TShark

Abstract

TShark is a network protocol analyzer. It lets you capture packet data from a live network, or read packets from a previously saved capture file, either printing a decoded form of those packets to the standard output or writing the packets to a file. TShark's native capture file format is pcap format, which is also the format used by tcpdump and various other tools.

Without any options set, TShark will work much like tcpdump. It will use the pcap library to capture traffic from the first available network interface and displays a summary line on stdout for each received packet.

Source: tshark man page

```
$ man tshark
```

Where to Acquire

Included with Wireshark.

Examples/Use Case

Read a pcap file:

```
$ tshark -r /pcaps/zeus-gameover-loader.pcap
```

Read a pcap, don't resolve names (layers 3 or 4):

```
$ tshark -nr /pcaps/zeus-gameover-loader.pcap
```

Read a pcap, use the display filter "http.request.method==GET":

```
$ tshark -r /pcaps/zeus-gameover-loader.pcap -R "http.request.method==GET"
```

Read a pcap, show TCP SYN packets not sent to port 80, don't resolve names:

```
$ tshark -r /pcaps/zeus-gameover-loader.pcap -n -R "not tcp.port==80 and tcp.flags == 0x0002"
```

Print TCP conversations in a pcap:

```
$ tshark -n -r /pcaps/virut-worm.pcap -q -z conv,tcp
```

Print HTTP User-Agents in a pcap:

```
$ tshark -nr /pcaps/normal/http/normal-user-agent.pcap -R "http.user_agent" -Tfields -e http.user_agent
```

Print X.509 certificates in a pcap:

```
$ tshark -r /pcaps/normal/https/alexa-top-500.pcap -T fields -R "ssl.handshake.certificate" -e x509sat.p
```

Additional Info