tshark

tshark

- **What is tshark?**
  - A command-line tool that you run from a terminal window
- **What can you do with tshark?**
  - Capture packets
  - Display packets
  - Select interfaces
  - Run statistics
  - Use profiles
  - More

tshark

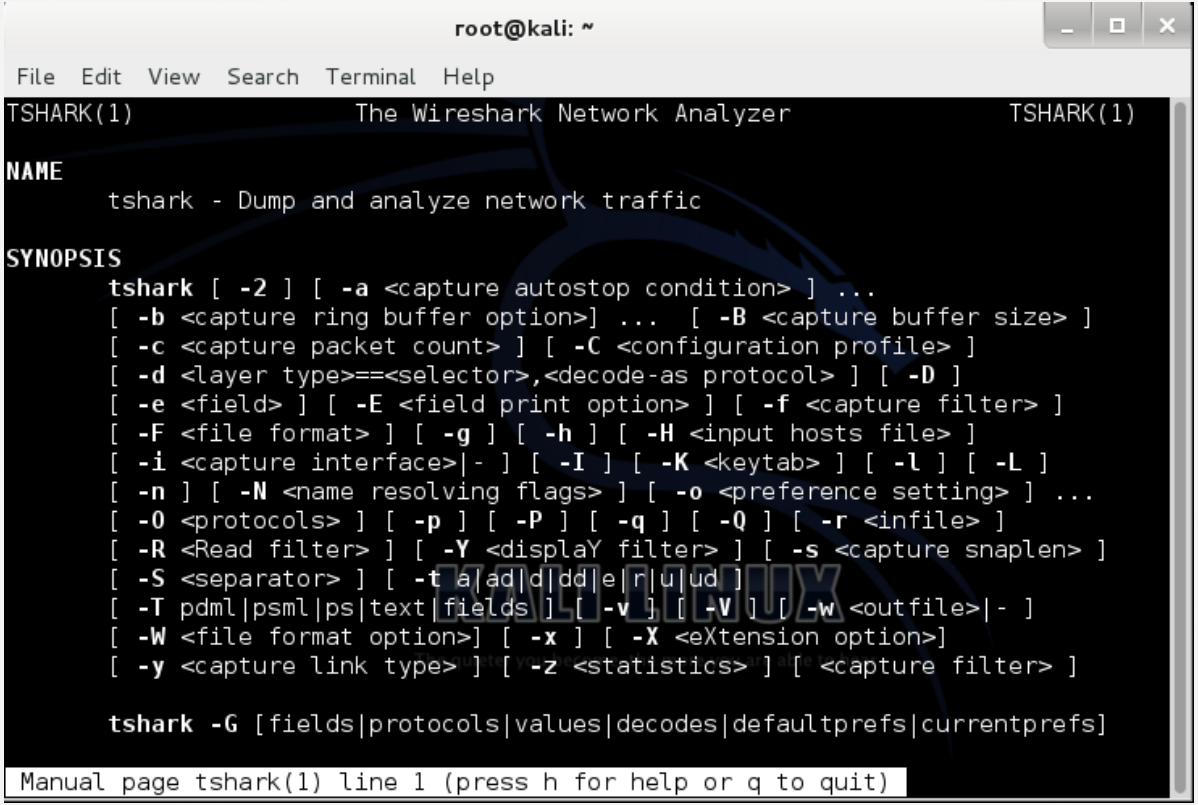
```
  0.000000 192.168.73.1 -> 192.168.73.255 NBNS 92 Name query NB WPAD<00>
1   0.756992 192.168.73.1 -> 192.168.73.255 NBNS 92 Name query NB WPAD<00>
2   1.508195 192.168.73.1 -> 192.168.73.255 NBNS 92 Name query NB WPAD<00>
3   3.001069 192.168.73.1 -> 192.168.73.255 NBNS 92 Name query NB WPAD<00>
4   3.750429 192.168.73.1 -> 192.168.73.255 NBNS 92 Name query NB WPAD<00>
5   4.500475 192.168.73.1 -> 192.168.73.255 NBNS 92 Name query NB WPAD<00>
6   9.713187 192.168.73.1 -> 224.0.0.251  MDNS 143 Standard query 0x0000  PTR _a
pple-mobdev._tcp.local, "QM" question PTR 501b058c._sub._apple-mobdev2._tcp.loca
l, "QM" question PTR _sleep-proxy._udp.local, "QM" question
7  37.676828 192.168.73.1 -> 192.168.73.255 NBNS 92 Name query NB WPAD<00>
8  38.422712 192.168.73.1 -> 192.168.73.255 NBNS 92 Name query NB WPAD<00>
9  39.172751 192.168.73.1 -> 192.168.73.255 NBNS 92 Name query NB WPAD<00>
10  42.187566 192.168.73.1 -> 192.168.73.255 NBNS 92 Name query NB WPAD<00>
 42.207488 192.168.73.1 -> 192.168.73.255 NBNS 92 Name query NB WPAD<00>
12  42.948851 192.168.73.1 -> 192.168.73.255 NBNS 92 Name query NB WPAD<00>
 42.964337 192.168.73.1 -> 192.168.73.255 NBNS 92 Name query NB WPAD<00>
14  43.713236 192.168.73.1 -> 192.168.73.255 NBNS 92 Name query NB WPAD<00>
```

tshark

How do you use tshark?

- Need Unix/Linux System administrator skills
- Must be SU
- Must have Wireshark installed
- Run from a terminal window
- Learn more using the man pages

tshark



Questions?