Packet Analysis with Wireshark

EE3204: Computer Communication Networks I

Mehul Motani

motani@nus.edu.sg

* The material is adapted from J.F. Kurose & K.W. Ross, "*Computer Networking: A Top-Down Approach Featuring the Internet*", 4rd Edition.

Packet Analysis and Sniffing

- Currently data travels around the network like a train. With a packet sniffer, you can capture the data and look inside the packets to see what is actually moving around the network.
- Process of capturing, decoding, and analyzing network traffic
  - Why is the network slow
  - What is the network traffic pattern
  - How is the traffic being shared between nodes
- Also known as traffic analysis, protocol analysis, sniffing, network analysis, eavesdropping, etc.
- Common packet analyzers
  - Wireshark
  - Ethereal
  - Windump

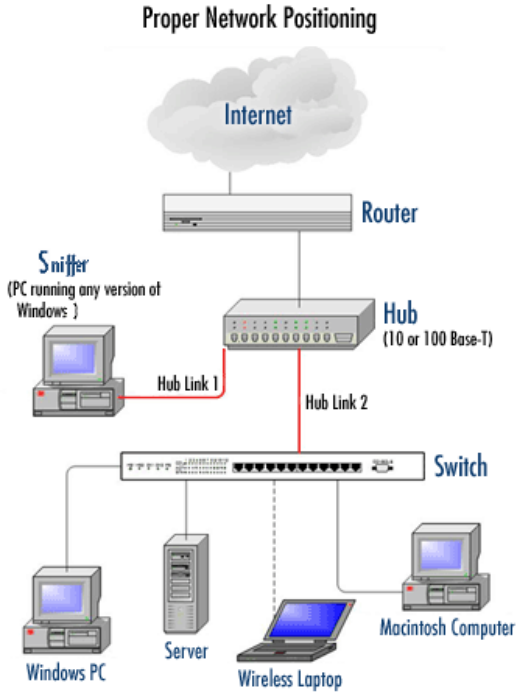
Who Uses Packet Analyzers

- System administrators
  - Understand system problems and performance
  - Intrusion detection
- Malicious individuals (intruders)
  - Capture cleartext data
  - Passively collect data on vulnerable protocols
    - FTP, POP3, IMAP, SMATP, rlogin, HTTP, etc.
    - Capture VoIP data
  - Mapping the target network
  - Traffic pattern discovery
  - Actively break into the network (backdoor techniques)

Packet Capturer + Packet Analyzer

- Packet Sniffer = Packet Capturer + Packet Analyzer
- A combination of hardware and software tools what can detect, decode, and manipulate traffic on the network
- Packet Capture module
  - Receives a copy of every link-layer frame that is sent from or received by your computer
  - Libpcap (UNIX) and Winpcap (Windows)
- Packet Analyzer
  - Displays the contents of all fields within a protocol message
  - Understands the structure of all messages exchanged by protocols

Packet Sniffer in the Network



Packet Sniffer

- Captures messages being sent/received
- Store and/or display the contents of the various protocol fields in these captured messages.
- A packet sniffer itself is passive.
- Packets are never explicitly addressed to the packet sniffer.

What is Wireshark?

- An free open source packet analyzer
- Captures network packets (link layer PDUs)
- Displays detailed PDU information
- Decodes over 750 protocols
- Compatible with many other sniffers
- Plenty of online resources are available
- Supports command-line and GUI interfaces
- Formerly called ***Ethereal***

Why use Wireshark ?

- Troubleshoot a network.
- Debug protocol implementations
- Detect network intrusion attempts.
- Monitor the network usage and filter for suspicious content
- Spy on other network users and collect their passwords. ← **Don't do this!**

Packet Analyzer

Is Wireshark a Packet Analyzer or Packet Capturer

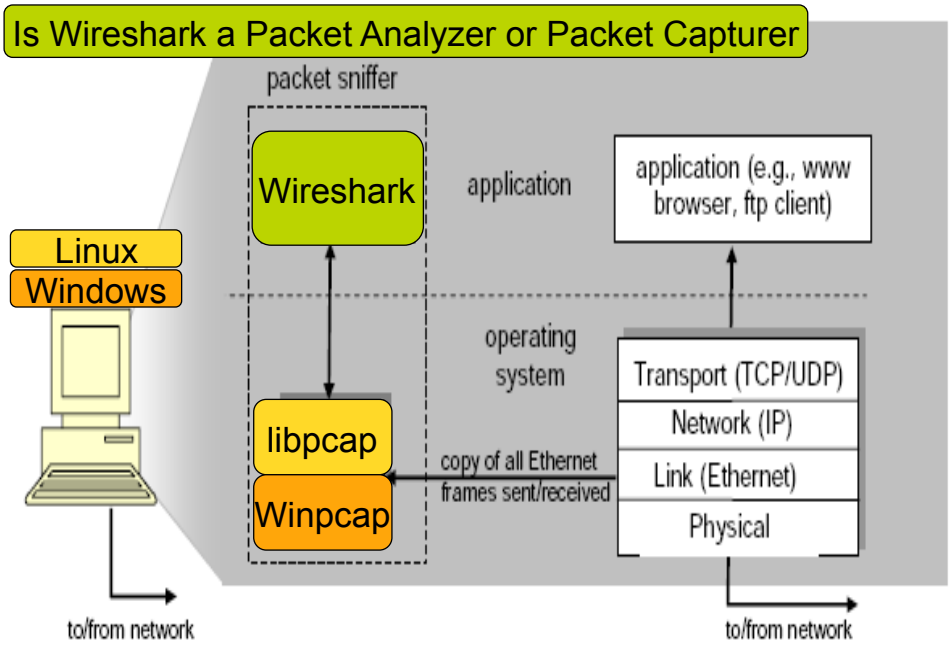


Figure 1: Packet sniffer structure

Wireshark User Interface

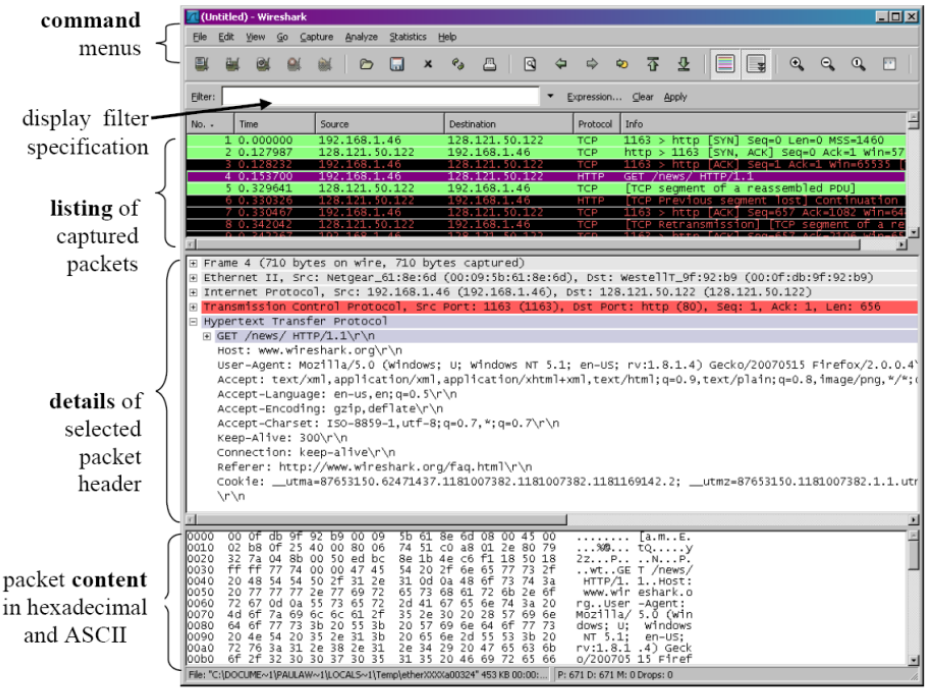
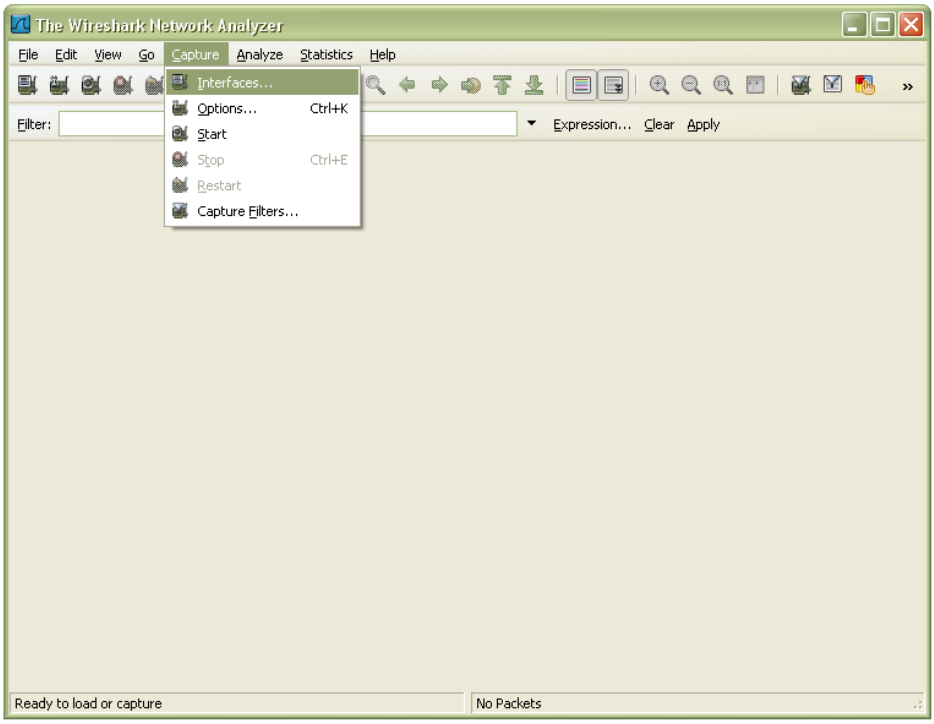
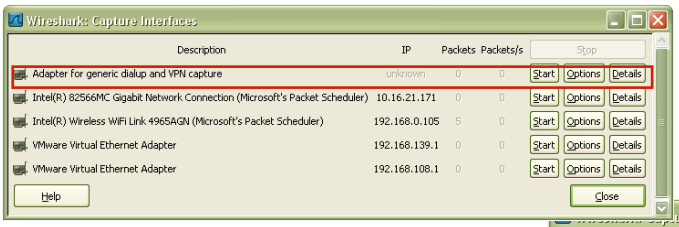


Figure 2: Wireshark Graphical User Interface

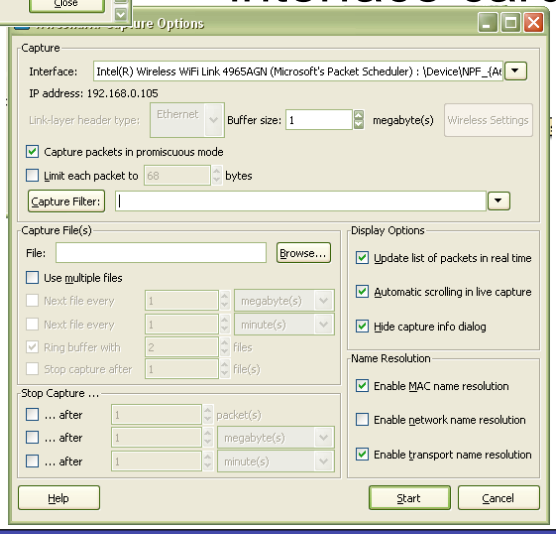
Running Wireshark



Running Wireshark



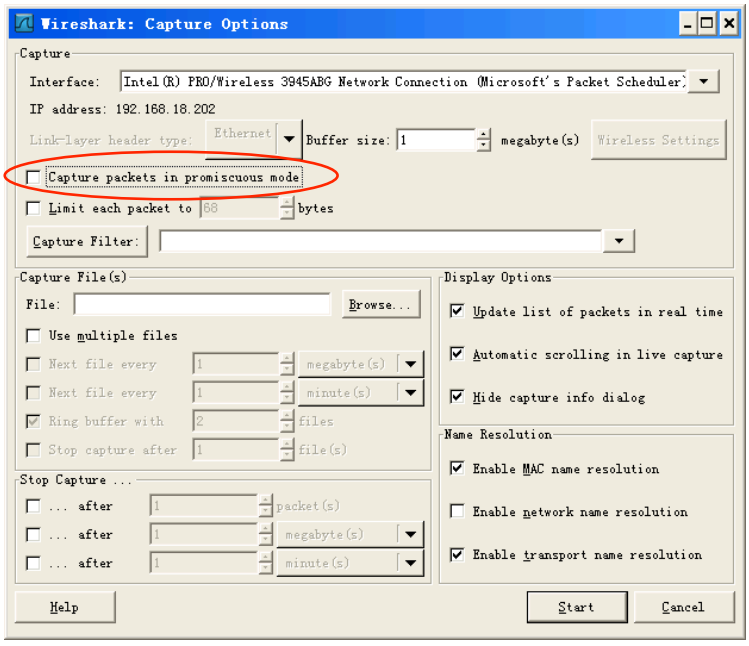
•Choose a network interface card

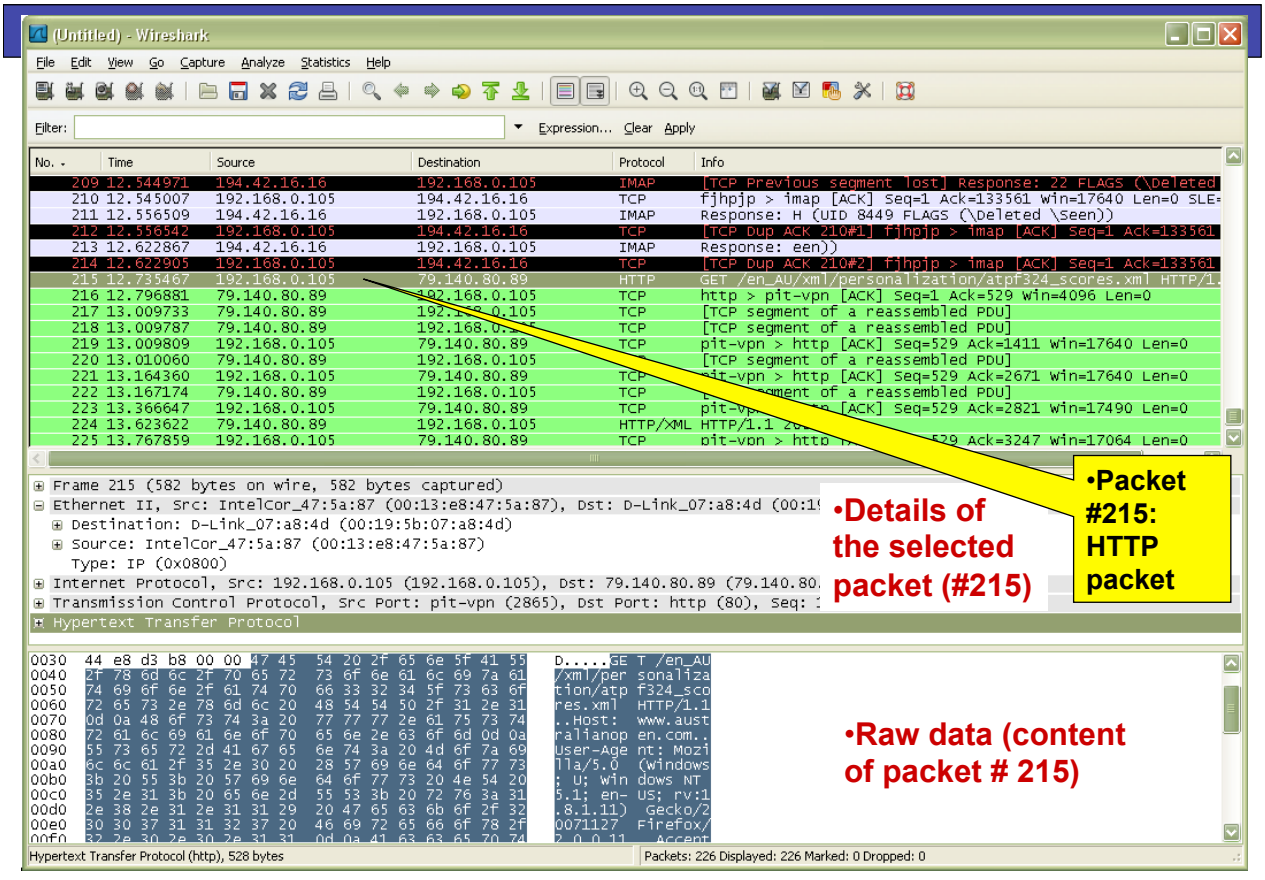


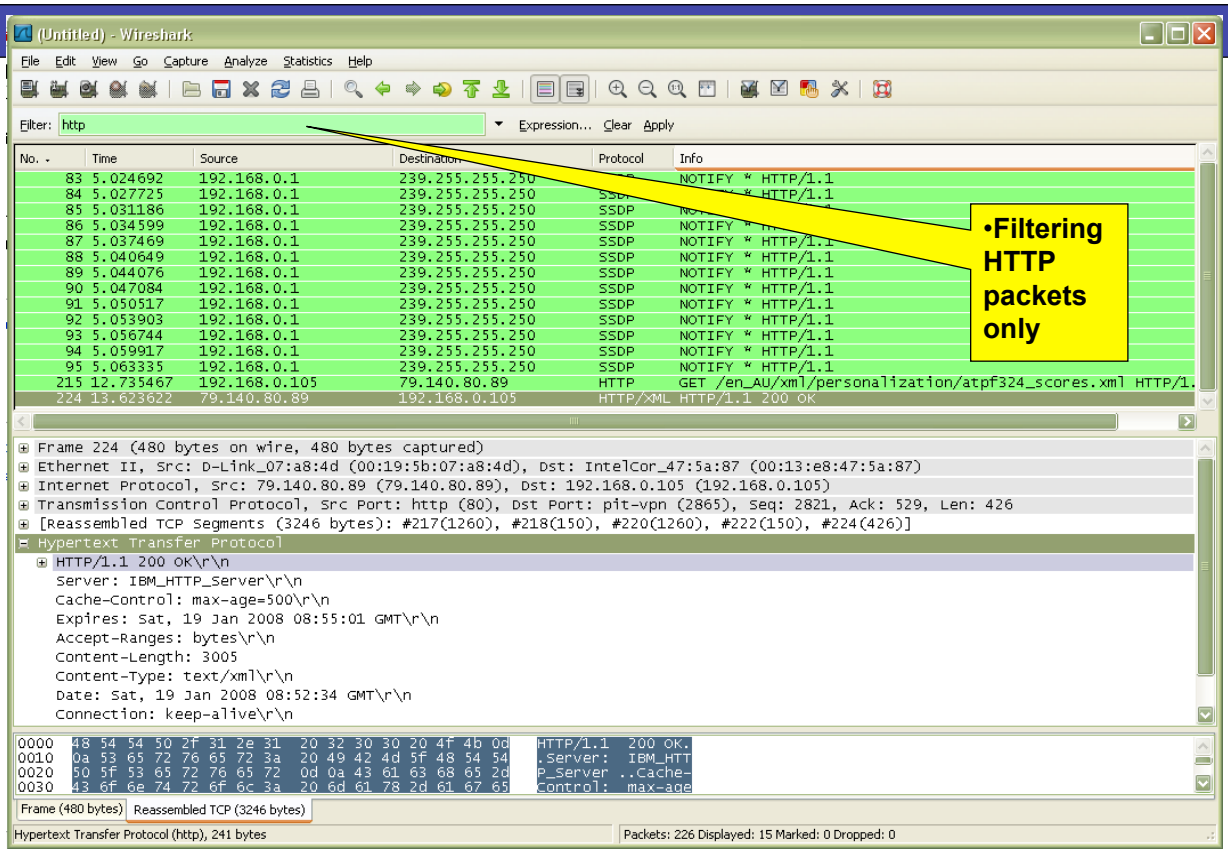
•Sniffing parameters on the selected network interface card

Promiscuous mode

This checkbox puts the interface in **promiscuous** mode when capturing, else Wireshark only captures packets going to or from your computer (not all packets on your LAN segment).





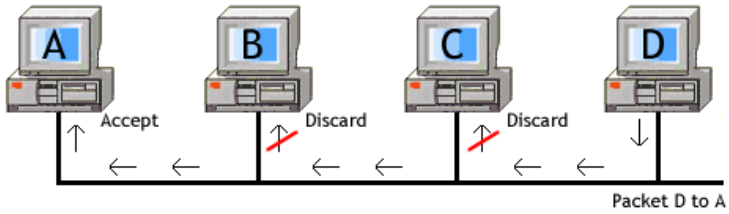


Other features

- Filters can be setup to capture or display the packets of the desired patterns
- Captured packets can be stored in disk for later re-loading and analyzing
- Supported OS: Win32, Linux, FreeBSD, Solaris, Mac OS

How is it possible to capture other users packets?

- Ethernet was built around a "shared" principle: all machines on a local network share the same wire. So, all machines are able to "see" all the traffic on the same wire. Thus, Ethernet hardware is built with a "filter" that ignores all traffic that doesn't belong to it.
- It does this by ignoring all frames whose MAC address doesn't match. If you put your Ethernet Hardware into "promiscuous mode“, you will deactivate the mentioned “filter” and start accepting packets rather than discarding them...

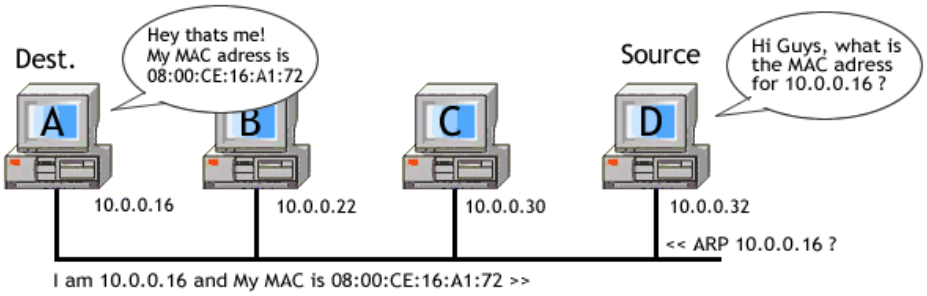


Media Access Control (MAC) Address

- MAC Address is a 12-digit hex number (6 bytes or 48 bits), embedded in your Ethernet card, that uniquely identifies you over the Ethernet.
- The first 24-bits identify the vendor of the Ethernet board, the second 24-bits is a serial number assigned by the vendor.
- Example MAC address : 00:C0:49:A7:25:45
- 00:C0:49 is Registered for the vendor U.S Robotics. This number is called OUI ("Organizationally Unique Identifier").
- You can find the list of vendor/OUI codes at http://standards.ieee.org/regauth/oui/
- Windows: Run the program "ipconfig /all" from the command-line to see the MAC address for your adapter.
- Linux: Run the program "ifconfig". To see the MAC address for your adapter.

How do hosts communicate over Ethernet?

- Each Host in the same ethernet network has an IP adress.
- In order to send data to a destination host, first we have to know the MAC Adress for the destination host. To get the IP adress of the destination, the source broadcasts an ARP packet over the network. ARP stands for Adress Resolution Protocol. (RFC 826)



Protocol	Protocol Adress	Hardware Address (MAC)
IP	10.1.32.5	BA D0 BE EF FF FA
IP	10.1.32.9	BA D0 BE EF FF 03

Download and Installation

- Download Wireshark
  - http://www.wireshark.org/download.html
- Support
  - User's Guide: http://www.wireshark.org/docs/wsug_html_chunked/index.html
  - Wiki: http://wiki.wireshark.org/
- WinPcap – For reference only
  - Wireshark automatically installs WinPcap
  - http://www.winpcap.org/install/default.htm