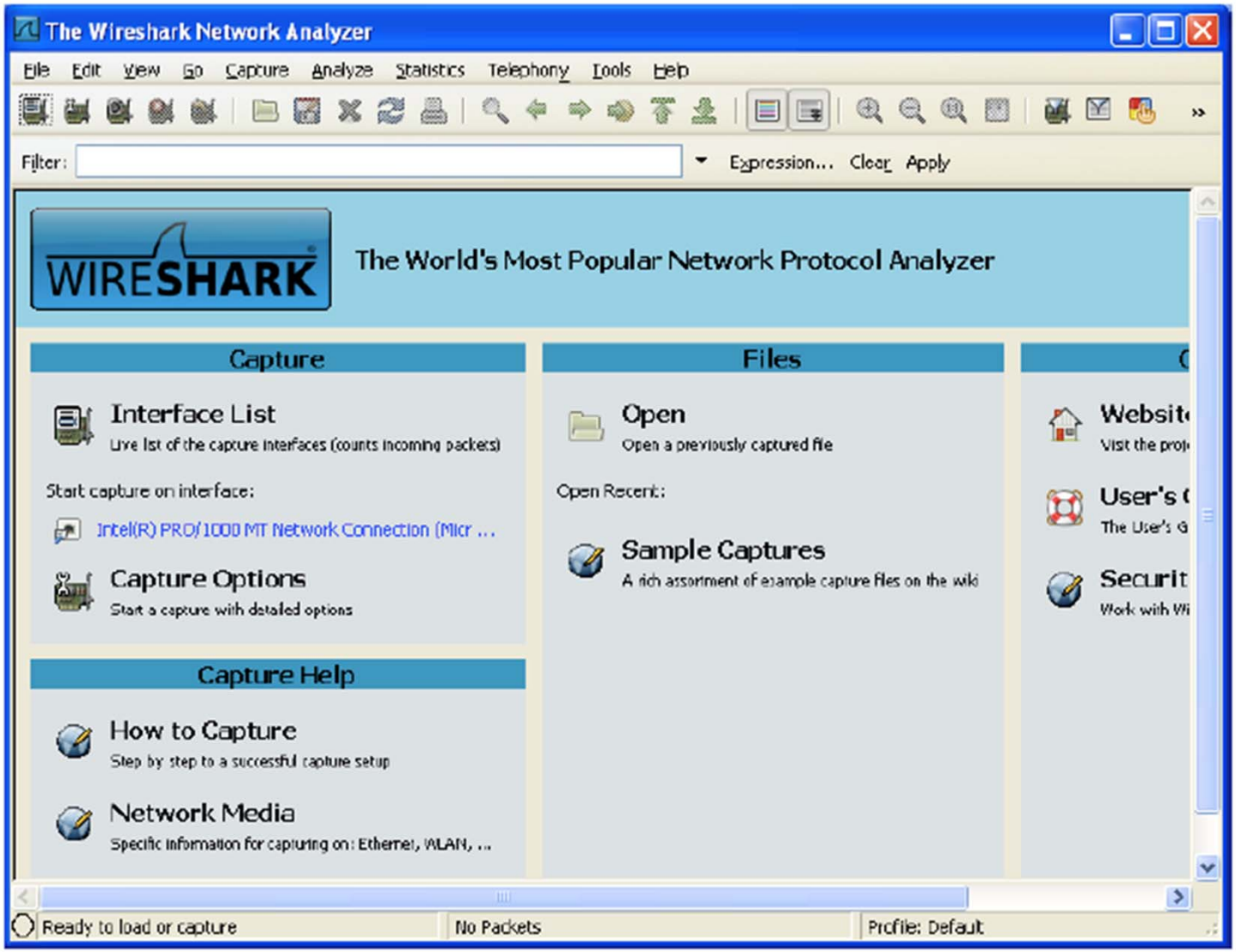
CSE 3214: Computer Network Protocols and Applications

–Network Monitoring & Protocol Analysis

Dr. Peter Lian, Professor
Department of Computer Science and Engineering
York University
Email: peterlian@cse.yorku.ca
Office: 1012C Lassonde Building
Course website:
http://wiki.cse.yorku.ca/course_archive/2012-13/W/3214

Wireshark


The Wireshark Network Analyzer
File Edit View Go Capture Analyze Statistics Telephony Tools Help
Filter:
Expression... Clear Apply
WIRESHARK
The World's Most Popular Network Protocol Analyzer
Capture
Interface List
Live list of the capture interfaces (counts incoming packets)
Start capture on interface:
Intel(R) PRO/1000 MT Network Connection (Micr ...
Capture Options
Start a capture with detailed options
Files
Open
Open a previously captured file
Open Recent:
Sample Captures
A rich assortment of example capture files on the wiki
Capture Help
How to Capture
Step by step to a successful capture setup
Network Media
Specific information for capturing on: Ethernet, WLAN, ...
Ready to load or capture
No Packets
Profile: Default

Network Monitoring & Protocol Analysis

- Process of capturing network traffic and inspecting it closely to determine type and amount of data:
  - Traveling through your network, or
  - Arriving at your computer
- Network/protocol analysis is also known as "sniffing"

Network Analyzer

- Standalone hardware device or software installed on a computer – decodes data packets of common protocol and displays their content in human-readable format
- Network analyzers are either free and commercial
- Differences between network analyzers include:
  - Number of supported protocol decodes
  - Quality of packet decodes
  - User interface
  - Graphing and statistical capabilities

Network Analyzer Applications

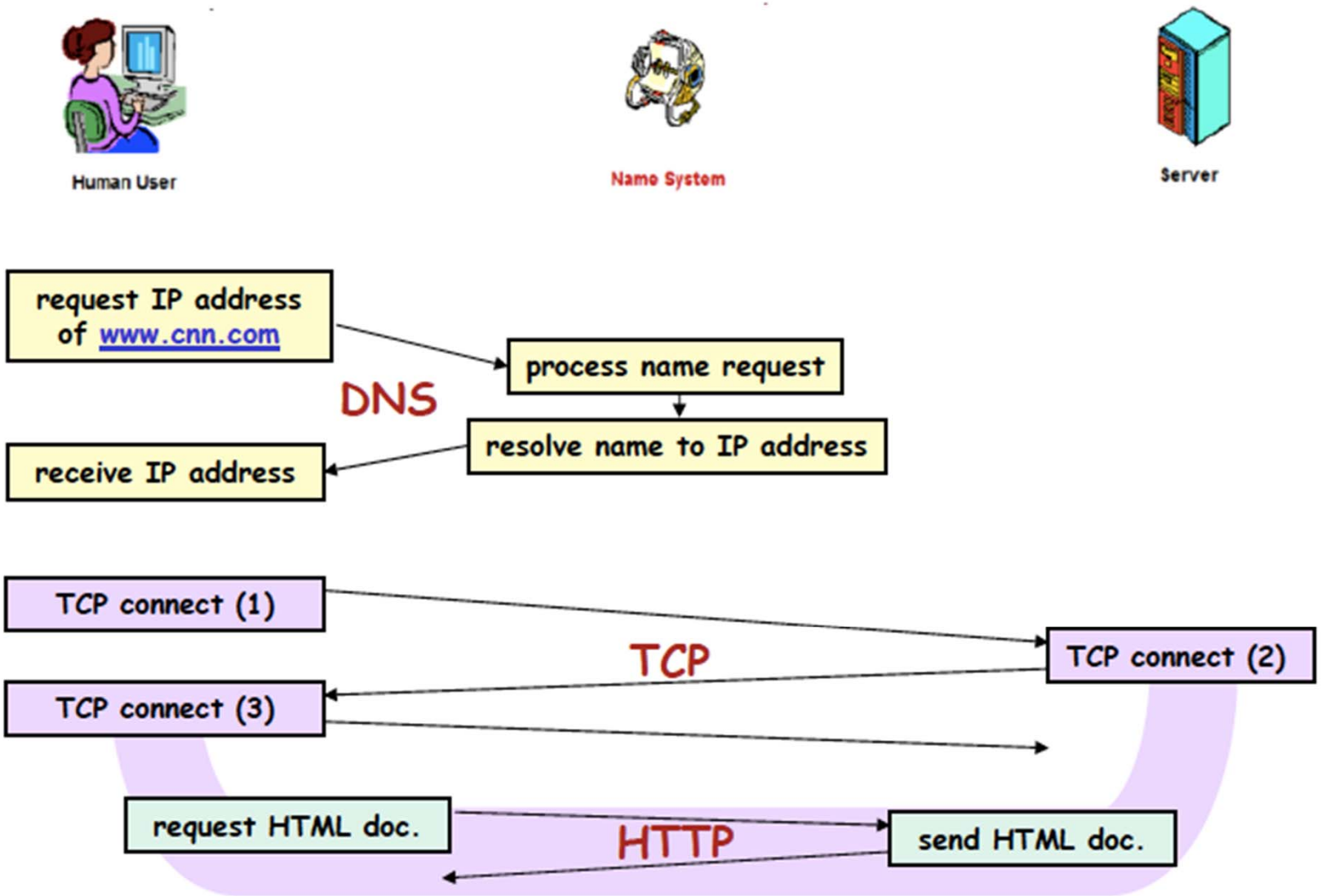
- As an educational resource when learning about protocols
- Analyzing the operations of applications and protocols they rely upon
- Network intrusion detection
- Debugging in the development stage of network programming
- Reverse-engineering of protocols in order to write supporting programs

Common Network Analyzer

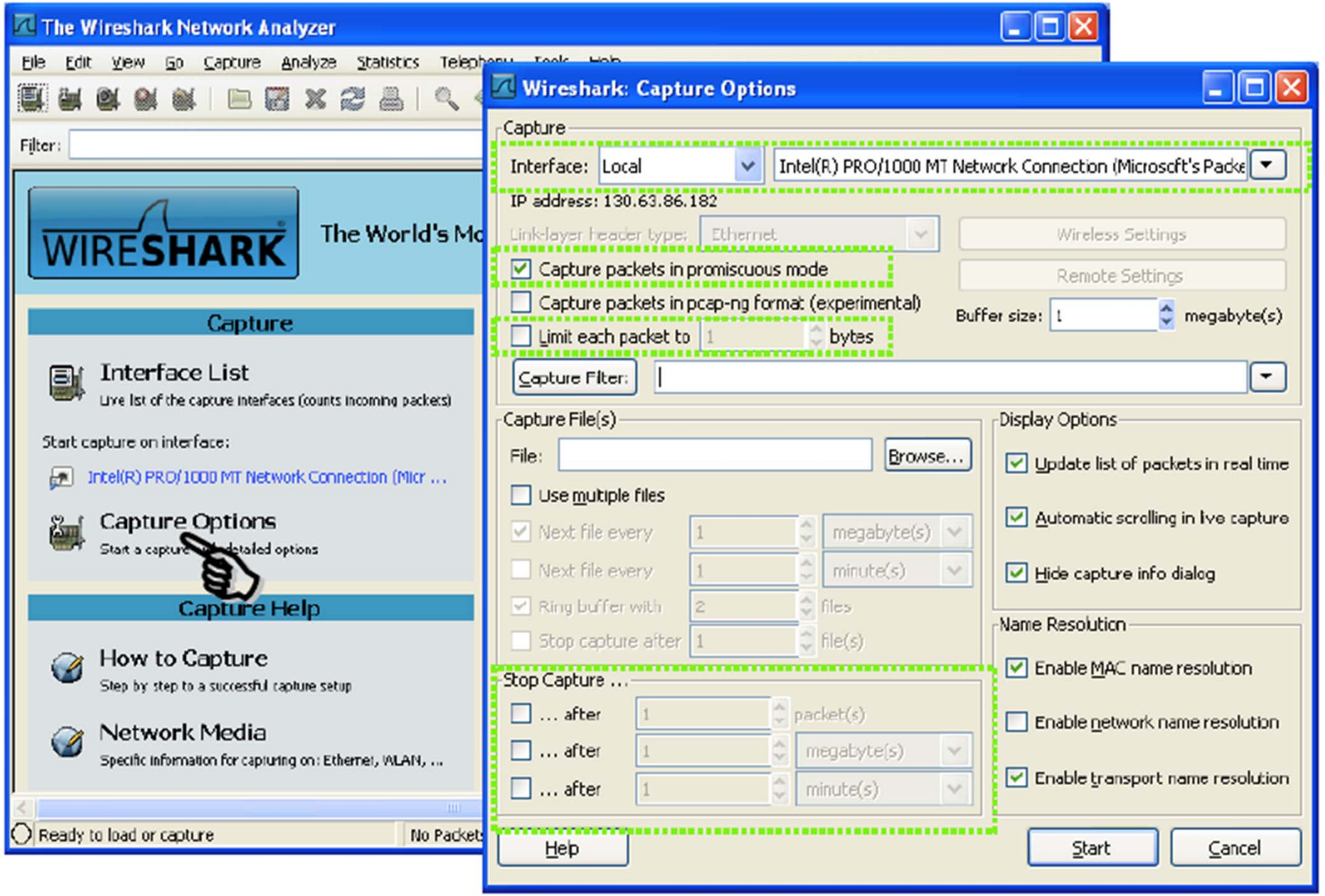
- Wireshark – freeware, runs on different platforms, decodes hundreds of protocols
- Snort, WinDump/TcpDump, Dsniff, etc.

Wireshark Network Analyzer

Example: retrieval of www.cnn.com web page

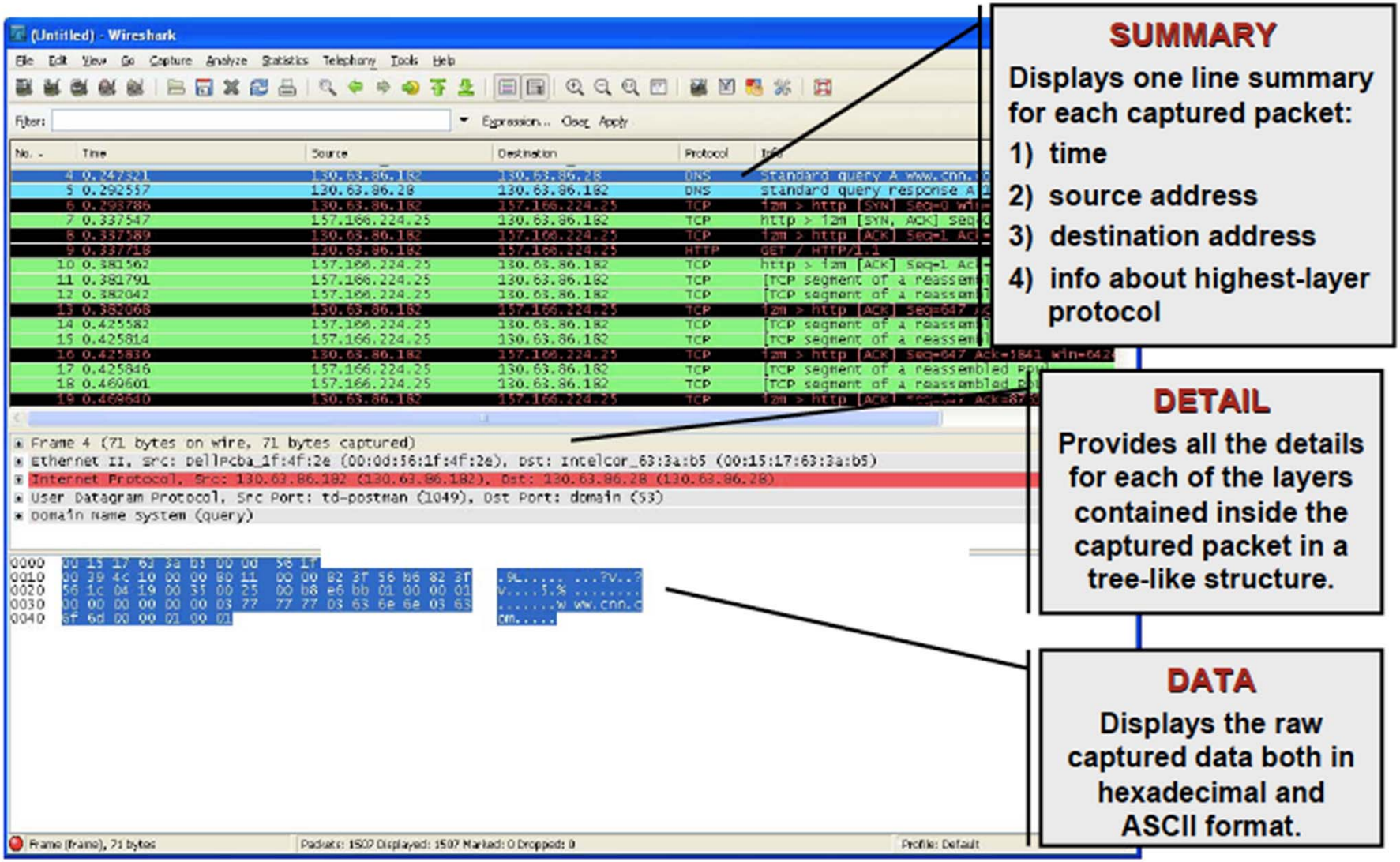


Wireshark Network Analyzer



Wireshark Network Analyzer

Wireshark Display Window – captures traffic in three panes



SUMMARY

Displays one line summary for each captured packet:

1) time
2) source address
3) destination address
4) info about highest-layer protocol

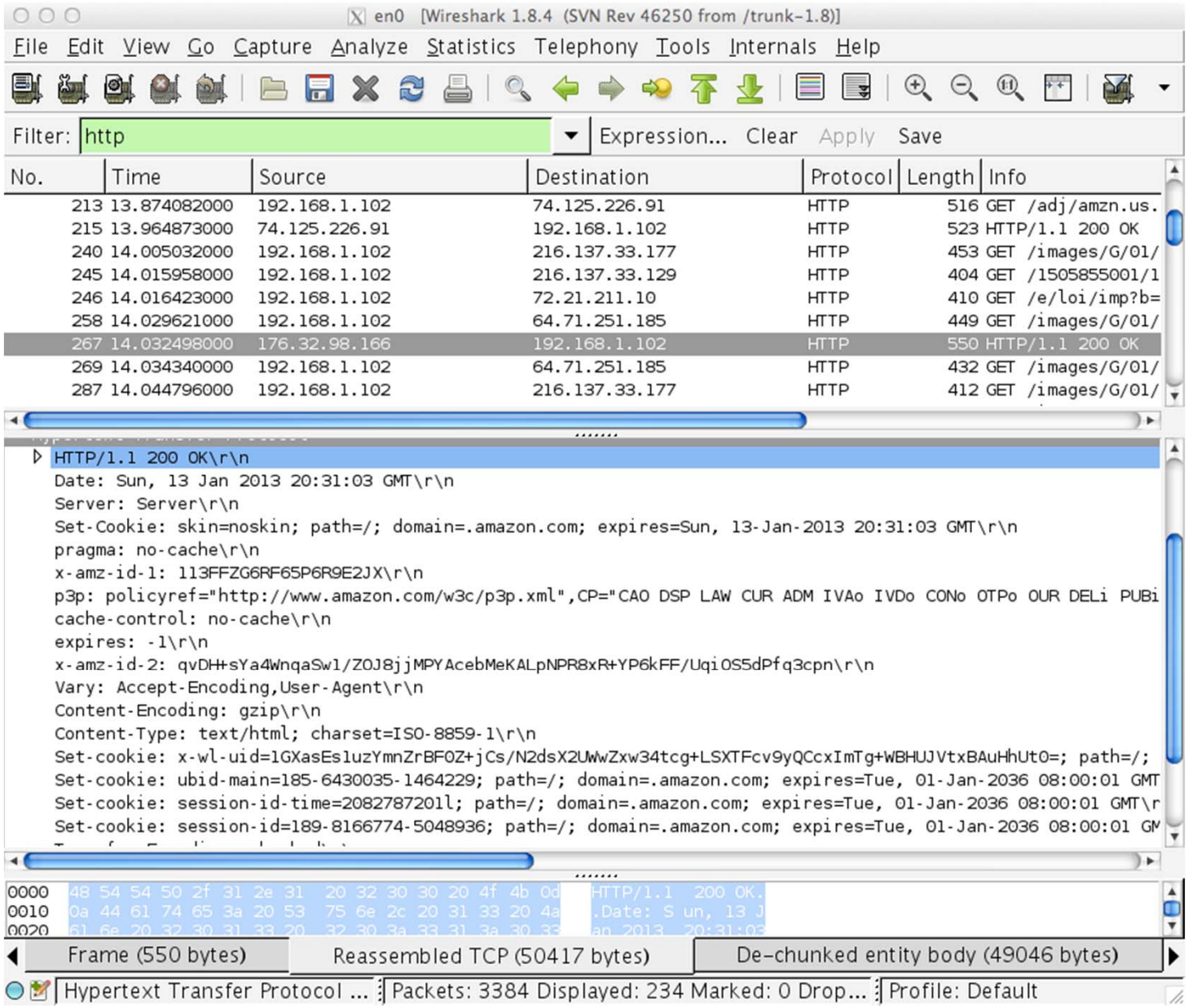
DETAIL

Provides all the details for each of the layers contained inside the captured packet in a tree-like structure.

DATA

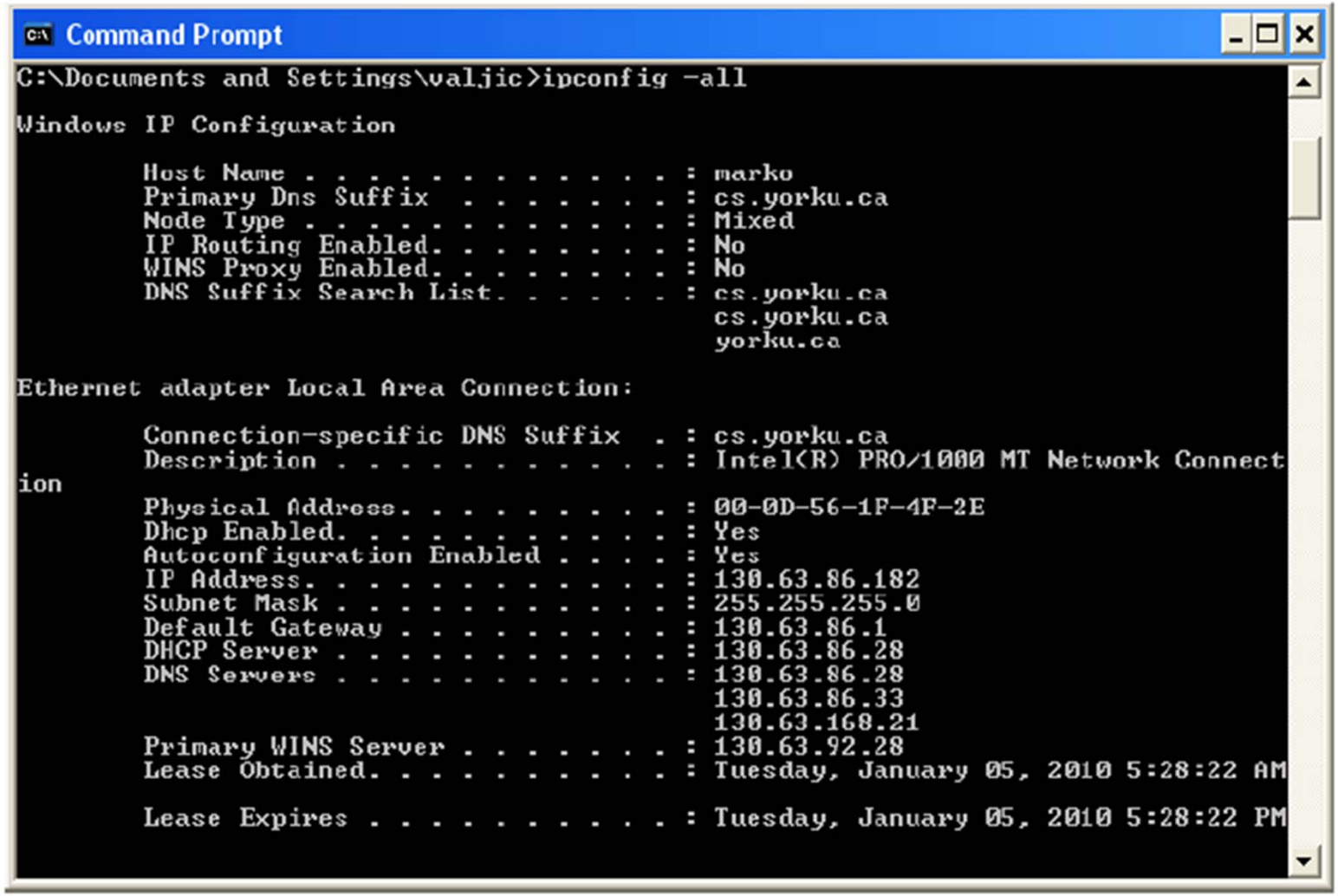
Displays the raw captured data both in hexadecimal and ASCII format.

Wireshark Network Analyzer



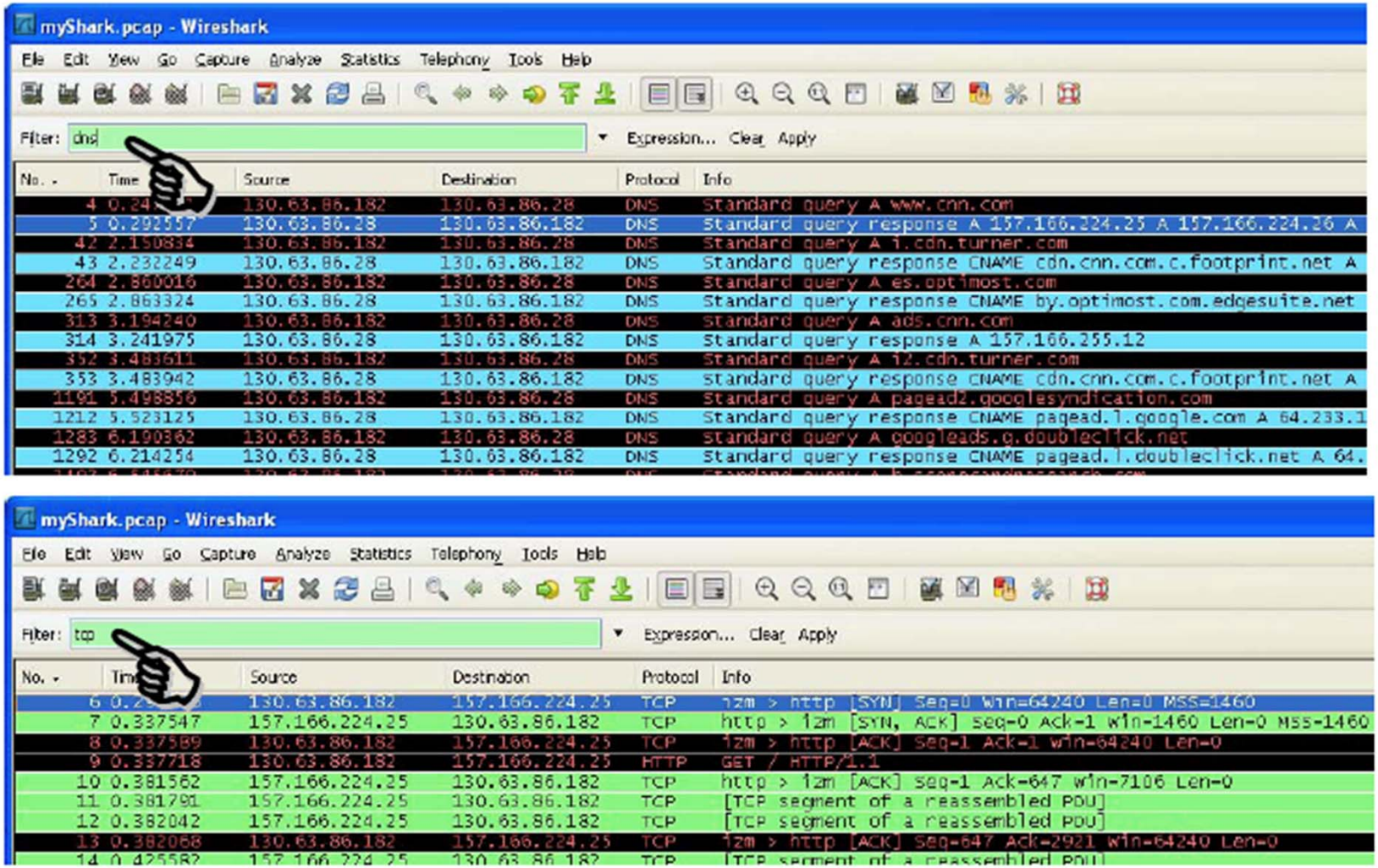
Wireshark Network Analyzer

ipconfig –all – reveals own MAC & IP address, and IP address of DNS & DHCP server



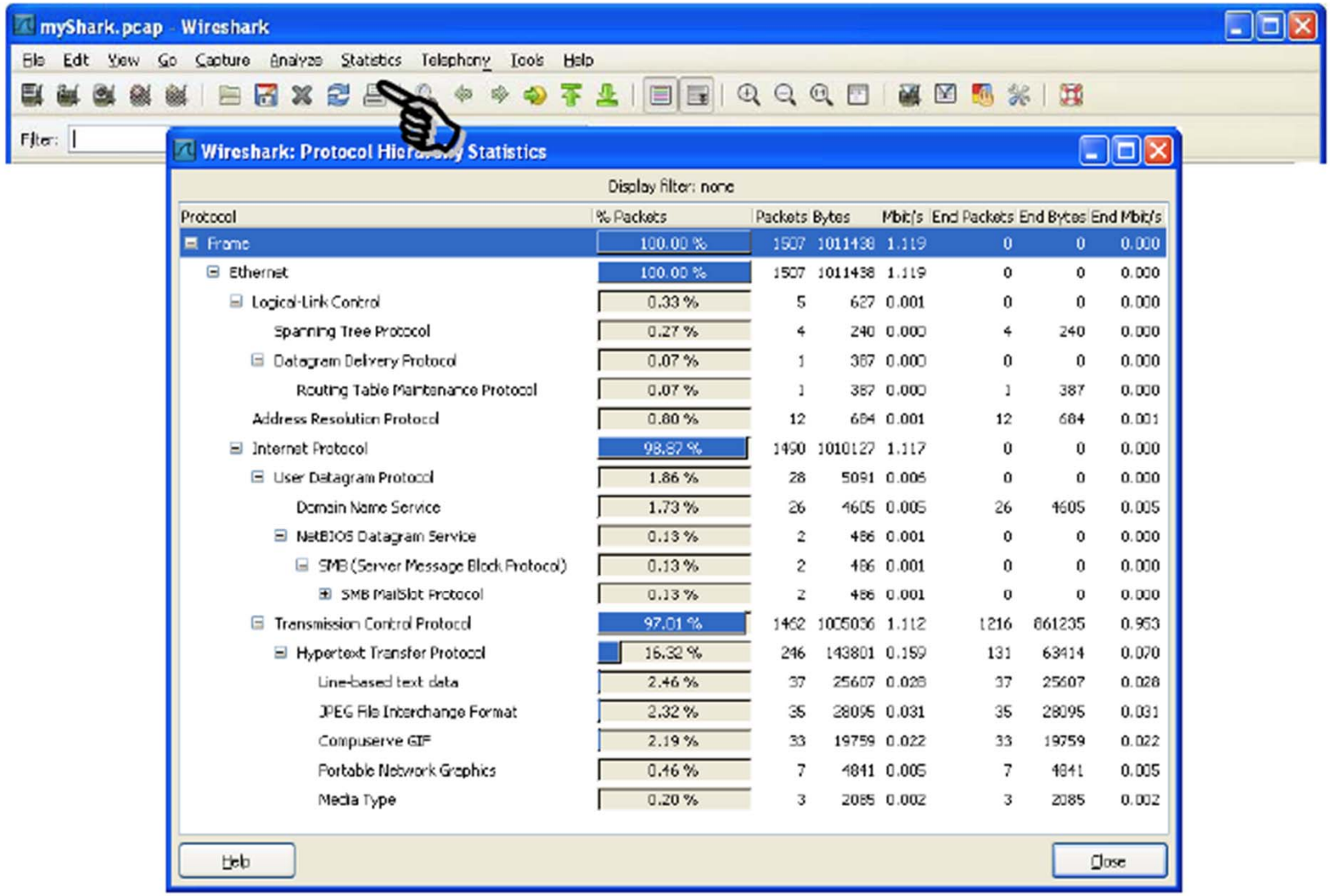
Wireshark Network Analyzer

Wireshark Display Filter Feature



Wireshark Network Analyzer

Wireshark Statistics Summary Feature



Wireshark Installation

- www.wireshark.org