



#sf21veu

Know your preferences



Uli Heilmeier
Syskron GmbH



#sf21veu

Hello!

*I am **Uli Heilmeyer***

I am here because I love packets.

You can find me at **@pizza_4u**



#sf21veu



#sf21veu

Runtime / Argument

-o preference_name:value

Profile specific

\$HOME/.wireshark/profiles/<profile_name>/preferences

Personal specific

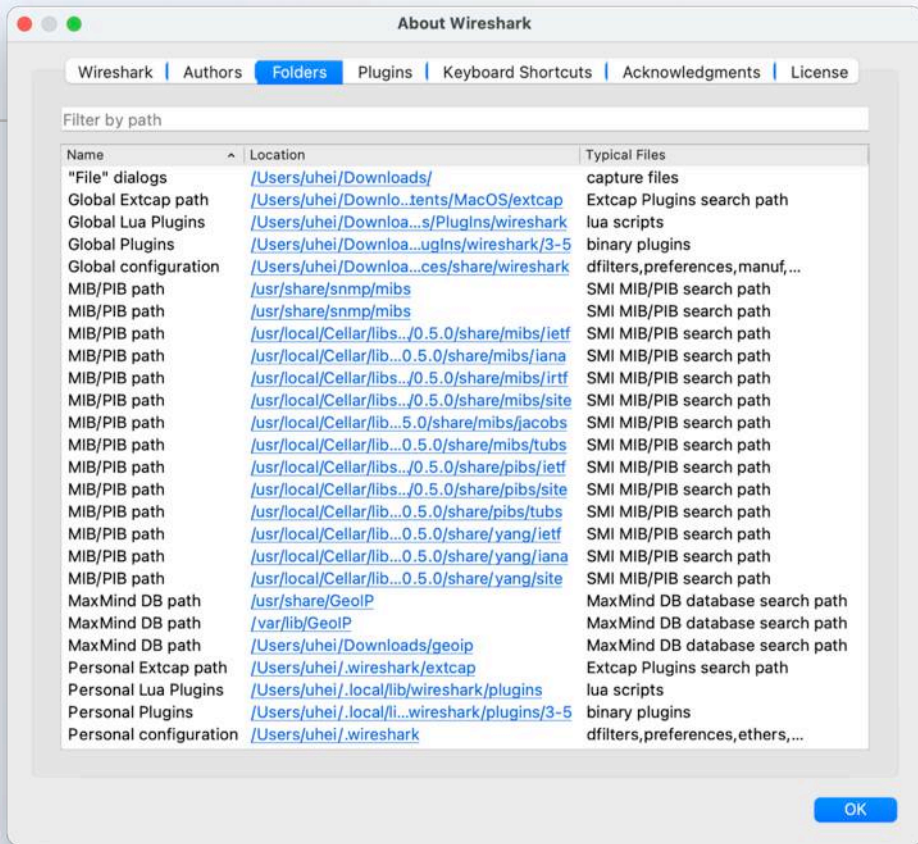
\$HOME/.wireshark/preferences

Global

APPDIR/Contents/Resources/share/wireshark/preferences



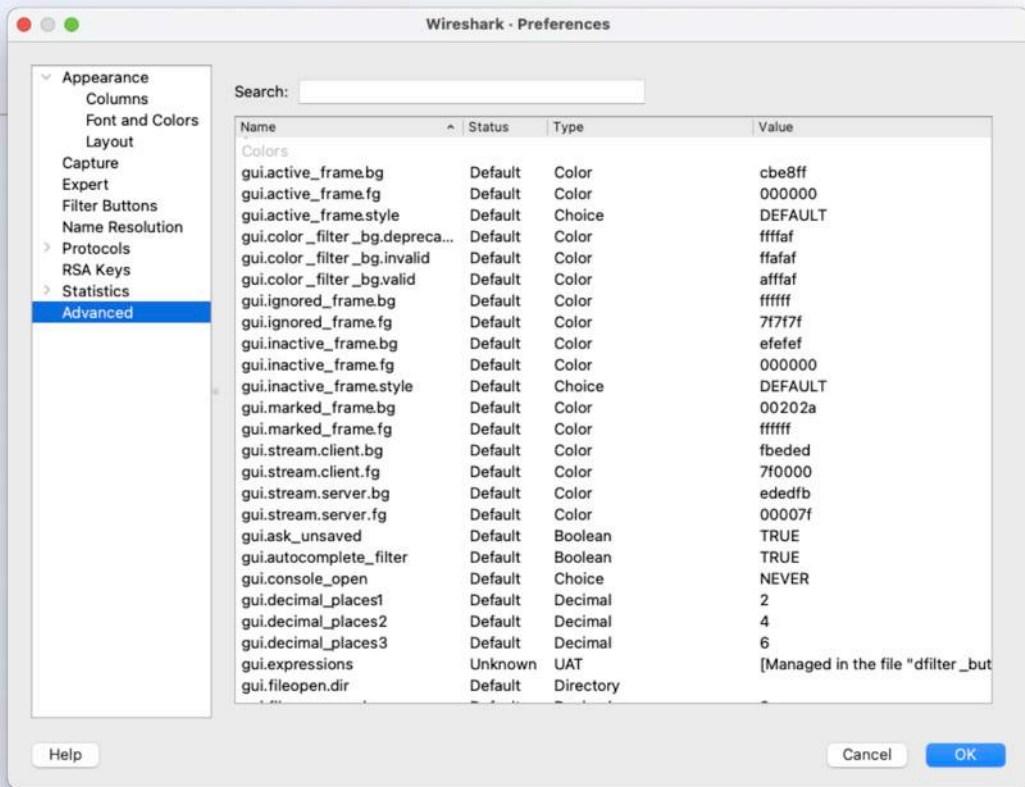
#sf21veu



./tshark -G folders



#sf21veu



```
./tshark -G currentprefs
```

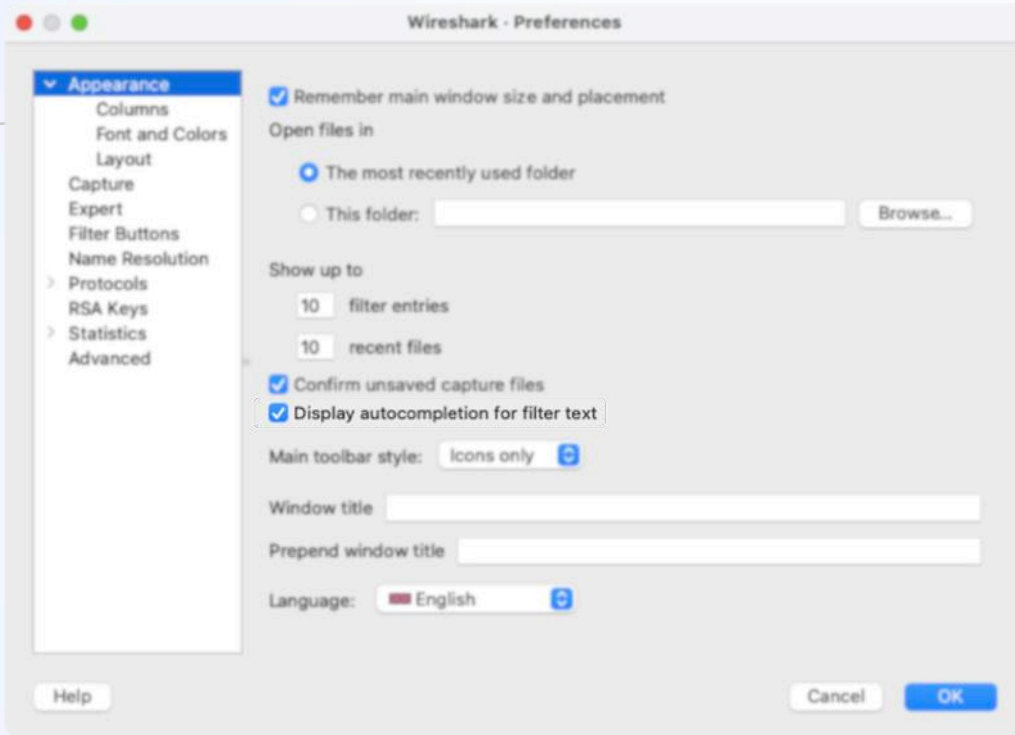
```
./tshark -G defaultprefs
```



#sf21veu



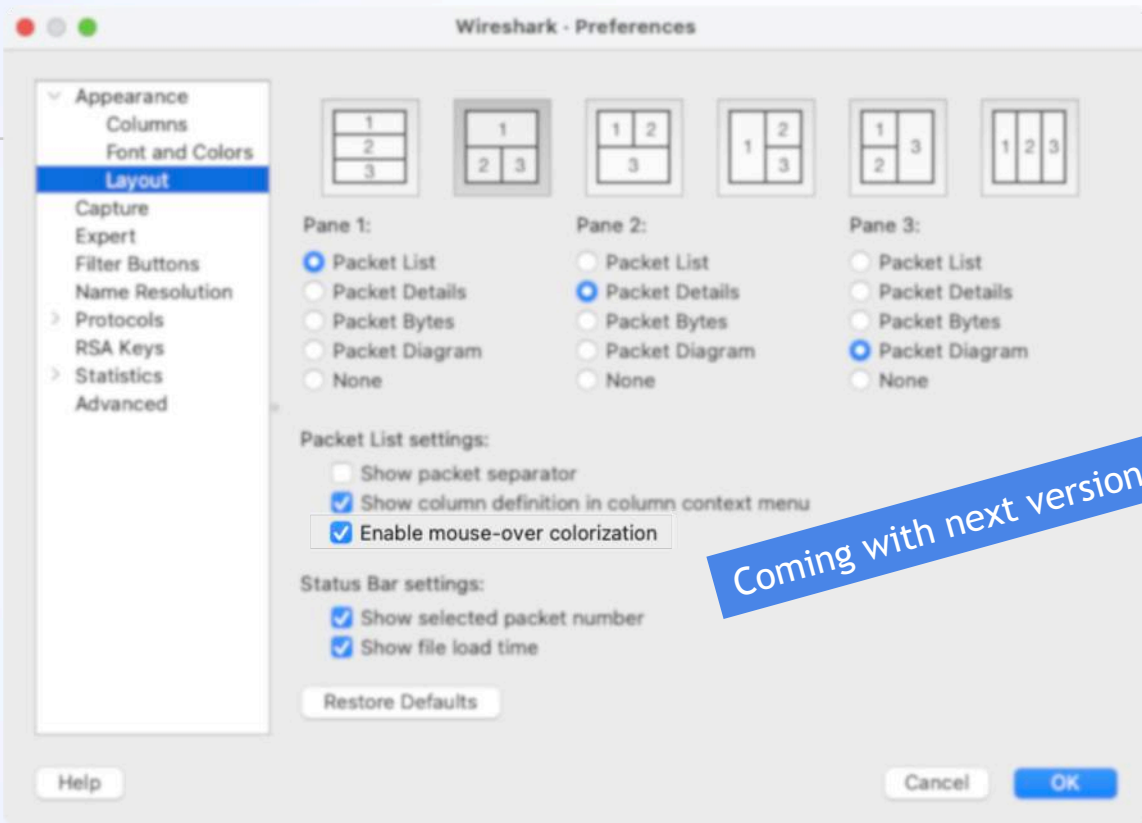
#sf21veu



`gui.autocomplete_filter`



#sf21veu



`gui.packet_list_hover_style.enable`



#sf21veu

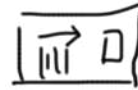
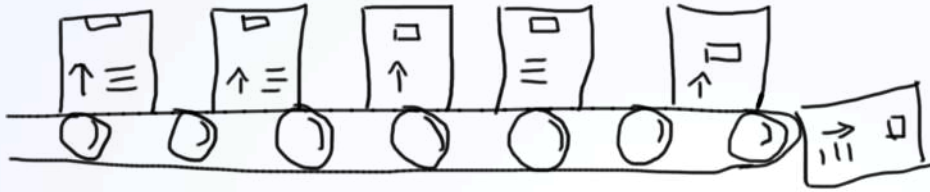
The image shows the Wireshark Preferences dialog box in the foreground, with the packet details pane visible in the background. The Preferences dialog is set to the 'Layout' tab. It features three panes (Pane 1, Pane 2, and Pane 3) where 'Packet Diagram' is selected for all. Under 'Packet List settings', 'Show column definition in column context menu' and 'Enable mouse-over colorization' are checked. Under 'Status Bar settings', 'Show selected packet number' and 'Show file load time' are checked. The background shows a packet list with several entries, and the packet details pane for 'Selected Packet: 7' showing Ethernet II and Internet Protocol Version 6 fields.

0	15	16	31
Destination			
Source			
Type			

0	15	16	31
Version	Traffic Class	Flow Label	
Payload Length		Next Header	Hop Limit
Source Address			
Destination Address			

`gui.layout_content_[123]`

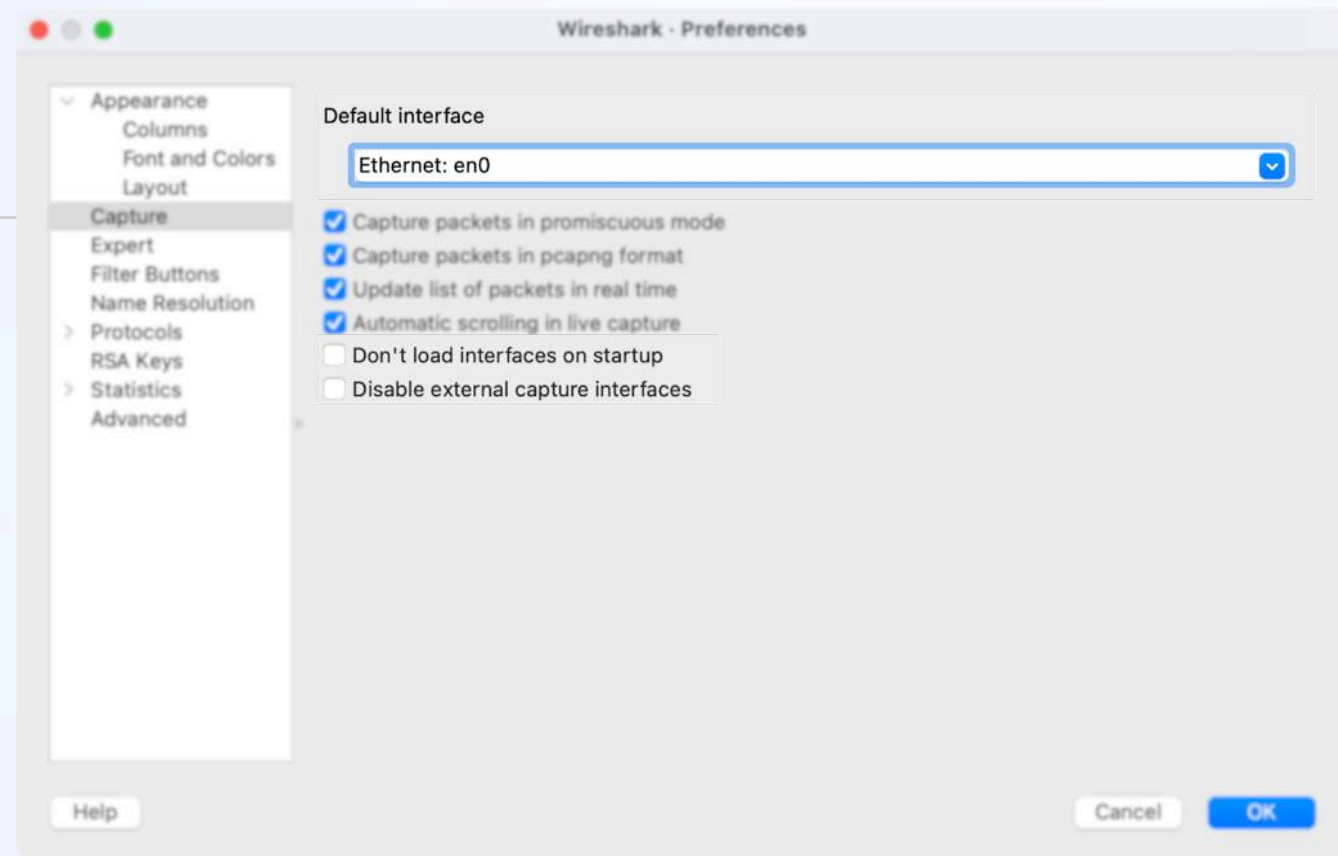
`gui.show_selected_packet.enabled`



#sf21veu



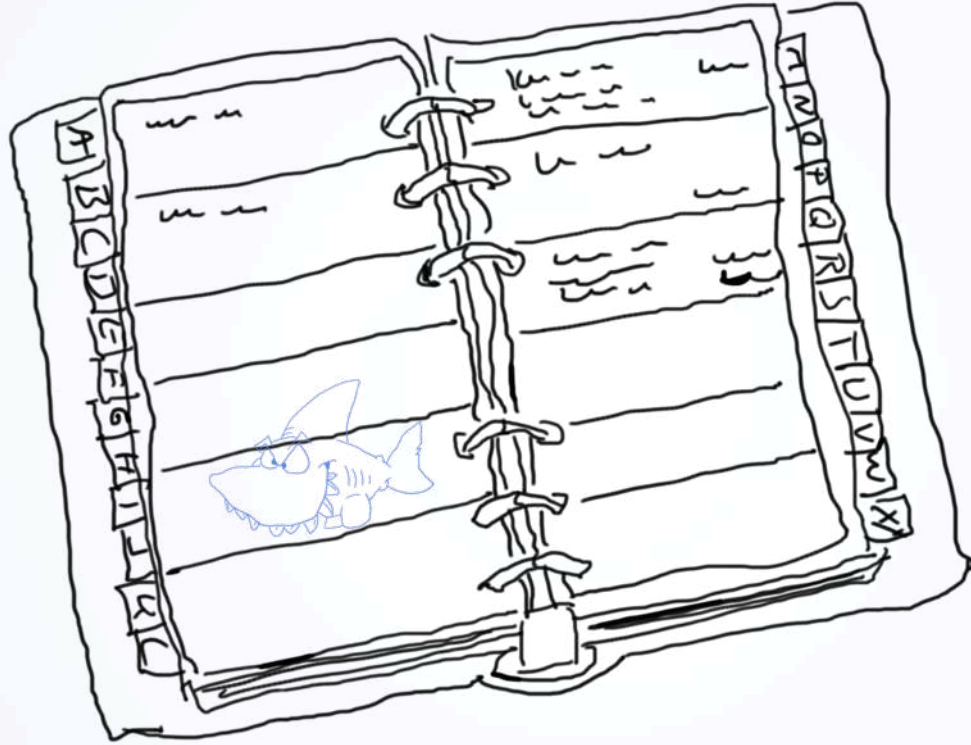
#sf21veu



`capture.device`

`capture.no_extcap`

`capture.no_interface_load`



#sf21veu



#sf21veu

Files:

hosts

addr_resolve_dns_servers

vlangs

smi_paths

smi_modules

maxmind_db_paths

Wireshark · Preferences

Appearance

Columns

Font and Colors

Layout

Capture

Expert

Filter Buttons

Name Resolution

Protocols

RSA Keys

Statistics

Advanced

Name Resolution

Resolve MAC addresses

Resolve transport names

Resolve network (IP) addresses

Use captured DNS packet data for address resolution

Use an external network name resolver

Use custom list of DNS servers for name resolution

DNS Servers

Maximum concurrent requests

Only use the profile "hosts" file

Resolve VLAN IDs

Resolve SS7 PCs

Enable OID resolution

Suppress SMI errors

SMI (MIB and PIB) paths

SMI (MIB and PIB) modules

MaxMind database directories


Help

Cancel

OK



#sf21veu



```
namerres.dns_pkt_addr_resolution  
nameres.use_external_name_resolver  
nameres.use_custom_dns_servers  
nameres.vlan_name  
nameres.load_smi_modules
```




#sf21veu

Advanced stuff



#sf21veu



`gui.restore_filter_after_following_stream`
`gui.max_export_objects`



#sf21veu

SNMP

SMTP

HTTP

IPv6

Radius

MQTT

TCP

TLS

Dissectors

DTLS

openSsh

DNS

DHCP

Data

Kerberos

Ethernet

IMF

IP

SIP



#sf21veu



Generic stuff

Enable/Disable Protocols

Decode as

Default Port



#sf21veu



HTTP

Reassemble HTTP headers/bodies spanning multiple TCP segments

Uncompress entity bodies

Custom HTTP header fields

SIP is quite similar



#sf21veu



TCP

Allow subdissector to reassemble TCP streams

Analyze TCP sequence numbers

Relative sequence numbers

Scaling factor to use when not available from capture



#sf21veu



MQTT

Show message as text

Message decoding



#sf21veu



IP v4/v6

Enable IPv4/IPv6 geolocation

Reassemble fragmented IPv4/IPv6 datagrams



#sf21veu



IMF / SMTP

Custom IMF header

Reassemble SMTP commands and response lines spanning multiple TCP segments

Reassemble SMTP DATA command spanning multiple TCP segments

Decode Base64 encoded AUTH parameters



#sf21veu



TLS / DTLS

<https://lekensteyn.nl/files/wireshark-tls-debugging-sharkfest19eu.pdf>

<https://lekensteyn.nl/files/wireshark-ssl-tls-decryption-secrets-sharkfest18eu.pdf>

<https://sharkfesteurope.wireshark.org/assets/presentations16eu/07.pdf>



#sf21veu



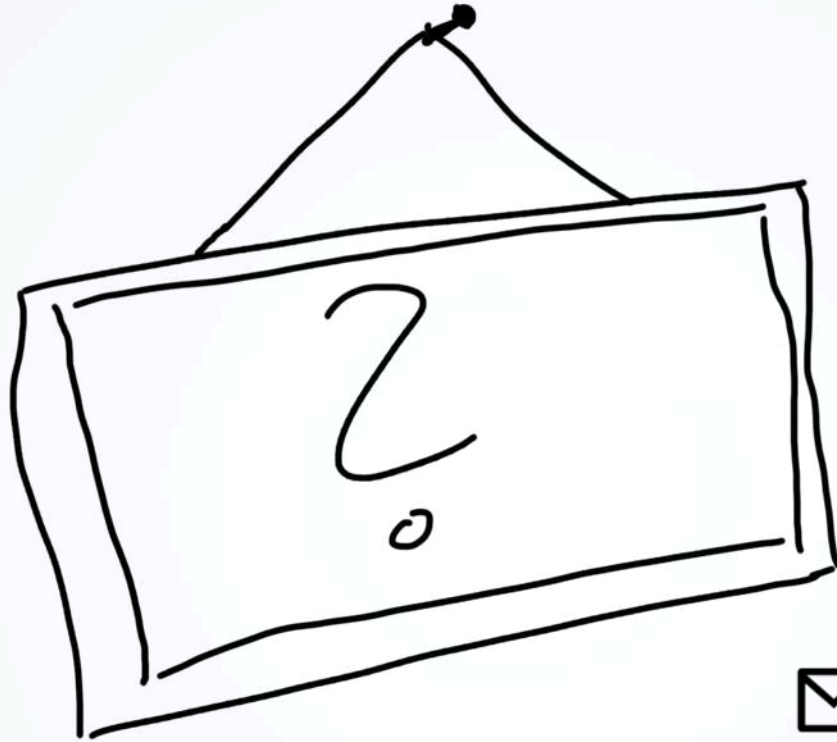
Feedback

<https://forms.gle/GGRAzkJcEuDkx5r36>





#sf21veu



✉ uh@heilmeier.eu

🐦 [@pizza_4u](https://twitter.com/pizza_4u)

🗨️ [@uhei@chaos.social](https://chaos.social/@uhei)



#sf21veu



Kerberos v5 / Radius / SNMP

Decrypt (Keytab / Shared Secret / Users Table)

OID Resolving (s. Name resolving)



#sf21veu



Data

Try to uncompress zlib compressed data

Show data as text

Generate MD5 hash



#sf21veu



DHCP

Endianness of UUID

Custom DHCP/BootP Options



#sf21veu

Expert Severity



#sf21veu

mqtt-json.pcapng — FooBar

Apply a display filter ...<?>

Time	dTime	Time delta from previous display
1 16:28:56...	0.000	0.0
2 16:28:56...	0.000	0.0
3 16:28:56...	0.018	0.0
4 16:28:56...	0.001	0.0
5 16:28:56...	0.000	0.0
6 16:28:56...	1.500	1.5

000. = Reserved: Not set
...0 = Nonce: Not set
... 0... = Congestion Window
... .0.. = ECN-Echo: Not set
... ..0. = Urgent: Not set
... ...1 = Acknowledgment: Set
... 0... = Push: Not set
... ..0.. = Reset: Not set
...0. = Syn: Not set
... ..1 = Fin: Set

[Expert Info (Chat/Sequence): Connection finish (FIN)]
[Severity level: Chat]
[Group: Sequence]

[TCP Flags:A...F]

[Expert Info (Error/Sequence): This frame undergoes the connection reset]
[Severity level: Error]
[Group: Sequence]

Window: 506
[Calculated window size: 506]
[Window size scaling factor: -1 (unknown)]

Expert Info (_ws.expert)

Selected Packet: 4 · Packets: 20 · Displayed: 20 (100.0%) · Load time: 0:0.9 · Profile: Default

Wireshark · Preferences

- Appearance
 - Columns
 - Font and Colors
 - Layout
- Capture
- Expert
- Filter Buttons
- Name Resolution
- Protocols
 - RSA Keys
 - Statistics
 - Advanced

Field name	Severity
tcp.connection.fin_passive	Error

+ - [] ^ v [] Copy from /Users/uhei/wireshark/expert_severity

Help Cancel OK

File: expert_severity



#sf21veu

The screenshot shows the Wireshark interface with a packet capture list on the left and a packet details pane on the right. A 'Wireshark - Preferences' dialog box is open in the foreground, showing the 'Appearance' section. The 'Columns' list is expanded, and the following columns are checked:

- dTime
- Time delta from previous displayed frame

The 'Time delta from previous displayed frame' column is set to 'Custom' with the value 'frametime_delta_displayed' and '0'.

The packet capture list shows the following data:

No.	Time	Source	Destination	Protocol	Info
6	0.000	0.000000000	0.000000000	0.000000000	0.000000000
7	0.000	0.000300000	0.000300000	0.000300000	0.000300000
5	0.018	0.018673000	0.018673000	0.018673000	0.018673000
7	0.001	0.001862000	0.001862000	0.001862000	0.001862000
7	0.000	0.000078000	0.000078000	0.000078000	0.000078000