Welcome to OzBerry Chatswood

Wireshark 101

Very Basic Introduction to Packets and Wireshark

ozberry Meetup

Phil Storey

7 Dec 2019

Agenda

- What are Packets
- What is Wireshark and a little history
- Why would I use Wireshark
- Capturing, displaying and filtering
- Live capture and analysis

As usual → Interrupt and ask questions along the way

What are Packets?

- A network packet is a formatted unit of data carried by a packet-switched network.
- A packet consists of control information and user data, which is also known as the payload.
- Control information provides data for delivering the payload, for example: source and destination network addresses, error detection codes, and sequencing information.
- Typically, control information is found in packet headers and trailers.
- In packet switching, the bandwidth of the communication medium is shared between multiple communication sessions.

https://en.wikipedia.org/wiki/Network_packet

History

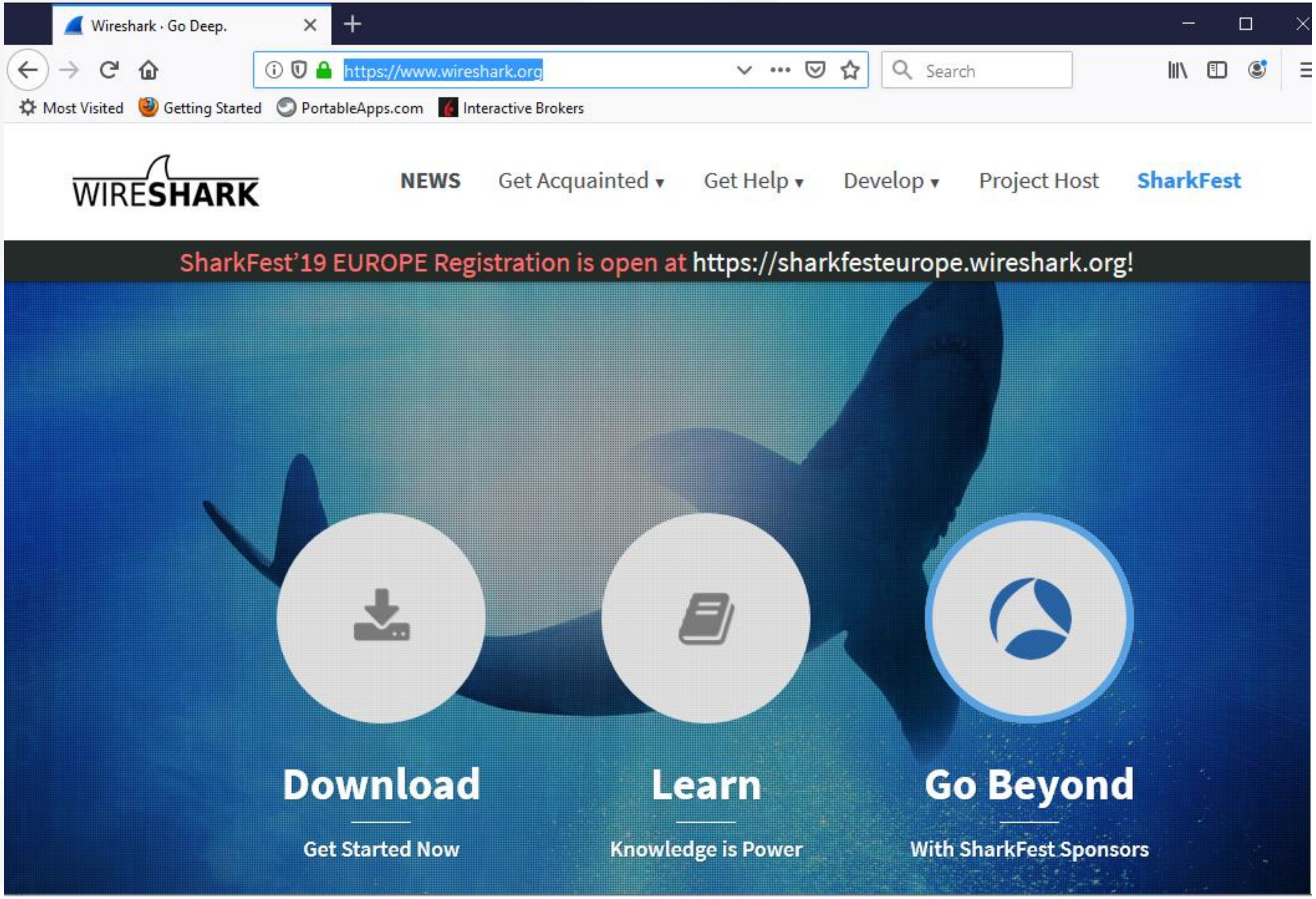
- Invented by Gerald Combs in 1998 and called “Ethereal”.
- Re-named “Wireshark” as the “Ethereal” name trademarked by someone else.
- Enormous community support and patches.
- Widely accepted as the de facto network protocol analyzer available today.
- An open source software project, released under the GNU General Public License (GPL).
- Currently sponsored by Riverbed.
- Website lists over 600 contributing authors.
- Annual “SharkFest” conferences in USA and Europe.

https://en.wikipedia.org/wiki/Wireshark

Wireshark Official Website

- Note the ".org"
- The "Download" page offers various executables as well as the source code.
- There is lots of online help available.
- The "SharkFest" links contain an enormous volume of videos and presentation papers from many Wireshark experts.

https://www.wireshark.org/

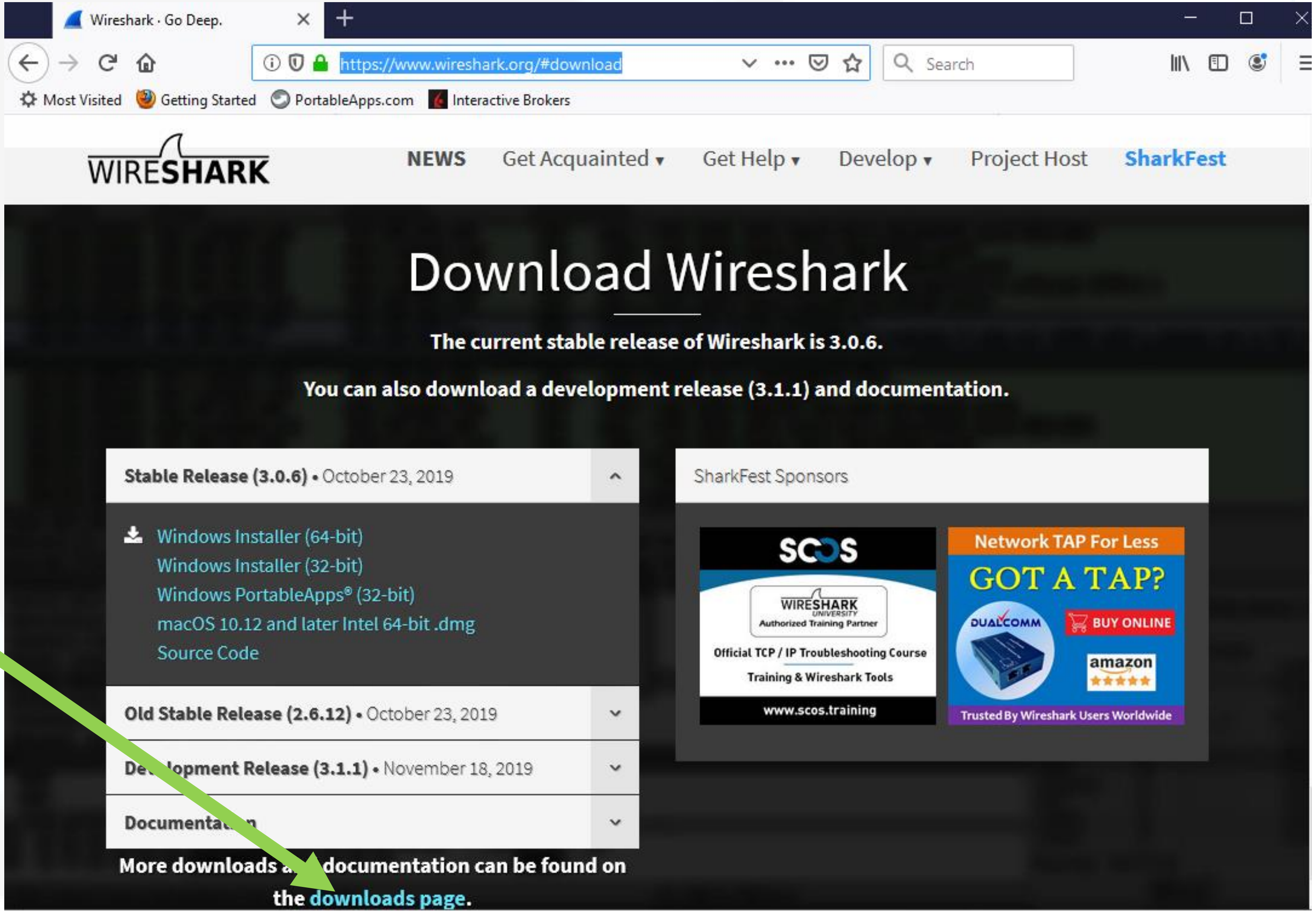


SharkFest'19 EUROPE Registration is open at https://sharkfesteurope.wireshark.org!

Wireshark Official Website - Download

- The deeper “downloads” page offers links to installation versions for several Linux variants (from the websites of the various distributions)
- Which one for Raspberry Pi?

https://www.wireshark.org/#download



Download Wireshark

The current stable release of Wireshark is 3.0.6.

You can also download a development release (3.1.1) and documentation.

Stable Release (3.0.6) • October 23, 2019

- Windows Installer (64-bit)
- Windows Installer (32-bit)
- Windows PortableApps® (32-bit)
- macOS 10.12 and later Intel 64-bit .dmg
- Source Code

Old Stable Release (2.6.12) • October 23, 2019

Development Release (3.1.1) • November 18, 2019

Documentation

More downloads and documentation can be found on the downloads page.

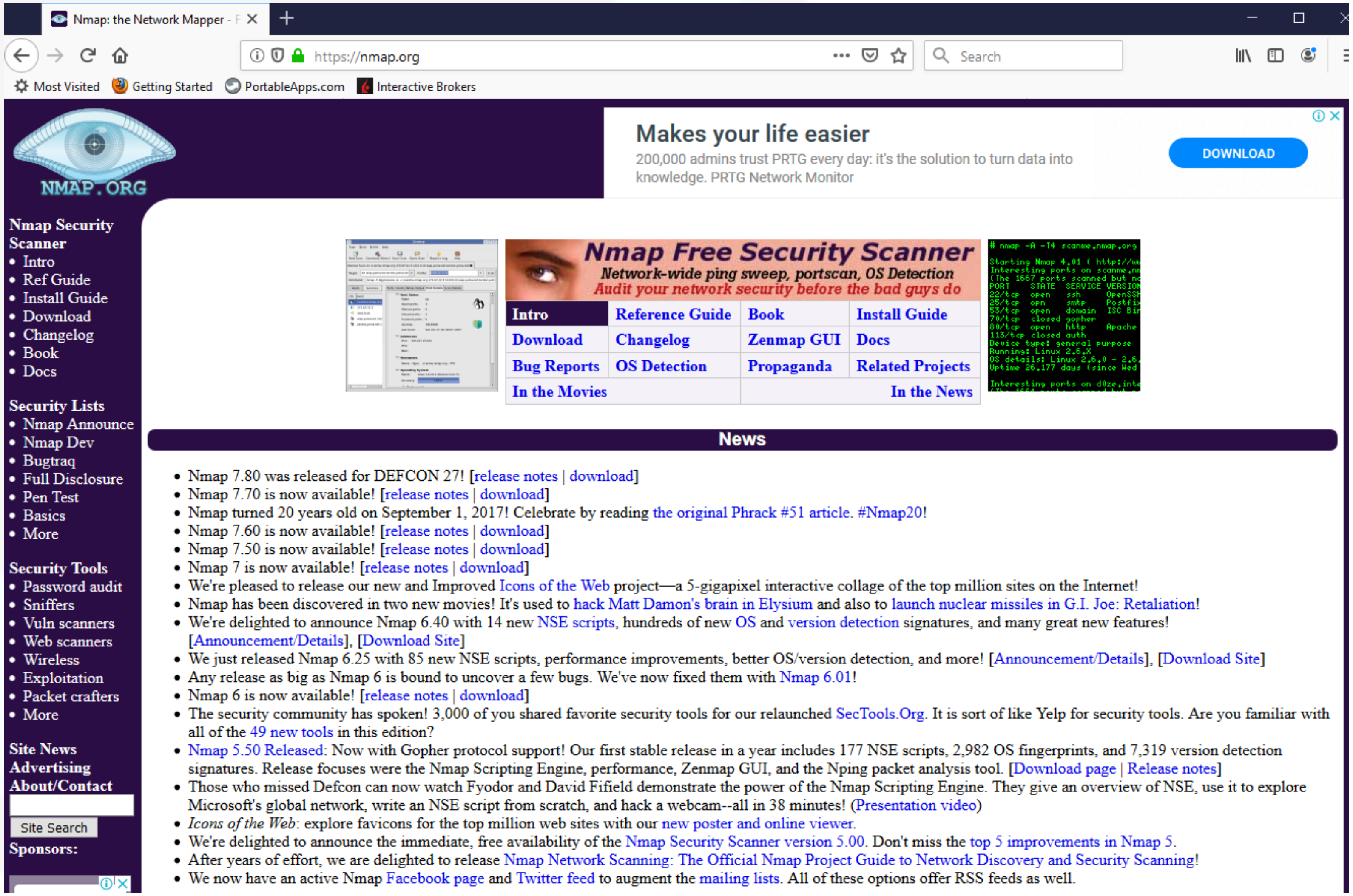
SharkFest Sponsors

SCOS
WIRESHARK UNIVERSITY Authorized Training Partner
Official TCP / IP Troubleshooting Course
Training & Wireshark Tools
www.scos.training
Network TAP For Less
GOT A TAP?
DUALCOMM
BUY ONLINE
amazon
Trusted By Wireshark Users Worldwide

Nmap Official Website

- Wireshark used to use (and still mentions on their website) a driver called, “WinPCAP”, to perform the packet capture within Windows.
- This was recently superseded by a more modern and still actively updated driver, “Nmap”.
- For Windows, you don’t need to get the Nmap driver yourself – it is included with the Wireshark Windows installer.
- There is also an optional USBcap driver.

https://nmap.org/



Nmap Security Scanner
- Intro
- Ref Guide
- Install Guide
- Download
- Changelog
- Book
- Docs

Security Lists
- Nmap Announce
- Nmap Dev
- Bugtraq
- Full Disclosure
- Pen Test
- Basics
- More

Security Tools
- Password audit
- Sniffers
- Vuln scanners
- Web scanners
- Wireless
- Exploitation
- Packet crafters
- More

Site News
Advertising
About/Contact

Site Search

Sponsors:

Nmap Free Security Scanner
Network-wide ping sweep, portscan, OS Detection
Audit your network security before the bad guys do

Intro	Reference Guide	Book	Install Guide
Download	Changelog	Zenmap GUI	Docs
Bug Reports	OS Detection	Propaganda	Related Projects
In the Movies			In the News

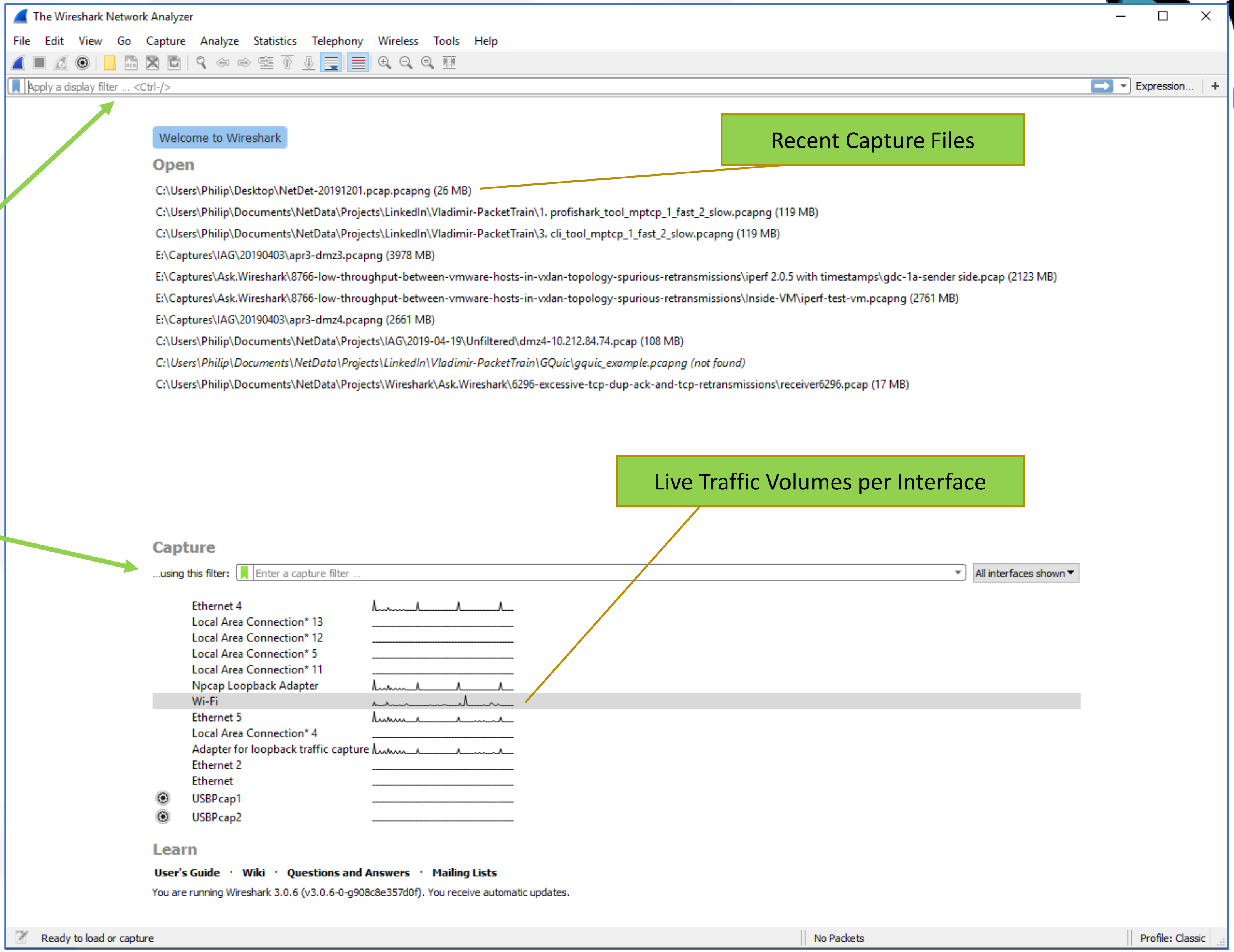
```
# nmap -A -T4 scanme.nmap.org

Starting Nmap 4.01 ( http://ww
Interesting ports on scanme.nm
(The 1667 ports scanned but no
PORT    STATE  SERVICE VERSION
22/tcp  open   ssh     OpenSSH
25/tcp  opn    smtp    Postfix
53/tcp  open   domain  ISC Bin
70/tcp  closed gopher
80/tcp  open   http    Apache
113/tcp closed auth
Device type: general purpose
Running: Linux 2.6.X
OS details: Linux 2.6.0 - 2.6.
Uptime 26.177 days (since Wed

Interesting ports on d0ze.inte
```

News

- Nmap 7.80 was released for DEFCON 27! [release notes | download]
- Nmap 7.70 is now available! [release notes | download]
- Nmap turned 20 years old on September 1, 2017! Celebrate by reading the original Phrack #51 article. #Nmap20!
- Nmap 7.60 is now available! [release notes | download]
- Nmap 7.50 is now available! [release notes | download]
- Nmap 7 is now available! [release notes | download]
- We're pleased to release our new and Improved Icons of the Web project—a 5-gigapixel interactive collage of the top million sites on the Internet!
- Nmap has been discovered in two new movies! It's used to hack Matt Damon's brain in Elysium and also to launch nuclear missiles in G.I. Joe: Retaliation!
- We're delighted to announce Nmap 6.40 with 14 new NSE scripts, hundreds of new OS and version detection signatures, and many great new features! [Announcement/Details], [Download Site]
- We just released Nmap 6.25 with 85 new NSE scripts, performance improvements, better OS/version detection, and more! [Announcement/Details], [Download Site]
- Any release as big as Nmap 6 is bound to uncover a few bugs. We've now fixed them with Nmap 6.01!
- Nmap 6 is now available! [release notes | download]
- The security community has spoken! 3,000 of you shared favorite security tools for our relaunched SecTools.Org. It is sort of like Yelp for security tools. Are you familiar with all of the 49 new tools in this edition?
- Nmap 5.50 Released: Now with Gopher protocol support! Our first stable release in a year includes 177 NSE scripts, 2,982 OS fingerprints, and 7,319 version detection signatures. Release focuses were the Nmap Scripting Engine, performance, Zenmap GUI, and the Nping packet analysis tool. [Download page | Release notes]
- Those who missed Defcon can now watch Fyodor and David Fifield demonstrate the power of the Nmap Scripting Engine. They give an overview of NSE, use it to explore Microsoft's global network, write an NSE script from scratch, and hack a webcam--all in 38 minutes! (Presentation video)
- *Icons of the Web*: explore favicons for the top million web sites with our new poster and online viewer.
- We're delighted to announce the immediate, free availability of the Nmap Security Scanner version 5.00. Don't miss the top 5 improvements in Nmap 5.
- After years of effort, we are delighted to release Nmap Network Scanning: The Official Nmap Project Guide to Network Discovery and Security Scanning!
- We now have an active Nmap Facebook page and Twitter feed to augment the mailing lists. All of these options offer RSS feeds as well.

Wireshark Initial Display

- Recent trace files
  - Double-click to re-open
- List of interfaces
  - Live indication of traffic on each interface
  - Double-click to start capturing on just that interface
- Display Filter Bar
- Capture Filter field



Recent Capture Files

C:\Users\Philip\Desktop\NetDet-20191201.pcap.pcapng (26 MB)
C:\Users\Philip\Documents\NetData\Projects\LinkedIn\Vladimir-PacketTrain\1. profishark_tool_mptcp_1_fast_2_slow.pcapng (119 MB)
C:\Users\Philip\Documents\NetData\Projects\LinkedIn\Vladimir-PacketTrain\3. cli_tool_mptcp_1_fast_2_slow.pcapng (119 MB)
E:\Captures\IAG\20190403\apr3-dmz3.pcapng (3978 MB)
E:\Captures\Ask.Wireshark\8766-low-throughput-between-vmware-hosts-in-vxlan-topology-spurious-retransmissions\iperf 2.0.5 with timestamps\gdc-1a-sender side.pcap (2123 MB)
E:\Captures\Ask.Wireshark\8766-low-throughput-between-vmware-hosts-in-vxlan-topology-spurious-retransmissions\Inside-VM\iperf-test-vm.pcapng (2761 MB)
E:\Captures\IAG\20190403\apr3-dmz4.pcapng (2661 MB)
C:\Users\Philip\Documents\NetData\Projects\IAG\2019-04-19\Unfiltered\dmz4-10.212.84.74.pcap (108 MB)
C:\Users\Philip\Documents\NetData\Projects\LinkedIn\Vladimir-PacketTrain\GQuic\gquic_example.pcapng (not found)
C:\Users\Philip\Documents\NetData\Projects\Wireshark\Ask.Wireshark\6296-excessive-tcp-dup-ack-and-tcp-retransmissions\receiver6296.pcap (17 MB)

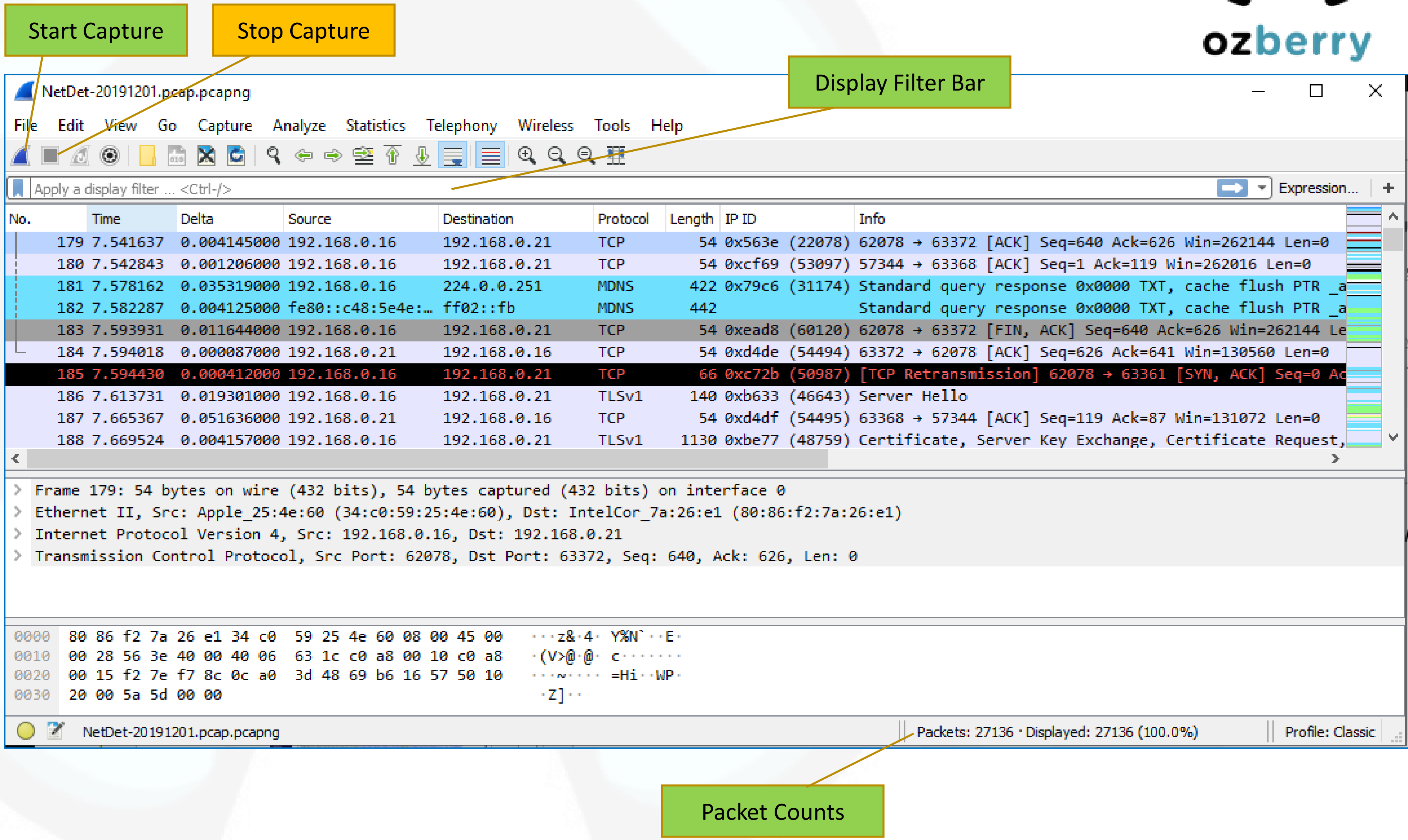
Live Traffic Volumes per Interface

Ethernet 4
Local Area Connection* 13
Local Area Connection* 12
Local Area Connection* 5
Local Area Connection* 11
Npcap Loopback Adapter
Wi-Fi
Ethernet 5
Local Area Connection* 4
Adapter for loopback traffic capture
Ethernet 2
Ethernet
USBPcap1
USBPcap2

You are running Wireshark 3.0.6 (v3.0.6-0-g908c8e357d0f). You receive automatic updates.

Wireshark Display

- Menu options
  - File
  - Edit
  - Capture
  - Analyze
- Buttons
  - Start
  - Stop
- Display Filter Bar
- Panes
  - Packet List
  - Packet Details
  - Packet Bytes
- Colours



Start Capture

Stop Capture

Display Filter Bar

Packet Counts

```
No.     Time     Delta       Source            Destination    Protocol Length IP ID          Info
    179 7.541637 0.004145000 192.168.0.16      192.168.0.21   TCP         54 0x563e (22078) 62078 → 63372 [ACK] Seq=640 Ack=626 Win=262144 Len=0
    180 7.542843 0.001206000 192.168.0.16      192.168.0.21   TCP         54 0xcf69 (53097) 57344 → 63368 [ACK] Seq=1 Ack=119 Win=262016 Len=0
    181 7.578162 0.035319000 192.168.0.16      224.0.0.251    MDNS       422 0x79c6 (31174) Standard query response 0x0000 TXT, cache flush PTR _a
    182 7.582287 0.004125000 fe80::c48:5e4e:…  ff02::fb       MDNS       442                Standard query response 0x0000 TXT, cache flush PTR _a
    183 7.593931 0.011644000 192.168.0.16      192.168.0.21   TCP         54 0xead8 (60120) 62078 → 63372 [FIN, ACK] Seq=640 Ack=626 Win=262144 Le
    184 7.594018 0.000087000 192.168.0.21      192.168.0.16   TCP         54 0xd4de (54494) 63372 → 62078 [ACK] Seq=626 Ack=641 Win=130560 Len=0
    185 7.594430 0.000412000 192.168.0.16      192.168.0.21   TCP         66 0xc72b (50987) [TCP Retransmission] 62078 → 63361 [SYN, ACK] Seq=0 Ac
    186 7.613731 0.019301000 192.168.0.16      192.168.0.21   TLSv1      140 0xb633 (46643) Server Hello
    187 7.665367 0.051636000 192.168.0.21      192.168.0.16   TCP         54 0xd4df (54495) 63368 → 57344 [ACK] Seq=119 Ack=87 Win=131072 Len=0
    188 7.669524 0.004157000 192.168.0.16      192.168.0.21   TLSv1     1130 0xbe77 (48759) Certificate, Server Key Exchange, Certificate Request,
```

```
> Frame 179: 54 bytes on wire (432 bits), 54 bytes captured (432 bits) on interface 0
> Ethernet II, Src: Apple_25:4e:60 (34:c0:59:25:4e:60), Dst: IntelCor_7a:26:e1 (80:86:f2:7a:26:e1)
> Internet Protocol Version 4, Src: 192.168.0.16, Dst: 192.168.0.21
> Transmission Control Protocol, Src Port: 62078, Dst Port: 63372, Seq: 640, Ack: 626, Len: 0
```

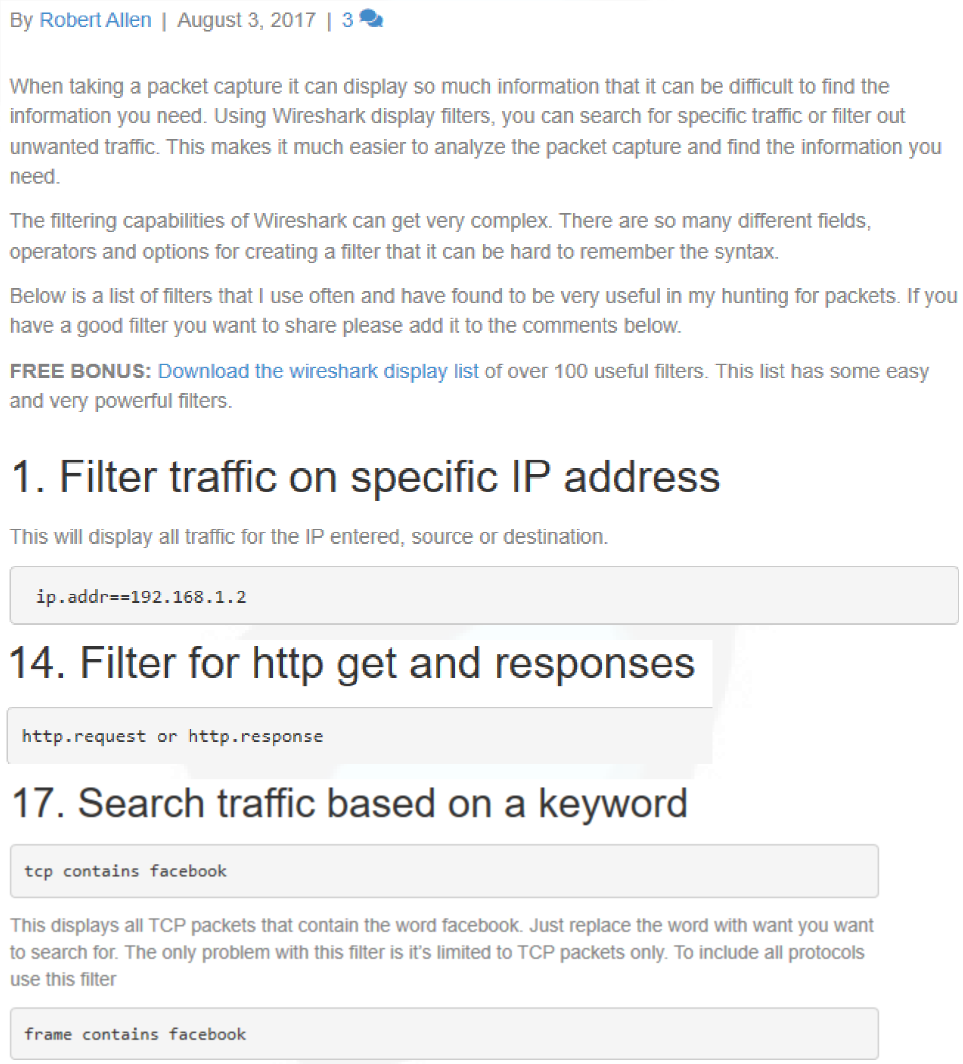
```
0000  80 86 f2 7a 26 e1 34 c0  59 25 4e 60 08 00 45 00   ···z&·4· Y%N`··E·
0010  00 28 56 3e 40 00 40 06  63 1c c0 a8 00 10 c0 a8   ·(V>@·@· c·······
0020  00 15 f2 7e f7 8c 0c a0  3d 48 69 b6 16 57 50 10   ···~···· =Hi··WP·
0030  20 00 5a 5d 00 00                                   ·Z]··
```

NetDet-20191201.pcap.pcapng | Packets: 27136 · Displayed: 27136 (100.0%) | Profile: Classic

Wireshark Display Filters

- Use these to “drill-down” into the capture.
- Syntax is different to “Capture Filters”.
- Capture filters are used to filter out packets during the capture phase (so that the “pcap” files are smaller).

https://networksecuritytools.com/list-wireshark-display-filters/



By Robert Allen | August 3, 2017 | 3

When taking a packet capture it can display so much information that it can be difficult to find the information you need. Using Wireshark display filters, you can search for specific traffic or filter out unwanted traffic. This makes it much easier to analyze the packet capture and find the information you need.

The filtering capabilities of Wireshark can get very complex. There are so many different fields, operators and options for creating a filter that it can be hard to remember the syntax.

Below is a list of filters that I use often and have found to be very useful in my hunting for packets. If you have a good filter you want to share please add it to the comments below.

FREE BONUS: Download the wireshark display list of over 100 useful filters. This list has some easy and very powerful filters.

1. Filter traffic on specific IP address

This will display all traffic for the IP entered, source or destination.

```
ip.addr==192.168.1.2
```

14. Filter for http get and responses

```
http.request or http.response
```

17. Search traffic based on a keyword

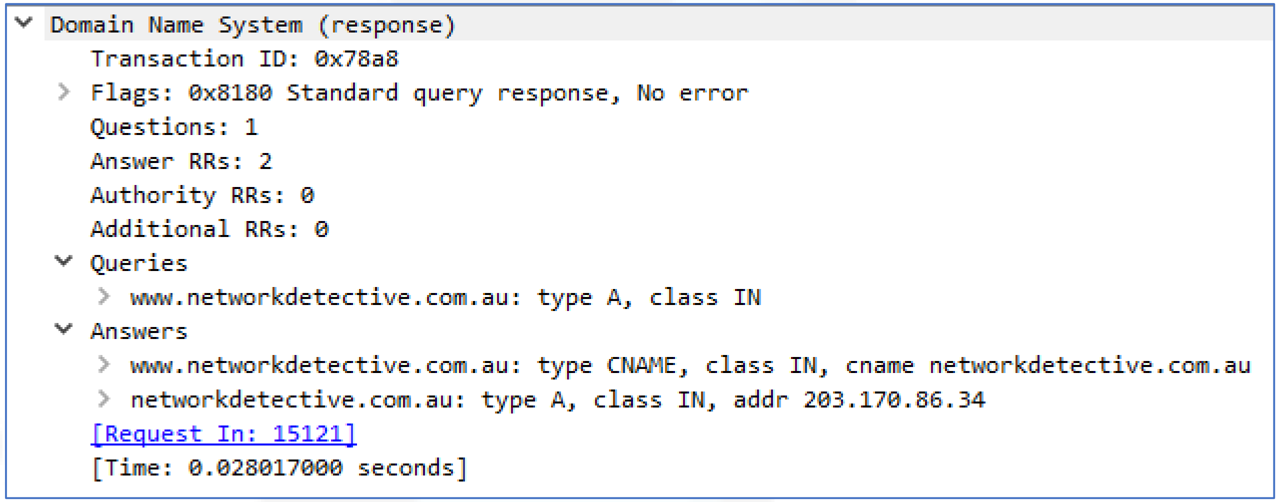
```
tcp contains facebook
```

This displays all TCP packets that contain the word facebook. Just replace the word with want you want to search for. The only problem with this filter is it's limited to TCP packets only. To include all protocols use this filter

```
frame contains facebook
```

DNS: Statistics – Resolved Addresses

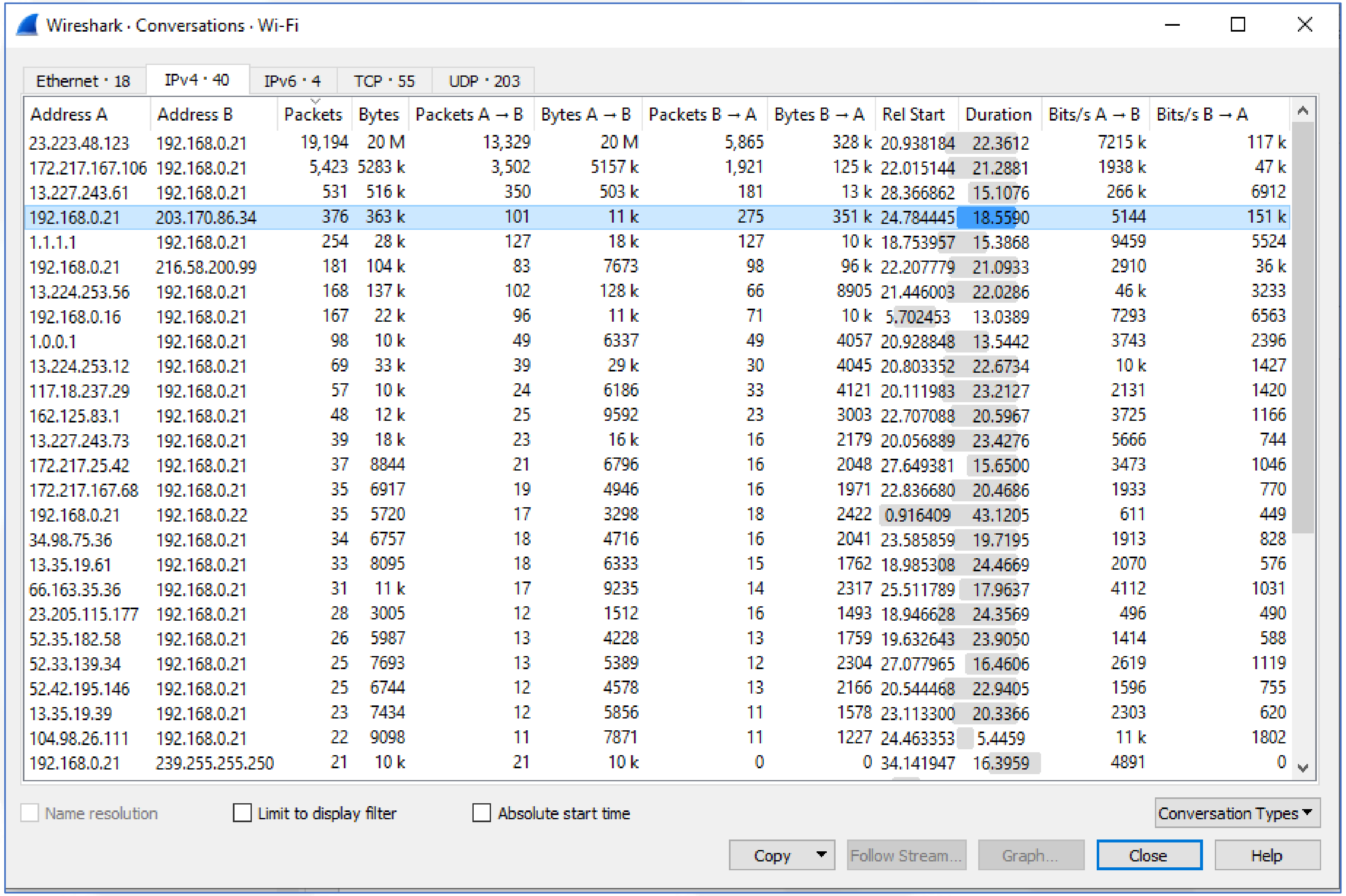
```
# Resolved addresses found in C:\Users\Philip\AppData\Local\Temp\wireshark_Wi-Fi_20191201161525_a17780.pcapng

# Comments

# No entries.

# Hosts

# 134 entries.
35.164.109.147    search.r53-2.services.mozilla.com
103.225.160.40    www.ulyssesclub.org
172.217.167.106   safebrowsing.googleapis.com
45.60.67.17       nvwxfl7.x.incapdns.net
52.33.139.34      shavar.prod.mozaws.net
35.155.241.126    shavar.prod.mozaws.net
104.98.26.111     e13569.x.akamaiedge.net
13.35.19.60       d6wjo2hisqfy2.cloudfront.net
162.125.83.1      www.dropbox-dns.com
35.167.176.219    bouncer-bouncer-elb.prod.mozaws.net
13.224.253.56     d2k03kvdk5cku0.cloudfront.net
13.224.253.29     d228z91au11ukj.cloudfront.net
144.2.0.1         pop-esy1-alpha.www.linkedin.com
203.170.86.34     networkdetective.com.au
104.16.143.228    www.mozilla.org.cdn.cloudflare.net
13.224.253.39     d2k03kvdk5cku0.cloudfront.net
52.89.48.8        shavar.prod.mozaws.net
52.33.61.229      shavar.prod.mozaws.net
216.58.199.78     youtube-ui.l.google.com
13.224.253.12     d228z91au11ukj.cloudfront.net
13.55.165.210     orders.motzapizza.com.au
172.217.25.46     youtube-ui.l.google.com
172.217.25.142    youtube-ui.l.google.com
172.217.25.174    youtube-ui.l.google.com
```



```
v Domain Name System (response)
    Transaction ID: 0x78a8
  > Flags: 0x8180 Standard query response, No error
    Questions: 1
    Answer RRs: 2
    Authority RRs: 0
    Additional RRs: 0
  v Queries
    > www.networkdetective.com.au: type A, class IN
  v Answers
    > www.networkdetective.com.au: type CNAME, class IN, cname networkdetective.com.au
    > networkdetective.com.au: type A, class IN, addr 203.170.86.34
    [Request In: 15121]
    [Time: 0.028017000 seconds]
```

Statistics - Conversations

- Note the various tabs
- Click on Headings to sort (here is sorted by "Packets")
- "IPv4" is likely to be the most interesting for now



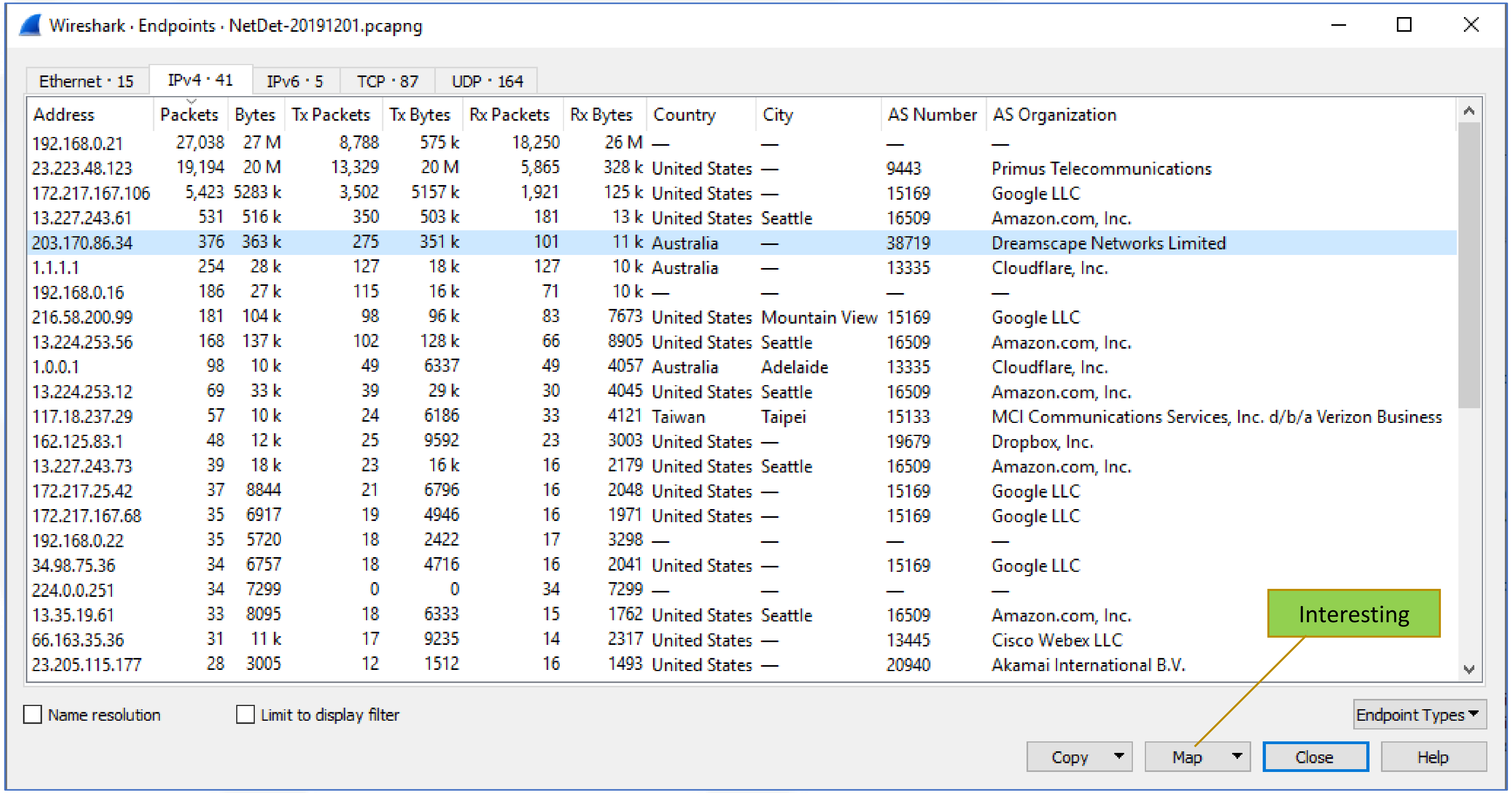
Address A	Address B	Packets	Bytes	Packets A → B	Bytes A → B	Packets B → A	Bytes B → A	Rel Start	Duration	Bits/s A → B	Bits/s B → A
23.223.48.123	192.168.0.21	19,194	20 M	13,329	20 M	5,865	328 k	20.938184	22.3612	7215 k	117 k
172.217.167.106	192.168.0.21	5,423	5283 k	3,502	5157 k	1,921	125 k	22.015144	21.2881	1938 k	47 k
13.227.243.61	192.168.0.21	531	516 k	350	503 k	181	13 k	28.366862	15.1076	266 k	6912
192.168.0.21	203.170.86.34	376	363 k	101	11 k	275	351 k	24.784445	18.5590	5144	151 k
1.1.1.1	192.168.0.21	254	28 k	127	18 k	127	10 k	18.753957	15.3868	9459	5524
192.168.0.21	216.58.200.99	181	104 k	83	7673	98	96 k	22.207779	21.0933	2910	36 k
13.224.253.56	192.168.0.21	168	137 k	102	128 k	66	8905	21.446003	22.0286	46 k	3233
192.168.0.16	192.168.0.21	167	22 k	96	11 k	71	10 k	5.702453	13.0389	7293	6563
1.0.0.1	192.168.0.21	98	10 k	49	6337	49	4057	20.928848	13.5442	3743	2396
13.224.253.12	192.168.0.21	69	33 k	39	29 k	30	4045	20.803352	22.6734	10 k	1427
117.18.237.29	192.168.0.21	57	10 k	24	6186	33	4121	20.111983	23.2127	2131	1420
162.125.83.1	192.168.0.21	48	12 k	25	9592	23	3003	22.707088	20.5967	3725	1166
13.227.243.73	192.168.0.21	39	18 k	23	16 k	16	2179	20.056889	23.4276	5666	744
172.217.25.42	192.168.0.21	37	8844	21	6796	16	2048	27.649381	15.6500	3473	1046
172.217.167.68	192.168.0.21	35	6917	19	4946	16	1971	22.836680	20.4686	1933	770
192.168.0.21	192.168.0.22	35	5720	17	3298	18	2422	0.916409	43.1205	611	449
34.98.75.36	192.168.0.21	34	6757	18	4716	16	2041	23.585859	19.7195	1913	828
13.35.19.61	192.168.0.21	33	8095	18	6333	15	1762	18.985308	24.4669	2070	576
66.163.35.36	192.168.0.21	31	11 k	17	9235	14	2317	25.511789	17.9637	4112	1031
23.205.115.177	192.168.0.21	28	3005	12	1512	16	1493	18.946628	24.3569	496	490
52.35.182.58	192.168.0.21	26	5987	13	4228	13	1759	19.632643	23.9050	1414	588
52.33.139.34	192.168.0.21	25	7693	13	5389	12	2304	27.077965	16.4606	2619	1119
52.42.195.146	192.168.0.21	25	6744	12	4578	13	2166	20.544468	22.9405	1596	755
13.35.19.39	192.168.0.21	23	7434	12	5856	11	1578	23.113300	20.3366	2303	620
104.98.26.111	192.168.0.21	22	9098	11	7871	11	1227	24.463353	5.4459	11 k	1802
192.168.0.21	239.255.255.250	21	10 k	21	10 k	0	0	34.141947	16.3959	4891	0

□ Name resolution □ Limit to display filter □ Absolute start time

Statistics - Endpoints

- Click on Headings to sort (here is sorted by “Packets”)
- “IPv4” is likely to be the most interesting for now
- The Geolocation information is a new feature. It needs an external set of data files that can be downloaded for free.

  https://dev.maxmind.com/geoip/geoip2/geolite2/



Wireshark · Endpoints · NetDet-20191201.pcapng

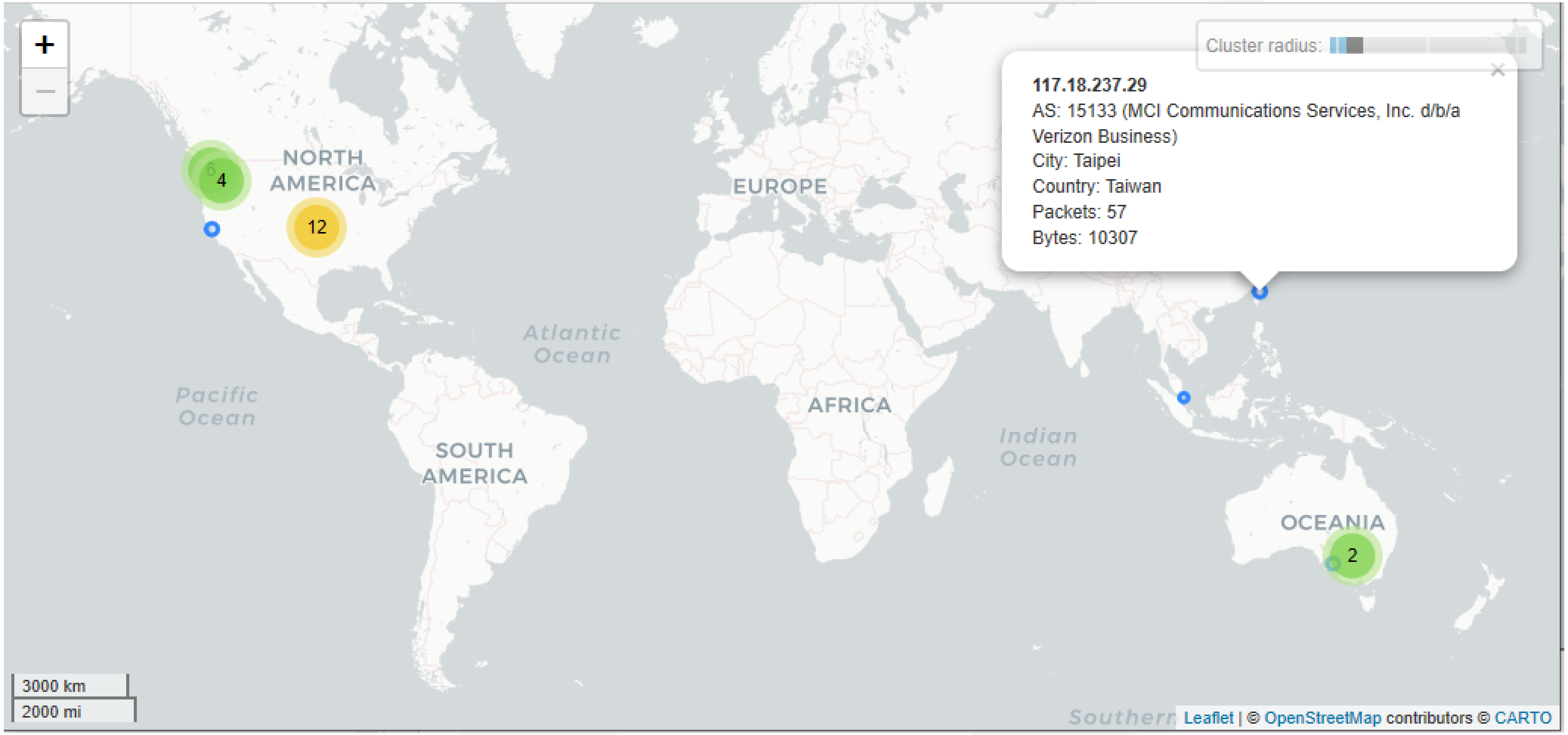
Address	Packets	Bytes	Tx Packets	Tx Bytes	Rx Packets	Rx Bytes	Country	City	AS Number	AS Organization
192.168.0.21	27,038	27 M	8,788	575 k	18,250	26 M	—	—	—	—
23.223.48.123	19,194	20 M	13,329	20 M	5,865	328 k	United States	—	9443	Primus Telecommunications
172.217.167.106	5,423	5283 k	3,502	5157 k	1,921	125 k	United States	—	15169	Google LLC
13.227.243.61	531	516 k	350	503 k	181	13 k	United States	Seattle	16509	Amazon.com, Inc.
203.170.86.34	376	363 k	275	351 k	101	11 k	Australia	—	38719	Dreamscape Networks Limited
1.1.1.1	254	28 k	127	18 k	127	10 k	Australia	—	13335	Cloudflare, Inc.
192.168.0.16	186	27 k	115	16 k	71	10 k	—	—	—	—
216.58.200.99	181	104 k	98	96 k	83	7673	United States	Mountain View	15169	Google LLC
13.224.253.56	168	137 k	102	128 k	66	8905	United States	Seattle	16509	Amazon.com, Inc.
1.0.0.1	98	10 k	49	6337	49	4057	Australia	Adelaide	13335	Cloudflare, Inc.
13.224.253.12	69	33 k	39	29 k	30	4045	United States	Seattle	16509	Amazon.com, Inc.
117.18.237.29	57	10 k	24	6186	33	4121	Taiwan	Taipei	15133	MCI Communications Services, Inc. d/b/a Verizon Business
162.125.83.1	48	12 k	25	9592	23	3003	United States	—	19679	Dropbox, Inc.
13.227.243.73	39	18 k	23	16 k	16	2179	United States	Seattle	16509	Amazon.com, Inc.
172.217.25.42	37	8844	21	6796	16	2048	United States	—	15169	Google LLC
172.217.167.68	35	6917	19	4946	16	1971	United States	—	15169	Google LLC
192.168.0.22	35	5720	18	2422	17	3298	—	—	—	—
34.98.75.36	34	6757	18	4716	16	2041	United States	—	15169	Google LLC
224.0.0.251	34	7299	0	0	34	7299	—	—	—	—
13.35.19.61	33	8095	18	6333	15	1762	United States	Seattle	16509	Amazon.com, Inc.
66.163.35.36	31	11 k	17	9235	14	2317	United States	—	13445	Cisco Webex LLC
23.205.115.177	28	3005	12	1512	16	1493	United States	—	20940	Akamai International B.V.

☐ Name resolution ☐ Limit to display filter

Interesting

Statistics – Endpoints: Map

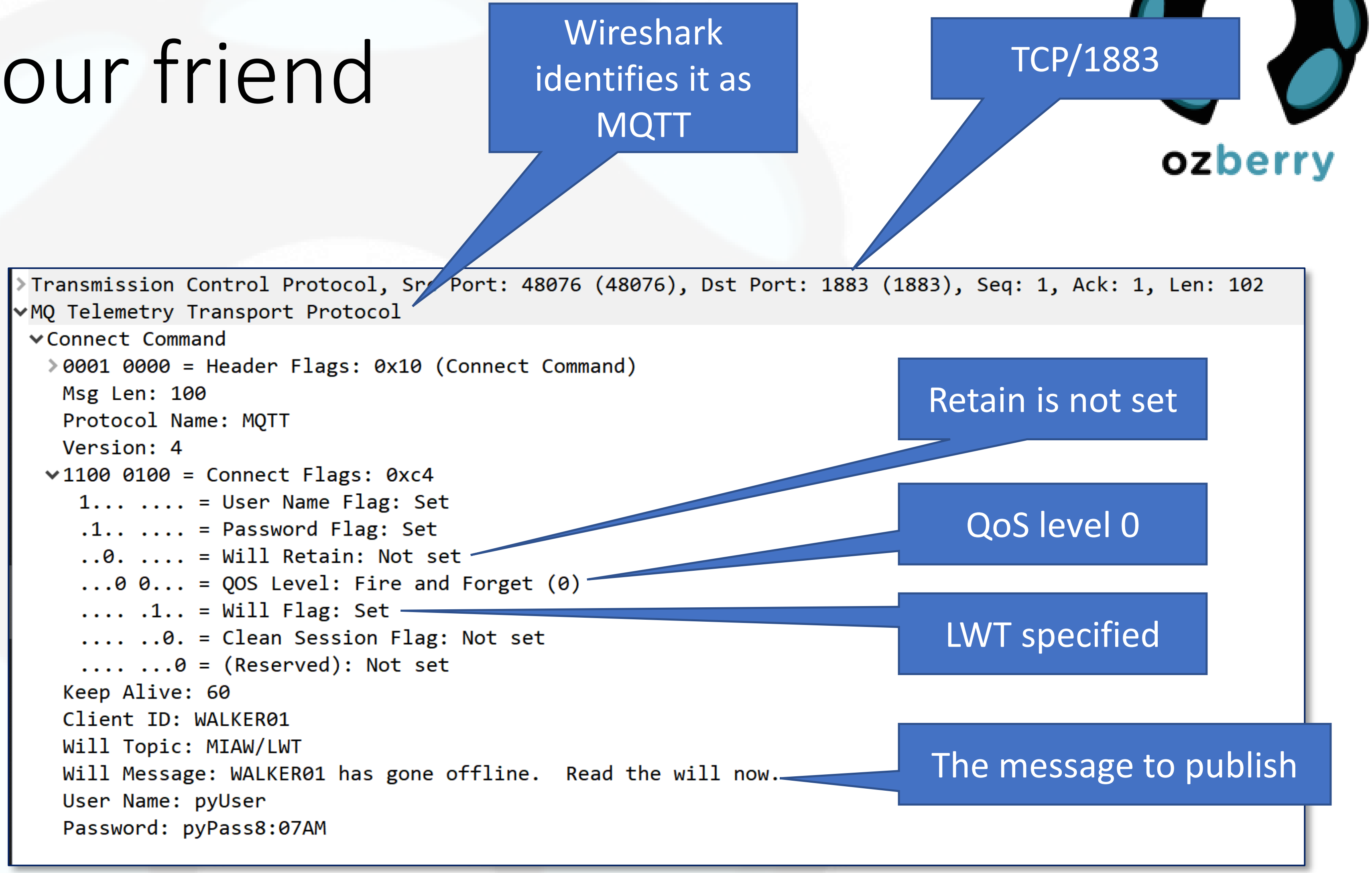
- The map is zoomable and hovering the cursor pops-up the underlying IP address.



117.18.237.29
AS: 15133 (MCI Communications Services, Inc. d/b/a Verizon Business)
City: Taipei
Country: Taiwan
Packets: 57
Bytes: 10307

Wireshark is your friend

- This shows a connect message with LWT specified
- If you have problems with any kind of network connection try Wireshark to capture the traffic



```
> Transmission Control Protocol, Src Port: 48076 (48076), Dst Port: 1883 (1883), Seq: 1, Ack: 1, Len: 102
v MQ Telemetry Transport Protocol
  v Connect Command
    > 0001 0000 = Header Flags: 0x10 (Connect Command)
      Msg Len: 100
      Protocol Name: MQTT
      Version: 4
    v 1100 0100 = Connect Flags: 0xc4
        1... .... = User Name Flag: Set
        .1.. .... = Password Flag: Set
        ..0. .... = Will Retain: Not set
        ...0 0... = QOS Level: Fire and Forget (0)
        .... .1.. = Will Flag: Set
        .... ..0. = Clean Session Flag: Not set
        .... ...0 = (Reserved): Not set
      Keep Alive: 60
      Client ID: WALKER01
      Will Topic: MIAW/LWT
      Will Message: WALKER01 has gone offline.  Read the will now.
      User Name: pyUser
      Password: pyPass8:07AM
```

Wireshark identifies it as MQTT

TCP/1883

Retain is not set

QoS level 0

LWT specified

The message to publish

This slide is from Ashley's talk about MQTT.

More Information

- This is a very popular software tool so there are hundreds of sources for tips, “how to” videos, etc.

SharkFest “Retrospectives”	https://sharkfestus.wireshark.org/retrospective
Laura Chappell	https://www.chappell-university.com/
Tony Fortunato	https://www.youtube.com/channel/UCGzLX2yif2uqobtoVTLbHhQ
Jasper Bongertz	https://www.youtube.com/channel/UCZd-4IZtcbE1zM-CnOxd31A
Chris Greer	https://www.youtube.com/user/packetpioneer
Betty DuBois	https://www.youtube.com/channel/UCy4XzAs0O6UpDfGOHiPshrg

- Me at a Sydney Linux User Group Meetup (very long!!)
  https://www.youtube.com/watch?v=ZZfTbZ78YVw

The Demonstration

- Launch Wireshark
- Capture some WiFi packets
- Visit www.networkdetective.com.au (non-SSL site)
- Look at the layout and packets
- Look at a few “Analyze” outputs

Phil Storey

Phil@NetworkDetective.com.au

www.NetworkDetective.com.au

au.linkedin.com/in/philipstorey3

@PhilStorey24

www.youtube.com/c/NetworkDetective

ask.wireshark.org: @philst