Troubleshooting with tshark

Troubleshooting with tshark

- What is tshark?
- How do you use tshark?
  - Command line (Windows and Linux)
- Command-line usage
  - Knowing switches
  - Knowing how to pipe to a file
  - Knowing how to save a file to further analyze

Troubleshooting with tshark

```
TSHARK(1)                The Wireshark Network Analyzer                TSHARK(1)

NAME
       tshark - Dump and analyze network traffic

SYNOPSIS
       tshark [ -2 ] [ -a <capture autostop condition> ] ...
       [ -b <capture ring buffer option>] ...  [ -B <capture buffer size> ]
       [ -c <capture packet count> ] [ -C <configuration profile> ]
       [ -d <layer type>==<selector>,<decode-as protocol> ] [ -D ]
       [ -e <field> ] [ -E <field print option> ] [ -f <capture filter> ]
       [ -F <file format> ] [ -g ] [ -h ] [ -H <input hosts file> ]
       [ -i <capture interface>|- ] [ -I ] [ -K <keytab> ] [ -l ] [ -L ]
       [ -n ] [ -N <name resolving flags> ] [ -o <preference setting> ] ...
       [ -O <protocols> ] [ -p ] [ -P ] [ -q ] [ -Q ] [ -r <infile> ]
       [ -R <Read filter> ] [ -Y <displaY filter> ] [ -s <capture snaplen> ]
       [ -S <separator> ] [ -t a|ad|d|dd|e|r|u|ud ]
       [ -T pdml|psml|ps|text|fields ] [ -v ] [ -V ] [ -w <outfile>|- ]
       [ -W <file format option>] [ -x ] [ -X <eXtension option>]
       [ -y <capture link type> ] [ -z <statistics> ] [ <capture filter> ]

       tshark -G [fields|protocols|values|decodes|defaultprefs|currentprefs]
```

Questions?