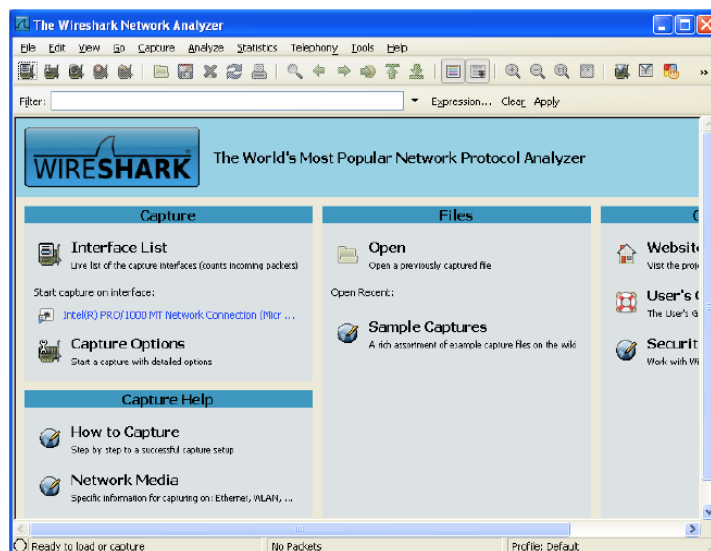


# CSE 3214: Computer Network Protocols and Applications

## —Network Monitoring & Protocol Analysis

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

## Wireshark



2

## 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”

3

## 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

4

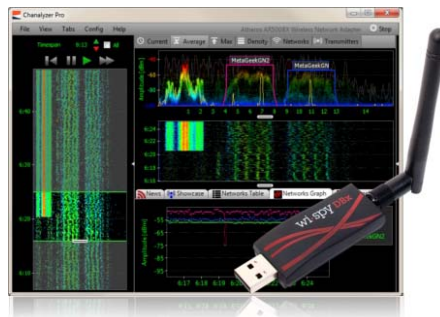
## Network Analyzer Applications

- 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

5

## Common Network Analyzer

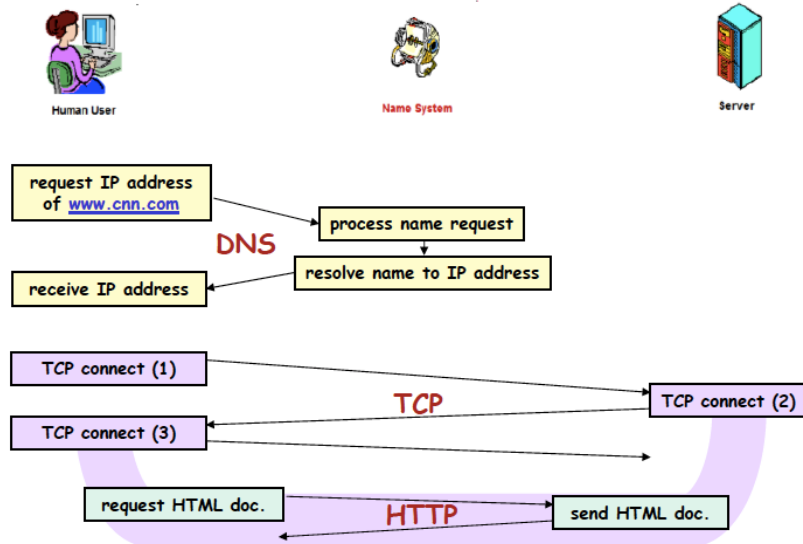
- Wireshark – freeware, runs on different platforms, decodes hundreds of protocols
- Snort, WinDump/TcpDump, Dsniff, etc.



6

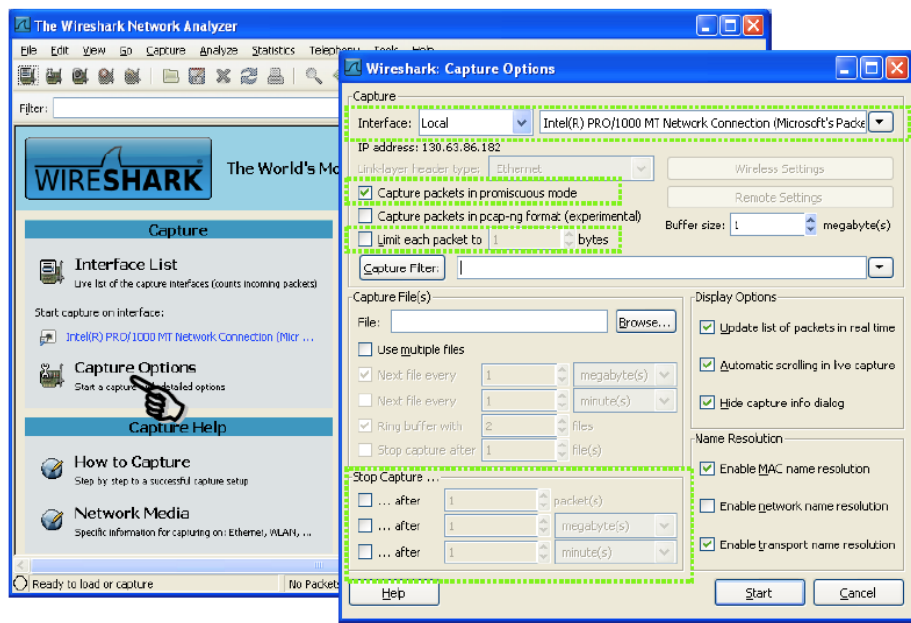
## Wireshark Network Analyzer

Example: retrieval of [www.cnn.com](http://www.cnn.com) web page



7

## Wireshark Network Analyzer





## Wireshark Network Analyzer

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

```

C:\Documents and Settings\marko>ipconfig /all

Windows IP Configuration

Host Name . . . . . : marko
Primary Dns Suffix . . . . . : cs.yorku.ca
Node Type . . . . . : Mixed
IP Routing Enabled. . . . . : No
WINS Proxy Enabled. . . . . : No
DNS Suffix Search List. . . . . : cs.yorku.ca
                                cs.yorku.ca
                                yorku.ca

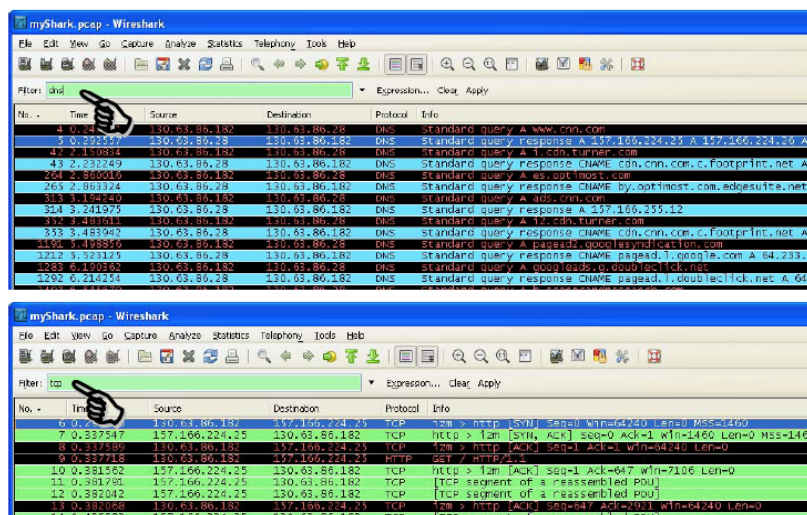
Ethernet adapter Local Area Connection:

    Connection-specific DNS Suffix  . : cs.yorku.ca
    Description . . . . . : Intel(R) PRO/1000 MT Network Connect
    Physical Address. . . . . : 00-0D-56-1F-4F-2E
    Dhcp Enabled. . . . . : Yes
    Autoconfiguration Enabled . . . . : Yes
    IP Address. . . . . : 130.63.86.182
    Subnet Mask . . . . . : 255.255.255.0
    Default Gateway . . . . . : 130.63.86.1
    DHCP Server . . . . . : 130.63.86.28
    DNS Servers . . . . . : 130.63.86.28
                          130.63.86.33
                          130.63.168.21
    Primary WINS Server . . . . . : 130.63.92.28
    Lease Obtained. . . . . : Tuesday, January 05, 2010 5:28:22 AM
    Lease Expires . . . . . : Tuesday, January 05, 2010 5:28:22 PM
  
```

11

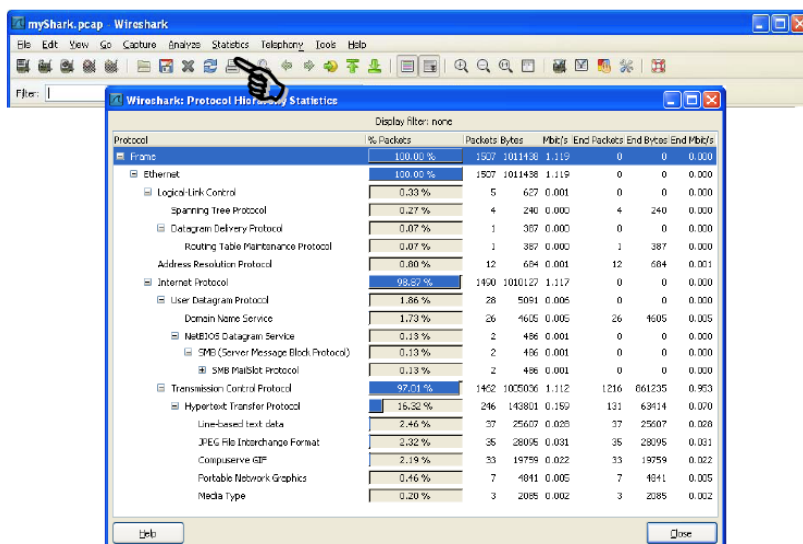
## Wireshark Network Analyzer

### Wireshark Display Filter Feature



# Wireshark Network Analyzer

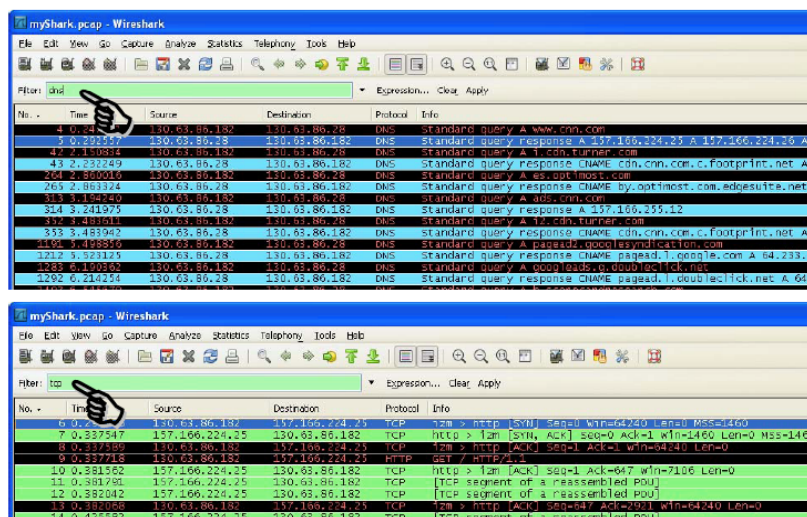
## Wireshark Statistics Summary Feature



13

# Wireshark Network Analyzer

## Wireshark Display Filter Feature



# Wireshark Installation

- [www.wireshark.org](http://www.wireshark.org)



15