T-Shark for the Win

Christian Landström, Airbus DS

About / Outline

- Basics on T-Shark
- Useful situations for switching to CLI
- Batch Jobbing
- „Data“ / Field extraction

- Demo, Demo, Demo…

Tshark basics

```
C:\Users\Landi\> tshark -h
```

- Tshark is the command line equivalent of Wireshark with access to nearly all features available for everyday use
- Sticks to the “Default” Profile if no other one is specified
- Dumps output to CLI which is useful for further processing e.g. using *grep/findstr, cut, (g)awk, sed*

Batch Jobbing

- When capturing big amounts of data, ring buffer with multiple files recommended for ease of analysis
- In most cases hundreds of files – each around 50-250 Mbytes
- Need for scripted, automated task offload of common or specific analysis objects for each and every trace file

- Target: Have smaller trace data to be able to load whole selection or time ranges into Wireshark without having too many packets overhead

- Typical example: Selection of all files containing packets from a certain host and filtering for that particular IP address

Batch Jobbing

```
tshark –r <infile> -Y <filter> -w <outfile>
```

- Uses Default Profile -> beware if settings e.g. Reassembly are set
- Profile can be set by using –C <profile> flag
- Recommended: Have a specific “CLI” profile with all unneeded features turned off for additional speed e.g. turn of GeoIP lookups if not needed

Batch Jobbing

```
C:\Users\Landi\>for %a in (*.pcap) DO tshark -r %a
-Y ip.addr==192.168.0.1 -w filtered\filter1_%a
```

- Used for automated working on multiple capture files for static content filtering e.g. source IP or VLAN filtering
- Remember to set “%%” in front of variable when using Windows .bat files

Field extraction

```
C:\Users\Landi\> tshark -r %a -Y ip.addr==192.168.0.1
-Tfields –e ip.src –e ip.dst
```

- Dumps values supplied by the “-e” flags instead of the whole packet list line
- Can be used to access all data which can be described by a display filter
- Can have multiple results per flag e.g. when having inner and outer IP headers or IP addresses within ICMP quotes etc.

2-stage batch jobs

```
C:\Users\Landi\> for %a in (*.pcap) DO tshark -r %a -Y tcp.analysis.retransmission -Tfields -e tcp.stream > streams_with_retransmissions_%a.txt
```

- Typically used for conditional filtering of sessions containing a certain marker, due to conditional filtering based on one item not possible within Wireshark

  e.g. → "Give me all TCP sessions containing packet loss"

- Can be eased by supplying the TCP Session ID (stream number) instead of IP / Port pairs

Demo Time

Example: Extracting the TTL values from DNS responses

```
# tshark -r „trace.pcap" -Y dns.flags.response==1 -Tfields -e
dns.resp.ttl | sed s/,/\r\n/g | sort -nr
80441
64022
52194
50364
49143
[…]
```

Demo Time

Example: 2-stage conversation filter containing retransmissions

```
1st stage: copy to file or attach „> error-streams.txt“
# tshark -r „trace.pcap" -Y tcp.analysis.retransmission -Tfields -e
tcp.stream | sort | uniq | srt -rn
154
137
130
126
[…]

2nd stage:
for /F %a in (error-streams.txt) DO
tshark -r trace.pcap -Y tcp.stream==%a –w filtered\errorstream_%a.pcap
```

Demo Time

Example: Extracting information about MTU problems from fragmentation needed packets

```
# tshark -r trace.pcap -Y "icmp.type==3 && icmp.code==4"
-Tfields -e ip.src -e icmp.mtu -e ip.dst

172.16.31.10,172.16.31.55       800     172.16.31.55,192.168.1.1
```

Src and Dst IP from ICMP IP header

MTU

Src and Dst IP from quote within ICMP

Demo Time

Example: Extracting the HTTP response codes and times** since request

```
# tshark -r „trace.pcap" -Y http.response -Tfields -e frame.number -e
http.response.code -e http.time
2       200     0.001896000
5       200     0.001051000
8       200     0.001849000
11      200     0.003594000
14      200     0.002530000
17      200     0.003147000
27      302     0.000431000
43      200     0.212918000
48      302     0.000003000

** beware the TCP stream reassembly setting
```

!! Thank you for attending !!

Questions?

---

eMail: landi@packet-foo.com
Web: www.packet-foo.com
Twitter: @0x6C616E6469