svn منتقل کنید.

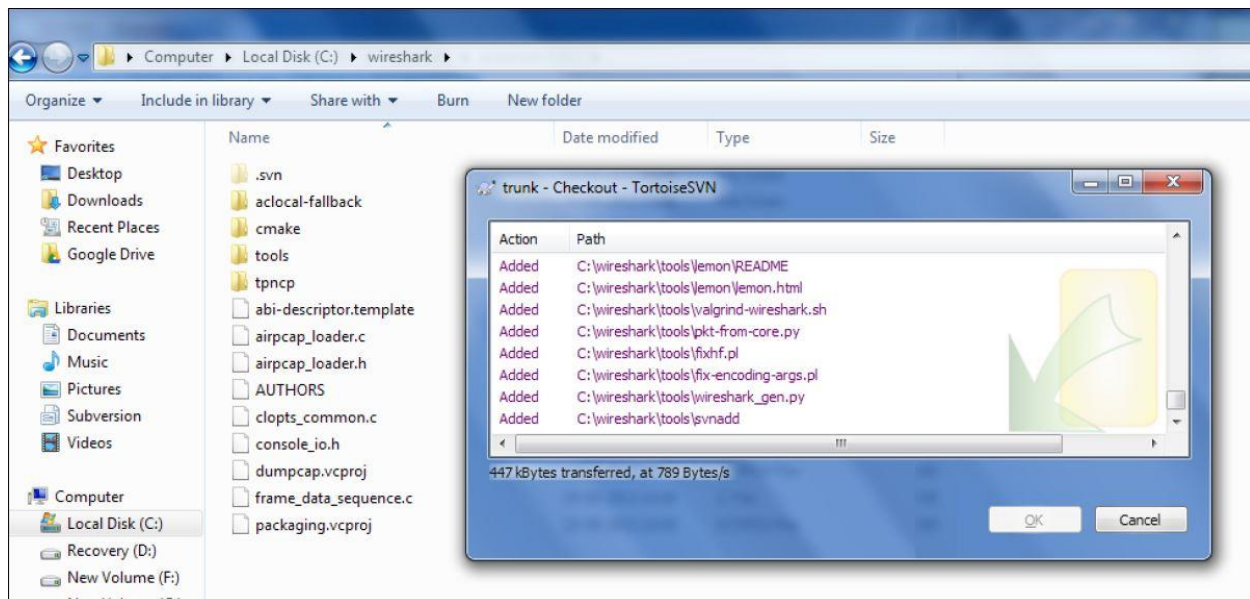
گام دو : تنظیم کردن مسیر Subversion

سپس در پنجره جدید، در قسمت Url of Repository آدرس <http://anonsvn.wireshark.org/wireshark/trunk> را وارد کرده و در قسمت Checkout directory اطمینان حاصل کنید که مسیر درست پوشه wireshark که در مرحله قبل ایجاد کرده بوده اید در این قسمت قرار دارد. سپس بر روی OK کلیک کنید، تا فرآیند به روز رسانی و شروع گردد.



گام سوم : وارسی (checkout)

هنگامی که Subversion شروع به پر کردن پوشه Wireshark می کند، مشاهده خواهید کرد که دایرکتوری های مختلفی ایجاد خواهند شد.



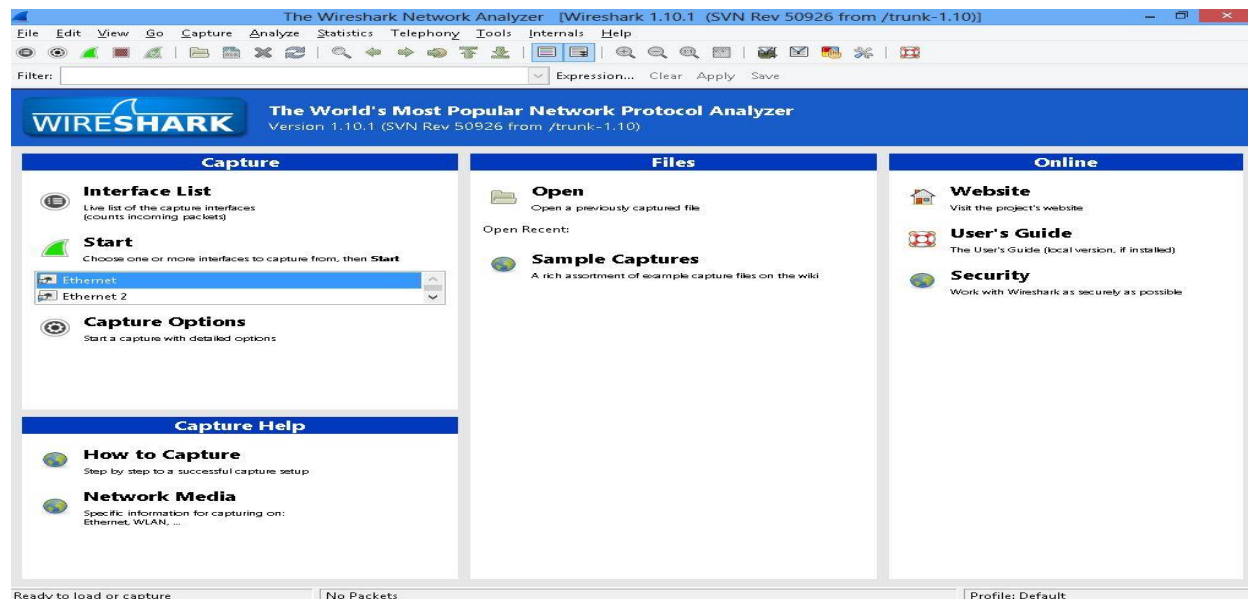
حال کلاینت tortoise تنظیم شده است و شما می توانید در هر زمان با کلیک راست کردن بر روی پوشه wireshark و انتخاب گزینه SVN update آن را به سرعت به روز رسانی کنید. این یک راهنمای سریع درباره راه اندازی Wireshark تحت محیط های مختلف بود. در قسمت بعدی، شما خواهید آموخت چگونه از Wireshark برای تحلیل اولین بسته شبکه ضبط شده خود استفاده کنید.

فصل سوم : ضبط اولین بسته شبکه با Wireshark

حال که ما توانستیم با موفقیت Wireshark را بر روی سیستم خود راه اندازی کنیم، می توانیم یک گام به جلو برداشته و ویژگی های آن را مورد بررسی قرار بدهیم. در این فصل، برخی از ویژگی های اساسی و راهنما های سریع مورد نیاز برای شروع ضبط¹ بسته های اطلاعاتی شبکه را ارائه خواهیم کرد. در ضمن ما از برخی پروتکل های شبکه رایج و واژگانی از قبیل TCP، Http و بسته های داده استفاده خواهیم کرد که آشنایی با این مفاهیم می تواند به شما در درک محتوای این کتابچه کمک به سزایی کند. حال بگذارید به جلو گامی برداریم و سفر خود به دنیای Wireshark را آغاز کنیم.

انتخاب رابط شبکه

اولین چیزی که در استفاده از Wireshark باید انجام بدهید، انتخاب رابط شبکه ای است که قصد دارید بسته های داده جاری در آن را ضبط کنید. با این حال؛ هنگامی که Wireshark را بر روی سیستم خود نصب می کنید، می توانیم به منظور اجرای آن بر روی آیکون برنامه wireshark در محیط دسکتاپ دو بار کلیک کنید یا از منوی Start سیستم عامل ویندوز برنامه Wireshark را اجرا کنید. همچنین در سیستم های مبتنی بر یونیکس، کافیت که فقط نام wireshark را در ترمینال اجرا کنید، تا برنامه برای شما اجرا گردد. سپس در اولین کاری که شما در استفاده از برنامه wireshark باید انجام بدهید، مشخص سازی رابط شبکه است. محیط برنامه wireshark به شکل زیر خواهد بود.



¹ Capture

همانطور که در تصویر بالا مشاهده می کنید، در پانل سمت چپ پنجره اصلی برنامه Wireshark در زیر دکمه Start رابط های شبکه مختلف سیستم برای ضبط بسته های اطلاعاتی نمایش داده شده اند، ما می توانیم هر کدام از آن ها را که می خواهیم، انتخاب کرده و با کلیک کردن بر روی Start بسته های اطلاعاتی آن را ضبط کنیم. به عنوان مثال، برای شنود ترافیک شبکه LAN جاری در سیستم، می توانید کارت شبکه Lan پیش فرض را انتخاب کنید (در این مثال رابط پیش فرض Ethernet 1 است) و مورد شنود قرار بدهید. مشابه همین عمل را می توانید برای شنود دیگر رابط های شبکه مورد خدمت بگیرید. هنگامی که رابط شبکه را انتخاب کردید، یک گام به جلو برداشته و بسته های اطلاعاتی شبکه را ضبط کنید، اما قبل از وارد شدن به این مبحث، بگذارید یک نگاه سطحی به محیط رابط برنامه Wireshark بیندازیم و برخی از ویژگی های مفید موجود در منوی آن را تشریح کنیم.

نگاهی سریع به رابط گرافیکی کاربر برنامه Wireshark

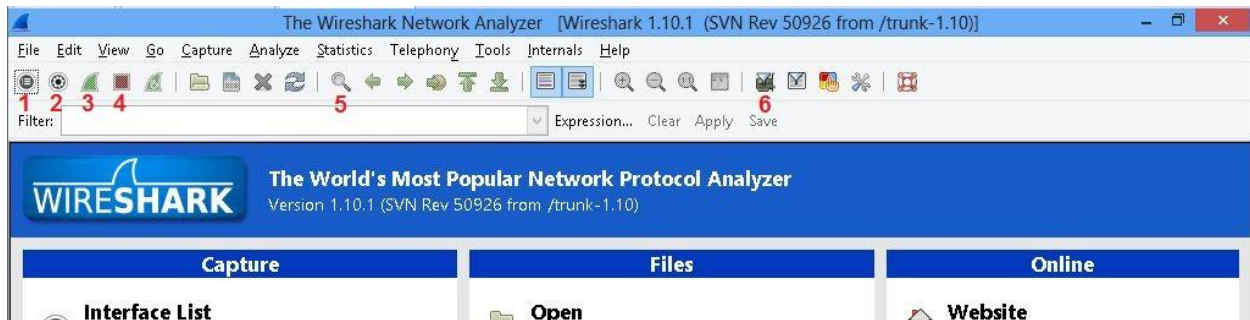
به تصویر 1-3 نگاه کنید، در این تصویر مشاهده می کنید منوی اصلی برنامه Wireshark شامل منوی های رایج از قبیل File, View, Edit و Help می شود، این منو ها عمومی هستند و شما در تمامی برنامه های دیگر مشاهده می کنید. اما دیگر منوی های این برنامه مانند Analyze و Capture در قسمت های بعدی این کتاب با جزئیات دقیق مورد بررسی قرار خواهند گرفت. منو ها شامل قسمت های زیر می باشد:

1. **File:** این قسمت شما بخش هایی برای بازکردن، ادغام فایل های دریافتی، ذخیره کردن، پرینت کردن، بیرون بردن¹ فایل های ضبط شده به طور جزئی یا کامل و خروج از Wireshark می باشد.
2. **Edit:** این قسمت شامل امکانات پیدا کردن یک بسته، مرجع زمان² یا نشانه گذاری یک یا چند پکت، تنظیم اولویت ها و ... می باشد.
3. **View:** این قسمت نمایش پکت های ضبط شده را کنترل می کند. همچنین شامل امکاناتی نظیر تعیین رنگ پکت ها، بزرگ کردن فونت ها، نمایش یک پکت در پنجره جداگانه و امکاناتی از این قبیل می باشد.
4. **Go:** این بخش شامل بخش هایی برای رفتن به یک پکت مشخص شده می باشد.
5. **Capture:** این قسمت امکان شروع یا متوقف کردن ضبط بسته ها و ویرایش فیلترهای ضبط شده را می دهد.
6. **Analyze:** این قسمت امکان دستکاری فیلترهای نمایش داده شده، فعال یا غیرفعال نمودن تجزیه پروتکل ها، پیکربندی کد برداری مشخص شده کاربر و دنبال کردن یک جریان TCP را ارائه می دهد.
7. **Statistics:** این قسمت شامل بخش هایی برای نمایش اطلاعات آماری نظیر خلاصه بسته های ضبط شده، نمایش آمار سلسله مراتب پروتکل و اطلاعاتی از این قبیل می باشد.
8. **Tools:** این قسمت شامل ابزارهای مختلف موجود در Wireshark نظیر Firewall ACL Rules می باشد.

¹ export

² Time reference

با این حال در زیر گزینه های موجود در منو، یک سری آیکون های خاص داریم که میانبری برای انجام برخی فرآیندها از قبیل ضبط بسته های شبکه و ... هستند. بگذارید در این قسمت یک نگاهی به آن ها هم بیندازیم.



- فهرست رابط های شبکه در دسترس کاربر (1): از این منو برای تعویض یا انتخاب یک رابط جدید هنگام ضبط بسته های شبکه استفاده می شود.
- نمایش گزینه های ضبط کردن (2): از این آیکون برای اجرای یک پانل کوچک به منظور سفارشی سازی تنظیمات ضبط بسته های شبکه استفاده می شود. برخی از این سفارشی سازی ها می تواند شامل موارد زیر شود.
 - تعویض نوع ضبط
 - تنظیم اندازهی بافر برای ضبط بسته ها
 - محدود سازی اندازه اطلاعات ضبط شده
 - مدیریت گزینه های نمایشی و تفکیک پذیری اسامی
- شروع یک ضبط زنده جدید (3): از این آیکون برای شروع یک ضبط جدید از رابط های انتخاب شده استفاده می شود.
- متوقف سازی ضبط زنده در حال اجرا (4): از این آیکون برای متوقف سازی فرآیند ضبط زنده بسته های شبکه استفاده می شود، تا بتوان بر روی بسته های ضبط شده تحلیل انجام داد.
- پیدا کردن یک بسته (5) : از این آیکون برای پیدا کردن یک متن، رشته یا پارامتر خاص در میان بسته های ضبط شده استفاده می شود.
- ویرایش فیلتر ضبط (6) : از این آیکون برای تغییر فیلتر های اعمال شده برای ضبط بسته های اطلاعات شبکه استفاده می شود. این ویژگی را در قسمت بعدی با جزئیات بیشتر مورد بررسی قرار خواهیم داد.

علاوه بر تمامی مباحث فوق الذکر، به جعبه فیلتر موجود در زیر آیکون های منو توجه کنید. از این جعبه برای اعمال فیلتر سریع بر روی بسته های شبکه ضبط شده استفاده می شود. به عنوان مثال، ما می توانیم تمامی بسته هایی که درخواست و پاسخ DNS داده اند را با تایپ کردن DNS در این جعبه مشاهده کنیم.

پانل های گرافیکی Wireshark

بگذارید حال به پانل های مختلف نمایش داده شده در Wireshark نگاهی بیندازیم. به طور معمول می توان پانل های Wireshark را به چهار قسمت : پانل ضبط¹، پانل جزئیات بسته ها²، پانل بایت های بسته ها³ و پانل وضعیت⁴ تقسیم کرد. تمامی این پانل ها را یکی یکی بررسی خواهیم کرد.

پانل ضبط

پانل ضبط، بسته های ضبط شده شبکه را به صورت سلسله مراتبی برای ما در معرض نمایش می گذارد. هر خط در این فهرست یک بسته مجزای ضبط شده شبکه را انعکاس می دهد. همچنین این پانل نمایشی، به صورت هوشمندانه اطلاعات را در سطر و ستون های تقسیم می کند که هر سطر در این فهرست یک بسته شبکه را نمایش می دهد در حالیکه ستون ها اطلاعات اضافی برای هر یک از بسته های ضبط شده به ما ارائه می دهند.

No.	Time	Source	Destination	Protocol	Length	Info
1	0.000000000	192.168.1.4	23.0.160.65	TCP	54	49260 > http [FIN, ACK] Seq=1 Ack=1 win=101
2	0.030888000	192.168.1.4	23.0.160.65	TCP	54	49262 > http [FIN, ACK] Seq=1 Ack=1 win=101
3	1.356718000	Vmware_9c:d3:95	CnetTech_d2:30:c0	ARP	42	who has 192.168.1.1? Tell 192.168.1.4
4	1.359220000	CnetTech_d2:30:c0	Vmware_9c:d3:95	ARP	60	192.168.1.1 is at 00:08:a1:d2:30:c0
5	1.410478000	fe80::18eb:7998:c25b:adbb	ff02::c	SSDP	208	M-SEARCH * HTTP/1.1
6	1.756746000	192.168.1.2	95.100.248.34	TCP	60	msfw-s-storage > http [FIN, ACK] Seq=1 Ack=
7	1.927535000	192.168.1.2	95.100.248.34	TCP	60	eyetv > http [FIN, ACK] Seq=1 Ack=1 win=160
8	2.197260000	192.168.1.2	95.100.248.34	TCP	60	msfw-storage > http [FIN, ACK] Seq=1 Ack=1
9	2.197265000	192.168.1.2	95.100.248.34	TCP	60	msfw-replica > http [FIN, ACK] Seq=1 Ack=1
10	2.236061000	AsustekC_2b:52:3f	CnetTech_d2:30:c0	ARP	60	who has 192.168.1.1? Tell 192.168.1.2
11	2.237121000	CnetTech_d2:30:c0	AsustekC_2b:52:3f	ARP	60	192.168.1.1 is at 00:08:a1:d2:30:c0
12	4.415710000	fe80::18eb:7998:c25b:adbb	ff02::c	SSDP	208	M-SEARCH * HTTP/1.1
13	4.492131000	192.168.1.4	23.0.160.65	TCP	54	[TCP Retransmission] 49260 > http [FIN, ACK]
14	4.602181000	192.168.1.4	23.0.160.65	TCP	54	[TCP Retransmission] 49262 > http [FIN, ACK]
15	7.200180000	192.168.1.2	95.100.248.34	TCP	60	[TCP Retransmission] msfw-s-storage > http
16	7.687359000	192.168.1.2	95.100.248.34	TCP	60	[TCP Retransmission] eyetv > http [FIN, ACK]
17	8.277428000	192.168.1.2	95.100.248.34	TCP	60	[TCP Retransmission] msfw-storage > http [F
18	8.277434000	192.168.1.2	95.100.248.34	TCP	60	[TCP Retransmission] msfw-replica > http [F
19	8.375532000	fe80::18eb:7998:c25b:adbb	ff02::c	SSDP	208	M-SEARCH * HTTP/1.1
20	11.376126000	fe80::18eb:7998:c25b:adbb	ff02::c	SSDP	208	M-SEARCH * HTTP/1.1
21	13.462741000	192.168.1.4	23.0.160.65	TCP	54	[TCP Retransmission] 49260 > http [FIN, ACK]
22	13.727712000	192.168.1.4	23.0.160.65	TCP	54	[TCP Retransmission] 49262 > http [FIN, ACK]
23	14.375836000	fe80::18eb:7998:c25b:adbb	ff02::c	SSDP	208	M-SEARCH * HTTP/1.1
24	15.509880000	fe80::18eb:7998:c25b:adbb	ff02::1:2	DHCPv6	150	Solicit XID: 0xac005d CID: 0001000118f52bcc
25	18.077970000	192.168.1.2	95.100.248.34	TCP	60	msfw-s-storage > http [RST, ACK] Seq=2 Ack=

تصویر : 3-1

اطلاعات اضافی ارائه شده توسط ستون ها به شرح زیر هستند:

- **No.** : این ستون عدد شماره بسته ها را ارائه می دهد که برای شناسایی یک بسته منحصر بفرد مفید مواقع می شود.
- **Time** : این ستون زمان ضبط شدن یک بسته را نمایش می دهد.

¹ Capture panel

² Packet details panel

³ Packet bytes panel

⁴ Status panel

- **Source** : این ستون آدرس های آی پی که بسته از آنجا می آید را نشان می دهد.
- **Destination** : این ستون آی پی آدرسی که بسته قصد دارد به آنجا برود را نمایش می دهد.
- **Protocol** : این گزینه نوع پروتکل استفاده شده توسط بسته را نمایش می دهد.
- **Length** : این ستون اندازه بسته ضبط شده را نمایش می دهد.
- **Info** : این ستون اطلاعات اضافی یک بسته را نمایش می دهد.

نکته : هر پروتکل منحصر بفرد در Wireshark با یک رنگ متفاوتی در پانل ضبط بسته ها نمایش داده می شود (تصویر 1-3 را مشاهده کنید). این قابلیت این امکان را به کاربر می دهد تا به سادگی میان پروتکل های استفاده شده توسط بسته ها تبعیض قائل شود. به عنوان مثال در خروجی نمایش داده شده در تصویر 1-3 بسته هایی که از پروتکل TCP استفاده کرده اند با رنگ مشکی و بسته هایی که از پروتکل ARP استفاده کرده اند با رنگ قهوه ای کم رنگ نمایش داده شده اند.

پانل مشخصات بسته

هنگامی که یک بسته داده را از پانل ضبط انتخاب می کنید، جزئیات اطلاعات آن در پانل جزئیات بسته نمایش داده می شود. شما می توانید محیط این پانل را در تصویر آورده شده زیر مشاهده کنید.

```

⊞ Frame 1: 54 bytes on wire (432 bits), 54 bytes captured (432 bits) on interface 0
⊞ Ethernet II, Src: Vmware_9c:d3:95 (00:0c:29:9c:d3:95), Dst: CnetTech_d2:30:c0 (00:08:a1:d2:30:c0)
⊞ Internet Protocol Version 4, Src: 192.168.1.4 (192.168.1.4), Dst: 23.0.160.65 (23.0.160.65)
⊞ Transmission Control Protocol, Src Port: 49260 (49260), Dst Port: http (80), Seq: 1, Ack: 1, Len: 0
  Source port: 49260 (49260)
  Destination port: http (80)
  [Stream index: 0]
  Sequence number: 1 (relative sequence number)
  Acknowledgment number: 1 (relative ack number)
  Header length: 20 bytes
  ⊞ Flags: 0x011 (FIN, ACK)
    Window size value: 1018
    [Calculated window size: 1018]
    [Window size scaling factor: -1 (unknown)]
  ⊞ Checksum: 0x7908 [validation disabled]

```

این پانل جزئیات پروتکل ها و پارامتر های مختلف مورد استفاده شده بسته را در سه ساختار مختلف نمایش می دهد که شما برای خواندن جزئیات آن ها کافیست بر روی + کلیک کنید تا اطلاعات آن ها نمایش داده شود. این اطلاعات می تواند برای شناسایی جرائم (forensics) بسیار مفید واقع شوند.

پانل بایت های بسته

این صفحه داده‌های بسته انتخاب شده را به شیوه hexdump نمایش می‌دهد که در آن offset داده‌های بسته در سمت چپ، داده‌های بسته در وسط به صورت هگزادسیمال و کاراکترهای اسکی معادل در سمت آن راست نشان داده می‌شود.

0000	00 08 a1 d2 30 c0 48 5b 39 2b 52 3f 08 00 45 000.H[9+R?...E.
0010	00 34 61 86 40 00 80 06 b9 3b c0 a8 01 02 ad c2	.4a.@... .;.....
0020	70 95 10 9d 01 bb a7 02 b4 ed fd b3 f1 c2 80 10	p.....
0030	fe 6f 5a 4c 00 00 01 01 05 0a fd b3 f3 a5 fd b3	.ozL....
0040	f4 31	.1

پانل وضعیت

پانل وضعیت، وضعیت جاری عملیات ما را نمایش می‌دهد. این پانل اطلاعاتی از قبیل وضعیت ضبط، شمارش بسته‌ها (بسته‌های ضبط شده، نمایش داده شده و نشانه گذاری شده) و محل ذخیره سازی بسته‌ها را نمایش می‌دهد.



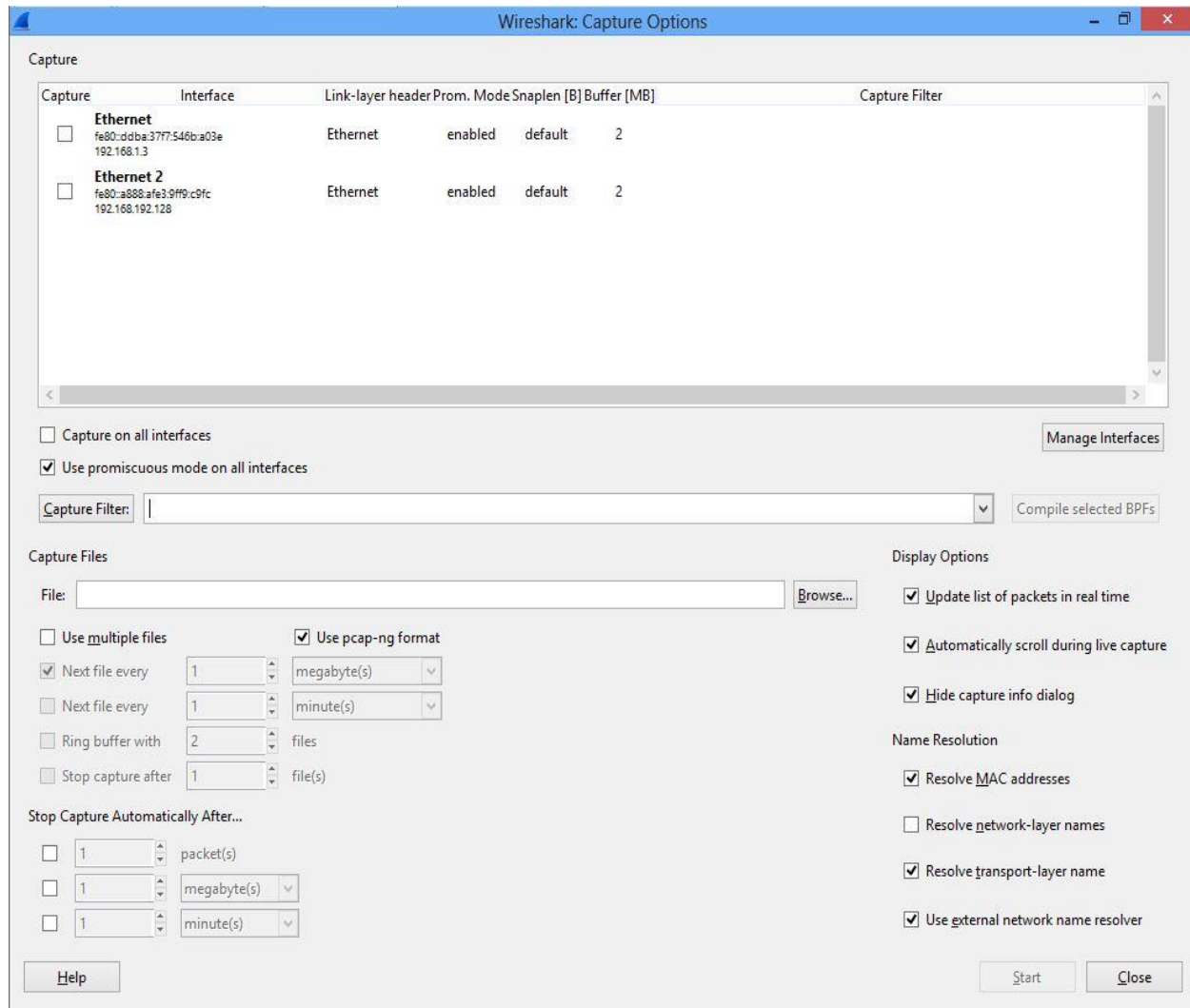
در این قسمت ما نگاهی به ویژگی‌های مهم موجود در رابط گرافیکی کاربر Wireshark انداختیم. حال در قسمت بعدی جنبه‌های تخصصی ضبط بسته‌های شبکه را مورد بحث قرار خواهیم داد.

تنظیم فیلترها¹

در اینجا ما تخصصی‌ترین و مفیدترین مبحث ضبط بسته‌های اطلاعاتی شبکه با استفاده از Wireshark را نشان خواهیم داد. فیلترها یک نقص کلیدی در ضبط بسته‌های اطلاعاتی شبکه دارند. هنگام کار کردن در یک شبکه محلی یا هنگام ضبط بسته‌های اطلاعاتی بر روی یک سرور که میزبان سرویس‌های بسیاری است، ممکن است با مشکلاتی برای برخی از بسته‌ها و سرویس‌ها رو به رو شویم، حال به منظور حذف این سربارها می‌توانیم از فیلترها استفاده کنیم. فیلترها را می‌توان در دو طرف اعمال کرد که نام آن‌ها فیلترهای ضبط و فیلترهای نمایش است. بگذارید تشریح این قسمت را با فیلترهای ضبط شروع کنیم.

¹ Setting up filters

فیلتر های ضبط¹ برای دیدهبانی بسته های انتخابی² به کار گرفته می شوند. این فیلتر ها می توانند فقط ترافیکی را که ما می خواهیم مورد شلر قرار دهند. به منظور انجام ضبط انتخابی ما باید دستورالعمل های winpcap را به wireshark عبور دهیم. تنظیمات فیلتر ضبط می تواند با کلیک کردن بر روی آیکون Edit Capture Filter در منو اجرا شود. با این حال بجای کلیک بر روی این آیکون، می توانید با رفتن به منوی Capture و سپس کلیک کردن بر روی گزینه Options پنجره تنظیمات فیلر بسته ها را اجرا کنید. پس از این عملیات پنجره ای به شکل زیر برایتان باز خواهد شد.



در پنجره تنظیمات فیلتر ها، می توانیم تنظیمات فیلتر خودمان را با پر کردن فیلد Capture Filter اعمال نمائیم. همچنین می توانیم با کلیک کردن بر روی دکمه Capture Filter قوانین فیلتر کردن خود را برای استفاده های بعدی

¹ Capture filters

² Packets Selectively

ذخیره سازی کنیم. اما سوال فعلی این است، چگونه می توانیم یک قاعده دستوری برای فیلتر بسته های شبکه بنویسیم؟ قوانین Winpcap برای ضبط بسته های شبکه از الگوی آورده شده در خروجی 1-3 پیروی می کند. این الگوی یک ساختمان ساده از نحوه نوشتن قواعد فیلترینگ برای Wireshark را شامل شده است.

<Protocol name><Direction><Host(s)><Value><Logical operations><Expressions>

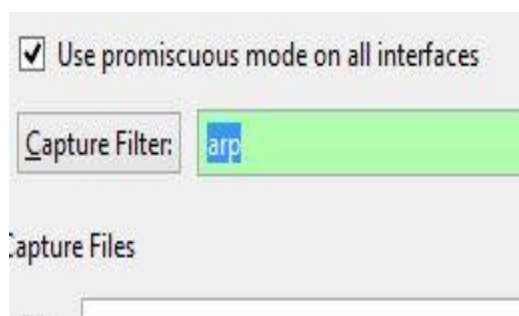
خروجی 1-3 : الگو تعریف قانون فیلتر کردن بسته در Wireshark

به عنوان مثال به منظور فیلتر کردن بسته های TCP هنگامی که درگاه منبع آن ها 443 است می توانیم قاعده دستوری¹ زیر را بنویسیم.

tcp src port 443

مثال 1 : مشابه دستور قبلی برای دیدن بسته های Arp می توانید در فیلد ضبط (Capture Filter) فقط دستور Arp را وارد کنید، تا تمامی بسته های Arp ترافیک شبکه فقط ضبط شوند. دستور زیر را در فیلد Capture Filter وارد کرده و خروجی را مشاهده کنید.

arp



پس از وارد کردن این فیلتر و کلیک کردن بر روی گزینه Start برنامه Wireshark فقط بسته های ARP ترافیک را ضبط کرده و در خروجی برای شما به نمایش می گذارد.

¹ rule

Filter:

▼ Expression... Clear Apply Save

No.	Time	Source	Destination	Protocol	Length	Info
1	0.000000000	AsustekC_2b:52:3f	CnetTech_d2:30:c0	ARP	60	who has 192.168.1.1? Tell 192.1
2	0.001025000	CnetTech_d2:30:c0	AsustekC_2b:52:3f	ARP	60	192.168.1.1 is at 00:08:a1:d2:30

<

⊞ Frame 1: 60 bytes on wire (480 bits), 60 bytes captured (480 bits) on interface 0

⊞ Ethernet II, Src: AsustekC_2b:52:3f (48:5b:39:2b:52:3f), Dst: CnetTech_d2:30:c0 (00:08:a1:d2:30:c0)

⊞ Address Resolution Protocol (request)

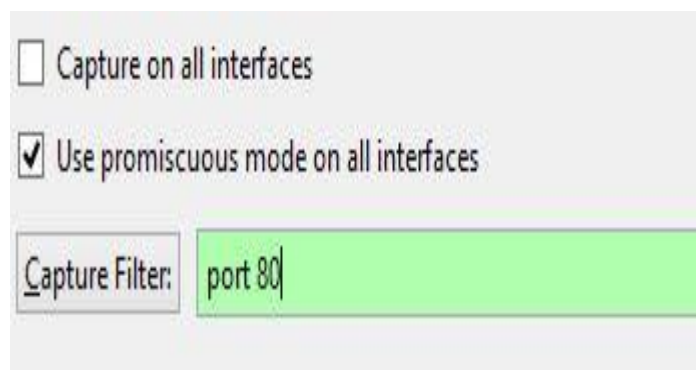
0000000800a1d230c0485b392b523f08060001.....0.H[9+R?....

0010080006040001485b392b523fc0a80102.....H[9+R?....

00200008a1d230c0c0a80101000000000000.....0...

00300000000000000000000000000000.....

مثال 2 : به منظور ضبط ترافیک ورودی و خروجی از درگاه 80 می توانید قاعده دستوری port 80 را در فیلد Capture Filter وارد کنید تا تمامی ترافیک Http برای شما به نمایش گذاشته شود.



پس از وارد کردن این فیلتر و کلیک کردن بر روی گزینه Start برنامه Wireshark فقط بسته های Http ترافیک را ضبط کرده و در خروجی برای شما به نمایش می گذارد.

No.	Time	Source	Destination	Protocol	Length	Info
890	8.088401000	192.168.1.2	23.21.76.43	TCP	60	12364 > http [ACK] Seq=503 Ack=378 Win=63864
891	8.089716000	23.21.76.43	192.168.1.2	HTTP	442	[TCP Out-of-Order] HTTP/1.1 403 Forbidden
892	8.089720000	192.168.1.2	23.21.76.43	TCP	66	[TCP Dup ACK 890#1] 12364 > http [ACK] Seq=503
893	8.089722000	192.168.1.2	23.21.76.43	TCP	60	12364 > http [FIN, ACK] Seq=503 Ack=378 Win=63864
894	8.091363000	23.21.76.43	192.168.1.2	TCP	66	http > 12364 [RST] Seq=1828601522 win=6912 Len=0
895	8.091712000	23.21.76.43	192.168.1.2	TCP	66	http > 12364 [RST] Seq=1828601522 win=6912 Len=0
896	8.091715000	23.21.76.43	192.168.1.2	TCP	66	http > 12364 [RST] Seq=1828601522 win=6912 Len=0
897	8.437836000	192.168.1.3	193.219.221.8	TCP	66	49392 > http [SYN] Seq=0 Win=65535 Len=0 MSS=65535
898	8.620901000	192.168.1.3	23.50.129.224	TCP	54	[TCP Retransmission] 49382 > http [FIN, ACK] Seq=49382
899	8.682875000	192.168.1.3	23.50.129.224	TCP	54	[TCP Retransmission] 49381 > http [FIN, ACK] Seq=49381
900	8.761826000	192.168.1.2	2.17.106.156	TCP	60	[TCP Retransmission] 12356 > http [FIN, ACK] Seq=12356
901	8.811856000	192.168.1.2	23.21.76.43	TCP	60	[TCP Retransmission] 12364 > http [FIN, ACK] Seq=12364
902	8.822555000	192.168.1.2	2.17.106.156	TCP	60	[TCP Retransmission] 12325 > http [FIN, ACK] Seq=12325
903	9.135910000	192.168.1.3	193.219.209.103	TCP	62	[TCP Retransmission] 49373 > http [SYN] Seq=0

Frame 1: 66 bytes on wire (528 bits), 66 bytes captured (528 bits) on interface 0	
Ethernet II, Src: AsustekC_2b:52:3f (48:5b:39:2b:52:3f), Dst: CnetTech_d2:30:c0 (00:08:a1:d2:30:c0)	
Internet Protocol Version 4, Src: 192.168.1.2 (192.168.1.2), Dst: 213.199.181.12 (213.199.181.12)	
Transmission Control Protocol, Src Port: 12319 (12319), Dst Port: http (80), Seq: 0, Len: 0	

0000	00 08 a1 d2 30 c0 48 5b 39 2b 52 3f 08 00 45 000.H[9+R?..E.
0010	00 34 7d 61 40 00 80 06 30 e4 c0 a8 01 02 d5 c7	.4}a@... 0.....
0020	b5 0c 30 1f 00 50 08 d8 21 a2 00 00 00 00 80 02	..0..P.. !.....
0030	fa f0 cc bd 00 00 02 04 05 b4 01 03 03 02 01 01
0040	04 02	..

مثال 3 : همچنین شما می توانید به منظور ضبط ترافیک ورودی از یک منبع خاص مانند 192.168.15.20 و درگاه 223 قاعده دستوری زیر را در Capture Filter اعمال کنید تا تمامی ترافیک ورودی از آن آدرس را Wireshark ضبط کرده و برای شما به نمایش بگذارد.

src 192.168.15.20 port 232

با این حال ما می توانیم قواعد دستوری (Rules) مختلفی را با هم دیگر به منظور فیلتر کردن جریان ضبط ترافیک مورد استفاده قرار بدهیم، همچنین به این نکته توجه داشته باشید، اگر ما در ضبط بسته های ترافیک شبکه هیچ فیلتری در برنامه Wireshark تعریف نکنیم، برنامه Wireshark به صورت پیش فرض تمامی بسته های ورودی و خروجی شبکه را ضبط می کند.

نکته : توجه کنید، اگر شما در پنجره تعریف فیلتر در فیلد Capture Filter قواعد دستوری فیلتر کردن را به شکل اشتباهی برای فیلتر کردن بسته های اطلاعاتی شبکه وارد کنید، رنگ پس زمینه فیلد Capture Filter به رنگ قرمز در می آید و اگر دستورالعمل را به شکل صحیح وارد کنید، رنگ پس زمینه آن به رنگ سبز در می آید.

گزینه بعدی، فیلتر نمایشی¹ است. از این گزینه برای اعمال فیلتر بر روی بسته های ضبط شده استفاده می شود. برخلاف فیلتر های ضبط بسته، فیلتر های نمایشی می توانند حتی پس از اینکه بسته ها ضبط شدند بر روی خروجی فهرست بسته های ضبط شده اعمال گردند. به منظور اجرای پنجره فیلتر نمایشی می توانید بر روی آیکون Edit/Apply Display filter در منوی آیکون های برنامه کلیک کنید، یا بجای آن با رفتن به منوی Analyze و کلیک کردن بر روی گزینه Display Filters پنجره مرتبط با آن را اجرا کنید. همچنین فیلتر های نمایشی از ساختار ثابت زیر به منظور تعریف فیلتر پیروی می کنند.

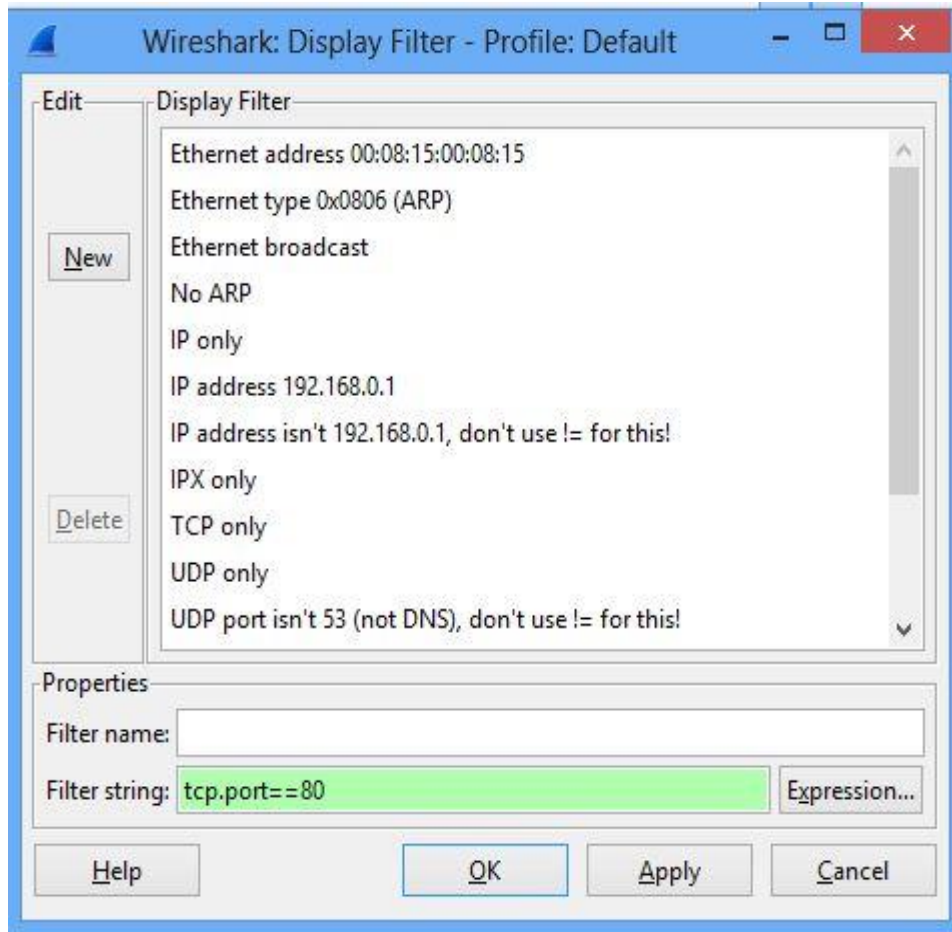
<Protocol> . <String 1> . <String 2> . <Comparison Operator><Value><Logical operators><Expressions>

خب حال اجازه بدهید برای به کارگیری این ساختار به منظور اعمال فیلتر بر روی بسته های ضبط شده، چندین مثال برای درک بیشتر بزنیم.

مثال 1 : در این قسمت به منظور مشاهده کردن بسته های TCP ضبط شده از درگاه 80 فیلتر زیر را اعمال کنید.

tcp.port==80

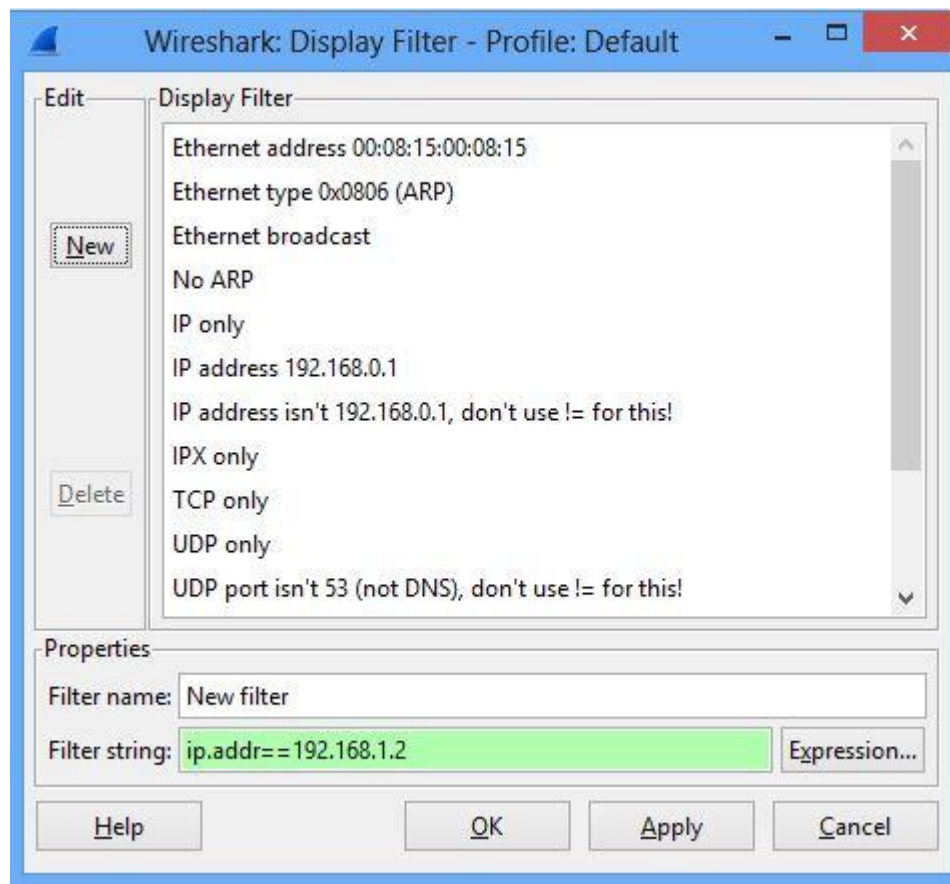
¹ Display Filter



پس از وارد کردن فیلتر و کلیک کردن بر روی دکمه Apply تمامی بسته هایی که از درگاه 80 پروتکل TCP استفاده کرده اند در خروجی برای شما نمایش داده خواهند شد.

مثال 2 : برای مشاهده بسته هایی ارسالی یا دریافتی از یک آی پی آدرس خاص کافست دستور زیر را در فیلد Filter string وارد کنید تا تمامی بسته های آن در خروجی برای شما به نمایش گذاشته شود. به عنوان مثال ما در این مثال قصد داریم بسته های اطلاعاتی ارسالی و دریافتی از آی پی آدرس 192.168.1.2 را مشاهده کنیم. بدین منظور دستور زیر را اعمال می نمائیم.

ip.addr==192.168.1.2

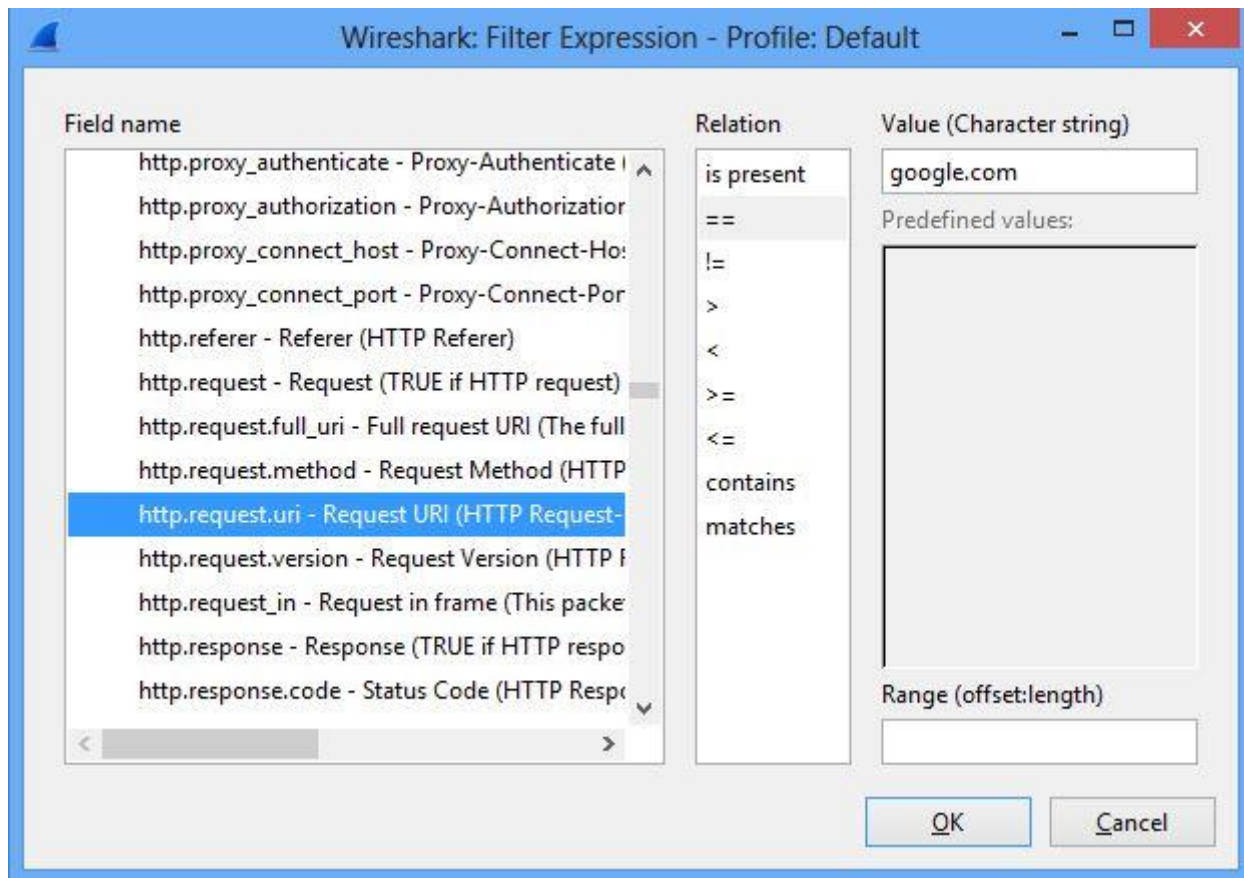


تصویر 2-3

پس از وارد کردن فیلتر و کلیک کردن بر روی دکمه Apply تمامی بسته هایی که از آدرس 192.168.1.2 استفاده کرده اند در خروجی برای شما نمایش داده خواهند شد. حال که قسمت سخت فیلترهای بسته های شبکه را نمایش دادیم، دریاچه یک راه سریع و آسان برای انجام هر دو گزینه فیلتر کردن بحث خواهیم کرد.

کار با جعبه محاوره ای Filter Expression

پنجره محاوره ای Filter Expression یک ویژگی است، که کار افراد مبتدی در استفاده از Wireshark را برای ایجاد، ضبط و نمایش فیلترها آسان می کند. این پنجره با کلیک کردن بر روی دکمه Expression در پنجره محاوره ای Display Filter که در تصویر 2-3 آن را مشاهده می کنید.



تصویر 3-3

با استفاده از این روش ما می توانیم به راحتی فیلتر صفحه نمایش و یا فیلتر ضبط ایجاد کنیم. این پنجره محاوره ای گزینه های متعددی همراه با برخی از عبارات از پیش بارگذاری شده به ما ارائه می کند. برای ایجاد یک عبارت می توانید گام های زیر را دنبال کنید.

1. به منظور تعریف یک فیلتر برای یک پروتکل خاص، با کلیک کردن بر روی علامت مثبت کنار نام پروتکل آن را گسترش داده و سپس یک فیلد خاص را انتخاب کنید.
2. هنگامی که معیار مد نظر خود را پیدا کردید با کلیک کردن بر روی گزینه های برابر(==) و بزرگتر از (>) آن را برای ایجاد یک عبارت فیلتر انتخاب کنید.
3. سپس به منظور دادن یک مقدار برای فیلتر، می توانید مقدار مد نظر خود را در قسمت Value وارد کنید (به عنوان مثال، در اینجا یک فیلتر برای پروتکل Http تعریف کردیم که مقدار آن را برابر با گوگل قرار دادیم. بدین منظور که تمامی بسته های Http درخواستی از google.com را برای ما فیلتر کند) با این حال ما می توانستیم مثال بالا را با دستور http.request.uri==google.com در قسمت تعریف فیلتر اعمال

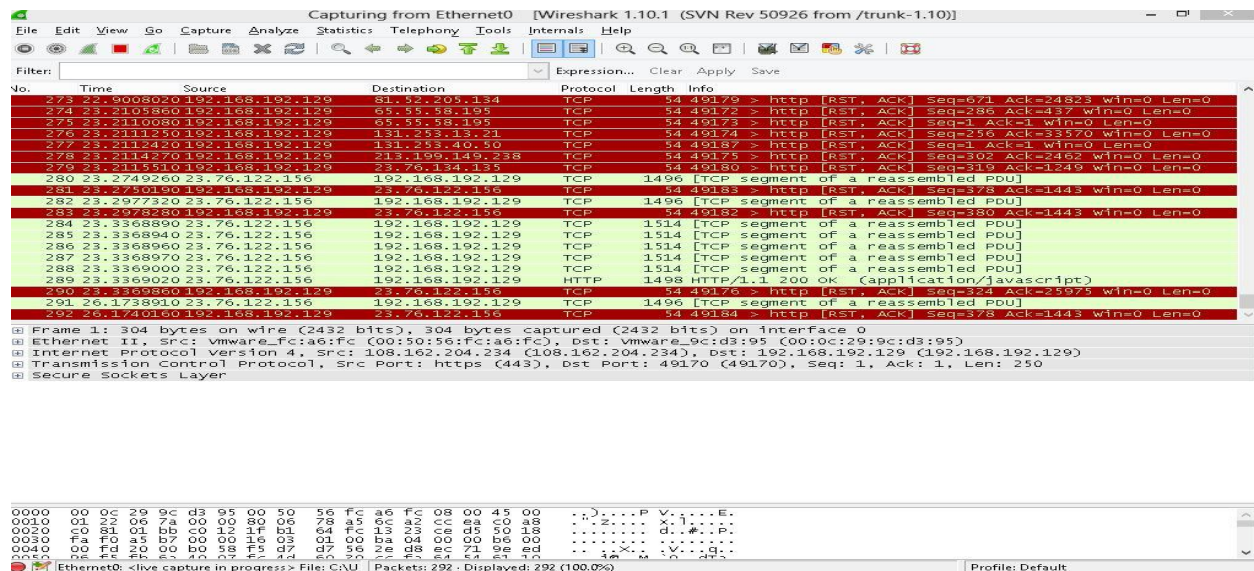
کنیم. این یک نمونه مثال ساده از نحوه استفاده کردن از Filter Expression بود. در قسمت بعدی ما شروع به کار کردن با اولین بسته ضبط شده خود خواهیم کرد.

ضبط زنده اطلاعات

حال که ما به اندازه کافی اطلاعات پایه درباره برنامه Wireshark داریم، می توانیم به منظور ضبط بسته های شبکه کار خود را آغاز کنیم. در این مثال، ما به نحوه ضبط بسته های شبکه با استفاده از wireshark نگاهی خواهیم انداخت. به هر حال برای ضبط بسته های اطلاعاتی در برنامه Wireshark گام های ساده آورده شده در زیر را دنبال کنید.

1. در گام اول برنامه Wireshark را اجرا کنید.
2. سپس یک فیلتر که مدنظرتان هست را اعمال کرده.
3. و در گام پایانی؛ یک رابط شبکه را به منظور ضبط بسته های اطلاعاتی انتخاب کنید.

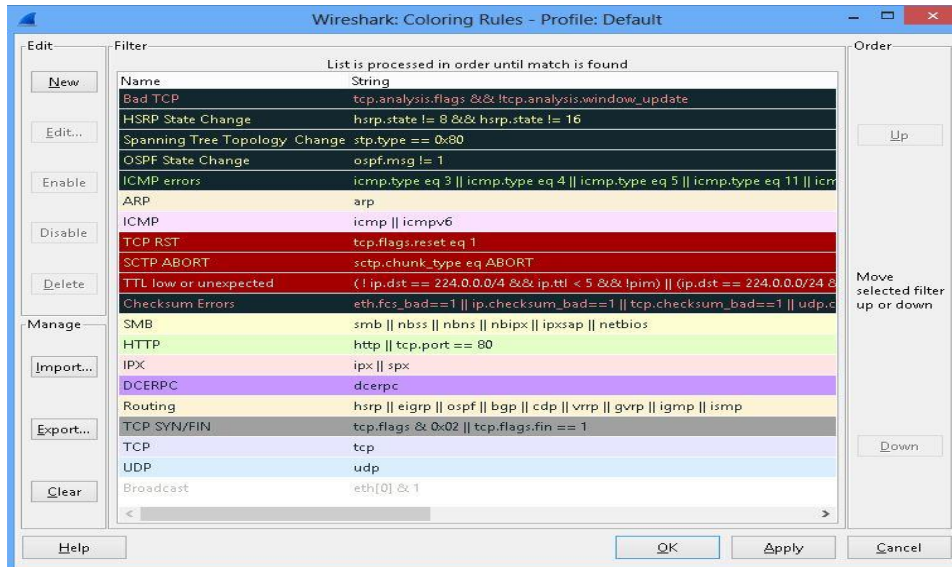
وقتی که رابط شبکه را انتخاب کردید، متوجه خواهید شد که برنامه شروع به ضبط بسته های شبکه خواهد کرد و تمامی بسته های ضبط شده را در پانل اصلی برنامه به نمایش خواهد گذاشت.



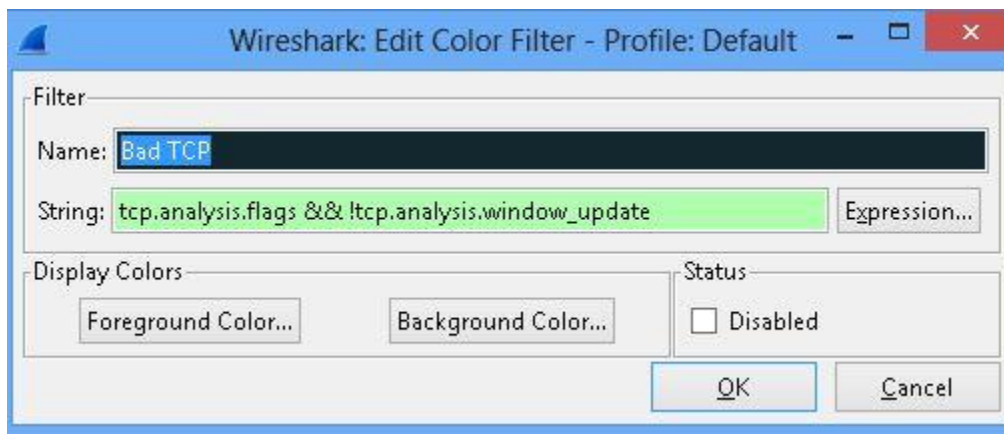
با این حال در هر زمان شما می توانید فرآیند ضبط بسته های شبکه را با کلیک کردن بر روی آیکن Stop متوقف سازید. همچنین برای شروع مجدد ضبط بسته های شبکه می توانید بر روی آیکن Restart the running live capture کلیک کنید. به نکته هم توجه داشته باشید، پس از اینکه بر روی آیکن Restart کلیک کردید، تمامی بسته های ضبط شده از صفحه اصلی برنامه Wireshark پاک خواهد شد.

آشنایی با رنگ آمیزی بسته ها توسط Wireshark

به احتمال زیاد تا به الان متوجه شدید که برنامه Wireshark برای نمایش بسته های اطلاعاتی پروتکل های گوناگون از رنگ های مختلفی استفاده می کند. در هر حال برای مشاهده نحوه رنگ بندی پروتکل ها می توانید بر روی آیکون Edit coloring rules کلیک کنید تا تنظیمات پیکربندی آن برای شما به نمایش گذاشته شود.



همانطور که در تصویر آورده شده در بالا مشاهده می کنید، از الگو های مختلف رنگ بندی پیش فرض برای نمایش پروتکل ها، خطا ها، خرابی ها و... در برنامه Wireshark استفاده شده است. همچنین طرح های پیش فرض می توانند با کلیک کردن بر روی دکمه Edit توسط کاربر تغییر یابند. به عنوان مثال برای تغییر رنگ بسته های Bad TCP کافیست آن را انتخاب کنید، سپس بر روی دکمه Edit کلیک کنید تا صفحه تنظیمات آن برای شما به نمایش گذاشته شود.



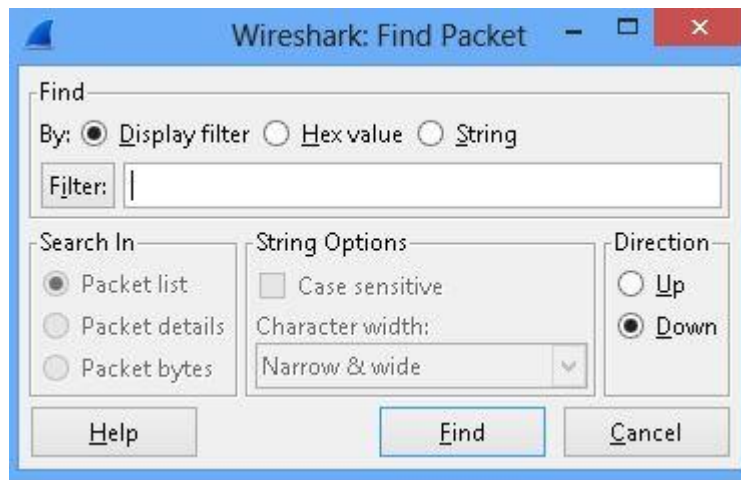
پس از نمایش این صفحه شما می توانید به راحتی رنگ پس زمینه، رنگ پیش زمینه، نام نمایشی پروتکل و الگوی رشته آن را تغییر بدهید.

کار با بسته های اطلاعاتی ضبط شده

دلیل اصلی ضبط بسته های اطلاعاتی شبکه تحلیل فعالیت های شبکه ای است. بسته های ضبط شده می توانند بسیار دقیق توسط Wireshark مورد تحلیل قرار گیرند. حال بگذارید فرآیند ضبط بسته های شبکه را متوقف سازیم و سپس شروع به تحلیل بسته های ضبط شده کنیم.

جستجو برای بسته ها

به منظور جستجوی اطلاعاتی خاص می توانید به منوی Edit رفته و بر روی گزینه Find Packets کلیک کنید یا کلید های ترکیبی Ctrl + F را بفشارید. پس از انجام این عمل پنجره ای با سه گزینه متفاوت با نام های Display filter، Hex value و String برای شما به نمایش گذاشته خواهد شد.



1. گزینه Display Filter به ما اجازه می دهد یک عبارت مانند فیلترهای نمایشی وارد کنیم تا فقط بسته ای که با آن فیلتر مطابقت دارد را در بین بسته های ضبط شده برای ما پیدا کند.
2. گزینه Hex Value برای پیدا کردن یک عدد سلسله مراتبی هکسادیسمال استفاده می شود.
3. گزینه جستجو String به ما اجازه می دهد به دنبال یک رشته خاص بگردیم. جستجو کردن رشته های خاص یک دیگر از گزینه های فعالی است که در قسمت Search in در پنجره Find Packet لیست شده است. برای جستجوی یک رشته مخصوص بین بسته های ضبط شده، می توانیم گزینه Packet list را انتخاب کنیم و همچنین به منظور دنبال کردن یک رشته مخصوص در سر آیند بسته ها می توانیم از گزینه Packet

bytes استفاده کنیم. و در پایان برای جستجو یک رشته خاص در میان داده های شامل شده یک بسته، می توانیم از گزینه Packet details استفاده کنیم.

علامت گذاری بسته ها

علامت گذاری بسته های مهم می تواند در سرعت بازبایی اطلاعات مورد نیاز ما بسیار مفید است. همچنین می تواند برای پیگیری بسته های مهم در یک لیست بسیار بزرگ از داده های ضبط شده مفید واقع شود. برای علامت گذاری هر بسته، بر روی آن راست کلیک کنید و گزینه Mark Packet(toggle) را انتخاب کنید. پس از علامت گذاری بسته رنگ پس زمینه آن به رنگ مشکی تغییر می یابد.

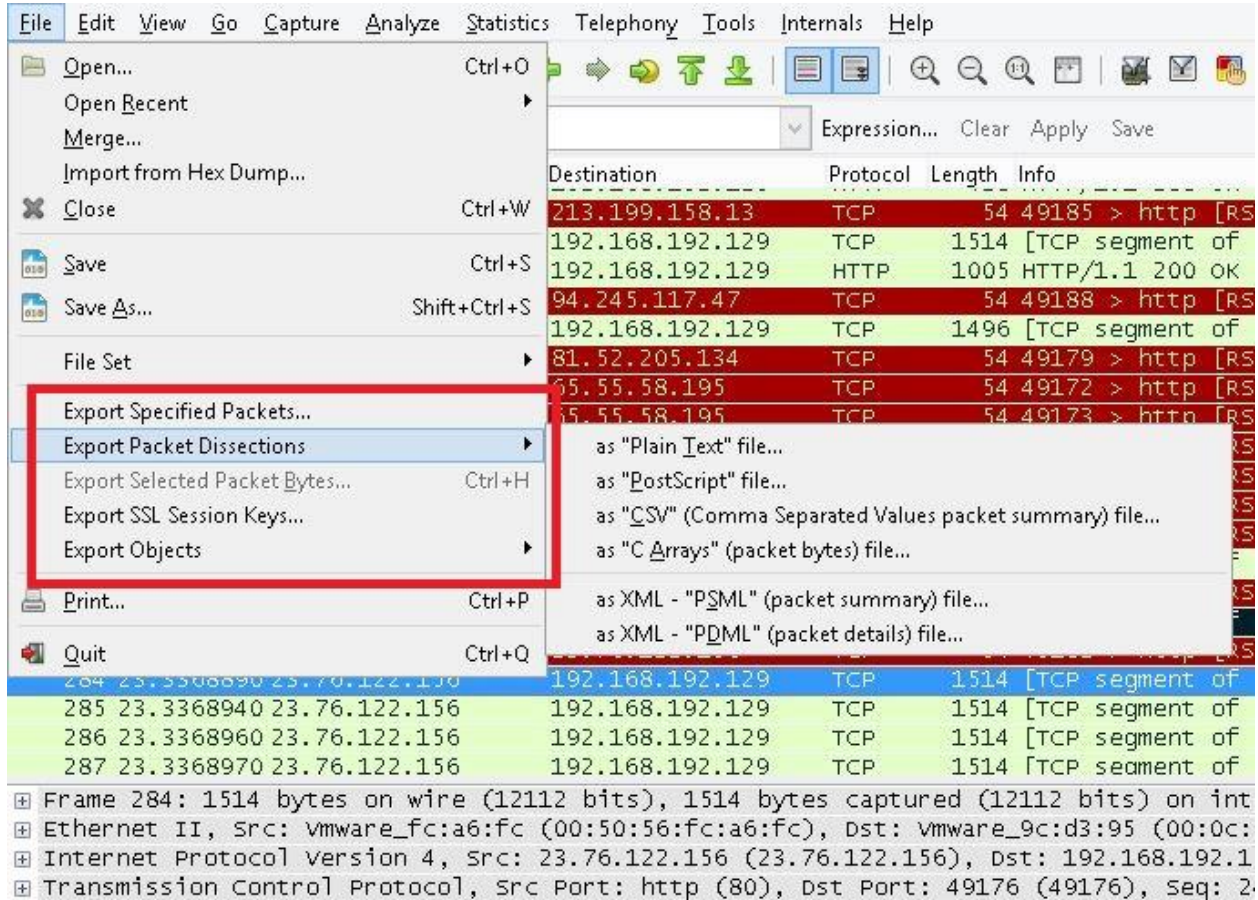
The screenshot displays the Wireshark network protocol analyzer interface. The packet list pane on the left shows a list of captured packets. Packet 284 is selected, and a right-click context menu is open over it. The menu includes options for marking, ignoring, and setting time reference for the packet, as well as options for following the stream, copying, and decoding. The packet details pane on the right shows the hierarchical structure of the selected packet, including Ethernet II, Internet Protocol version 4, and Transmission Control Protocol. The packet bytes pane at the bottom shows the raw data of the packet in hexadecimal and ASCII.

ذخیره سازی داده های ضبط شده

برای ذخیره سازی داده های ضبط شده به منوی File رفته و بر روی گزینه Save As کلیک کنید. در این قسمت می توانیم تمامی بسته های ضبط شده را به سادگی ذخیره سازی کنیم یا می توانیم ابتدا فیلتری اعمال کرده و فقط بسته های انتخابی خود را ذخیره سازی کنیم. همچنین برنامه Wireshark از قالب های مختلف ضبط بسته ها، از قبیل pcap، pcapng، و pcap پشتیبانی می کند.

صدور و ادغام بسته ها¹

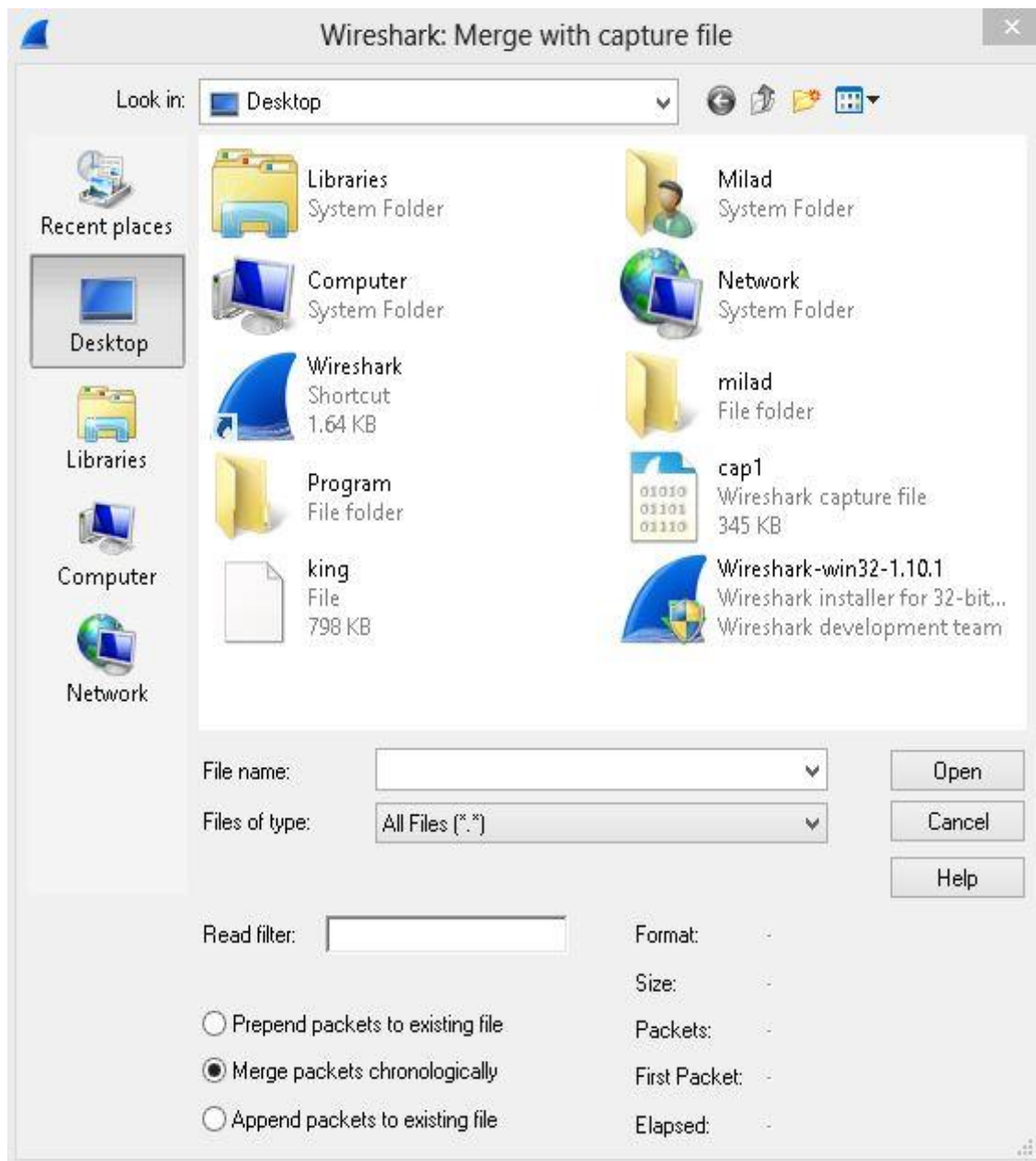
همچنین برنامه Wireshark به شما اجازه می دهد بسته های ضبط شده را با قالب های گوناگون از قبیل txt، csv، xml صادر کنید. این ویژگی هنگامی مفید است که داده ها در عملیات دیگر مورد استفاده قرار گیرند. برای صدور بسته ها در قالب های گوناگون می توانید به منوی File بروید و بر روی هر یک از گزینه های Exort که مد نظرتان هست کلیک کنید تا خروجی مد نظرتان تولید شود.



برنامه Wireshark قابلیت ادغام کردن فایل های مختلف ضبط شده با هم دیگر را ارائه می دهد. برای ادغام یک فایل ضبط شده، می توانید گام ها آورده شده در زیر را دنبال کنید.

1. فایلی را که می خواهید آن را ادغام کنید را باز کنید.
2. سپس به منوی File بروید و گزینه Merge را انتخاب کنید تا پنجره Merge with capture File نمایش داده شود.

¹ Exporting and merging packets



3. سپس فایلی را که می خواهید آن را با فایل باز کرده خود ادغام کنید را انتخاب کرده و سپس یک روش برای ادغام آن ها انتخاب کنید. شما می توانید فایل انتخاب شده را به فایلی که هم اکنون باز است، اضافه کنید¹ و یا آن ها را بر حسب برچسب زمانی² خود ادغام کنید.

¹ Append packet

² Merge packets chronologically

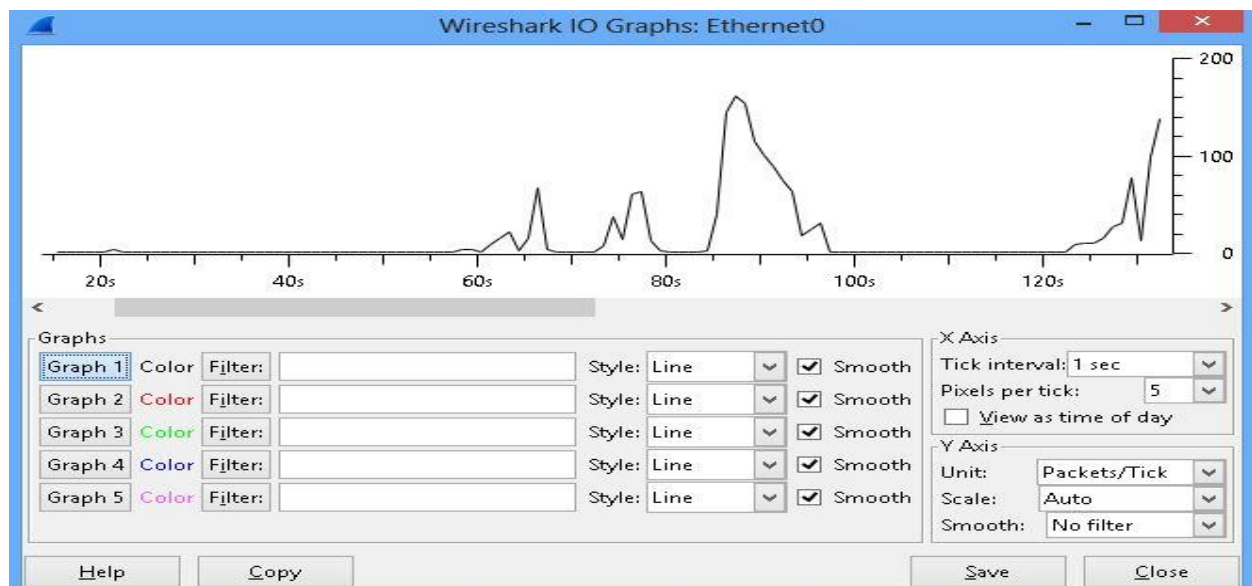
چاپ بسته های

برنامه Wireshark اجازه می دهد بسته های ضبط شده را در قالب یک فایل متنی، اسکریپت، یا یک خروجی مبتنی بر انتخاب شما چاپ کند. همچنین این برنامه اجازه می دهد محدوده مشخصی از شماره بسته های ضبط شده را انتخاب کنید و سپس آن محدوده را چاپ کنید. بدین منظور به منوی File رفته و بر روی print کلیک کنید تا پنجره چاپ نمایش داده شود. این یک نمایش ساده از چگونگی کار کردن با بسته های ضبط شده به منظور افزایش بهره وری از برنامه Wireshark بود. در قسمت بعد، ما بر روی برخی دیگر از ویژگی های کمتر شناخته شده برنامه Wireshark که می تواند در طی کالبدشکافی بسته ها و آزمایش نفوذپذیری شبکه مفید واقع شود تمرکز خواهیم کرد.

نکته : همچنین شما می توانید با دوبار کلیک کردن بر روی هر بسته ضبط شده اطلاعات آن را در یک پنجره مجزا دیگه به صورت کامل مشاهده و تحلیل کنید.

پنجره گراف ورودی و خروجی

برنامه Wireshark همچنین یک ویژگی فوق العاده برای مرور بسته های ضبط شده به صورت گرافیکی است. این ویژگی می تواند در نظارت بر مقدار جریان داده ها در سراسر شبکه مفید واقع شود. تجزیه و تحلیل گرافیکی همچنین می تواند در تجزیه و تحلیل مقادیر زیادی از داده ها مفید باشد. با این حال به منظور تولید یک نمایش گرافیکی از بسته های ضبط شده می توانید به منوی Statistics رفته و بر روی گزینه IO Graph کلیک کنید.



عملیات های گوناگونی وجود دارد که می توان با این گراف انجام داد.

گراف ها¹ : ما می توانیم پنج نمودار مقایسه مختلف را فعال سازیم و آنها را با رنگ بندی مختلف برای مشاهده آسان تر ارائه دهیم.

فیلتر : ما همچنین می توانیم از بسته های تجزیه و تحلیل خود برای ایجاد یک نمودار خاص استفاده کنیم. بدین منظور کافیست بر روی Filter کلیک کنید، تا پنجره ای اعمال فیلتر نمایش داده شود. سپس یک فیلتر اعمال کنید تا گراف آن بسته ها برای شما به نمایش گذاشته شود.

مدل گراف: مدل گراف می تواند يك از انواع Line ، Impulse ، Fbar یا Dot باشد.

نمودار مختصات

محور X

1. فاصله ی علامت²
2. تعداد پیکسل های هر علامت³: می توان از 1/2/5/10 پیکسل برای هر علامت استفاده کرد.
3. مشاهده به صورت زمان روز⁴: می توان محور x را به صورت روز به جای ثانیه یا دقیقه برچسب گذاری کرد.

محور Y

1. واحد⁵ محور y که می تواند به صورت Packets/Tick ، Bytes/Tick ، Bits/Tick ، Advanced و... باشد.
2. مقیاس⁶ محور (Logarithmic, Auto, 10, 20, 50, 100 و غیره)

اطلاعات تخصصی

اطلاعات تخصصی یکی دیگر از ویژگی های قدرتمند Wireshark است که شخص متخصص می تواند با استناد به آن هرگونه ناهنجاری که در ضبط بسته ها رخ می دهد را پیگیری کند. این ویژگی رویداد های ثبت شده تمامی

¹ Graphs

² Tick interval

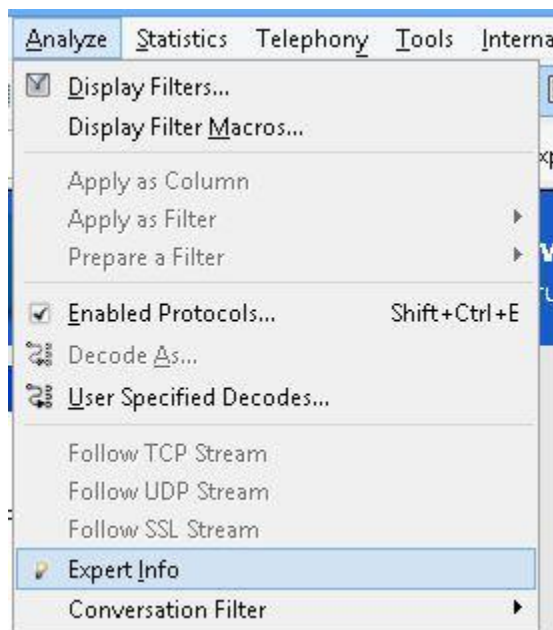
³ Pixels per tick

⁴ View as time of day

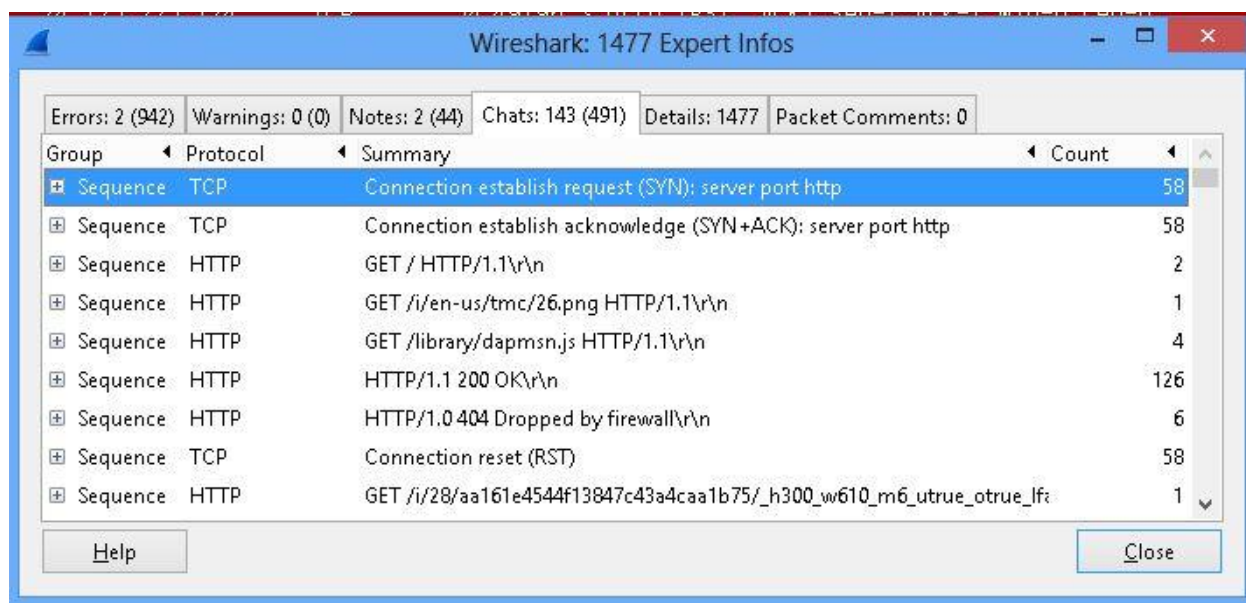
⁵ Unit

⁶ Scale

بسته ها را نگه می دارد و یک تحلیل تقریباً هوشمند ارائه می دهد. اطلاعات آن شامل گزارش دادن، خطاها، خرابی ها، پروتکل و... می شود. به منظور اجرا پنجره محاوره ای Expert Info به منوی Analyze بروید و بر روی Expert info Composite کلیک کنید.



پس از کلیک کردن بر روی گزینه Expert Info صفحه ای به شکل زیر برای شما به نمایش گذاشته می شود.

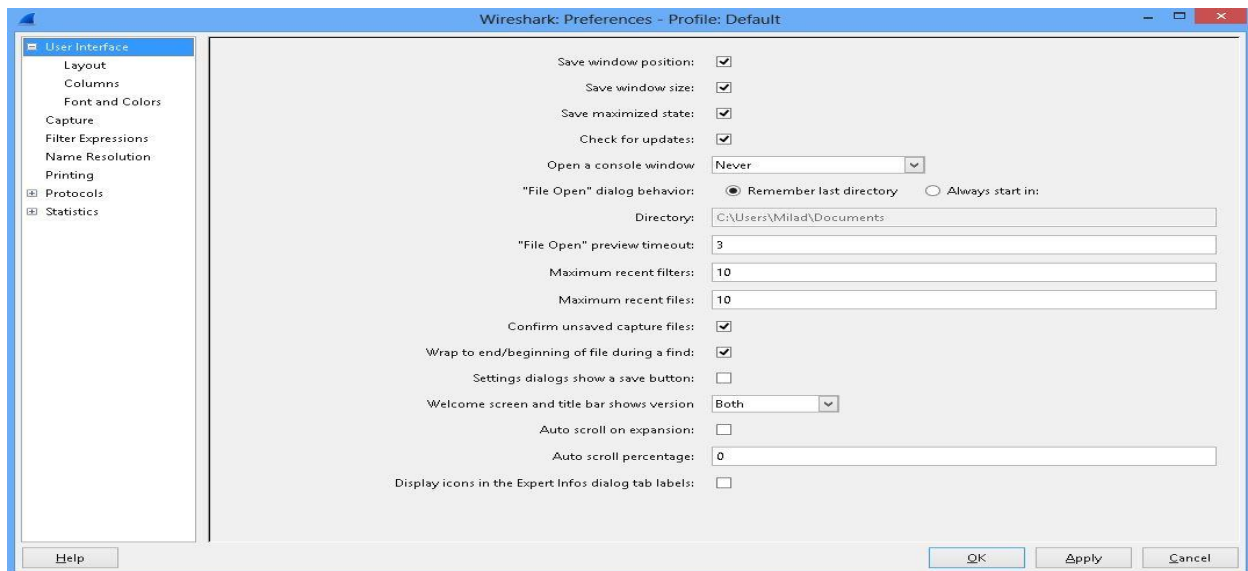


همانطور که در تصویر بالا مشاهده می کنید پنجره محاوره ای اطلاعات تخصصی شامل پنج تب می شود که هر کدام از آنها را به صورت مجزا تشریح خواهیم کرد.

1. **خطا ها (Errors) :** این تب تمامی خطاهایی که در حین ضبط بسته های شبکه رخ داده است را گزارش می دهد.
 2. **هشدار ها (Warnings):** این تب اطلاعات هشداردهنده مانند خطای تقسیم بندی و بسته های خارج از نظم را ارائه می دهد.
 3. **یادداشت ها (Notes):** این تب اطلاعات تقریبی درباره بسته های تکراری، مسائل پروتکل ها و ... ارائه می دهد.
 4. **ارتباطات (Chats):** این تب به ما اطلاعاتی درباره فراخوانی های ارتباطی از قبیل درخواست های TCP GET و فراخوانی برنامه های کاربردی را ارائه می دهد.
- هر کدام از زبانه ها (تب ها) که در قسمت گذشته مورد بحث قرار گرفت، یک جدول جداگانه است که اطلاعات موجود در آن تب یا زبانه را نمایش می دهد. هرکدام از این زبانه ها شامل چهار ستون با نام های Group، Protocol، Summary و Count می شود. بگذارید این چهار ستون را به صورت خلاصه تشریح کنیم.
1. **ستون Group :** این ستون به ما می گوید که اطلاعات بر اساس چه موضوعی طبقه بندی شده اند. طبقه بندی ها مختلف شامل checksum، sequence و request/response code می شود.
 2. **ستون Protocol :** این ستون پروتکل را نشان می دهد.
 3. **ستون Summary :** این ستون اطلاعات مختصر ارائه می دهد.
 4. **ستون Count :** این ستون موقعیت بسته را در کل فایل نمایش می دهد.
- این یک نمایش ساده از نحوه استفاده از Expert Info برای تحلیل بهتر شبکه بود. اما این تنها راه برای تجزیه و تحلیل شبکه نیست که برنامه Wireshark ارائه می دهد. همچنین ما می توانیم این اطلاعات را به صورت مستقیم در پانل ضبط مشاهده کنیم. برای اضافه این ستون ما می توانیم به منوی Preferences برویم. بگذارید این مبحث را در قسمت بعد مورد بررسی قرار بدهیم.

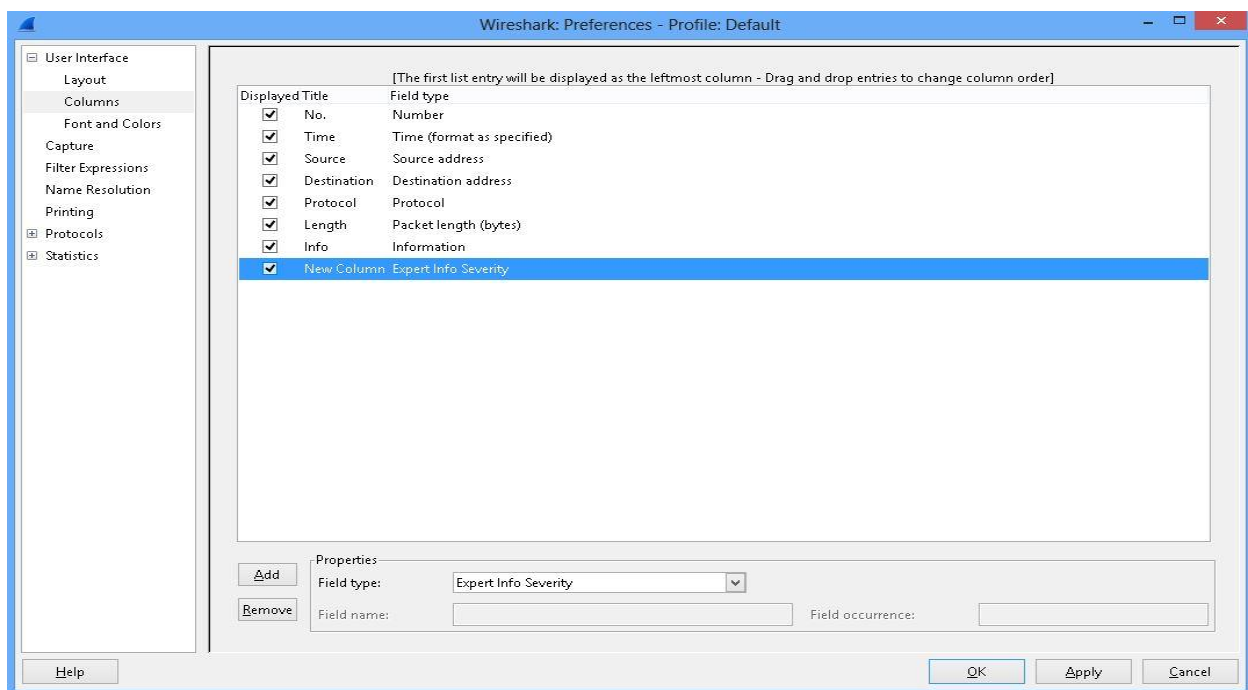
استفاده از پنجره Preferences

از پنجره preferences می توان برای تنظیم کردن گزینه های نمایشی برنامه Wireshark استفاده کرد. این گزینه قابلیت های Wireshark را افزایش می دهد، کاربر می تواند با استفاده از این گزینه چیز هایی که برای تجزیه و تحلیل مهم هستند را در پنجره اصلی Wireshark پیکربندی کنند. برای اجرای این گزینه می توانید به منوی Edit رفته و بر روی Preferences کلیک کنید تا اجرا گردد.



شما می توانید با استفاده از گزینه های پنجره Preferences چندین گزینه نمایشی مختلف را به پنجره اصلی برنامه اضافه با تغییر بدهید. بگذارید یک گام به جلو برداریو پانل Expert Info را به پانل ضبط اضافه نماییم.

1. گزینه Columns را از پانل سمت چپ انتخاب کنید.
2. در پنجره اصلی بر روی دکمه Add کلیک کنید. این عمل یک ستون جدید ایجاد می کند. سپس در منوی باز شو Field type گزینه Expert Info Severity را انتخاب کنید.



3. با کلیک بر روی دکمه Add نمای ستون را فعال سازید. سپس می توانید به منظور تغییر نام ستون هم بر روی آن دو بار کلیک کنید و سپس نام مد نظر خود را در آن وارد سازید.

هنگامی که این گام ها را با موفقیت به اتمام رساندید متوجه خواهید شد که در پانل ضبط یک ستون جدید با نامی که شما انتخاب کردید اضافه خواهد شد و جزئیات Expert Info را به نمایش می گذارد.

No.	New Column	Time	Source	Destination	Protocol	Length	Info
1415	Error	936.004162000	192.168.192.129	165.254.155.88	TCP	54	49194 > http [ACK] Seq=232 Ack=2722 win=64240
1416	Error	961.863331000	192.168.192.129	192.168.192.2	NBNS	110	Refresh NB WIN-L15MR25EDE0<00>
1417	Error	963.376277000	192.168.192.129	192.168.192.2	NBNS	110	Refresh NB WIN-L15MR25EDE0<00>
1418		964.093444000	fe80::e04c:7f8c:efaff02::1:2		DHCPv6	157	solicit XID: 0x21bf0f CID: 0001000119ca810a000
1419	Error	964.889342000	192.168.192.129	192.168.192.2	NBNS	110	Refresh NB WIN-L15MR25EDE0<00>
1420		966.683403000	vmware_9c:d3:95	vmware_fc:a6:fc	ARP	42	who has 192.168.192.2? Tell 192.168.192.129
1421		966.683545000	vmware_fc:a6:fc	vmware_9c:d3:95	ARP	60	192.168.192.2 is at 00:50:56:fc:a6:fc
1422	Chat	981.045512000	165.254.155.81	192.168.192.129	TCP	60	http > 49190 [FIN, PSH, ACK] Seq=2612 Ack=589
1423	Error	981.045626000	192.168.192.129	165.254.155.81	TCP	54	49190 > http [ACK] Seq=589 Ack=2613 win=65535
1424		1003.168555000	fe80::e59b:c9ae:41cfff02::1:3		LLMNR	84	Standard query 0x58cc A wpad
1425		1003.168558000	192.168.192.1	224.0.0.252	LLMNR	64	Standard query 0x58cc A wpad
1426		1003.368149000	192.168.192.1	192.168.192.255	NBNS	92	Name query NB WPAD<00>
1427		1004.117741000	192.168.192.1	192.168.192.255	NBNS	92	Name query NB WPAD<00>
1428		1004.867844000	192.168.192.1	192.168.192.255	NBNS	92	Name query NB WPAD<00>
1429	Chat	1020.042447000	165.254.155.81	192.168.192.129	TCP	60	http > 49191 [FIN, PSH, ACK] Seq=3896 Ack=865
1430	Error	1020.042568000	192.168.192.129	165.254.155.81	TCP	54	49191 > http [ACK] Seq=865 Ack=3897 win=65535
1431		1024.684756000	vmware_9c:d3:95	vmware_fc:a6:fc	ARP	42	who has 192.168.192.2? Tell 192.168.192.129
1432		1024.684913000	vmware_fc:a6:fc	vmware_9c:d3:95	ARP	60	192.168.192.2 is at 00:50:56:fc:a6:fc
1433	Error	1081.875161000	192.168.192.129	192.168.192.2	NBNS	110	Refresh NB WIN-L15MR25EDE0<00>
1434	Error	1083.419151000	192.168.192.129	192.168.192.2	NBNS	110	Refresh NB WIN-L15MR25EDE0<00>
1435	Error	1084.932232000	192.168.192.129	192.168.192.2	NBNS	110	Refresh NB WIN-L15MR25EDE0<00>
1436		1086.679284000	vmware_9c:d3:95	vmware_fc:a6:fc	ARP	42	who has 192.168.192.2? Tell 192.168.192.129
Frame 1: 92 bytes on wire (736 bits), 92 bytes captured (736 bits) on interface 0							
Ethernet II, Src: vmware_c0:00:08 (00:50:56:c0:00:08), Dst: Broadcast (ff:ff:ff:ff:ff:ff)							
Internet Protocol Version 4, Src: 192.168.192.1 (192.168.192.1), Dst: 192.168.192.255 (192.168.192.255)							
User Datagram Protocol, Src Port: netbios-ns (137), Dst Port: netbios-ns (137)							
NetBIOS Name Service							

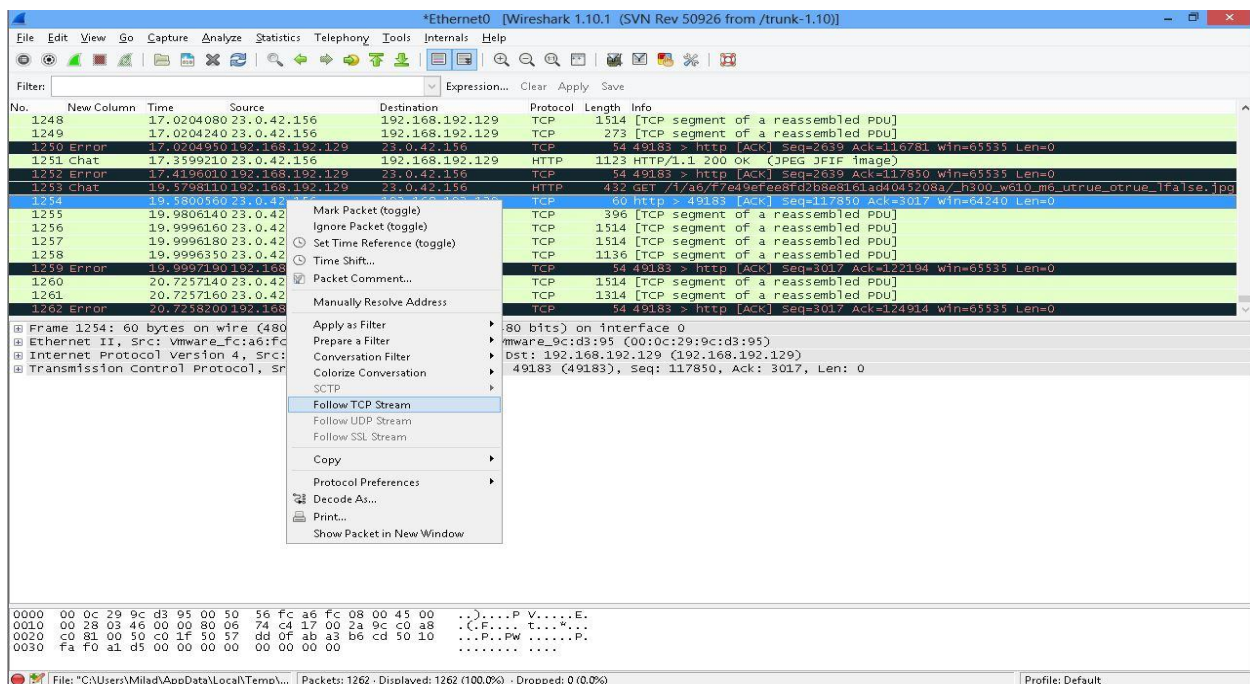
این یک توضیح مختصر از چگونگی استفاده از گزینه های preferences برای تغییر دادن صفحه نمایشی برنامه Wireshark مطابق با انتخاب شما بود. همچنین شما می توانید با استفاده از این ویژگی دیگر تنظیمات برنامه Wireshark را هم تغییر بدهید.

فصل چهارم : 5 ویژگی مهمی که شما باید درباره آن ها بدانید

هنگامی که شروع به استفاده از برنامه Wireshark می کنید، متوجه خواهید شد که طیف گسترده ای از کار ها وجود دارد که می توان با استفاده از Wireshark آن ها را انجام داد. در این بخش، به شما همه چیز در مورد عملیات هایی که به صورت رایج می توان با استفاده از Wireshark انجام داد و رایج ترین ویژگی های موجود در برنامه Wireshark را مستند خواهیم کرد.

کار با جریان های بسته¹

هنگام ضبط بسته های اطلاعاتی شبکه، ممکن است چند نمونه از فعالیت های شبکه همزمان رخ دهد. به عنوان مثال، در نظر بگیرید که بطور همزمان از طریق مرورگر به مرور چندین وب سایت پردازید. در این لحظه، چندین بسته اطلاعاتی TCP در سراسر شبکه برای این وب سایت ها جریان پیدا خواهد کرد. به همین دلیل، در این شرایط پیگیری بسته های اطلاعاتی برای یک جریان یا یک نشست خاص کمی خسته کننده خواهد شد. در اینجاست که برای حل این مشکل ویژگی Follow TCP stream وارد عمل می شود. با این حال، برای مشاهده یک جریان کامل، کافیست یک بسته TCP را انتخاب کرده (به عنوان مثال، یک بسته که درخواست GET یا POST ارسال کرده است) و سپس بر روی آن کلیک راست کرده و بر روی گزینه Follow TCP Stream کلیک کنید. پس از آن جریان بسته های اطلاعاتی آن نشست خاص فقط در پانل ضبط نمایش داده خواهد شد.



¹ Working with packet streams

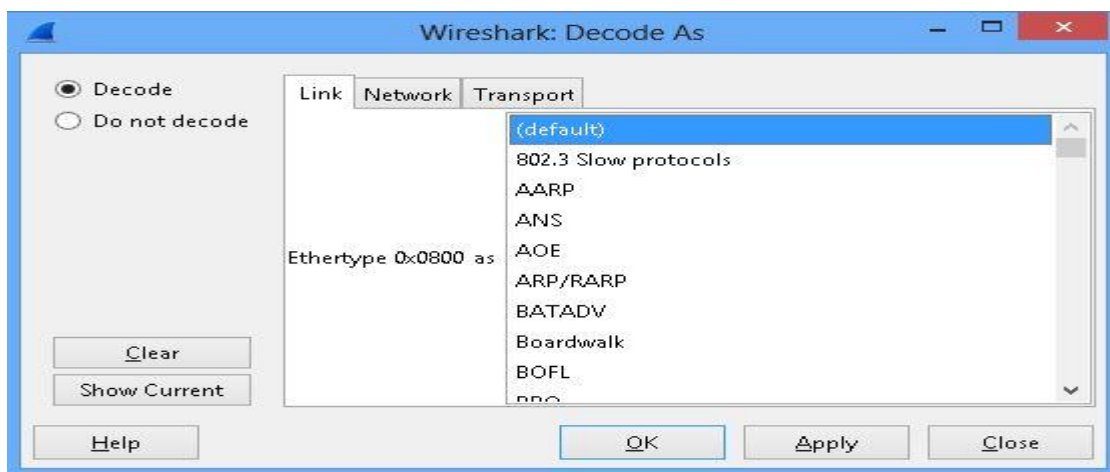
هنگامی که بر روی گزینه Follow TCP Stream کلیک می کنید، متوجه خواهید شد که یک فیلتر جدید برای Wireshark اعمال می شود و پانل ضبط اصلی تمامی بسته های آن جریان را بازتاب می دهد. این می تواند در کشف درخواست و پاسخوگی های مختلف که از طریق یک جلسه شبکه تعامل تولید شده است مفید واقع شود. اگر کمی دقت به فیلتر اعمال شده بر روی جریان کنید، شما یک قاعده دستوری مشابه tcp.stream eq <Number> مشاهده خواهید کرد. گزینه Number شماره بسته ای که شما قصد دنبال کردن جریان داده ای آن را داشتید را شامل می شود. شایان ذکر است، مشابه دنبال کردن جریان بسته های TCP، همچنین می توان جریان های UDP و SSL را هم دنبال کرد. بدین منظور کافیست که بر روی آن بسته اطلاعاتی کلیک راست کرده و یکی از گزینه های Follow UDP/SSL Stream را انتخاب کنید.

رمزگشایی بسته و صادرات اشیاء¹

برنامه Wireshark یک ویژگی بسیار قدرتمند برای رمزگشایی بسته های ضبط شده در قالب های مشخص شده توسط کاربر ارائه می دهد. ویژگی رمزگشایی Wireshark موقتا تشریحات پروتکال خاص را انتقال می دهد. این فرآیند می تواند در حالتی مفید واقع شود که داده ها بر روی چندین درگاه جریان داشته باشند یا به عنوان یک پروتکل به رسمیت شناخته نشده باشد. ویژگی رمزگشایی می تواند به سادگی برای انتقال بسته ها به پروتکل اصلیشان مورد استفاده قرار گیرد.

نکته : ویژگی رمزگشایی یک عملیات موقتی است و تغییرات آن از دست خواهد رفت مگر اینکه بسته رمزگشایی شده به طور جداگانه ذخیره شوند.

بر روی یک بسته کلیک راست کرده و سپس گزینه Decode as را انتخاب کنید. پس از آن یک پنجره که شامل تب ها و گزینه های مختلفی است به نمایش گذاشته می شود.

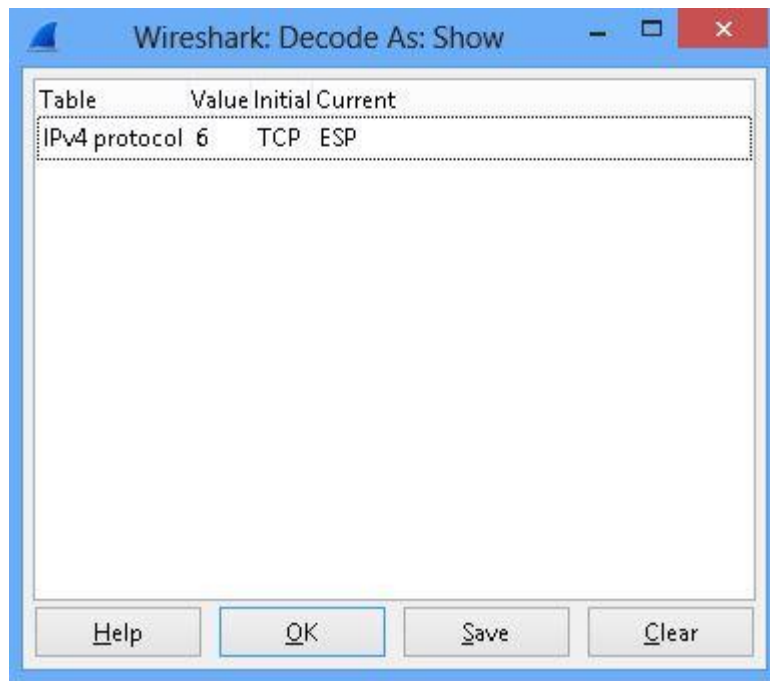


¹ Decoding packets and exporting objects

همانطور که در تصویر بالا مشاهده می کنید در این پنجره سه تب وجود دارد. بگذارید این سه تب را به صورت جداگانه تشریح کنیم.

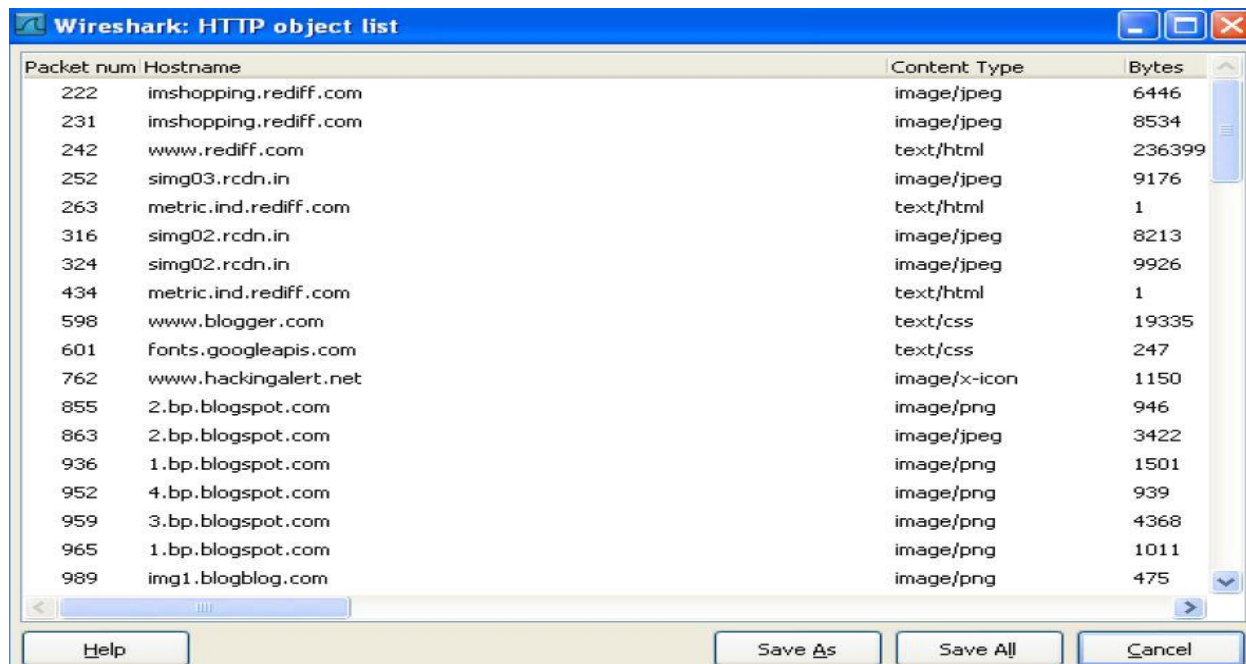
1. **تب Link :** انتخاب کردن این گزینه پروتکل های مختلف در لایه پیوند داده را نمایش می دهد. برگزیدن هر کدام از پروتکل ها و انتخاب گزینه رادیوی Decode بسته مشخص شده را به پروتکل مشخص شده توسط کاربر تبدیل می کند.
2. **تب Network :** این تب شامل پروتکل های مختلف لایه شبکه از قبیل TCP و UDP می شود. این ویژگی می تواند در تبدیل IPv4 به IPv6 مفید واقع شود.
3. **تب Transport :** این تب پروتکل های مختلف لایه انتقال را بازتاب می دهد که در آن می توان بسته ها را رمزگشایی کرد.

همچنین شما می توانید با کلیک کردن بر روی دکمه Show Current رمزگشایی های کاربر را مشاهده کنید.



پس از اینکه با کلیک کردن بر روی Apply رمزگشایی را انجام می دهید، با کلیک بر روی Show Current پنجره بالا به نمایش در می آید که گزارش تبدیلات انجام شده را می دهد. با این حال، به منظور پاک کردن گزارش تمامی تبدیل های انجام شده می توانید بر روی دکمه Clear کلیک کنید، همچنین می توانید با کلیک کردن بر روی Save این گزارشات را ذخیره سازی کنید.

خب، حال یک گام به جلو بر می داریم و یکی دیگر از ویژگی های مهم Wireshark را مورد بحث قرار می دهیم. برنامه Wireshark ویژگی مبنی بر ارسال اشیاء مختلف در جریان های ضبط شده را ارائه می دهد. با این حال، برای مشاهده اشیاء مختلف ضبط شده در یک ترافیک HTTP به منوی File و سپس Export Object بروید و بر روی گزینه HTTP کلیک کنید. بعد از کلیک بر روی این گزینه صفحه ای به شکل زیر برای شما به نمایش گذاشته می شود که تمام اشیاء ضبط شده در حال انتقال از ترافیک HTTP را نمایش می دهد.



هر کدام از اشیاء را که می خواهید انتخاب کرده و بر روی گزینه Save As کلیک کنید. سپس بسته ضبط شده را به نوع شی مد نظرتان تبدیل سازید. به عنوان مثال، یک نوع فایل image/JPEG را انتخاب کرده و آن را ذخیره سازی کنید، متوجه خواهید شد که یک فایل JPEG بر روی دیسک سخت سیستم شما ذخیره می شود. این یک راه بسیار سریع و کارآمد برای بازیابی انواع فایل های مختلف دانلود شده در طول ضبط بسته ها است.

آمارگیری بسته های ضبط شده¹

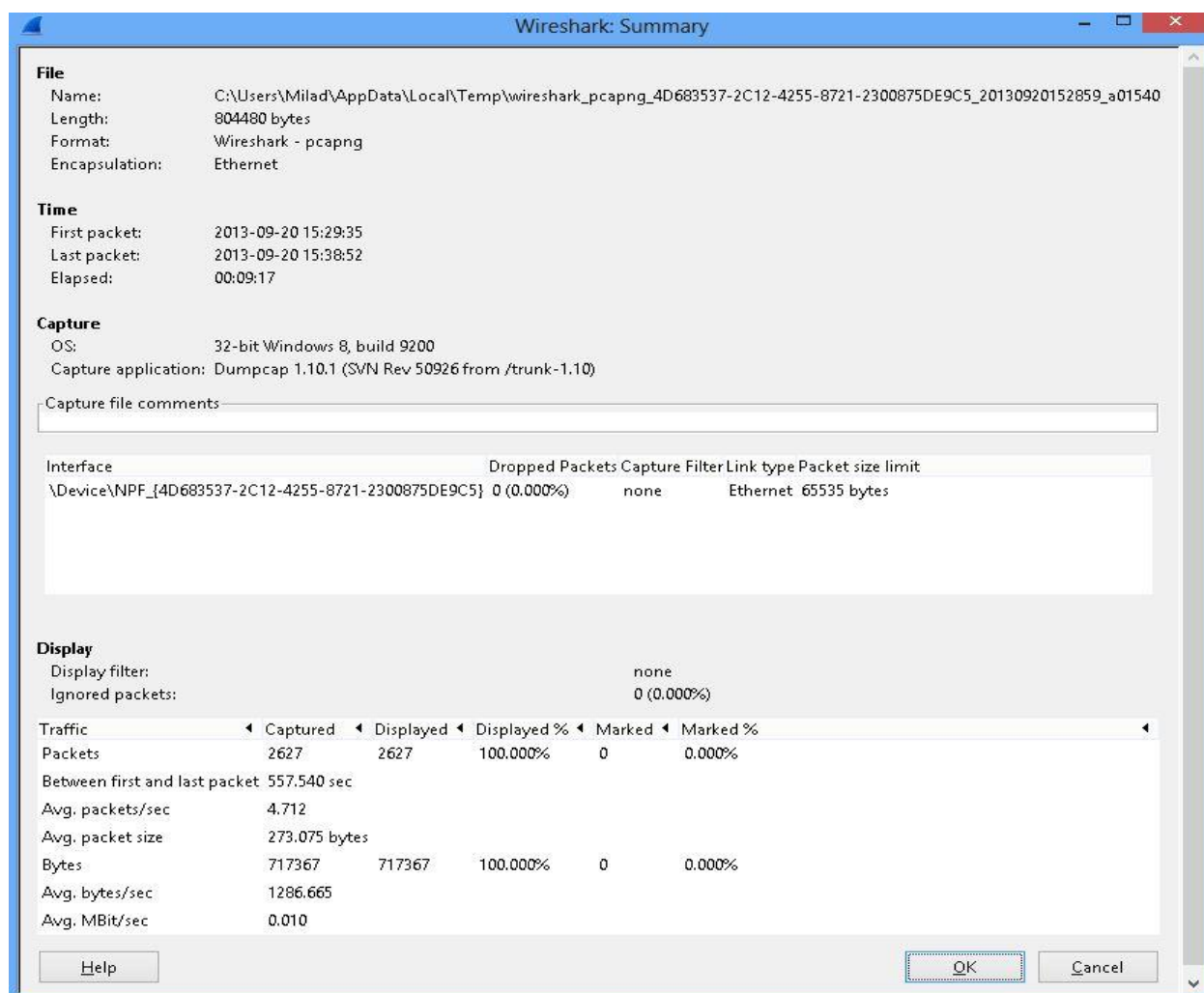
در این قسمت به نحوه ایجاد یک آمار برای بسته های ضبط شده به منظور مرور مجدد فعالیت های شبکه نگاه دقیقی خواهیم انداخت. پیش از این ما با گراف های ورودی و خروجی در قسمت های گذشته آشنا شدیم. حالا در اینجا برخی از مهم ترین جنبه های تولید آمار بسته های ضبط شده را آشکار خواهیم کرد. گزینه منو Statistics در برنامه Wireshark دارای برخی از عالی ترین ویژگی های آمارگیری است که می تواند در ایجاد یک آمار برای بسته های ضبط شده به منظور مرور مجدد فعالیت های شبکه مورد استفاده قرار گیرند. در این قسمت ما پنج ابزار مهم،

¹ Statistics of the captured packets

Summary، Protocol Hierarchy، Conversations، Endpoint و Flow Graph را تشریح خواهیم کرد. حال اجازه دهید هر کدام از آن ها را جداگانه مورد بحث قرار بدهیم.

خلاصه آمار¹

گزینه Summary در منوی Statistics درباره کل فرآیند ضبط توسط منعکس کردن نکات کلیدی از قبیل، رابط های شبکه، مدت زمان ضبط، شماره و اندازه بسته های ضبط شده گزارش بسیار سریعی ارائه می دهد.. گزینه Summary همه این اطلاعات را به صورت خلاصه ارائه می کند. شایان ذکر است، Summary بسیار مفید می باشد در کالبد شکافی² جرایم رخ داده شبکه زمانی که یک مرور سریع از فعالیت های شبکه مورد نیاز است.



¹ Summary

² forensics

نمایش سلسله مراتبی پروتکل¹

نمایش سلسله مراتب پروتکل ها نشان دهنده اطلاعات آماری از پروتکل های مختلف دیده شده در طول تجزیه و تحلیل شبکه در یک فرم گره ای است. این گزینه پروتکل ها را با توجه به لایه و نمایش آن ها در فایل ضبط شده به صورت در صد تنظیم می کند.

Wireshark: Protocol Hierarchy Statistics

Display filter: none

Protocol	% Packets	Packets	% Bytes	Bytes	Mbit/s	End	Packets	End	Bytes	End	Mbit/s
Frame	100.00 %	2627	100.00 %	717367	0.010	0	0	0	0.000		
Ethernet	100.00 %	2627	100.00 %	717367	0.010	0	0	0	0.000		
Internet Protocol Version 4	97.87 %	2571	99.30 %	712336	0.010	0	0	0	0.000		
User Datagram Protocol	4.42 %	116	1.76 %	12594	0.000	0	0	0	0.000		
Domain Name Service	2.78 %	73	1.05 %	7543	0.000	73	7543	0.000			
NetBIOS Datagram Service	0.08 %	2	0.07 %	494	0.000	0	0	0.000			
SMB (Server Message Block Protocol)	0.08 %	2	0.07 %	494	0.000	0	0	0.000			
SMB MailSlot Protocol	0.08 %	2	0.07 %	494	0.000	0	0	0.000			
Microsoft Windows Browser Protocol	0.08 %	2	0.07 %	494	0.000	2	494	0.000			
NetBIOS Name Service	1.48 %	39	0.54 %	3858	0.000	39	3858	0.000			
Bootstrap Protocol	0.08 %	2	0.10 %	699	0.000	2	699	0.000			
Ethernet over IP	93.22 %	2449	97.50 %	699418	0.010	0	0	0.000			
Ethernet	93.22 %	2449	97.50 %	699418	0.010	0	0	0.000			
Data	93.11 %	2446	97.48 %	699256	0.010	2446	699256	0.010			
Malformed Packet	0.11 %	3	0.02 %	162	0.000	3	162	0.000			
Internet Group Management Protocol	0.23 %	6	0.05 %	324	0.000	6	324	0.000			
Internet Protocol Version 6	1.29 %	34	0.54 %	3909	0.000	0	0	0.000			

Help

Close

مکالمات

گزینه مکالمات یکی دیگر از ویژگی های خارق العاده تجزیه و تحلیل آماری بسته های اطلاعاتی است که ارتباط میان آی پی آدرس های مختلف و همچنین آمار مکالمه پروتکل های مختلف منتقل شده از یک IP را را نمایش می دهد. این تجزیه و تحلیل آماری هنگامی که یک تجزیه و تحلیل نظیر به نظیر میان میزبان و سرور رخ می دهد بسیار عالی است.

¹ Protocol Hierarchy

Conversations: Ethernet0

Ethernet: 2087 Fibre Channel FDDI IPv4: 35 IPv6: 5 IPX JXTA NCP RSVP SCTP TCP Token Ring UDP: 55 USB WLAN

IPv4 Conversations

Address A	Address B	Packets	Bytes	Packets A→B	Bytes A→B	Packets B→A	Bytes B→A	Rel Start	Duration	bps A→B	bps B→A
192.168.192.2	192.168.192.129	77	8 529	28	4 205	49	4 324	0.000000000	538.6702	62.45	64.22
70.37.131.11	192.168.192.129	80	26 853	40	9 240	40	17 613	0.066588000	538.0317	137.39	261.89
70.37.131.51	192.168.192.129	135	120 474	91	113 078	44	7 396	3.783274000	534.4370	1692.67	110.71
192.168.192.129	213.199.149.173	12	3 487	6	655	6	2 832	7.219884000	140.9298	37.18	160.76
192.168.192.1	192.168.192.255	20	2 150	20	2 150	0	0	8.348272000	450.8684	38.15	N/A
65.52.108.11	192.168.192.129	28	8 211	14	3 342	14	4 869	8.669093000	529.4429	50.50	73.57
41.221.242.101	192.168.192.129	398	27 885	350	21 000	48	6 885	8.669699000	548.8704	306.08	100.35
2.20.218.156	192.168.192.129	1 008	146 206	448	68 432	560	77 774	9.507402000	530.4423	1032.07	1172.97
192.168.192.129	204.79.197.200	137	132 281	42	4 043	95	128 238	10.967989000	528.0102	61.26	1942.96
165.254.40.122	192.168.192.129	46	5 456	21	2 250	25	3 206	11.014245000	527.3915	34.13	48.63
31.13.81.65	192.168.192.129	39	2 494	6	360	33	2 134	11.025476000	546.1137	5.27	31.26
23.52.241.224	192.168.192.129	72	11 515	32	4 880	40	6 635	11.173712000	528.6125	73.85	100.41
94.245.117.47	192.168.192.129	30	10 290	16	6 829	14	3 461	11.269529000	517.5292	105.56	53.50
10.10.34.34	192.168.192.129	28	20 279	17	19 244	11	1 035	11.928158000	136.5160	1127.72	60.65
94.245.121.177	192.168.192.129	46	16 252	23	13 229	23	3 023	12.187276000	518.7854	204.00	46.62
94.232.172.101	192.168.192.129	29	18 633	19	17 384	10	1 249	12.531573000	132.6917	1048.08	75.30
23.0.160.43	192.168.192.129	12	3 933	6	3 240	6	693	14.798196000	134.5027	192.71	41.22
54.236.176.185	192.168.192.129	26	4 754	13	2 371	13	2 383	15.03527000	516.1180	36.75	36.94
138.108.7.20	192.168.192.129	21	5 014	11	2 550	10	2 464	15.802252000	526.1151	38.77	37.47
192.168.192.129	213.199.149.251	90	66 034	32	3 103	58	62 931	17.230011000	522.6037	47.50	963.35
66.119.33.141	192.168.192.129	24	6 028	12	2 720	12	3 308	17.547033000	513.7256	42.36	51.51
192.168.192.129	199.38.164.155	24	5 553	12	2 035	12	3 518	17.726130000	513.7105	31.69	54.79

☒ Name resolution ☐ Limit to display filter

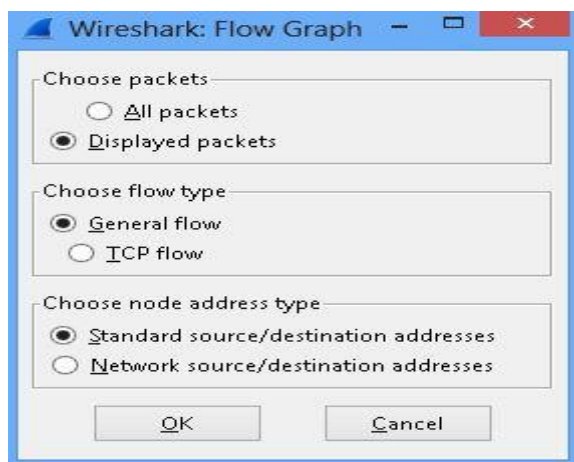
Help Copy Follow Stream Graph A→B Graph B→A Close

نقطه انتهایی¹

آمارگیر نقطه انتهایی شبیه گزینه مکالمات است. این گزینه آمار ترافیک ورودی و خروجی از یک آدرس آی پی را منعکس می کند.

گراف جریان²

نمودار جریان یک نمایش جدول زمانی مبتنی بر آمار های ارتباطی است که نشان دهنده مکالمات مختلف بر اساس فواصل زمانی است. بر روی گزینه Flow Graph کلیک کنید تا یک پنجره محاوره ای اجرا شود که از شما چند اطلاعات اولیه برای تولید گراف می پرسد.



¹ Endpoints

² Flow graph

ما می توانیم اطلاعاتی از قبیل انتخاب بسته ها، نوع جریان، و حالت انعکاس اطلاعات گراف را مشخص سازیم. این آمار تحلیلی در خواندن جدول زمانی فعالیت های شبکه مفید است. همچنین در فهم بار ترافیک شبکه هم به ما کمک می کند. به هر حال، این یک نمایش ساده از گزینه های تحلیل آماری موجود در Wireshark به منظور درک بهتر فعالیت های شبکه بود. در قسمت بعدی برخی از روش های تکنیکال به منظور دمونتاژ و تفکیک اسامی را مورد بررسی قرار خواهیم داد.

تفکیک اسامی و مونتاز دوباره بسته ها¹

در این قسمت به برخی از مهم ترین ویژگی های تعبیه شده در Wireshark که فرآیند تحلیل شبکه را برای ما تسهیل می بخشند، نگاهی خواهیم انداخت. با این حال، ما کار خود را در این قسمت با تفکیک اسامی شروع می کنیم.

تفکیک پذیری اسامی

تفکیک پذیری اسامی فرآیند تبدیل یک آدرس شناسایی به یک آدرس دیگر برای درک بهتر است. به عنوان مثال، اگر یک کامپیوتر یک آدرس فیزیکی مانند CD:6C:8B:24:00:16 داشته باشد، پروتکل های DNS و ARP به ما اجازه می دهند یک نام قابل مشاهده مانند MiladPC برای آن استفاده کنیم. این ارتباط فرآیند شناسایی دستگاه های مختلف در شبکه را آسان می سازد. برنامه Wireshark ابزار های مختلفی برای تفکیک پذیری اسامی ارائه می دهد که آدرس های فیزیکی را به یک نام خواندنی فایل ملاحظه تغییر می دهند. بگذارید یک نگاه سریع به برخی از ابزار های تفکیک پذیری اسامی حاضر در Wireshark بیندازیم.

تفکیک پذیری نام MAC

تفکیک پذیری نام MAC از پروتکل های ARP/RARP برای تبدیل آدرس های فیزیکی (MAC) به یک آدرس منطقی قابل ملاحظه (IP) استفاده می کند.

تفکیک پذیر نام شبکه²

تفکیک پذیری نام شبکه آدرس منطقی (IP) را به یک نام DNS برای درک بهتر تبدیل می کند. به عنوان مثال، آدرس 173.194.72.101 تبدیل به google.com می شود.

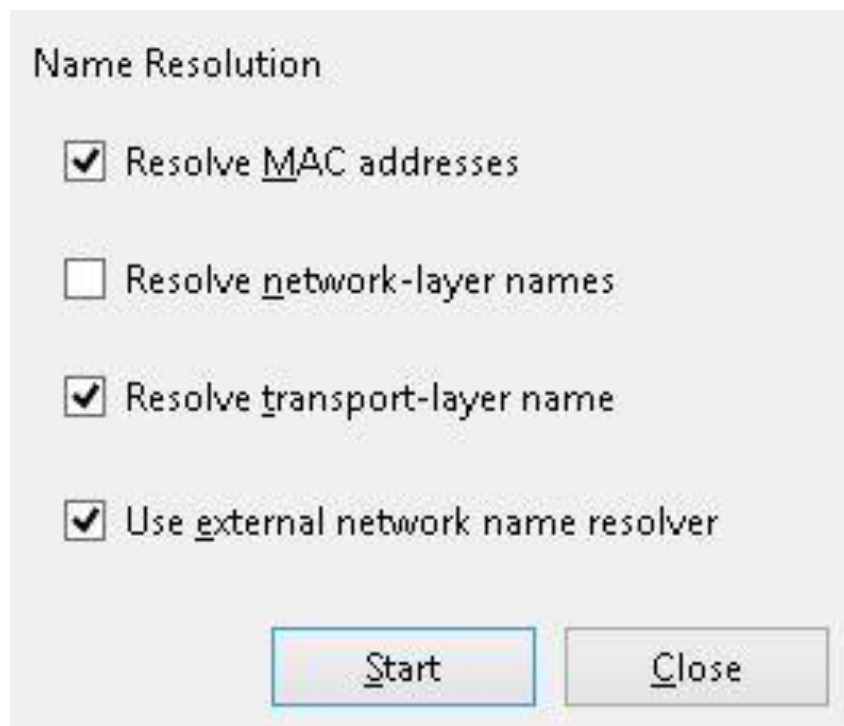
¹ Name resolution and packet reassembling

² Network name resolution

تفکیک پذیری نام انتقال¹

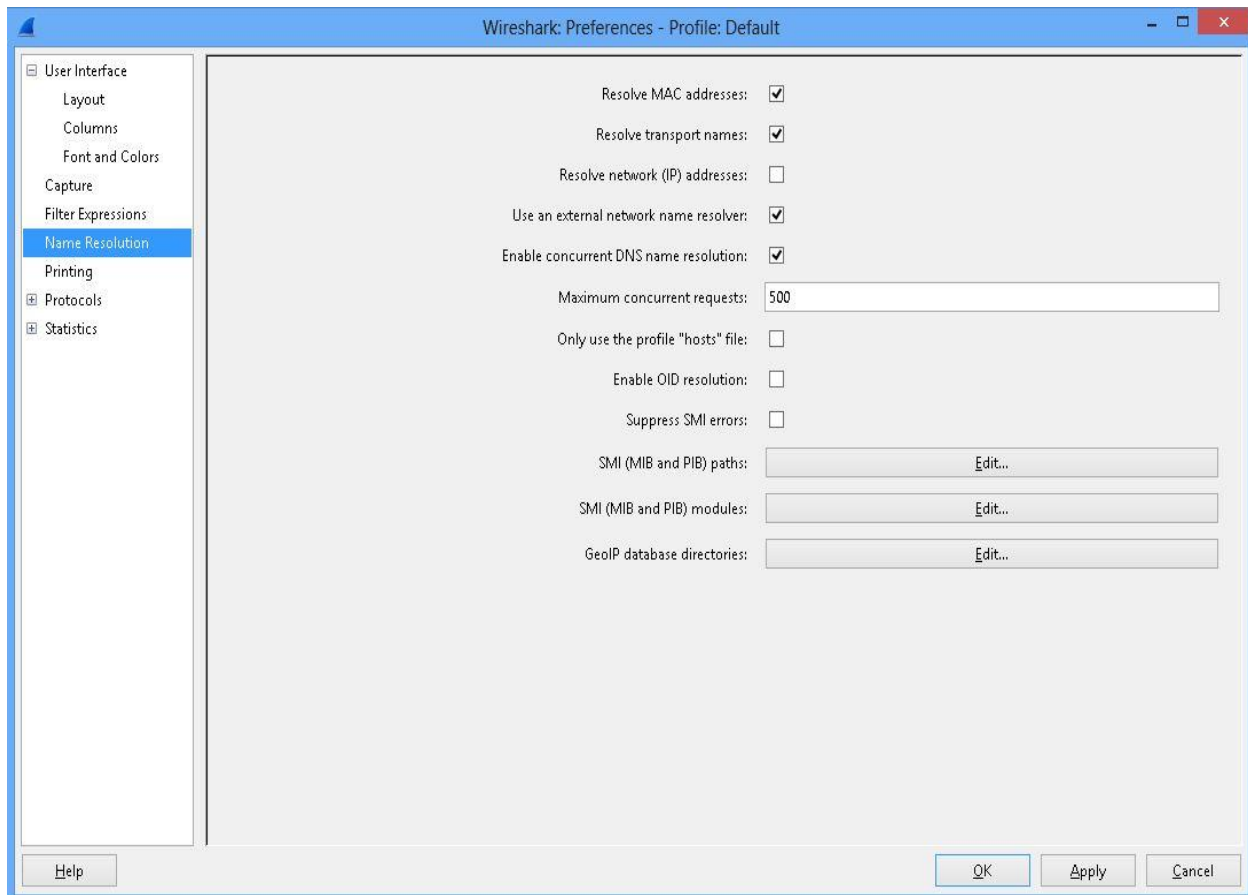
این روش تفکیک پذیری، نام سرویس ها را مطابق با شماره درگاهشان شناسایی می کند. به عنوان مثال، درگاه 80 سرویس HTTP در ماشین میزبان است.

برای فعال سازی تفکیک پذیری اسامی در برنامه Wireshark به منوی Capture بروید و گزینه Capture Options را انتخاب کنید. اینپنجره محاوره ای گزینه های ضبط را اجرا می کند که ما قبلا آن را مشاهده کرده بودیم. قسمت سمت راست Name Resolutions گزینه های مختلف برای تفکیک پذیری اسامی را نمایش می دهد.



شما می توانید چک باکس های مختلف را بر اساس نیازهای خود انتخاب کنید. بدین منظور به منوی Edit رفته و سپس بر روی گزینه Preferences کلیک کنید. پس از آن از گزینه های سمت راست Name Resolution را انتخاب کنید.

¹ Transport name resolution



این پنجره گزینه های پیشرفته تر در مقایسه با قبل ارائه می کند. در اینجا ما می توانیم کلیک کردن بر روی گزینه Edit جلوی GeoIP Database directories یک بانک اطلاعاتی از GeoIP ها را به Wireshark ارائه دهیم تا قدرت تفکیک پذیری Wireshark را بهبود ببخشیم و در شناسایی مناطق ارسالی بسته بر اساس GeoIP به Wireshark کمک کنیم. این ویژگی تعبیه شده در برنامه Wireshark نه تنها تحلیل شبکه را ساده تر می کند، بلکه توانایی Wireshark را در شناسایی سرویس ها و پروتکل ها هم افزایش می دهد. اما تفکیک پذیری اسامی دارای چندین ضعف هست که نیاز است در این قسمت ذکر شوند.

1. تفکیک پذیری اسامی ممکن است در طی ضبط زنده بسته های شبکه یا باز کردن یک فایل ضبط ذخیره شده با شکست رو به رو شود.
2. تفکیک پذیری اسامی بایت های اضافی فضا های درون فایل ضبط شده ایجاد می کنند که در نتیجه بر روی نمودار آماری تاثیر می گذارد.
3. تفکیک پذیری اسامی در حین پردازش بسته های سرآیند های اضافی به بسته ها اضافه می کند.

حالا اجازه دهید یک گام به جلو بردازیم و به بحث مهم بعدی این بخش پردازیم می کند.

مونتاژ دوباره بسته ها

مونتاژ دوباره بسته ها، فرآیندی است که در طی آن یک مقدار بسیار بزرگ از داده ها به بسته های کوچک تجزیه می شوند و سپس آن ها با هم ترکیب شده و قالب کامل اولیه خود را بدست می آورند. به منظور تولید مجدد بسته های اطلاعاتی ضبط شده، برنامه Wireshark روش مونتاژ دوباره خود را مورد استفاده قرار می دهد. در این روش، برنامه Wireshark تکه های مختلف بسته های اطلاعاتی را جمع آوری کرده و سپس آن ها را دوباره مونتاژ می کند تا فایل کامل آن را از طریق پانل بایت های بسته ارائه دهد.

0000	00 0c 29 9c d3 95 00 50	56 fc a6 fc 08 00 45 00	..)....P V.....E.
0010	02 59 1a 9d 00 00 80 06	c0 27 02 14 da 9c c0 a8	.Y.....'.....
0020	c0 81 00 50 c0 2b 0b 1a	2f ab 66 6a 02 c7 50 18	...P.+.../.fj...P.
0030	fa f0 52 9f 00 00 31 c8	ca 47 04 e4 7b 56 6d b7	..R...1. .G...{vm.
0040	07 ae 6b a2 f1 2f ce ce	cd d7 26 b9 44 66 56 c8	..k.../.. ..&.DfV.
0050	24 1a f2 e1 b1 e9 4f 73	65 58 e3 da 92 41 bf bd	\$......Os eX...A..
0060	57 49 1b 68 19 e9 cd 4c	ac 7f 9d 68 84 54 9e 2c	WI.h...L ...h.T.,
0070	82 31 db bd 25 ac 39 23	8a b0 dc 80 4d 49 fe ae	.1..%.9#MI..

Frame (615 bytes) Reassembled TCP (36611 bytes)

File: "C:\Users\Milad\AppData\Local\Temp\w\ Packets: 517 · Displayed: 517 (100.0%) · Dropped: 0 (0.0%)

به عنوان مثال، یک درخواست HTTP Get می تواند به بسته های اطلاعاتی کوچک تری تقسیم شود. هنگامی که فرآیند انتقال تکمیل شود، برنامه Wireshark بسته های مختلف را مونتاژ دوباره می کند و یک صفحه HTML دوباره مونتاژ شده ایجاد می کند. پانل جزئیات بسته شامل اطلاعات اضافی (Reassembled TCP segments) درباره شماره بسته های مختلف می شود که مونتاژ دوباره شده اند.

Flags: 0x018 (PSH, ACK) window size value: 64240 [Calculated window size: 64240] [window size scaling factor: -2 (no window scaling used)] Checksum: 0x9f4a [validation disabled] [SEQ/ACK analysis] TCP segment data (921 bytes)		
[16 Reassembled TCP Segments (22569 bytes): #451(1460), #452(1424), #471(1460), #472(1460), #473(1460)]		
[Frame: 451, payload: 0-1459 (1460 bytes)] [Frame: 452, payload: 1460-2883 (1424 bytes)] [Frame: 471, payload: 2884-4343 (1460 bytes)] [Frame: 472, payload: 4344-5803 (1460 bytes)] [Frame: 473, payload: 5804-7263 (1460 bytes)]		
0000	48 54 54 50 2f 31 2e 31 20 32 30 30 20 4f 4b 0d	HTTP/1.1 200 OK.
0010	0a 43 61 63 68 65 2d 43 6f 6e 74 72 6f 6c 3a 20	.Cache-Control:
0020	6e 6f 2d 63 61 63 68 65 2c 20 6e 6f 2d 73 74 6f	no-cache, no-sto
0030	72 65 2c 20 6e 6f 2d 74 72 61 6e 73 66 6f 72 6d	re, no-t ransform
0040	0d 0a 50 72 61 67 6d 61 3a 20 6e 6f 2d 63 61 63	..Pragma: no-cac
0050	68 65 0d 0a 43 6f 6e 74 65 6e 74 2d 54 79 70 65	he..Content-Type
0060	3a 20 74 65 78 74 2f 68 74 6d 6c 3b 20 63 68 61	: text/html; cha
0070	72 73 65 74 3d 75 74 66 2d 38 0d 0a 43 6f 6e 74	rset=utf -8..Cont

Frame (975 bytes) Reassembled TCP (22569 bytes) Uncompressed entity body (72333 bytes)

TCP Segments (tcp.segments), 22569 bytes Packets: 517 · Displayed: 517 (100.0%) · Dropped: 0 (0.0%)

داده های کاملاً دوباره مونتاژ شده در تب Uncompressed entity body از پانل بایت های بسته انعکاس داده می شود و Hex Dump شده بسته ها تحت تب Reassembled TCP انعکاس داده می شود. شایان ذکر است، مونتاژ دوباره بسته ها به صورت پیش فرض در برنامه Wireshark فعال است.

ابزار های تحت خط فرمان Wireshark

حال که ما تقریباً تمامی پیاده سازی های Wireshark را مورد بررسی قرار دادیم، در پایان می توانیم با بحث در مورد ابزار های تحت خط فرمان Wireshark از قدرت برنامه Wireshark یک نتیجه گیری کلی کنیم. بگذارید برخی از این فرمان ها را محیط خط فرمان ویندوز تحلیل مورد تحلیل قرار بدهیم. این فرمان ها مشابهها در لینوکس می توانند مورد استفاده قرار گیرند. بدین منظور، ابتدا به محل نصب Wireshark بروید و سپس دستور tshark -h را اجرا کنید. هنگامی که برنامه tshark را با پارامتر h- اجرا می کنید، فایل راهنمای آن نمایش داده می شود. حال بگذارید این دستور را اجرا کنیم و خروجی آن را مورد مطالعه قرار بدهیم.

برنامه Terminal Wireshark یا Tshark

دستور tshark یک فرمان برای شروع بسیاری از عملیات ها Wireshark تحت محیط خط فرمان است. بگذارید کار خود را با استفاده از این برنامه آغاز کنیم، همانطور که پیش از این گفته شد، برای اجرای این برنامه تحت خط فرمان، ابتدا به مسیر نصب برنامه رفته و سپس دستور آورده شده در زیر را اجرا کنید. دستور زیر راهنمای برنامه tshark را به نمایش می گذارد.

```
C:\Program Files\Wireshark>tshark -h
```

```
TShark 1.6.1 (SVN Rev 38096 from /trunk-1.6)
```

```
Dump and analyze network traffic. See http://www.wireshark.org for more information.
```

```
Copyright 1998-2011 Gerald Combs <gerald@wireshark.org> and contributors.
```

```
This is free software; see the source for copying conditions. There is NO warranty; not even for  
MERCHANTABILITY or FITNESS FOR A PARTICULAR PURPOSE.
```

```
Usage: tshark [options] ...
```

بیشتر پارامتر هایی که شما می توانید به همراه tshark مورد استفاده قرار بدهید توضیحاتشان در برنامه آورده شده است و شما به راحتی می توانید عملکرد آنها را درک کنید. به عنوان مثال، بگذارید لیست رابط های شبکه در سیستم را با استفاده از tshark لیست کنیم.

C:\Program Files\Wireshark>tshark -D

1. \Device\NPF_{730CDBFB-F346-4654-8196-5C20B7A69E12} (AMD PCNET Family Ethernet Adapter (Microsoft's Packet Scheduler))
2. \Device\NPF_{DD763ED6-6670-4281-8551-A3C651241F95} (AMD PCNET Family Ethernet Adapter (Microsoft's Packet Scheduler))

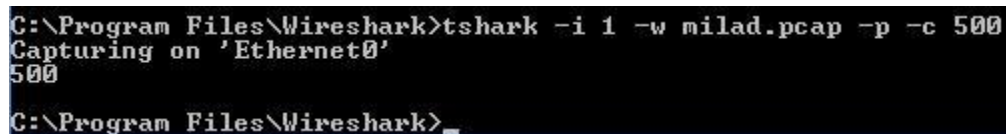
همانطور که مشاهده می کنید، پارامتر -D به tshark عبور داده شد، تا تمامی رابط های شبکه موجود در سیستم را برای ما به نمایش بگذارد. مشابه همین دستور ما می توانیم هر کدام از رابط های شبکه را که می خواهیم با استفاده از پارامتر -i و شماره رابط شبکه، آن رابط را بر روی ضبط بسته ها قرار بدهیم. بدین منظور کافیست دستور Tshark را به همراه پارامتر -i و به همراه این پارامتر شماره رابط شبکه را وارد کنیم و به منظور ذخیره سازی بسته های ضبط شده از پارامتر -w و به همراه آن یک نام برای ذخیره سازی بسته های ذخیره شده استفاده کنیم. همچنین ما می توانیم چندین پارامتر را به صورت ترکیبی در یک فرمان مورد استفاده قرار بدهیم. بگذارید یک مثال بزنیم تا نحوه عملکرد ضبط بسته های شبکه در محیط خط فرمان را بهتر درک کنیم.

C:\Program Files\Wireshark>tshark -i 1 -w milad.pcap -p -c 500

Capturing on AMD PCNET Family Ethernet Adapter (Microsoft's Packet Scheduler)

500

C:\Program Files\Wireshark>



```
C:\Program Files\Wireshark>tshark -i 1 -w milad.pcap -p -c 500
Capturing on 'Ethernet0'
500
C:\Program Files\Wireshark>
```

مشاهده کردید که پارامتر های گوناگونی به فرمان Tshark عبور داده شده است. فرمان آورده شده در بالا را می توان با یک زبان ساده تر تشریح کرد: در دستوری که مشاهده می کنید، ما با آوردن پارامتر 1 -i به برنامه tshark گفته ایم رابط شبکه شماره 1 را مورد شنود قرار بدهد و سپس خروجی را با نام milad.pcap ذخیره سازی کند. همچنین با استفاده از پارامتر p- گفته ایم که در حالت بی قاعده ترافیک را ضبط نکند و در پایان با دستور 500 -c گفته ایم که شماره بسته ها هنگامی که به 500 رسید فرآیند ضبط را متوقف سازد. قابل ذکر است، فایل milad.cap در همان مسیری ایجاد می شود که برنامه tshark قرار دارد. در گام بعد شما می توانید با استفاده از فرمان r- فایل های ضبط شده را باز کنید. به عنوان مثال ما با فرمان زیر فایل ضبط شده milad.pcap را در محیط خط فرمان باز می کنیم.

```
C:\Program Files\Wireshark>tshark -r capture.pcap
```

```
0.000000 10.0.2.15 -> 173.194.72.94 TLSv1 91 Application Data 0.000822
```

```
173.194.72.94 -> 10.0.2.15 TCP 60 https > opsmgr [ACK] Seq=1 Ack= 38 Win=65535 Len=0
```

```
0.148540 173.194.72.94 -> 10.0.2.15 TLSv1 91 Application Data 0.314759
```

```
10.0.2.15 -> 173.194.72.94 TCP 54 opsmgr > https [ACK] Seq=38 Ack =38 Win=62839 Len=0
```

```
0.527277 10.0.2.15 -> 31.13.79.20 TLSv1 606 Application Data
```

```
0.527761 31.13.79.20 -> 10.0.2.15 TCP 60 https > hiq [ACK] Seq=1 Ack=553 Win=65535 Len=0
```

```
1.097436 31.13.79.20 -> 10.0.2.15 TCP 1404 [TCP segment of a reassembled PDU]
```

```
1.107744 31.13.79.20 -> 10.0.2.15 TLSv1 229 Application Data
```

```
1.107790 10.0.2.15 -> 31.13.79.20 TCP 54 hiq > https [ACK] Seq=553 Ack=15 26 Win=64240  
Len=0
```

```
1.127783 31.13.79.20 -> 10.0.2.15 TCP 1404 [TCP segment of a reassembled PDU]
```

```
1.147908 31.13.79.20 -> 10.0.2.15 TLSv1 1234 Application Data
```

```
1.147942 10.0.2.15 -> 31.13.79.20 TCP 54 hiq > https [ACK] Seq=553 Ack=40 56 Win=64240  
Len=0
```

1.167471 31.13.79.20 -> 10.0.2.15 TCP 1404 [TCP segment of a reassembled PDU]

اگر متوجه شده باشید خروجی شبیه محیط GUI تولید شده است که اطلاعاتی از قبیل زمان ضبط، منبع/مقصد و پروتکل بسته را انعکاس داده است. اینگونه ما می توانیم قدرت Wireshark را از طریق خط فرمان مورد ارزیابی قرار بدهیم. حال بگذارید برخی از ابزار های جالب دیگر را مورد بررسی قرار بدهیم.

Rawshark، انباشت و تجزیه و تحلیل ترافیک

از Rawshark برای خواندن جریان بسته ها از فایل ضبط شده استفاده می شود. این عملیات مشابه عملیات Follow TCP Stream است که ما در قسمت کار با جریان های بسته آن را مورد بررسی قرار دادیم. برای مشاهده گزینه های موجود در Rawshark می توانیم از دستور rawshark -h استفاده کنیم. یک الگو ساده از rawshark به شکل زیر است.

```
C:\Program Files\Wireshark>rawshark -d proto:http -r milad
```

این فرمان به دنبال جریان بسته های پروتکل HTTP درون فایل مشخص شده با نام milad می گردد.

برنامه editcap

از برنامه editcap برای انجام عملیات های اضافی بر روی فایل ضبط شده از قبیل تصحیح خطا، و فیلتر و... استفاده می شود. برای مشاهده پارامتر های گوناگون این برنامه کافیست دستور editcap -h را اجرا کنید. به شکل زیر:

```
C:\Program Files\Wireshark>editcap -d capture.pcap capture1.pcap 1
```

100

Add_Selected: 1

Not inclusive ... 1

Add_Selected: 100

Not inclusive ... 100

100 packets seen, 0 packets skipped with duplicate window of 5 packets.

فرمانی که مشاهده می کنید، بسته هایی را که در محدوده 1 تا 100 در فایل capture.pcap دو بار تکرار شده اند را حذف می کند و سپس تغییرات اعمال شده بر روی فایل را با نام جدید capture1.pcap ذخیره می کند.

برنامه mergcap

برنامه mergcap برای ادغام دو یا بیش از دو فایل ضبط بسته های اطلاعاتی در یک فایل مورد استفاده قرار می گیرد. برنامه mergcap گزینه هایی برای الحاق و کوتاه کردن فایل های ضبط بسته ها ارائه می دهد. یک فرمان ساده از mergcap که دو فایل pcap را با هم الحاق می کند در زیر آورده شده است.

```
C:\Program Files\Wireshark>text2pcap -o h text.txt converted.pcap
```

Input from: text.txt

Output to: converted.pcap

Wrote packet of 37 bytes at 0

Wrote packet of 37 bytes at 37

Read 2 potential packets, wrote 2 packets

این یک نمایش ساده از ابزار های تحت خط فرمان برنامه Wireshark بود. البته اگر توجه کرده باشید، متوجه شده اید که تمامی این قابلیت ها در فضای گرافیکی برنامه Wireshark به شما ارائه می شود. امیدوارم این راهنما براتون مفید واقع شده باشد.

4 شهریور ۱۳۹۲