Setting Capture & Display Filters

Setting Capture & Display Filters

- Using filters with tshark (command line)
- Capture filters
  - Same theory applies, uses Berkley and applied prior
- Display filters
  - Uses same theory, applied after, more flexible
  - Used on already saved captures

Setting Capture & Display Filters

```
Output:
  -w <outfile|->           write packets to a pcap-format file named "outfile"
                           (or to the standard output for "-")
  -C <config profile>      start with specified configuration profile
  -F <output file type>    set the output file type, default is pcapng
                           an empty "-F" option will list the file types
  -V                       add output of packet tree        (Packet Details)
  -O <protocols>           Only show packet details of these protocols, comma
                           separated
  -P                       print packet summary even when writing to a file
  -S <separator>           the line separator to print between packets
  -x                       add output of hex and ASCII dump (Packet Bytes)
  -T pdml|ps|psml|text|fields
                           format of text output (def: text)
  -e <field>               field to print if -Tfields selected (e.g. tcp.port, c
ol.Info);
```

Questions?