# Command-Line Tools

# Command-Line Tools

- **Why use the command line?**
  - For quick and easy access to the raw data that Wireshark captures and manipulates
- **Command-line tools**
  - tshark
  - tcpdump
  - dumpcap
  - capinfos
  - rawshark
  - editcap
  - mergecap
  - Others

# Command-Line Tools

```
  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>
```

# Command-Line Tools

- **Other tools, such as TCPdump**
  - Used to capture data
  - Used on most Unix/Linux distributions to capture and analyze data
  - Used on most firewall deployments
  - Captures data that you can parse for more information

# Command-Line Tools

```
listening on eth0, link-type EN10MB (Ethernet), capture size 65535 bytes
20:40:23.184819 IP 192.168.73.128.47081 > 10.1.1.1.ftp: Flags [S], seq 103440827
6, win 29200, options [mss 1460,sackOK,TS val 4294913916 ecr 0,nop,wscale 10], l
ength 0
20:40:23.208782 IP 192.168.73.128.43338 > 192.168.73.2.domain: 55739+ PTR? 1.1.1
.10.in-addr.arpa. (39)
20:40:23.213014 IP 192.168.73.2.domain > 192.168.73.128.43338: 55739 NXDomain 0/
0/0 (39)
20:40:23.216597 IP 192.168.73.128.39142 > 192.168.73.2.domain: 48916+ PTR? 128.7
3.168.192.in-addr.arpa. (45)
20:40:23.229840 IP 192.168.73.2.domain > 192.168.73.128.39142: 48916 NXDomain 0/
0/0 (45)
20:40:23.230343 IP 192.168.73.128.45291 > 192.168.73.2.domain: 11352+ PTR? 2.73.
168.192.in-addr.arpa. (43)
20:40:23.243455 IP 192.168.73.2.domain > 192.168.73.128.45291: 11352 NXDomain 0/
0/0 (43)
20:40:24.185137 IP 192.168.73.128.47081 > 10.1.1.1.ftp: Flags [S], seq 103440827
```

# Questions?