

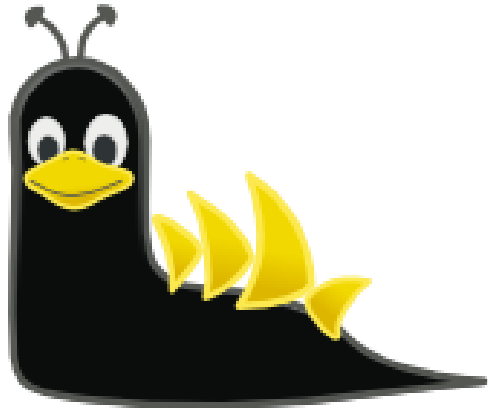


Welcome to Sydney Linux User Group

<https://slug.org.au/>

Download the Presentation PDF here:

<http://www.networkdetective.com.au/PDFs/SLUG-Meetup-Wireshark-2023-07-28.pdf>



WIRESHARK

Wireshark – Basic Introduction

SLUG Meetup

Phil Storey

28 July 2023



Agenda

The aim is to give you a quick run through of Wireshark and some features – so that you can get started on your own.

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

As usual → Interrupt and ask questions along the way





What are Packets?

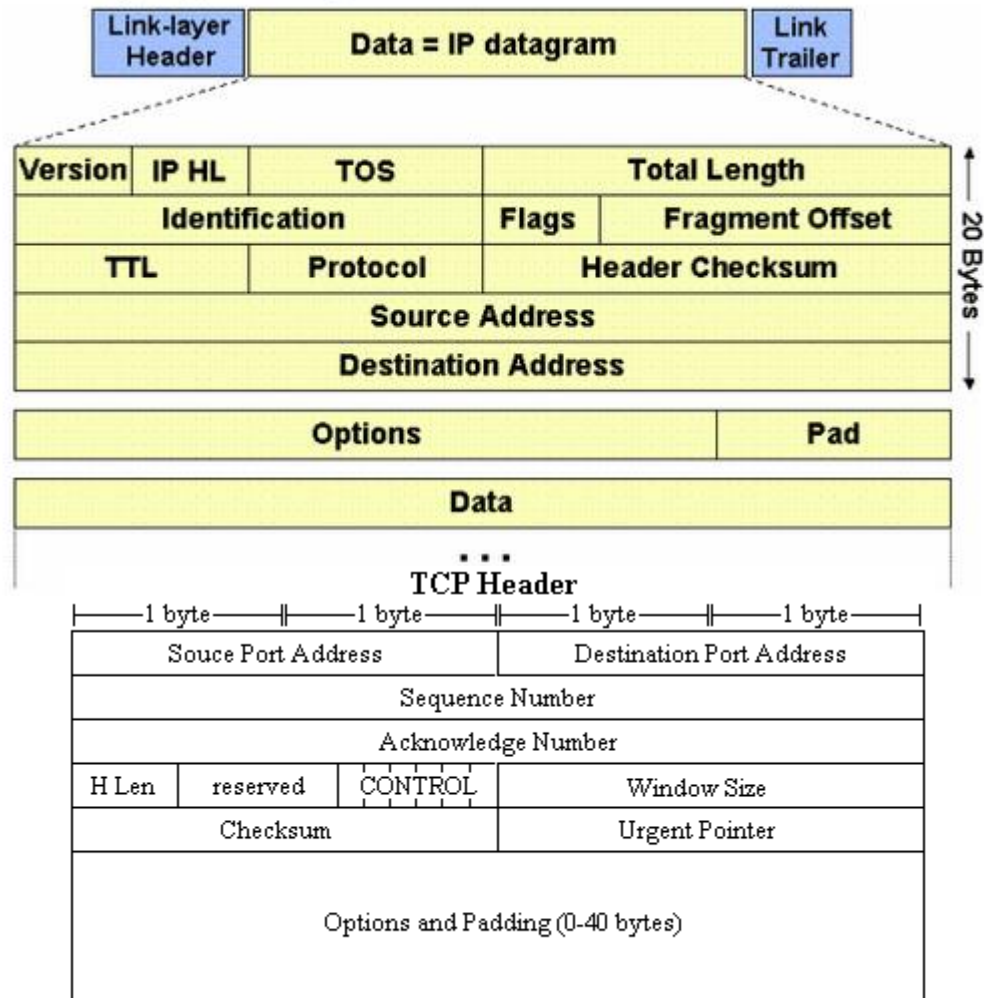
- A network packet is a formatted unit of data carried by a packet-switched network.
- A packet consists of control information and user data, which is also known as the payload.
- Control information provides data for delivering the payload, for example: source and destination network addresses, error 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://pressbooks.howardcc.edu/cmsy164/chapter/packet-analysis-ip-headers-tools-and-notes/>
https://www.ardenstone.com/projects/seniorsem/reports/TCP_Protocol.html



Ethernet frame maximum size is 1500 bytes.

IP header is 20 bytes, leaving 1480 bytes for the IP data payload.



TCP header is 20-40 bytes, leaving 1440-1460 bytes for the TCP data payload.



Wireshark 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 analyser available today.
- An open source software project, released under the GNU General Public License (GPL).
- Was sponsored by Riverbed but now stands alone as a non-profit.
- Website lists over 600 contributing authors.
- Annual “SharkFest” conferences in USA and Europe (sometimes Asia).

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/>

The screenshot shows the Wireshark website homepage. At the top, a blue banner reads "We're now a non-profit! Support open source packet analysis by making a donation." with a sun icon on the right. Below the banner is a navigation menu with links: "News", "SharkFest", "Get Acquainted", "Get Help", "Develop", "Shop", and "Members". A "Donate" button is located in the top right corner. The main content area features the Wireshark logo on the left and a large blue button labeled "Download Wireshark Now" with a right-pointing arrow. Below this, the text reads "The world's most popular network protocol analyzer" and "Get started with Wireshark today and see why it is the standard across many commercial and non-profit enterprises." A "Get started" button is positioned at the bottom left of this section. On the right side, there is a video thumbnail titled "Wireshark 4.0 Overview" with a play button icon and a shark fin graphic.

Wireshark Official Website - Download



- Various installation options for Windows and Mac.
- The deeper “downloads” page offers information about versions for several Linux variants (from the websites of the various distributions).

<https://www.wireshark.org>

Download Wireshark

- ▼ Stable Release: 4.0.6
 - Windows Intel Installer
 - Windows Intel PortableApps®
 - macOS Arm Disk Image
 - macOS Intel Disk Image
 - </> [Source Code](#)
- ▶ Old Stable Release: 3.6.14
- ▶ [Documentation](#)

More downloads and documentation can be found on the [downloads page](#).

WIRESHARK

© Wireshark Foundation · [Privacy Policy](#)
[Facebook](#) · [Mastodon](#) · [Twitter](#) · [YouTube](#)

- Get Wireshark
- Download
- Code of Conduct
- Get Help
- Ask a Question
- FAQs
- Documentation

- Contribute
- Developer's Guide
- Browse the Code
- Authors
- Members
- Donate
- Learn

Wireshark Official Website - Download



https://www.wireshark.org/docs/wsug_html_chunked/ChBuildInstallUnixInstallBins.html#installing_from_rpms_under_red_hat_and_alike

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

2.6.2. Installing from debs under Debian, Ubuntu and other Debian derivatives

If you can just install from the repository then use

apt install wireshark

Apt should take care of all of the dependency issues for you.

[Note] Capturing requires privileges

By installing Wireshark packages non-root, users won't gain rights automatically to capture packets. To allow non-root users to capture packets follow the procedure described in <https://gitlab.com/wireshark/wireshark/-/blob/master/packaging/debian/README.Debian> (/usr/share/doc/wireshark-common/README.Debian.gz)

Third-Party Packages	
Wireshark packages are available for most platforms, including the ones listed below.	
Standard package: Wireshark is available via the default packaging system on that platform.	
Vendor / Platform	Sources
Alpine / Alpine Linux	Standard package
Apple / macOS	Homebrew cask (includes UI) Homebrew formula (CLI only) MacPorts Fink
Arch Linux / Arch Linux	Standard package
Canonical / Ubuntu	Standard package Latest stable PPA
Debian / Debian GNU/Linux	Standard package
The FreeBSD Project / FreeBSD	Standard package
Gentoo Foundation / Gentoo Linux	Standard package
HP / HP-UX	Porting And Archive Centre for HP-UX
NetBSD Foundation / NetBSD	Standard package
NixOS / NixOS	Standard package
openSUSE / openSUSE	Standard package
Offensive Security / Kali Linux	Standard package
OpenPKG / OpenPKG Project	Standard package
PC-BSD Software · iXsystems / PC-BSD	Push Button Installer
PCLinuxOS / PCLinuxOS	Standard package
Red Hat / Fedora	Standard package
Red Hat / Red Hat Enterprise Linux	Standard package
Slackware Linux / Slackware	SlackBuilds.org
Oracle / Solaris 11	Standard package CSWUNIX Packages
* / *	The Written Word

Nmap Official Website



<https://nmap.org/>

- Wireshark used to use a driver called, “WinPCAP”, to perform the packet capture within Windows.
- This has been superseded by a more modern and still actively updated driver, “Nmap”.
- You shouldn’t need to get the Nmap driver yourself – it is included with the Wireshark installer. You should be aware though, just in case.
- There is also an optional USBcap driver.

Npcap.com Seclists.org Sectools.org Insecure.org

NMAP.ORG Site Search

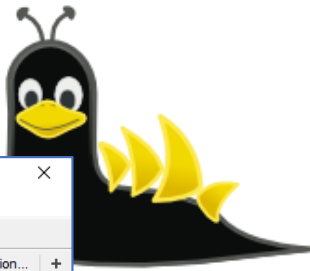
Download Reference Guide Book Docs Zenmap GUI In the Movies

[Get Nmap 7.94 here](#)

News

- Nmap.org has been redesigned! Our new mobile-friendly layout is also on [Npcap.com](#), [Seclists.org](#), [Insecure.org](#), and [Sectools.org](#).
- Nmap 7.90 has been released with Npcap 1.00 along with dozens of other performance improvements, bug fixes, and feature enhancements! [\[Release Announcement\]](#) [\[Download page\]](#)
- After more than 7 years of development and 170 public pre-releases, we're delighted to announce Npcap version 1.00! [\[Release Announcement\]](#) [\[Download page\]](#)
- Nmap 7.80 was released for DEFCON 27! [\[release notes\]](#) [\[download\]](#)
- Nmap turned 20 years old on September 1, 2017! Celebrate by reading [the original Phrack #51 article](#). [#Nmap20!](#)
- 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 Ellysium](#) 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

The screenshot shows the Wireshark Network Analyzer window. The menu bar includes File, Edit, View, Go, Capture, Analyze, Statistics, Telephony, Wireless, Tools, and Help. The toolbar contains icons for file operations, capture, and analysis. The main area is divided into several sections:

- Recent Capture Files:** A list of recently opened trace files, including `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)`, and others.
- Display Filter Bar:** A bar at the top with the text "Apply a display filter ... <Ctrl-/>" and a search icon.
- Capture Filter Field:** A field labeled "Capture" with the text "...using this filter: [Enter a capture filter ...]" and a dropdown menu set to "All interfaces shown".
- Live Traffic Volumes per Interface:** A list of network interfaces with corresponding traffic volume indicators (waveforms). The interfaces listed are Ethernet 4, Local Area Connection* 13, Local Area Connection* 12, Local Area Connection* 5, Local Area Connection* 11, Npcap Loopback Adapter, Wi-Fi (highlighted), Ethernet 5, Local Area Connection* 4, Adapter for loopback traffic capture, Ethernet 2, Ethernet, USBPcap1, and USBPcap2.
- Learn Section:** Links to "User's Guide", "Wiki", "Questions and Answers", and "Mailing Lists". Below this, it states "You are running Wireshark 3.0.6 (v3.0.6-0-g908c8e357d0f). You receive automatic updates."

Annotations in the image include a green arrow pointing from the "Display Filter Bar" text to the filter bar, another green arrow pointing from the "Capture Filter field" text to the capture filter field, and two yellow boxes with arrows pointing to the "Recent Capture Files" and "Live Traffic Volumes per Interface" sections.

Wireshark Display



- Menu options

- File
- Edit
- Capture
- Analyze

- Buttons

- Start
- Stop

- Display Filter Bar

- Panes

- Packet List
- Packet Details
- Packet Bytes

- Colours

The screenshot shows the Wireshark interface with the following callouts:

- Start Capture**: A green box pointing to the Start Capture button in the toolbar.
- Stop Capture**: A yellow box pointing to the Stop Capture button in the toolbar.
- Display Filter Bar**: A green box pointing to the display filter input field above the packet list.
- Packet Counts**: A green box pointing to the status bar at the bottom right, which shows "Packets: 27136 · Displayed: 27136 (100.0%)".

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,

Packet details for frame 179:

- > 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

Packet bytes:

```
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]..
```



Wireshark Capture at Home

- I ran Wireshark for 55 seconds.
- In that time, I went to Wireshark, Nmap and my own website (www.networkdetective.com.au).
- There were 2,724 packets captured in that short time.
- We'll see that there was traffic to/from my laptop to/from lots of places.



Using My Own Website (Not HTTPS)

- I went to various websites, but most these days use HTTPS (encrypted)
- In order for us to see the same data in the PCAP, I used my own HTTP (non-encrypted) website.
- This is the home page.

www.networkdetective.com.au

Home Assistant PM-J1900 eBay World Clock nabTrade HotCopper BigCharts LinkedIn HA Community AW-Home Assistant

NETWORK Detective

NETWORK DETECTIVE
Network and Application Performance Investigation via Packet Analysis

Home Blog Recent Engagements Downloads Contact About

HOME

Welcome to the home page of Phil Storey.

A freelance network and application performance analyst and investigator, based in Sydney, Australia.

Troubleshooter of complex, multi-tier, multi-vendor, multi-network performance problems.

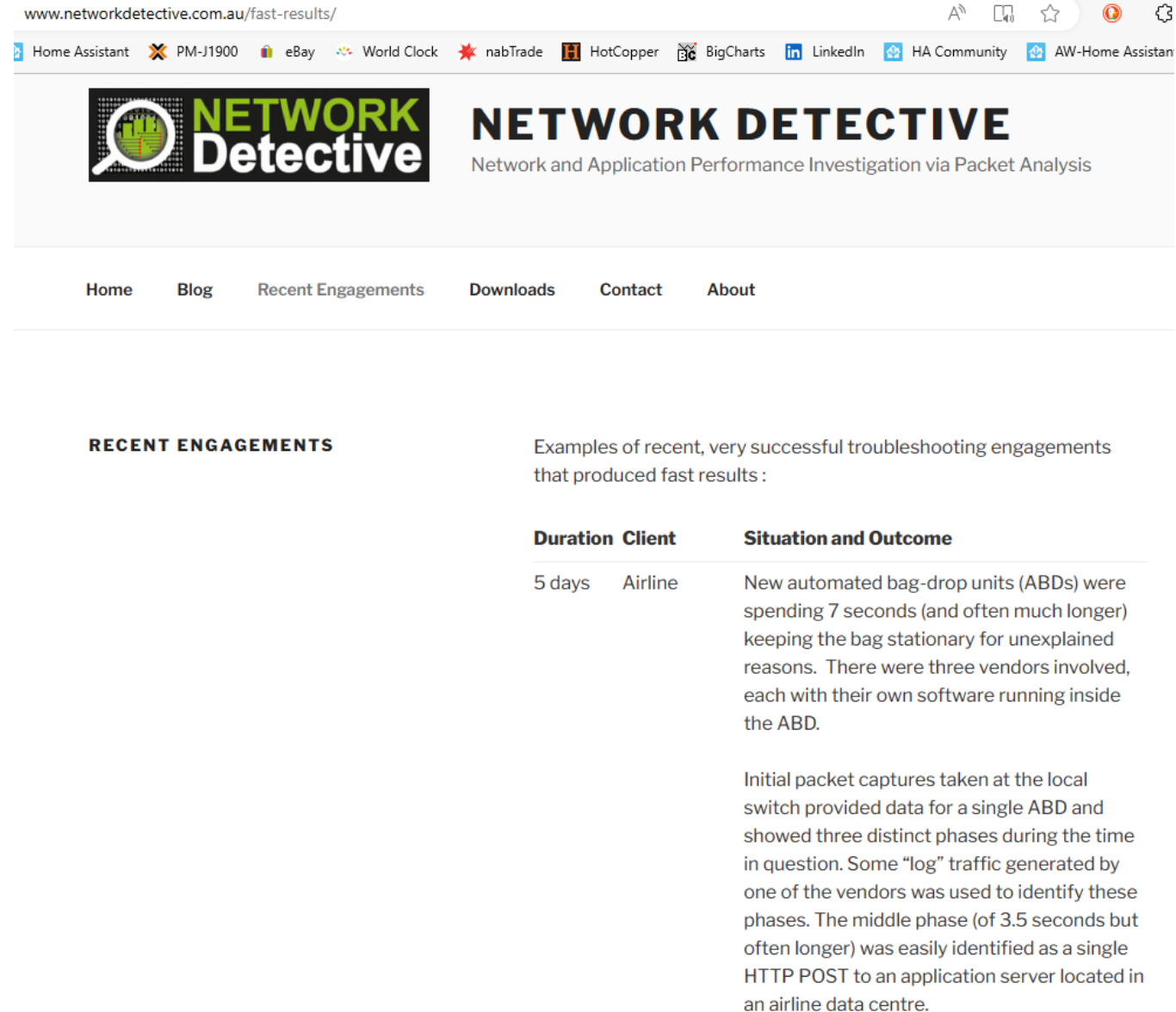
The primary methodology that I use is analysis of packet capture data using an Australian commercial software called NetData. Other tools such as Wireshark are, of course, used where appropriate.

Local PCAP

- This is the “Recent Engagements” page.
- Can we find this data in the PCAP?

Note: The URL is:

<http://www.networkdetective.com.au/fast-results/>



www.networkdetective.com.au/fast-results/

Home Assistant PM-J1900 eBay World Clock nabTrade HotCopper BigCharts LinkedIn HA Community AW-Home Assistan

NETWORK Detective NETWORK DETECTIVE
Network and Application Performance Investigation via Packet Analysis

Home Blog Recent Engagements Downloads Contact About

RECENT ENGAGEMENTS

Examples of recent, very successful troubleshooting engagements that produced fast results :

Duration	Client	Situation and Outcome
5 days	Airline	<p>New automated bag-drop units (ABDs) were spending 7 seconds (and often much longer) keeping the bag stationary for unexplained reasons. There were three vendors involved, each with their own software running inside the ABD.</p> <p>Initial packet captures taken at the local switch provided data for a single ABD and showed three distinct phases during the time in question. Some “log” traffic generated by one of the vendors was used to identify these phases. The middle phase (of 3.5 seconds but often longer) was easily identified as a single HTTP POST to an application server located in an airline data centre.</p>



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://wiki.wireshark.org/DisplayFilters/>

Display filter is not a capture filter

Capture filters (like `tcp.port 80`) are not to be confused with display filters (like `tcp.port == 80`). See also [CaptureFilters: Capture filter is not a display filter](#).

Examples

Show only SMTP (port 25) and ICMP traffic:

```
tcp.port eq 25 or icmp
```

Show only traffic in the LAN (192.168.x.x), between workstations and servers – no Internet:

```
ip.src==192.168.0.0/16 and ip.dst==192.168.0.0/16
```

TCP buffer full – Source is instructing Destination to stop sending data

```
tcp.window_size == 0 && tcp.flags.reset != 1
```

Filter on Windows – Filter out noise, while watching Windows Client - DC exchanges

```
smb || nbns || dcerpc || nbss || dns
```

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 what 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



Note the various tabs and the dropdown.

- Highlighted my own website.
- Notice that my website domain name resolves to 203.170.86.34.
- Also notice all the other websites/IP addresses that were active in this 55 seconds.
- There are many more in this list.

Address	Name
142.250.76.106	jnn-pa.googleapis.com
142.250.66.202	jnn-pa.googleapis.com
142.250.71.74	jnn-pa.googleapis.com
203.170.86.34	networkdetective.com.au
45.33.49.119	nmap.org
142.250.76.110	play.google.com
18.67.111.52	sb.scorecardresearch.com
18.67.111.113	sb.scorecardresearch.com
18.67.111.28	sb.scorecardresearch.com
18.67.111.98	sb.scorecardresearch.com
4.199.0.29	wd-prod-ss-au-southeast-1-fe.australiasoutheast.cloudapp.azure.
172.67.75.39	www.wireshark.org
104.26.10.240	www.wireshark.org
104.26.11.240	www.wireshark.org
142.250.204.14	youtube-ui.l.google.com
142.251.221.78	youtube-ui.l.google.com



Name Resolution

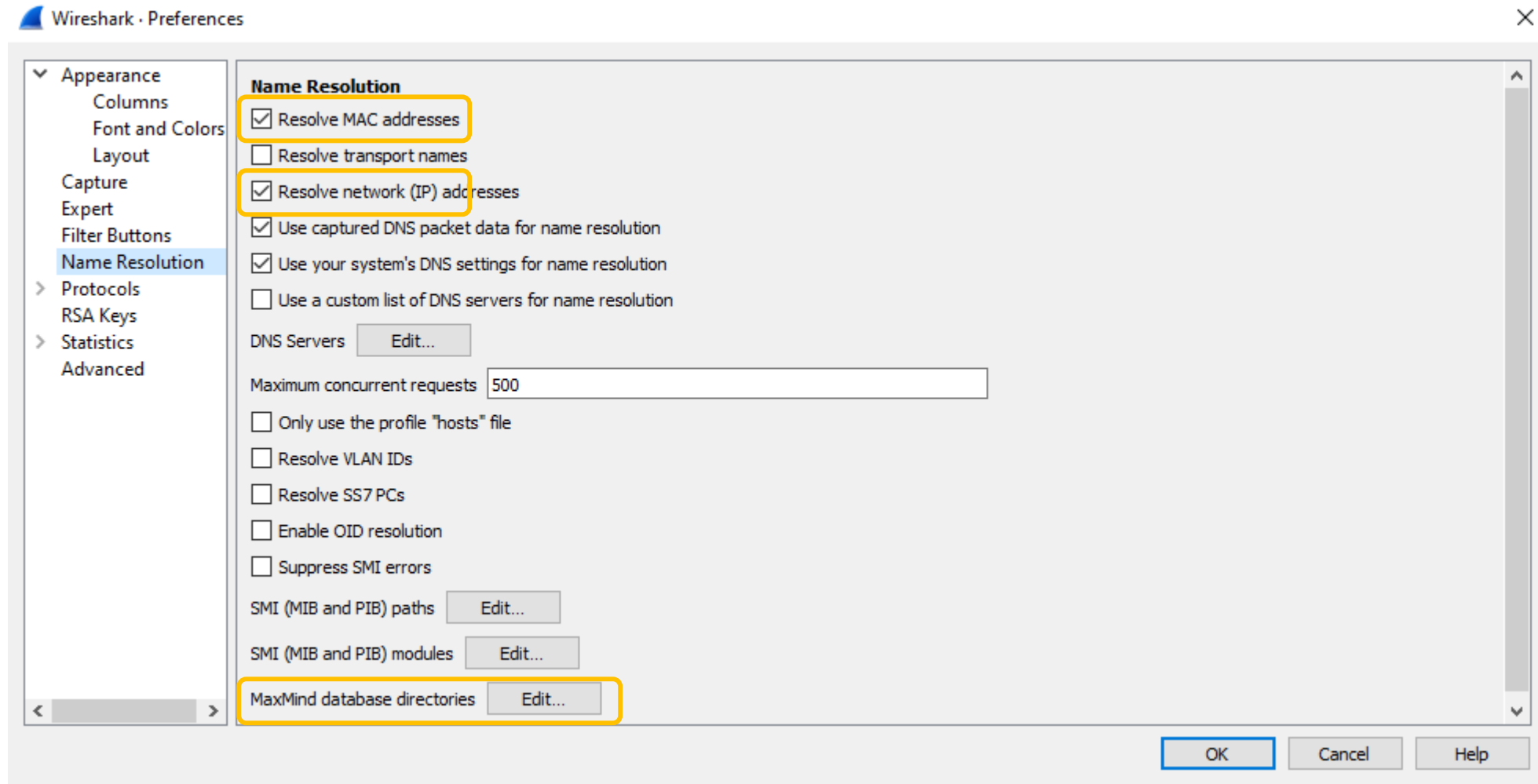
Edit

- Preferences
 - Name Resolution

You can choose whether to display names in the various parts of Wireshark's displays.

Note difference between

- MAC (Ethernet)
- IP (TCP/IP)
- Maxmind GEO Data



Wireshark Layout, Packet Diagram Form



Edit

- Preferences
 - Layout

You can choose how you want Wireshark's main display to be laid out.

“Packet Diagram” is interesting.

The screenshot shows the 'Wireshark - Preferences' dialog box. On the left is a tree view with 'Appearance' expanded, and 'Layout' selected. The main area shows three panes (Pane 1, Pane 2, Pane 3) with radio button options for 'Packet List', 'Packet Details', 'Packet Bytes', 'Packet Diagram', and 'None'. Above the panes are six layout icons representing different pane arrangements. In Pane 3, the 'Packet Diagram' option is selected and highlighted with a yellow box. Below the pane options are sections for 'Packet List settings' and 'Status Bar settings', each with several checkboxes. At the bottom right are 'OK', 'Cancel', and 'Help' buttons.

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
- UDP is taking over these days – due to Google’s QUIC protocol
- Notice that my website (203.170.86.34) was only the 8th largest in size of transfer.

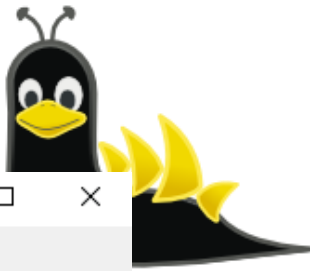
Wireshark · Conversations · SLUG-Prep.pcapng

Ethernet · 46		IPv4 · 69		IPv6 · 7		TCP · 49		UDP · 119			
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
192.168.0.21	172.217.167.110	396	282 k	183	103 k	213	178 k	11.906573	5.1364	161 k	278 k
192.168.0.21	142.250.66.202	256	194 k	85	15 k	171	178 k	13.296507	0.8572	146 k	1663 k
192.168.0.21	23.62.8.82	202	141 k	68	11 k	134	129 k	31.334462	20.5534	4665	50 k
192.168.0.21	20.42.65.85	181	97 k	88	85 k	93	12 k	31.314225	3.8685	175 k	24 k
192.168.0.21	204.79.197.203	161	132 k	47	10 k	114	121 k	47.345361	3.3347	25 k	292 k
192.168.0.21	4.199.0.29	128	77 k	62	21 k	66	55 k	12.110531	30.3917	5619	14 k
192.168.0.21	192.168.0.1	114	14 k	57	4356	57	9761	9.434827	39.0635	892	1998
192.168.0.21	203.170.86.34	102	92 k	32	3295	70	89 k	18.771211	28.5760	922	25 k
192.168.0.21	104.26.11.240	83	36 k	45	17 k	38	19 k	9.457932	4.8041	28 k	32 k
192.168.0.21	142.250.76.110	80	27 k	40	15 k	40	12 k	43.900285	1.1986	100 k	84 k
192.168.0.1	192.168.0.255	53	6095	53	6095	0	0	0.315339	54.0571	902	0
192.168.0.21	204.79.197.200	49	24 k	21	4688	28	19 k	31.366464	0.4836	77 k	322 k
192.168.0.21	45.33.49.119	47	25 k	18	2880	29	22 k	8.590365	13.7826	1671	13 k
192.168.0.21	192.168.0.215	44	4862	22	2398	22	2464	2.127907	50.1392	382	393
192.168.0.21	23.62.8.96	44	24 k	21	21 k	23	2835	48.498733	0.2283	758 k	99 k
192.168.0.245	255.255.255.255	42	2673	42	2673	0	0	0.304167	54.5840	391	0
192.168.0.21	192.168.0.203	36	4721	24	2668	12	2053	2.003992	52.5684	406	312
192.168.0.21	23.206.198.27	34	4478	16	2238	18	2240	31.363190	11.0198	1624	1626
192.168.0.21	20.43.111.112	33	7354	14	1974	19	5380	24.916718	28.7830	548	1495
192.168.0.21	204.79.197.219	33	15 k	13	2076	20	13 k	31.367304	0.0748	222 k	1483 k
192.168.0.21	13.107.21.200	29	14 k	14	4847	15	9447	31.845770	0.2495	155 k	302 k
192.168.0.21	142.250.76.118	27	11 k	13	4086	14	7536	13.301484	0.1288	253 k	467 k
192.168.0.21	20.205.115.81	27	11 k	14	3663	13	8239	31.333385	0.9246	31 k	71 k
192.168.0.21	172.217.167.78	26	14 k	12	4694	14	9564	15.982817	0.3003	125 k	254 k
192.168.0.202	192.168.0.21	24	8112	24	8112	0	0	34.108191	7.2784	8916	0
184.105.129.23	192.168.0.21	20	1220	9	576	11	644	0.000523	54.1662	85	95
192.168.0.21	18.67.111.52	17	3077	9	1823	8	1254	31.334076	0.2454	59 k	40 k
192.168.0.21	255.255.255.255	14	3430	14	3430	0	0	0.760521	30.1461	910	0
192.168.0.24	255.255.255.255	11	2354	11	2354	0	0	1.032155	50.0637	376	0
192.168.0.63	255.255.255.255	11	2354	11	2354	0	0	1.225693	49.9730	376	0
192.168.0.151	255.255.255.255	11	2354	11	2354	0	0	1.955839	50.0594	376	0
192.168.0.208	255.255.255.255	11	2530	11	2530	0	0	4.305626	49.9659	405	0
192.168.0.209	255.255.255.255	11	2530	11	2530	0	0	1.635451	49.9949	404	0
192.168.0.218	255.255.255.255	11	2530	11	2530	0	0	3.888264	49.9703	405	0
192.168.0.219	255.255.255.255	11	2354	11	2354	0	0	3.873073	49.9659	376	0

Name resolution Limit to display filter Absolute start time Conversation Types ▾

Copy ▾ Follow Stream... Graph... Close Help

Statistics - Endpoints



- Click on Headings to sort (here is sorted by “Packets”)
- “IPv4” is likely to be the most interesting for now, but UDP (QUIC) is picking up.
- The Geolocation information is a new feature. It needs an external set of data files that can be downloaded for free.
- See YouTube video: <https://www.youtube.com/watch?v=6p20HQnf-Bw>

Wireshark · Endpoints · SLUG-Prep.pcapng

Ethernet · 36 IPv4 · 64 IPv6 · 9 TCP · 78 UDP · 136

Address	Packets	Bytes	Tx Packets	Tx Bytes	Rx Packets	Rx Bytes	Country	City	AS Number	AS Organization
192.168.0.21	2,277	1289 k	980	361 k	1,297	928 k	—	—	—	—
172.217.167.110	396	282 k	213	178 k	183	103 k	United States	—	15169	GOOGLE
142.250.66.202	256	194 k	171	178 k	85	15 k	United States	—	15169	GOOGLE
23.62.8.82	202	141 k	134	129 k	68	11 k	Australia	Sydney	20940	Akamai International B.V.
255.255.255.255	185	34 k	0	0	185	34 k	—	—	—	—
20.42.65.85	181	97 k	93	12 k	88	85 k	United States	Tappahannock	8075	MICROSOFT-CORP-MSN-AS-BLOCK
192.168.0.1	173	22 k	116	18 k	57	4356	—	—	—	—
204.79.197.203	161	132 k	114	121 k	47	10 k	United States	—	8068	MICROSOFT-CORP-MSN-AS-BLOCK
4.199.0.29	128	77 k	66	55 k	62	21 k	Australia	Melbourne	8075	MICROSOFT-CORP-MSN-AS-BLOCK
203.170.86.34	102	92 k	70	89 k	32	3295	Australia	—	38719	Dreamscape Networks Limited
104.26.11.240	83	36 k	38	19 k	45	17 k	—	—	13335	CLOUDFLARENET
142.250.76.110	80	27 k	40	12 k	40	15 k	United States	—	15169	GOOGLE
192.168.0.255	55	6585	0	0	55	6585	—	—	—	—
192.168.0.215	49	5908	27	3510	22	2398	—	—	—	—
204.79.197.200	49	24 k	28	19 k	21	4688	United States	—	8068	MICROSOFT-CORP-MSN-AS-BLOCK
45.33.49.119	47	25 k	29	22 k	18	2880	United States	Fremont	63949	Akamai Connected Cloud
23.62.8.96	44	24 k	23	2835	21	21 k	Australia	Sydney	20940	Akamai International B.V.
192.168.0.203	44	6186	20	3518	24	2668	—	—	—	—
192.168.0.245	42	2673	42	2673	0	0	—	—	—	—
23.206.198.27	34	4478	18	2240	16	2238	Australia	Sydney	20940	Akamai International B.V.
20.43.111.112	33	7354	19	5380	14	1974	Australia	Sydney	8075	MICROSOFT-CORP-MSN-AS-BLOCK
204.79.197.219	33	15 k	20	13 k	13	2076	United States	—	8068	MICROSOFT-CORP-MSN-AS-BLOCK
192.168.0.202	30	10 k	30	10 k	0	0	—	—	—	—
13.107.21.200	29	14 k	15	9447	14	4847	United States	—	8068	MICROSOFT-CORP-MSN-AS-BLOCK
20.205.115.81	27	11 k	13	8239	14	3663	Hong Kong	Hong Kong	8075	MICROSOFT-CORP-MSN-AS-BLOCK
142.250.76.118	27	11 k	14	7536	13	4086	United States	—	15169	GOOGLE
172.217.167.78	26	14 k	14	9564	12	4694	United States	—	15169	GOOGLE
224.0.0.251	24	5653	0	0	24	5653	—	—	—	—

Name resolution Limit to display filter Endpoint Types ▾

Copy ▾ Map ▾ Close Help

Interesting

Statistics – Endpoints: Map



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



Wireshark Can be Useful

Wireshark identifies it as MQTT

TCP/1883



- 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
  ▼ MQ Telemetry Transport Protocol
    ▼ Connect Command
      > 0001 0000 = Header Flags: 0x10 (Connect Command)
        Msg Len: 100
        Protocol Name: MQTT
        Version: 4
      ▼ 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
```

Retain is not set

QoS level 0

LWT specified

The message to publish



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>
 - Tony Fortunato <https://www.youtube.com/channel/UCGzLX2yif2uqobtoVTLbHhQ>
 - Jasper Bongertz <https://www.youtube.com/channel/UCZd-4lZtcbE1zM-CnOxd31A>
 - Chris Greer <https://www.youtube.com/user/packetpioneer>
 - Betty DuBois <https://www.youtube.com/channel/UCy4XzAs0O6UpDfGOHiPshrg>
 - Kary Rogers <https://www.youtube.com/@PacketBomb>
 - Laura Chappell <https://www.chappell-university.com/>
- Me at a previous 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](https://twitter.com/PhilStorey24)

www.youtube.com/c/NetworkDetective



ask.wireshark.org: [@philst](https://ask.wireshark.org/@philst)





NetData

An Australian packet analysis tool, focussed on providing data graphically.
Use Wireshark to do the packet capture, then NetData to do the analysis.

The author of NetData, Bob Brownell, regularly updates the software.

A free “NetDataLite” version can always be downloaded here:

<https://www.dropbox.com/sh/s572ctzcd70mb28/AADfk5TQex4RrC4ipttb8XgQa?dl=0>

Here’s a Kary Rogers (PacketBomb) video where I discuss NetData:

<https://www.youtube.com/watch?v=Tkx18Ec8Vy0&t>

***Note that NetData (and Lite) is a Windows only application.**

Example NetData Charts (from Same PCAP)

