Wireshark Tutorial

Network Startup Resource Center

www.ws.nsrc.org

UNIVERSITY OF OREGON

NSRC Network Startup Resource Center

Who am I?

- Dean Pemberton
- Long time network engineer
  - Ascend
  - Lucent
  - Juniper
  - Telstra NZ
- Now in network security with CASSINI

www.cassini.nz

Thanks to…

certnz

… for letting me use their office to present from

Network Packet Analysis… with Wireshark

What you hope network packet analysis is like...

Photo by Mick Haupt on Unsplash

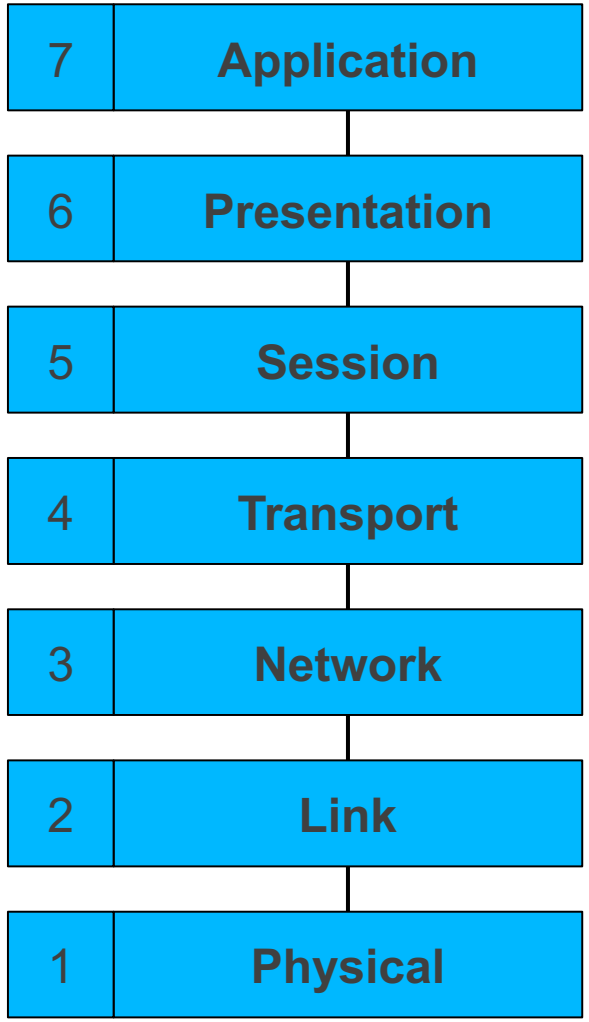
What network packet analysis is really like!

Overview

- Review of the OSI Model
- Wireshark
  - Capturing Packets
  - A tour of the Wireshark UI
  - Reviewing/Analysing Packets
  - Filtering
  - Demos

Review of the OSI Model

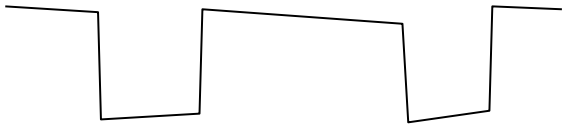
Our old friend the 7-layer OSI model



Layer 1: Physical Layer

- Transfers a stream of bits
- Defines physical characteristics
  - Connectors, pinouts
  - Cable types, voltages, modulation
  - Fibre types, lambdas
  - Transmission rate (bps)
- No knowledge of bytes or frames

101101 →



Layer 2: (Data) Link Layer

- Organises data into *frames*
- May detect transmission errors (corrupt frames)
- May support shared media
  - Addressing (unicast, multicast) – who should receive this frame
  - Access control, collision detection
- Usually identifies the L3 protocol carried
- E.g. Ethernet, Wifi

Layer 3: (Inter)Network Layer

- Connects Layer 2 networks together
  - Forwarding data from one network to another
  - These different networks are called subnets (short for sub-network)
- Unified addressing scheme
  - Independent of the underlying L2 network(s)
  - Addresses organised so that it can scale globally (aggregation)
- Identifies the layer 4 protocol being carried
- Fragmentation and reassembly
- E.g. IP

Layer 4: Transport Layer

- Identifies the *endpoint* process
  - Another level of addressing (port number)
- May provide reliable delivery
  - Streams of unlimited size
  - Error correction and retransmission
  - In-sequence delivery
  - Flow control
- Might just be unreliable datagram transport
- E.g. TCP, UDP

Layers 5 and 6

- Session Layer: long-lived sessions
  - Re-establish transport connection if it fails
  - Multiplex data across multiple transport connections
- Presentation Layer: data reformatting
  - Character set translation
- Neither exist in the TCP/IP suite: the application is responsible for these functions

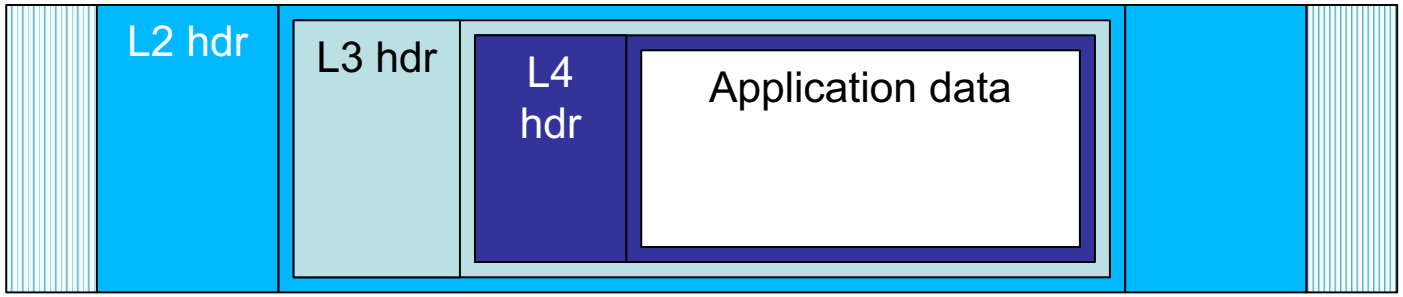
Layer 7: Application layer

- The actual work you want to do
- Protocols specific to each application
- E.g. telnet, http, https, imap

Encapsulation

- Each layer provides services to the layer above
- Each layer makes use of the layer below
- Data from one layer is *encapsulated* in frames of the layer below

Encapsulation in action



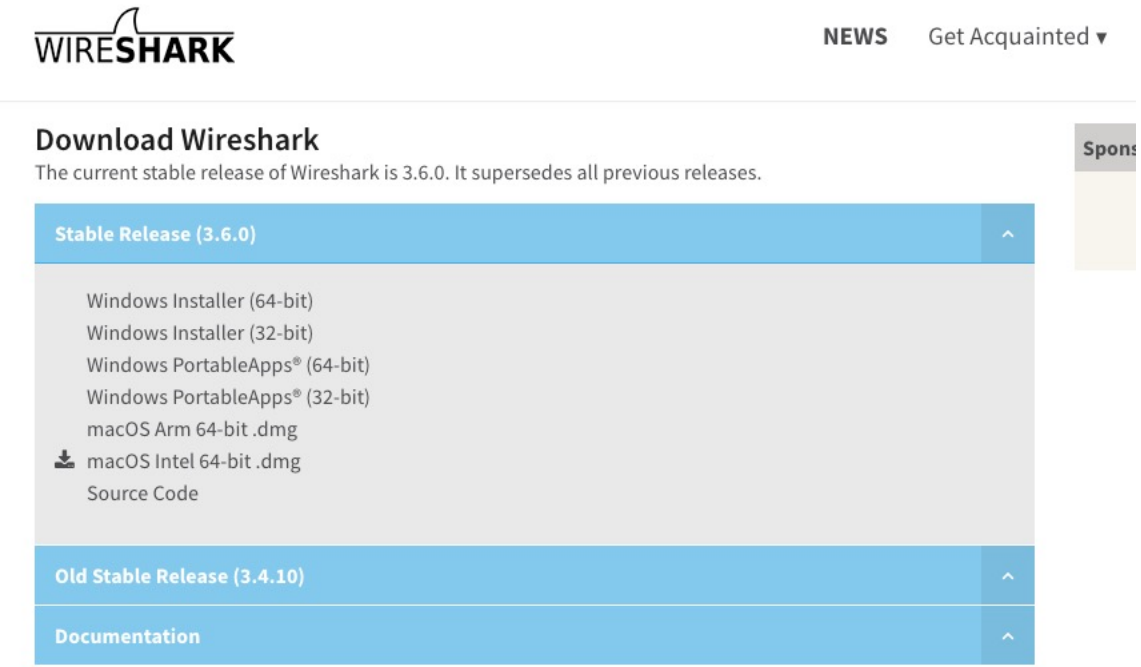
- L4 segment contains part of stream of application protocol
- L3 datagram contains L4 segment
- L2 frame has L3 datagram in data portion

Wireshark

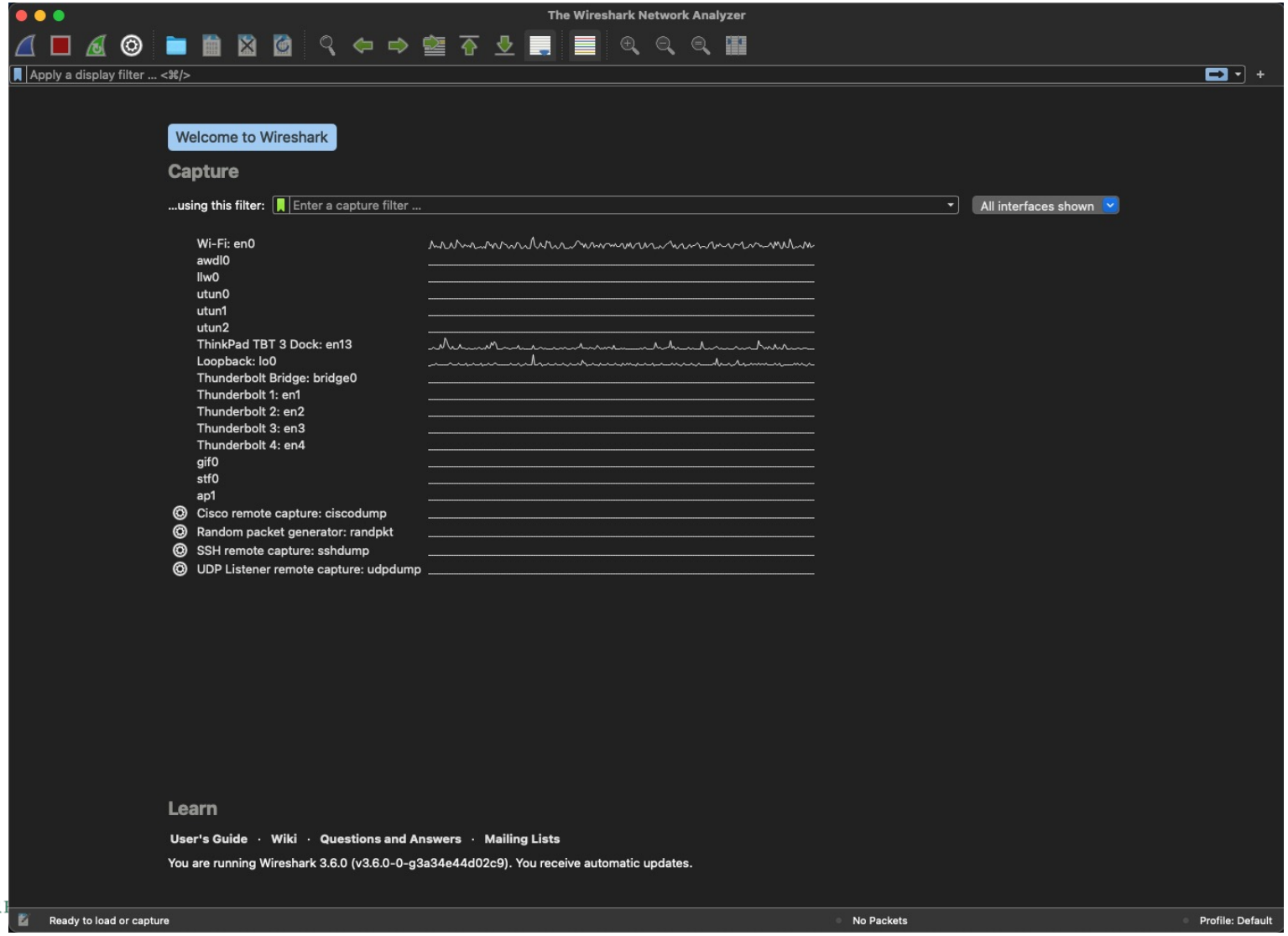
- …is a free and open-source packet analyser.

Downloading

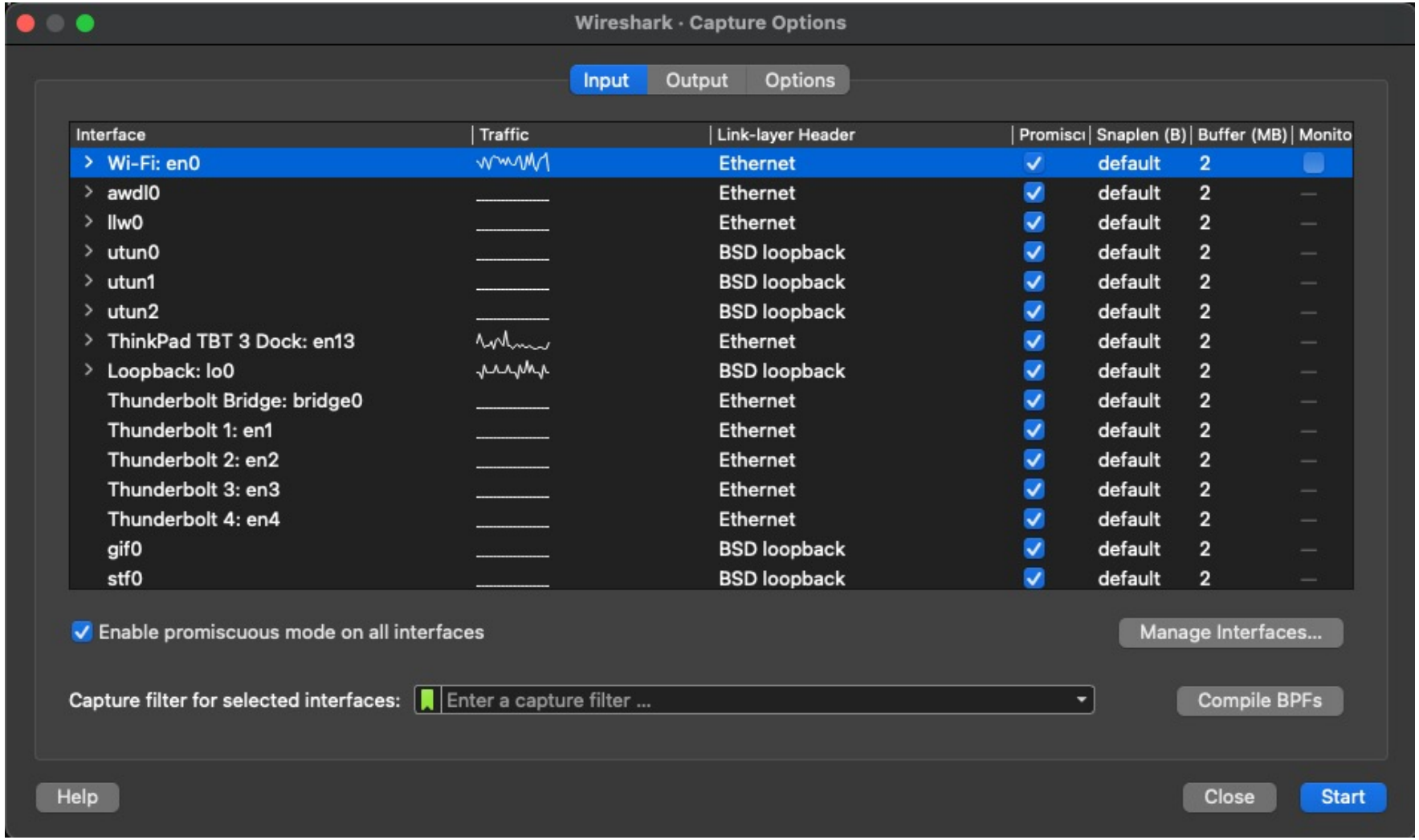
- https://www.wireshark.org/download.html



Welcome Screen

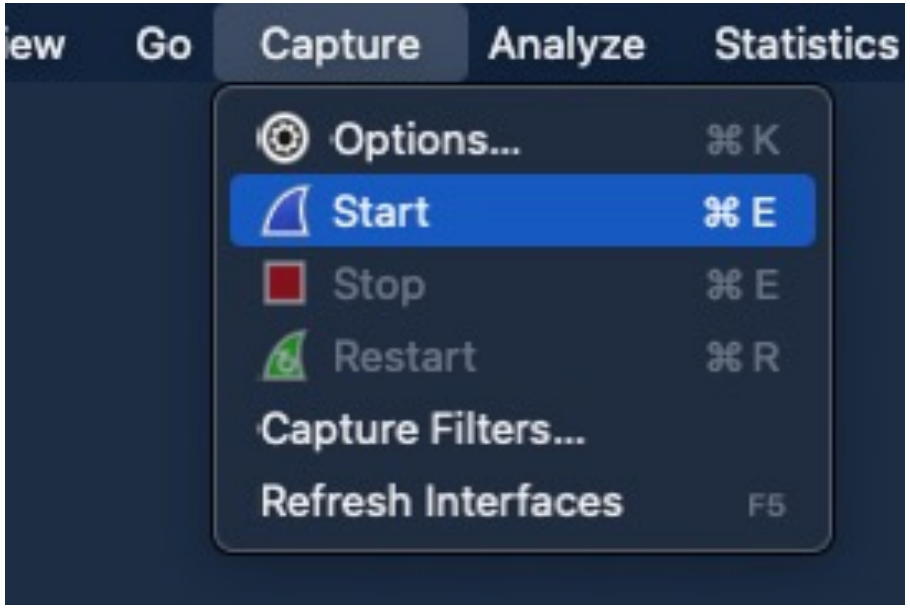


Interface Selection



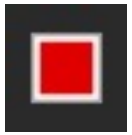
Starting a capture

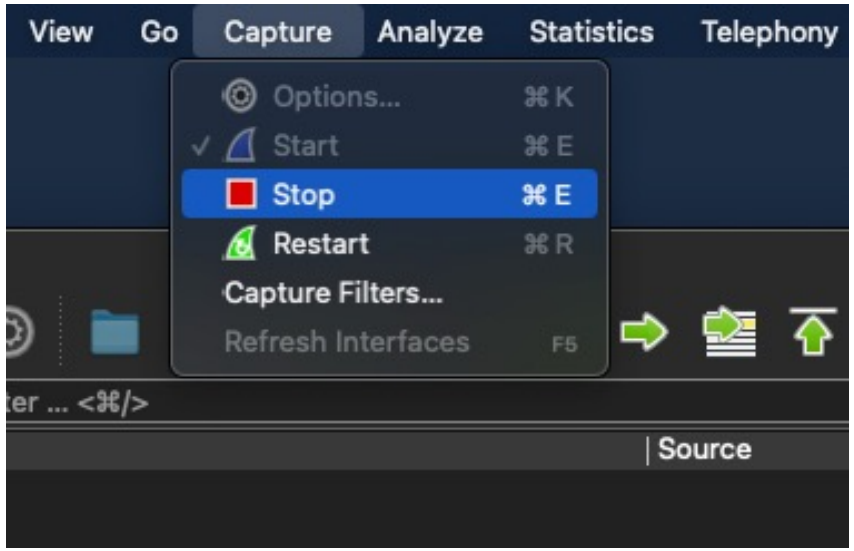
- Click on the Shark icon
- Select Start from the menu



Stopping a Capture

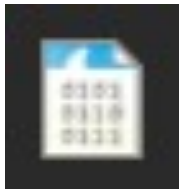
- Click on the Stop icon
- Select Stop from the menu

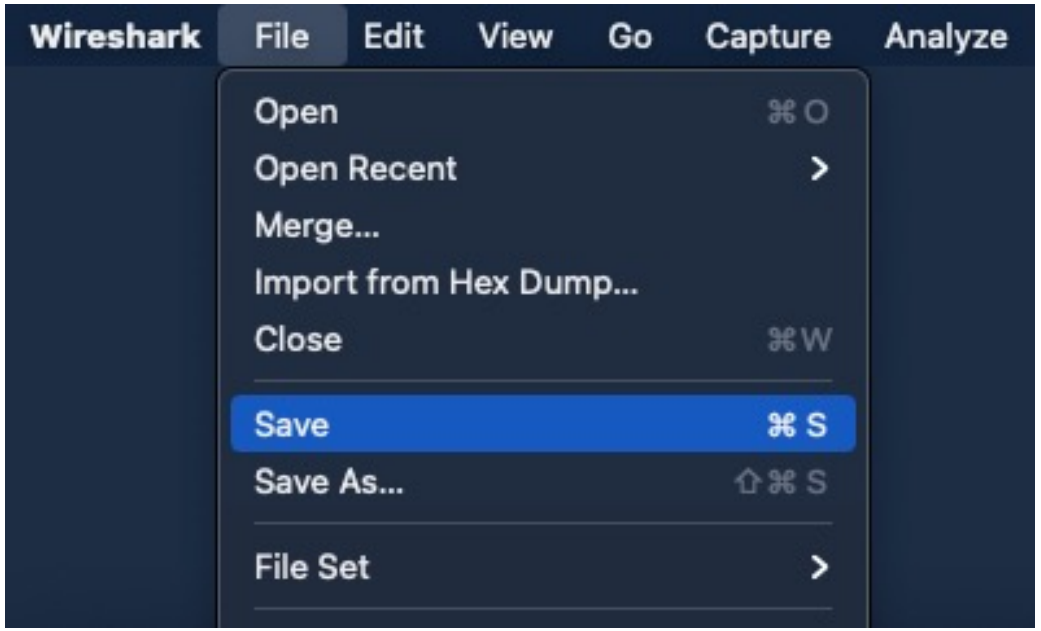




Saving a capture file

- Click on the Save icon
- Select Save from the menu



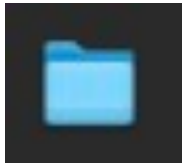


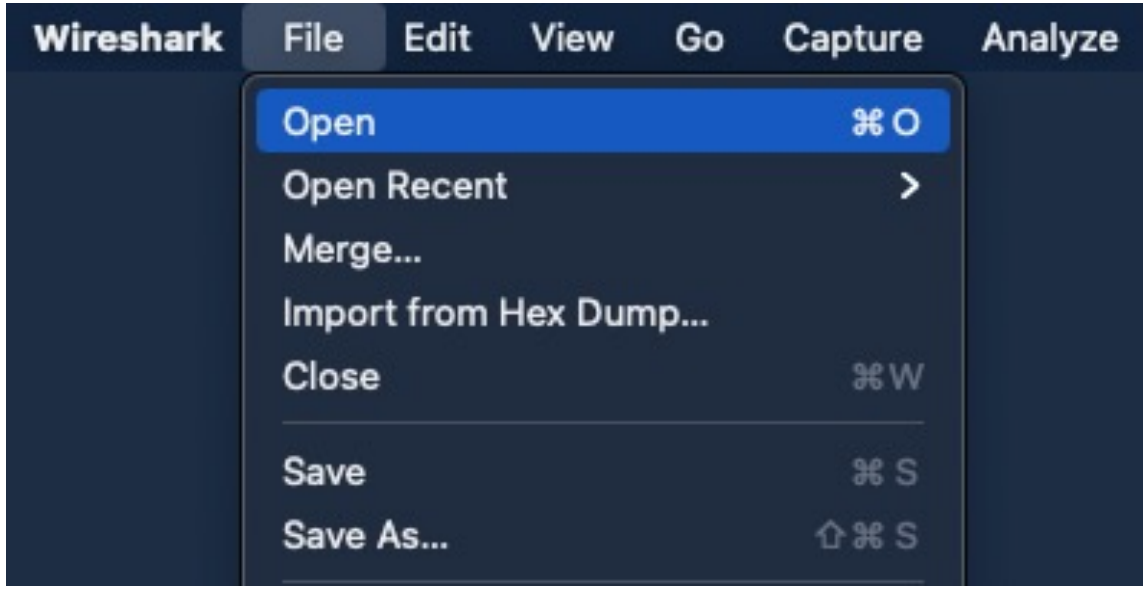
Sample PCAP files

- https://wiki.wireshark.org/SampleCaptures

Opening a capture file

- Select the Folder icon
- Select Open from the menu





Why do we need more than tcpdump?

```
reading from file telnet-cooked.pcap, link-type EN10MB (Ethernet)
15:12:38.387203 IP 192.168.0.2.1550 > 192.168.0.1.23: Flags [S], seq 2579865836, win 32120, options [mss 1460,sackOK,TS val 10233636 ecr 0,nop,wscale 0], length 0
15:12:38.389728 IP 192.168.0.1.23 > 192.168.0.2.1550: Flags [S.], seq 401695549, ack 2579865837, win 17376, options [mss 1448,nop,wscale 0,nop,nop,TS val 2467372 ecr 10233636], length 0
15:12:38.389775 IP 192.168.0.2.1550 > 192.168.0.1.23: Flags [.], ack 1, win 32120, options [nop,nop,TS val 10233636 ecr 2467372], length 0
15:12:38.391363 IP 192.168.0.2.1550 > 192.168.0.1.23: Flags [P.], seq 1:28, ack 1, win 32120, options [nop,nop,TS val 10233636 ecr 2467372], length 27 [telnet DO SUPPRESS GO AHEAD, WILL TERMINAL TYPE, WILL NAWS, WILL TSPEED, WILL LFLOW, W
ILL LINEMODE, WILL NEW-ENVIRON, DO STATUS, WILL XDISPLOC [|telnet]
15:12:38.537538 IP 192.168.0.1.23 > 192.168.0.2.1550: Flags [P.], seq 1:4, ack 28, win 17349, options [nop,nop,TS val 2467372 ecr 10233636], length 3 [telnet DO AUTHENTICATION [|telnet]
15:12:38.537605 IP 192.168.0.2.1550 > 192.168.0.1.23: Flags [.], ack 4, win 32120, options [nop,nop,TS val 10233651 ecr 2467372], length 0
15:12:38.537777 IP 192.168.0.2.1550 > 192.168.0.1.23: Flags [P.], seq 28:31, ack 4, win 32120, options [nop,nop,TS val 10233651 ecr 2467372], length 3 [telnet WONT AUTHENTICATION [|telnet]
15:12:38.539149 IP 192.168.0.1.23 > 192.168.0.2.1550: Flags [.], ack 31, win 17376, options [nop,nop,TS val 2467372 ecr 10233651], length 0
15:12:38.540860 IP 192.168.0.1.23 > 192.168.0.2.1550: Flags [P.], seq 4:29, ack 31, win 17376, options [nop,nop,TS val 2467372 ecr 10233651], length 25 [telnet WILL SUPPRESS GO AHEAD, DO TERMINAL TYPE, DO NAWS, DO TSPEED, DO LFLOW, DO LIN
EMODE, SB LINEMODE SEND 0xb SE [|telnet]
15:12:38.541068 IP 192.168.0.2.1550 > 192.168.0.1.23: Flags [P.], seq 31:95, ack 29, win 32120, options [nop,nop,TS val 10233651 ecr 2467372], length 64 [telnet SB NAWS IS 0x50 0 0x20 SE, SB LINEMODE 0x3 0x1 0 0 0x3 0x62 0x3 0x4 0x2 0xf 0
x5 0 0 0x7 0x62 0x1c 0x8 0x2 0x4 0x9 0x42 0x1a 0xa 0x2 0x7f 0xb 0x2 0x15 0xf 0x2 0x11 0x10 0x2 0x13 0x11 0 0 0x12 0 0 SE, DO SUPPRESS GO AHEAD, SB LINEMODE SEND 0xf SE [|telnet]
15:12:38.542187 IP 192.168.0.1.23 > 192.168.0.2.1550: Flags [.], ack 95, win 17312, options [nop,nop,TS val 2467372 ecr 10233651], length 0
15:12:38.542780 IP 192.168.0.1.23 > 192.168.0.2.1550: Flags [P.], seq 29:47, ack 95, win 17312, options [nop,nop,TS val 2467372 ecr 10233651], length 18 [telnet DO NEW-ENVIRON, WILL STATUS, DO XDISPLOC, WILL ENCRYPT, DO ENCRYPT, DO OLD-EN
VIRON [|telnet]
15:12:38.542859 IP 192.168.0.2.1550 > 192.168.0.1.23: Flags [P.], seq 95:104, ack 47, win 32120, options [nop,nop,TS val 10233651 ecr 2467372], length 9 [telnet DONT ENCRYPT, WONT ENCRYPT, WONT OLD-ENVIRON [|telnet]
15:12:38.543849 IP 192.168.0.1.23 > 192.168.0.2.1550: Flags [.], ack 104, win 17367, options [nop,nop,TS val 2467372 ecr 10233651], length 0
15:12:38.546219 IP 192.168.0.1.23 > 192.168.0.2.1550: Flags [P.], seq 47:71, ack 104, win 17376, options [nop,nop,TS val 2467372 ecr 10233651], length 24 [telnet SB TSPEED SEND SE, SB XDISPLOC SEND SE, SB NEW-ENVIRON SEND SE, SB TERMINAL
TYPE SEND SE [|telnet]
15:12:38.546430 IP 192.168.0.2.1550 > 192.168.0.1.23: Flags [.], ack 71, win 32120, options [nop,nop,TS val 10233652 ecr 2467372], length 0
15:12:38.547047 IP 192.168.0.2.1550 > 192.168.0.1.23: Flags [P.], seq 104:189, ack 71, win 32120, options [nop,nop,TS val 10233652 ecr 2467372], length 85 [telnet SB TSPEED IS 0x39 0x36 0x30 0x30 0x2c 0x39 0x36 0x30 0x30 SE, SB XDISPLOC I
S 0x62 0x61 0x6d 0x2e 0x7a 0x69 0x6e 0x67 0x2e 0x6f 0x72 0x67 0x3a 0x30 0x2e 0x30 SE, SB NEW-ENVIRON IS 0 0x44 0x49 0x53 0x50 0x4c 0x41 0x59 0x1 0x62 0x61 0x6d 0x2e 0x7a 0x69 0x6e 0x67 0x2e 0x6f 0x72 0x67 0x3a 0x30 0x2e 0x30 SE, SB TERMIN
AL TYPE IS 0x78 0x74 0x65 0x72 0x6d 0x2d 0x63 0x6f 0x6c 0x6f 0x72 SE [|telnet]
15:12:38.548221 IP truncated-ip - 85 bytes missing! 192.168.0.2.1550 > 192.168.0.1.23: Flags [P.], seq 104:189, ack 71, win 32120, options [nop,nop,TS val 10233652 ecr 2467372], length 85 [|telnet]
15:12:38.568470 IP 192.168.0.1.23 > 192.168.0.2.1550: Flags [P.], seq 71:74, ack 189, win 17376, options [nop,nop,TS val 2467372 ecr 10233652], length 3 [telnet DO ECHO [|telnet]
15:12:38.568581 IP 192.168.0.2.1550 > 192.168.0.1.23: Flags [P.], seq 189:192, ack 74, win 32120, options [nop,nop,TS val 10233654 ecr 2467372], length 3 [telnet WONT ECHO [|telnet]
15:12:38.569718 IP 192.168.0.1.23 > 192.168.0.2.1550: Flags [.], ack 192, win 17373, options [nop,nop,TS val 2467372 ecr 10233654], length 0
15:12:38.583509 IP 192.168.0.1.23 > 192.168.0.2.1550: Flags [P.], seq 74:86, ack 192, win 17376, options [nop,nop,TS val 2467372 ecr 10233654], length 12 [telnet WILL ECHO, SB LFLOW INFO SE, WONT ECHO [|telnet]
15:12:38.583630 IP 192.168.0.2.1550 > 192.168.0.1.23: Flags [P.], seq 192:198, ack 86, win 32120, options [nop,nop,TS val 10233655 ecr 2467372], length 6 [telnet DO ECHO, DONT ECHO [|telnet]
15:12:38.584705 IP 192.168.0.1.23 > 192.168.0.2.1550: Flags [.], ack 198, win 17370, options [nop,nop,TS val 2467372 ecr 10233655], length 0
15:12:38.585489 IP 192.168.0.1.23 > 192.168.0.2.1550: Flags [P.], seq 86:101, ack 198, win 17370, options [nop,nop,TS val 2467372 ecr 10233655], length 15 [telnet SB LINEMODE 0x3 0x5 0x80 0 0x11 0x80 0 0x12 0x80 0 SE [|telnet]
15:12:38.596419 IP 192.168.0.2.1550 > 192.168.0.1.23: Flags [.], ack 101, win 32120, options [nop,nop,TS val 10233657 ecr 2467372], length 0
15:12:38.597730 IP 192.168.0.1.23 > 192.168.0.2.1550: Flags [P.], seq 101:133, ack 198, win 17376, options [nop,nop,TS val 2467372 ecr 10233657], length 32
15:12:38.616442 IP 192.168.0.2.1550 > 192.168.0.1.23: Flags [.], ack 133, win 32120, options [nop,nop,TS val 10233659 ecr 2467372], length 0
15:12:39.705066 IP 192.168.0.1.23 > 192.168.0.2.1550: Flags [P.], seq 133:140, ack 198, win 17376, options [nop,nop,TS val 2467374 ecr 10233659], length 7
15:12:39.716432 IP 192.168.0.2.1550 > 192.168.0.1.23: Flags [.], ack 140, win 32120, options [nop,nop,TS val 10233769 ecr 2467374], length 0
15:12:40.949196 IP 192.168.0.2.1550 > 192.168.0.1.23: Flags [P.], seq 198:204, ack 140, win 32120, options [nop,nop,TS val 10233892 ecr 2467374], length 6
15:12:40.950568 IP truncated-ip - 6 bytes missing! 192.168.0.2.1550 > 192.168.0.1.23: Flags [P.], seq 198:204, ack 140, win 32120, options [nop,nop,TS val 10233892 ecr 2467374], length 6 [|telnet]
15:12:40.962649 IP 192.168.0.1.23 > 192.168.0.2.1550: Flags [P.], seq 140:143, ack 204, win 17376, options [nop,nop,TS val 2467377 ecr 10233892], length 3 [telnet WILL ECHO [|telnet]
15:12:40.962801 IP 192.168.0.2.1550 > 192.168.0.1.23: Flags [P.], seq 204:207, ack 143, win 32120, options [nop,nop,TS val 10233893 ecr 2467377], length 3 [telnet DO ECHO [|telnet]
15:12:40.963879 IP 192.168.0.1.23 > 192.168.0.2.1550: Flags [.], ack 207, win 17373, options [nop,nop,TS val 2467377 ecr 10233893], length 0
15:12:40.964875 IP 192.168.0.1.23 > 192.168.0.2.1550: Flags [P.], seq 143:152, ack 207, win 17376, options [nop,nop,TS val 2467377 ecr 10233893], length 9
15:12:40.976432 IP 192.168.0.2.1550 > 192.168.0.1.23: Flags [.], ack 152, win 32120, options [nop,nop,TS val 10233895 ecr 2467377], length 0
```

Wireshark can give us much more information about a network capture

UI – Overview

telnet-cooked.pcap

Apply a display filter ... <⌘/>

No.	Time	Source	Destination	Protocol	Length	Info
1	0.000000	192.168.0.2	192.168.0.1	TCP	74	1550 → 23 [SYN] Seq=0 Win=32120 Len=0 MSS=1460 SACK_PERM=1 TSval=
2	0.002525	192.168.0.1	192.168.0.2	TCP	74	23 → 1550 [SYN, ACK] Seq=0 Ack=1 Win=17376 Len=0 MSS=1448 WS=1 TS
3	0.002572	192.168.0.2	192.168.0.1	TCP	66	1550 → 23 [ACK] Seq=1 Ack=1 Win=32120 Len=0 TSval=10233636 TSecr=
4	0.004160	192.168.0.2	192.168.0.1	TELNET	93	Telnet Data ...
5	0.150335	192.168.0.1	192.168.0.2	TELNET	69	Telnet Data ...
6	0.150402	192.168.0.2	192.168.0.1	TCP	66	1550 → 23 [ACK] Seq=28 Ack=4 Win=32120 Len=0 TSval=10233651 TSecr
7	0.150574	192.168.0.2	192.168.0.1	TELNET	69	Telnet Data ...
8	0.151946	192.168.0.1	192.168.0.2	TCP	66	23 → 1550 [ACK] Seq=4 Ack=31 Win=17376 Len=0 TSval=2467372 TSecr=
9	0.153657	192.168.0.1	192.168.0.2	TELNET	91	Telnet Data ...
10	0.153865	192.168.0.2	192.168.0.1	TELNET	130	Telnet Data ...
11	0.154984	192.168.0.1	192.168.0.2	TCP	66	23 → 1550 [ACK] Seq=29 Ack=95 Win=17312 Len=0 TSval=2467372 TSecr
12	0.155577	192.168.0.1	192.168.0.2	TELNET	84	Telnet Data ...
13	0.155656	192.168.0.2	192.168.0.1	TELNET	75	Telnet Data ...
14	0.156646	192.168.0.1	192.168.0.2	TCP	66	23 → 1550 [ACK] Seq=47 Ack=104 Win=17367 Len=0 TSval=2467372 TSec
15	0.159016	192.168.0.1	192.168.0.2	TELNET	90	Telnet Data ...
16	0.159227	192.168.0.2	192.168.0.1	TCP	66	1550 → 23 [ACK] Seq=104 Ack=71 Win=32120 Len=0 TSval=10233652 TSe
17	0.159844	192.168.0.2	192.168.0.1	TELNET	151	Telnet Data ...

```
> Frame 1: 74 bytes on wire (592 bits), 74 bytes captured (592 bits)
> Ethernet II, Src: Lite-OnU_3b:bf:fa (00:a0:cc:3b:bf:fa), Dst: WesternD_9f:a0:97 (00:00:c0:9f:a0:97)
> Internet Protocol Version 4, Src: 192.168.0.2, Dst: 192.168.0.1
> Transmission Control Protocol, Src Port: 1550, Dst Port: 23, Seq: 0, Len: 0
```

```
0000  00 00 c0 9f a0 97 00 a0  cc 3b bf fa 08 00 45 10   ........ .;....E.
0010  00 3c 46 3c 40 00 40 06  73 1c c0 a8 00 02 c0 a8   .<F<@.@. s.......
0020  00 01 06 0e 00 17 99 c5  a0 ec 00 00 00 00 a0 02   ........ ........
0030  7d 78 e0 a3 00 00 02 04  05 b4 04 02 08 0a 00 9c   }x...... ........
0040  27 24 00 00 00 00 01 03  03 00                     '$...... ..
```

telnet-cooked.pcap Packets: 92 · Displayed: 92 (100.0%) Profile: Default

UI - Statistics

UI – Protocol Hierarchy

Wireshark · Protocol Hierarchy Statistics · telnet-cooked.pcap

Protocol	Percent Packets	Packets	Percent Bytes	Bytes	Bits/s	End Packets	End Bytes	End Bits/s
Frame	100.0	92	100.0	7748	1566	0	0	0
Ethernet	100.0	92	16.6	1288	260	0	0	0
Internet Protocol Version 4	100.0	92	23.7	1840	371	0	0	0
Transmission Control Protocol	100.0	92	59.6	4620	934	46	1514	306
Telnet	50.0	46	21.1	1634	330	45	1633	330
Malformed Packet	1.1	1	0.0	0	0	1	0	0

Wireshark · Protocol Hierarchy Statistics · Wi-Fi: en0

Protocol	Percent Packets	Packets	Percent Bytes	Bytes	Bits/s	End Packets	End Bytes	End Bits/s
Frame	100.0	164	100.0	26973	16 k	0	0	0
Ethernet	100.0	164	8.5	2296	1425	0	0	0
Internet Protocol Version 6	1.8	3	0.4	120	74	0	0	0
Internet Control Message Protocol v6	1.8	3	0.4	96	59	3	96	59
Internet Protocol Version 4	98.2	161	11.9	3220	1999	0	0	0
User Datagram Protocol	25.0	41	1.2	328	203	0	0	0
Data	25.0	41	35.7	9636	5982	41	9636	5982
Transmission Control Protocol	73.2	120	41.8	11277	7001	68	3342	2075
Transport Layer Security	31.7	52	23.2	6271	3893	52	6271	3893

UI – Conversations

Wireshark · Conversations · telnet-cooked.pcap

Ethernet · 1 | IPv4 · 1 | IPv6 | TCP · 1 | UDP

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
00:a0:cc:3b:bf:fa	00:00:c0:9f:a0:97	92	7748	48	3465	44	4283	0.000000	39.5713	700	865

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

Help | Copy | Follow Stream... | Graph... | Close

Wireshark · Conversations · telnet-cooked.pcap

Ethernet · 1 | IPv4 · 1 | IPv6 | TCP · 1 | UDP

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
192.168.0.2	192.168.0.1	92	7748	48	3465	44	4283	0.000000	39.5713	700	865

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

Help | Copy | Follow Stream... | Graph... | Close

Wireshark · Conversations · telnet-cooked.pcap

Ethernet · 1 | IPv4 · 1 | IPv6 | TCP · 1 | UDP

Address A	Port A	Address B	Port B	Packets	Bytes	Packets A → B	Bytes A → B	Packets B → A	Bytes B → A	Rel Start	Duration	Bits/s A → B	Bits/
192.168.0.2	1550	192.168.0.1	23	92	7748	48	3465	44	4283	0.000000	39.5713	700	

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

Help | Copy | Follow Stream... | Graph... | Close

UI – Flow Graph

Wireshark · Flow · telnet-cooked.pcap

Time	192.168.0.2		192.168.0.1	Comment
0.000000	1550	1550 → 23 [SYN] Seq=0 Win=32120 Len=0 ... →	23	TCP: 1550 → 23 [SYN] Seq=0 Win=32120 Len=...
0.002525	1550	← 23 → 1550 [SYN, ACK] Seq=0 Ack=1 Win=17...	23	TCP: 23 → 1550 [SYN, ACK] Seq=0 Ack=1 Win=...
0.002572	1550	1550 → 23 [ACK] Seq=1 Ack=1 Win=32120 Le... →	23	TCP: 1550 → 23 [ACK] Seq=1 Ack=1 Win=32120...
0.004160	1550	Telnet Data ... →	23	TELNET: Telnet Data ...
0.150335	1550	← Telnet Data ...	23	TELNET: Telnet Data ...
0.150402	1550	1550 → 23 [ACK] Seq=28 Ack=4 Win=32120 ... →	23	TCP: 1550 → 23 [ACK] Seq=28 Ack=4 Win=321...
0.150574	1550	Telnet Data ... →	23	TELNET: Telnet Data ...
0.151946	1550	← 23 → 1550 [ACK] Seq=4 Ack=31 Win=17376 ...	23	TCP: 23 → 1550 [ACK] Seq=4 Ack=31 Win=1737...
0.153657	1550	← Telnet Data ...	23	TELNET: Telnet Data ...
0.153865	1550	Telnet Data ... →	23	TELNET: Telnet Data ...
0.154984	1550	← 23 → 1550 [ACK] Seq=29 Ack=95 Win=17312...	23	TCP: 23 → 1550 [ACK] Seq=29 Ack=95 Win=17...
0.155577	1550	← Telnet Data ...	23	TELNET: Telnet Data ...
0.155656	1550	Telnet Data ... →	23	TELNET: Telnet Data ...
0.156646	1550	← 23 → 1550 [ACK] Seq=47 Ack=104 Win=1736...	23	TCP: 23 → 1550 [ACK] Seq=47 Ack=104 Win=17...
0.159016	1550	← Telnet Data ...	23	TELNET: Telnet Data ...
0.159227	1550	1550 → 23 [ACK] Seq=104 Ack=71 Win=3212... →	23	TCP: 1550 → 23 [ACK] Seq=104 Ack=71 Win=32...

Packet 16: TCP: 1550 → 23 [ACK] Seq=104 Ac...32120 Len=0 TSval=10233652 TSecr=2467372

Limit to display filter Flow type: All Flows Addresses: Any

Help Reset Diagram Export Close

UNIVERSIT

NSRC Network Startup Resource Center

Reviewing captured packets

Packet List

Apply a display filter ... <⌘/>

No.	Time	Source	Destination	Protocol	Length	Info
1	0.000000	192.168.0.2	192.168.0.1	TCP	74	1550 → 23 [SYN] Seq=0 Win=32120 Len=0 MSS=1460 SACK_PERM=1 TSval=10233636 TSecr=0 WS
2	0.002525	192.168.0.1	192.168.0.2	TCP	74	23 → 1550 [SYN, ACK] Seq=0 Ack=1 Win=17376 Len=0 MSS=1448 WS=1 TSval=2467372 TSecr=1
3	0.002572	192.168.0.2	192.168.0.1	TCP	66	1550 → 23 [ACK] Seq=1 Ack=1 Win=32120 Len=0 TSval=10233636 TSecr=2467372
4	0.004160	192.168.0.2	192.168.0.1	TELNET	93	Telnet Data ...
5	0.150335	192.168.0.1	192.168.0.2	TELNET	69	Telnet Data ...
6	0.150402	192.168.0.2	192.168.0.1	TCP	66	1550 → 23 [ACK] Seq=28 Ack=4 Win=32120 Len=0 TSval=10233651 TSecr=2467372
7	0.150574	192.168.0.2	192.168.0.1	TELNET	69	Telnet Data ...
8	0.151946	192.168.0.1	192.168.0.2	TCP	66	23 → 1550 [ACK] Seq=4 Ack=31 Win=17376 Len=0 TSval=2467372 TSecr=10233651
9	0.153657	192.168.0.1	192.168.0.2	TELNET	91	Telnet Data ...
10	0.153865	192.168.0.2	192.168.0.1	TELNET	130	Telnet Data ...
11	0.154984	192.168.0.1	192.168.0.2	TCP	66	23 → 1550 [ACK] Seq=29 Ack=95 Win=17312 Len=0 TSval=2467372 TSecr=10233651
12	0.155577	192.168.0.1	192.168.0.2	TELNET	84	Telnet Data ...
13	0.155656	192.168.0.2	192.168.0.1	TELNET	75	Telnet Data ...
14	0.156646	192.168.0.1	192.168.0.2	TCP	66	23 → 1550 [ACK] Seq=47 Ack=104 Win=17367 Len=0 TSval=2467372 TSecr=10233651
15	0.159016	192.168.0.1	192.168.0.2	TELNET	90	Telnet Data ...
16	0.159227	192.168.0.2	192.168.0.1	TCP	66	1550 → 23 [ACK] Seq=104 Ack=71 Win=32120 Len=0 TSval=10233652 TSecr=2467372
17	0.159844	192.168.0.2	192.168.0.1	TELNET	151	Telnet Data ...
18	0.161018	192.168.0.2	192.168.0.1	TCP	66	1550 → 23 [PSH, ACK] Seq=104 Ack=71 Win=32120 Len=0 TSval=10233652 TSecr=2467372
19	0.181267	192.168.0.1	192.168.0.2	TELNET	69	Telnet Data ...
20	0.181378	192.168.0.2	192.168.0.1	TELNET	69	Telnet Data ...
21	0.182515	192.168.0.1	192.168.0.2	TCP	66	23 → 1550 [ACK] Seq=74 Ack=192 Win=17373 Len=0 TSval=2467372 TSecr=10233654
22	0.196306	192.168.0.1	192.168.0.2	TELNET	78	Telnet Data ...
23	0.196427	192.168.0.2	192.168.0.1	TELNET	72	Telnet Data

> Frame 1: 74 bytes on wire (592 bits), 74 bytes captured (592 bits)

Packet List

- Columns
  - Time – the timestamp at which the packet crossed the interface.
  - Source – the originating host of the packet.
  - Destination – the host to which the packet was sent.
  - Protocol – the highest-level protocol that Wireshark can detect.
  - Length – the length in bytes of the packet on the wire.
  - Info – an informational message pertaining to the protocol in the protocol column.

Modifying time format

No.	Time	Source	Destination	Protocol
1	0.000000	192.168.0.2	192.168.0.1	TCP
2	0.002525	192.168.0.1	192.168.0.2	TCP
3	0.002572	192.168.0.2	192.168.0.1	TCP
4	0.004160	192.168.0.2	192.168.0.1	TELNET

No.	Time	Source	Destination	Protocol
1	1999-11-28 15:12:38.387203	192.168.0.2	192.168.0.1	TCP
2	1999-11-28 15:12:38.389728	192.168.0.1	192.168.0.2	TCP
3	1999-11-28 15:12:38.389775	192.168.0.2	192.168.0.1	TCP
4	1999-11-28 15:12:38.391363	192.168.0.2	192.168.0.1	TELNET

No.	Time	Source	Destination	Protocol
1	943755158.387203000	192.168.0.2	192.168.0.1	TCP
2	943755158.389728000	192.168.0.1	192.168.0.2	TCP
3	943755158.389775000	192.168.0.2	192.168.0.1	TCP
4	943755158.391363000	192.168.0.2	192.168.0.1	TELNET

No.	Time	Source	Destination	Protocol
1	0.000000	192.168.0.2	192.168.0.1	TCP
2	0.002525	192.168.0.1	192.168.0.2	TCP
3	0.000047	192.168.0.2	192.168.0.1	TCP
4	0.001588	192.168.0.2	192.168.0.1	TELNET

- Date and Time of Day (1970-01-01 01:02:03.123456)
- Year, Day of Year, and Time of Day (1970/001 01:02:03.123456)
- Time of Day (01:02:03.123456)
- Seconds Since 1970-01-01
- Seconds Since Beginning of Capture
- Seconds Since Previous Captured Packet
- Seconds Since Previous Displayed Packet
- UTC Date and Time of Day (1970-01-01 01:02:03.123456)
- UTC Year, Day of Year, and Time of Day (1970/001 01:02:03.123456)
- UTC Time of Day (01:02:03.123456)

Wireshark File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help

telnet-cooked.pcap

Apply a display filter ... <⌘/>

No.	Time	Source	Protocol	Length	Info
1	0.000000	192.16	TCP	74	1550 → 23 [SYN] Seq=0 Win=32120 Len=0 MSS=14
2	0.002525	192.16	TCP	74	23 → 1550 [SYN, ACK] Seq=0 Ack=1 Win=17376 L
3	0.002572	192.16	TCP	66	1550 → 23 [ACK] Seq=1 Ack=1 Win=32120 Len=0
4	0.004160	192.16	TELNET	93	Telnet Data ...
5	0.150335	192.16	TELNET	69	Telnet Data ...
6	0.150402	192.16	TCP	66	1550 → 23 [ACK] Seq=28 Ack=4 Win=32120 Len=0
7	0.150574	192.16			
8	0.151946	192.16			
9	0.153657	192.16			
10	0.153865	192.16			
11	0.154984	192.16			
12	0.155577	192.16			
13	0.155656	192.16			
14	0.156646	192.16			
15	0.159016	192.16			
16	0.159227	192.16			
17	0.159844	192.16			

> Frame 1: 74 bytes on wi
> Ethernet II, Src: Lite-
> Internet Protocol Versi
> Transmission Control Pr

```
0000  00 00 c0 9f a0 97 0
0010  00 3c 46 3c 40 00 4
0020  00 01 06 0e 00 17 9
0030  7d 78 e0 a3 00 00 0
0040  27 24 00 00 00 00 01 03  03 00
```

- ✓ Main Toolbar
- ✓ Filter Toolbar
- ✓ Status Bar
- Full Screen ^⌘F
- ✓ Packet List
- ✓ Packet Details
- ✓ Packet Bytes
- Packet Diagram
- Time Display Format >
- Name Resolution >
- Zoom >
- Expand Subtrees ⇧→
- Collapse Subtrees ⇧←
- Expand All ⌘→
- Collapse All ⌘←
- ✓ Colorize Packet List
- Coloring Rules...
- Colorize Conversation >
- Reset Layout ⇧⌘W
- Resize Columns ⇧⌘R
- Internals >
- Show Packet in New Window
- Reload as File Format/Capture ⇧⌘F
- Reload ⌘R

- Date and Time of Day (1970-01-01 01:02:03.123456) ⌥⌘1
- Year, Day of Year, and Time of Day (1970/001 01:02:03.123456)
- Time of Day (01:02:03.123456) ⌥⌘2
- Seconds Since 1970-01-01 ⌥⌘3
- ✓ Seconds Since Beginning of Capture ⌥⌘4
- Seconds Since Previous Captured Packet ⌥⌘5
- Seconds Since Previous Displayed Packet ⌥⌘6
- UTC Date and Time of Day (1970-01-01 01:02:03.123456) ⌥⌘7
- UTC Year, Day of Year, and Time of Day (1970/001 01:02:03.123456)
- UTC Time of Day (01:02:03.123456) ⌥⌘8
- ✓ Automatic (from capture file)
- Seconds
- Tenths of a second
- Hundredths of a second
- Milliseconds
- Microseconds
- Nanoseconds
- Display Seconds With Hours and Minutes

Reviewing specific captured packets

Layer 2

Apply a display filter ... <⌘/>

No.	Time	Source	Destination	Protocol	Length	Info
1	0.000000	192.168.0.2	192.168.0.1	TCP	74	1550 → 23 [SYN] Seq=0 Win=32120 Len=0 MSS=1460 SACK_PERM=1 TSval=10233636 TSecr=0 WS
2	0.002525	192.168.0.1	192.168.0.2	TCP	74	23 → 1550 [SYN, ACK] Seq=0 Ack=1 Win=17376 Len=0 MSS=1448 WS=1 TSval=2467372 TSecr=1
3	0.002572	192.168.0.2	192.168.0.1	TCP	66	1550 → 23 [ACK] Seq=1 Ack=1 Win=32120 Len=0 TSval=10233636 TSecr=2467372
4	0.004160	192.168.0.2	192.168.0.1	TELNET	93	Telnet Data ...
5	0.150335	192.168.0.1	192.168.0.2	TELNET	69	Telnet Data ...
6	0.150402	192.168.0.2	192.168.0.1	TCP	66	1550 → 23 [ACK] Seq=28 Ack=4 Win=32120 Len=0 TSval=10233651 TSecr=2467372

```
> Frame 4: 93 bytes on wire (744 bits), 93 bytes captured (744 bits)
v Ethernet II, Src: Lite-OnU_3b:bf:fa (00:a0:cc:3b:bf:fa), Dst: WesternD_9f:a0:97 (00:00:c0:9f:a0:97)
  > Destination: WesternD_9f:a0:97 (00:00:c0:9f:a0:97)
  > Source: Lite-OnU_3b:bf:fa (00:a0:cc:3b:bf:fa)
    Type: IPv4 (0x0800)
> Internet Protocol Version 4, Src: 192.168.0.2, Dst: 192.168.0.1
> Transmission Control Protocol, Src Port: 1550, Dst Port: 23, Seq: 1, Ack: 1, Len: 27
> Telnet
```

Layer 3

Apply a display filter ... <⌘/>

No.	Time	Source	Destination	Protocol	Length	Info
1	0.000000	192.168.0.2	192.168.0.1	TCP	74	1550 → 23 [SYN] Seq=0 Win=32120 Len=0 MSS=1460 SACK_PERM=1 TSval=10233636 TSecr=0 WS
2	0.002525	192.168.0.1	192.168.0.2	TCP	74	23 → 1550 [SYN, ACK] Seq=0 Ack=1 Win=17376 Len=0 MSS=1448 WS=1 TSval=2467372 TSecr=1
3	0.002572	192.168.0.2	192.168.0.1	TCP	66	1550 → 23 [ACK] Seq=1 Ack=1 Win=32120 Len=0 TSval=10233636 TSecr=2467372
4	0.004160	192.168.0.2	192.168.0.1	TELNET	93	Telnet Data ...
5	0.150335	192.168.0.1	192.168.0.2	TELNET	69	Telnet Data ...
6	0.150402	192.168.0.2	192.168.0.1	TCP	66	1550 → 23 [ACK] Seq=28 Ack=4 Win=32120 Len=0 TSval=10233651 TSecr=2467372

```
> Frame 4: 93 bytes on wire (744 bits), 93 bytes captured (744 bits)
> Ethernet II, Src: Lite-OnU_3b:bf:fa (00:a0:cc:3b:bf:fa), Dst: WesternD_9f:a0:97 (00:00:c0:9f:a0:97)
v Internet Protocol Version 4, Src: 192.168.0.2, Dst: 192.168.0.1
    0100 .... = Version: 4
    .... 0101 = Header Length: 20 bytes (5)
  > Differentiated Services Field: 0x10 (DSCP: Unknown, ECN: Not-ECT)
    Total Length: 79
    Identification: 0x463e (17982)
  > Flags: 0x40, Don't fragment
    ...0 0000 0000 0000 = Fragment Offset: 0
    Time to Live: 64
    Protocol: TCP (6)
    Header Checksum: 0x7307 [validation disabled]
    [Header checksum status: Unverified]
    Source Address: 192.168.0.2
    Destination Address: 192.168.0.1
> Transmission Control Protocol, Src Port: 1550, Dst Port: 23, Seq: 1, Ack: 1, Len: 27
> Telnet
```

Layer 4

Apply a display filter ... <⌘/>

No.	Time	Source	Destination	Protocol	Length	Info
1	0.000000	192.168.0.2	192.168.0.1	TCP	74	1550 → 23 [SYN] Seq=0 Win=32120 Len=0 MSS=1460 SACK_PERM=1 TSval=10233636 TSecr=0 WS
2	0.002525	192.168.0.1	192.168.0.2	TCP	74	23 → 1550 [SYN, ACK] Seq=0 Ack=1 Win=17376 Len=0 MSS=1448 WS=1 TSval=2467372 TSecr=1
3	0.002572	192.168.0.2	192.168.0.1	TCP	66	1550 → 23 [ACK] Seq=1 Ack=1 Win=32120 Len=0 TSval=10233636 TSecr=2467372
4	0.004160	192.168.0.2	192.168.0.1	TELNET	93	Telnet Data ...
5	0.150335	192.168.0.1	192.168.0.2	TELNET	69	Telnet Data ...
6	0.150402	192.168.0.2	192.168.0.1	TCP	66	1550 → 23 [ACK] Seq=28 Ack=4 Win=32120 Len=0 TSval=10233651 TSecr=2467372

```
> Frame 4: 93 bytes on wire (744 bits), 93 bytes captured (744 bits)
> Ethernet II, Src: Lite-OnU_3b:bf:fa (00:a0:cc:3b:bf:fa), Dst: WesternD_9f:a0:97 (00:00:c0:9f:a0:97)
> Internet Protocol Version 4, Src: 192.168.0.2, Dst: 192.168.0.1
v Transmission Control Protocol, Src Port: 1550, Dst Port: 23, Seq: 1, Ack: 1, Len: 27
    Source Port: 1550
    Destination Port: 23
    [Stream index: 0]
    [Conversation completeness: Complete, WITH_DATA (31)]
    [TCP Segment Len: 27]
    Sequence Number: 1    (relative sequence number)
    Sequence Number (raw): 2579865837
    [Next Sequence Number: 28    (relative sequence number)]
    Acknowledgment Number: 1    (relative ack number)
    Acknowledgment number (raw): 401695550
    1000 .... = Header Length: 32 bytes (8)
  > Flags: 0x018 (PSH, ACK)
    Window: 32120
    [Calculated window size: 32120]
    [Window size scaling factor: 1]
    Checksum: 0x6e67 [unverified]
    [Checksum Status: Unverified]
    Urgent Pointer: 0
  > Options: (12 bytes), No-Operation (NOP), No-Operation (NOP), Timestamps
  > [Timestamps]
  > [SEQ/ACK analysis]
    TCP payload (27 bytes)
> Telnet
```

Layer 7

Apply a display filter ... <⌘/>

No.	Time	Source	Destination	Protocol	Length	Info
1	0.000000	192.168.0.2	192.168.0.1	TCP	74	1550 → 23 [SYN] Seq=0 Win=32120 Len=0 MSS=1460 SACK_PERM=1 TSval=10233636 TSecr=0 WS
2	0.002525	192.168.0.1	192.168.0.2	TCP	74	23 → 1550 [SYN, ACK] Seq=0 Ack=1 Win=17376 Len=0 MSS=1448 WS=1 TSval=2467372 TSecr=1
3	0.002572	192.168.0.2	192.168.0.1	TCP	66	1550 → 23 [ACK] Seq=1 Ack=1 Win=32120 Len=0 TSval=10233636 TSecr=2467372
4	0.004160	192.168.0.2	192.168.0.1	TELNET	93	Telnet Data ...
5	0.150335	192.168.0.1	192.168.0.2	TELNET	69	Telnet Data ...
6	0.150402	192.168.0.2	192.168.0.1	TCP	66	1550 → 23 [ACK] Seq=28 Ack=4 Win=32120 Len=0 TSval=10233651 TSecr=2467372

```
> Frame 4: 93 bytes on wire (744 bits), 93 bytes captured (744 bits)
> Ethernet II, Src: Lite-OnU_3b:bf:fa (00:a0:cc:3b:bf:fa), Dst: WesternD_9f:a0:97 (00:00:c0:9f:a0:97)
> Internet Protocol Version 4, Src: 192.168.0.2, Dst: 192.168.0.1
> Transmission Control Protocol, Src Port: 1550, Dst Port: 23, Seq: 1, Ack: 1, Len: 27
v Telnet
  v Do Suppress Go Ahead
      Command: Do (253)
      Subcommand: Suppress Go Ahead
  v Will Terminal Type
      Command: Will (251)
      Subcommand: Terminal Type
  v Will Negotiate About Window Size
      Command: Will (251)
      Subcommand: Negotiate About Window Size
  v Will Terminal Speed
      Command: Will (251)
      Subcommand: Terminal Speed
  v Will Remote Flow Control
      Command: Will (251)
      Subcommand: Remote Flow Control
  > Will Linemode
  > Will New Environment Option
  > Do Status
  > Will X Display Location
```

Raw Packet

```
> Will Linemode
> Will New Environment Option
> Do Status
> Will X Display Location
```

```
0000  00 00 c0 9f a0 97 00 a0  cc 3b bf fa 08 00 45 10   ····· ·;····E·
0010  00 4f 46 3e 40 00 40 06  73 07 c0 a8 00 02 c0 a8   ·OF>@·@· s·····
0020  00 01 06 0e 00 17 99 c5  a0 ed 17 f1 63 3e 80 18   ····· ····c>··
0030  7d 78 6e 67 00 00 01 01  08 0a 00 9c 27 24 00 25   }xng···· ····'$·%
0040  a6 2c ff fd 03 ff fb 18  ff fb 1f ff fb 20 ff fb   ·,····· ····· ··
0050  21 ff fb 22 ff fb 27 ff  fd 05 ff fb 23            !··"··'· ····#
```

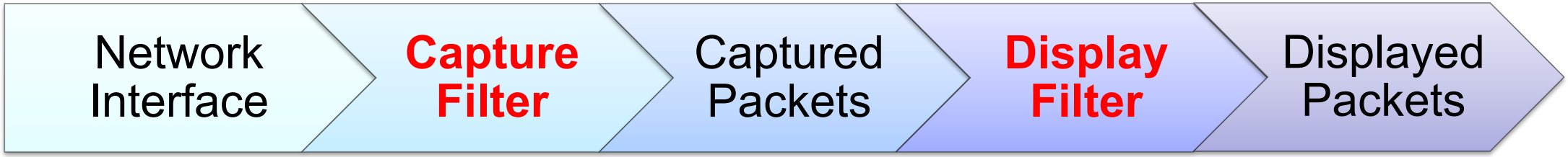
Demo raw packet highlighting

Remember this?

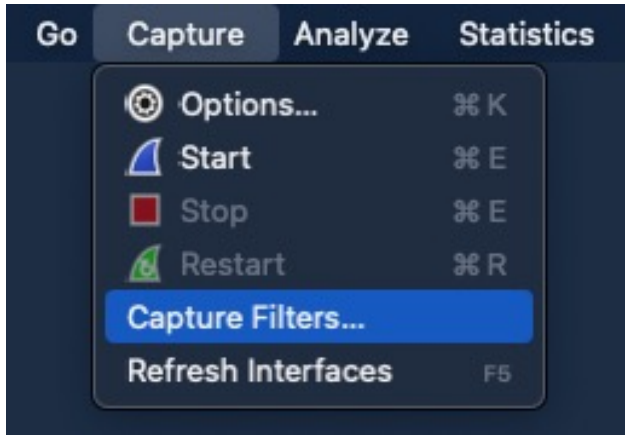
Filtering

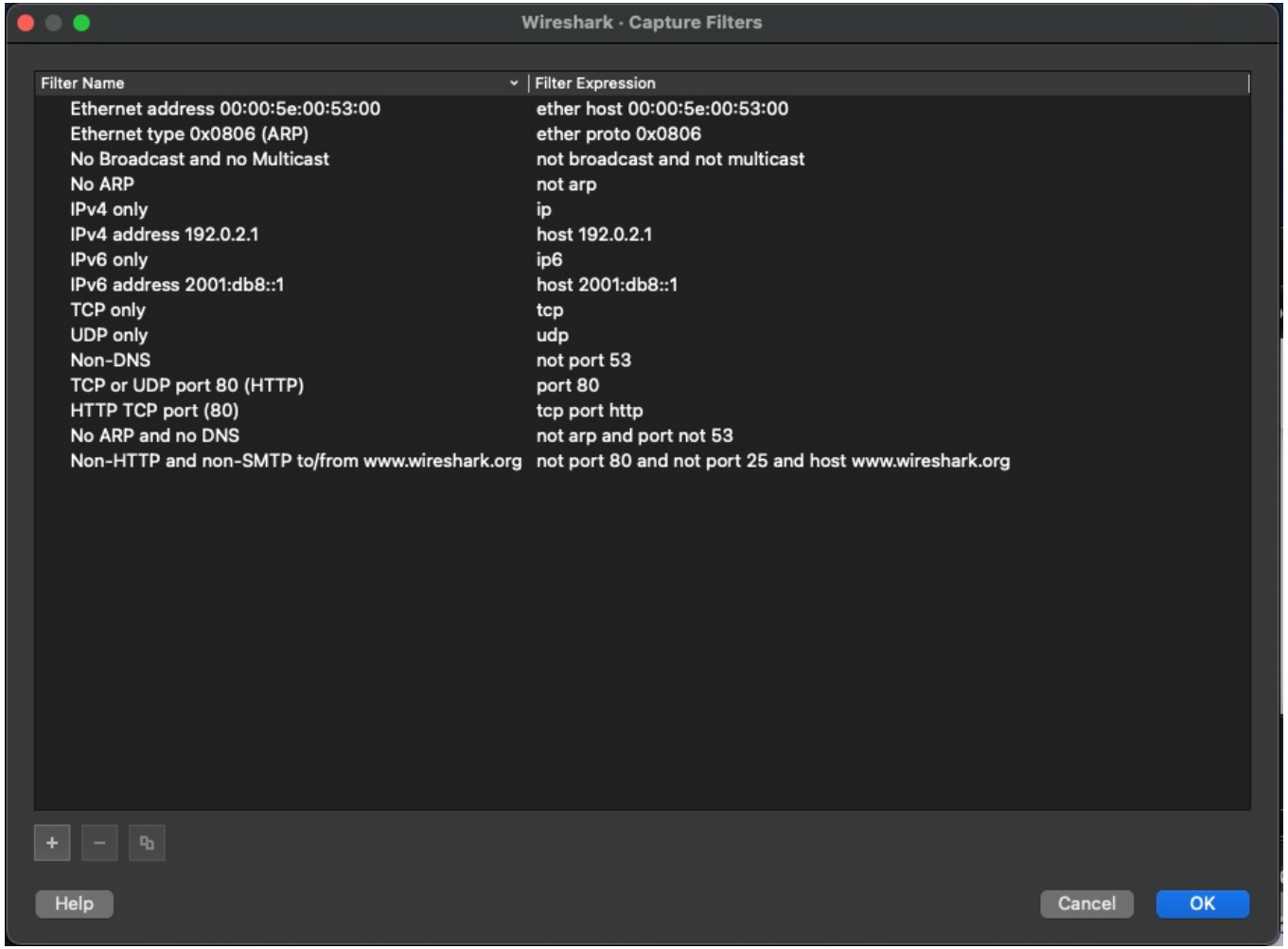
- Capture Filters
- Display Filters
  - Enter Expression Directly
  - Use Expressions Editor

Filtering


Network Interface
Capture Filter
Captured Packets
Display Filter
Displayed Packets

Filtering – Capture Filters





Filter Name	Filter Expression
Ethernet address 00:00:5e:00:53:00	ether host 00:00:5e:00:53:00
Ethernet type 0x0806 (ARP)	ether proto 0x0806
No Broadcast and no Multicast	not broadcast and not multicast
No ARP	not arp
IPv4 only	ip
IPv4 address 192.0.2.1	host 192.0.2.1
IPv6 only	ip6
IPv6 address 2001:db8::1	host 2001:db8::1
TCP only	tcp
UDP only	udp
Non-DNS	not port 53
TCP or UDP port 80 (HTTP)	port 80
HTTP TCP port (80)	tcp port http
No ARP and no DNS	not arp and port not 53
Non-HTTP and non-SMTP to/from www.wireshark.org	not port 80 and not port 25 and host www.wireshark.org

Display Filters – Enter Expression Directly

ip.addr == 192.168.0.2

No.	Time	Source	Destination	P
1	0.000000	192.168.0.2	192.168.0.1	T
2	0.002525	192.168.0.1	192.168.0.2	T
3	0.002572	192.168.0.2	192.168.0.1	T
4	0.004160	192.168.0.2	192.168.0.1	T

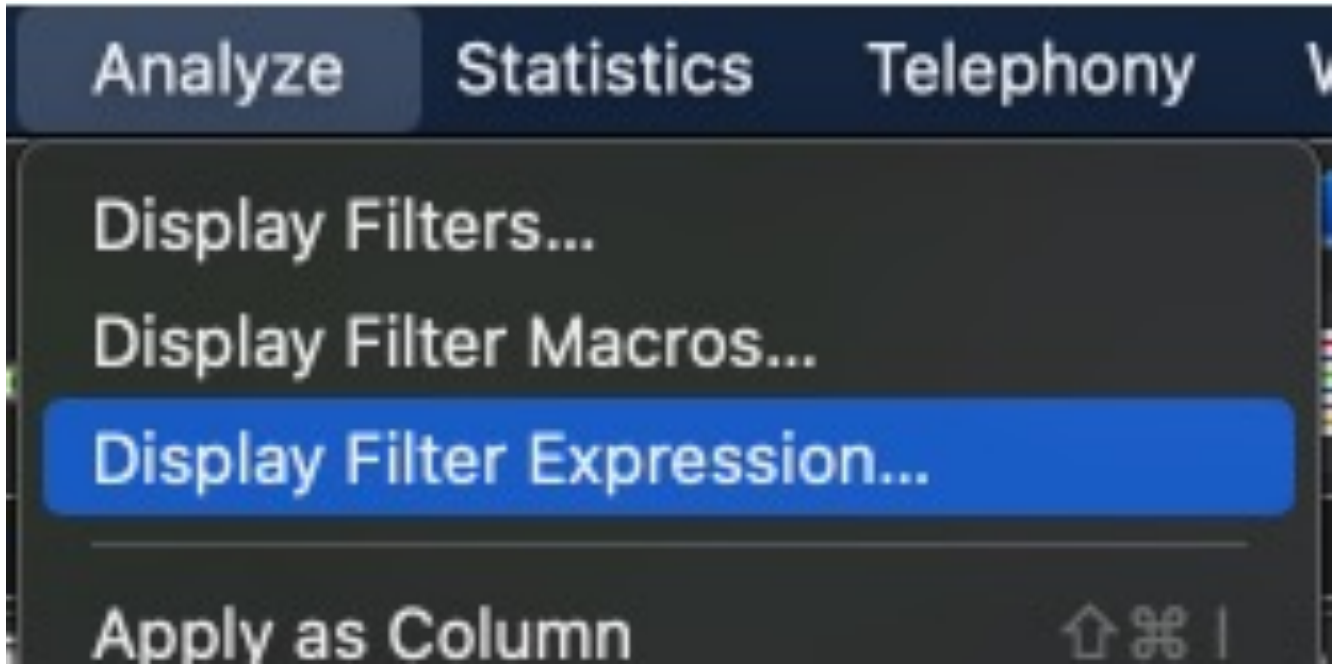
ip.addr == 192.168.0.RUBBISH

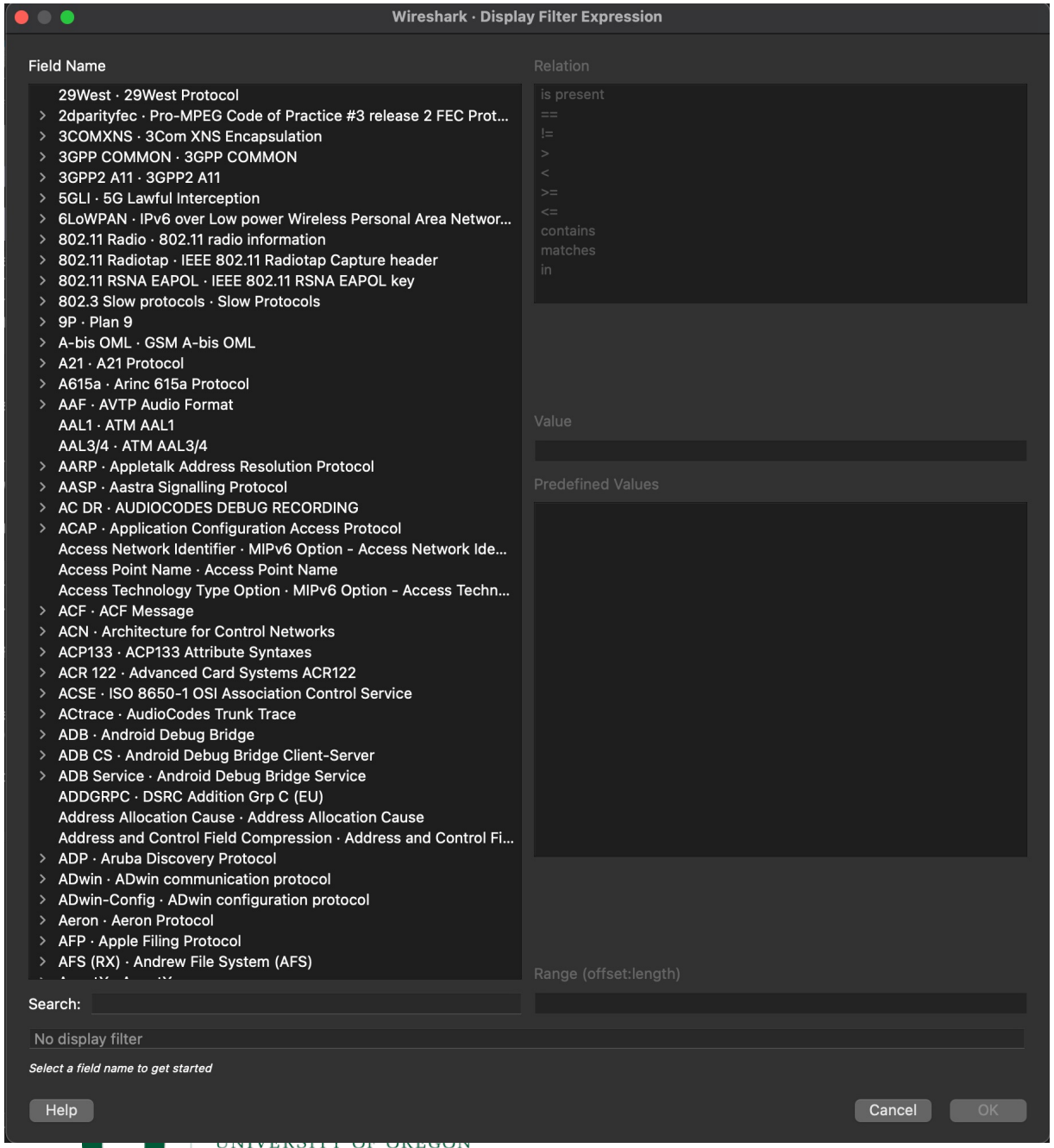
No.	Time	Source	Destination
1	0.000000	192.168.0.2	192.168.0.1
2	0.002525	192.168.0.1	192.168.0.2
3	0.002572	192.168.0.2	192.168.0.1
4	0.004160	192.168.0.2	192.168.0.1
5	0.150335	192.168.0.1	192.168.0.2
6	0.150402	192.168.0.2	192.168.0.1

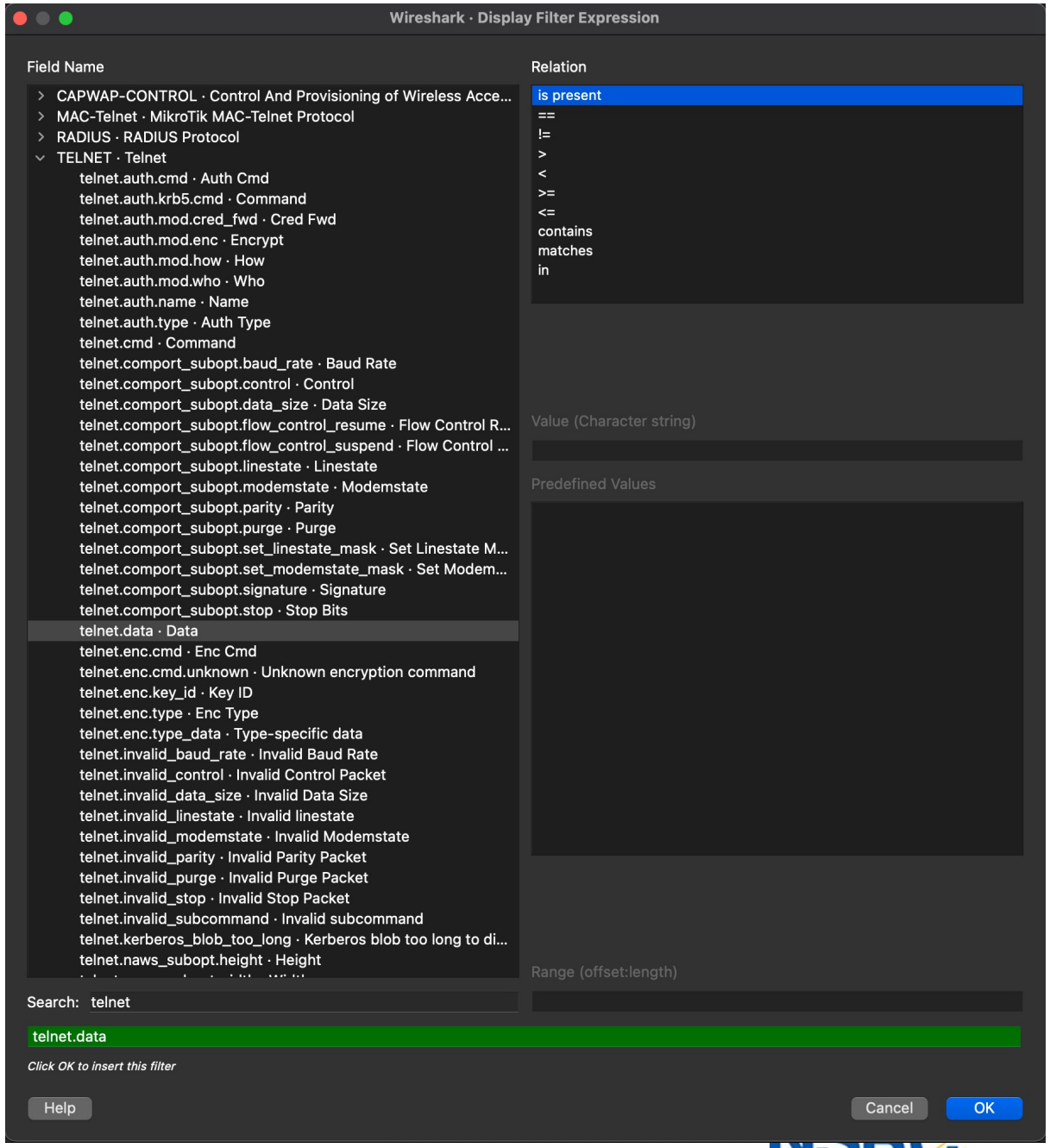
Display Filter examples

- **http.request** – Display all HTTP requests.
- **http.request || http.response** – Display all HTTP request and responses.
- **ip.addr == 127.0.0.1** – Display all IP packets whose source or destination is localhost.
- **tcp.len < 100** – Display all TCP packets whose data length is less than 100 bytes.
- **http.request.uri matches "(gif)$"** - Display all HTTP requests in which the uri ends with "gif".
- **dns.query.name == "www.google.com"** - Display all DNS queries for "www.google.com".

Display Filters – Use the expressions editor




Wireshark · Display Filter Expression
Field Name
Relation
29West · 29West Protocol
2dparityfec · Pro-MPEG Code of Practice #3 release 2 FEC Prot...
3COMXNS · 3Com XNS Encapsulation
3GPP COMMON · 3GPP COMMON
3GPP2 A11 · 3GPP2 A11
5GLI · 5G Lawful Interception
6LoWPAN · IPv6 over Low power Wireless Personal Area Networ...
802.11 Radio · 802.11 radio information
802.11 Radiotap · IEEE 802.11 Radiotap Capture header
802.11 RSNA EAPOL · IEEE 802.11 RSNA EAPOL key
802.3 Slow protocols · Slow Protocols
9P · Plan 9
A-bis OML · GSM A-bis OML
A21 · A21 Protocol
A615a · Arinc 615a Protocol
AAF · AVTP Audio Format
AAL1 · ATM AAL1
AAL3/4 · ATM AAL3/4
AARP · Appletalk Address Resolution Protocol
AASP · Aastra Signalling Protocol
AC DR · AUDIOCODES DEBUG RECORDING
ACAP · Application Configuration Access Protocol
Access Network Identifier · MIPv6 Option - Access Network Ide...
Access Point Name · Access Point Name
Access Technology Type Option · MIPv6 Option - Access Techn...
ACF · ACF Message
ACN · Architecture for Control Networks
ACP133 · ACP133 Attribute Syntaxes
ACR 122 · Advanced Card Systems ACR122
ACSE · ISO 8650-1 OSI Association Control Service
ACtrace · AudioCodes Trunk Trace
ADB · Android Debug Bridge
ADB CS · Android Debug Bridge Client-Server
ADB Service · Android Debug Bridge Service
ADDGRPC · DSRC Addition Grp C (EU)
Address Allocation Cause · Address Allocation Cause
Address and Control Field Compression · Address and Control Fi...
ADP · Aruba Discovery Protocol
ADwin · ADwin communication protocol
ADwin-Config · ADwin configuration protocol
Aeron · Aeron Protocol
AFP · Apple Filing Protocol
AFS (RX) · Andrew File System (AFS)
is present
==
!=
>
<
>=
<=
contains
matches
in
Value
Predefined Values
Range (offset:length)
Search:
No display filter
Select a field name to get started
Help
Cancel
OK


Wireshark · Display Filter Expression
Field Name
Relation
CAPWAP-CONTROL · Control And Provisioning of Wireless Acce...
MAC-Telnet · MikroTik MAC-Telnet Protocol
RADIUS · RADIUS Protocol
TELNET · Telnet
telnet.auth.cmd · Auth Cmd
telnet.auth.krb5.cmd · Command
telnet.auth.mod.cred_fwd · Cred Fwd
telnet.auth.mod.enc · Encrypt
telnet.auth.mod.how · How
telnet.auth.mod.who · Who
telnet.auth.name · Name
telnet.auth.type · Auth Type
telnet.cmd · Command
telnet.comport_subopt.baud_rate · Baud Rate
telnet.comport_subopt.control · Control
telnet.comport_subopt.data_size · Data Size
telnet.comport_subopt.flow_control_resume · Flow Control R...
telnet.comport_subopt.flow_control_suspend · Flow Control ...
telnet.comport_subopt.linestate · Linestate
telnet.comport_subopt.modemstate · Modemstate
telnet.comport_subopt.parity · Parity
telnet.comport_subopt.purge · Purge
telnet.comport_subopt.set_linestate_mask · Set Linestate M...
telnet.comport_subopt.set_modemstate_mask · Set Modem...
telnet.comport_subopt.signature · Signature
telnet.comport_subopt.stop · Stop Bits
telnet.data · Data
telnet.enc.cmd · Enc Cmd
telnet.enc.cmd.unknown · Unknown encryption command
telnet.enc.key_id · Key ID
telnet.enc.type · Enc Type
telnet.enc.type_data · Type-specific data
telnet.invalid_baud_rate · Invalid Baud Rate
telnet.invalid_control · Invalid Control Packet
telnet.invalid_data_size · Invalid Data Size
telnet.invalid_linestate · Invalid linestate
telnet.invalid_modemstate · Invalid Modemstate
telnet.invalid_parity · Invalid Parity Packet
telnet.invalid_purge · Invalid Purge Packet
telnet.invalid_stop · Invalid Stop Packet
telnet.invalid_subcommand · Invalid subcommand
telnet.kerberos_blob_too_long · Kerberos blob too long to di...
telnet.naws_subopt.height · Height
is present
==
!=
>
<
>=
<=
contains
matches
in
Value (Character string)
Predefined Values
Range (offset:length)
Search: telnet
telnet.data
Click OK to insert this filter
Help
Cancel
OK

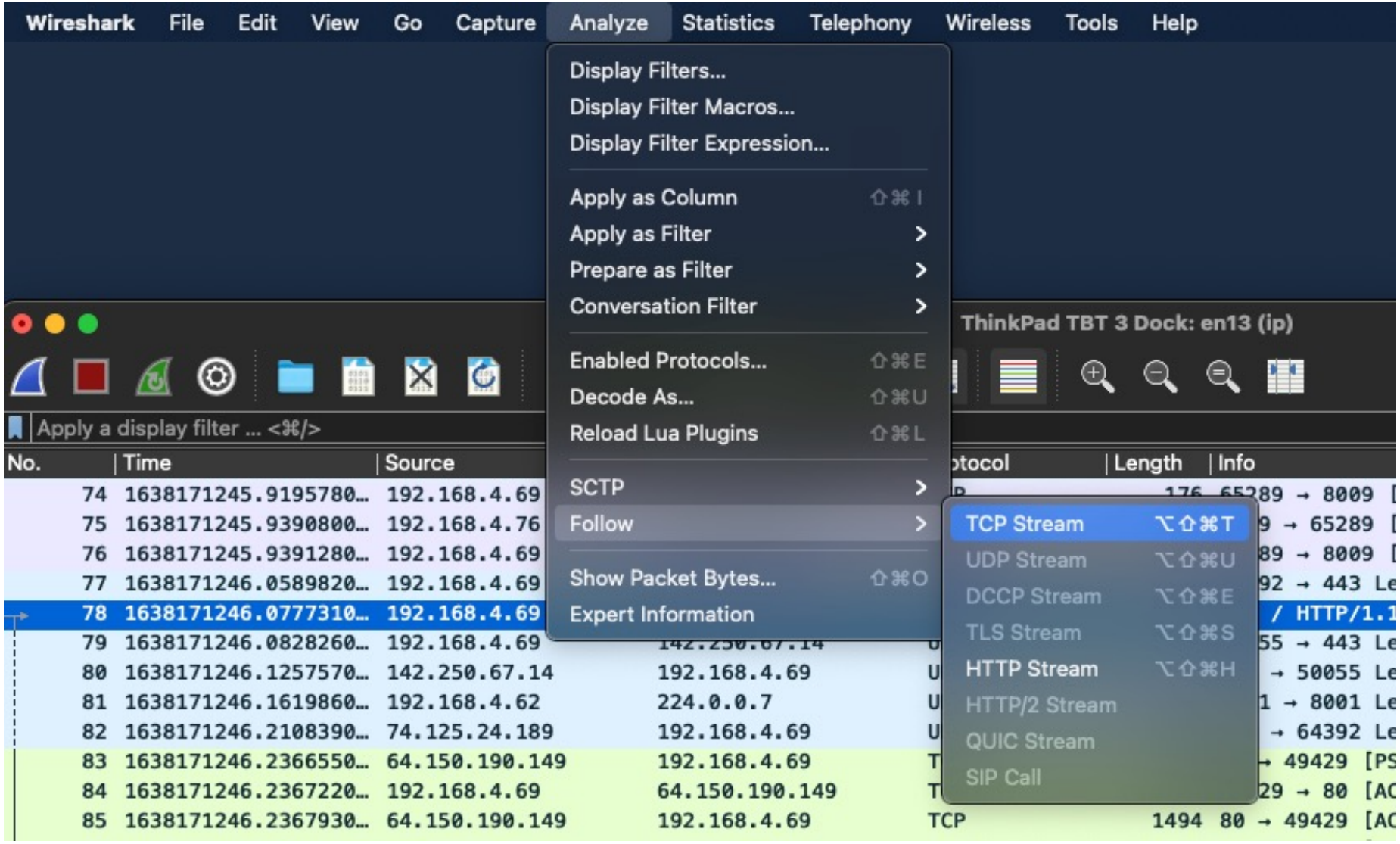
telnet.data

No.	Time	Source	Destination	Protocol	Length	Info
27	0.210527	192.168.0.1	192.168.0.2	TELNET	98	Telnet Data ...
29	1.317863	192.168.0.1	192.168.0.2	TELNET	73	Telnet Data ...
31	2.561993	192.168.0.2	192.168.0.1	TELNET	72	Telnet Data ...
36	2.577672	192.168.0.1	192.168.0.2	TELNET	75	Telnet Data ...
38	3.581505	192.168.0.2	192.168.0.1	TELNET	72	Telnet Data ...
40	3.847152	192.168.0.1	192.168.0.2	TELNET	68	Telnet Data ...
45	5.141492	192.168.0.1	192.168.0.2	TELNET	126	Telnet Data ...
47	5.161150	192.168.0.1	192.168.0.2	TELNET	554	Telnet Data ...
49	5.198668	192.168.0.1	192.168.0.2	TELNET	68	Telnet Data ...
51	19.908277	192.168.0.2	192.168.0.1	TELNET	92	Telnet Data ...
55	20.313976	192.168.0.1	192.168.0.2	TELNET	117	Telnet Data ...
57	20.387293	192.168.0.1	192.168.0.2	TELNET	130	Telnet Data ...

> Frame 27: 98 bytes on wire (784 bits), 98 bytes captured (784 bits)
> Ethernet II, Src: WesternD_9f:a0:97 (00:00:c0:9f:a0:97), Dst: Lite-On_3b:bf:fa (00:a0:cc:3b:bf:fa)

Following a stream

No.	Time	Source	Destination	Protocol	Length	Info
74	1638171245.9195780…	192.168.4.69	192.168.4.76	TCP	176	65289 → 8009 [PSH, ACK] Seq=1 Ack=1 Win=2048 Len=110 TSval=3003906371 TSec
75	1638171245.9390800…	192.168.4.76	192.168.4.69	TCP	176	8009 → 65289 [PSH, ACK] Seq=1 Ack=111 Win=277 Len=110 TSval=6096536 TSecr=
76	1638171245.9391280…	192.168.4.69	192.168.4.76	TCP	66	65289 → 8009 [ACK] Seq=111 Ack=111 Win=2046 Len=0 TSval=3003906390 TSecr=6
77	1638171246.0589820…	192.168.4.69	74.125.24.189	UDP	75	64392 → 443 Len=33
78	1638171246.0777310…	192.168.4.69	64.150.190.149	HTTP	1012	GET / HTTP/1.1
79	1638171246.0828260…	192.168.4.69	142.250.67.14	UDP	75	50055 → 443 Len=33
80	1638171246.1257570…	142.250.67.14	192.168.4.69	UDP	68	443 → 50055 Len=26
81	1638171246.1619860…	192.168.4.62	224.0.0.7	UDP	240	8001 → 8001 Len=198
82	1638171246.2108390…	74.125.24.189	192.168.4.69	UDP	67	443 → 64392 Len=25
83	1638171246.2366550…	64.150.190.149	192.168.4.69	TCP	658	80 → 49429 [PSH, ACK] Seq=1 Ack=947 Win=252 Len=592 TSval=582748517 TSecr=
84	1638171246.2367220…	192.168.4.69	64.150.190.149	TCP	66	49429 → 80 [ACK] Seq=947 Ack=593 Win=2038 Len=0 TSval=3237570255 TSecr=582
85	1638171246.2367930…	64.150.190.149	192.168.4.69	TCP	1494	80 → 49429 [ACK] Seq=593 Ack=947 Win=252 Len=1428 TSval=582748517 TSecr=32
86	1638171246.2367940…	64.150.190.149	192.168.4.69	TCP	1494	80 → 49429 [ACK] Seq=2021 Ack=947 Win=252 Len=1428 TSval=582748517 TSecr=3
87	1638171246.2368170…	192.168.4.69	64.150.190.149	TCP	66	49429 → 80 [ACK] Seq=947 Ack=3449 Win=2003 Len=0 TSval=3237570255 TSecr=58
88	1638171246.2369490…	64.150.190.149	192.168.4.69	TCP	1494	80 → 49429 [ACK] Seq=3449 Ack=947 Win=252 Len=1428 TSval=582748517 TSecr=3237570


Wireshark
File
Edit
View
Go
Capture
Analyze
Statistics
Telephony
Wireless
Tools
Help
Display Filters...
Display Filter Macros...
Display Filter Expression...
Apply as Column
Apply as Filter
Prepare as Filter
Conversation Filter
Enabled Protocols...
Decode As...
Reload Lua Plugins
SCTP
Follow
Show Packet Bytes...
Expert Information
TCP Stream
UDP Stream
DCCP Stream
TLS Stream
HTTP Stream
HTTP/2 Stream
QUIC Stream
SIP Call
ThinkPad TBT 3 Dock: en13 (ip)
Apply a display filter ... <⌘/>
No.
Time
Source
Length
Info

ThinkPad TBT 3 Dock: en13 (ip)

tcp.stream eq 12

No.	Time	Source	Destination	Protocol	Length	Info
78	1638171246.0777310…	192.168.4.69	64.150.190.149	HTTP	1012	GET / HTTP/1.1
83	1638171246.2366550…	64.150.190.149	192.168.4.69	TCP	658	80 → 49429 [PSH, ACK] Seq=1 Ack=947 Win=252 Len=592 TSval=582748517 TSecr=
84	1638171246.2367220…	192.168.4.69	64.150.190.149	TCP	66	49429 → 80 [ACK] Seq=947 Ack=593 Win=2038 Len=0 TSval=3237570255 TSecr=582
85	1638171246.2367930…	64.150.190.149	192.168.4.69	TCP	1494	80 → 49429 [ACK] Seq=593 Ack=947 Win=252 Len=1428 TSval=582748517 TSecr=32
86	1638171246.2367940…	64.150.190.149	192.168.4.69	TCP	1494	80 → 49429 [ACK] Seq=2021 Ack=947 Win=252 Len=1428 TSval=582748517 TSecr=3
87	1638171246.2368170…	192.168.4.69	64.150.190.149	TCP	66	49429 → 80 [ACK] Seq=947 Ack=3449 Win=2003 Len=0 TSval=3237570255 TSecr=58
88	1638171246.2369490…	64.150.190.149	192.168.4.69	TCP	1494	80 → 49429 [ACK] Seq=3449 Ack=947 Win=252 Len=1428 TSval=582748517 TSecr=3
89	1638171246.2369500…	64.150.190.149	192.168.4.69	TCP	1494	80 → 49429 [ACK] Seq=4877 Ack=947 Win=252 Len=1428 TSval=582748517 TSecr=3
90	1638171246.2369510…	64.150.190.149	192.168.4.69	TCP	1494	80 → 49429 [ACK] Seq=6305 Ack=947 Win=252 Len=1428 TSval=582748517 TSecr=3
91	1638171246.2369760…	192.168.4.69	64.150.190.149	TCP	66	49429 → 80 [ACK] Seq=947 Ack=7733 Win=1936 Len=0 TSval=3237570255 TSecr=58
92	1638171246.2371380…	64.150.190.149	192.168.4.69	TCP	1494	80 → 49429 [ACK] Seq=7733 Ack=947 Win=252 Len=1428 TSval=582748517 TSecr=3
93	1638171246.2371580…	192.168.4.69	64.150.190.149	TCP	66	49429 → 80 [ACK] Seq=947 Ack=9161 Win=1914 Len=0 TSval=3237570255 TSecr=58
94	1638171246.2372800…	64.150.190.149	192.168.4.69	TCP	1494	80 → 49429 [ACK] Seq=9161 Ack=947 Win=252 Len=1428 TSval=582748517 TSecr=3
95	1638171246.2372810…	64.150.190.149	192.168.4.69	TCP	1494	80 → 49429 [ACK] Seq=10589 Ack=947 Win=252 Len=1428 TSval=582748517 TSecr=
96	1638171246.2372820…	64.150.190.149	192.168.4.69	TCP	1494	80 → 49429 [ACK] Seq=12017 Ack=947 Win=252 Len=1428 TSval=582748517 TSecr=3237570

Wireshark · Follow TCP Stream (tcp.stream eq 12) · ThinkPad TBT 3 Dock: en13 (ip)

```
GET / HTTP/1.1
Host: www.pita.org.fj
Connection: keep-alive
Cache-Control: max-age=0
Upgrade-Insecure-Requests: 1
User-Agent: Mozilla/5.0 (Macintosh; Intel Mac OS X 10_15_7) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/96.0.4664.55 Safari/537.36
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/avif,image/webp,image/apng,*/*;q=0.8,application/signed-exchange;v=b3;q=0.9
Referer: https://www.google.com/
Accept-Encoding: gzip, deflate
Accept-Language: en-GB,en-US;q=0.9,en;q=0.8
Cookie: CFID=12739267; CFTOKEN=46499e25c047fee7-2A098EFE-0E1E-940B-5970EFC19338682F;
CFGLOBALS=urltoken%3DCFID%23%3D12739267%26CFTOKEN%23%3D46499e25c047fee7%2D2A098EFE%2D0E1E%2D940B%2D5970EFC19338682F%23lastvisit%3D%7Bts%20%272021
%2D11%2D29%2020%3A33%3A47%27%7D%23hitcount%3D3%23timecreated%3D%7Bts%20%272021%2D11%2D29%2020%3A33%3A46%27%7D%23cftoken%3D46499e25c047fee7%2D2A09
8EFE%2D0E1E%2D940B%2D5970EFC19338682F%23cfid%3D12739267%23

HTTP/1.1 200 OK
Transfer-Encoding: chunked
Content-Type: text/html;charset=UTF-8
Server: Microsoft-IIS/7.5
Set-Cookie:
CFGLOBALS=urltoken%3DCFID%23%3D12739267%26CFTOKEN%23%3D46499e25c047fee7%2D2A098EFE%2D0E1E%2D940B%2D5970EFC19338682F%23lastvisit%3D%7Bts%20%272021
%2D11%2D29%2020%3A34%3A05%27%7D%23hitcount%3D4%23timecreated%3D%7Bts%20%272021%2D11%2D29%2020%3A33%3A46%27%7D%23cftoken%3D46499e25c047fee7%2D2A09
8EFE%2D0E1E%2D940B%2D5970EFC19338682F%23cfid%3D12739267%23; Expires=Wed, 22-Nov-2051 07:34:05 GMT; Path=/; HttpOnly
X-Powered-By: ASP.NET
Date: Mon, 29 Nov 2021 07:34:05 GMT

5013
<!DOCTYPE HTML PUBLIC "-//W3C//DTD HTML 4.01 Transitional//EN" "http://www.w3.org/TR/html4/loose.dtd">
<html>
<head>
<title>PITA :: Pacific Islands Telecommunications Association</title>
<meta http-equiv="Content-Type" content="text/html; charset=iso-8859-1">
<meta name="keywords" content="PITA, pacific, islands, telecommunications, association, island, nations, Pacific Region ">
<meta name="description" content="The Pacific Islands Telecommunications Association (PITA) is a non-profit organisation formed to represent the
interests of small island nations in the Pacific Region in the field of telecommunications. ">
<link href="styles.css" rel="stylesheet" type="text/css">
<link rel="shortcut icon" href="favicon.ico" type="image/x-icon">
<link rel="stylesheet" type="text/css" href="ajaxtabs/ajaxtabs.css" />



<script type="text/javascript" src="_resources/articles/image-fade.js"></script>
<script type="text/javascript" src="_resources/js/date-time.js"></script>
<script type="text/javascript" src="_resources/js/showtext.js"></script>


<script type="text/javascript" src="ajaxtabs/ajaxtabs.js">

/***********************************************
* Ajax Tabs Content script v2.1- .. Dynamic Drive DHTML code library (www.dynamicdrive.com)
* This notice MUST stay intact for legal use
* Visit Dynamic Drive at http://www.dynamicdrive.com/ for full source code
***********************************************/

</script>
```

3 client pkts, 20 server pkts, 5 turns.

Entire conversation (27 kB) | Show data as ASCII | Stream 12

Find: | Find Next

Help | Filter Out This Stream | Print | Save as... | Back | Close

Demo – Telnet

- Don’t forget to follow the TCP stream

Demo – SIP

- Don’t forget to play the telephone call

Demp – BGP

- Don’t forget to look for the disconnect message

Mystery

```
$ tcpdump -n -s 0 -r mystery.pcap
reading from file mystery.pcap, link-type EN10MB (Ethernet)

16:35:03.821897 IP6 2402:f000:1:8e01::5555 > 2607:fcd0:100:2300::b108:2a6b: IP
16.0.0.200 > 192.52.166.154: GREv1, call 6016, seq 430001, ack 539254, length 119: IP
172.16.44.3.40768 > 8.8.8.8.53: 42540+ AAAA? xqt-detect-mode2-97712e88-167a-45b9-93ee-
913140e76678. (71)

16:35:04.035791 IP6 2607:fcd0:100:2300::b108:2a6b > 2402:f000:1:8e01::5555: IP
192.52.166.154 > 16.0.0.200: GREv1, call 17, seq 539320, length 190: IP 8.8.8.8.53 >
172.16.44.3.40768: 42540 NXDomain 0/1/0 (146)
```

No.	Time	Source	Destination	Protocol	Length	Info
1	0.000000	172.16.44.3	8.8.8.8	DNS	197	Standard query 0xa6
2	0.213894	8.8.8.8	172.16.44.3	DNS	268	Standard query resp

```
> Frame 1: 197 bytes on wire (1576 bits), 197 bytes captured (1576 bits)
> Ethernet II, Src: JuniperN_f2:61:3d (00:12:1e:f2:61:3d), Dst: c5:00:00:00:82:c4 (c5:00:00:00:82:c4)
> 802.1Q Virtual LAN, PRI: 0, DEI: 0, ID: 100
> Internet Protocol Version 6, Src: 2402:f000:1:8e01::5555, Dst: 2607:fcd0:100:2300::b108:2a6b
> Internet Protocol Version 4, Src: 16.0.0.200, Dst: 192.52.166.154
> Generic Routing Encapsulation (PPP)
> Point-to-Point Protocol
> Internet Protocol Version 4, Src: 172.16.44.3, Dst: 8.8.8.8
> User Datagram Protocol, Src Port: 40768, Dst Port: 53
> Domain Name System (query)
```

```
0000  c5 00 00 00 82 c4 00 12  1e f2 61 3d 81 00 00 64   ······ ·· ·a=···d
0010  86 dd 60 00 00 00 00 8b  04 f6 24 02 f0 00 00 01   ··`····· ··$·····
0020  8e 01 00 00 00 00 00 00  55 55 26 07 fc d0 01 00   ····· UU&·····
0030  23 00 00 00 00 00 b1 08  2a 6b 45 00 00 8b 8c af   #····· *kE·····
0040  00 00 40 2f 75 fe 10 00  00 c8 c0 34 a6 9a 30 81   ··@/u··· ···4··0·
0050  88 0b 00 67 17 80 00 06  8f b1 00 08 3a 76 ff 03   ···g···· ····:v··
0060  00 21 45 00 00 63 00 00  40 00 3c 11 56 67 ac 10   ·!E··c·· @·<·Vg··
0070  2c 03 08 08 08 08 9f 40  00 35 00 4f 2d 23 a6 2c   ,·····@ ·5·O-#·,
0080  01 00 00 01 00 00 00 00  00 00 35 78 71 74 2d 64   ····· ··5xqt-d
0090  65 74 65 63 74 2d 6d 6f  64 65 32 2d 39 37 37 31   etect-mo de2-9771
00a0  32 65 38 38 2d 31 36 37  61 2d 34 35 62 39 2d 39   2e88-167 a-45b9-9
00b0  33 65 65 2d 39 31 33 31  34 30 65 37 36 36 37 38   3ee-9131 40e76678
00c0  00 00 1c 00 01                                     ·····
```

Demo – GRE

Demo – OSPF over GRE

Extending Wireshark - Lua

- Too long for this tutorial.

- https://wiki.wireshark.org/Lua/Dissectors

```lua
-- trivial protocol example
-- declare our protocol
trivial_proto = Proto("trivial","Trivial Protocol")
-- create a function to dissect it
function trivial_proto.dissector(buffer,pinfo,tree)
    pinfo.cols.protocol = "TRIVIAL"
    local subtree = tree:add(trivial_proto,buffer(),"Trivial Protocol Data")
    subtree:add(buffer(0,2),"The first two bytes: " .. buffer(0,2):uint())
    subtree = subtree:add(buffer(2,2),"The next two bytes")
    subtree:add(buffer(2,1),"The 3rd byte: " .. buffer(2,1):uint())
    subtree:add(buffer(3,1),"The 4th byte: " .. buffer(3,1):uint())
end
-- load the udp.port table
udp_table = DissectorTable.get("udp.port")
-- register our protocol to handle udp port 7777
udp_table:add(7777,trivial_proto)
```

Questions?

Thank you