



Wireshark Tutorial

EECS3214

Winter 2018

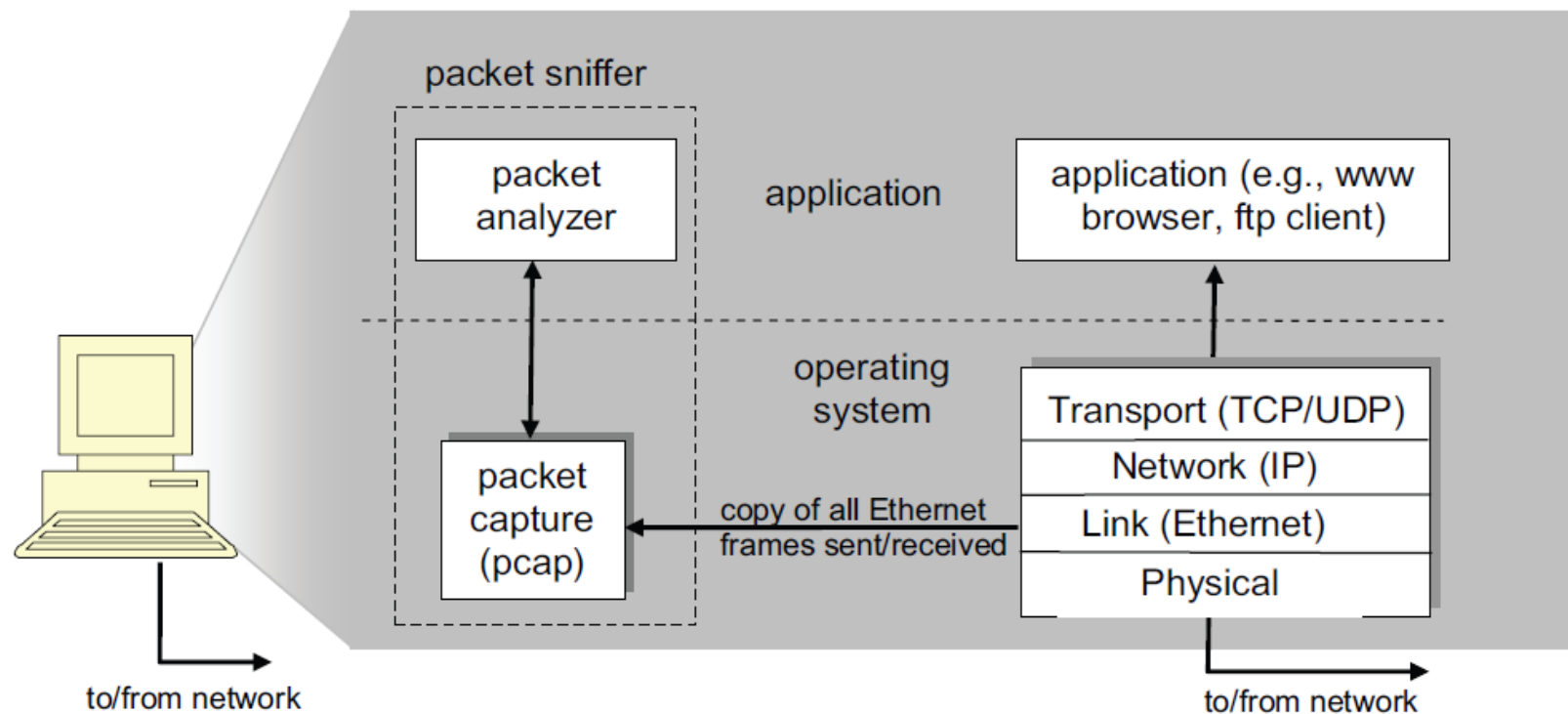


What is Wireshark?

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

command menus

display filter specification

listing of captured packets

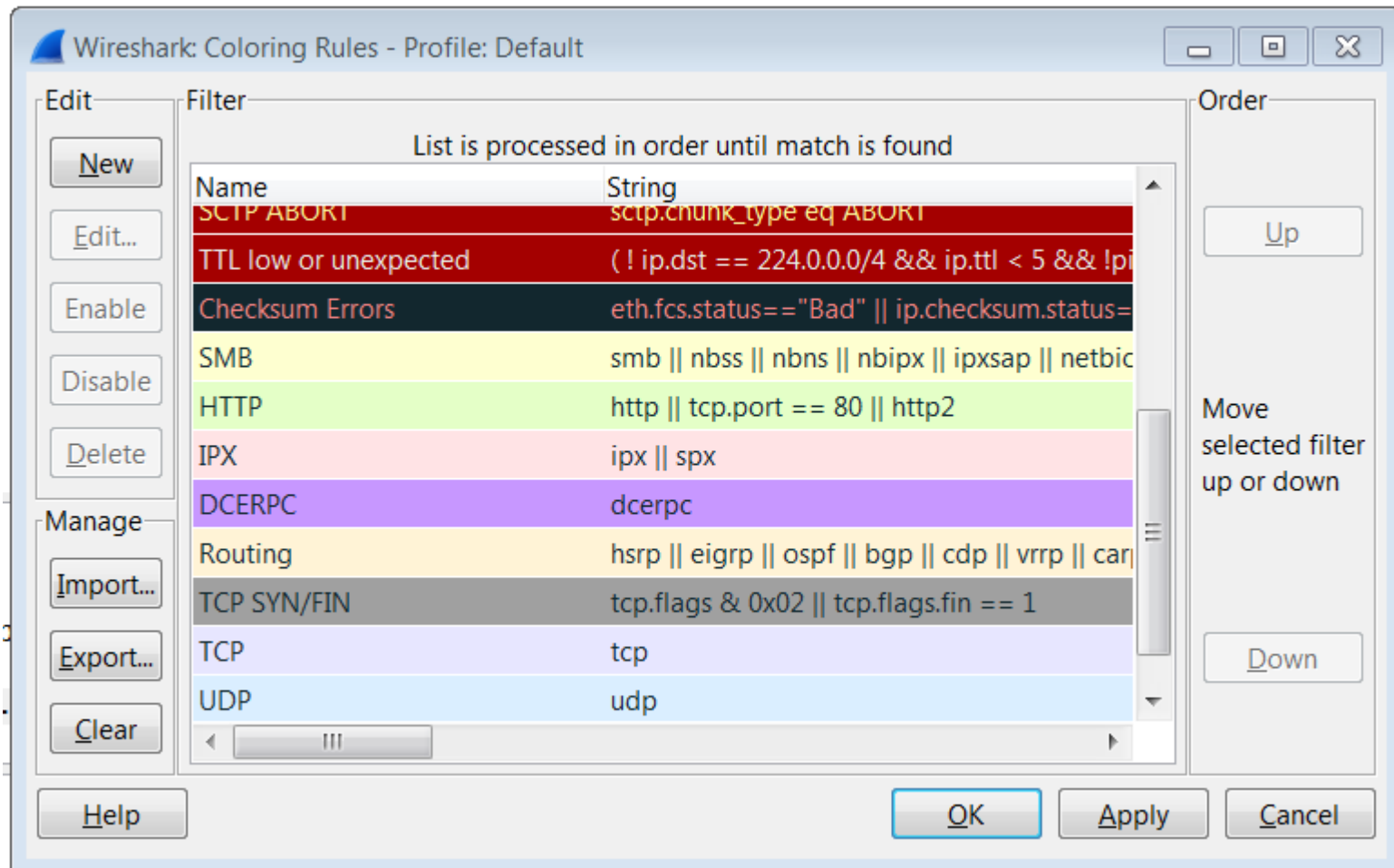
details of selected packet header

packet content in hexadecimal and ASCII

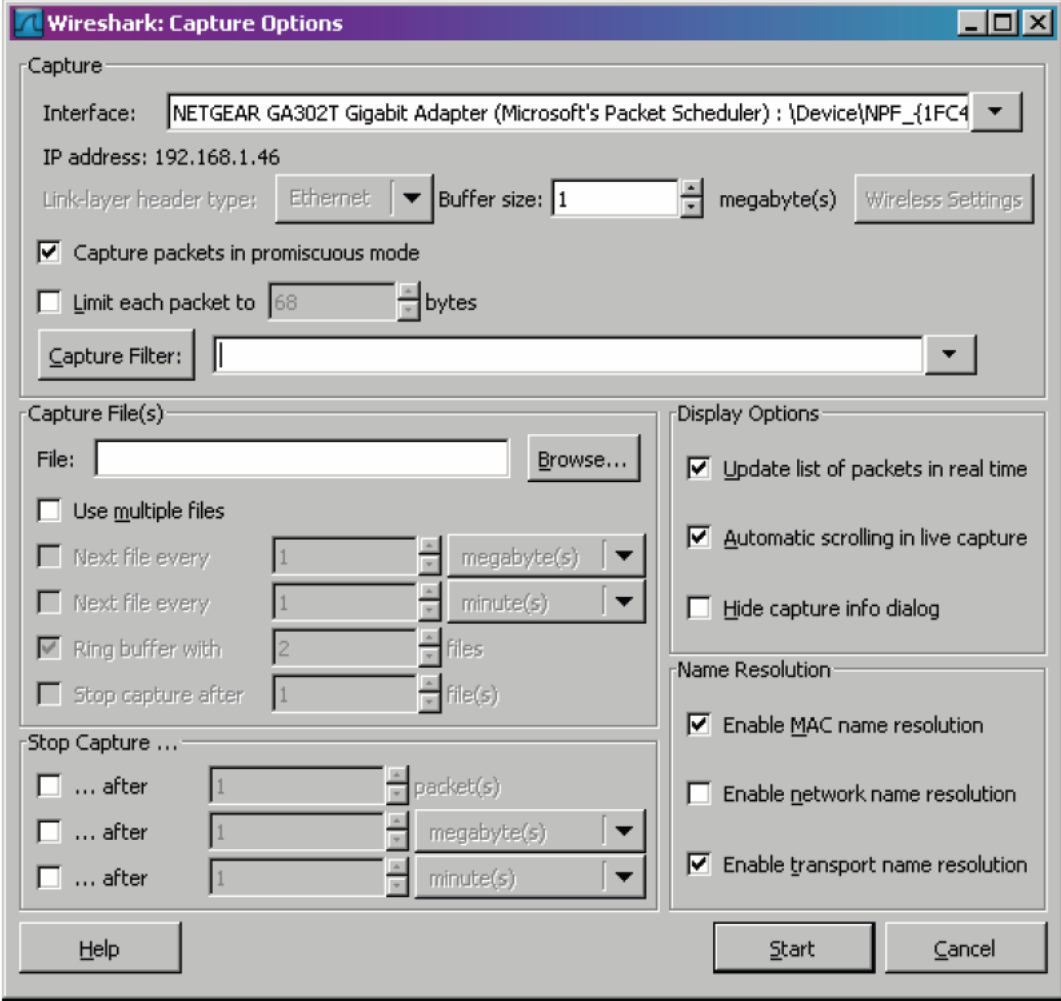
The screenshot displays the Wireshark interface with the following components:

- Menu Bar:** File, Edit, View, Go, Capture, Analyze, Statistics, Help.
- Toolbar:** Icons for file operations, capture, and analysis.
- Filter:** A text box for specifying display filters.
- Packet List:** A table showing captured packets with columns for No., Time, Source, Destination, Protocol, and Info.
- Packet Details:** A pane showing the hierarchical structure of the selected packet (Frame 4), including Ethernet II, Internet Protocol, Transmission Control Protocol, and Hypertext Transfer Protocol.
- Packet Bytes:** A pane showing the raw data of the selected packet in hexadecimal and ASCII.
- Status Bar:** Displays the file path and packet statistics.

View --> Coloring Rules



Capture Options



The image shows the 'Wireshark: Capture Options' dialog box. It is divided into several sections: 'Capture', 'Capture File(s)', 'Stop Capture ...', 'Display Options', and 'Name Resolution'. The 'Capture' section includes fields for 'Interface' (NETGEAR GA302T Gigabit Adapter), 'IP address' (192.168.1.46), 'Link-layer header type' (Ethernet), and 'Buffer size' (1 megabyte(s)). It also has checkboxes for 'Capture packets in promiscuous mode' (checked) and 'Limit each packet to 68 bytes'. The 'Capture File(s)' section has a 'File' field, a 'Browse...' button, and checkboxes for 'Use multiple files', 'Next file every 1 megabyte(s)', 'Next file every 1 minute(s)', 'Ring buffer with 2 files' (checked), and 'Stop capture after 1 file(s)'. The 'Stop Capture ...' section has three rows of checkboxes for stopping capture after a certain number of packets, megabytes, or minutes. The 'Display Options' section has checkboxes for 'Update list of packets in real time' (checked), 'Automatic scrolling in live capture' (checked), and 'Hide capture info dialog' (unchecked). The 'Name Resolution' section has checkboxes for 'Enable MAC name resolution' (checked), 'Enable network name resolution' (unchecked), and 'Enable transport name resolution' (checked). At the bottom, there are 'Help', 'Start', and 'Cancel' buttons.

Wireshark: Capture Options

Capture

Interface: NETGEAR GA302T Gigabit Adapter (Microsoft's Packet Scheduler) : \Device\NPF_{1FC4}...

IP address: 192.168.1.46

Link-layer header type: Ethernet Buffer size: 1 megabyte(s) [Wireless Settings](#)

☒ Capture packets in promiscuous mode

☐ Limit each packet to 68 bytes

Capture Filter: |

Capture File(s)

File: [Browse...](#)

☐ Use multiple files

☐ Next file every 1 megabyte(s)

☐ Next file every 1 minute(s)

☒ Ring buffer with 2 files

☐ Stop capture after 1 file(s)

Stop Capture ...

☐ ... after 1 packet(s)

☐ ... after 1 megabyte(s)

☐ ... after 1 minute(s)

Display Options

☒ Update list of packets in real time

☒ Automatic scrolling in live capture

☐ Hide capture info dialog

Name Resolution

☒ Enable MAC name resolution

☐ Enable network name resolution

☒ Enable transport name resolution

[Help](#) [Start](#) [Cancel](#)