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
Know your preferences
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
To list all folders, you can use the command:

```
./tshark -G folders
```
./tshark -G currentprefs
./tshark -G defaultprefs
gui.autocomplete_filter
Coming with next version 3.6

gui.packet_list_hover_style.enable
gui.layout_content_[123]

gui.show_selected_packet.enabled
capture.device
capture.no_extcap
capture.no_interface_load
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
Advanced stuff
gui.restore_filter_after_following_stream

gui.max_export_objects
Dissectors

SNMP  SMTP  HTTP  IPv6  Radius
TLS  MQTT  TCP  DTLS
openSafty  DNS  DHCP  Data
Ethemet  IMF  P  SIP
Verberos
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
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://sharkfesteurope.wireshark.org/assets/presentations16eu/07.pdf
Feedback

https://forms.gle/GGRAzkJcEuDkx5r36
Kerberos v5 / Radius / SNMP

Decrypt (Keytab / Shared Secret / Users Table)

OID Resolving (s. Name resolving)
Try to uncompressed zlib compressed data
Show data as text
Generate MD5 hash
DHCP

Endianness of UUID

Custom DHCP/BootP Options
Expert Severity
File: expert_severity