#sf21veu

Know your preferences

Uli Heilmeier
Syskron GmbH

Hello!

I am Uli Heilmeier

I am here because I love packets.

You can find me at @pizza_4u

#sf21veu

Runtime / Argument

`-o preference_name:value`

Profile specific

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

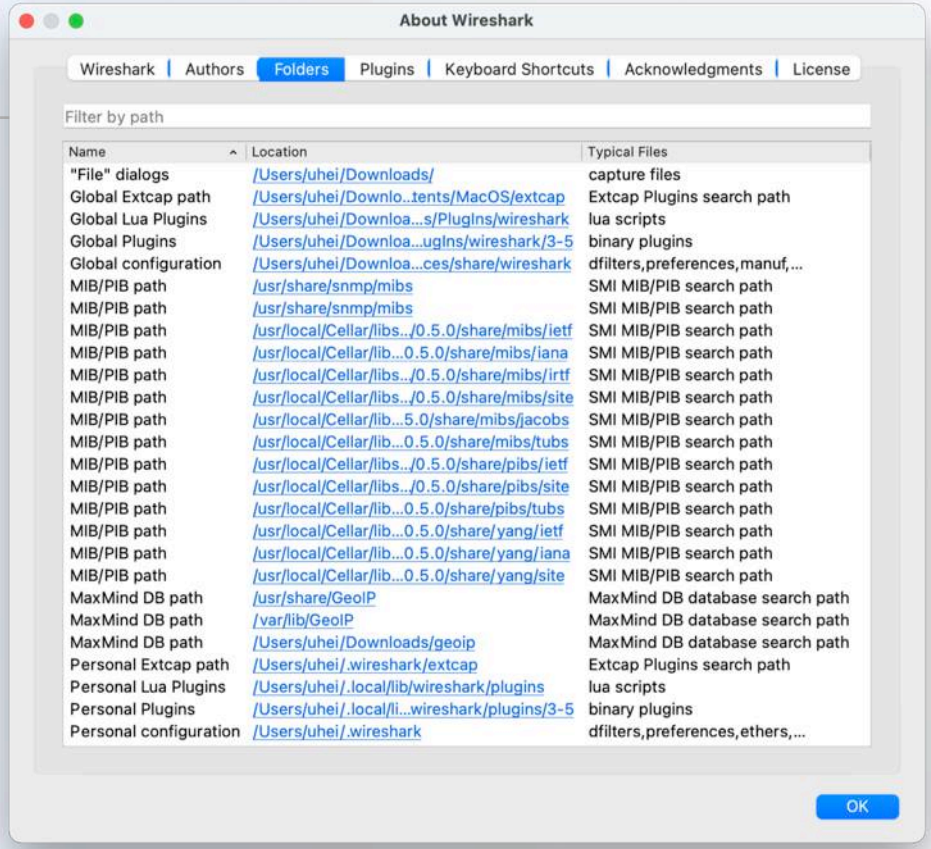
Personal specific

`$HOME/.wireshark/preferences`

Global

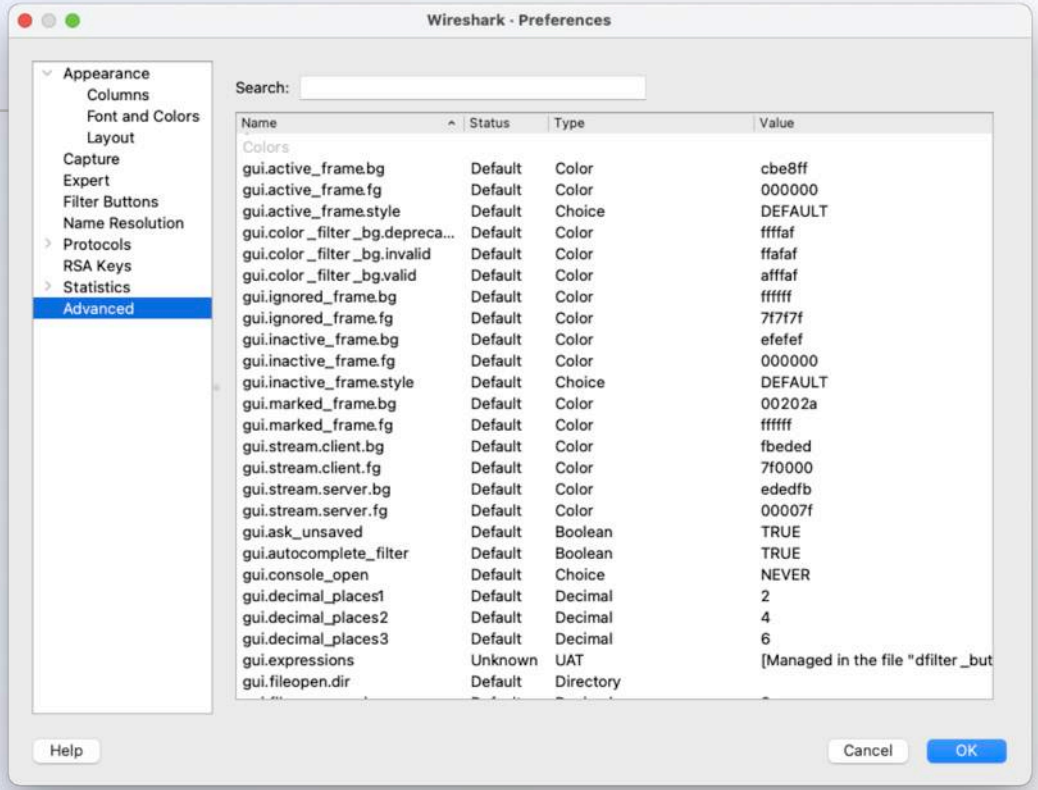
`APPDIR/Contents/Resources/share/wireshark/preferences`

Paths are examples for macOS



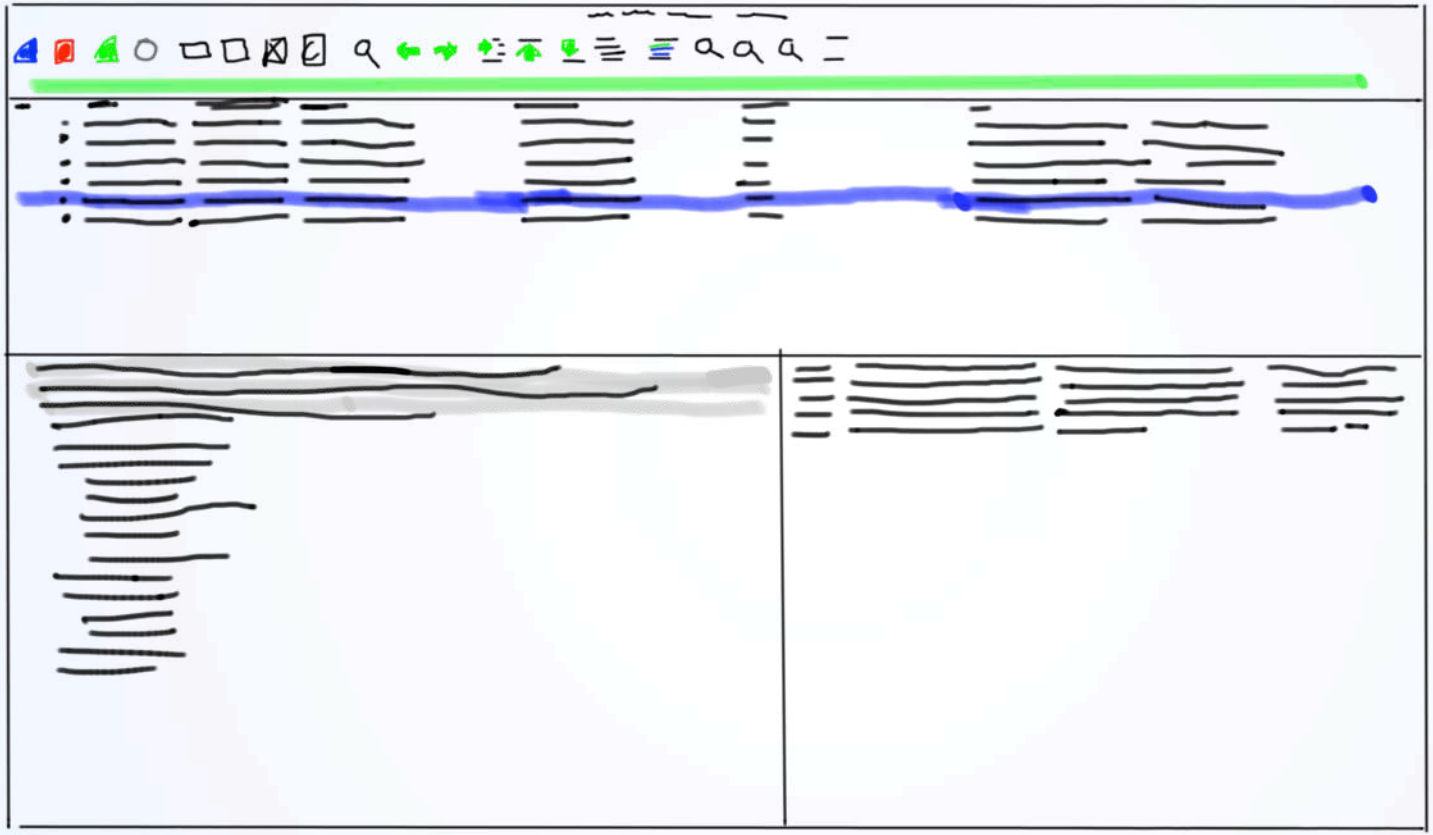
#sf21veu

```
./tshark -G folders
```

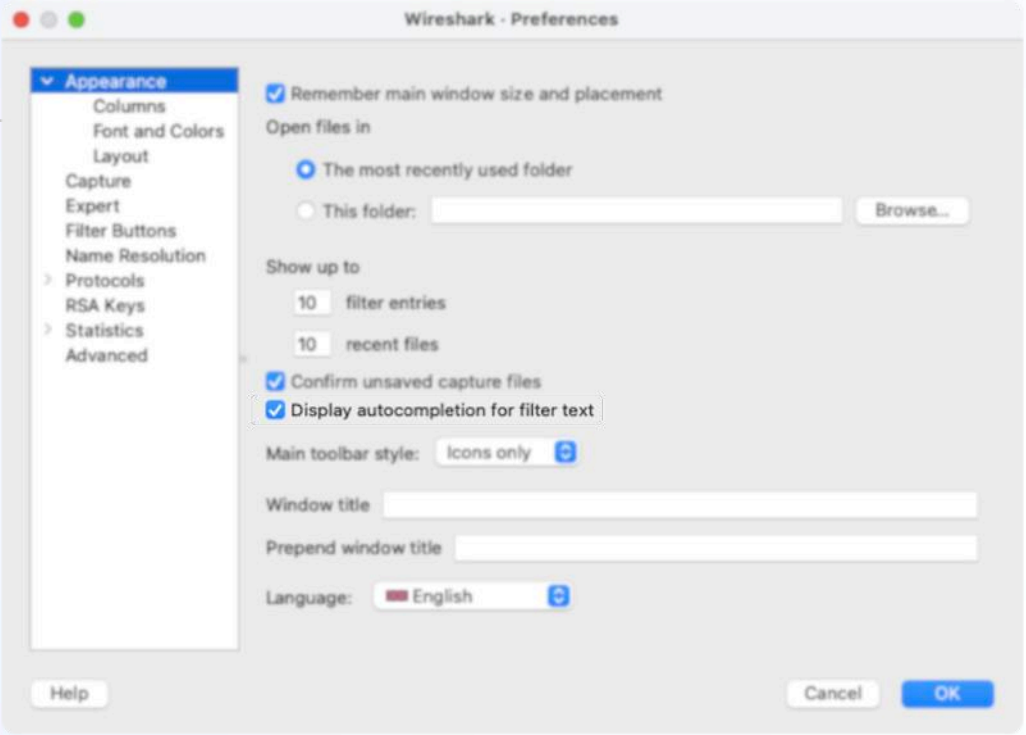


#sf21veu

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

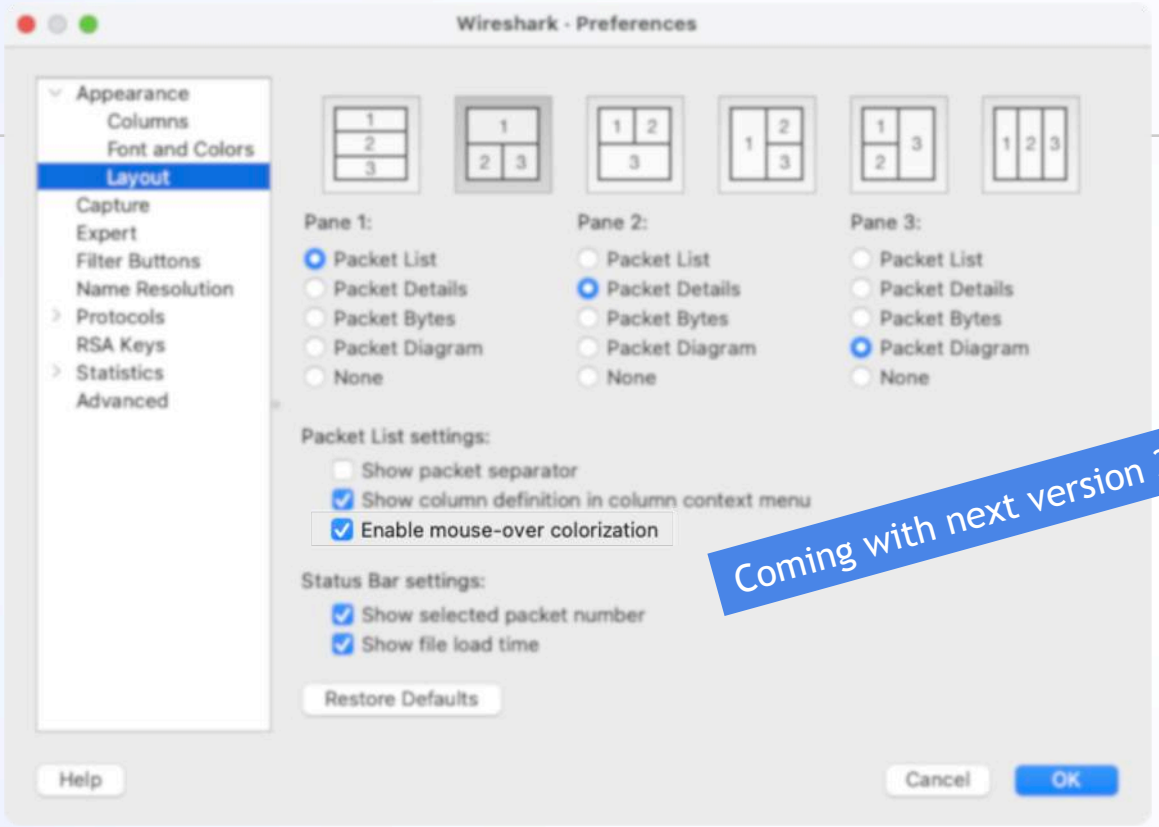


#sf21veu



#sf21veu

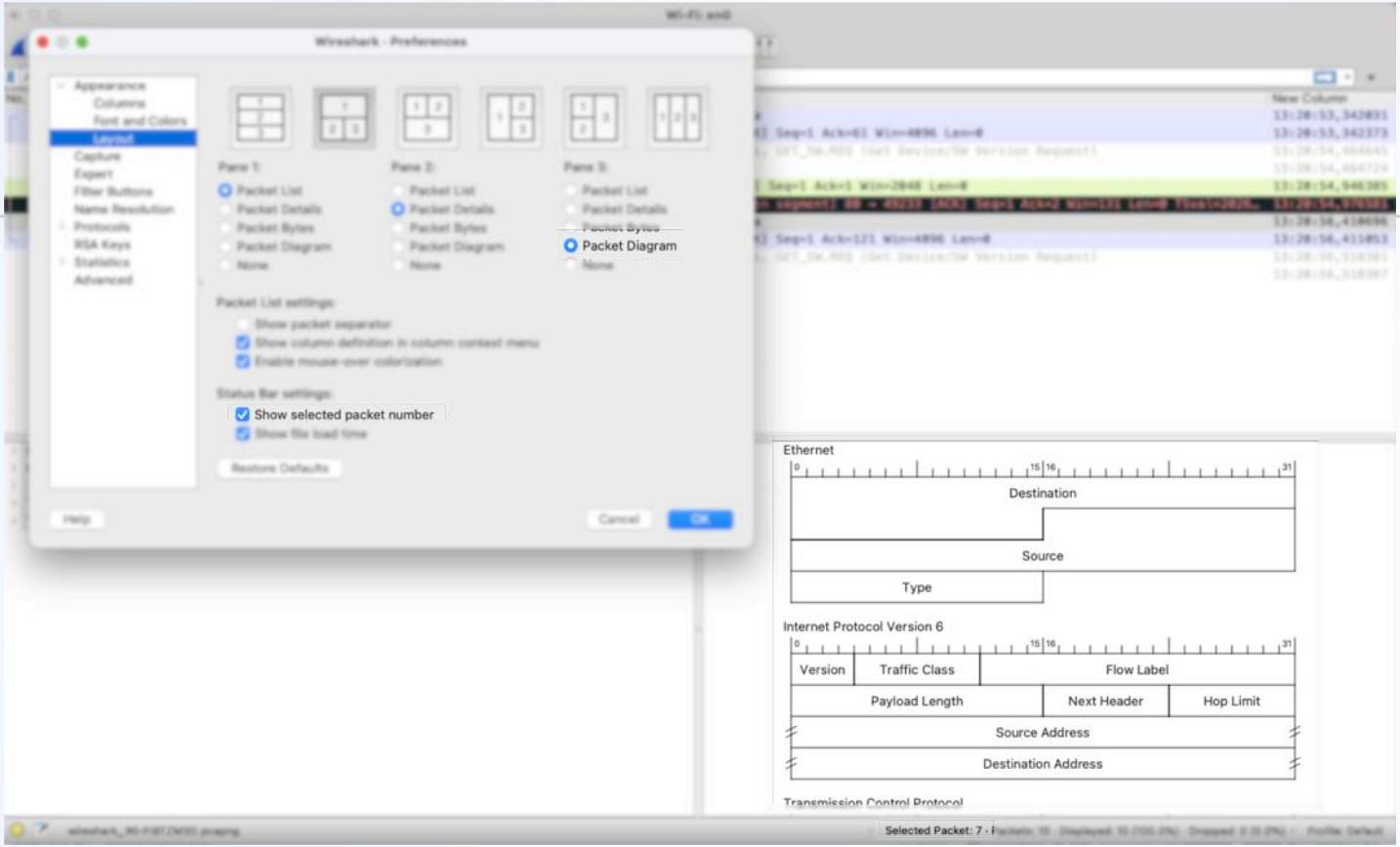
gui.autocomplete_filter



Coming with next version 3.6

#sf21veu

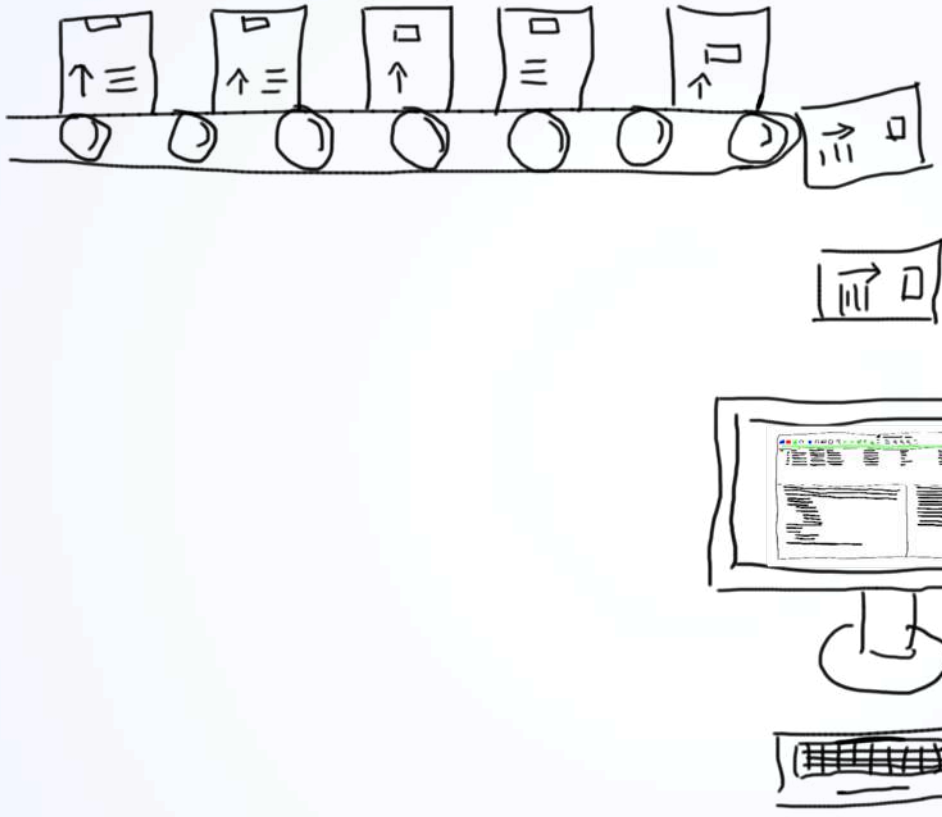
`gui.packet_list_hover_style.enable`



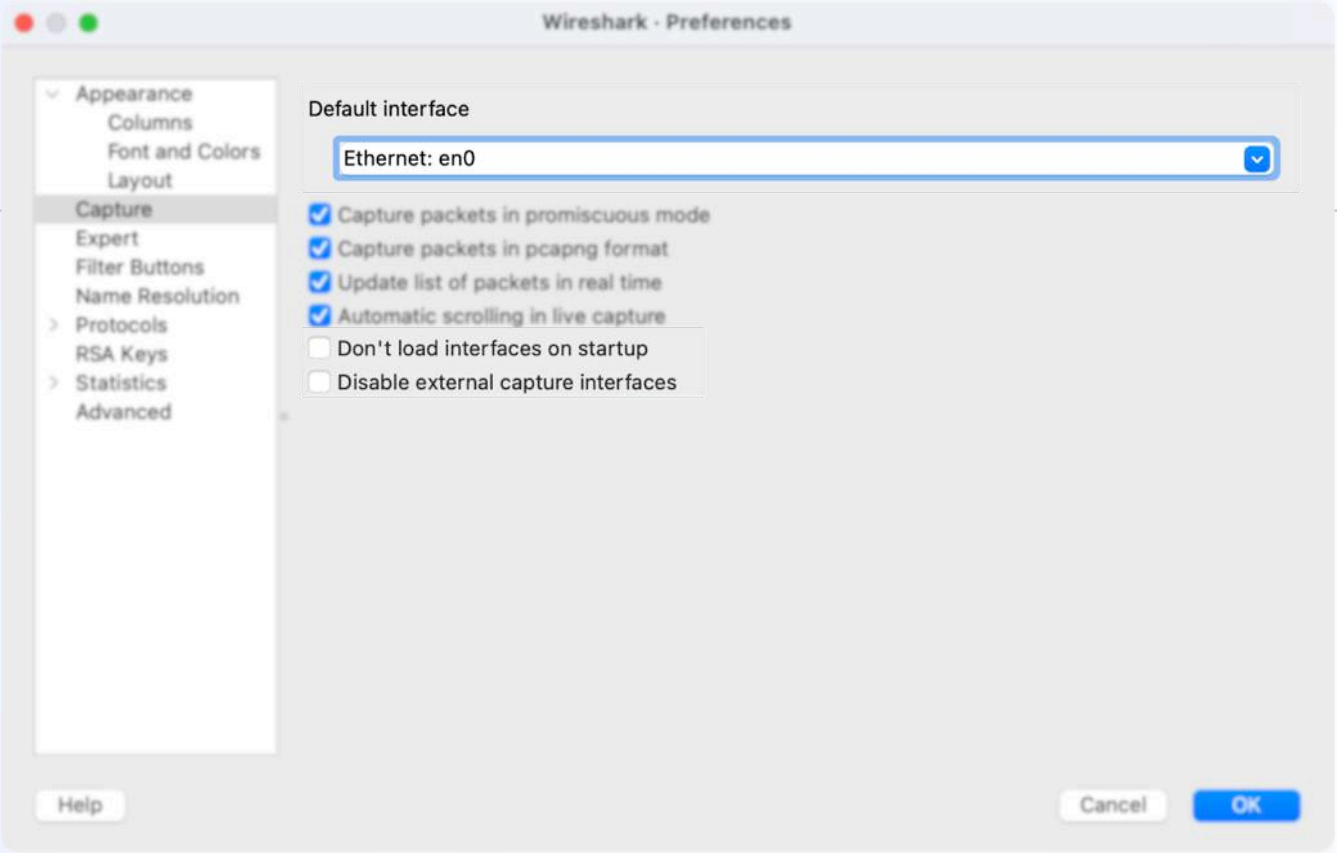
#sf21veu

gui.layout_content_[123]

gui.show_selected_packet.enabled



#sf21veu



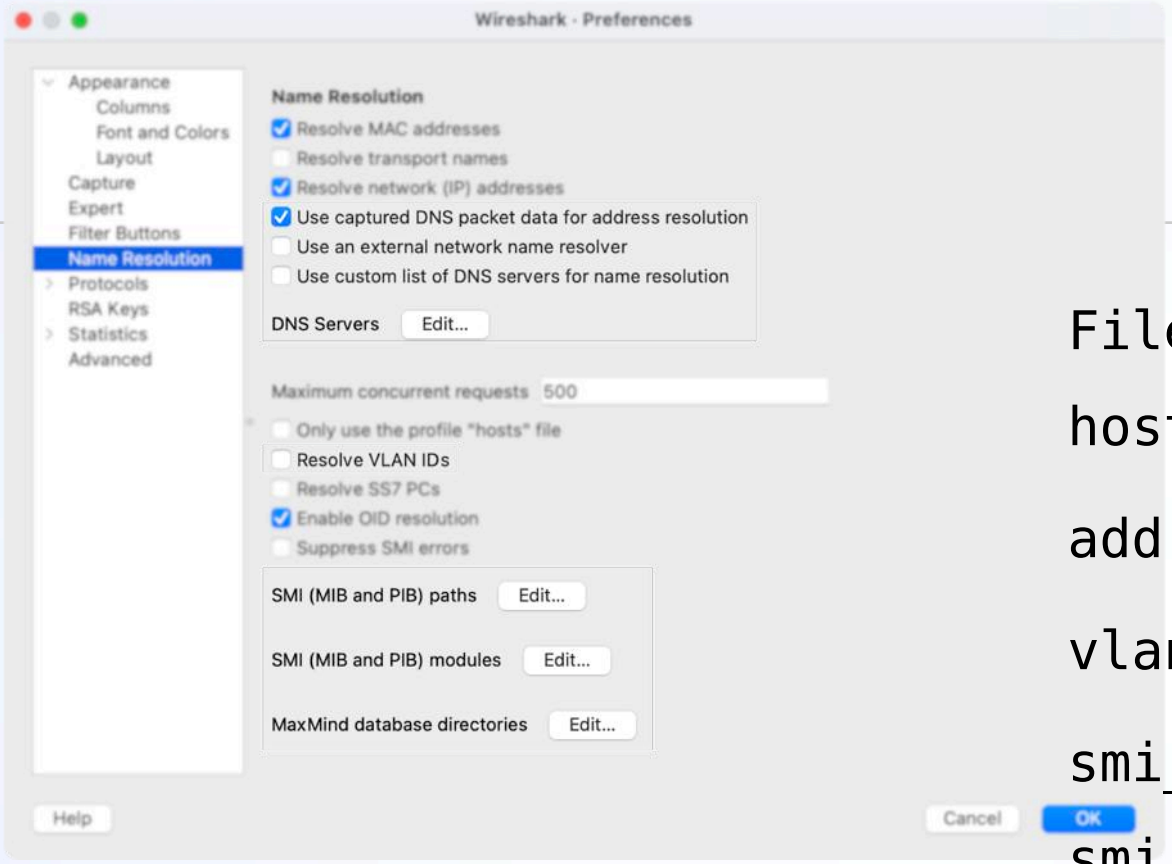
#sf21veu

`capture.device`

`capture.no_extcap`

`capture.no_interface_load`

#sf21veu



#sf21veu

Files:

hosts

addr_resolve_dns_servers

vlans

smi_paths

smi_modules

maxmind_db_paths


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

#sf21veu

Advanced stuff

gui.restore_filter_after_following_stream

gui.max_export_objects


SNMP
SMTP
IPv6
Radius
HTTP
MQTT
TCP
TLS
Dissectors
DTLS
openSafety
DNS
DHCP
Data
Kerberos
Ethernet
IMF
IP
SIP

#sf21veu

Generic stuff

Enable/Disable Protocols

Decode as

Default Port

HTTP

Reassemble HTTP headers/bodies spanning multiple TCP segments

Uncompress entity bodies

Custom HTTP header fields

SIP is quite similar

TCP

Allow subdissector to reassemble TCP streams

Analyze TCP sequence numbers

Relative sequence numbers

Scaling factor to use when not available from capture

MQTT

Show message as text

Message decoding

IP v4/v6

Enable IPv4/IPv6 geolocation

Reassemble fragmented IPv4/IPv6 datagrams

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

TLS / DTLS

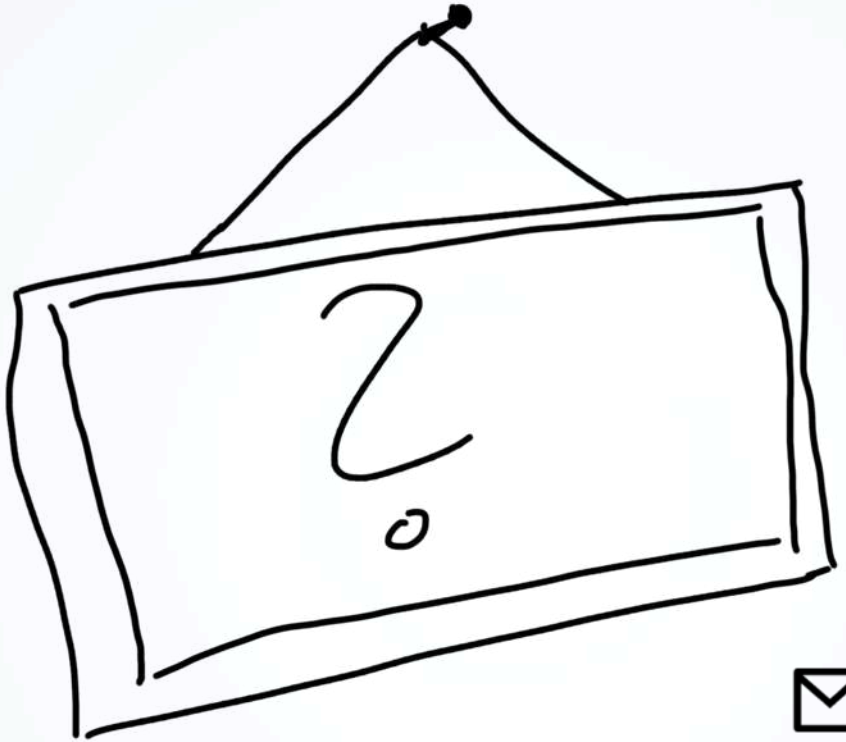
https://lekensteyn.nl/files/wireshark-tls-debugging-sharkfest19eu.pdf

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

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

Feedback

https://forms.gle/GGRAzkJcEuDkx5r36



#sf21veu

uh@heilmeier.eu

@pizza_4u

@uhei@chaos.social

Kerberos v5 / Radius / SNMP

Decrypt (Keytab / Shared Secret / Users Table)

OID Resolving (s. Name resolving)

Data

Try to uncompress zlib compressed data

Show data as text

Generate MD5 hash

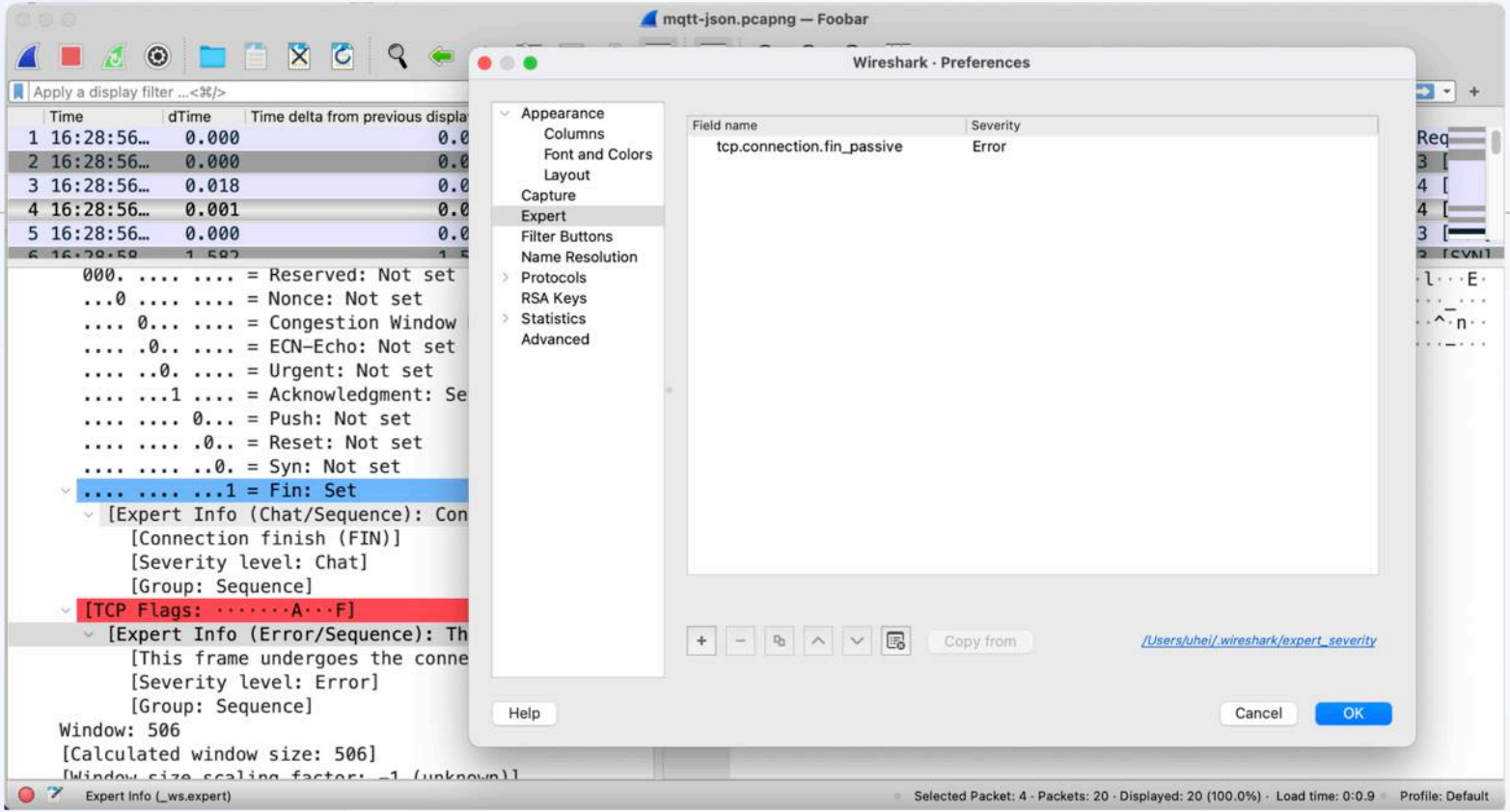
DHCP

Endianness of UUID

Custom DHCP/BootP Options

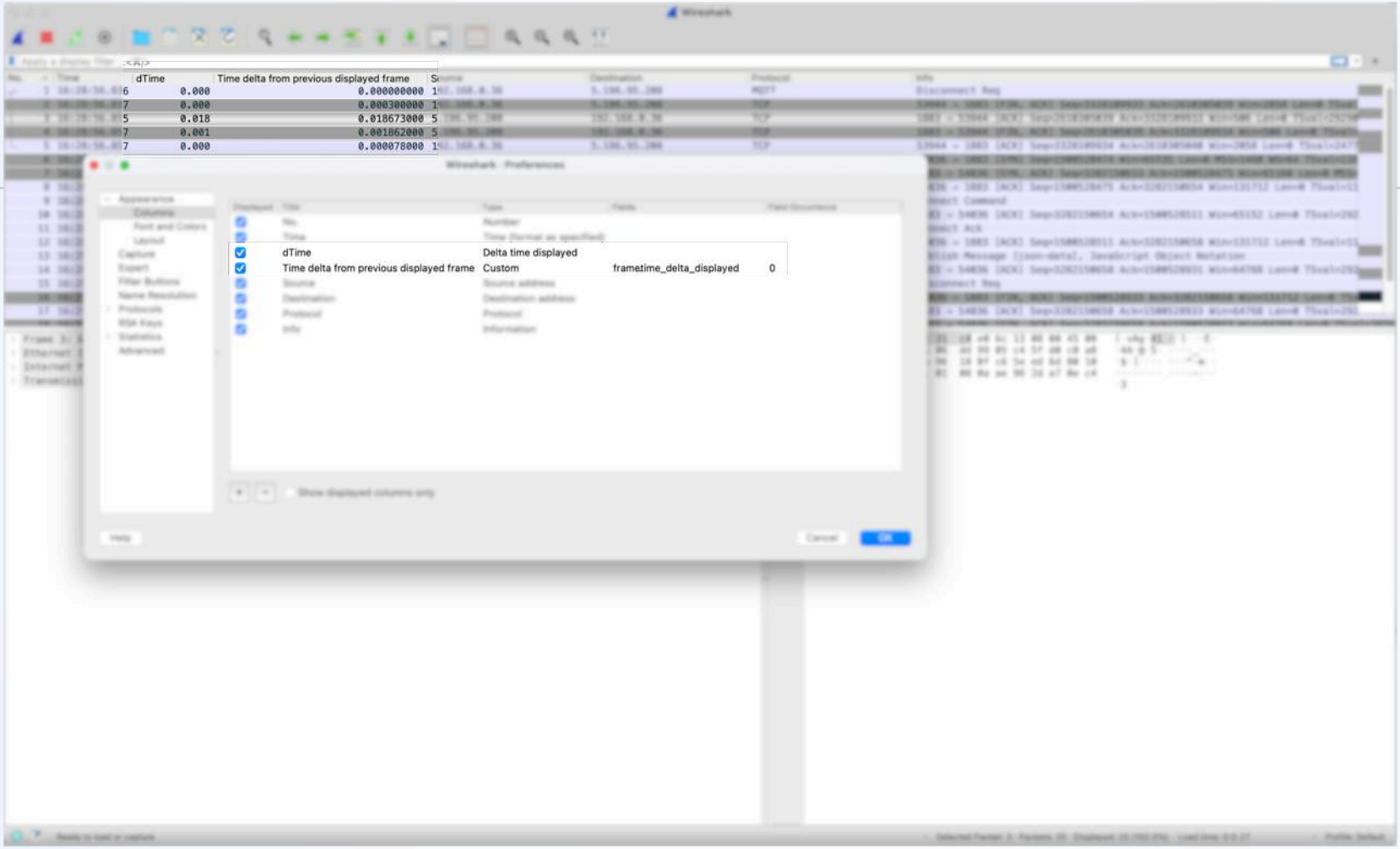
#sf21veu

Expert Severity



#sf21veu

File: expert_severity


dTime
Time delta from previous displayed frame
0.000 0.000000000
0.000 0.000300000
0.018 0.018673000
0.001 0.001862000
0.000 0.000078000
Wireshark · Preferences
dTime
Delta time displayed
Time delta from previous displayed frame
Custom
frametime_delta_displayed
0

#sf21veu