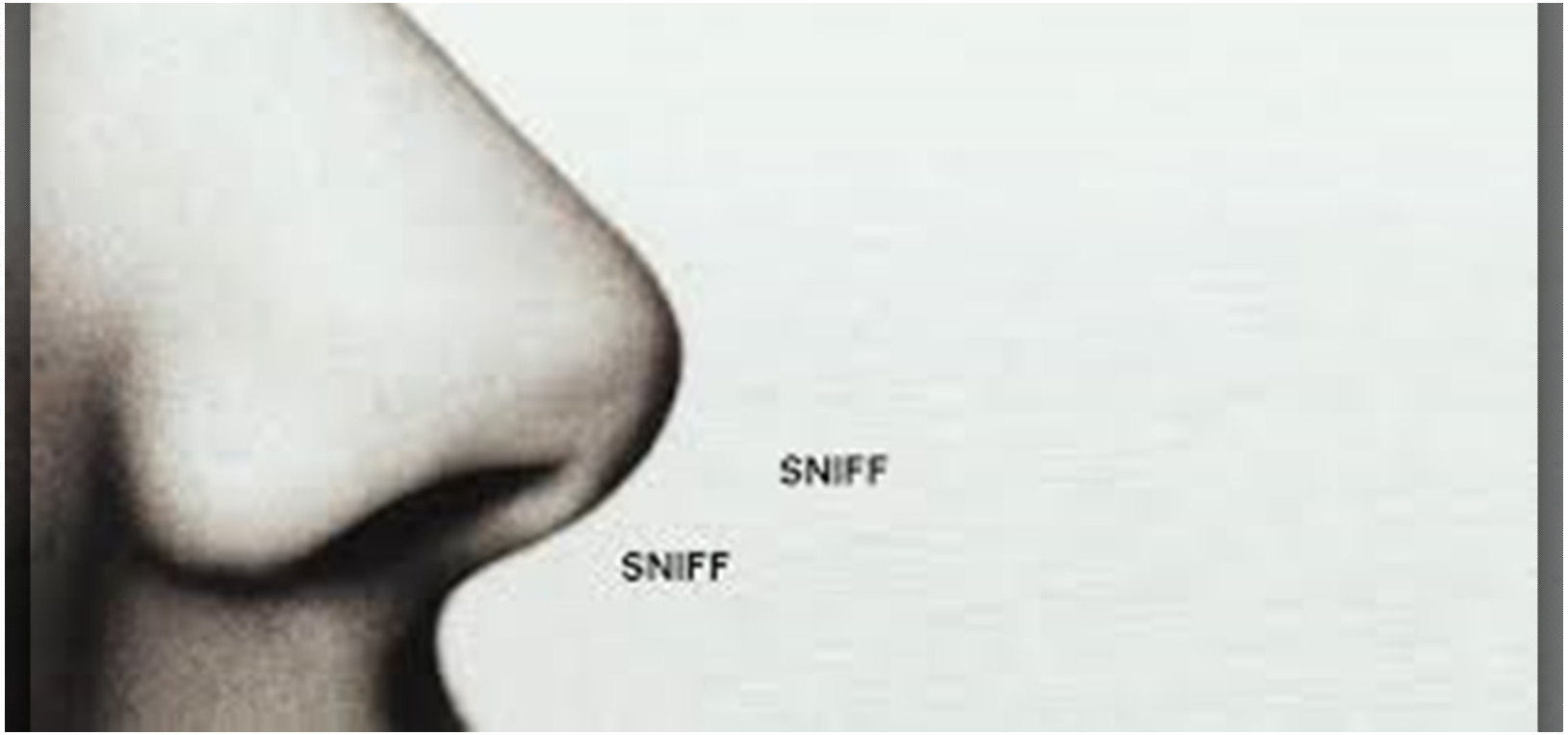


Wireshark Tutorial

EECS3214

Winter 2018

What is Wireshark?

Packet Sniffer:

- tool for observing the messages exchanged between executing protocol entities

  - captures ("sniffs") messages being sent/received from/by your computer

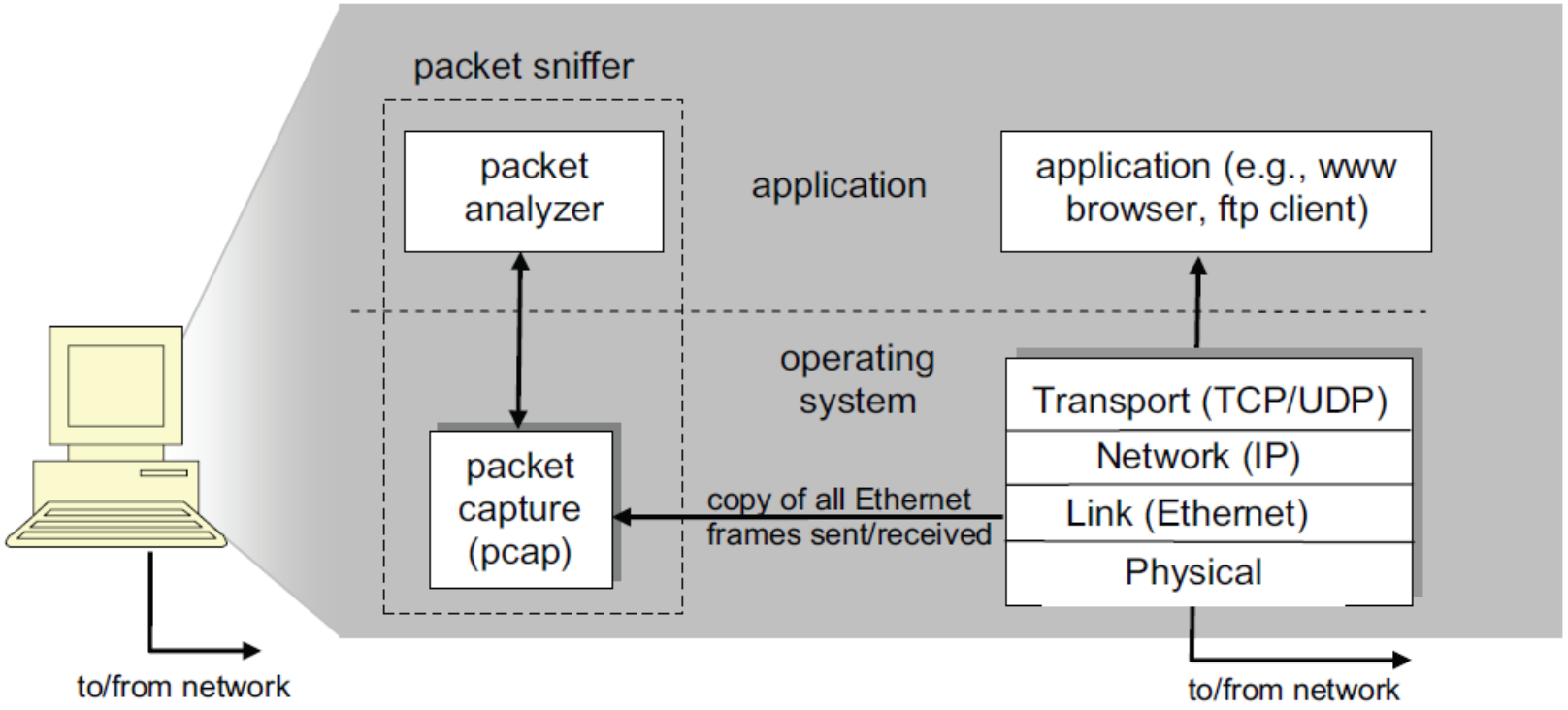
  - store and/or display the contents of the various protocol fields in these captured messages

- A packet sniffer itself is passive

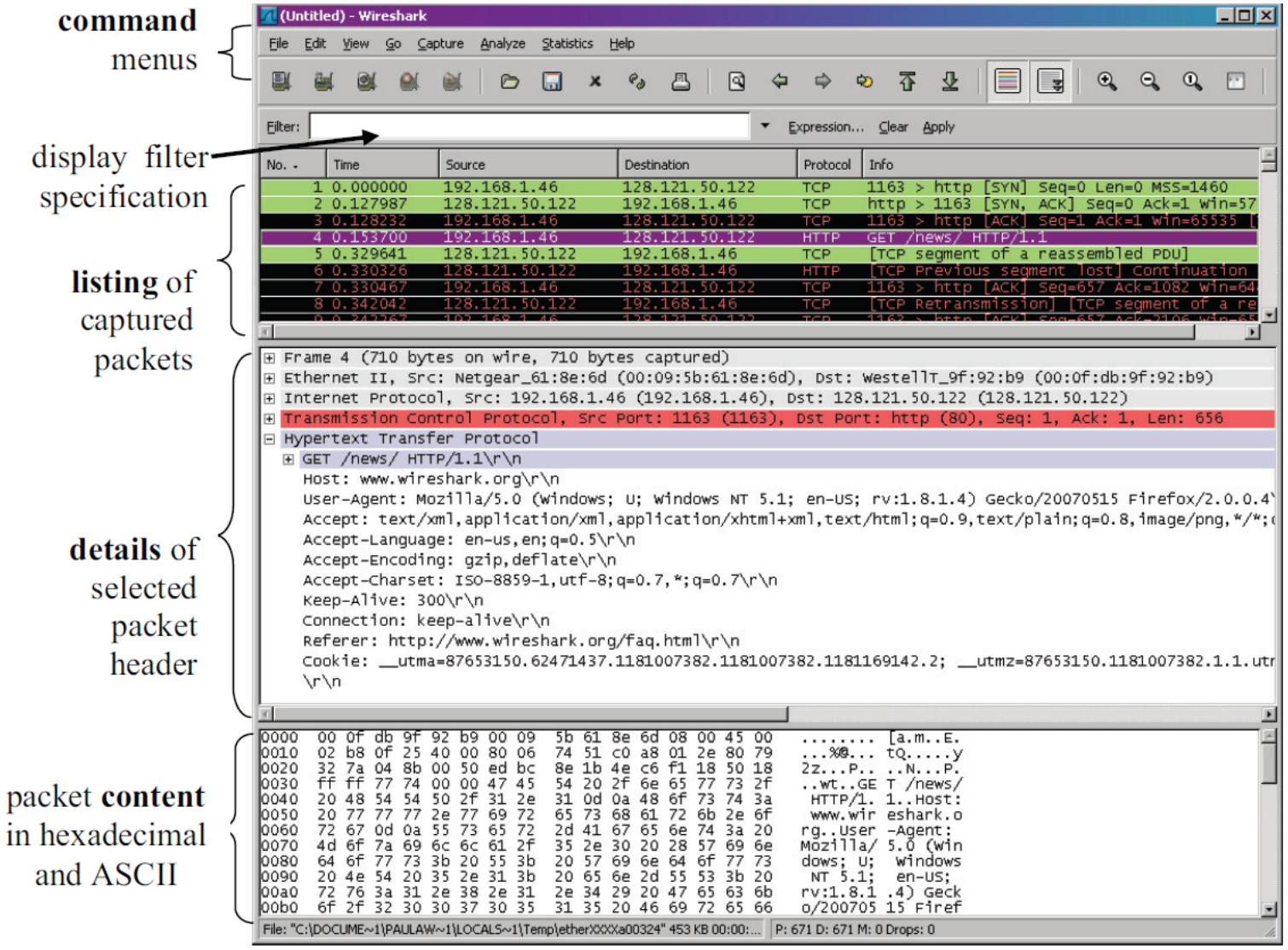
  -observes messages being sent, but never sends packets itself

  - received packets are never explicitly addressed to the packet sniffer. receives a copy of packets

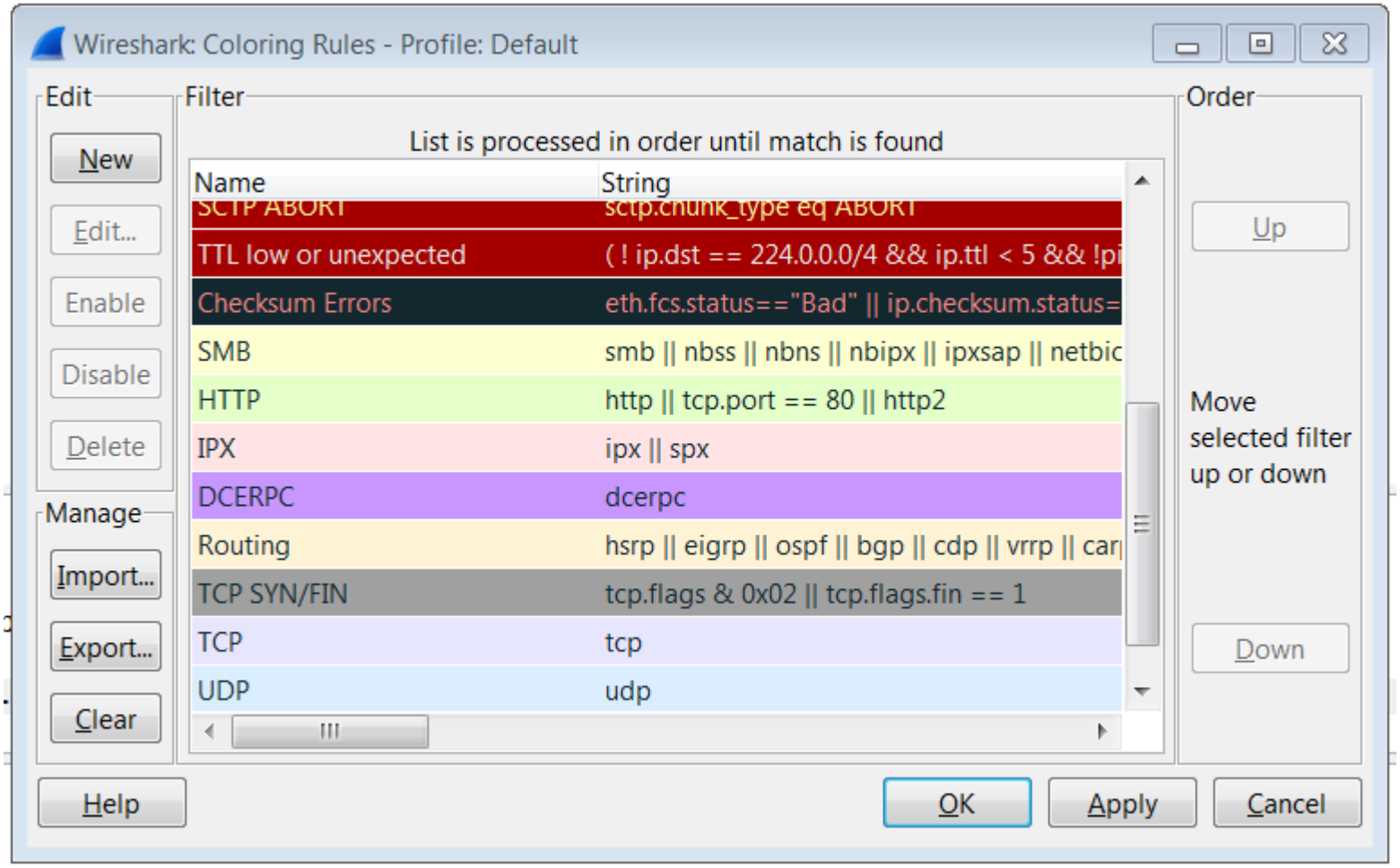
Packet Sniffer Structure



Running Wireshark



View --> Coloring Rules



Capture Options