tshark Packet analyzer CLI

CONCEPTS

> Only capture on networks and hosts you are authorised to monitor. Packet data can contain passwords and personal data; store and share captures with care.

Capture -i, -f filter
↓ -w
pcapng file raw packets
↓ -r
Display filter -Y
↓ -T / -z
Output text, fields, JSON, stats

> Two filter languages: -f is a capture filter (BPF, same as tcpdump, applied while capturing); -Y is a display filter (Wireshark fields like ip.addr, applied after dissection).

CAPTURE

`tshark -D`
List capture interfaces

`tshark -i <iface>`
Capture live on an interface

`tshark -i <iface> -c <n>`
Stop after n packets

`tshark -i <iface> -f "<filter>"`
Capture filter (BPF syntax)

FILES AND STOPPING

`tshark -i <iface> -w <file>`
Write raw packets to a file

`tshark -r <file>`
Read a capture file

`tshark -i <iface> -a duration:<s>`
Stop after n seconds

DISPLAY FILTERS

`-Y "ip.addr == <ip>"`
Packets to or from a host

DISPLAY FILTERS (cont.)

`-Y "tcp.port == <n>"`
TCP port, either side

`-Y "http.request"`
HTTP requests

`-Y "dns.qry.name contains \"<name>\""`
DNS queries by name

`-Y "<a> && !(<b>)"`
Combine with and, or, not

OUTPUT

`tshark -r <file> -V`
Full packet detail

`tshark -r <file> -n`
No name resolution

EXTRACT FIELDS

`tshark -r <file> -T fields -e <field>`
Print chosen fields only

`-T fields -e ip.src -e ip.dst -e tcp.dstport`
Several fields, tab separated

`-T fields -E header=y`
Add a header row

`-T fields -E separator=,`
Comma separated output

STATISTICS

`tshark -r <file> -q -z io,phs`
Protocol hierarchy

`tshark -r <file> -q -z conv,tcp`
TCP conversations

STREAMS AND OBJECTS

`tshark -r <file> -q -z follow,tcp,ascii,<n>`
Follow TCP stream n as text

`-Y "tcp.stream == <n>"`
All packets of one TCP stream