Wireshark 101®

Essential Skills for Network Analysis

Course Contents

- [Enter the topics you wish to cover.]

WARNING

Before you capture your first packet, **ensure you have permission to listen to the network traffic**. If you are an IT staff member, obtain written permission to listen in to network traffic for troubleshooting, optimization, security, and application analysis.

Consult a legal specialist to understand your local and national laws regarding packet capture on wired or wireless networks.

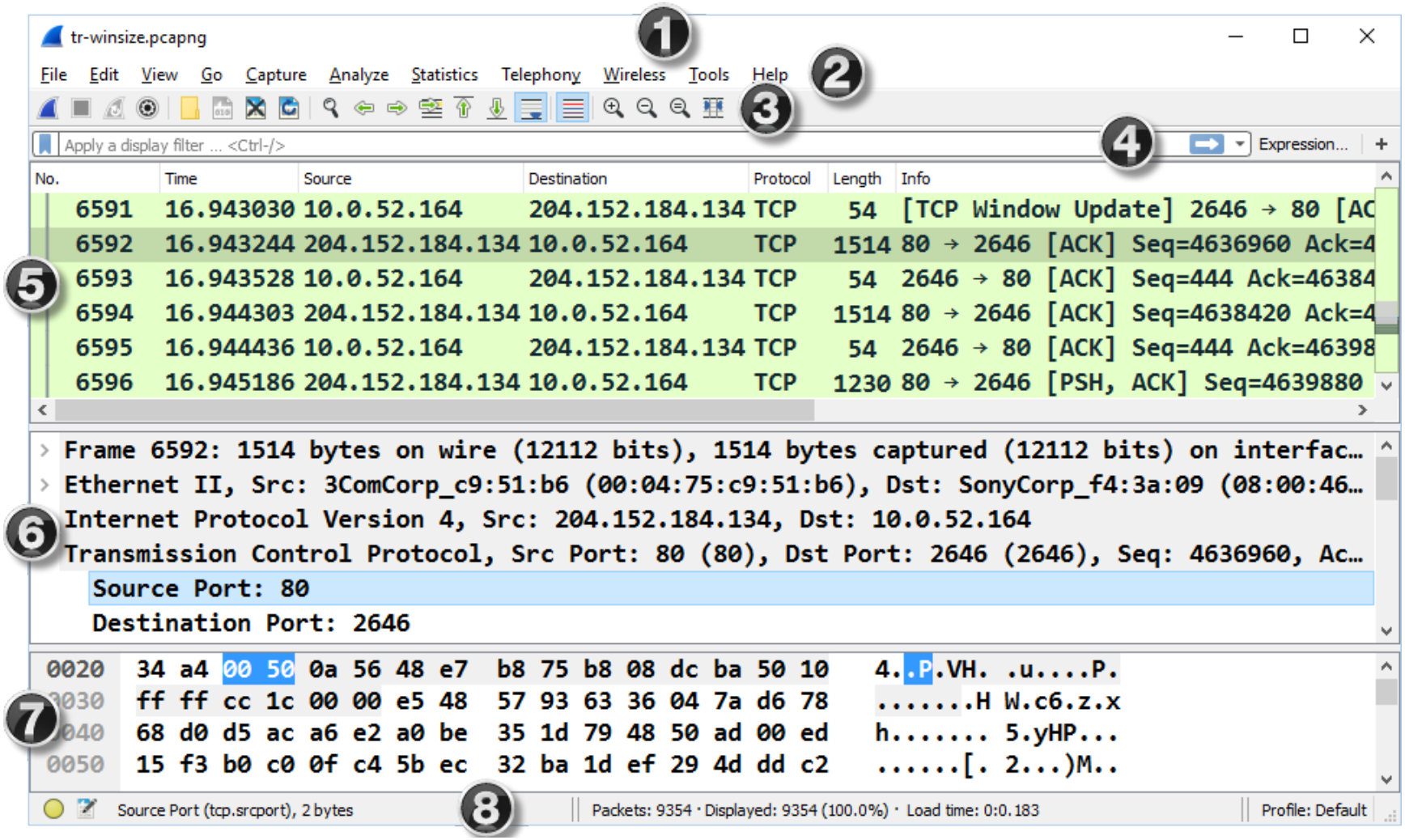
Fundamentals – Why Wireshark?

- **Wireshark Capabilities**
  - General traffic analysis
  - Troubleshooting
  - Security
  - Application analysis
- **Supported OSes**
  - Windows
  - *NIX
  - MAC

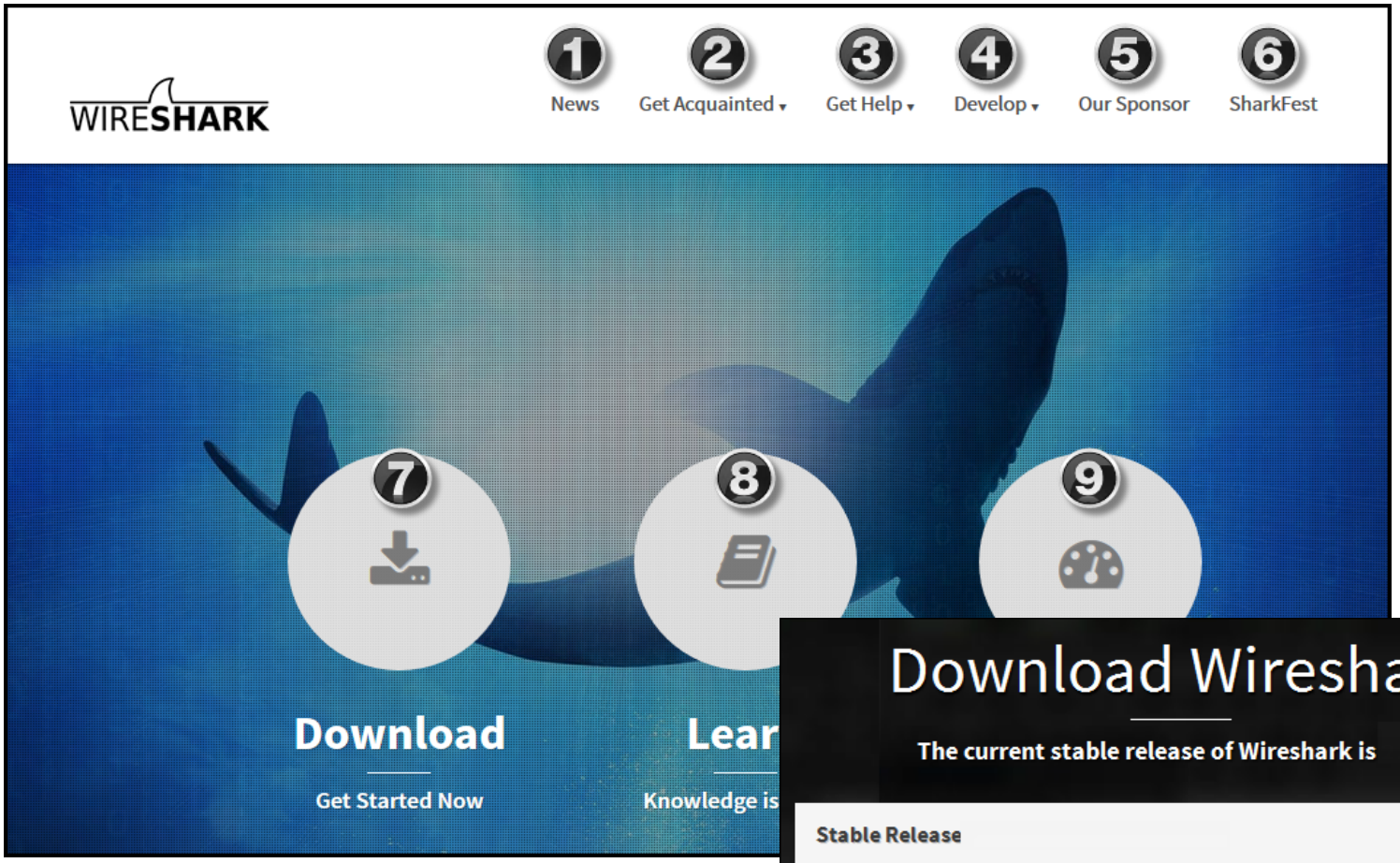
- Determine **who is talking** in the trace file
- Determine **which applications** are in use
- Filter on the **conversation** of interest
- Graph the **IO rate** to look for drops in throughput
- Open the **Expert** to look for problems
- Determine the **round trip time** to identify path latency

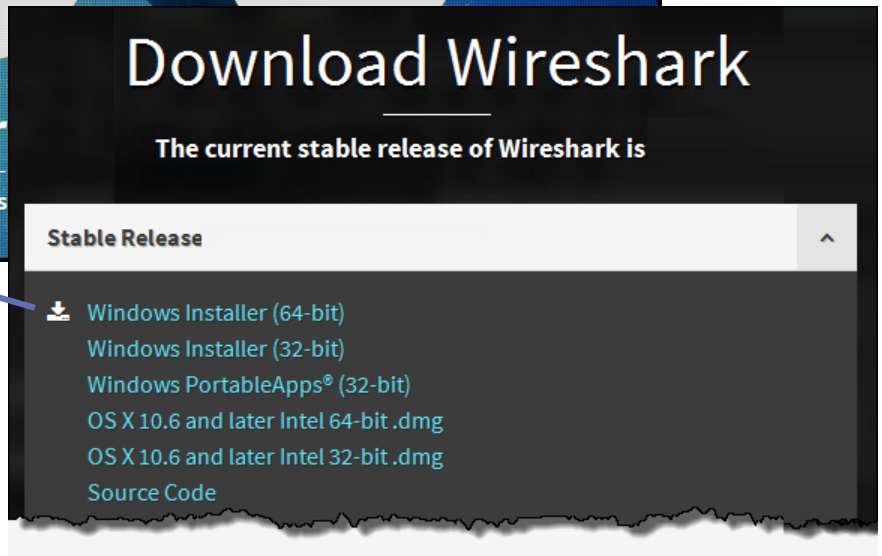
Quick Reference

Key Graphical Interface Elements



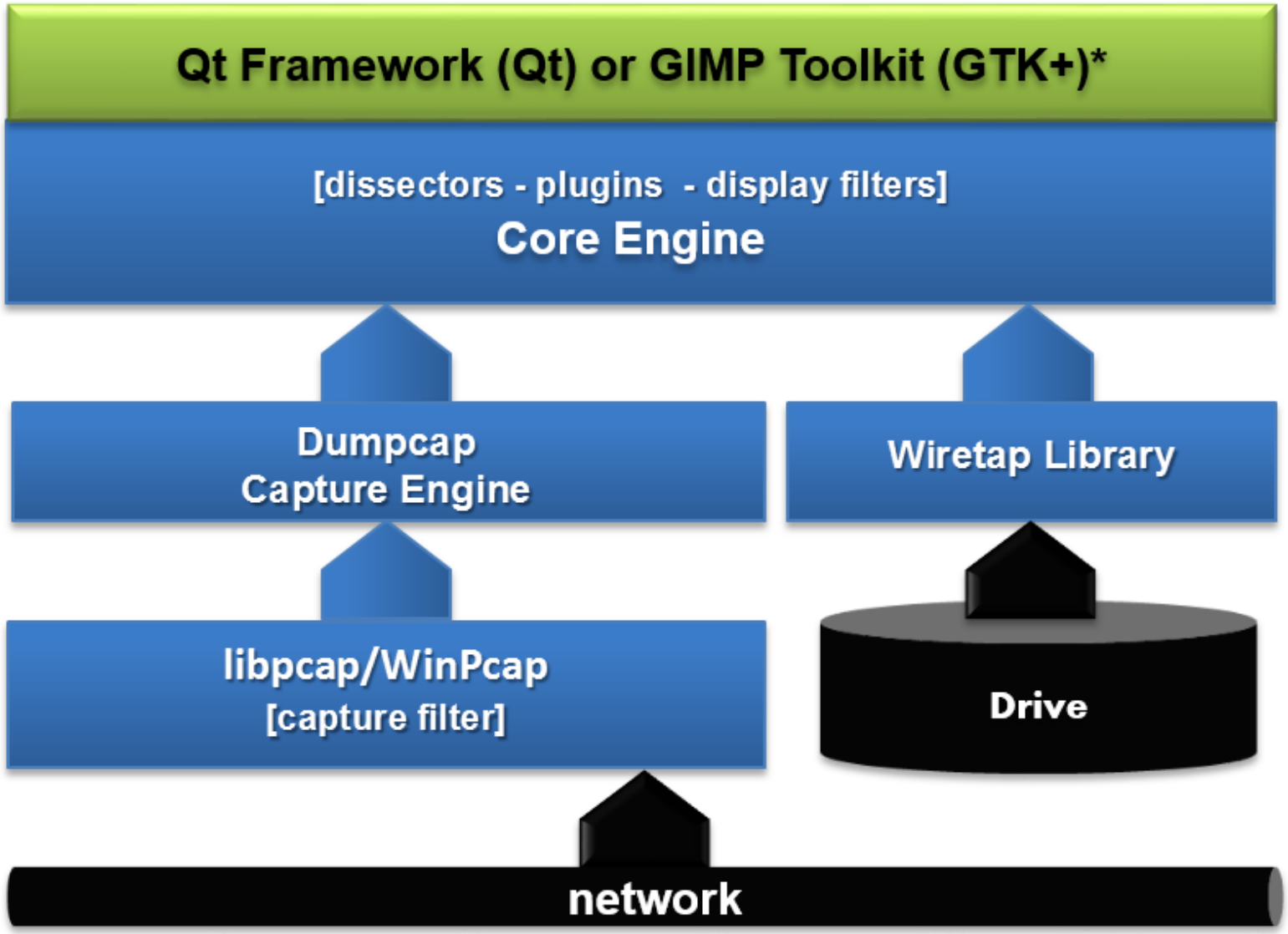
wireshark.org/download.html





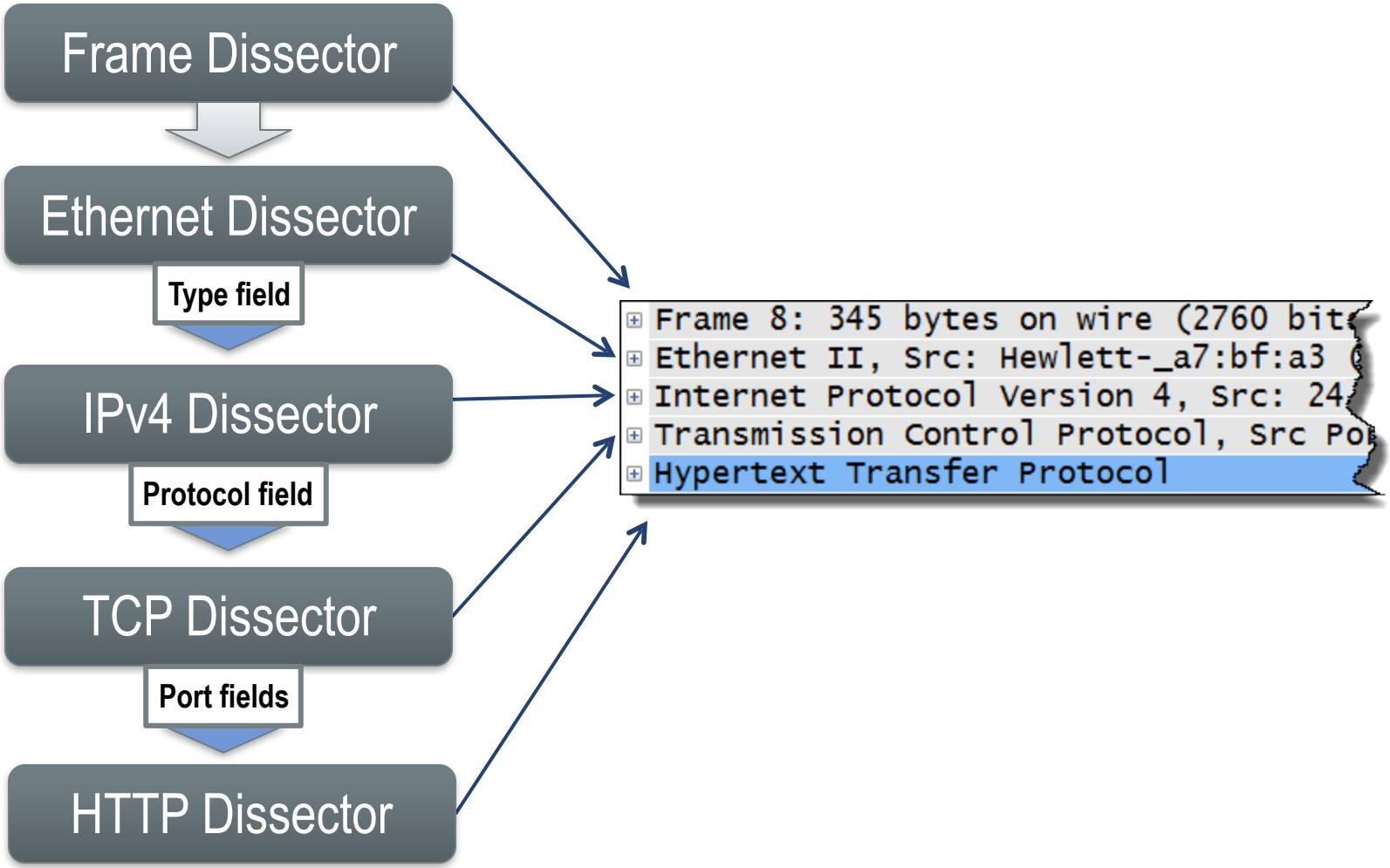
NOTE
The download.html page suggests the version that matches your incoming HTTP GET request

Wireshark Capture Elements

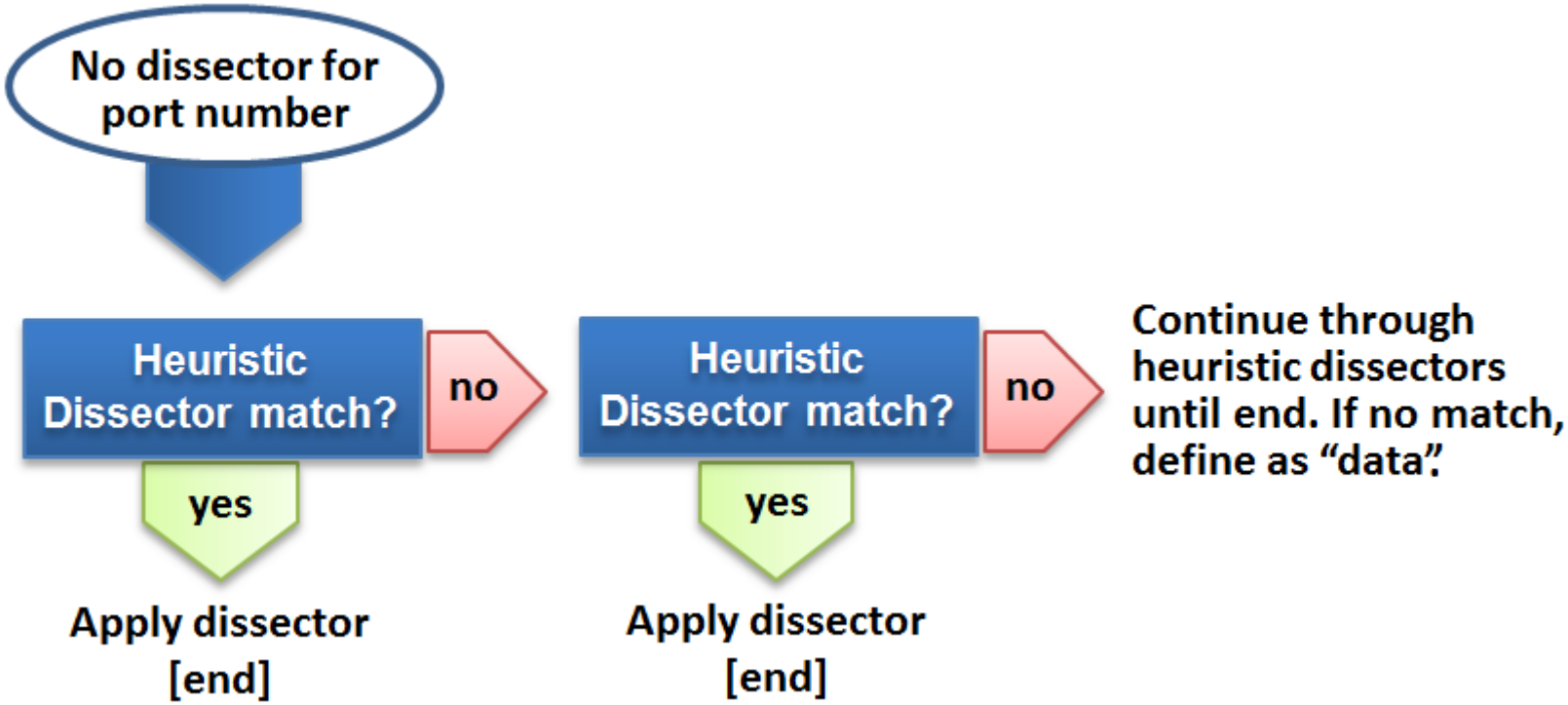


* GTK support will eventually be discontinued in Wireshark v2.

Dissect the Wireshark Dissectors



How Heuristic Dissectors Work



Frames vs. Packets vs. Segments

The *Frame* section contains metadata displayed by Wireshark

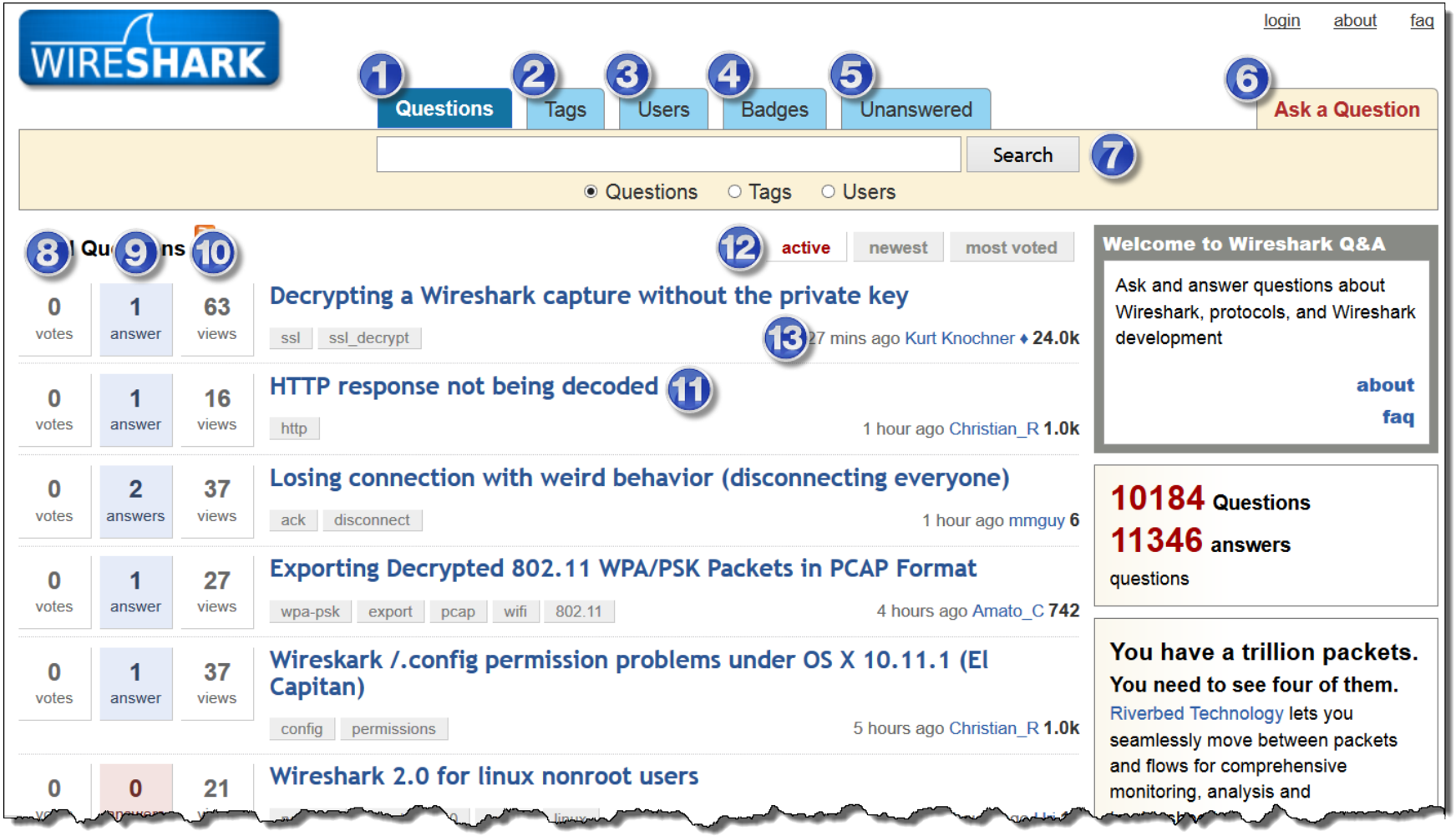
Frame

Packet

Segment

```
Frame 2284: 345 bytes on wire (2760 bits), 345 bytes captured (2760 bits) on
    Interface id: 0 (\Device\NPF_{98657C67-2DE2-4C46-B5FE-5101D6F0227D})
    Encapsulation type: Ethernet (1)
    Arrival Time: Dec  2, 2015 19:14:36.182840000 Pacific Standard Time
    [Time shift for this packet: 0.000000000 seconds]
    Epoch Time: 1449112476.182840000 seconds
    [Time delta from previous captured frame: 0.000139000 seconds]
    [Time delta from previous displayed frame: 2.561500000 seconds]
    [Time since reference or first frame: 10.111596000 seconds]
    Frame Number: 2284
    Frame Length: 345 bytes (2760 bits)
    Capture Length: 345 bytes (2760 bits)
    [Frame is marked: False]
    [Frame is ignored: False]
    [Protocols in frame: eth:ethertype:ip:tcp:http]
    [Coloring Rule Name: HTTP]
    [Coloring Rule String: http || tcp.port == 80 || http2]
Ethernet II, Src: GemtekTe_cc:7d:da (20:10:7a:cc:7d:da), Dst: HonHaiPr_fa:0e
Internet Protocol Version 4, Src: 192.168.44.7, Dst: 198.66.239.146
Transmission Control Protocol, Src Port: 26170 (26170), Dst Port: 80 (80), S
Hypertext Transfer Protocol
    GET / HTTP/1.1\r\n
    Host: www.chappellu.com\r\n
    User-Agent: Mozilla/5.0 (Windows NT 6.3; WOW64; rv:42.0) Gecko/20100101 F
    Accept: text/html,application/xhtml+xml,application/xml;q=0.9,*/*;q=0.8\r
    Accept-Language: en-US,en;q=0.5\r\n
    Accept-Encoding: gzip, deflate\r\n
    Connection: keep-alive\r\n
    \r\n
    [Full request URI: http://www.chappellu.com/]
```

Wireshark Resource: Q & A Forum



The Default Three-Pane View

http-google101.pcapng

File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help

Apply a display filter ... <Ctrl-/> Expression... +

No.	Time	Source	Destination	Protocol	Length	Info
1	0…	24.6.173.220	75.75.75.75	DNS	74	Standard query 0xae0b A www.google.…
2	0…	75.75.75.75	24.6.173.220	DNS	154	Standard query response 0xae0b A ww…
3	0…	24.6.173.220	75.75.75.75	DNS	74	Standard
4	0…	75.75.75.75	24.6.173.220	DNS	102	Standard
5	0…	24.6.173.220	74.125.224…	TCP	66	35145 → 80 [SYN] Seq=0 Win=8192 Len…
6	0…	74.125.224…	24.6.173.220	TCP	66	80 → 35145 [SYN, ACK] Seq=0 Ack=1 W…
7	0…	24.6.173.220	74.125.224…	TCP	54	35145 → 80 [ACK] Seq=1 Ack=1 Win=65…

Packet List Pane

```
▷ Frame 1: 74 bytes on wire (592 bits), 74 bytes captured (592 bits) on interface 0
▷ Ethernet II, Src: HewlettP_a7:bf:a3 (d4:85:64:a7:bf:a3), Dst: Cadant_31:bb:c1 (00…
▷ Internet Protocol Version 4, Src: 24.6.173.220, Dst: 75.75.75.75
▷ User Datagram Protocol, Src Port: 51724 (51724), Dst Port: 53 (53)
◢ Domain Name System (query)
    [Response In: 2]
    Transaction ID: 0xae0b
  ▷ Flags: 0x0100 Standard query
    Questions: 1
    Answer RRs: 0
    Authority RRs: 0
    Additional RRs: 0
```

Packet Details Pane

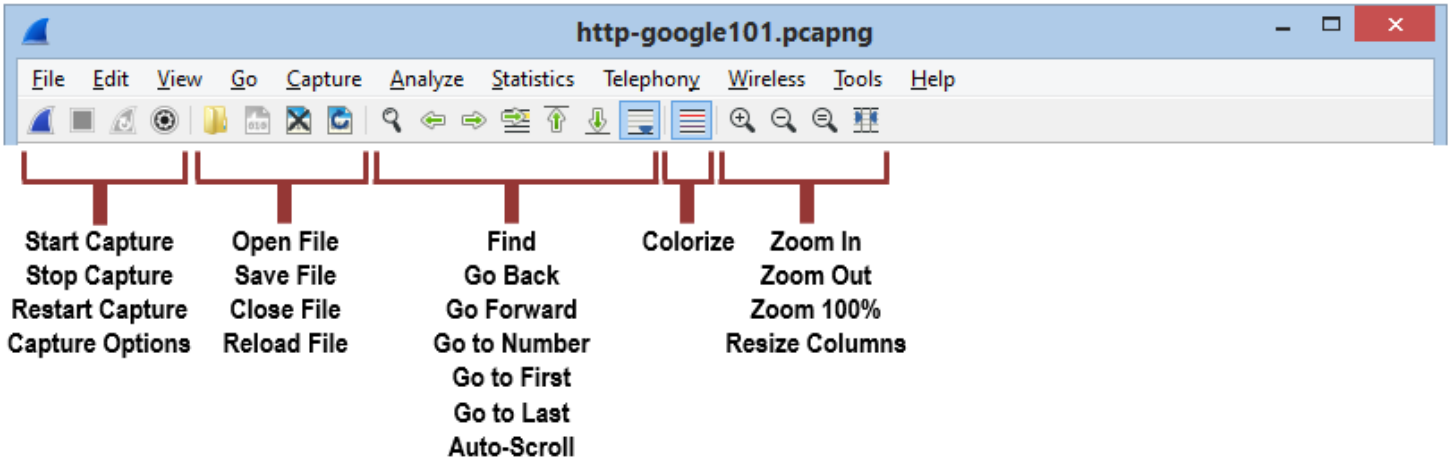
```
0010  00 3c 08 3d 00 00 80 11  00 00 18 06 ad dc 4b 4b   .<.=.... ......KK
0020  4b 4b ca 0c 00 35 00 28  5c b2 ae 0b 01 00 00 01   KK...5.( \.....
0030  00 00 00 00 00 00 03 77  77 77 06 67 6f 6f 67 6c
0040  65 03 63 6f 6d 00 00 01  00 01
```

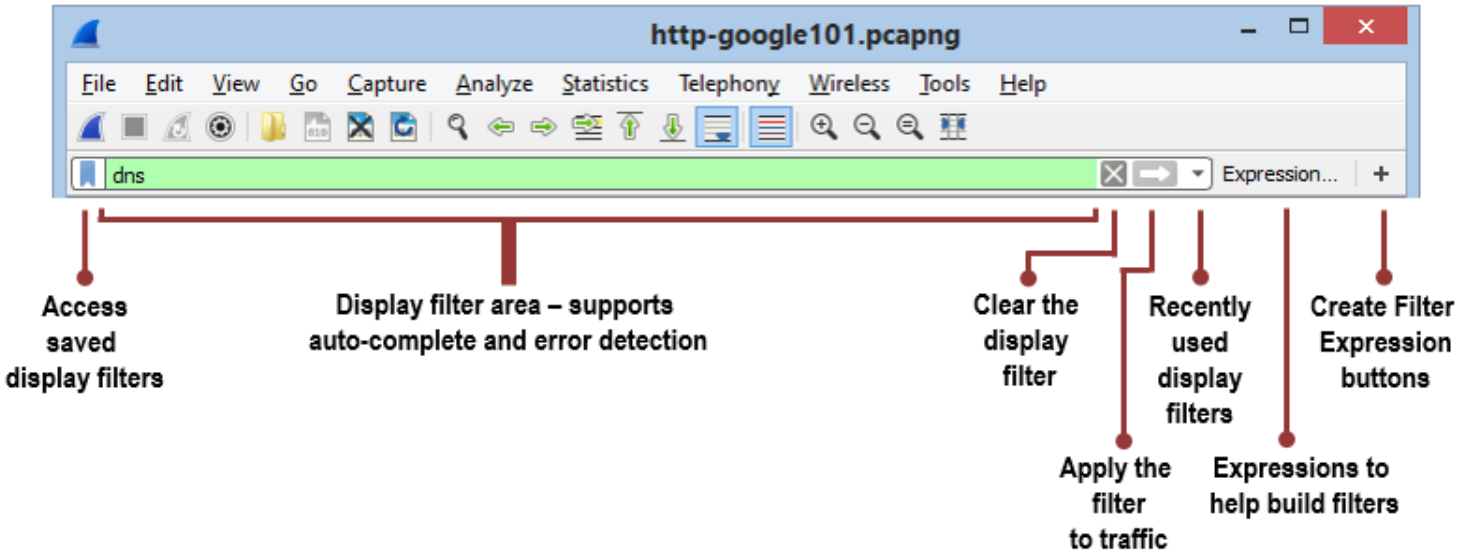
Packet Bytes Pane

Number of queries in packet (dns.count.queries), 2 bytes | Packets: 374 · Displayed: 374 (100.0%) · Load time: 0:0.9 | Profile: Default

Use the Main Wireshark View

Note: The Start page appears when no trace file is open. Become accustomed to using the menus and toolbars in Wireshark.





Wireshark Resource: Wiki Pages

http-google101.pcapng

File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help

Apply a display filter ... <Ctrl-/> Expression...

No.	Time	Source	Destination	Protocol	Length	Info
1	0.000000	24.6.173.220	75.75.75.75	DNS	74	Standard query 0xae0b …
2	0.013237	75.75.75.75	24.6.173.220	DNS	154	Standard query respons…
3	0.013971	24.6.173.220	75.75.75.75	DNS	74	Standard query 0x4553 …

Frame 1: 74 bytes on wire (592 bits), 74 bytes captured (592 bits) on interface 0
Ethernet II, Src: Hewlett… d4:85:64:a7:bf:a3), Dst: Cadant_31:bb:c1 (00:0…
Internet Protocol Version … 5.75
0100 .... = Version: 4
.... 0101 = Header Lengt…
Differentiated Services … CT)
Total Length: 60
Identification: 0x083d …
Flags: 0x00
Fragment offset: 0
Time to live: 128
Protocol: UDP (17)
Header checksum: 0x0000
Source: 24.6.173.220
Destination: 75.75.75.7…
[Source GeoIP: United St… cations, Inc., Milpitas…
[Destination GeoIP: Unit… mmunications, Inc., Ind…
User Datagram Protocol, Sr… 3 (53)
Domain Name System (query)

right-click

- Expand Subtrees — Shift+Right
- Expand All — Ctrl+Right
- Collapse All — Ctrl+Left
- Apply as Column
- Apply as Filter
- Prepare a Filter
- Conversation Filter
- Colorize with Filter
- Follow
- Copy
- Export Packet Bytes… — Ctrl+H
- Wiki Protocol Page
- Filter Field Reference
- Protocol Preferences
- Decode As…
- Go to Linked Packet
- Show Linked Packet in New Window

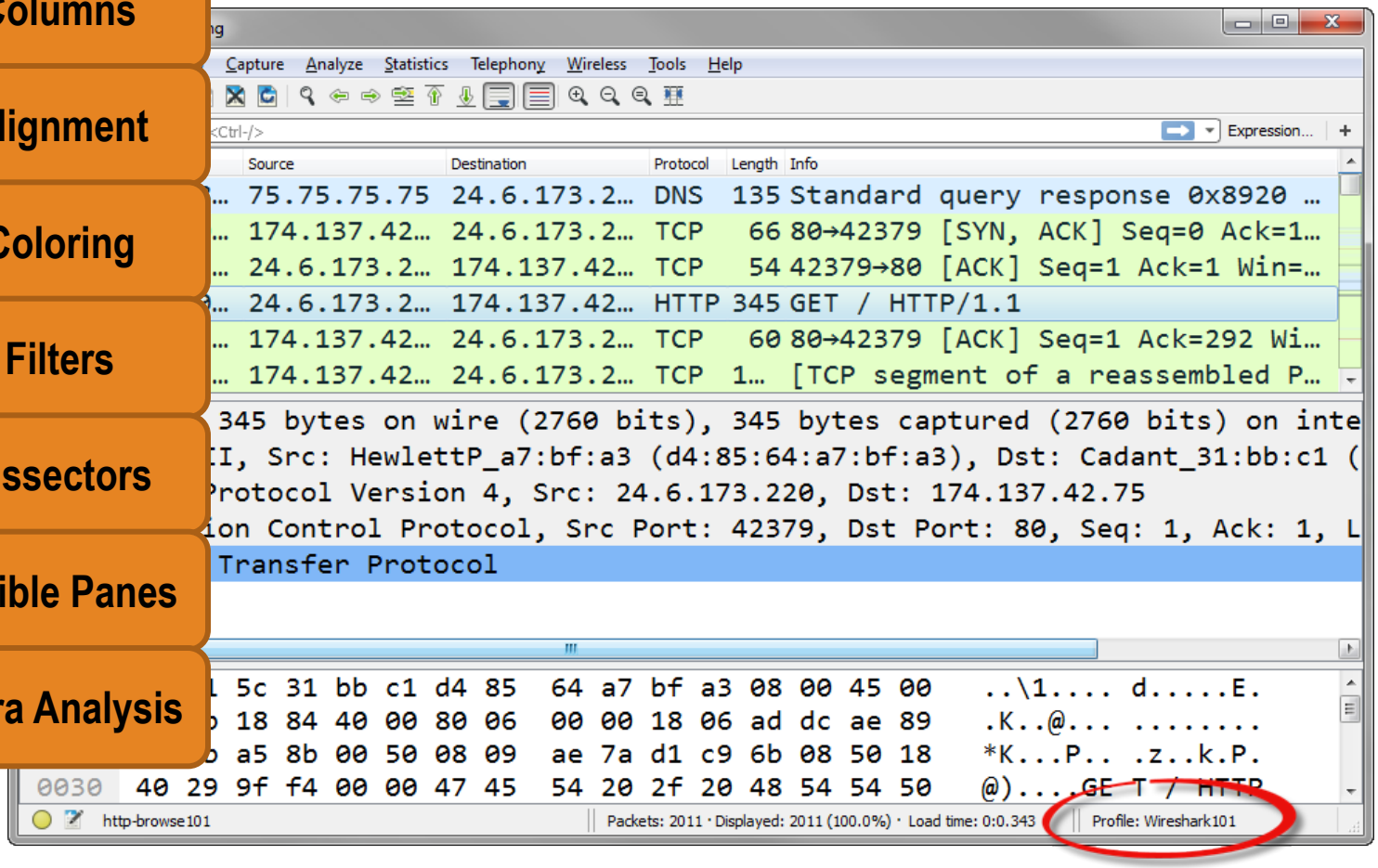
Internet Protocol Version 4 (ip), 20 bytes … 0.27 Profile: Default

PROFILES

p-browse101.pcapng

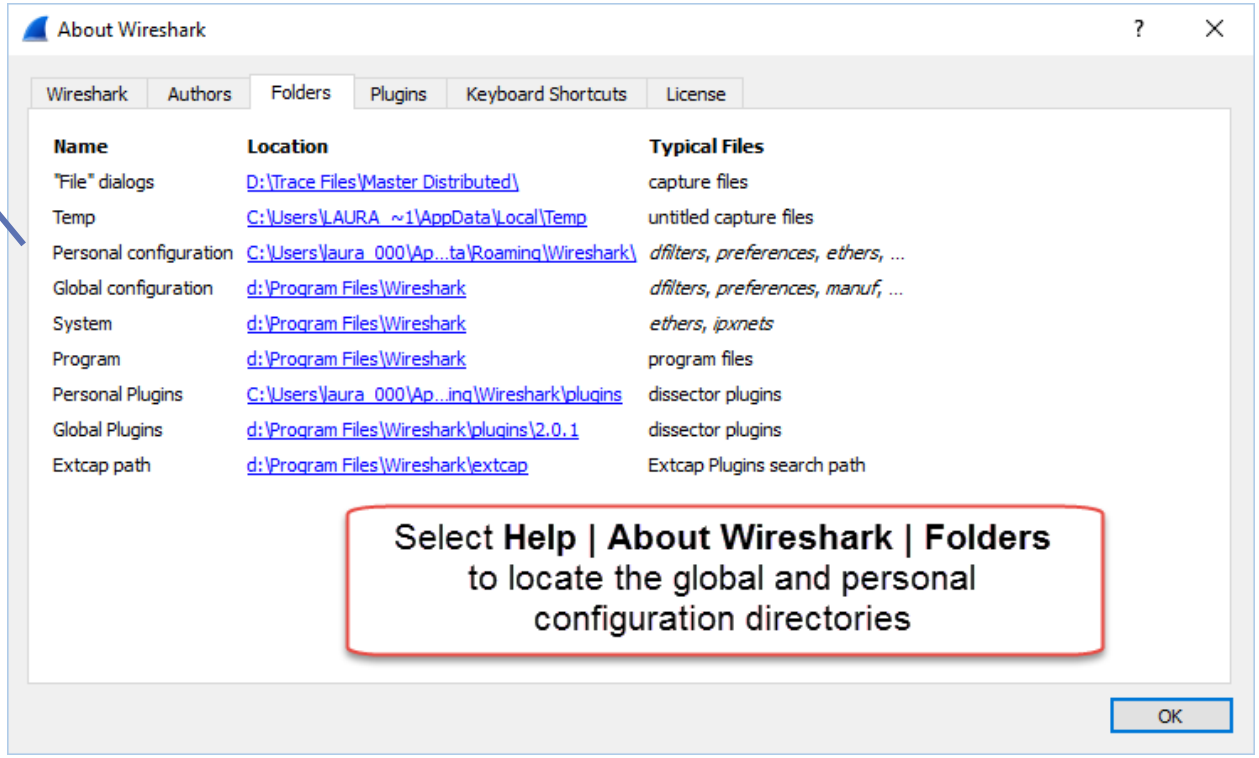
Customize Wireshark for Different Tasks

- Columns
- Alignment
- Coloring
- Filters
- Dissectors
- Visible Panes
- Extra Analysis

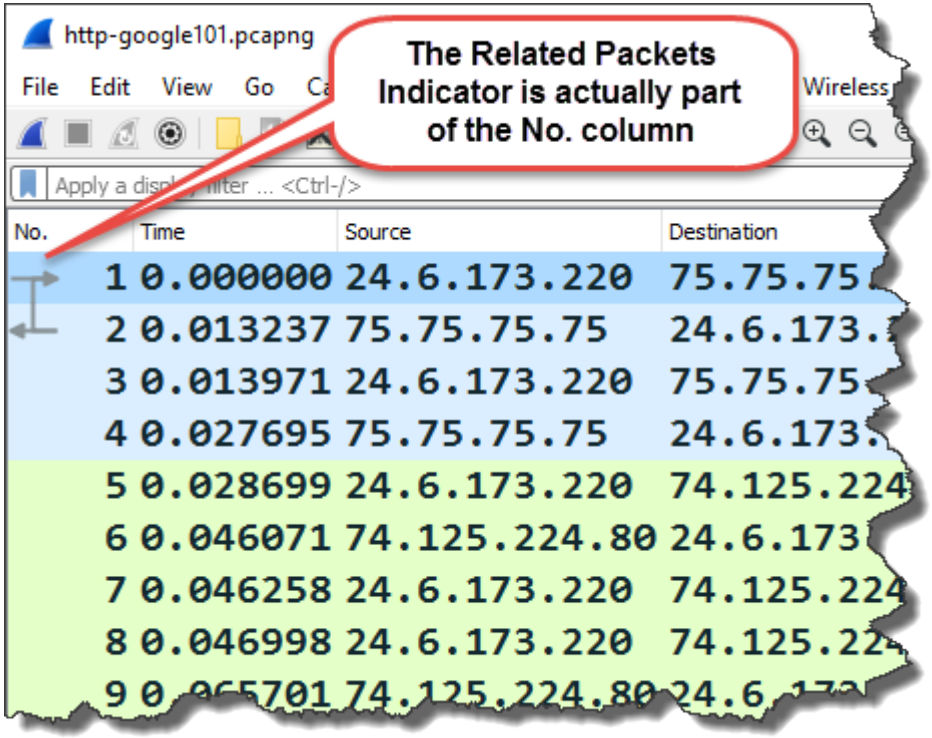


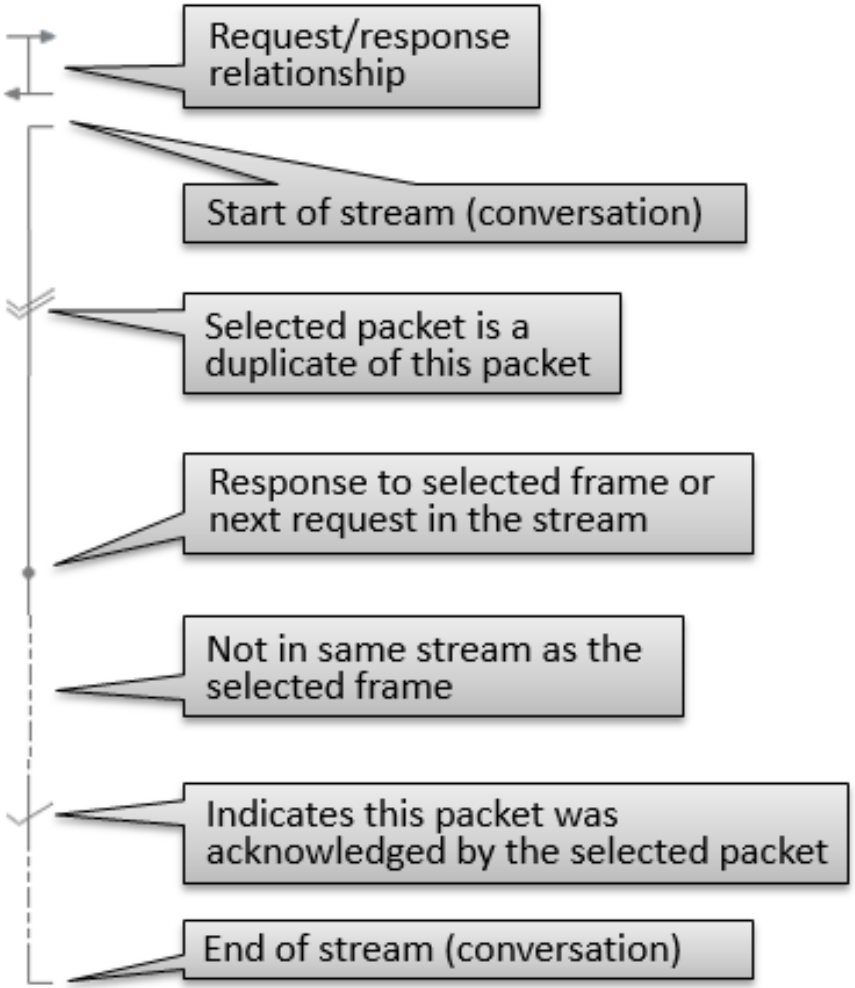
Locate Key Wireshark Configuration Files

Your custom profiles are located in a profiles directory under the Personal configuration folder



Related Packets Indicator





Work with Columns in the Packet List Pane

tp-espn101.pcapng

http-espn101.pcapng

File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help

Apply a display filter ... <Ctrl-/> Expression...

No.	Time	Source	Destination	Protocol	Length	Time to live	Info
1	0.000000	24.6.173.220	75.75.75.75	DNS	72	128	Standard quer…
2	0.014749	75.75		DNS	88	59	Standard quer…
3	0.015870	24.6.1		DNS	72	128	Standard quer…
4	0.029205	75.75		DNS	122	59	Standard quer…

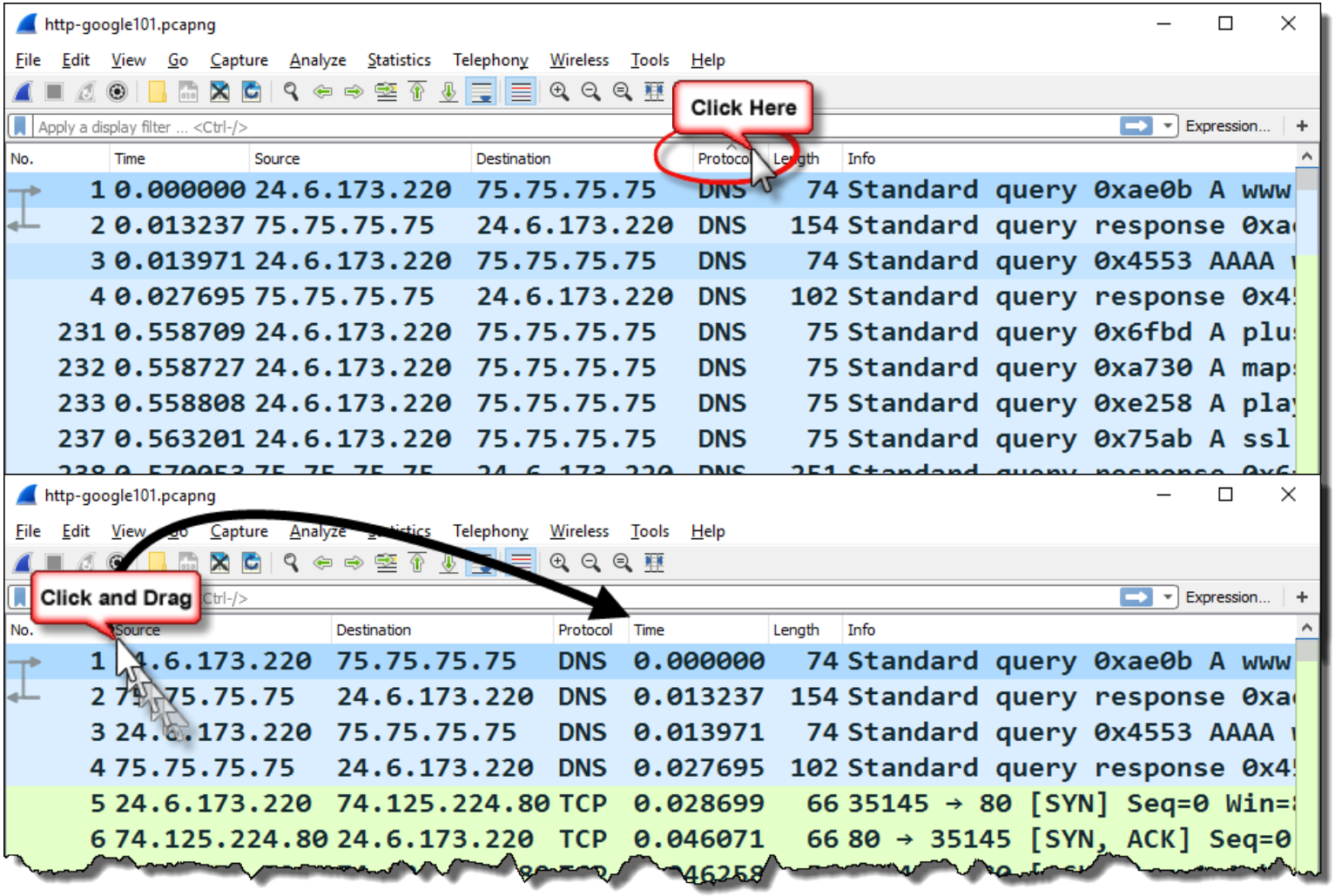
Internet Protocol Ve … , Dst: 75.75.75.75
0100 .... = Versio
.... 0101 = Header
Differentiated Ser … S0, ECN: Not-ECT)
0000 00.. = Diff … int: Default (0)
.... ..00 = Expl … on: Not ECN-Capable Transport…
Total Length: 58
Identification: 0x
Flags: 0x00
0... .... = Rese
.0.. .... = Don't
..0. .... = More
Fragment offset: 0
Time to live: 128

Expand Subtrees Shift+Right
Expand All Ctrl+Right
Collapse All Ctrl+Left
Apply as Column
Apply as Filter
Prepare a Filter
Conversation Filter
Colorize with Filter
Follow
Copy
Export Packet Bytes... Ctrl+H
Wiki Protocol Page
Filter Field Reference
Protocol Preferences
Decode As...
Go to Linked Packet
… d Packet in New Window

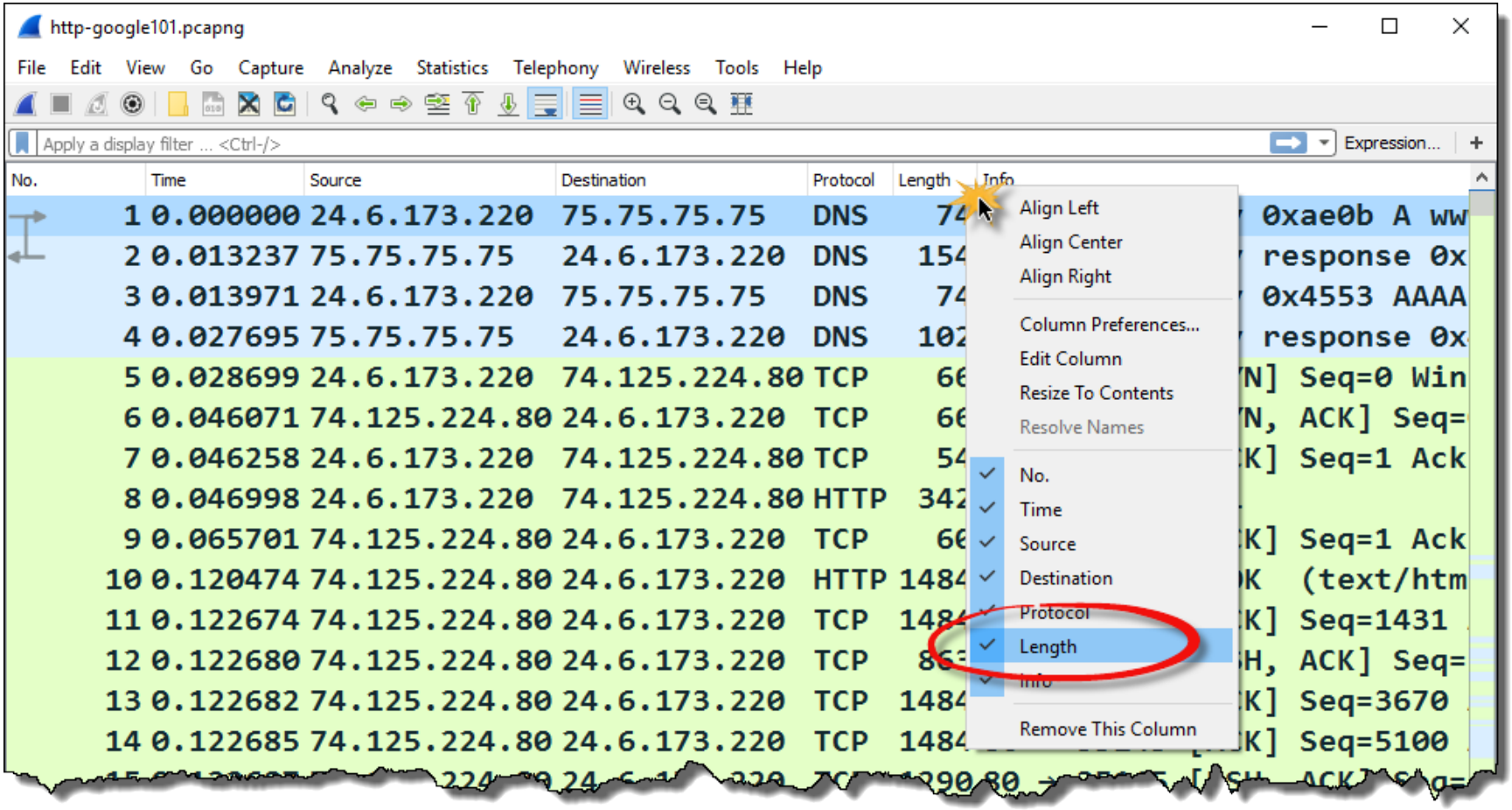
right-click

Time to live (ip.ttl), 1 byte | Packets: 4900 · Displayed: 4900 (100.0%) · Load time: 0:0.175 | Profile: Default

Sort and Reorder Columns

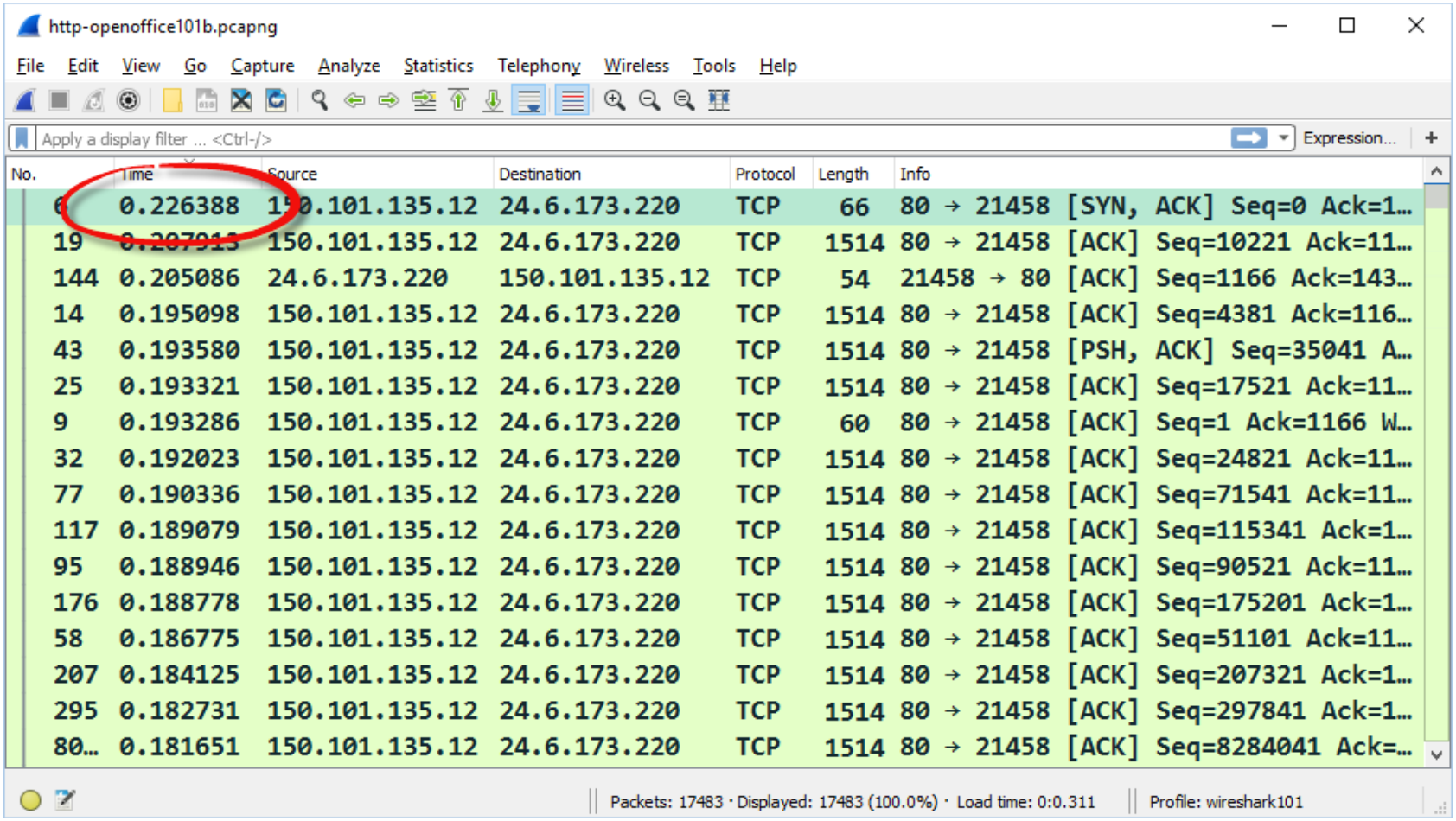


Hide, Display, Rename, and Remove Columns



Change the Time Column Setting

View | Time Display Format | Seconds Since Previous Displayed Packet



No.	Time	Source	Destination	Protocol	Length	Info
6	0.226388	150.101.135.12	24.6.173.220	TCP	66	80 → 21458 [SYN, ACK] Seq=0 Ack=1…
19	0.207915	150.101.135.12	24.6.173.220	TCP	1514	80 → 21458 [ACK] Seq=10221 Ack=11…
144	0.205086	24.6.173.220	150.101.135.12	TCP	54	21458 → 80 [ACK] Seq=1166 Ack=143…
14	0.195098	150.101.135.12	24.6.173.220	TCP	1514	80 → 21458 [ACK] Seq=4381 Ack=116…
43	0.193580	150.101.135.12	24.6.173.220	TCP	1514	80 → 21458 [PSH, ACK] Seq=35041 A…
25	0.193321	150.101.135.12	24.6.173.220	TCP	1514	80 → 21458 [ACK] Seq=17521 Ack=11…
9	0.193286	150.101.135.12	24.6.173.220	TCP	60	80 → 21458 [ACK] Seq=1 Ack=1166 W…
32	0.192023	150.101.135.12	24.6.173.220	TCP	1514	80 → 21458 [ACK] Seq=24821 Ack=11…
77	0.190336	150.101.135.12	24.6.173.220	TCP	1514	80 → 21458 [ACK] Seq=71541 Ack=11…
117	0.189079	150.101.135.12	24.6.173.220	TCP	1514	80 → 21458 [ACK] Seq=115341 Ack=1…
95	0.188946	150.101.135.12	24.6.173.220	TCP	1514	80 → 21458 [ACK] Seq=90521 Ack=11…
176	0.188778	150.101.135.12	24.6.173.220	TCP	1514	80 → 21458 [ACK] Seq=175201 Ack=1…
58	0.186775	150.101.135.12	24.6.173.220	TCP	1514	80 → 21458 [ACK] Seq=51101 Ack=11…
207	0.184125	150.101.135.12	24.6.173.220	TCP	1514	80 → 21458 [ACK] Seq=207321 Ack=1…
295	0.182731	150.101.135.12	24.6.173.220	TCP	1514	80 → 21458 [ACK] Seq=297841 Ack=1…
80…	0.181651	150.101.135.12	24.6.173.220	TCP	1514	80 → 21458 [ACK] Seq=8284041 Ack=…

Right-Click in the Packet List Pane

http-google101.pcapng

http-google101.pcapng

File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help

Apply a display filter ... <Ctrl-/> Expression... +

No.	Time	Source	Destination	Protocol	Length	Info
1	0.000000	24.6.173.220	75.75.75.75	DNS	74	Standard query 0xae0b A www
2	0.013237	75.75.75.75	24.6.173.220	DNS	154	Standard query response 0xa
3	0.013971	24.6.173.220	75.75.75.75			Standard query 0x4553 AAAA
4	0.027695	75.75.75.75	24.6.173.220			y response 0x4
5	0.028699	24.6.173.220	74.125.224.8			YN] Seq=0 Win=
6	0.046071	74.125.224.80	24.6.173.220			YN, ACK] Seq=0
7	0.046258	24.6.173.220	74.125.224.8			CK] Seq=1 Ack=
8	0.046998	24.6.173.220	74.125.224.8			1
9	0.065701	74.125.224.80	24.6.173.220			CK] Seq=1 Ack=
10	0.120474	74.125.224.80	24.6.173.220			OK (text/html

right-click

- Mark/Unmark Packet Ctrl+M
- Ignore/Unignore Packet Ctrl+D
- Set/Unset Time Reference Ctrl+T
- Time Shift... Ctrl+Shift+T
- Packet Comment...
- Edit Resolved Name
- Apply as Filter
- Prepare a Filter
- Conversation Filter
- Colorize Conversation
- SCTP
- Follow
- Copy
- Protocol Preferences
- Decode As...
- Show Packet in New Window

```
> Frame 3: 74 bytes on wire (592 bits), 7          its) on inter…
> Ethernet II, Src: HewlettP_a7:bf:a3 (d4          Cadant_31:bb:…
> Internet Protocol Version 4, Src: 24.6.          75
> User Datagram Protocol, Src Port: 63342          (53)

0000  00 01 5c 31 bb c1 d4 85  64 a7 bf          .. d.....E.
0010  00 3c 08 3e 00 00 80 11  00 00 18          .. ......KK
0020  4b 4b f7 6e 00 35 00 28  5c b2 45          ( \.ES....
0030  00 00 00 00 00 00 03 77  77 77 06 67 6f 6f 67 6c   .......w ww.googl
```

Packets: 374 · Displayed: 374 (100.0%) · Load time: 0:0.7 | Profile: Default

Right-Click in the Packet Details Pane

http-google101.pcapng

File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help

Apply a display filter ... <Ctrl-/> | Expression... | + | GET|POST | CONNECT | HEAD | HTTP4xx | HTTP5xx | HTTP3xx

No.	Time	Length	Source	Destination	Protocol	Info
1	0.000000	74	24.6.173.…	75.75.75.75	DNS	Standard query 0xae0b A www.…
2	0.013237	154	75.75.75.75	24.6.173.…	DNS	Standard query response 0xae…

Frame 1: 74 bytes on … its). 74 bytes captured (592 bits) on interfac…
Interface id: 0 (\D … 5E4-EEFF300A9B9F})
Encapsulation type:
Arrival Time: Oct 2 … fic Daylight Time
[Time shift for thi
Epoch Time: 1350938
[Time delta from pr … 000 seconds]
[Time delta from pr … 0000 seconds]
[Time since referen … seconds]
Frame Number: 1
Frame Length: 74 by
Capture Length: 74
[Frame is marked: F
[Frame is ignored:
[Protocols in frame
[Coloring Rule Name
[Coloring Rule Stri
Ethernet II, Src: Hew … a3), Dst: Cadant_31:bb:c1 …

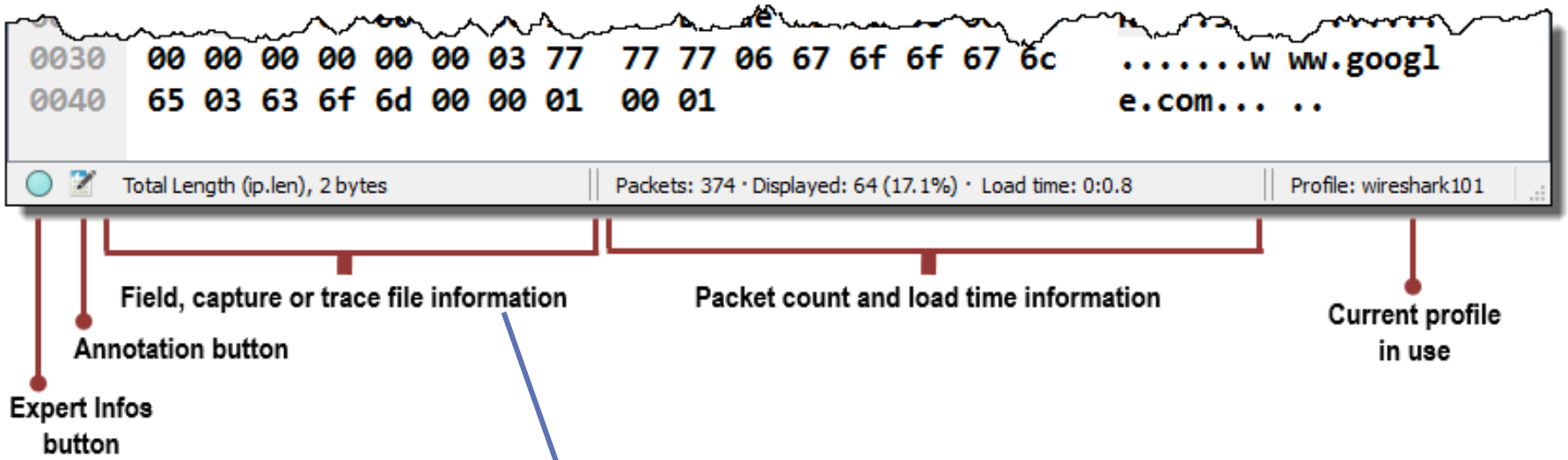
right-click

- Expand Subtrees — Shift+Right
- Expand All — Ctrl+Right
- Collapse All — Ctrl+Left
- Apply as Column
- Apply as Filter
- Prepare a Filter
- Conversation Filter
- Colorize with Filter
- Follow
- Copy
- Export Packet Bytes... — Ctrl+H
- Wiki Protocol Page
- Filter Field Reference
- Protocol Preferences
- Decode As...
- Go to Linked Packet
- Show Linked Packet in New Window

Frame (frame), 74 bytes | Packets: 374 · Displayed: 374 (100.0%) · Load time: 0:0.11 | Profile: wireshark101

NOTE
Right-click to view numerous options in the Packet Details pane

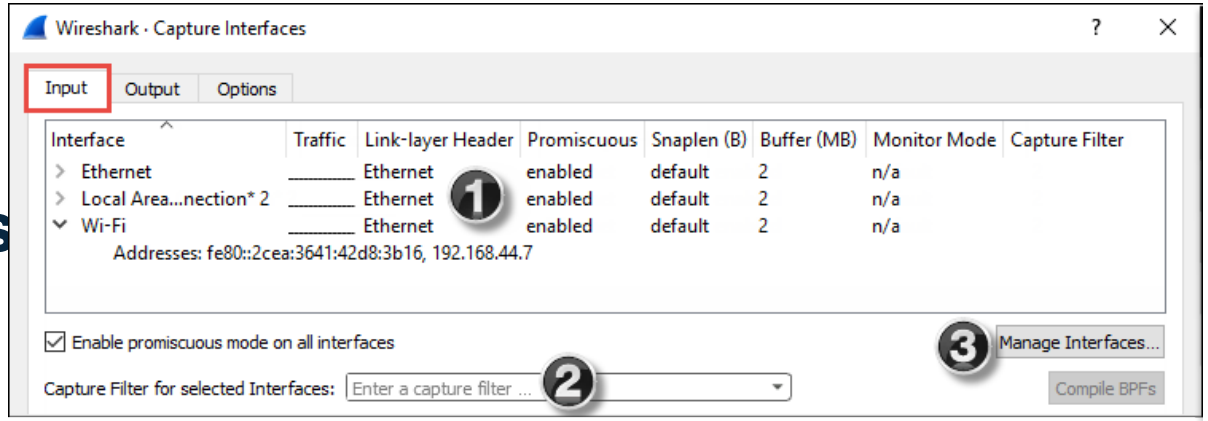
Pay Attention to the Status Bar

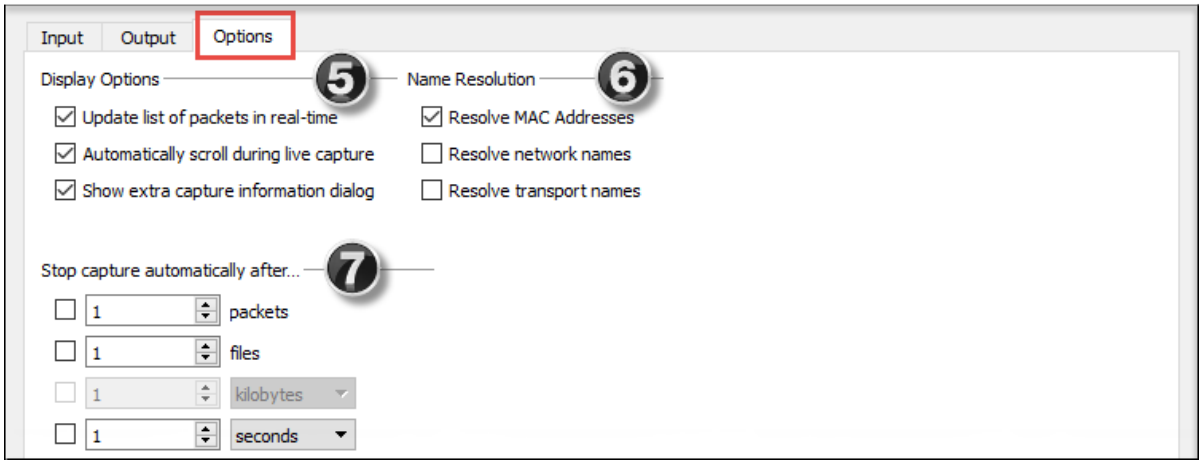


NOTE

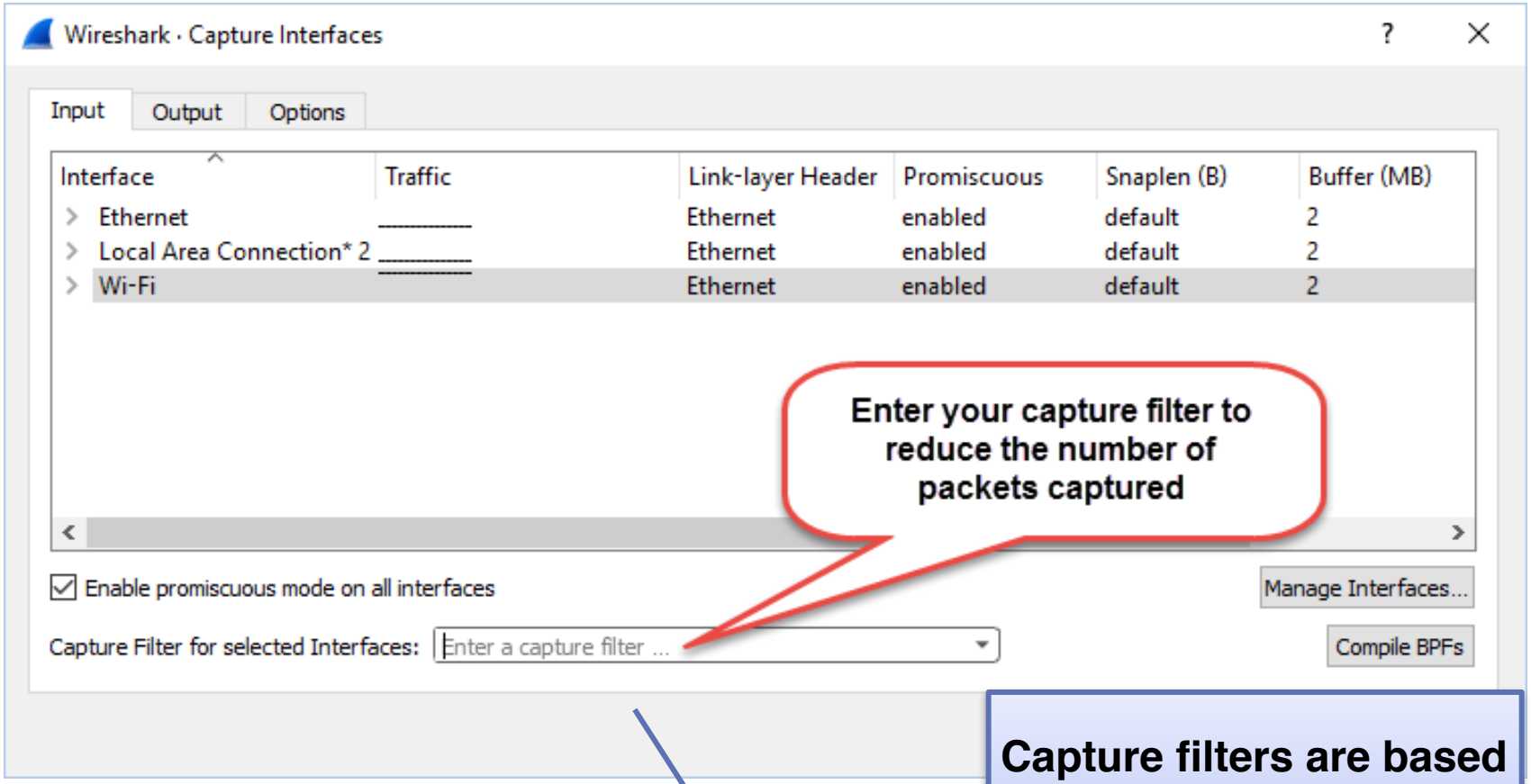
Contents of this column changes depending on what you've highlighted in the three panes

Capture Options



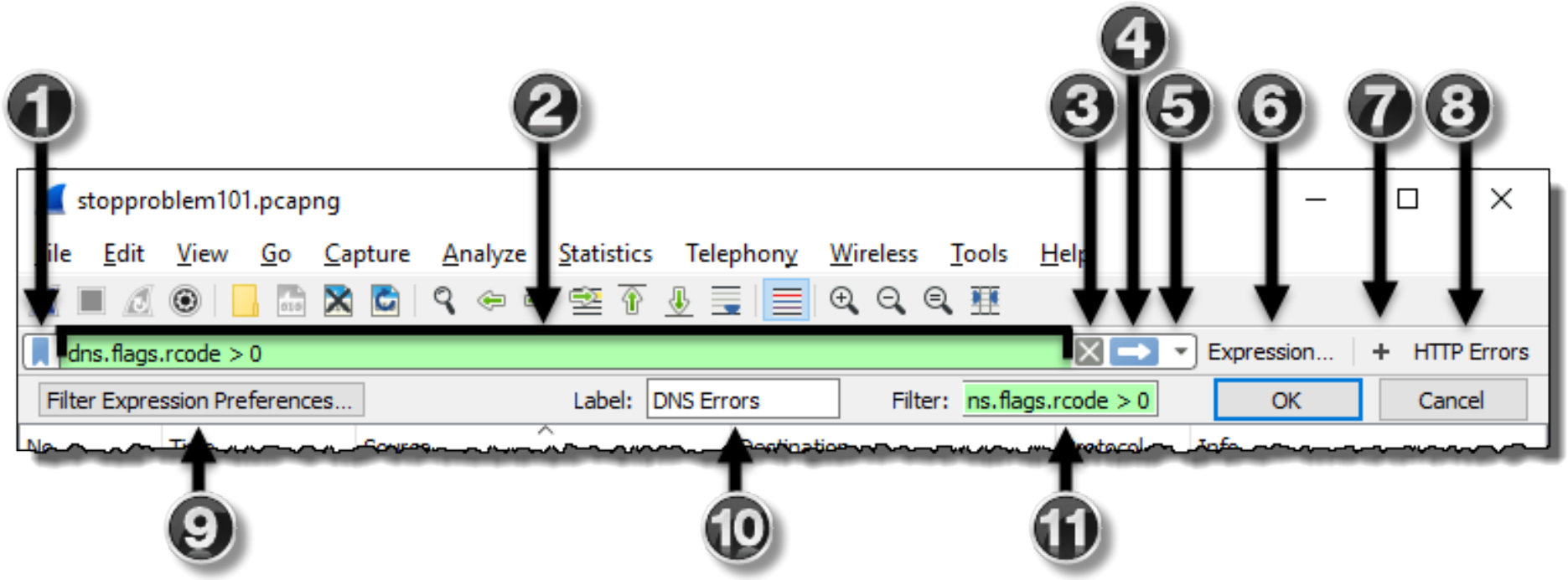


Apply Capture Filters



Capture filters are based on the Berkeley Packet Filtering (BPF) format

Display Filter Area



Use Proper Display Filter Syntax
(Wireshark-Specific Syntax)

Filter Type	Filter Example
Protocol	`arp`
Application	`dns`
Field Existence	`http.host`
Characteristic Existence	`tcp.analysis.zero_window`
Field Value	`http.host=="www.wireshark.org"`
Regex* Search Term	`http.host matches "\.(?i)(exe|zip)"`

*Wireshark uses the Pearl-Compatible Regular Expression (PCRE) engine.

Display Filter Techniques

- **Type in** if you know the field names/syntax (error detection mechanism)
- **Auto-complete** to walk you through building a display filter
- **Expressions** to walk you through building a display filter with/without comparison operators
- **Recall** saved or previously-used filter
- **Right-click** in the Packet List pane for conversation filters or on a Table row
- **Create buttons** out of your favorite display filters.

Learn the Field Names

http-browse101.pcapng

File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help

Apply a display filter ... <Ctrl-/> Expression... + HTTP Errors

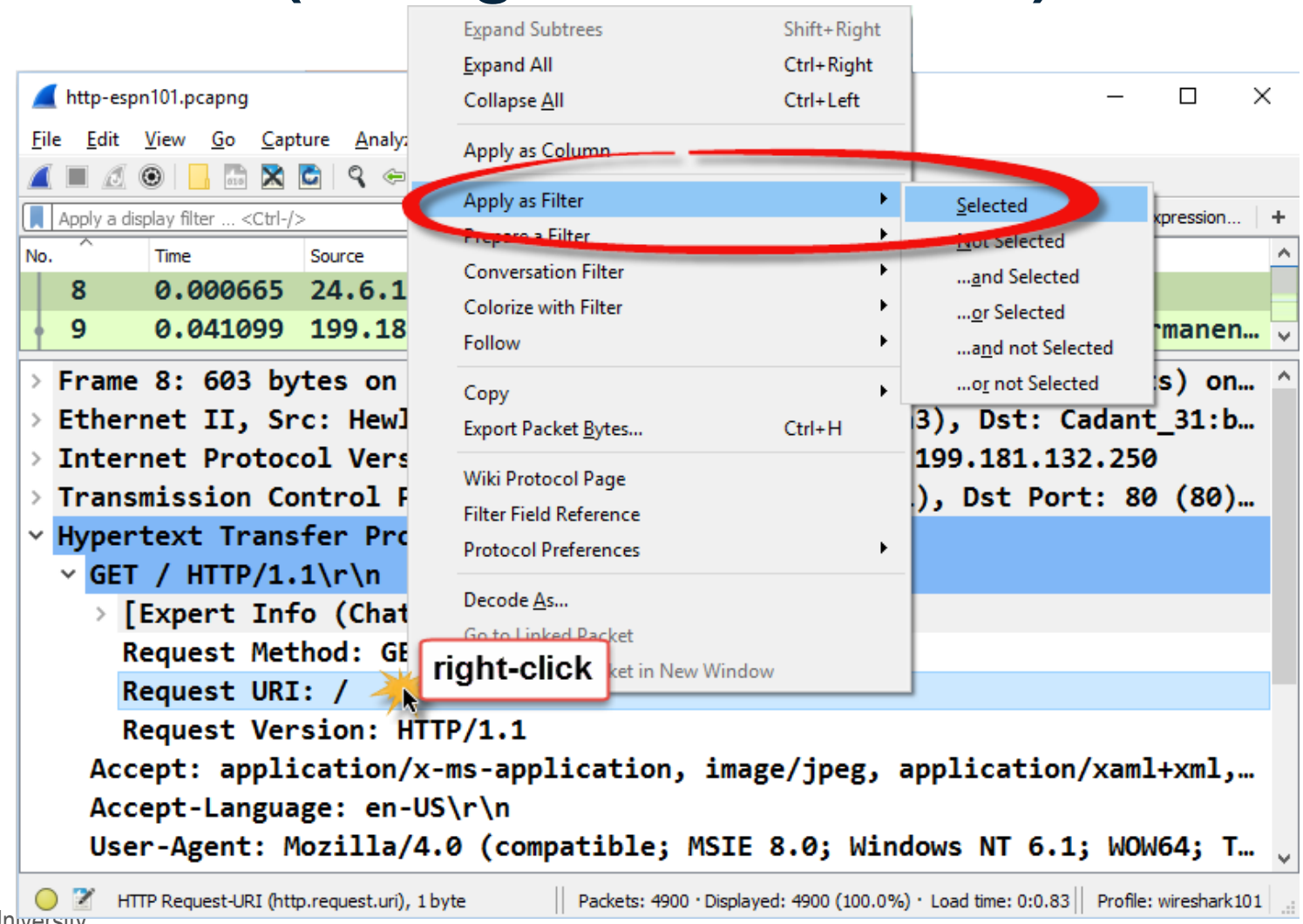
No.	Time	Source	Destination	Protocol	Info
10	0.000853	24.6.173.220	174.137.42.75	HTTP	GET / HTTP/1.1
11	0.020101	174.137.42.75	24.6.173.220	TCP	80 → 42379 [ACK] Seq=1 Ack=292 Win=6912 …
12	0.003404	174.137.42.75	24.6.173.220	HTTP	HTTP/1.1 200 OK [Unreassembled Packet]
13	0.001870	174.137.42.75	24.6.173.220	TCP	80 → 42379 [ACK] Seq=1461 Ack=292 Win=69…
14	0.000662	24.6.173.220	174.137.42.75	TCP	42379 → 80 [ACK] Seq=292 Ack=2921 Win=65…

```
> Frame 10: 345 bytes on wire (2760 bits), 345 bytes captured (2760 bits) on interface 0
> Ethernet II, Src: HewlettP_a7:bf:a3 (d4:85:64:a7:bf:a3), Dst: Cadant_31:bb:c1 (00:01:5c:3…
> Internet Protocol Version 4, Src: 24.6.173.220, Dst: 174.137.42.75
> Transmission Control Protocol, Src Port: 42379 (42379), Dst Port: 80 (80), Seq: 1, Ack: 1…
v Hypertext Transfer Protocol
  v GET / HTTP/1.1\r\n
    > [Expert Info (Chat/Sequence): GET / HTTP/1.1\r\n]
      Request Method: GET
      Request URI: /
      Request Version: HTTP/1.1
```

HTTP Request Method (http.request.method), 3 bytes | Packets: 2011 · Displayed: 2011 (100.0%) · Load time: 0:0.34 | Profile: wireshark101

tp-espn101.pcapng

Quickly Filter on a Field in a Packet
(the right-click method)



Use Auto-Complete to Build Display Filters

http-browse101.pcapng

File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help

http.request.

Expression... + HTTP Errors

http.request.full_uri
http.request.line
http.request.method
http.request.uri
http.request.version

No.	Destination	Protocol	Info
1	75.75.75.75	DNS	Standard query 0x9ba8 A www.wireshark.…
2			dard query response 0x9ba8 A www.w…
3	0.000783 24.6.17		rd query 0x8920 AAAA www.wiresha…
4	0.030017 24.6.17		rd query 0x8920 AAAA www.wiresha…
5	0.003284 75.75.75.75		standard query response 0x8920 AAAA ww…
6			

Auto-complete lists all available display filters that begin with `http.request.`

http-browse101.pcapng

File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help

tcp.analysis.

Expression... + HTTP Errors

tcp.analysis.ack_lost_segment
tcp.analysis.ack_rtt
tcp.analysis.acks_frame
tcp.analysis.bytes_in_flight
tcp.analysis.duplicate_ack
tcp.analysis.duplicate_ack_frame
tcp.analysis.duplicate_ack_num
tcp.analysis.fast_retransmission
tcp.analysis.flags
tcp.analysis.initial_rtt
tcp.analysis.keep_alive
tcp.analysis.keep_alive_ack
tcp.analysis.lost_segment
tcp.analysis.out_of_order
tcp.analysis.retransmission
tcp.analysis.reused_ports
tcp.analysis.rto
tcp.analysis.rto_frame
tcp.analysis.spurious_retransmission
tcp.analysis.tfo_syn

No.	Destination	Protocol	Info
1	75.75.75.75	DNS	Standard query 0x9ba8 A www.wireshark.…
2	24.6.173.220	DNS	Standard query response 0x9ba8 A www.w…
3	75.75.75.75	DNS	Standard query 0x8920 AAAA www.wiresha…
4	75.75.75.75	DNS	Standard query 0x8920 AAAA www.wiresha…
5	24.6.17		response 0x8920 AAAA ww…
6	174.		Seq=0 Win=8192 Len=0 …
7	24.6		esponse 0x8920 AAAA ww…
8	24.6		ACK] Seq=0 Ack=1 Win=…
9	174.1		Seq=1 Ack=1 Win=65700…
10	174.137.42.75	HTTP	GET / HTTP/1.1
11	24.6.173.220	TCP	80 → 42379 [ACK] Seq=1 Ack=292 Win=691…
12	24.6.173.220	HTTP	HTTP/1.1 200 OK [Unreassembled Packet]

TCP packets analyzed by Wireshark's Expert System can be viewed using one of the filters beginning with `tcp.analysis.`

Comparison Operators

Operation	English	Example	Description
==	eq	ip.src == 10.2.2.2	Display all IPv4 traffic from 10.2.2.2
!=	ne	tcp.srcport != 80	Display all TCP traffic from any port except port 80
>	gt	frame.time_relative > 1	Display packets that arrived more than 1 second after the previous packet in the trace file
<	lt	tcp.window_size < 1460	Display when the TCP receive window size is less than 1460 bytes
>=	ge	dns.count.answers >= 10	Display DNS response packets that contain at least 10 answers
<=	lt	ip.ttl <= 10	Display any packets that have 10 or less in the IP Time to Live field
	contains	http contains "GET"	Display all the HTTP client GET requests

Note: Be careful using the `!=` operator.

tp-espn101.pcapng

Filter on a Single TCP or UDP Conversation

(the right-click method)

http-espn101.pcapng

File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help

Apply a display filter ... <Ctrl-/> Expression... +

No.	Time	Source	Destination
508	0.000303	24.6.173.220	184.84.222.48
509	0.000188	24.6.173.220	184.84.222.48
510	0.000040	24.6.173.220	75.75.75.75
511	0.000250	24.6.173.220	75.75.75.75
512	0.000003	24.6.173.220	184.84.222.48

right-click

Mark/Unmark Packet Ctrl+M
Ignore/Unignore Packet Ctrl+D
Set/Unset Time Reference Ctrl+T
Time Shift... Ctrl+Shift+T
Packet Comment...
Edit Resolved Name
Apply as Filter
Prepare a Filter
Conversation Filter
Colorize Conversation
SCTP
Follow
Copy
Protocol Preferences
Decode As...
Show Packet in New Window

ENIP IO
ENIP Explicit
Ethernet
IPv4
IPv6
TCP
UDP
PN-CBA
PN-IO AR
PN-IO AR (with data)

Frame 508: 476 bytes on wire (3808 bits), 47 ... on interface 0
Ethernet II, Src: HewlettP_a7:bf:a3 (d4:85:6 ... bb:c1 (00:01:5c:…
Internet Protocol Version 4, Src: 24.6.173.2
Transmission Control Protocol, Src Port: 199
Hypertext Transfer Protocol
GET /prod/assets/tabs-A-sprite.png HTTP/1.
[Expert Info (Chat/Sequence): GET /prod/
Request Method: GET
Request URI: /prod/assets/tabs-A-sprite.
Request Version: HTTP/1.1
Accept: */*\r\n

Packets: 4900 · Displayed: 4900 (100.0%) · Load time: 0:0.80 Profile: wireshark101

Use Filters to Spot Communication Delays

Calculate Conversations Timestamps setting must be enabled to see this [Timestamps] section

http-download101d.pcapng

File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help

tcp.time_delta > 1

Expression...

	Source	Destination	Protocol	Info
000000	216.239.11…	192.168.1.64	TCP	[TCP Retransmission] 80 → 1828…
.885…	216.239.11…	192.168.1.64	TCP	80 → 18280 [ACK] Seq=2249861 A…
9.41…	216.239.11…	192.168.1.64	TCP	[TCP Retransmission] 80 → 1828…
129637	216.239.11…	192.168.1.64	TCP	80 → 18280 [ACK] Seq=20165661 …

```
 size value: 5840
lated window size: 5840]
w size scaling factor: -1 (unknown)]
um: 0x6fd5 [validation disabled]
urgent pointer: 0
> [SEQ/ACK analysis]
v [Timestamps]
    [Time since first frame in this TCP stream: 37.248064000 seconds]
    [Time since previous frame in this TCP stream: 1.518125000 seconds]
```

Time delta from previous frame...is TCP stream (tcp.time_delta | Packets: 24098 · Displayed: 4 (0.0%) · Load time: 0:0.431 | Profile: wireshark101

tp-espn101.pcapng

Use Right-Click to Follow a Stream

http-espn101.pcapng

File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help

tcp.stream eq 0

Expression...

No.	Time	Source	Destination	Protocol	Info
5	0	173.220	99.181.132.250	TCP	19941 → 80 [SYN] Seq=0 Win=8192 Len=…
6			173.220	TCP	80 → 19941 [SYN, ACK] Seq=0 Ack=1 Wi…
7			81.132.250	TCP	19941 → 80 [ACK] Seq=1 Ack=1 Win=657…
8			1.132.250	HTTP	GET / HTTP/1.1
9			173.220		
31			81.132.250	TC	

right-click

Mark/Unmark Packet Ctrl+M
Ignore/Unignore Packet Ctrl+D
Set/Unset Time Reference Ctrl+T
Time Shift... Ctrl+Shift+T
Packet Comment...
Edit Resolved Name
Apply as Filter
Prepare a Filter
Conversation Filter
Colorize Conversation
SCTP
Follow
Copy
Protocol Preferences
Decode As...
Show Packet in New Window

TCP Stream
UDP Stream
SSL Stream

Frame
Ether
Inter
Trans
Sou
De
[St
[TC
Sec
Ack
Hea

ts), 66 byte
a3 (d4:85:64
24.6.173.22
c Port: 1994
sequence nu

Wireshark · Follow TCP Stream (tcp.stream eq 0) · http-espn...

```
GET / HTTP/1.1
Accept: application/x-ms-
application, image/jpeg,
application/xaml+xml, image/gif,
image/pjpeg, application/x-ms-xbap,
application/vnd.ms-excel,
pplication/vnd.ms-powerpoint,
```

Packet 8. 1 client pkt(s), 1 server pkt(s), 1 turn. Click to select.

Entire conversation (979 bytes) Show data as ASCII Stream 0

Find: Find Next

Hide this stream Print Save as... Close Help

Packets: 4900 · Displayed: 7 (0.1%) · Load time: 0:0.101 Profile: wireshark101

tp-espn101.pcapng

Filter on a Conversation from Wireshark Statistics

Wireshark · Conversations · http-espn101

Ethernet · 1 | IPv4 · 37 | IPv6 | TCP · 63 | UDP · 82

Address A	Port A	Address B	Port B	Packets	Bytes A → B	Packets B → A	Bytes B → A	Rel Start	Duration	Bits/s A → B	Bits/s
24.6.173.220	19996	184.84.222.88	80	1,855	30 k	1322	1989 k	9.726479000	64.450526	3765	
24.6.173.220	19976	184.84.222.120	80	534				000	62.455871	1413	
24.6.173.220	19980	184.84.222.10	80	251				000	61.220801	620	
24.6.173.220	19945	184.84.222.48	80	150				000	68.853274	847	
24.6.173.220	19956	184.84.222.152	80	137				000	17.293814	3944	
24.6.173.220	19942	68.71.216.176	80	127				000	24.512076	2332	
24.6.173.220	19944	184.84.222.48	80	121	116 k	42		000	68.853471	665	
24.6.173.220	19981	184.84.222.10	80	120	119 k	41		000	61.220638	359	
24.6.173.220	20002	68.71.216.157	80	112	10 k	57		000	42.514690	586	
24.6.173.220	19983	184.84.222.152	80	111	111 k	38	6082	73	000	66.207100	734
24.6.173.220	19961	74.125.224.59	80	110	103 k	37	3751	73	000	65.383440	458
24.6.173.220	19943	184.84.222.48	80	90	81 k	34	5823	56	000	68.852948	676
24.6.173.220	19950	184.84.222.48	80	88	85 k	29	4579	59	000	57.356422	638
24.6.173.220	19954	184.84.222.48	80	67	62 k	25	4006	42	58 k	3.216284000	56.403650	568
24.6.173.220	19978	184.84.222.120	80	61	59 k	21	1734	40	57 k	7.913036000	61.259194	226

right-click

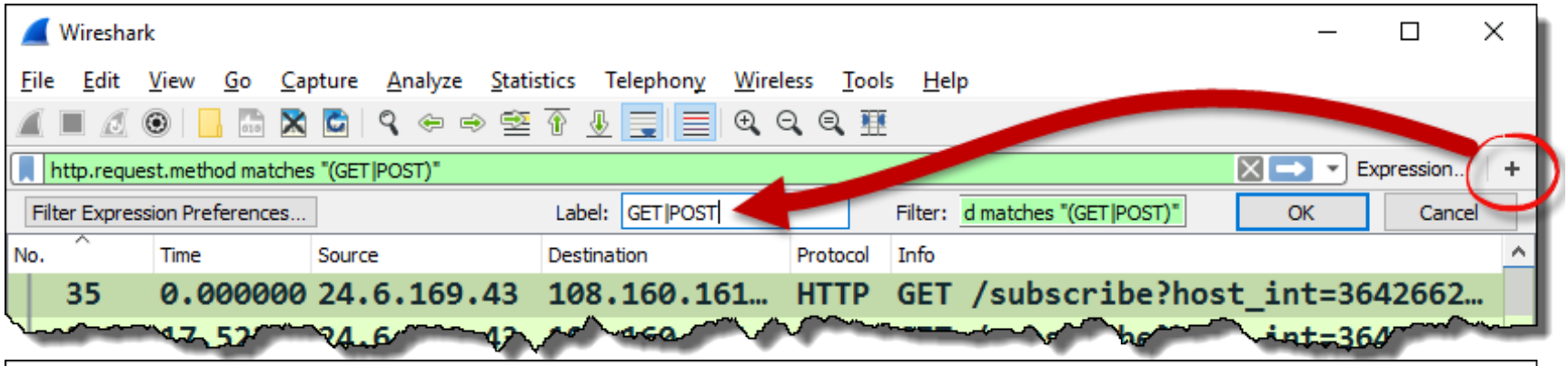
- Apply as Filter
  - Selected
    - A ↔ B
    - A → B
    - B → A
    - A ↔ Any
    - A → Any
    - Any → A
    - Any ↔ B
    - Any → B
    - B → Any
  - Not Selected
  - ...and Selected
  - ...or Selected
  - ...and not Selected
  - ...or not Selected
- Prepare a Filter
- Find
- Colorize

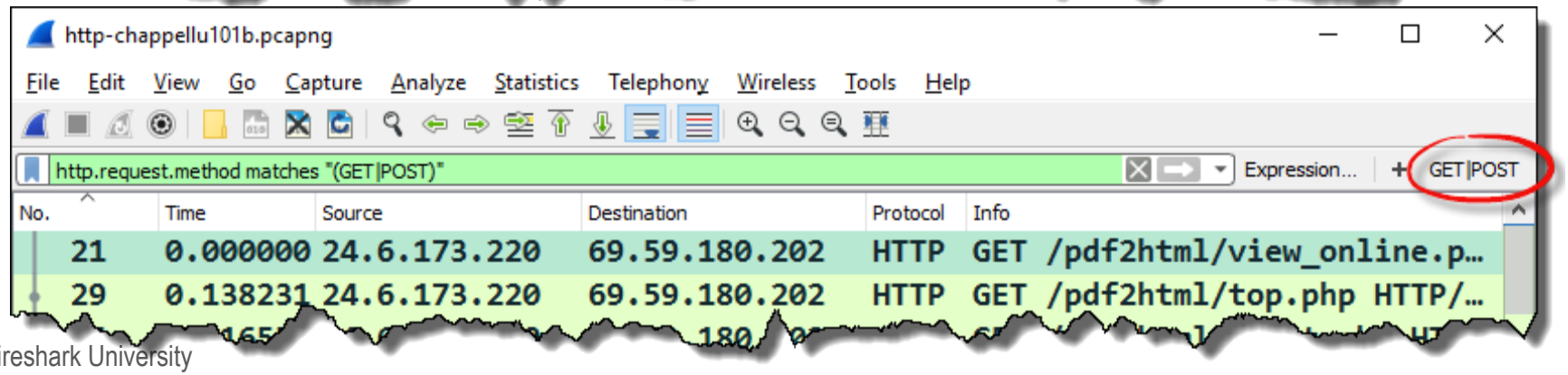
Name resolution | Limit to display filter | Conversation Types

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

Turn Your Key Display Filters into Buttons

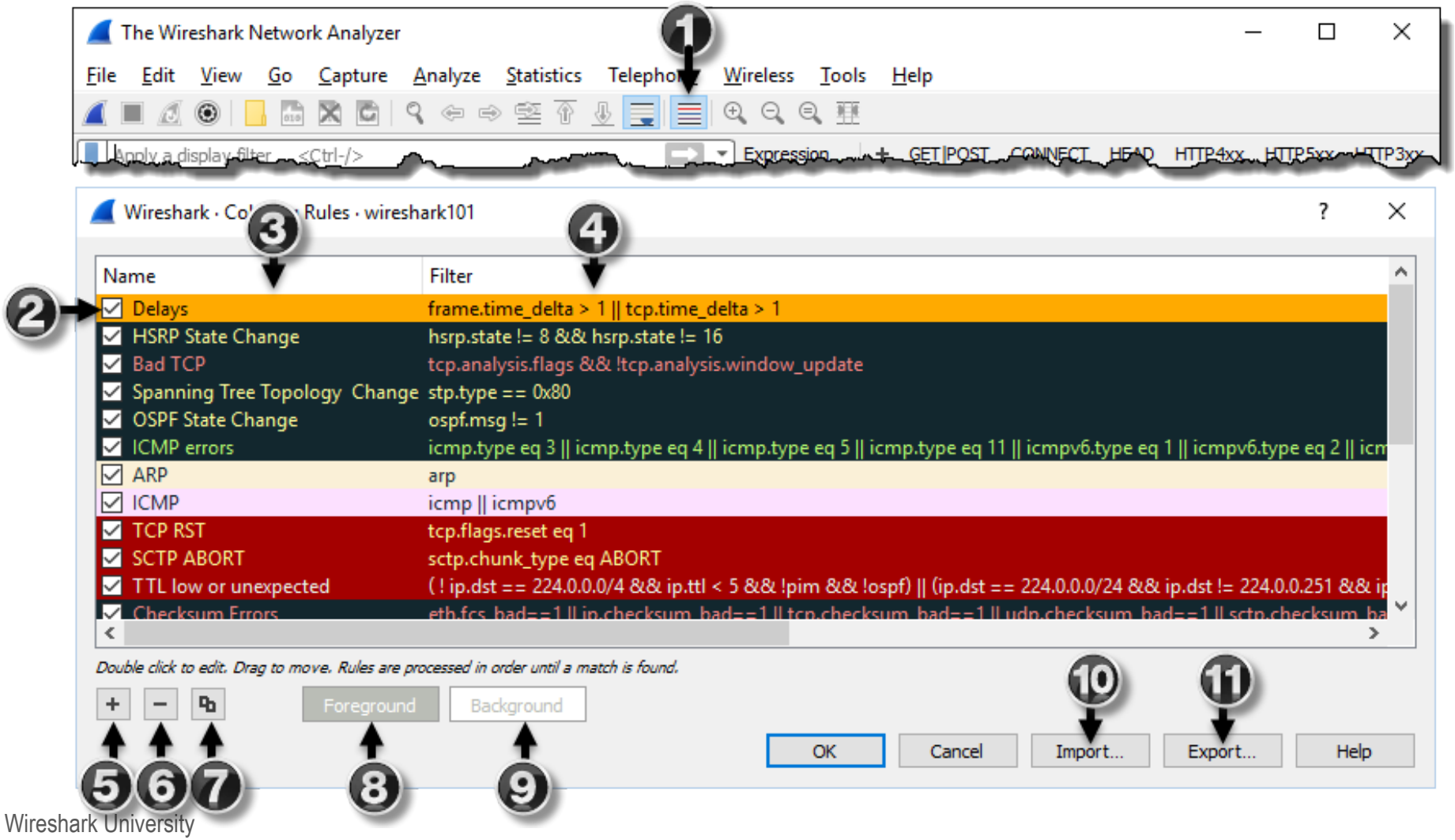
1. Create a display filter and click +.
2. Name your Filter Expression button.
   (Reorder/edit/disable or delete in **Preferences | Filter Expression.**)





Quick Reference

Coloring Rules Interface



c-nessus101.pcapng

Identify Applied Coloring Rules

sec-nessus.pcapng

File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help

Apply a display filter ... <Ctrl-/> Expression... + GET|POST CONNECT HEAD HTTP4xx HTTP5xx HTTP3xx

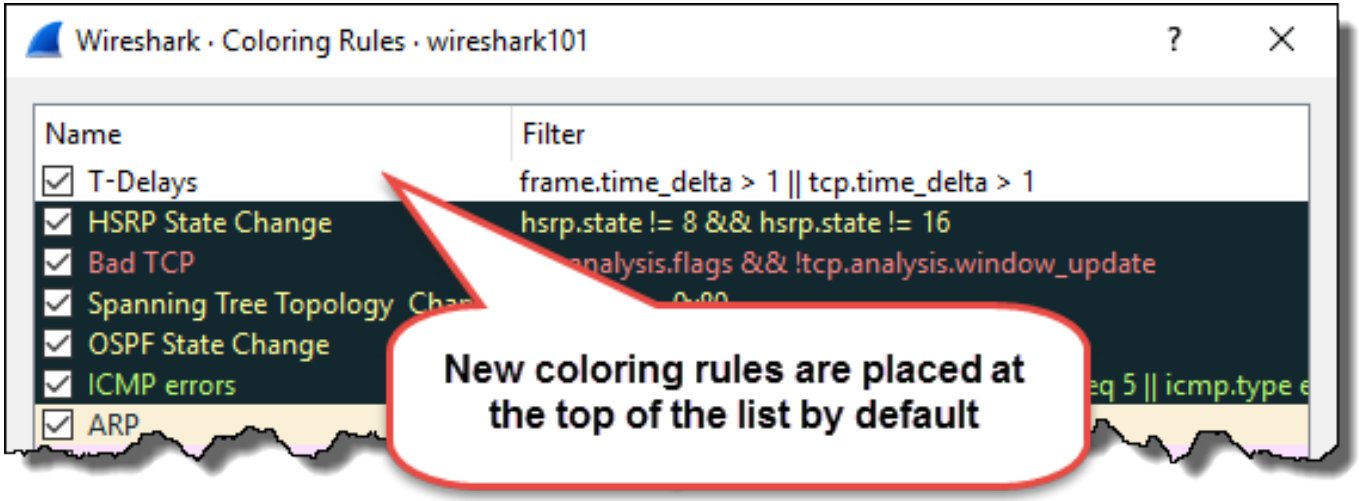
No.	Time	Source	Destination	Protocol	Info
1	0.000000	192.168.1.141	192.168.1.123	ICMP	Echo (ping) request id=0xdb2…
2	0.000034	192.168.1.123	192.168.1.141	ICMP	Echo (ping) reply id=0xdb2…
3	0.007928	192.168.1.141	192.168.1.123	ICMP	Echo (ping) request id=0xdb2…

```
> Packet comments
v Frame 1: 98 bytes on wire (784 bits), 98 bytes captured (784 bits) on interfac…
    Interface id: 0 (unknown)
    Encapsulation type: Ethernet (1)
    Arrival Time: Jan 10, 2006 09:56:33.941505000 Pacific Standard Time
    [Time shift for this packet: 0.000000000 seconds]
    Epoch Time: 1136915793.941505000 seconds
    [Time delta from previous captured frame: 0.000000000 seconds]
    [Time delta from previous displayed frame: 0.000000000 seconds]
    [Time since reference or first frame: 0.000000000 seconds]
    Frame Number: 1
    Frame Length: 98 bytes (784 bits)
    Capture Length: 98 bytes (784 bits)
    [Frame is marked: False]
    [Frame is ignored: False]
    [Protocols in frame: eth:ethertype:ip:icmp:data]
    [Coloring Rule Name: ICMP]
    [Coloring Rule String: icmp || icmpv6]
```

sec-nessus | Packets: 2021 · Displayed: 2021 (100.0%) · Load time: 0:0.620 | Profile: wireshark101

Build a Coloring Rule to Highlight Delays

```
frame.time_delta > 1 || tcp.time_delta > 1
```



Master the Intelligent Scrollbar

ftp-bounce.pcapng

File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help

Apply a display filter ... <Ctrl-/> Expression... + GET|POST CONNECT HEAD HTTP4xx HTTP5xx HTTP3xx

No.	Time	Source	Destination	Protocol	Info
30	0.201725	204.181.64.2	24.6.103.134	TCP	64712 → 21 [ACK] Seq=63 Ack=322 …
31	7.209497	204.181.64.2	24.6.103.134	FTP	Request: TYPE I
32	0.040956	24.6.103.134	204.181.64.2	FTP	Response: 200 Type se to I.
33	0.097859	204.181.64.2	24.6.103.134	FTP	Re
34	0.126899	24.6.103.134	204.181.64.2	FTP	Re M…
35	0.090889	204.181.64.2	24.6.103.134	TCP	64 5…
36	0.000165	24.6.103.134	204.181.64.2	TCP	1303 → 64444 [SYN, ACK] 0 Ac…
37	0.089448	204.181.64.2	24.6.103.134	TCP	64444 → 1303 [ACK] Seq=1 Ack= W…
38	0.001690	204.181.64.2	24.6.103.134	FTP	Request: STOR in design template…
39	0.133418	24.6.103.134	204.181.64.2	TCP	21 …
40	0.002159	24.6.103.134	204.181.64.2	FTP	Re …
41	0.057583	24.6.103.134	204.181.64.2	TCP	1303 → 4 [FIN, ACK] 1 Ac…
42	0.000090	24.6.103.134	204.181.64.2	FTP	Respon : 425 Error: Possible bo…
43	0.051747	204.181.64.2	24.6.103.134	FTP…	FTP Data: 512 bytes
44	0.000074	24.6.103.134	204.181.64.2	TCP	1303 → 64444 [RST] Seq=2 Win=0 L…
45	0.002597	204.181.64.2	24.6.103.134	FTP…	FTP Data: 512 bytes

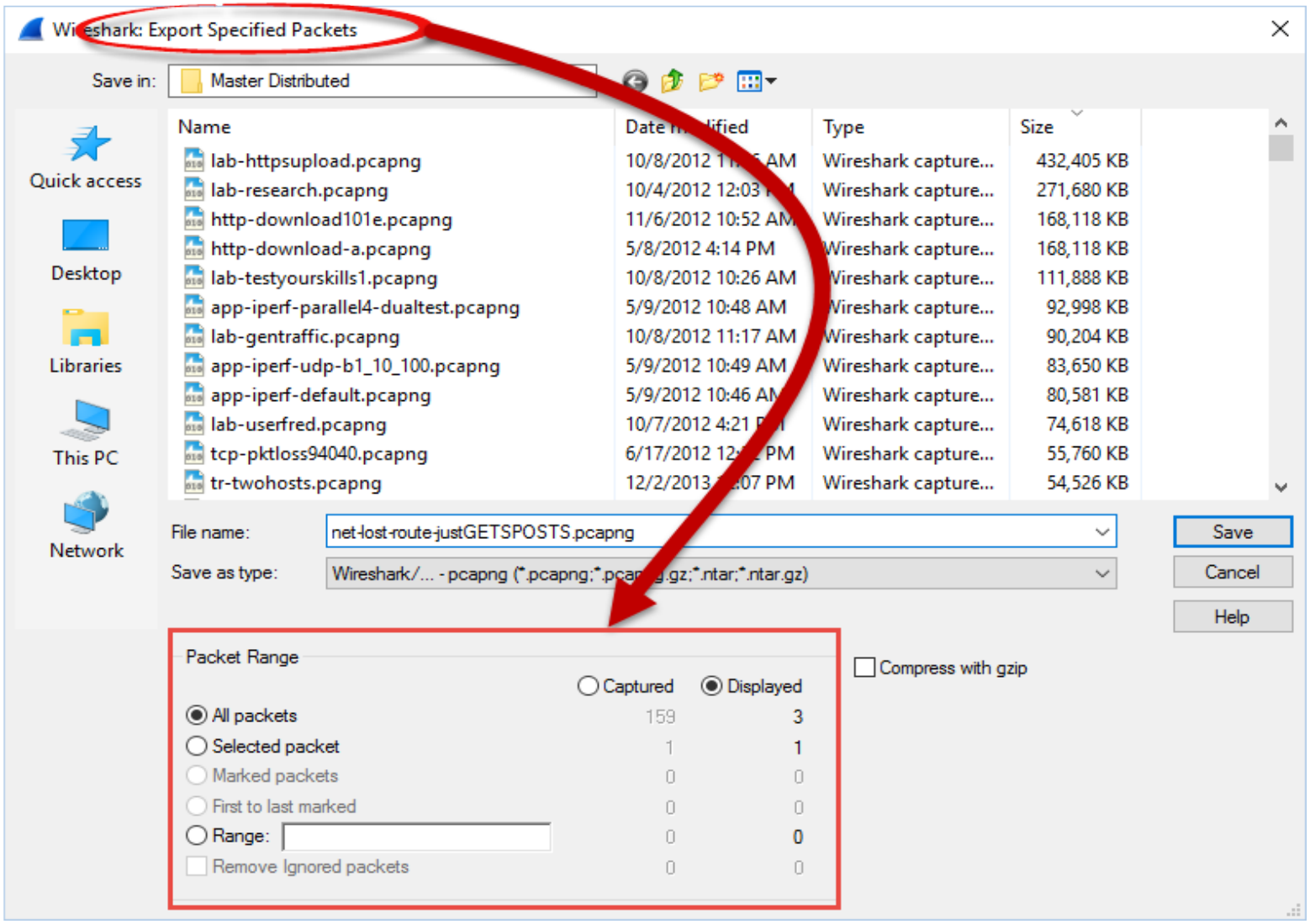
Orange stripe is an FTP command - custom coloring rule

Red stripes are TCP Resets - a default coloring rule

Thumb

Packets: 53 · Displayed: 53 (100.0%) · Load time: 0:0.5 Profile: wireshark101

Export Packets that Interest You



p browse101.pcapng

Export Packet Details

http-browse101.pcapng

File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help

Open Ctrl+O
Open Recent
Merge...
Import from Hex Dump...
Close Ctrl+W
Save Ctrl+S
Save As... Ctrl+Shift+S
File Set
Export Specified Packets...
Export Packet Dissections
Export Packet Bytes... Ctrl+H
Export PDUs to File...
Export SSL Session Keys...
Export Objects
Print... Ctrl+P
Quit Ctrl+Q

As Plain Text...
As CSV...
As "C" Arrays...
As PSML XML...
As PDML XML...

Expression... + GET|POST CONNECT HEAD HTTP4xx HTTP5xx HTTP3xx

All column data will be exported - add columns as desired to export additional information

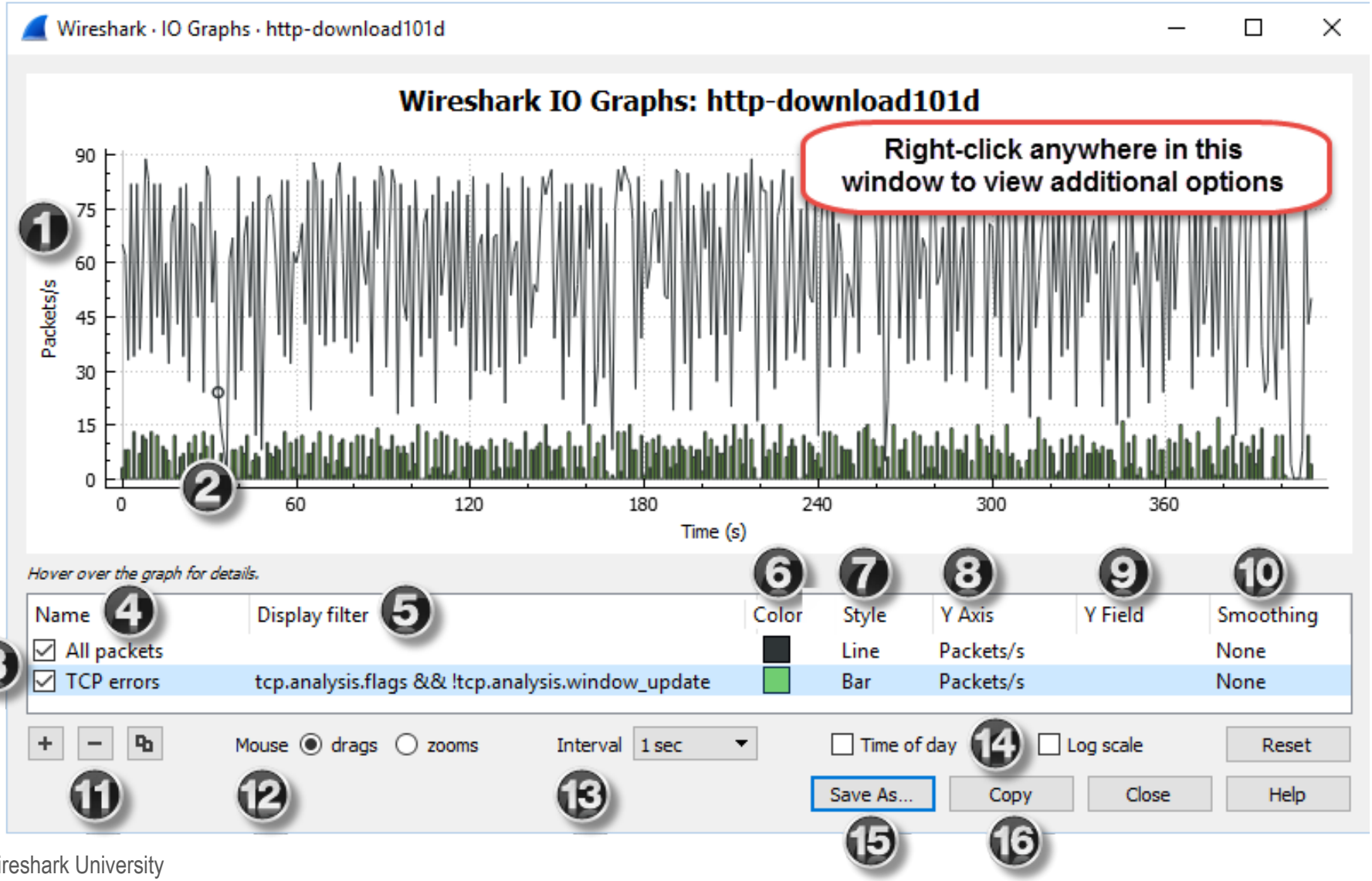
Packets: 2011 · Displayed: 2011 (100.0%) · Load time: 0:0.34 | Profile: wireshark101

Section 5 Skills

Build and Interpret Charts and Graphs

Quick Reference

IO Graph Interface



tp-espn101.pcapng

Find Out Who's Talking to Whom

Wireshark · Conversations · http-espn101

Ethernet · 1 | IPv4 · 37 | IPv6 | TCP · 63 | UDP · 82

Address A	Address B	Packets	Bytes	Packets A → B	Bytes A → B	Packets B → A	Bytes B → A	Rel Start
24.6.173.220	184.84.222.88	1,855	2020 k	533	30 k	1322	1989 k	9.726479000
24.6.173.220	184.84.222.48	720	649 k	265	43 k	455	605 k	0.322923000
24.6.173.220	184.84.222.120	613	628 k	195	14 k	418	614 k	6.716176000
24.6.173.220	184.84.222.10	371	382 k	119	7502	252	374 k	7.950911000
24.6.173.220	184.84.222.152	303	286 k	110	25 k	193	261 k	3.261301000
24.6.173.220	68.71.216.176	127	134 k	38	7147	89	127 k	0.168701000
24.6.173.220	74.125.224.59	142	115 k	51	9643	91	105 k	2.843065000
24.6.173.220	184.84.222.16	41	36 k	15	1768	26	35 k	7.951909000
24.6.173.220	184.84.222.75	36	33 k	12	1602	24	32 k	5.377013000
24.6.173.220	138.108.7.20	31	24 k	11	1675	20	23 k	5.436636000
24.6.173.220	68.71.216.171	29	24 k	12	1007	17	23 k	5.192672000
24.6.173.220	75.75.75.75	180	22 k	90	6973	90	15 k	0.000000000
24.6.173.220	68.71.216.157	132	20 k	66	3672	66	16 k	21.802866000
24.6.173.220	184.84.222.137	30	19 k	14	1638	16	17 k	3.270647000

Name resolution | Limit to display filter | Conversation Types

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

Locate the Top Talkers

Wireshark · Conversations · http-misctraffic101

Ethernet · 1 | IPv4 · 2 | IPv6 | TCP · 7 | UDP

Address A	Port A	Address B	Port B	Packets	Bytes	Packets A → B	Bytes A → B	Packets B → A	Bytes B
24.6.181.160	1266	107.6.133.250	80	475	533 k	126	8261	349	
24.6.181.160	1260	208.118.237.137	80	127	122 k	37	3086	90	
24.6.181.160	1264	208.118.237.137	80	40	36 k	14	1705	26	
24.6.181.160	1261	208.118.237.137	80	10	2141	5	1174	5	
24.6.181.160	1263	208.118.237.137	80	10	2012	5	1175	5	
24.6.181.160	1262	208.118.237.137	80	10	2011	5	1174	5	
24.6.181.160	1265	208.118.237.137	80	10	1821	5	1169	5	

Name resolution | Limit to display filter | Conversation Types

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

List Active Applications

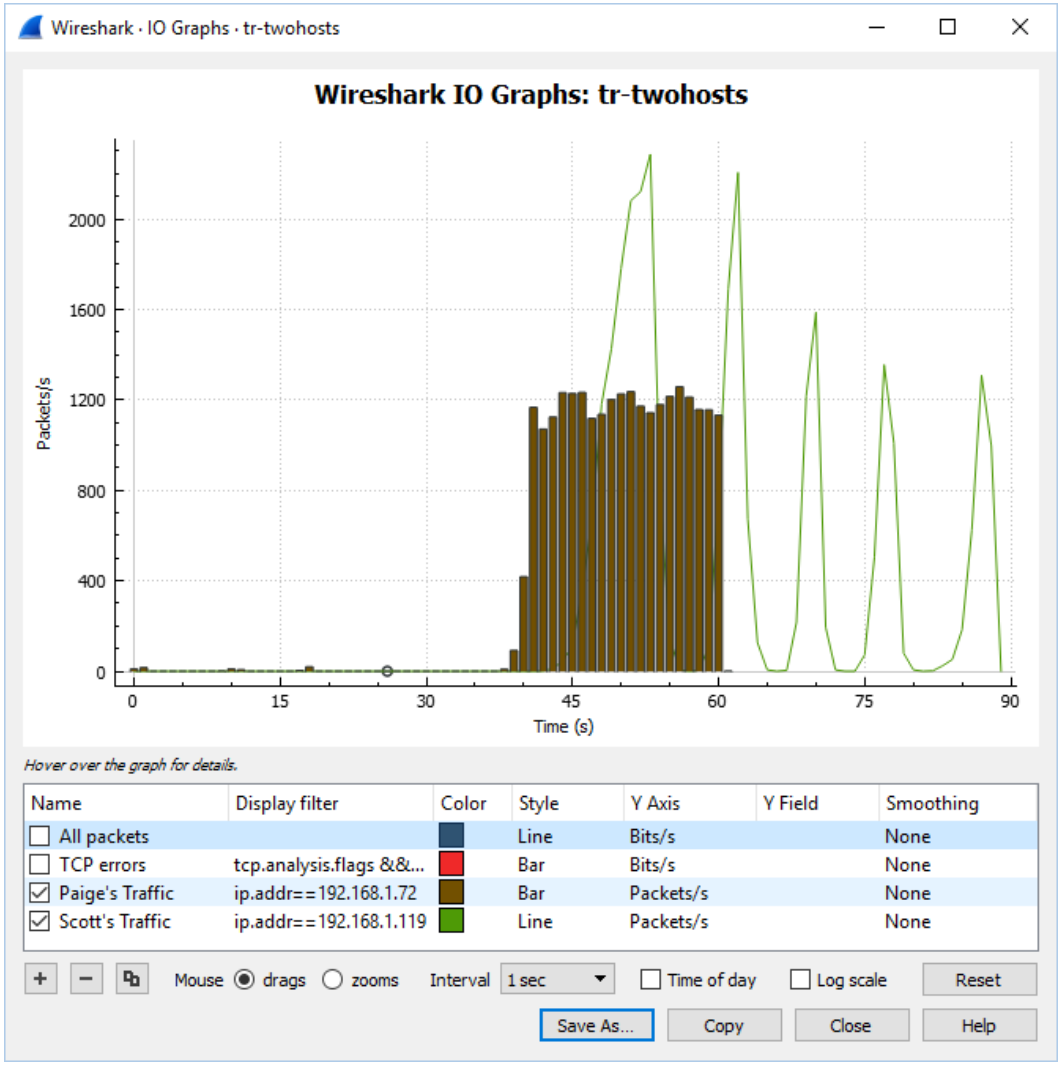
Wireshark · Protocol Hierarchy Statistics · http-browse101b

Protocol	Percent Packets	Packets	Percent Bytes	Bytes	Bits/s	End Packets	End Bytes	End Bits/s
Frame	100.0	195	100.0	107708	108 k	0	0	0
Ethernet	100.0	195	100.0	107708	108 k	0	0	0
Internet Protocol Version 6	8.2	16	1.9	2062	2074	0	0	0
User Datagram Protocol	8.2	16	1.9	2062	2074	0	0	0
Domain Name System	8.2	16	1.9	2062	2074	16	2062	2074
Internet Protocol Version 4	91.8	179	98.1	105646	106 k	0	0	0
Transmission Control Protocol	91.8	179	98.1	105646	106 k	114	59681	60 k
Hypertext Transfer Protocol	33.3	65	42.7	45965	46 k	33	13364	13 k
Portable Network Graphics	0.5	1	1.1	1229	1236	1	1229	1236
Media Type	0.5	1	1.4	1514	1523	1	1514	1523
Line-based text data	2.1	4	4.8	5176	5207	4	5176	5207
JPEG File Interchange Format	2.1	4	5.6	6056	6092	4	6056	6092
Compuserve GIF	11.3	22	17.3	18626	18 k	16	9542	9599
Unreassembled Fragmented Packet	3.1	6	8.4	9084	9139	6	9084	9139

No display filter.

Close | Copy | Help

Graph Application and Host Bandwidth Usage



Identify TCP Errors on the Network

```
> Differentiated Services Field: 0x00 (DSCP: CS0, ECN
  Total Length: 58
  Identification: 0x622a (25130)
> Flags: 0x00
```

Packets: 4900 · Displayed: 4900 (100.0%) · Load time: 0:0.119

Wireshark · Expert Information · http-espn101

Severity	Group	Pr
Warn	Sequence	
Warn	Malformed	
Note	Sequence	
Note	Malformed	
Chat	Sequence	
Chat	Sequence	

No display filter set.

Limit to Display Filter Search:

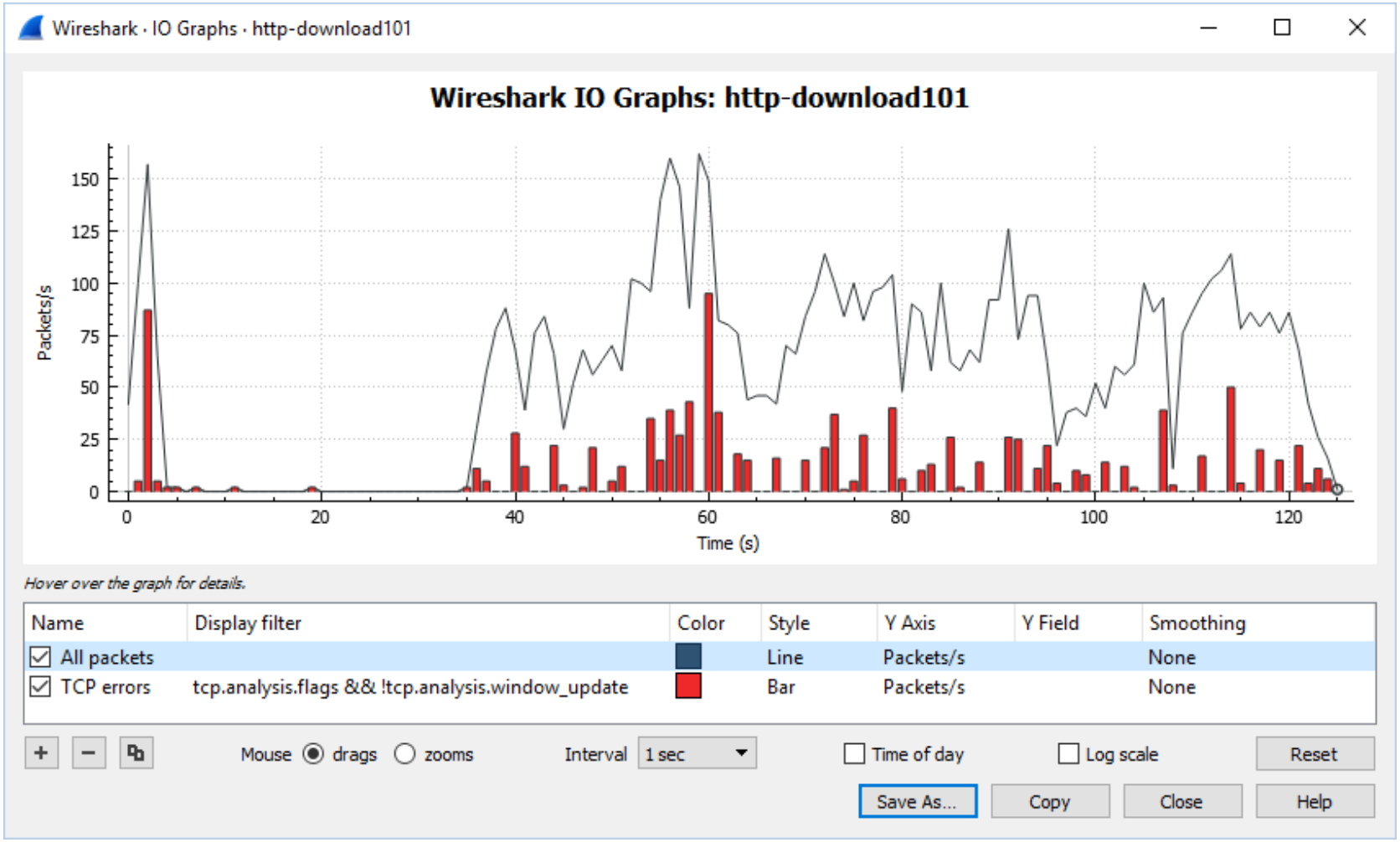
By default Wireshark displays all five levels of severity - in this case there are no Error or Comment items to show

Hoping this is going to change

Understand what the Expert Infos Errors Mean

- Packet Loss, Recovery, and Faulty Trace Files
- Asynchronous or Multiple Path Indications
- Keep-Alive Indication
- Receive Buffer Congestion Indications
- TCP Connection Port Reuse Indication
- Possible Router Problem Indication
- Misconfiguration or ARP Poisoning Indication

Graph Various Network Errors



Quick Reference

File and Object Reassembly Options

http-disney101.pcapng

File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help

Open Ctrl+O
Open Recent
Merge...
Import from Hex Dump...
Close Ctrl+W
Save Ctrl+S
Save As... Ctrl+Shift+S
File Set
Export Specified Packets...
Export Packet Dissections
Export Packet Bytes... Ctrl+H
Export PDUs to File...
Export SSL Session Keys...
Export Objects
Print... Ctrl+P
Quit Ctrl+Q

DICOM...
HTTP... (1)
SMB...
TFTP

Expression... + GET|POST CONNECT HEAD HTTP4xx HTTP5xx HTTP3xx

Destination Protocol Info

right-click

Mark/Unmark Packet Ctrl+M
Ignore/Unignore Packet Ctrl+D
Set/Unset Time Reference Ctrl+T
Time Shift... Ctrl+Shift+T
Packet Comment...
Edit Resolved Name
Apply as Filter
Prepare a Filter
Conversation Filter
Colorize Conversation
SCTP
Follow (2)
Copy
Protocol Preferences
Decode As...
Show Packet in New Window

TCP Stream (2)
UDP Stream (3)
SSL Stream (4)

.... 0101 = Header Length: 20 bytes
Differentiated Services Field: 0x00 (DSC
Total Length: 60
Identification: 0x697e (27006)
Flags: 0x00

Packets: 6143 · Displayed: 6143 (100.0%) · Load time: 0:0.124 Profile: wireshark101

Reassemble Web Browsing Sessions

p browse101.pcapng

Wireshark · Follow TCP Stream (tcp.stream eq 0) · http-browse101

```
GET / HTTP/1.1
Host: www.wireshark.org
User-Agent: Mozilla/5.0 (Windows NT 6.1; WOW64; rv:
16.0) Gecko/20100101 Firefox/16.0
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

HTTP/1.1 200 OK
Server: Apache/2
Vary: Accept-Encoding
X-Slogan: If it can shock or blind you it's layer 1.
Cache-Control: no-cache
Content-Type: text/html
Date: Sat, 20 Oct 2012 23:37:20 GMT
Keep-Alive: timeout=5, max=67
Transfer-Encoding: chunked
ETag: "240b17-40ad-4cb18943247f3"
```

Packet 10. 1 client pkt(s), 9 server pkt(s), 1 turn. Click to select.

Entire conversation (13 kB) | Show data as ASCII | Stream 0

Find: | Find Next

Hide this stream | Print | Save as... | Close | Help

Reassemble a File Transferred via FTP

-download101.pcapng

ftp-download101.pcapng

File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help

Apply a display filter ... <Ctrl-/> Expression... + GET|POST CONNECT HEAD HTTP4xx HTTP5xx HTTP3xx

No.	Time	Source	Destination	Protocol	Info
79	0.000944	24.6.173.220	131.246.123.4	FTP	Request: RETR /pub/wireshar…
80	0.210322	131.246.123.4	24.6.173.220	FTP	Response: 150 Opening BINAR…
81	0.026085	131.246.123.4	24.6.173.220	FTP	FTP Data: 1460 bytes
82	0.000984	131.246.123.4	24.6.173.220		…tes
83	0.000004	131.246.123.4	24.6.173.220		…tes
84	0.000173	24.6.173.220	131.246.123.4		…K] Seq=1 A…
85	0.167047	24.6.173.220	131.246.123.4		…Seq=420 Ac…
86	0.044281	131.246.123.4	24.6.173.220		…tes
87	0.000981	131.246.123.4	24.6.173.220		…tes
88	0.000002	131.246.123.4	24.6.173.220		…tes

> Frame 81: 1514 bytes on wire (12112 bits) … bits) on i…
> Ethernet II, Src: Cadant_31:bb:c1 (00:01: … a7:bf:a3 (d…
> Internet Protocol Version 4, Src: 131.246
> Transmission Control Protocol, Src Port: … 66 (64666),…
> FTP Data (1460 bytes data)

right-click

- Mark/Unmark Packet Ctrl+M
- Ignore/Unignore Packet Ctrl+D
- Set/Unset Time Reference Ctrl+T
- Time Shift... Ctrl+Shift+T
- Packet Comment...
- Edit Resolved Name
- Apply as Filter
- Prepare a Filter
- Conversation Filter
- Colorize Conversation
- SCTP
- Follow
  - TCP Stream
  - UDP Stream
  - SSL Stream
- Copy
- Protocol Preferences
- Decode As...
- Show Packet in New Window

Packets: 22479 · Displayed: 22479 (100.0%) · Load time: 0:0.273 Profile: wireshark101

tp-espn101.pcapng

Export HTTP Objects Transferred in a Web Browsing Session

Enable *Allow subdissector to reassemble TCP stream* (TCP preference).

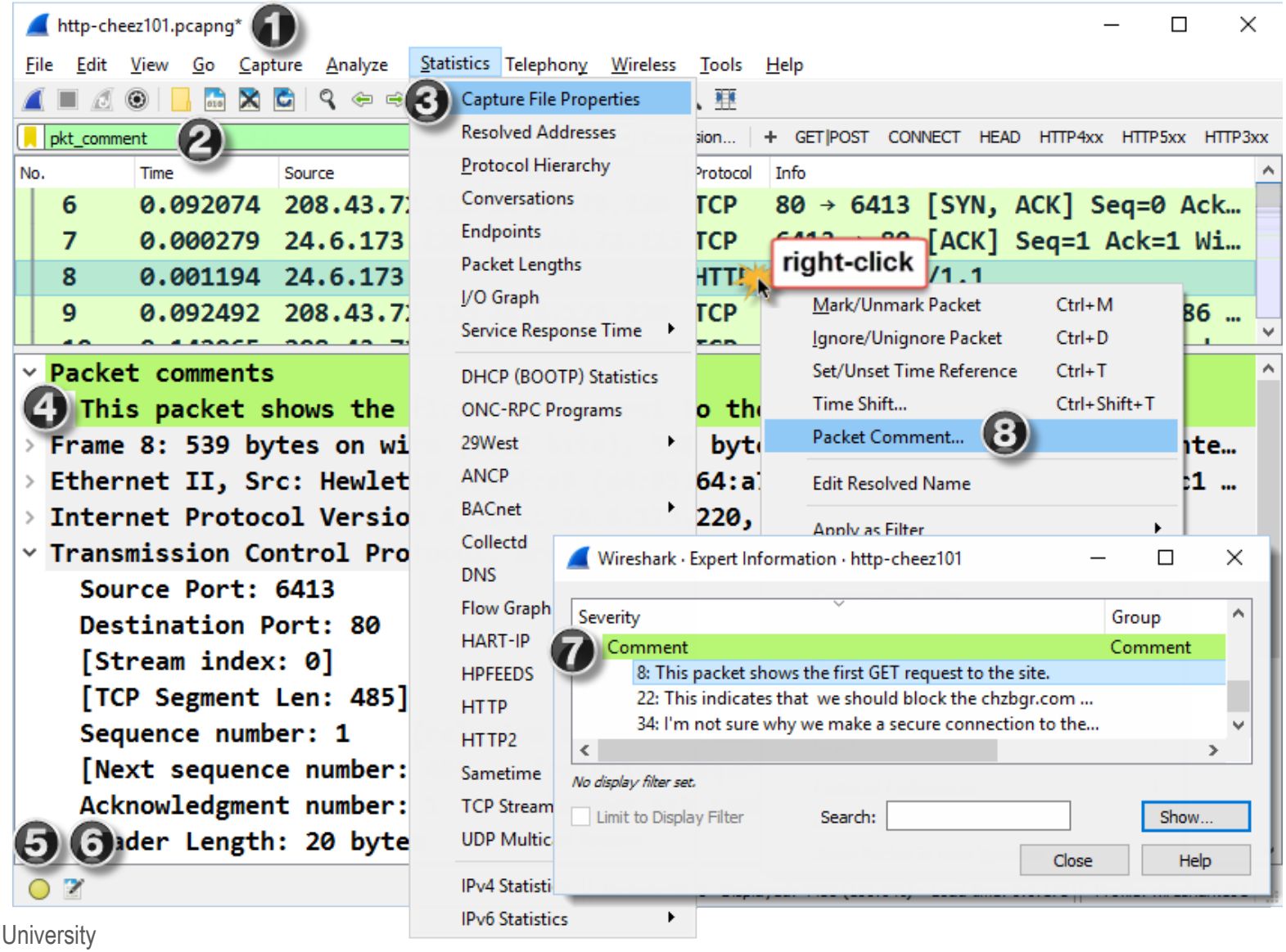
Wireshark · Export · HTTP object list

Packet	Hostname	Content Type	Size	Filename
9	www.espn.com	text/html	227 bytes	\
107	a.espncdn.com	application/x-javascript	26 kB	mbox.js
128	espn.go.com	text/html	266 kB	\
132	a.espncdn.com	text/css	74 kB	c?css=espn.teams.r4j.css
178	a.espncdn.com	text/css	309 kB	btn-toggle-tablet.css
180	ratings-wrs.symantec.com	text/xml	329 bytes	brief?url=http:%2F%2Fespn.go.com%2F&shz=1&guid=%7
291	a.espncdn.com	application/x-javascript	431 kB	espn.insider.201112021227.js,espn.espn360.stub.r9.js,espn.n
320	a1.espncdn.com	image/jpeg	491 bytes	bg_frontpage_red.jpg
325	espndotcom.tt.omtrdc.net		92 bytes	standard?mboxHost=espn.go.com&mboxSession=1325973
339	a.espncdn.com	image/png	245 bytes	social_facebook_14.png
340	broadband.espn.go.com	text/html	87 bytes	user?callback=jQuery171044244468988128804_13259732489
350	a1.espncdn.com	image/png	114 bytes	trans_border.png
351	a1.espncdn.com	image/jpeg	16 kB	bg_frontpage_elements.jpg
366	a1.espncdn.com	image/png	10 kB	header_sprite_fp.v3.png

Save | Save All | Close | Help

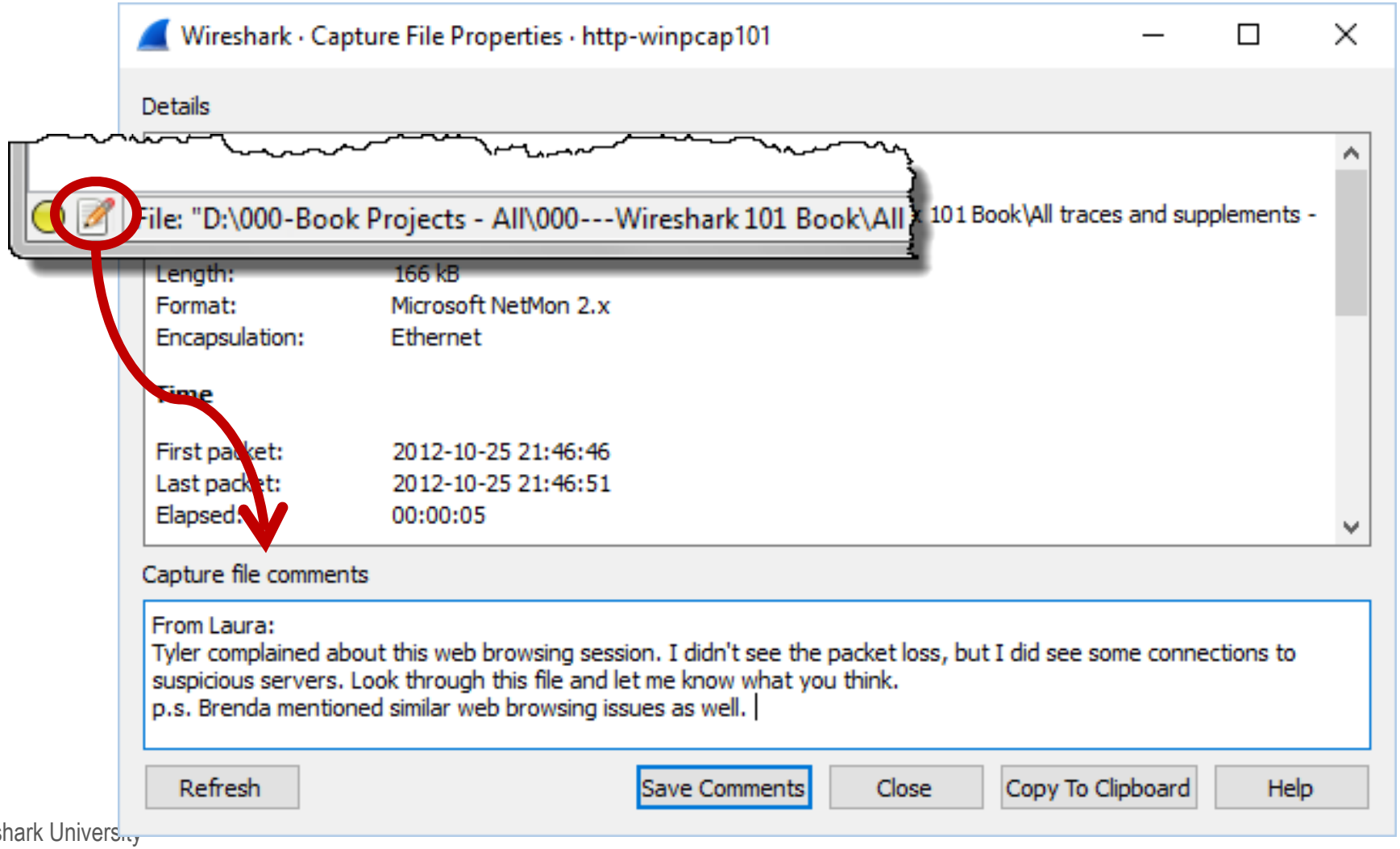
Quick Reference

File and Packet Annotation Options

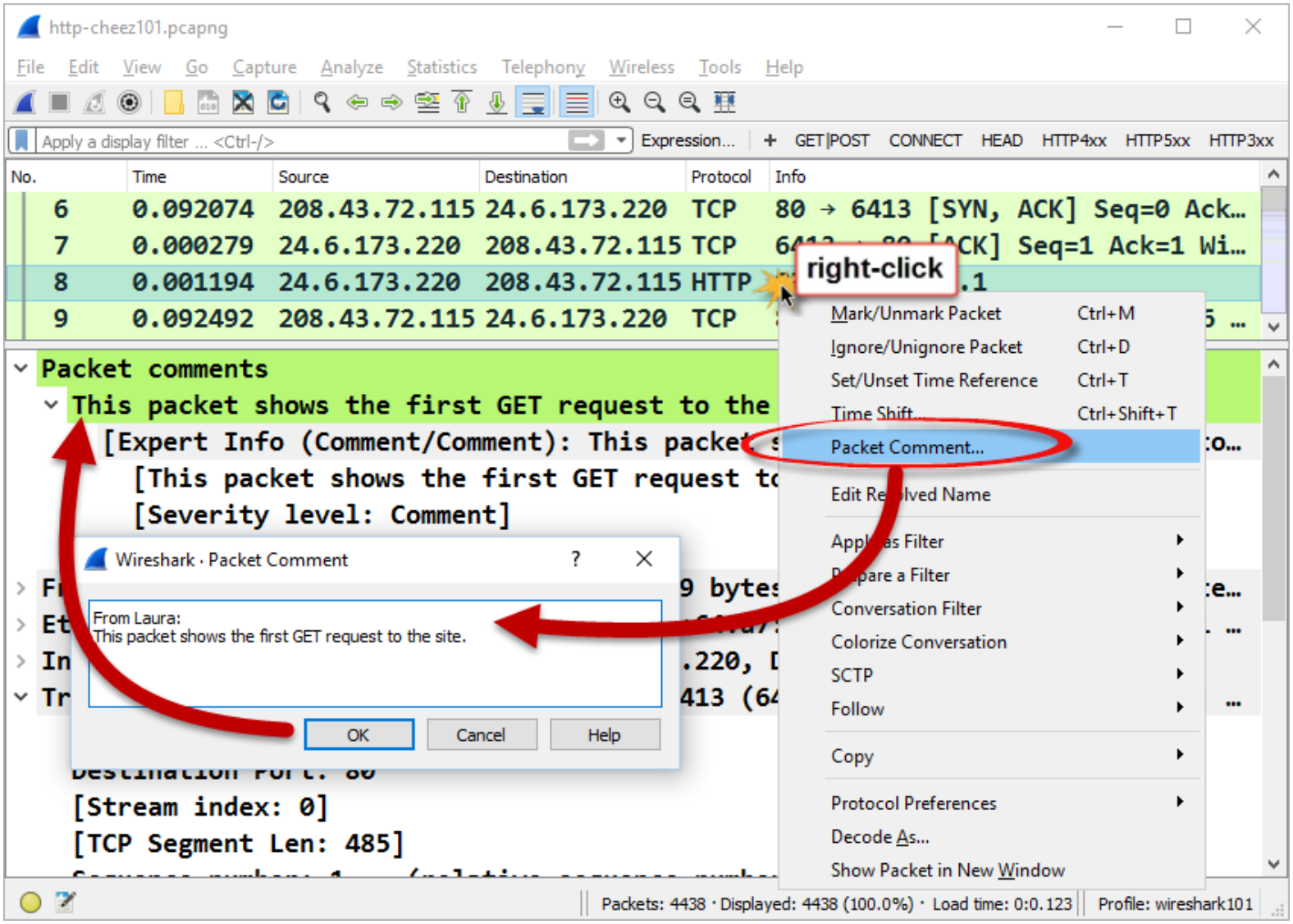


Add Your Comments to Trace Files

Only *.pcapng* file format supports comments.



Add Comments to Individual Packets



-suspicious101.pcapng

Export Packet Comments for a Report

sec-suspicious101.pcapng

File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help

pkt_comment | Expression... | + | GET|POST | CONNECT | HEAD | HTTP4xx | HTTP5xx | HTTP3xx

No.	Time	Source	Destination	Protocol	Comment
1	0.000000	24.6.173.220	74.125.224.84	HTTP	This is the original search query for the
5	0.062672	74.125.224.84	24.6.173.220	HTTP	In this response, the server sends numero
7	0.475050	24.6.173.220	74.125.224.84	HTTP	Now we clicked on the image load the expa
12	0.043454	74.125.224.84	24.6.173.220	HTTP	We get the expanded image through Google

```
Packet comments
  This is the original search query for the "Peter Lik for sale" images.
    [Expert Info (Comment/Comment): This is the original search query for the "Peter Li…
      [This is the original search query for the "Peter Lik for sale" images.]
      [Severity level: Comment]
      [Group: Comment]
Frame 1: 1097 bytes on wire (8776 bits), 1097 bytes captured (8776 bits) on interface 0
Ethernet II, Src: HewlettP_a7:bf:a3 (d4:85:64:a7:bf:a3), Dst: Cadant_31:bb:c1 (00:01:5c…
Internet Protocol Version 4, Src: 24.6.173.220, Dst: 74.125.224.84
Transmission Control Protocol, Src Port: 50263 (50263), Dst Port: 80 (80), Seq: 1, Ack:
```

Packets: 172 · Displayed: 19 (11.0%) · Load time: 0:0.6 | Profile: wireshark101

Quick Reference

Command-Line Tools Key Options

EDITCAP

`editcap -h`	View Editcap parameters.
`editcap -i 360 big.pcapng 360secs.pcapng`	Split *big.pcapng* into separate *360secs*.pcapng* files with up to 360 seconds of traffic in each file.
`editcap -c 500 big.pcapng 500pkts.pcapng`	Split *big.pcapng* into separate *500pkts*.pcapng* files with up to 500 packets in each file.

MERGECAP

`mergecap -h`	View Mergecap parameters.
`mergecap -w merged.pcapng files*.pcapng`	Merge *files*.pcapng* into a single file called *merged.pcapng* (merge based on packet timestamps).
`mergecap -a -w ab.pcapng a.pcapng b.pcapng`	Merge *a.pcapng* and *b.pcapng* into a single file called *ab.pcapng* (merge based on the order files are listed).

TSHARK

`tshark -h`	View Tshark parameters.
`tshark -D`	List the available capture interfaces that can be used with the –i parameter.
`tshark -i2 -f "tcp" -w tcp.pcapng`	Capture only TCP-based traffic on interface 2 and save it to tcp.pcapng.
`tshark -i1 -Y "ip.addr==10.2.1.1"`	Capture all traffic on interface 1, but only display traffic to or from 10.2.1.1.
`tshark -r "myfile.pcapng" -Y "http.host contains ".ru"" -w myfile-ru.pcapng`	Open a trace file called myfile.pcapng and apply a display filter for the value “.ru” in the HTTP host field – save the results to a file called myfile-ru.pcapng.

Split a Large Trace File into a File Set

- Use **`capinfos <filename>`** to obtain file information first.

Split based on packet count

- **`editcap -c 1000 a.pcapng a1000set.pcapng`**

Split based on time (seconds)

- **`editcap -i 360 b.pcapng b360set.pcapng`**

Merge Trace Files

List all Mergecap parameters

- `mergecap -h`

Use Wildcards when Merging

- `mergecap -w c.pcapng c30set*.*`

Capture Traffic at Command Line

Tshark Examples

- `tshark -h`
- `tshark -D`
- `tshark -c 100 -w 100.pcapng`

Command Prompt

```
D:\Traces101>tshark -r http-espn101.pcapng -Y "dns.flags.response==1"
 -w dns-espn-responsesonly.pcapng

D:\Traces101>dir dns-espn-responsesonly.pcapng
 Volume in drive D is MainDrive
 Volume Serial Number is 4EAF-C465

 Directory of D:\Traces101

01/11/2016  04:06 PM            18,212 dns-espn-responsesonly.pcapng
               1 File(s)         18,212 bytes
               0 Dir(s)  1,756,655,288,320 bytes free

D:\Traces101>_
```

Use Capture Filters during Command-Line Capture

Use the –f parameter

Command Prompt

```
D:\Traces101>dumpcap -i3 -f "tcp port 21" -w port21.pcapng
              Capturing on 'Wi-Fi'
File: port21.pcapng
Packets captured: 164
Packets received/dropped on interface 'Wi-Fi': 164/0 (pcap:0/dumpcap:0/
flushed:0/ps_ifdrop:0) (100.0%)

D:\Traces101>
```

Command Prompt

```
D:\Traces101>tshark -i3 -f "tcp port 21 and host 192.168.44.7"
 -w "myport21.pcapng"
Capturing on 'Wi-Fi'
293

D:\Traces101>
```

Use Display Filters during Command-Line Capture

Consider a two-step process if you want to capture, apply a display filter, and save the trace file

Command Prompt

```
D:\Traces101>tshark -i3 -f "tcp" -w tcptraffic.pcapng
Capturing on 'Wi-Fi'
496

D:\Traces101>
```

Command Prompt

```
D:\Traces101>tshark -r "tcptraffic.pcapng" -Y "tcp.analysis.flags"
-w tcpanalysisflags.pcapng

D:\Traces101>dir tcpanalysisflags.pcapng
 Volume in drive D is MainDrive
 Volume Serial Number is 4EAF-C465

 Directory of D:\Traces101

01/11/2016  04:44 PM             1,072 tcpanalysisflags.pcapng
               1 File(s)          1,072 bytes
               0 Dir(s)  1,756,563,681,280 bytes free

D:\Traces101>
```

Use Tshark to Export Specific Field Values and Statistics from a Trace File

-T fields -e <field name>

Command Prompt

```
D:\Traces101>tshark -i3 -f "dst port 80 and host 192.168.44.7" -T fields
-e frame.number -e ip.src -e ip.dst -e tcp.window_size
Capturing on 'Wi-Fi'
1       192.168.44.7    68.71.212.186   63620
2       192.168.44.7    23.59.197.231   261
3       192.168.44.7    23.216.11.9     251
4       192.168.44.7    23.216.11.9     256
5       192.168.44.7    68.71.222.248   63397
6       192.168.44.7    64.233.177.156  256
7       192.168.44.7    23.61.194.170   256
8       192.168.44.7    23.61.194.170   256
9       192.168.44.7    23.61.194.170   256
10      192.168.44.7    23.61.194.170   256
11      192.168.44.7    23.61.194.170   256
12      192.168.44.7    23.61.194.170   256
13      192.168.44.7    23.216.11.9     796
14      192.168.44.7    23.216.11.9     796
15      192.168.44.7    23.216.10.218   254
16      192.168.44.7    23.216.10.218   254
17      192.168.44.7    23.61.194.243   256
18      192.168.44.7    23.216.11.9     256
```

Continue Learning about Wireshark and Network Analysis

- Visit ***www.wiresharkbook.com*** (other Wireshark books and links to related tools).
- Visit ***www.wireshark.org*** to sign up for the Wireshark-Announce mailing list (new Wireshark version information).
- Sign up for the newsletter at ***www.chappellU.com*** to participate in free online Wireshark events.
- Practice capturing your own traffic.
- Continue customizing Wireshark by adding new profiles and new display filters, coloring rules, and Filter Expression buttons.
- Share your customized settings with other IT team members to create a master profile that improves your team's network analysis efficiency.

Course Conclusion

Filtering Slides

IPv4/IPv6 Capture Filters

`host 10.3.1.1`	Capture traffic to/from 10.3.1.1
`host 2406:da00:ff00::6b16:f02d`	Capture traffic to/from the IPv6 address 2406:da00:ff00::6b16:f02d
`not host 10.3.1.1`	Capture all traffic except traffic to/from 10.3.1.1
`src host 10.3.1.1`	Capture traffic from 10.3.1.1
`dst host 10.3.1.1`	Capture traffic to 10.3.1.1
`host 10.3.1.1 or host 10.3.1.2`	Capture traffic to/from 10.3.1.1 and any host it is communicating with and traffic to/from 10.3.1.2 and any host it is communicating with
`host www.espn.com`	Capture traffic to/from any IP address that resolves to www.espn.com (this will only work if the host name can be resolved by Wireshark prior to capture)

Subnet Capture Filters

`net 10.3.0.0/16`	Capture traffic to/from any host on network 10.3.0.0
`net 10.3.0.0 mask 255.255.0.0`	Same result as previous filter
`ip6 net 2406:da00:ff00::/64`	Capture traffic to/from any host on network 2406:da00:ff00:0000 (IPv6)
`not dst net 10.3.0.0/16`	Capture all traffic except traffic to an IP address starting with 10.3
`dst net 10.3.0.0/16`	Capture traffic to any IP address starting with 10.3
`src net 10.3.0.0/16`	Capture traffic from any IP address starting with 10.3
`net 10.3.0.0/16`	Capture traffic to/from any host on network 10.3.0.0

Broadcast and Multicast Capture Filters

`ip broadcast`	Capture traffic to 255.255.255.255
`ip multicast`	Capture traffic to 224.0.0.0 through 239.255.255.255 (also catches traffic to 255.255.255.255 unless you add and not ip broadcast)
`dst host ff02::1`	Capture traffic to the IPv6 multicast address for all hosts
`dst host ff02::2`	Capture traffic to the IPv6 multicast address for all routers

MAC Address Capture Filters

`ether host 00:08:15:00:08:15`	Capture traffic to or from 00:08:15:00:08:15
`ether src 02:0A:42:23:41:AC`	Capture traffic from 02:0A:42:23:41:AC
`ether dst 02:0A:42:23:41:AC`	Capture traffic to 02:0A:42:23:41:AC
`not ether host 00:08:15:00:08:15`	Capture traffic to or from any MAC address except for traffic to or from 00:08:15:00:08:15

Capture Traffic for a Specific Application

`port 53`	Capture UDP/TCP traffic to or from port 53 (typically DNS traffic)
`not port 53`	Capture all UDP/TCP traffic except traffic to or from port 53
`port 80`	Capture UDP/TCP traffic to or from port 80 (typically HTTP traffic)
`udp port 67`	Capture UDP traffic to or from port 67 (typically DHCP traffic)
`tcp dst port 21`	Capture TCP traffic to port 21 (typically the FTP command channel)
`portrange 1-80`	Capture UDP/TCP traffic to or from ports from 1 through 80
`tcp portrange 1-80`	Capture TCP traffic to or from ports from 1 through 80

Combine Port-Based Capture Filters

`port 20 or port 21`	Capture all UDP/TCP traffic to or from port 20 or port 21 (typically FTP data and command ports)
`host 10.3.1.1 and port 80`	Capture UDP/TCP traffic to or from port 80 that is being sent to or from 10.3.1.1
`host 10.3.1.1 and not port 80`	Capture UDP/TCP traffic to or from 10.3.1.1 except traffic to or from port 80
`udp src port 68 and udp dst port 67`	Capture all UDP traffic from port 68 to port 67 (typically traffic sent from a DHCP client to a DHCP server)
`udp src port 67 and udp dst port 68`	Capture all UDP traffic from port 67 to port 68 (typically traffic sent from a DHCP server to a DHCP client)
`port 20 or port 21`	Capture all UDP/TCP traffic to or from port 20 or port 21 (typically FTP data and command ports)
`host 10.3.1.1 and port 80`	Capture UDP/TCP traffic to or from port 80 that is being sent to or from 10.3.1.1

Capture Specific ICMP Traffic

`icmp`	Capture all ICMP packets.
`icmp[0]=8`	Capture all ICMP Type 8 (Echo Request) packets.
`icmp[0]=17`	Capture all ICMP Type 17 (Address Mask Request) packets.
`icmp[0]=8 or icmp[0]=0`	Capture all ICMP Type 8 (Echo Request) packets or ICMP Type 0 (Echo Reply) packets.
`icmp[0]=3 and not icmp[1]=4`	Capture all ICMP Type 3 (Destination Unreachable) packets except for ICMP Type 3/Code 4 (Fragmentation Needed and Don't Fragment was Set) packets.
`icmp`	Capture all ICMP packets.
`icmp[0]=8`	Capture all ICMP Type 8 (Echo Request) packets.

Apply Display Filters based on an IP Address, Range of Addresses, or Subnet

Address Filter Type	Filter Example
Single IPv4 Address	`ip.addr==10.3.1.1`
Single IPv6 Address	`ipv6.addr==2406:da00:ff00::6b16:f02d`
Host Name*	`ip.host==www.wireshark.org`
Range of Addresses	`ip.addr > 10.3.0.1 && ip.addr < 10.3.0.5`
Subnet (IPv4)	`ip.addr==10.3.0.0/16`
Subnet (IPv6)	`ipv6.addr >= fe80:: && ipv6.addr < fec0::`

* You must enable Wireshark's **Resolve network (IP) addresses** setting (**Edit | Preferences | Name Resolution**) in order to use this display filter.

Expand Display Filters with Multiple Include and Exclude Conditions (using Operators)

Operator	English	Example	Description
`&&`	`and`	`ip.src==10.2.2.2 && tcp.port==80`	View all IPv4 traffic from 10.2.2.2 that is to or from port 80
`||`	`or`	`tcp.port==80 || tcp.port==443`	View all TCP traffic to or from ports 80 or 443
`!`	`not`	`!arp`	View all traffic except ARP traffic
`!=`	`ne`	`tcp.flags.syn != 1`	View TCP frames that do not have the TCP SYN flag (synchronize sequence numbers) set to 1

Why Didn't my Filter Work?

Incorrect	`ip.addr != 10.2.2.2`	Display packets that do not have 10.2.2.2 in the IP source address field *or* IP destination address field.
Correct	`!ip.addr == 10.2.2.2`	Display packets that do not have 10.2.2.2 in the IP source address field and also does not have 10.2.2.2 in the destination address field.
Incorrect	`!tcp.flags.syn==1`	Display all packets that do not have a TCP SYN bit set to 1 (regardless of whether they are a TCP packet or not)
Correct	`tcp.flags.syn !=1`	This filter will only display TCP packets that contain a SYN set to 0.

Use Parentheses to Change Filter Meaning

```
(tcp.port==80 && ip.src==10.2.2.2) || tcp.flags.syn==1
```

OR

```
tcp.port==80 && (ip.src==10.2.2.2 || tcp.flags.syn==1)
```

OR

Determine Why Your Display Filter Area is Yellow

Yellow Background: This filter may not work as expected.

Green Background: The syntax is correct, but it doesn't ensure the logic is correct.

Red Background: This filter will not work – there is a syntax error.

p-clientside101.pcapng

Filter on a Keyword in a Trace File

Use `contains` for a general filter

Use `matches` for a Regex filter

ftp-clientside101.pcapng

File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help

Apply a display filter ... <Ctrl-/> Expression... +

No.	Time	Source	Destination	Protocol	Info
6	3.695004	192.168.0.101	10.251.30.69	FTP	Request: USER anonymous
7	0.095841	10.251.30.69	192.168.0.101	TCP	21 → 52912 [ACK] Seq=21 Ack=17…

```
> Frame 6: 70 bytes on wire (560 bits), 70 bytes captured (560 bits) on interface 0
> Ethernet II, Src: IntelCor_d0:27:d7 (00:18:de:d0:27:d7), Dst: D-LinkCo_cc:a3:ea (0…
> Internet Protocol Version 4, Src: 192.168.0.101, Dst: 10.251.30.69
> Transmission Control Protocol, Src Port: 52912 (52912), Dst Port: 21 (21), Seq: 1,…
v File Transfer Protocol (FTP)
  v USER anonymous\r\n
      Request command: USER
      Request arg: anonymous
```

Request arg (ftp.request.arg), 9 bytes | Packets: 5859 · Displayed: 5859 (100.0%) · Load time: 0:0.86 | Profile: wireshark101

```
ftp.request.arg contains "anonymous"
```

Using `matches` for Regex Filters

Consider case sensitivity

```
ftp.request.arg matches "anonymous"
ftp.request.arg matches "(?i)anonymous"
```

Consider variable characters

```
frame matches "building[Aa]eng"
frame matches "building[AaBb]eng"
frame matches "(?i)(cat|dog)"
```

p-crack101.pcapng

Use Wildcards in Display Filters

```
ftp.request.arg matches "me.r"
```

"." indicates any character except a carriage return or line feed

```
ftp.request.arg matches "me..r"
```

Now we're looking for any two characters between `me` and `r`

```
ftp.request.arg matches "me.{1,3}r"
```

{#,#} indicates minimum and maximum number of repeating characters

Challenge Slides

Section 0 Challenge

Open challenge101-0.pcapng and use the techniques covered in this Section to answer these Challenge questions. The answer key is located in Appendix A.

We will focus on what you can learn about communications based on the main Wireshark view.

Question 0-1.	How many packets are in this trace file?
Question 0-2.	What IP hosts are making a TCP connection in frames 1, 2, and 3?
Question 0-3.	What HTTP command is sent in frame 4?
Question 0-4.	What is the length of the largest frame in this trace file?
Question 0-5.	What protocols are seen in the **Protocol** column?
Question 0-6.	What responses are sent by the HTTP server?
Question 0-7.	Is there any IPv6 traffic in this trace file?

Section 1 Challenge

Open challenge101-1.pcapng and use the techniques covered in this Section to answer these Challenge questions. The answer key is located in Appendix A.

Important: This trace file includes an HTTP communication running over a non-standard port number. Before you can answer these questions, you must force Wireshark to dissect this traffic as HTTP.

Question 1-1. In which frame number does the client request the default web page ("/")?

Question 1-2. What response code does the server send in frame 17?

Question 1-3. What is the largest TCP delta value seen in this trace file?

Question 1-4. How many SYN packets arrived after at least a 1 second delay?

Section 2 Challenge

This challenge requires access to the Internet. You will capture traffic to a web site and analyze your findings. The answer key is located in Appendix A.

First, configure Wireshark to capture only traffic to and from your MAC address and port 80, and save the traffic to a file named mybrowse.pcapng. Then ping and browse to www.chappellU.com. Stop the capture and examine the trace file contents.

Question 2-1. Did you capture any ICMP traffic?

Question 2-2. What protocols are listed for your browsing session to www.chappellU.com?

Now configure Wireshark to capture all your ICMP traffic, and save your traffic to a file called myicmp.pcapng. Again, ping and browse to www.chappellU.com. Stop the capture and examine the trace file contents.

Question 2-3. How many ICMP packets did you capture?

Question 2-4. What ICMP Type and Code numbers are listed in your trace file?

Section 3 Challenge

Open *challenge101-3.pcapng* and use your display filter and coloring rule skills to locate traffic based on addresses, protocols and keywords to answer these Challenge questions.

You will practice your display filter to locate traffic based on addresses, protocols, and keywords.

Question 3-1. How many frames travel to or from 80.78.246.209?

Question 3-2. How many DNS packets are in this trace file?

Question 3-3. How many frames have the TCP SYN bit set to 1?

Question 3-4. How many frames contain the string “set-cookie” in upper case or lower case?

Question 3-5. How many frames contain a TCP delta time greater than 1 second?

Section 4 Challenge

Open *challenge101-4.pcapng* and use your packet coloring and export skills in this Section to answer these Challenge questions.

Question 4-1. What coloring rule does frame 170 match?

Question 4-2. Temporarily color TCP stream 5 with a light blue background and apply a filter on this traffic. How many packets match your filter?

Question 4-3. Create and apply a coloring rule for TCP delta delays greater than 100 seconds. How many frames match this coloring rule?

Question 4-4. Export this filtered TCP delta information in CSV format. Using a spreadsheet program, what is the average TCP delta time?

Section 5 Challenge

Open *challenge101-5.pcapng* and use the techniques covered in this Section to answer these Challenge questions.

Question 5-1. Create an IO Graph for this trace file. What is the highest packets-per-second value seen in this trace file?

Question 5-2. What is the highest bits-per-second value seen in this trace file?

Question 5-3. How many TCP conversations are in this trace file?

Question 5-4. How many times has “Previous segment not captured” been detected in this trace file?

Question 5-5. How many retransmissions and fast retransmissions are seen in this trace file?

Section 6 Challenge

Open *challenge101-6.pcapng* and use the techniques covered in this Section to answer these Challenge questions. The answer key is located in Appendix A.

Question 6-1.	What two .jpg files can be exported from this trace file?
Question 6-2.	On what HTTP server and in what directory does next-active.png reside?
Question 6-3.	Export *booksmall.png* from this trace file. What is in the image?
Question 6-4.	Reassemble TCP stream 7. What type of browser is the client using in this stream?

Section 7 Challenge

Open *challenge101-7.pcapng* and use the techniques covered in this Section to answer these Challenge questions. The answer key is located in Appendix A.

Question 7-1. What information is contained in the trace file annotation?

Question 7-2. What packet comments are contained in this trace file?

Question 7-3. Add a comment to the POST message in this trace file. What packet did you alter?

Section 8 Challenge

Use *challenge101-8.pcapng* and the command-line tool techniques covered in this Section to answer these Challenge questions. The answer key is located in Appendix A.

Question 8-1. What Tshark parameter should you use to list active interfaces on your Wireshark system?

Question 8-2. Using Tshark to extract protocol hierarchy information, how many UDP frames are in *challenge101-8.pcapng*?

Question 8-3. Use Tshark to export all DNS packets from *challenge101-8.pcapng* to a new trace file called *ch8dns.pcapng*. How many packets were exported?

Lab Slides

Starting at Lab 4

Lab 4

http-disney101.pcapng

Add the HTTP Host Field as a Column

During a browsing session, an HTTP client sends requests for HTTP objects to one or more HTTP servers. In each of the requests, the client specifies the name or the IP address of the target HTTP server. This can be very revealing.

Note: All frames from 24.6.173.220 will appear with a black background and red foreground if Wireshark is set to validate IP header checksums. You will disable this feature in Lab 6.

Lab 5

http-pcaprnet101.pcapng

Set Key Wireshark Preferences (IMPORTANT LAB)

Wireshark offers several key preference settings to enhance your analysis sessions. In this lab you will use the Edit Preferences button on the main toolbar and the right-click method to view and change the preference settings.

These are the settings we will view and alter in this lab:

- Increase the number of display filters that Wireshark remembers.
- Increase the number of recently opened files that Wireshark remembers.
- Ensure IP, UDP, and TCP checksum validations are disabled.
- Enable the TCP *Calculate conversation timestamps* setting.
- Enable the TCP *Track number of bytes in flight* setting.
- Disable the TCP *Allow subdissector to reassemble* TCP streams setting.

Lab 6

Create a New Profile Based on the Default Profile

Profiles enable you to work with customized settings to be more efficient when analyzing traffic.

In this lab you will create a new profile called "**wireshark101**."

You will base it on your Default profile to ensure any previously created settings will be copied over to your new profile.

Lab 7

httpdnsprofile2.zip
and
dns-nmap101.pcapng

Import a DNS/HTTP Errors Profile

Once you've created that fabulous profile that detects various types of HTTP or DNS problems perhaps, consider installing that profile on your other Wireshark systems.

Since Wireshark bases profiles on text files, this is a simple process.

Lab 8

http-slow101.pcapng

Spot Path and Server Latency Problems

Let's practice using these two columns to detect latency.

In this lab you will set the Time column to **Seconds Since Previous Displayed Packet** and add the **TCP Delta** column.

You may have some of these columns set already if you followed along with the previous section in your Student Manual.

Lab 9

Capture to File Sets

In this lab you will get a chance to practice capturing to file sets using an auto-stop condition.

Lab 10

Use a Ring Buffer to Conserve Drive Space

In this lab exercise, we will set up a ring buffer to ensure we see the most recent traffic.

We will create a problem and manually stop the capture to analyze the issue.

Lab 11

Capture Only Traffic to or from Your IP Address

In this lab you will determine your current IP address and apply a capture filter for that traffic.

Lab 12

Capture Only Traffic to or from Everyone Else's MAC Address

In this lab you will determine your current MAC address and apply a capture filter that filters out your traffic—you are interested in everyone else's traffic only.

If you have a dual-stack host, it is much more effective to make a single filter based on your MAC address than to make a more complex filter based on your IPv4 and IPv6 addresses.

Lab 13

Create, Save and Apply a DNS Capture Filter

In this exercise you will use several skills learned in this Section. You will configure Wireshark to capture only DNS traffic and save that traffic to a file called **mydns101.pcapng**.

Lab 14

http-sfgate101.pcapng

Use Auto-Complete to Find Traffic to a Specific HTTP Server

In this lab we use Wireshark's auto-complete feature to filter on specific HTTP communications.

Ultimately, we are interested in client requests to a particular server. This trace file, *http-sfgate101.pcapng*, was captured as someone browsed a web site and then filled in a feedback form on that site asking about iPad support.

Lab 15

Use a Default Filter as a "Seed" for a New Filter

You can use the default display filters as a template to create and save new custom display filters.

This method helps you remember the display filter syntax and ensures that the syntax is correct. We will create a display filter for all traffic to or from your IP address.

Lab 16

http-disney101.pcapng

Filter on HTTP Traffic the Right Way

This is a quick lab.

We will just compare the results from applying two different display filters to the traffic.

We will use `http` and then we will replace it with the proper filter for this web browsing traffic.

Lab 17

mybackground101.pcapng

Filter on Traffic to or from Online Backup Subnets

In this lab, we will apply a subnet display filter to examine traffic to or from a backup server for Memeo which offers an online backup product.

This traffic runs in the background, constantly checking in with the server.

Lab 18

http-errors101.pcapng

Filter on DNS Name Errors or HTTP 404 Responses

In this lab we will look for specific DNS or HTTP error responses using the right-click method.

This is a great filter that you may want to save.

Lab 19

gen-startupchatty101.pcapng

Detect Background File Transfers on Startup

There may be a number of background processes that run when you start up your machine.

Some of these may update your virus detection mechanism, your operating system, or applications.

In this lab, you will detect and filter on the most active conversation of a host that is just starting up.

Lab 20

general101b.pcapng

Locate TCP Connection Attempts to a Client

Client processes send TCP connection requests to server processes. There are very few reasons to allow incoming TCP connections to user machines on your network (as they typically won't be running server processes).

In this lab we will create a display filter that detects incoming TCP connection attempts to anyone on a particular subnet.

We will focus on subnet 24.6.0.0/16.

Lab 21

http-pictures101.pcapng

Filter to Locate a Set of Key Words in a Trace File

In this lab we will use the matches operator to find the keywords *sombrero* or *football* in upper case or lower case anywhere in a trace file.

Lab 22

http-pictures101.pcapng

Filter with Wildcards between Words

In this lab we will use the matches operator to find the keywords baby and smiling in a trace file. We will see how the repeating character option settings can affect what matches your filter.

Our display filter **`ftp.request.arg matches "me.{1,3}r"`** would look for the "." up to three times between the "**`me`**" and "**`r`**" as mentioned in this section.

This time we will look for the keywords *baby* and *smiling* with up to three characters separating the words.

Lab 23

dfilters_sample.txt

Import Display Filters into a Profile

In this lab you will import a set of display filters from your student USB stick (or the *wiresharkbook.com* website) into your existing display filter file (*dfilters*).

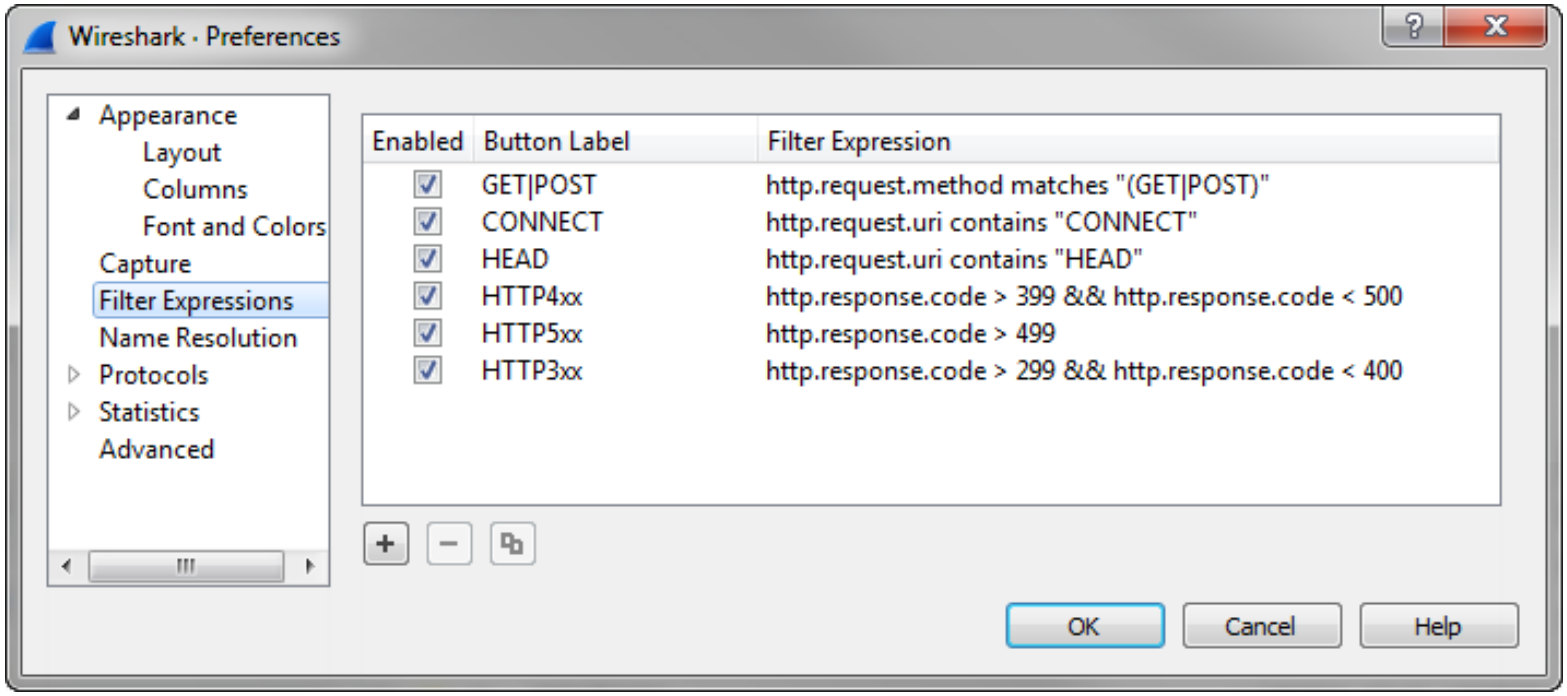
Use this same technique if you want to move display filters from one profile to another on a single host or other Wireshark systems.

Lab 24

http-chappellu101b.pcapng and *filterexpressions101.txt*

Create and Import HTTP Filter Expression Buttons

We will begin by creating a single Filter Expression button and then we'll import the set of Filter Expression buttons shown below into your *wireshark101* profile.



Lab 25

http-sfgate101.pcapng

Add a Column to Display Coloring Rules in Use

Adding a column to identify coloring rules is a great idea when you are new to Wireshark or you just aren't familiar with the coloring rules set.

Lab 26

ftp-crack101.pcapng

Build a Coloring Rule to Highlight FTP User Names, Passwords, etc.

In this lab you will create a coloring rule to call your attention to FTP request arguments, including those associated with USER, PASS, TYPE, SIZE, MDTM, RETR, and CWD commands.

Lab 27

http-browse101d.pcapng

Create Temporary Conversation Coloring Rules

In this lab, you will apply three temporary coloring rules to differentiate TCP conversations. When you scroll through the trace file, you will be able to easily see when an earlier conversation begins to surface.

Lab 28

net-lost-route.pcapng

Create Temporary Conversation Coloring Rules

In this lab we will create a new coloring rule to identify TCP retransmissions. TCP retransmissions are a sign of packet loss on a network and are part of Wireshark's TCP analysis flagged packets. We'd like to just look at the Intelligent Scrollbar to know if retransmissions (packet loss indications) are seen.

Lab 29

http-misctraffic101.pcapng

Export a Single TCP Conversation

When you are focused on a specific application or a specific file download, it helps to extract conversations into separate trace files. In this lab, you will create and extract a new trace file after locating traffic from an executable file download process.

Lab 30

http-au101b.pcapng

Export a List of HTTP Host Field Values from a Trace File

In this lab, you will alter the Packet List pane to display the HTTP Host field before exporting information to CSV format.

Lab 31

http-misctraffic101.pcapng

Filter on the Most Active TCP Conversation

Pulling out the most active conversation is a common network analysis task when trace files contain tens or even hundreds of conversations.

Lab 33

http-browse101c.pcapng

Set up GeoIP to Map Targets Globally

Wireshark can use the MaxMind GeoLite database files to list the country, city, AS (Autonomous System) number, latitude, and longitude of an IP address and map IPv4 and IPv6 addresses on a map of the earth. In this lab, you will configure Wireshark to use this database and map IP addresses seen in a trace file.

Lab 34

general101c.pcapng

Detect Suspicious Protocols or Applications

When you are concerned that there may be a security issue in your trace file, open the Protocol Hierarchy window first.

Look for suspicious applications or protocols and the dreaded “data” under IP, UDP, or TCP.

Lab 35

http-espn101.pcapng

Compare Traffic to/from a Subnet to Other Traffic

In this lab you will compare all the traffic to or from subnet 184.0.0.0/8 to all other traffic. To do this, you will use two IP address filters—one inclusion filter and one exclusion filter.

Lab 35

http-download101.pcapng

Identify an Overloaded Client

In this lab we use the Expert Infos window to identify the cause of poor network performance. Not only is the client overloaded in this trace file, but there is packet loss along the path as well.

Lab 36

general101d.pcapng

Detect and Graph File Transfer Problems

In this lab we examine a file transfer process that takes place over TCP. Before we can consider troubleshooting the application itself, we must rule out TCP problems.

Lab 37

http-wiresharkdownload101.pcapng

Use Reassembly to Find a Web Site's Hidden HTTP Message

It is not unusual to have numerous "hidden" messages sent to your browser when you hit a web site. In this lab you will analyze a trace file that contains two hidden messages. Afterwards, visit the same web site again to catch other interesting messages.

Lab 38

ftp-clientside101.pcapng

Extract a File from an FTP File Transfer

In this lab you will follow an FTP data stream to reassemble the file that was transferred.

First you will reassemble the command channel traffic to see the client login and file retrieval commands, and then you will reassemble the data transfer channel traffic to view the file transferred.

Lab 39

http-college101.pcapng

Carve Out an HTTP Object from a Web Browsing Session

In this lab, you will open a trace file that contains a web browsing session.

Using the **File | Export Objects** process, you will extract one of the images transferred during the web browsing session.

Lab 40

sec-suspicous101.pcapng

Read Analysis Notes in a Malicious Redirection Trace File

It can be a blessing to have notes inside the trace file to assist other analysts (or even you) in following along with the traffic flow.

In this lab you will examine the notes left in a trace file that contains unusual communications.

Lab 41

sec-suspicous101.pcapng

Export Malicious Redirection Packet Comments

We will use the *sec-suspicious101.pcapng* trace file again in this lab. We will use a two-step process for comment export.

First we will prepare the trace file to export the field information we are most interested in. We will export the fields in text format.

Unlike in the previous section, we will export the packet comments using the Packet summary line.

Lab 42

http download101c.pcapng

Split a File and Work with Filtered File Sets

You will be working with *http-download101c.pcapng* in this lab. This trace file is only 27 MB, but we will use it to practice splitting a file.

After splitting the file, we will move through the file set while a display filter is applied.

Wireshark automatically applies the display filter to each file as it is opened.

Lab 43

http-downloadc5000*.pcapng

Merge a Set of Files using a Wildcard

In this lab you will merge the six-file *http-downloadc5000*.pcapng* set that you created in Lab 42.

You will use a wildcard to make this process a bit easier and less error-prone.

Lab 44

Use Tshark to Capture to File Sets with an Autostop Condition

In this lab, you will get a chance to use Tshark with various parameters. We'll define file set "next file" parameters and include an autostop condition for unattended capture.

Lab 45

http-espn101.pcapng

Use Tshark to Extract HTTP GET Requests

In this lab you will use the **`-r`** parameter to read a trace file and then apply a display filter with the **`-R`** parameter.

Finally you will save a trace file that contains only the HTTP GET requests.

Lab 46

Use Tshark to Extract HTTP Host Names and IP Addresses

In this lab we will use a combination of display filters and field names to create a file that contains both the IP addresses and host names of HTTP servers contacted on the network.