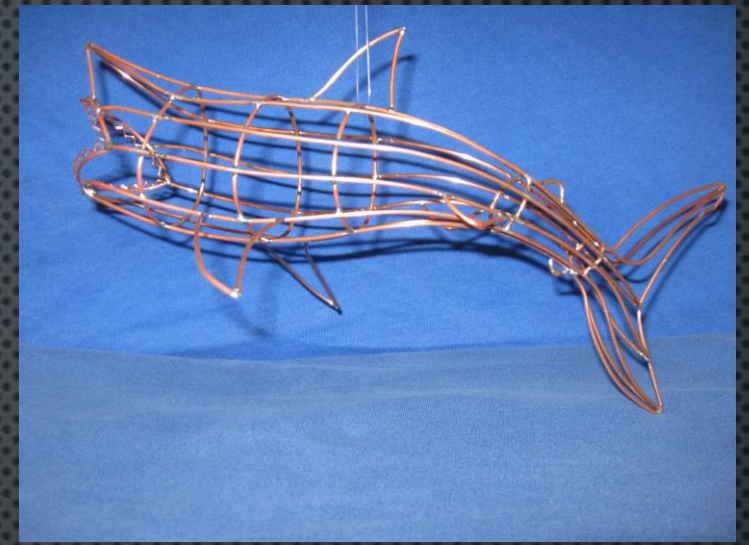


10 THINGS I WANT TO SHOW YOU ABOUT WIRESHARK

KEVAN VANHOFF

SOME WORDS ON WIRESHARK



- WIRESHARK IS THE WORLD'S FOREMOST NETWORK PROTOCOL ANALYZER. IT LETS YOU SEE WHAT'S HAPPENING ON YOUR NETWORK AT A MICROSCOPIC LEVEL. IT IS THE DE FACTO (AND OFTEN DE JURE) STANDARD ACROSS MANY INDUSTRIES AND EDUCATIONAL INSTITUTIONS.
- WIRESHARK IS VULNERABLE (ALWAYS UPDATE!)
- WIRESHARK IS OPEN SOURCE AND FREE

If you want to follow along, the PCAP file in the screen shots is available at: <http://smashbadger.com/http.zip>

GENERAL RULES FOR WIRESHARK

- YOU SHOULD RARELY NEED TO SCROLL TO FIND THINGS
- YOU SHOULD NEVER HAVE TO SEARCH FOR MORE THAN 30 SECONDS FOR THE PACKETS YOU CARE ABOUT
- “DON’T WORRY ABOUT GETTING RID OF THE ANTS WHEN YOU’VE GOT ELEPHANTS.”
- EVERY NETWORK IS FULL OF LITTLE PROBLEMS. DON’T GET DISTRACTED BY LOW VALUE ENDEAVORS. YOU HAVE MORE IMPORTANT THINGS TO DO.
- SYSTEMS WANT THE THING THEY ASKED FOR, THE FIRST TIME THEY ASK, AND THEY DON’T WANT TO HAVE TO WAIT VERY LONG FOR IT.

THE UI

The image shows the Wireshark network protocol analyzer interface. The title bar reads "http.pcap.pcapng". The menu bar includes File, Edit, View, Go, Capture, Analyze, Statistics, Telephony, Wireless, Tools, and Help. The toolbar contains icons for file operations, capture, analysis, and statistics. A filter bar at the top of the packet list shows "Apply a display filter ... <Ctrl-/>". The packet list table displays 17 packets with columns for No., Time, Source, Destination, Stream index, Protocol, Length, Data, and Name. The selected packet (No. 1) is an MDNS packet from 192.168.1.161 to 224.0.0.251. The packet details pane shows the structure of the first packet: Frame 1: 81 bytes on wire (648 bits), 81 bytes captured (648 bits) on interface wlan0, id 0; Ethernet II, Src: RivetNet_f0:2f:e9 (9c:b6:d0:f0:2f:e9), Dst: IPv4mcast_fb (01:00:5e:00:00:fb); Internet Protocol Version 4, Src: 192.168.1.161, Dst: 224.0.0.251; User Datagram Protocol, Src Port: 5353, Dst Port: 5353; Multicast Domain Name System (query). The packet bytes pane shows the raw data in hexadecimal and ASCII. Annotations with green arrows point to the Main Toolbar, Filter Toolbar, Packet List, Packet Details, and Packet Bytes sections.

Main Toolbar

Filter Toolbar

Packet List

Packet Details

Packet Bytes

No.	Time	Source	Destination	Stream index	Protocol	Length	Data	Name
1	0.000000000	192.168.1.161	224.0.0.251		MDNS	81		_ultimaker_tcp.local
2	1.431481653	192.168.1.1	255.255.255.255		UDP	215	4b414e4e4f55254e00000...	
3	2.557902682	192.168.1.164	224.0.0.251		MDNS	81		DESKTOP-5K3JDSR.local
4	2.558068348	192.168.1.164	224.0.0.251		MDNS	119		
5	4.503585585	192.168.1.1	255.255.255.255		UDP	215	4b414e4e4f55254e00000...	
6	7.575605641	192.168.1.1	255.255.255.255		UDP	215	4b414e4e4f55254e00000...	
7	7.679021647	192.168.1.152	192.168.1.255		UDP	288	544346320200000049443...	
8	8.917721972	192.168.1.120	162.159.200.123		NTP	90		
9	8.939011204	162.159.200.123	192.168.1.120		NTP	90		
10	10.547063387	192.168.1.1	255.255.255.255		UDP	215	4b414e4e4f55254e00000...	
11	10.918071988	192.168.1.120	204.11.201.12		NTP	90		
12	10.918314362	192.168.1.120	162.159.200.1		NTP	90		
13	10.918382320	192.168.1.120	171.66.97.126		NTP	90		
14	10.944906901	204.11.201.12	192.168.1.120		NTP	90		
15	10.947687638	162.159.200.1	192.168.1.120		NTP	90		
16	10.964252475	171.66.97.126	192.168.1.120		NTP	90		
17	13.615855251	192.168.1.1	255.255.255.255		UDP	215	4b414e4e4f55254e00000...	

> Frame 1: 81 bytes on wire (648 bits), 81 bytes captured (648 bits) on interface wlan0, id 0
> Ethernet II, Src: RivetNet_f0:2f:e9 (9c:b6:d0:f0:2f:e9), Dst: IPv4mcast_fb (01:00:5e:00:00:fb)
> Internet Protocol Version 4, Src: 192.168.1.161, Dst: 224.0.0.251
> User Datagram Protocol, Src Port: 5353, Dst Port: 5353
> Multicast Domain Name System (query)

```
0000 01 00 5e 00 00 fb 9c b6 d0 f0 2f e9 08 00 45 00  ..^......./...E.
0010 00 43 14 79 00 00 ff 11 03 ec c0 a8 01 a1 e0 00  .C.y.....
0020 00 fb 14 e9 14 e9 00 2f 4d 57 00 00 00 00 01  ....../ MW.....
0030 00 00 00 00 00 00 0a 5f 75 6c 74 69 6d 61 6b 65  ...._ultimake
0040 72 04 5f 74 63 70 05 6c 6f 63 61 6c 00 00 0c 00  r_tcp_l ocal...
0050 01
```

http.pcap.pcapng | Packets: 39342 · Displayed: 39342 (100.0%) | Profile: Default

CAPTURING

The image shows the Wireshark network protocol analyzer interface. A green box labeled "Status" has a large green arrow pointing down to the status bar at the bottom. Another green box labeled "Notice the graphs" has a green arrow pointing to the packet list and packet details pane. A third green box labeled "Mouse-over connections to check IP or get other clues" has a green arrow pointing to the mouse-over tooltip for the selected interface.

Capture

...using this filter:

Interfaces shown ▼

Interface	Graph
vEthernet (NAT-inside)	
VirtualBox Host-Only Network	
Local Area Connection* 9	
Local Area Connection* 1	
Local Area Connection* 2	
Bluetooth Network Connection 2	
Network Bridge	
vEthernet (internet)	
Local Area Connection* 10	
Local Area Connection* 8	
vEthernet (Default Switch)	
Adapter for loopback traffic capture	

Status

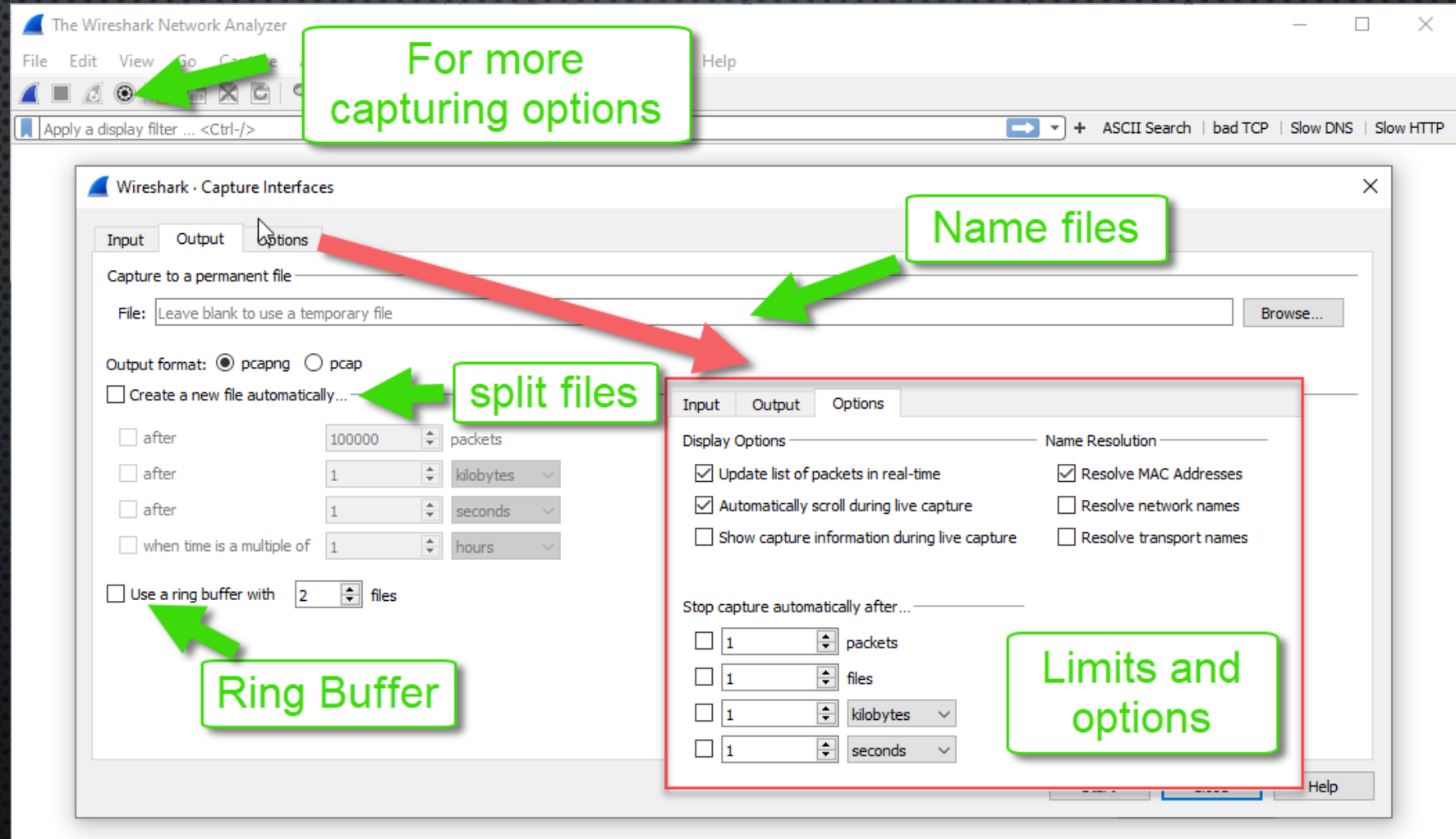
Learn

[User's Guide](#) · [Wiki](#) · [Questions and Answers](#) · [Mailing Lists](#)

You are running Wireshark 3.2.3 (v3.2.3-0-gf39b50865a13). You receive automatic updates.

Ready to load or capture | No Packets | Profile: example-profile

CAPTURING



CAPTURE FILTERS

Capture

...using this filter:

☐ not tcp port 22 and not tcp port 3389



All interfaces shown ▼

vEthernet (NAT-inside)
VirtualBox Host-Only Network
Local Area Connection* 9
Local Area Connection* 1
Local Area Connection* 2
Bluetooth Network Connection 2
Network Bridge
vEthernet (internet)
Local Area Connection* 10
Local Area Connection* 8
vEthernet (Default Switch)
Adapter for loopback traffic capture

if you have remote
access into a
machine, avoid
capturing the session

Learn

[User's Guide](#) · [Wiki](#) · [Questions and Answers](#) · [Mailing Lists](#)

You are running Wireshark 3.2.3 (v3.2.3-0-gf39b50865a13). You receive automatic updates.

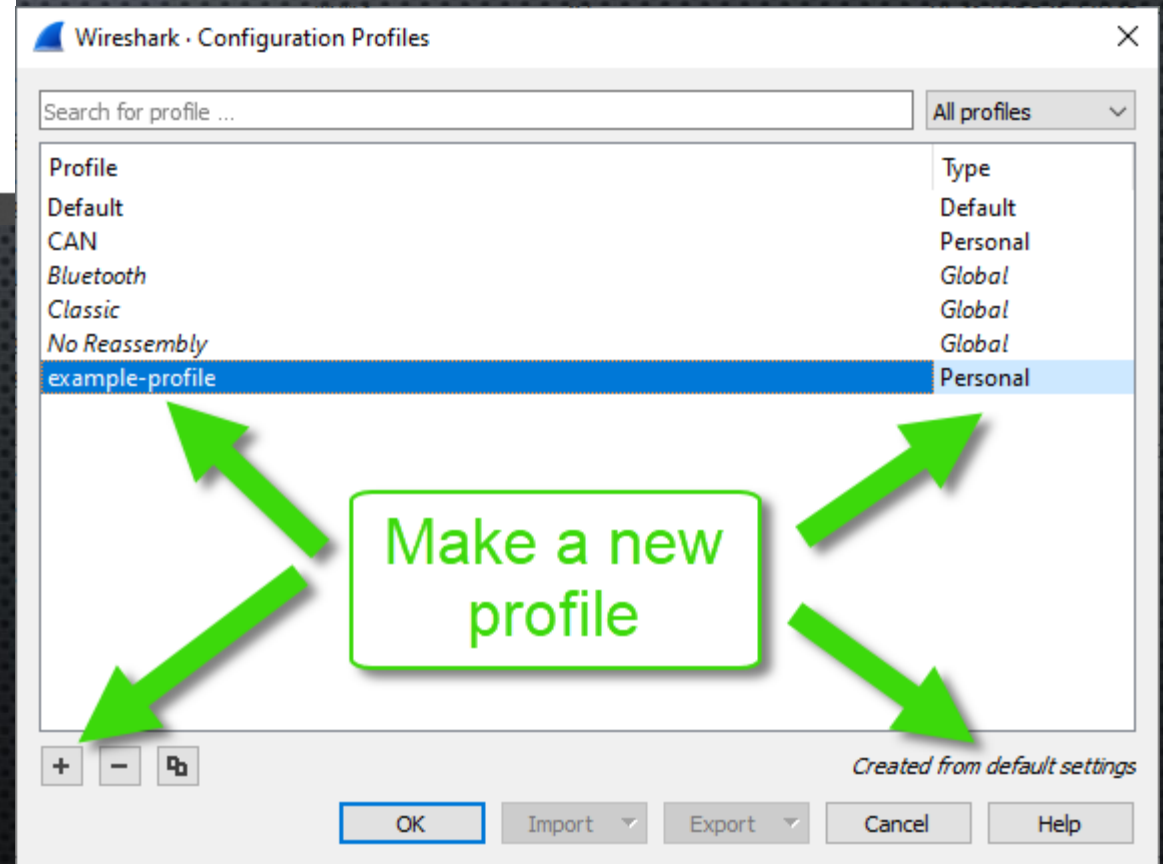
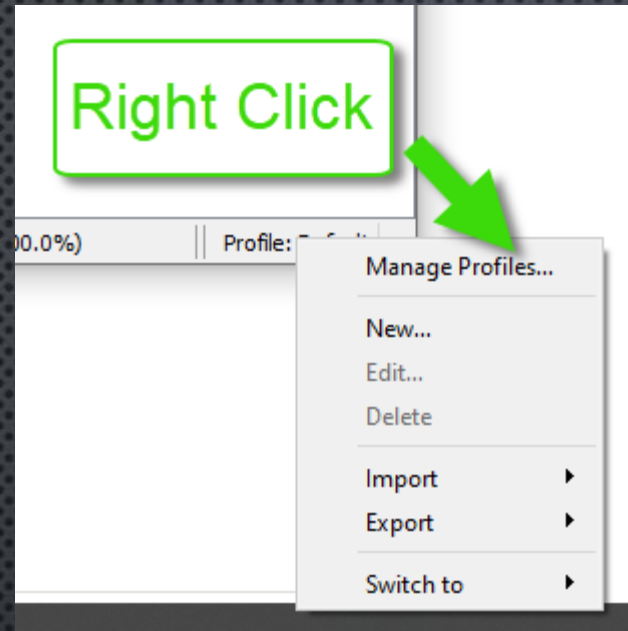
CAPTURE FILTERS

- CAPTURE FILTERS ARE NOT DISPLAY FILTERS THEY ARE BPF/PCAP FORMAT
- CAPTURE FILTERS REDUCE THE SIZE OF A CAPTURE RATHER THAN HIDE PACKETS FROM THE LIST
- HERE ARE SOME USEFUL BPF EXAMPLES
 - NOT TCP PORT 22 AND NOT TCP PORT 3389
 - HOST 192.168.5.20
 - NET 192.168.0.0/24
 - NOT BROADCAST AND NOT MULTICAST
 - IP (THIS GETS RID OF ARP AND STP FRAMES)
 - $((\text{NOT ETHER PROTO } 0x8100) \text{ AND } (\text{TCP SRC PORT } 443 \text{ AND } (\text{TCP}[(\text{TCP}[12] \& 0xF0) \gg 4] * 4] = 0x18) \text{ AND } (\text{TCP}[(\text{TCP}[12] \& 0xF0) \gg 4] * 4 + 1] = 0x03) \text{ AND } (\text{TCP}[(\text{TCP}[12] \& 0xF0) \gg 4] * 4 + 2] < 0x04) \text{ AND } ((\text{IP}[2:2] - 4 * (\text{IP}[0] \& 0x0F) - 4 * ((\text{TCP}[12] \& 0xF0) \gg 4) > 69)))) \text{ OR } (\text{VLAN AND } (\text{TCP SRC PORT } 443 \text{ AND } (\text{TCP}[(\text{TCP}[12] \& 0xF0) \gg 4] * 4] = 0x18) \text{ AND } (\text{TCP}[(\text{TCP}[12] \& 0xF0) \gg 4] * 4 + 1] = 0x03) \text{ AND } (\text{TCP}[(\text{TCP}[12] \& 0xF0) \gg 4] * 4 + 2] < 0x04) \text{ AND } ((\text{IP}[2:2] - 4 * (\text{IP}[0] \& 0x0F) - 4 * ((\text{TCP}[12] \& 0xF0) \gg 4) > 69))))$

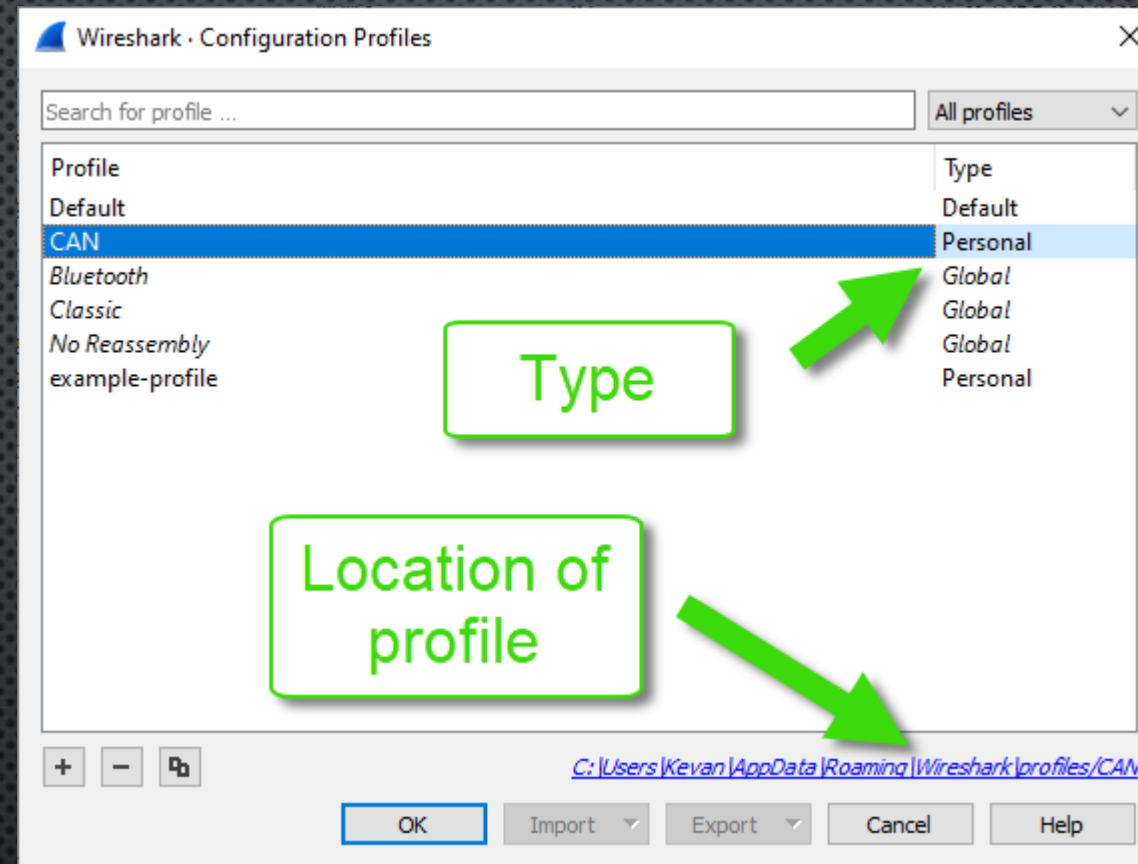
That's heartbleed



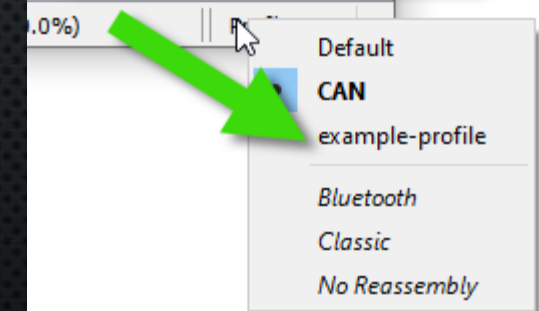
PROFILES



PROFILES



Click and switch to new profile



THE FRAME

The image shows a Wireshark packet capture of a DNS response. The packet list at the top shows several DNS queries and responses. The selected packet (No. 923) is a DNS response from 192.168.1.1 to 192.168.1.120. The packet details pane shows the structure of the packet, including the Ethernet II header, Internet Protocol Version 4 header, User Datagram Protocol header, and the Domain Name System (response) section. The packet bytes pane at the bottom shows the raw data in hexadecimal and ASCII.

Picture the OSI model upside down

Anything inside [] is calculated by Wireshark

Dissected info from the packet

HEX 'n ASCII

No.	Time	Source	Destination	Protocol	Length	Info
909	37.791537370	192.168.1.1	192.168.1.120	DNS	130	Standard query response 0xc01f A www.wired.com CNAME h2.conde...
910	37.791641203	192.168.1.1	192.168.1.120	DNS	142	Standard query response 0x3620 A www.theguardian.com CNAME du...
913	37.791745911	192.168.1.1	192.168.1.120	DNS	122	Standard query response 0xcd67 A simplisafe.com A 54.236.67.1...
921	37.805415679	192.168.1.1	192.168.1.120	DNS	126	Standard query response 0xc2a3 A www.vox.com CNAME vox-chorus...
923	37.811340276	192.168.1.1	192.168.1.120	DNS	138	Standard query response 0xcfb3 A lifehacker.com A 151.101.2.1...
925	37.816680667	192.168.1.1	192.168.1.120	DNS	138	Standard query response 0x1e29 A www.rollingstone.com CNAME...
934	38.320807172	192.168.1.1	192.168.1.120	DNS	103	Standard query response 0x722 A safebrowsing.google.com CNAME...
949	38.409890788	192.168.1.1	192.168.1.120	DNS	124	Standard query response 0x8489 A ocs.pki.goog A 157.140.2.2...
4816	39.828653919	192.168.1.1	192.168.1.120	DNS	166	Standard query response 0xb2e A skillet.lifef...

> Frame 923: 138 bytes on wire (1104 bits), 138 bytes captured (1104 bits) on interface wlan0, id 0

> Ethernet II, Src: Tp-LinkT_cf:5a:88 (0c:80:63:cf:5a:88), Dst: AMPAKTec_2e:e0:1c (c0:84:7d:2e:e0:1c)

> Internet Protocol Version 4, Src: 192.168.1.1, Dst: 192.168.1.120

> User Datagram Protocol, Src Port: 53, Dst Port: 48347

Source Port: 53

Destination Port: 48347

Length: 104

Checksum: 0x80de [unverified]

[Checksum Status: Unverified]

[Stream index: 53]

> [Timestamps]

[Time since first frame: 0.018070414 seconds]

[Time since previous frame: 0.018035706 seconds]

> Domain Name System (response)

Transaction ID: 0xcfb3

> Flags: 0x8180 Standard query response, No error

Questions: 1

Answer RRs: 4

Authority RRs: 0

Additional RRs: 0

> Queries

> Answers

lifehacker.com: type A, class IN, addr 151.101.2.166

Name: lifehacker.com

Type: A (Host Address) (1)

Class: IN (0x0001)

Time to live: 1742 (29 minutes, 2 seconds)

Data length: 4

Address: 151.101.2.166

```
0000 c0 84 7d 2e e0 1c 0c 80 63 cf 5a 88 08 00 45 40  ...}. ... c.Z...E@
0010 00 7c 00 00 40 00 39 11 bd 67 c0 a8 01 01 c0 a8  ...|. ...9...g...
0020 01 78 00 35 bc db 00 68 80 de cf b3 81 80 00 01  ...x.5...h...
0030 00 04 00 00 00 00 0a 6c 69 66 65 68 61 63 6b 65  ........l ifehacke
0040 72 03 63 6f 6d 00 00 01 00 01 c0 0c 00 01 00 01  ...r.com...
0050 00 00 06 ce 00 04 97 65 02 a6 c0 0c 00 01 00 01  ........e...
0060 00 00 06 ce 00 04 97 65 42 a6 c0 0c 00 01 00 01  ........e B...
```

Response Address (dns.a), 4 bytes

Packets: 39342 · Displayed: 118 (0.3%)

Profile: example-profile

STREAMS

The image shows the Wireshark network protocol analyzer interface. The top menu bar includes File, Edit, View, Go, Capture, Analyze, Statistics, Telephony, Wireless, Tools, and Help. The toolbar contains various icons for file operations, capture, and analysis. The main display area is divided into three panes: the packet list, packet details, and packet bytes.

Packet List Pane: Displays a list of captured packets. The selected packet is 5760, which is an HTTP GET request. A red circle with the number 1 is placed over the packet number 5760.

Packet Details Pane: Shows the hierarchical structure of the selected packet. The selected protocol is Hypertext Transfer Protocol. A red circle with the number 2 is placed over the 'Hypertext Transfer Protocol' entry.

Packet Bytes Pane: Displays the raw bytes of the selected packet in hexadecimal and ASCII format. A red circle with the number 3 is placed over the 'Hypertext Transfer Protocol' entry in the details pane.

Context Menu: A right-click context menu is open over the selected packet. The menu options include: Mark/Unmark Packet (Ctrl+M), Ignore/Unignore Packet (Ctrl+D), Set/Unset Time Reference (Ctrl+T), Time Shift... (Ctrl+Shift+T), Packet Comment... (Ctrl+Alt+C), Edit Resolved Name, Apply as Filter, Prepare as Filter, Conversation Filter, Colorize Conversation, SCTP, Follow (Ctrl+Alt+Shift+T), Copy, Protocol Preferences, Decode As..., and Show Packet in New Window. The 'Follow' option is highlighted, and a sub-menu is open showing the following streams: TCP Stream (Ctrl+Alt+Shift+T), UDP Stream (Ctrl+Alt+Shift+U), TLS Stream (Ctrl+Alt+Shift+S), HTTP Stream (Ctrl+Alt+Shift+H), HTTP/2 Stream, and QUIC Stream. A red circle with the number 3 is placed over the 'HTTP Stream' option.

Annotations:

- Right Click on a packet in the stream you want to follow
- I follow the highest layer protocol available (when it makes sense)

The status bar at the bottom shows: http.pcap.pcapng | Packets: 39342 · Displayed: 657 (1.7%) | Profile: example-profile

STREAMS

Wireshark · Follow HTTP Stream (tcp.stream eq 25) · http.pcap.pcapng

```
GET / HTTP/1.1
Host: 192.168.1.133
User-Agent: Mozilla/5.0 (X11; Ubuntu; Linux aarch64; rv:71.0) Gecko/20100101 Firefox/71.0
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,*/*;q=0.8
Accept-Language: en-US,en;q=0.5
Accept-Encoding: gzip, deflate
Connection: keep-alive
Upgrade-Insecure-Requests: 1

HTTP/1.1 200 OK
Content-Length: 376024
X-Robots-Tag: noindex, nofollow, noimageindex
X-Content-Type-Options: nosniff
Last-Modified: Wed, 08 Apr 2020 04:39:22 GMT
Etag: "ec6df094ef83fc8971882dc58f52fa18717c8fc0"
X-From-Cache: true
Cache-Control: no-cache, must-revalidate
X-Clacks-Overhead: GNU Terry Pratchett
Content-Type: text/html; charset=utf-8
X-Frame-Options: sameorigin

<!DOCTYPE html>
<html>
  <head>
    <title data-bind="text: title">OctoPrint</title>

    <link rel="shortcut icon" href="/static/img/tentacle-32x32.png">
    <link rel="mask-icon" href="/static/img/mask.svg" color="#56BE37">
    <link rel="mask-icon-theme" href="/static/img/mask-theme.svg" color="#56BE37">
    <link rel="apple-touch-icon" sizes="114x114" href="/static/img/apple-touch-icon-114x114.png">
    <link rel="apple-touch-icon" sizes="144x144" href="/static/img/apple-touch-icon-144x144.png">

    <meta name="robots" content="noindex, nofollow, noimageindex">
    <meta name="referrer" content="no-referrer">
    <meta name="theme-color" data-bind="attr: { content: theme_color }">

    <link href="/static/webassets/packed_libs.css?ec88168c" rel="stylesheet" media="all">
    <link href="/static/webassets/packed_core.css?b577b523" rel="stylesheet" media="all">

    <script src="/static/js/lib/less.min.js" type="text/javascript"></script>
    <script type="text/javascript">
```

Client request

Server Response

that's the webpage

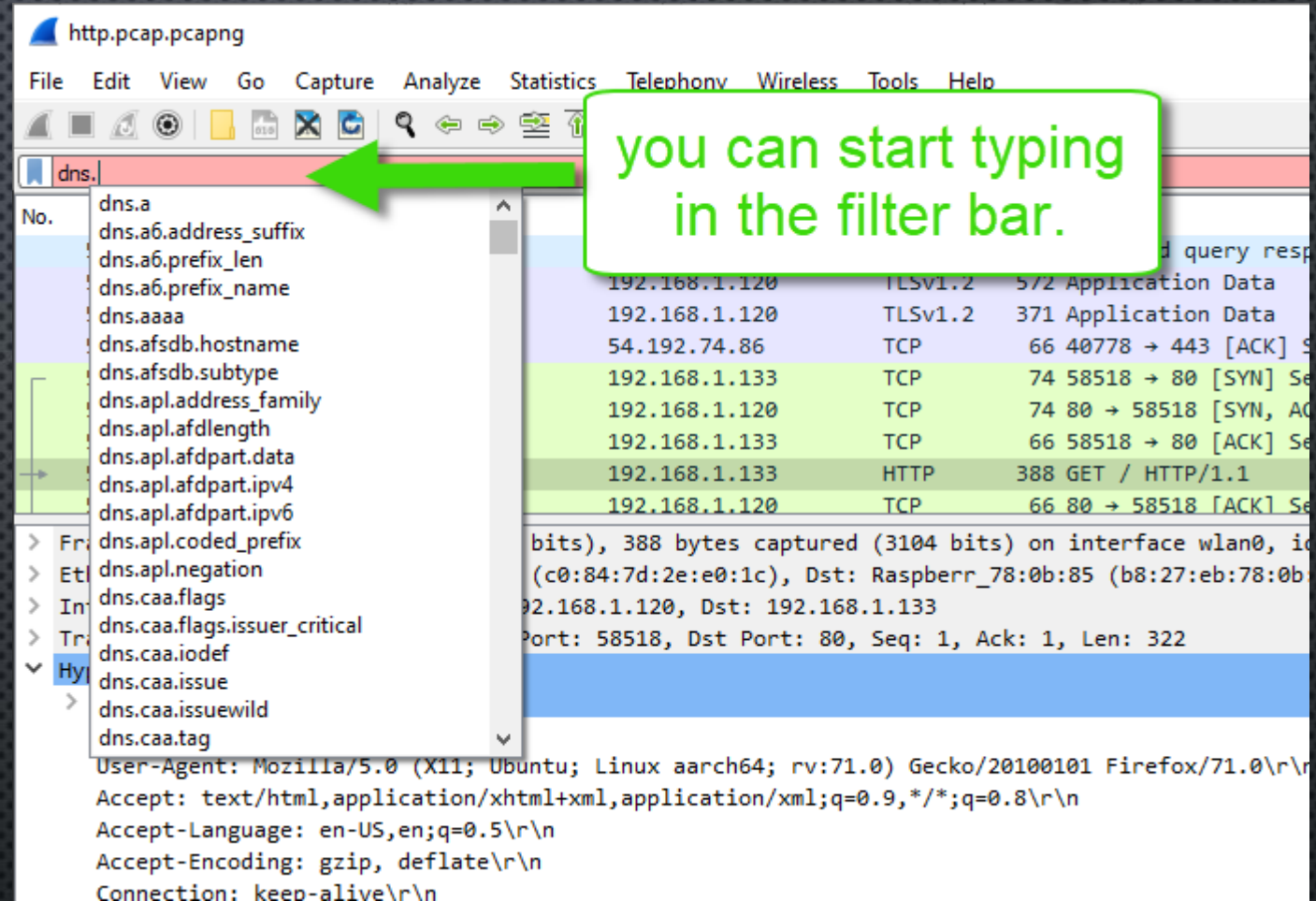
ways to display the stream

Search

Find Next

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

DISPLAY FILTERS



The screenshot shows the Wireshark network protocol analyzer interface. The title bar indicates the file is 'http.pcap.pcapng'. The menu bar includes File, Edit, View, Go, Capture, Analyze, Statistics, Telephony, Wireless, Tools, and Help. The toolbar contains various icons for file operations, capture, and analysis. The 'Filter' bar at the top shows the current display filter is 'dns.'. A green arrow points to this bar with a text box that says 'you can start typing in the filter bar.' Below the filter bar, a list of filters is displayed, including 'dns.a', 'dns.a6.address_suffix', 'dns.a6.prefix_len', 'dns.a6.prefix_name', 'dns.aaaa', 'dns.afsdb.hostname', 'dns.afsdb.subtype', 'dns.apl.address_family', 'dns.apl.afdlength', 'dns.apl.afdpart.data', 'dns.apl.afdpart.ipv4', 'dns.apl.afdpart.ipv6', 'dns.apl.coded_prefix', 'dns.apl.negation', 'dns.caa.flags', 'dns.caa.flags.issuer_critical', 'dns.caa.iodef', 'dns.caa.issue', 'dns.caa.issuewild', and 'dns.caa.tag'. The main packet list shows several packets, with the selected packet being an HTTP GET request from 192.168.1.133 to 192.168.1.120 on port 80. The packet details pane shows the structure of the HTTP request, including the User-Agent, Accept, Accept-Language, Accept-Encoding, and Connection headers.

http.pcap.pcapng

File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help

Filter: dns.

you can start typing in the filter bar.

No. dns.a
dns.a6.address_suffix
dns.a6.prefix_len
dns.a6.prefix_name
dns.aaaa
dns.afsdb.hostname
dns.afsdb.subtype
dns.apl.address_family
dns.apl.afdlength
dns.apl.afdpart.data
dns.apl.afdpart.ipv4
dns.apl.afdpart.ipv6
dns.apl.coded_prefix
dns.apl.negation
dns.caa.flags
dns.caa.flags.issuer_critical
dns.caa.iodef
dns.caa.issue
dns.caa.issuewild
dns.caa.tag

192.168.1.120 TLSv1.2 572 Application Data
192.168.1.120 TLSv1.2 371 Application Data
54.192.74.86 TCP 66 40778 → 443 [ACK] S
192.168.1.133 TCP 74 58518 → 80 [SYN] Se
192.168.1.120 TCP 74 80 → 58518 [SYN, AC
192.168.1.133 TCP 66 58518 → 80 [ACK] Se
192.168.1.133 HTTP 388 GET / HTTP/1.1
192.168.1.120 TCP 66 80 → 58518 [ACK] Se

bits), 388 bytes captured (3104 bits) on interface wlan0, id
(c0:84:7d:2e:e0:1c), Dst: Raspberr_78:0b:85 (b8:27:eb:78:0b
92.168.1.120, Dst: 192.168.1.133
Port: 58518, Dst Port: 80, Seq: 1, Ack: 1, Len: 322

User-Agent: Mozilla/5.0 (X11; Ubuntu; Linux aarch64; rv:71.0) Gecko/20100101 Firefox/71.0\r\n\r\nAccept: text/html,application/xhtml+xml,application/xml;q=0.9,*/*;q=0.8\r\n\r\nAccept-Language: en-US,en;q=0.5\r\n\r\nAccept-Encoding: gzip, deflate\r\n\r\nConnection: keep-alive\r\n\r\n

DISPLAY FILTERS

The screenshot shows the Wireshark network protocol analyzer interface. The top menu bar includes File, Edit, View, Go, Capture, Analyze, Statistics, Telephony, Wireless, Tools, and Help. The toolbar contains icons for various functions. The main display area is divided into three panes: the packet list, the packet details, and the packet bytes.

Packet List Pane: Displays a list of captured packets. The selected packet is 5752, a DNS Standard query response for tracking-protection.cdn.mozilla.net. The list includes columns for No., Time, Source, Destination, Protocol, Length, and Info.

Packet Details Pane: Shows the hierarchical structure of the selected packet. It includes sections for DNS Standard query response, tracking-protection.cdn.mozilla.net: type CNAME, class IN, cname d1zkz3k4cclnv6.cloudfront.net, and d1zkz3k4cclnv6.cloudfront.net: type A, class IN, addr 54.192.74.36. The selected packet is 5752, a DNS Standard query response for tracking-protection.cdn.mozilla.net.

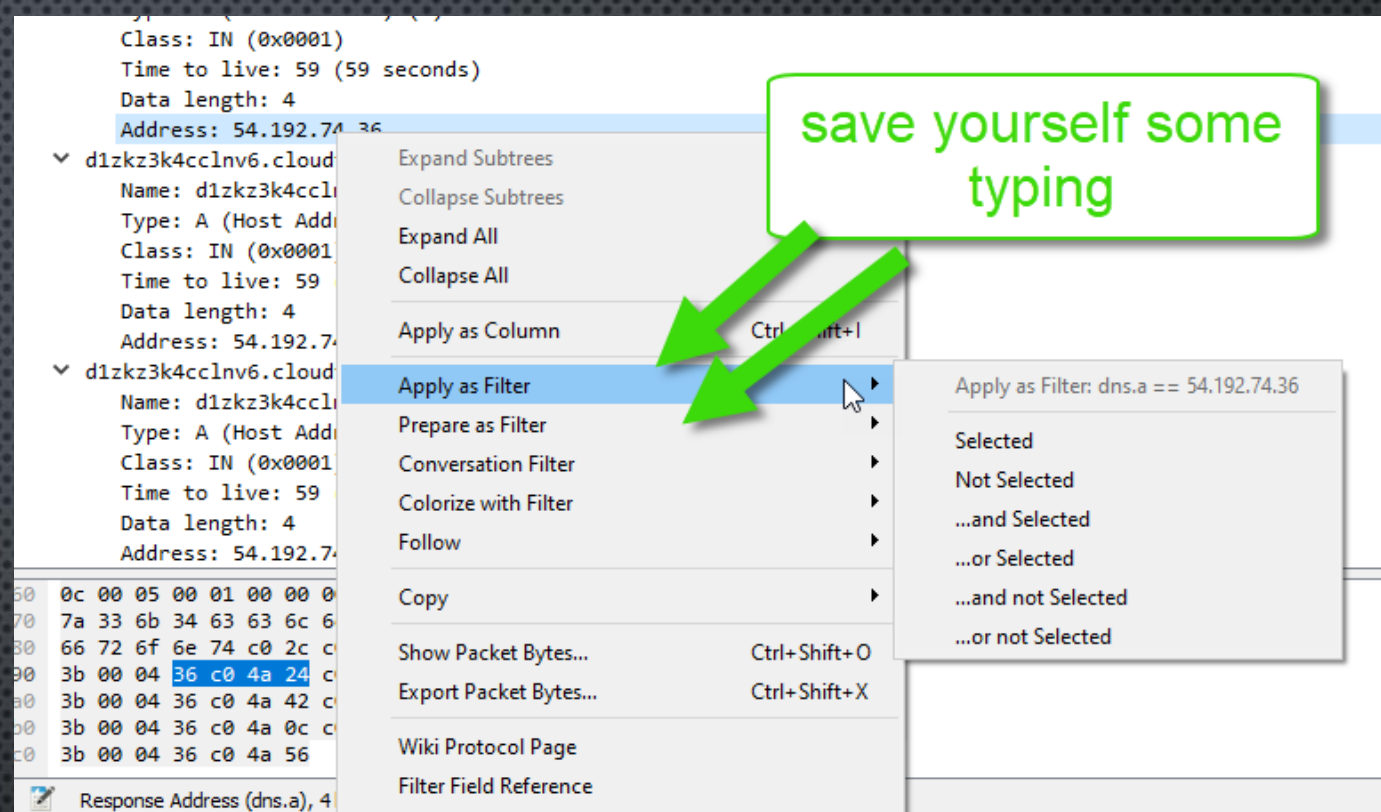
Packet Bytes Pane: Displays the raw bytes of the selected packet in hexadecimal and ASCII. The selected packet is 5752, a DNS Standard query response for tracking-protection.cdn.mozilla.net.

Annotations:

- A green box at the top right says "Unsure about what to search for? Find an interesting packet..." with a green arrow pointing to the packet list.
- A green box in the middle right says "Look for the interesting part of the packet." with a green arrow pointing to the packet details pane.
- A green box at the bottom right says "The status bar tells you what you're looking at." with a green arrow pointing to the status bar.

Status Bar: Located at the bottom of the interface, it displays "Response Address (dns.a), 4 bytes" and "Packets: 39342 · Displayed: 594 (1.5%)".

DISPLAY FILTERS

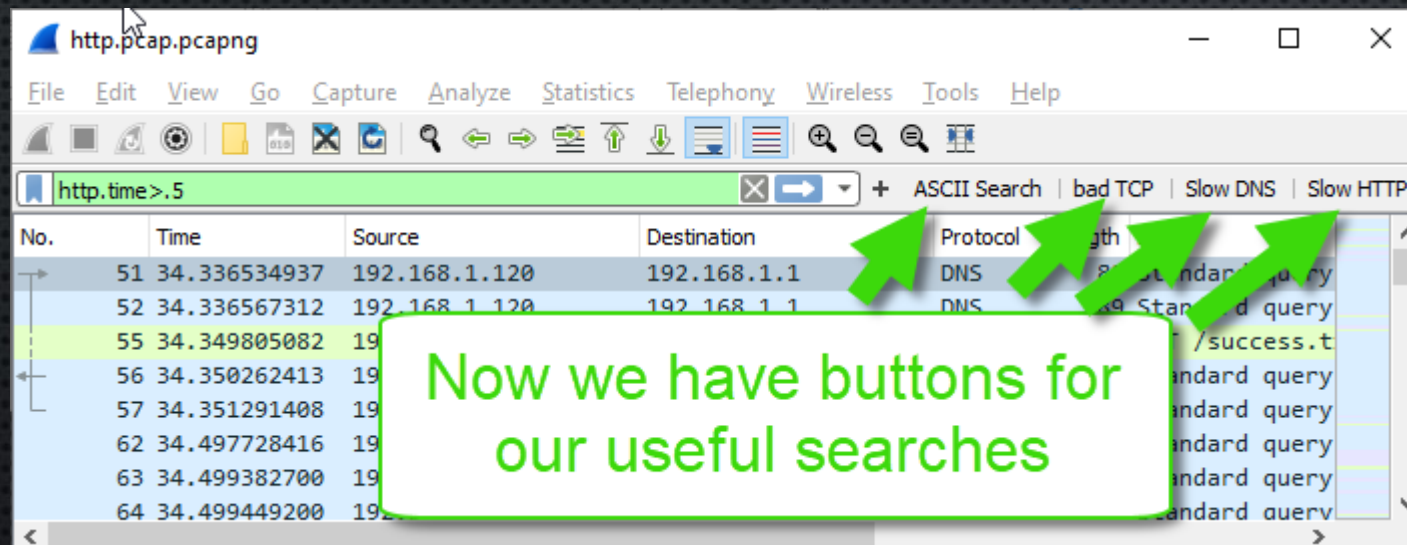
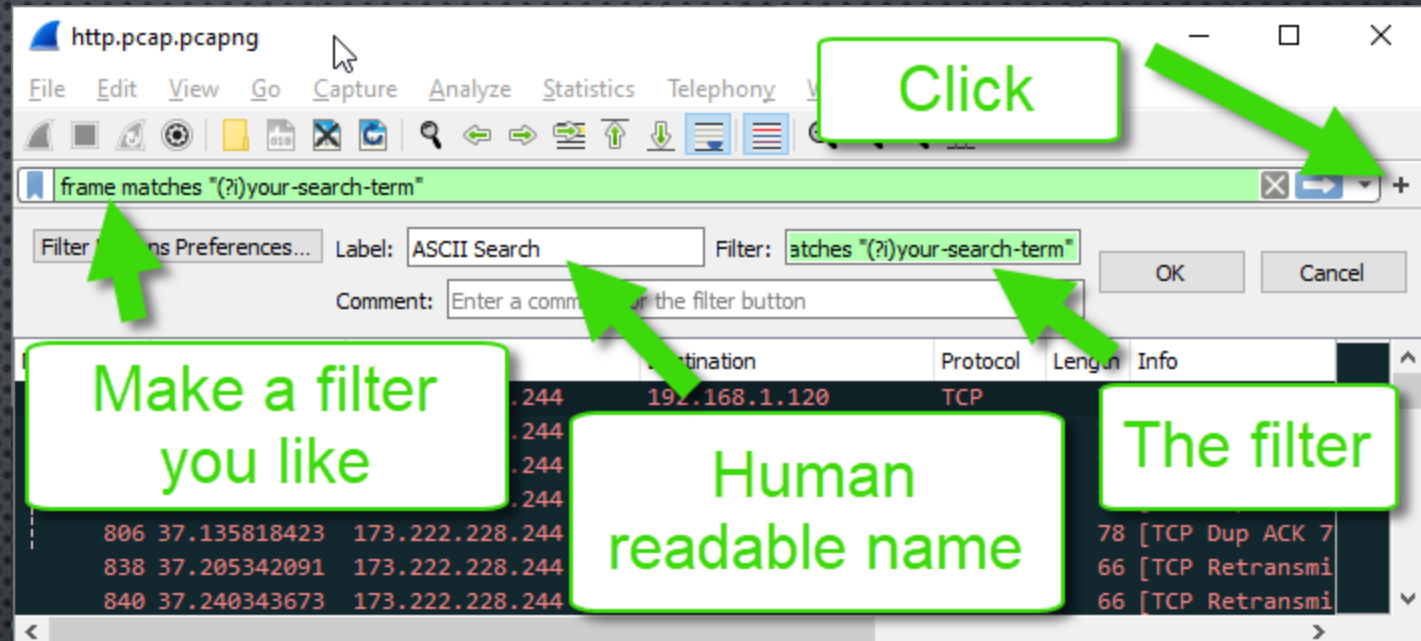


- MY FAVORITE COMPARISON OPERATORS: ==, <, >, CONTAINS
- LOGICAL OPERATORS: &&, ||, !, ^^ (THAT'S XOR)
- USE () TO GROUP THINGS
- YOU CAN FILTER FOR EXISTENCE OR A VALUE

DISPLAY FILTERS

- SOME FILTERS I LIKE (ALL LOWERCASE):
 - IP.ADDR==192.168.1.100
 - TCP.PORT==80
 - UDP.PORT==53
 - DNS, HTTP, FTP, NTP (THAT KIND OF THING)
 - HTTP.RESPONSE.CODE>399 (BROKEN HTTP)
 - TCP.TIME_DELTA>.5 (SLOW TCP)
 - HTTP.TIME>.5 (SLOW HTTP)
 - DNS.TIME>.5 (SLOW DNS)
 - FRAME MATCHES "(?i)MOZILLA" (FINDS FRAMES WITH CASE INSENSITIVE ASCII "MOZILLA" IN THERE)
 - TCP.ANALYSIS.FLAGS && !(TCP.ANALYSIS.KEEP_ALIVE | | TCP.ANALYSIS.KEEP_ALIVE_ACK) && !(TCP.ANALYSIS.WINDOW_UPDATE) (TCP PROBLEMS)

BUTTONS



COLUMNS

Apply something interesting as a column

The screenshot shows the Wireshark network protocol analyzer interface. The top menu bar includes File, Edit, View, Go, Capture, Analyze, Statistics, Telephony, Wireless, Tools, and Help. Below the menu is a toolbar with various icons. The packet list pane at the top shows a list of captured packets. The packet details pane on the left shows the structure of the selected packet (HTTP/1.1 200 OK). The packet bytes pane on the right shows the raw data of the selected packet. A context menu is open over the selected packet, with the 'Apply as Column' option highlighted. A green box with the text 'Apply something interesting as a column' and two green arrows points to the 'Apply as Column' option and the packet details pane.

No.	Time	Source	Destination	Protocol	Length	Info
192.168.1.120				HTTP	332	HTTP/1.1 200 OK (application/javascript)
192.168.1.120				HTTP	452	HTTP/1.1 200 OK (application/javascript)
192.168.1.120				HTTP	880	HTTP/1.1 200 OK (application/json)
192.168.1.120				HTTP	880	HTTP/1.1 200 OK (application/json)
192.168.1.120				HTTP	880	HTTP/1.1 200 OK (application/json)
192.168.1.120				HTTP	880	HTTP/1.1 200 OK (application/json)
192.168.1.120				HTTP	880	HTTP/1.1 200 OK (application/json)
192.168.1.120				HTTP	880	HTTP/1.1 200 OK (application/ison)

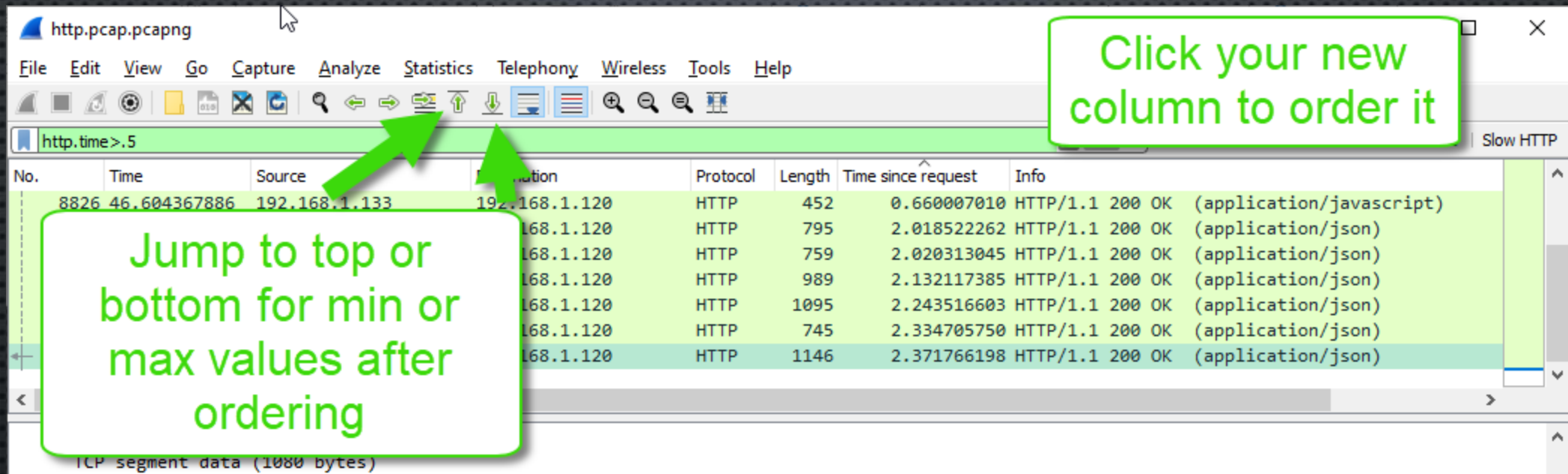
Context Menu Options:

- Expand Subtrees
- Collapse Subtrees
- Expand All
- Collapse All
- Apply as Column (Ctrl+Shift+I)
- Apply as Filter
- Prepare as Filter
- Conversation Filter
- Colorize with Filter
- Follow
- Copy
- Show Packet Bytes... (Ctrl+Shift+O)
- Export Packet Bytes... (Ctrl+Shift+X)
- Wiki Protocol Page
- Filter Field Reference
- Protocol Preferences
- Decode As...
- Go to Linked Packet
- Show Linked Packet in New Window

Packet Details:

- TCP payload (266 bytes)
- TCP segment data (266 bytes)
- [500 Reassembled TCP Segments (7228 bytes)]
- Hypertext Transfer Protocol
 - HTTP/1.1 200 OK\r\n
 - [Expanded Info (Chat/Sequence):]
 - Response Version: HTTP/1.1
 - Status code: 200
 - [Status code Description: OK]
 - Response phrase: OK
 - Content-Length: 722505\r\n
 - X-Robots-Tag: noindex, nofollow,
 - X-Content-Type-Options: nosniff\r\n
 - Accept-Ranges: bytes\r\n
 - Last-Modified: Thu, 16 Apr 2020
 - Etag: 1587066796\r\n
 - Date: Sat, 18 Apr 2020 00:13:20
 - X-Frame-Options: sameorigin\r\n
 - Content-Type: application/javascript\r\n
 - [HTTP response 1/10]
 - [Time since request: 0.502066766 seconds]

COLUMNS



The image shows the Wireshark network protocol analyzer interface. The title bar indicates the file is 'http.pcap.pcapng'. The menu bar includes File, Edit, View, Go, Capture, Analyze, Statistics, Telephony, Wireless, Tools, and Help. The toolbar contains various icons for file operations, capture, analysis, and display. The packet list pane shows a filter 'http.time>.5' and a list of 8 packets. The first packet is selected. Two green callout boxes provide instructions: one points to the 'Sort Ascending' icon in the toolbar with the text 'Click your new column to order it', and the other points to the vertical scrollbar with the text 'Jump to top or bottom for min or max values after ordering'.

http.pcap.pcapng

File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help

http.time>.5

Slow HTTP

No.	Time	Source	Destination	Protocol	Length	Time since request	Info
8826	46.604367886	192.168.1.133	192.168.1.120	HTTP	452	0.660007010	HTTP/1.1 200 OK (application/javascript)
			192.168.1.120	HTTP	795	2.018522262	HTTP/1.1 200 OK (application/json)
			192.168.1.120	HTTP	759	2.020313045	HTTP/1.1 200 OK (application/json)
			192.168.1.120	HTTP	989	2.132117385	HTTP/1.1 200 OK (application/json)
			192.168.1.120	HTTP	1095	2.243516603	HTTP/1.1 200 OK (application/json)
			192.168.1.120	HTTP	745	2.334705750	HTTP/1.1 200 OK (application/json)
			192.168.1.120	HTTP	1146	2.371766198	HTTP/1.1 200 OK (application/json)

Jump to top or bottom for min or max values after ordering

Click your new column to order it

TCP segment data (1080 bytes)

EXPERT INFOS

Click the dot in the corner

Warnings and errors are worth looking into.

Severity Summary Group Protocol Count

> Warning	This frame is a (suspected) out-of-order segment	Sequence	TCP	
> Warning	Previous segment(s) not captured (common at capture sta...	Sequence	TCP	
> Warning	Connection reset (RST)	Sequence	TCP	
> Note	ACK to a TCP keep-alive segment	Sequence	TCP	
> Note	TCP keep-alive segment	Sequence	TCP	
> Note	This frame is a (suspected) retransmission	Sequence	TCP	
> Note	Duplicate ACK (#1)	Sequence	TCP	
> Note	This session reuses previously negotiated keys (Session res...	Sequence	TLS	
> Note	"Time To Live" != 255 for a packet sent to the Local Networ...	Sequence	IPv4	
> Chat	TCP window update	Sequence	TCP	
> Chat	Connection finish (FIN)	Sequence	TCP	
> Chat	GET /success.txt HTTP/1.1\r\n	Sequence	HTTP	
> Chat	Connection establish acknowledge (SYN+ACK): server por...	Sequence	TCP	
> Chat	Connection establish request (SYN): server port 80	Sequence	TCP	

Display filter: "http.time>.5"

☐ Limit to Display Filter ☒ Group by summary Search:

Frame (332 bytes) Reassembled TCP (7260 to bytes)

http.pcap.pcapng Packets: 39342 · Displayed: 1

This is relative to the current display filter

NEXT STEPS

- THIS WAS JUST AN INTRO TO AN OVERVIEW OF A SUMMARY OF THE TIP OF THE ICEBERG
- I HOPE THIS HELPS SPEED YOUR PACKET ANALYSIS JOBS ALONG
- QUESTIONS, COMMENTS, HATEMAIL: KEVAN@BSDDRAKE.COM
- THIS PRESENTATION AND PCAP CAN BE FOUND AT: [HTTP://SMASHBADGER.COM/HTTP.ZIP](http://SMASHBADGER.COM/HTTP.ZIP)