

CSE 3214: Computer Network Protocols and Applications

–Network Monitoring & Protocol Analysis

Dr. Peter Lian, Professor
Department of Computer Science and Engineering
York University

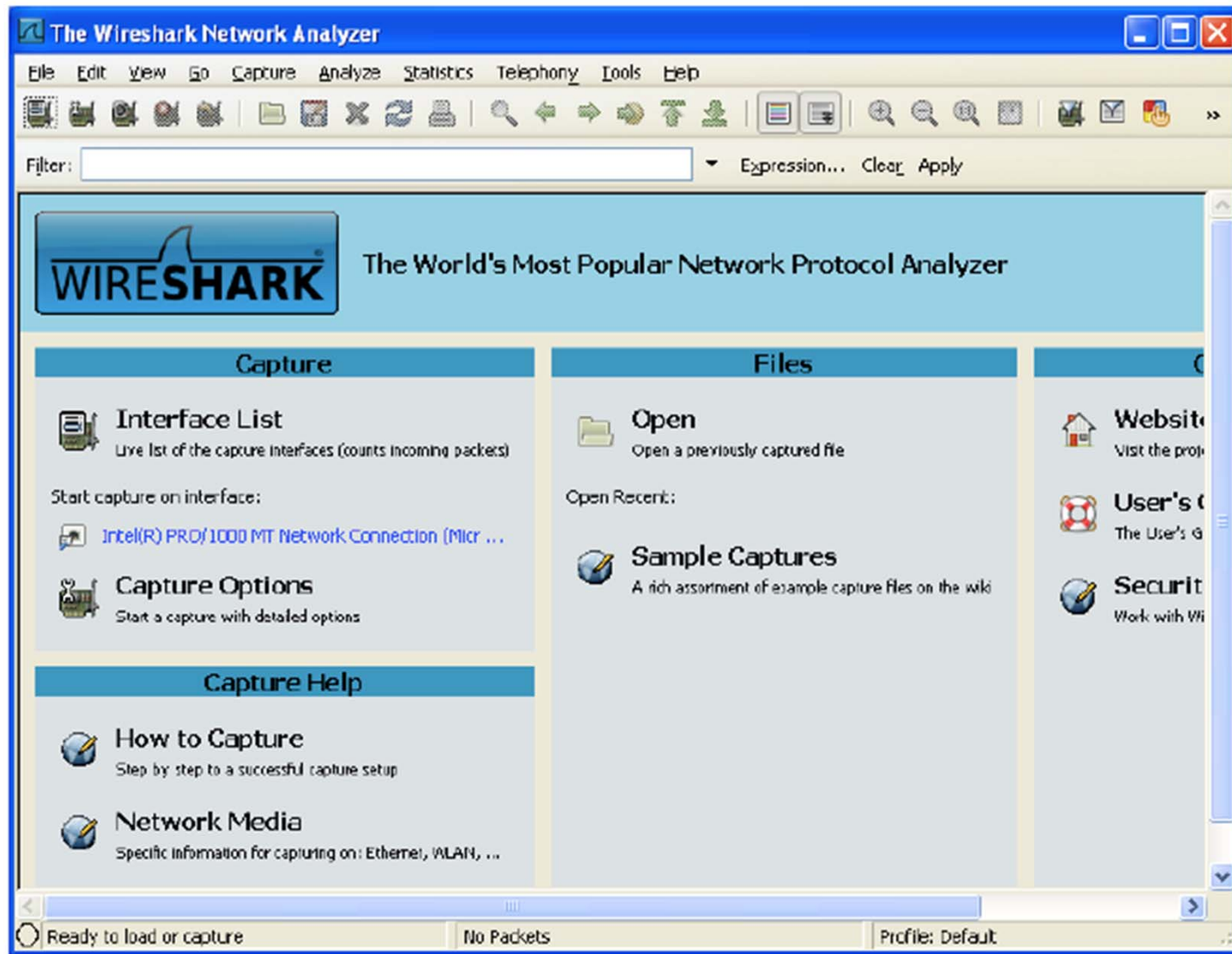
Email: peterlian@cse.yorku.ca

Office: 1012C Lassonde Building

Course website:

http://wiki.cse.yorku.ca/course_archive/2012-13/W/3214

Wireshark



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



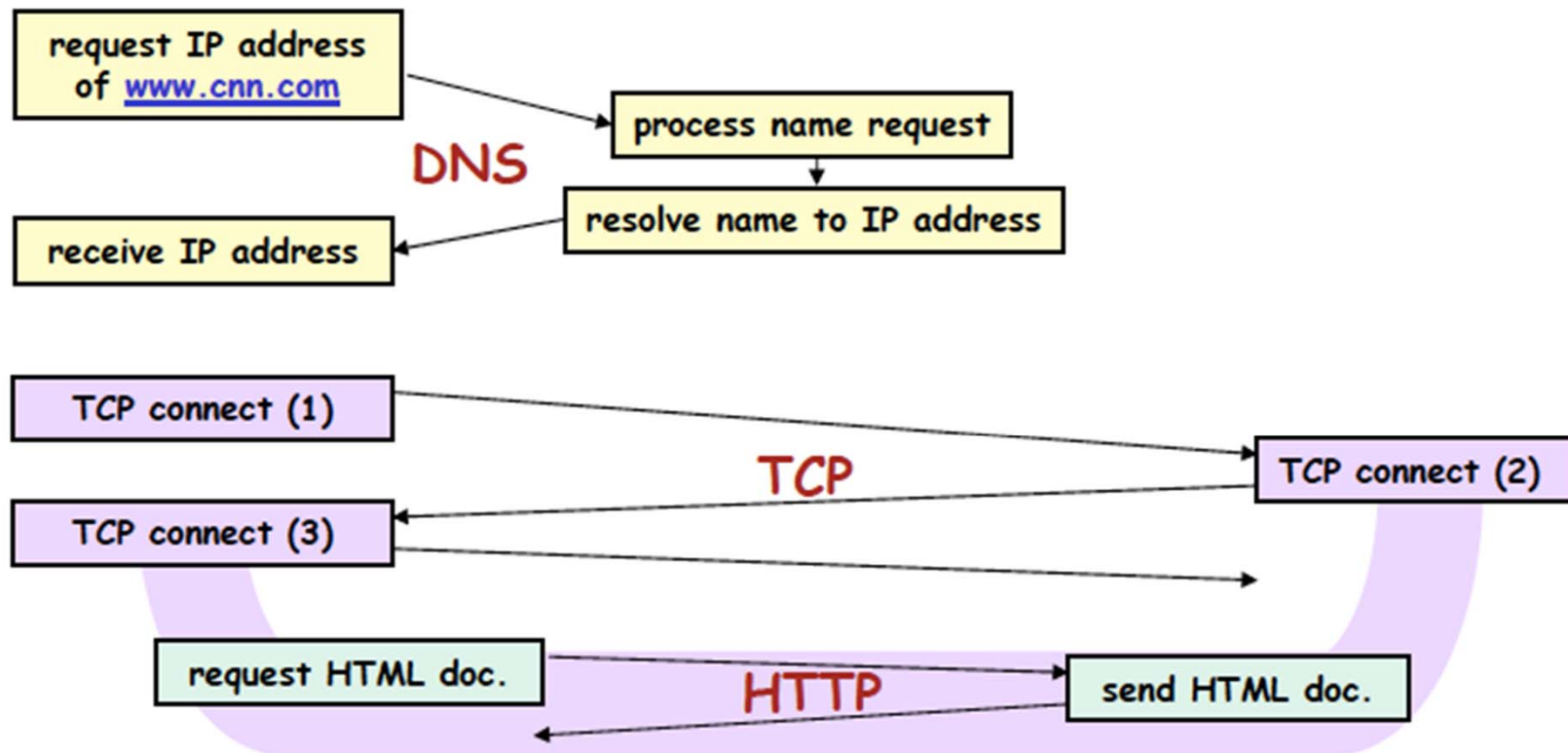
Human User



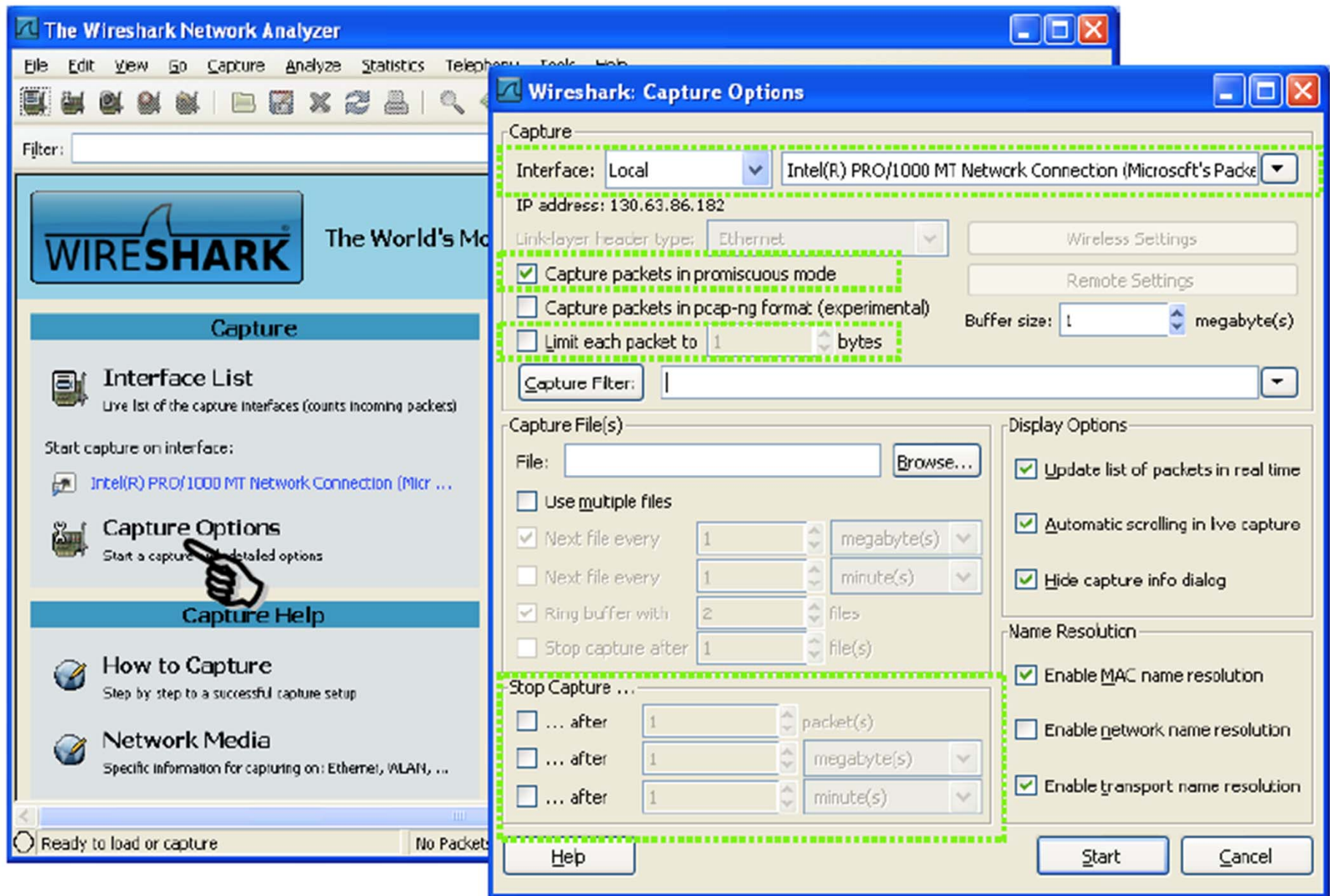
Name System



Server



Wireshark Network Analyzer



Wireshark Network Analyzer

Wireshark Display Window – captures traffic in three panes

The screenshot shows the Wireshark interface with the following panes:

- Summary Pane:** Displays a list of captured packets with columns for No., Time, Source, Destination, Protocol, and Info. The selected packet (No. 4) is highlighted in blue.
- Detail Pane:** Provides a hierarchical view of the selected packet's structure. It shows the Ethernet II, Internet Protocol, User Datagram Protocol, and Domain Name System (query) layers.
- Data Pane:** Displays the raw captured data in hexadecimal and ASCII format.

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 1.8.4 (SVN Rev 46250 from /trunk-1.8)

Filter: **http** Expression... Clear Apply Save

No.	Time	Source	Destination	Protocol	Length	Info
213	13.874082000	192.168.1.102	74.125.226.91	HTTP	516	GET /adj/amzn.us.
215	13.964873000	74.125.226.91	192.168.1.102	HTTP	523	HTTP/1.1 200 OK
240	14.005032000	192.168.1.102	216.137.33.177	HTTP	453	GET /images/G/01/
245	14.015958000	192.168.1.102	216.137.33.129	HTTP	404	GET /1505855001/1
246	14.016423000	192.168.1.102	72.21.211.10	HTTP	410	GET /e/loi/imp?b=
258	14.029621000	192.168.1.102	64.71.251.185	HTTP	449	GET /images/G/01/
267	14.032498000	176.32.98.166	192.168.1.102	HTTP	550	HTTP/1.1 200 OK
269	14.034340000	192.168.1.102	64.71.251.185	HTTP	432	GET /images/G/01/
287	14.044796000	192.168.1.102	216.137.33.177	HTTP	412	GET /images/G/01/

HTTP/1.1 200 OK\r\n

Date: Sun, 13 Jan 2013 20:31:03 GMT\r\n

Server: Server\r\n

Set-Cookie: skin=noskin; path=/; domain=.amazon.com; expires=Sun, 13-Jan-2013 20:31:03 GMT\r\n

pragma: no-cache\r\n

x-amz-id-1: 113FFZG6RF65P6R9E2JX\r\n

p3p: policyref="http://www.amazon.com/w3c/p3p.xml", CP="CAO DSP LAW CUR ADM IVAo IVDo CONo OTPo OUR DELi PUBi

cache-control: no-cache\r\n

expires: -1\r\n

x-amz-id-2: qvDH+sYa4WnqaSw1/ZOJ8jjMPYAcEbMeKALpNPR8xR+YP6kFF/Uqi0SSdPf q3cpn\r\n

Vary: Accept-Encoding, User-Agent\r\n

Content-Encoding: gzip\r\n

Content-Type: text/html; charset=ISO-8859-1\r\n

Set-cookie: x-wl-uid=1GXasEsluzYmnZrBF0Z+jCs/N2dsX2UwWzXw34tcg+LSXTFcv9yQCcxImTg+WBHUVtxBAuHhUt0=; path=/;

Set-cookie: ubid-main=185-6430035-1464229; path=/; domain=.amazon.com; expires=Tue, 01-Jan-2036 08:00:01 GMT

Set-cookie: session-id-time=2082787201l; path=/; domain=.amazon.com; expires=Tue, 01-Jan-2036 08:00:01 GMT\r

Set-cookie: session-id=189-8166774-5048936; path=/; domain=.amazon.com; expires=Tue, 01-Jan-2036 08:00:01 GM

0000 48 54 54 50 2f 31 2e 31 20 32 30 30 20 4f 4b 0d HTTP/1.1 200 OK.

0010 0a 44 61 74 65 3a 20 53 75 6e 2c 20 31 33 20 4a .Date: S un, 13 J

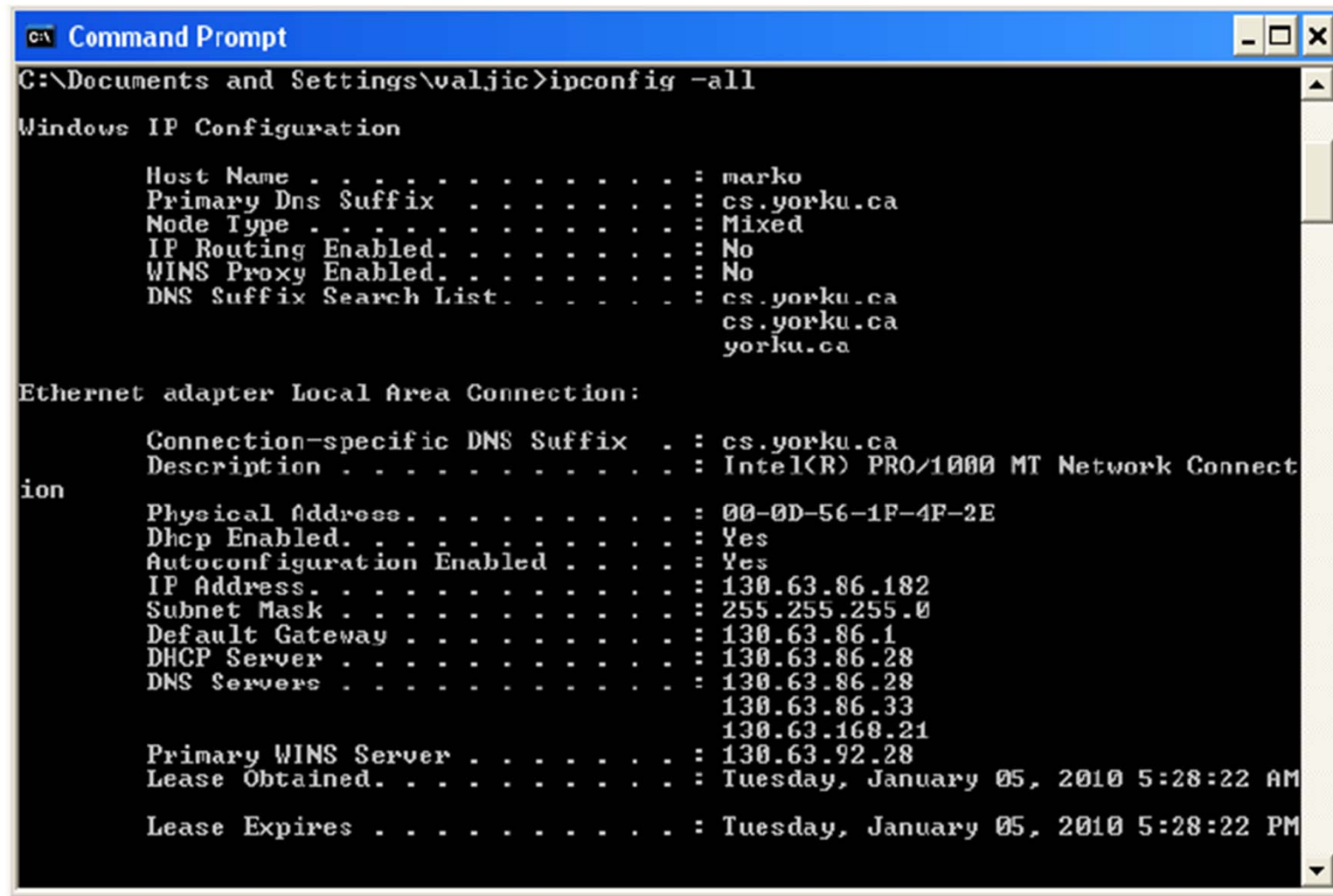
0020 61 6e 20 32 30 31 33 20 32 30 3a 33 31 3a 30 33 an 2013 20:31:03

Frame (550 bytes) Reassembled TCP (50417 bytes) De-chunked entity body (49046 bytes)

Hypertext Transfer Protocol ... Packets: 3384 Displayed: 234 Marked: 0 Drop... Profile: Default

Wireshark Network Analyzer

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



```
Command Prompt
C:\Documents and Settings\valjic>ipconfig -all

Windows IP Configuration

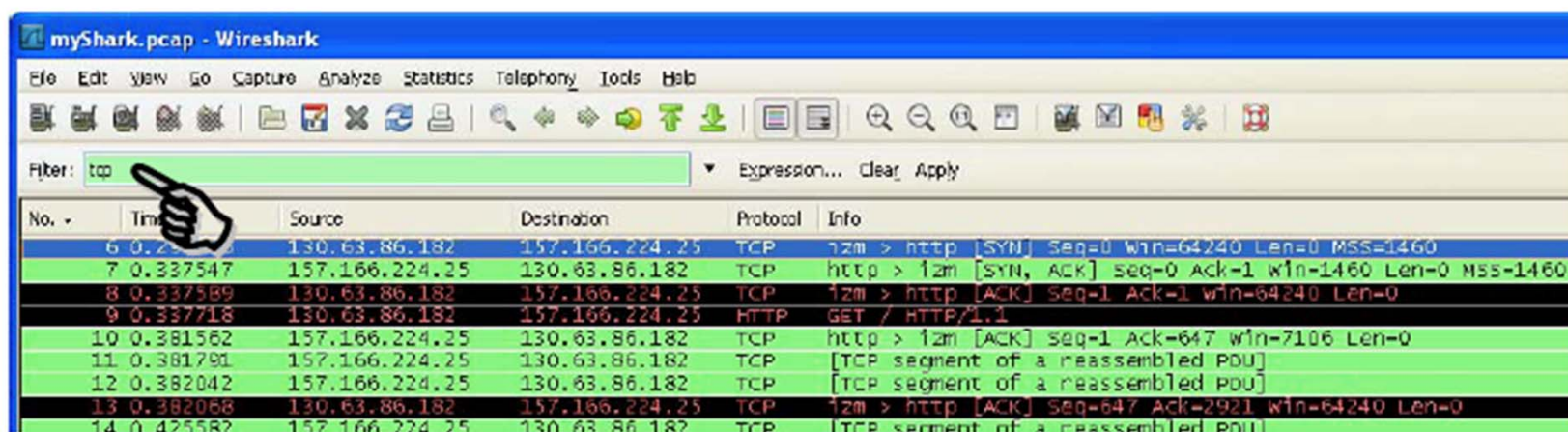
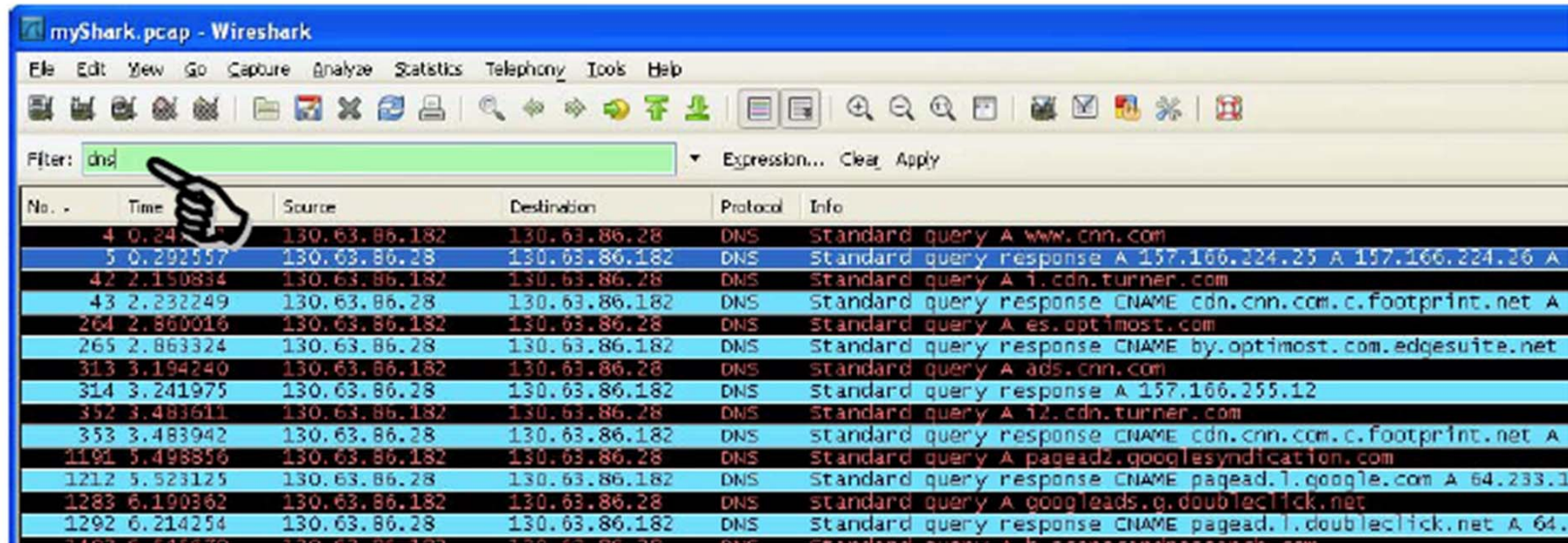
    Host Name . . . . . : marko
    Primary Dns Suffix . . . . . : cs.yorku.ca
    Node Type . . . . . : Mixed
    IP Routing Enabled. . . . . : No
    WINS Proxy Enabled. . . . . : No
    DNS Suffix Search List. . . . . : cs.yorku.ca
                                      cs.yorku.ca
                   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

Ethernet adapter Local Area Connection:

    Connection-specific DNS Suffix . : cs.yorku.ca
    Description . . . . . : Intel(R) PRO/1000 MT Network Connect
ion
    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
```

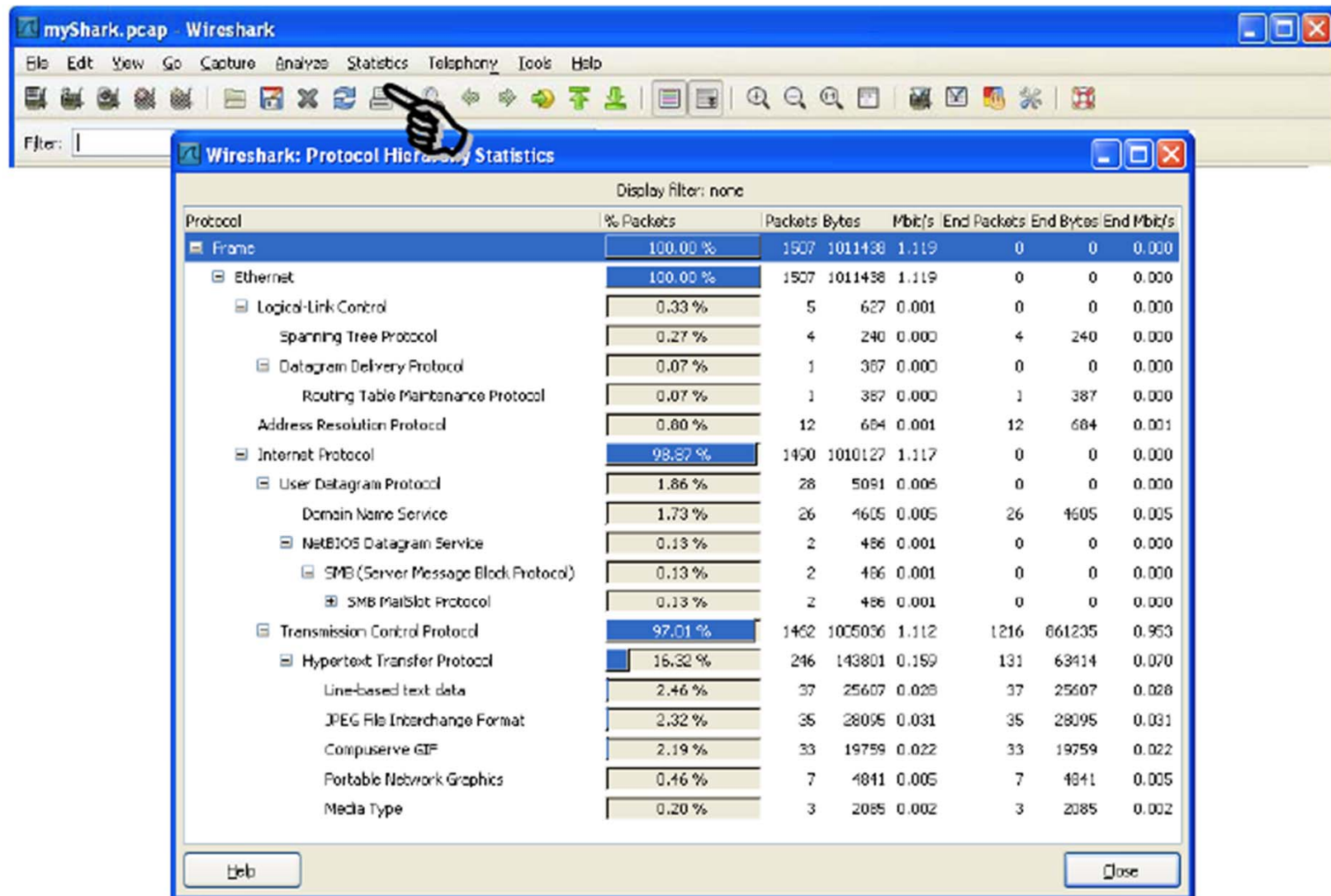
Wireshark Network Analyzer

Wireshark Display Filter Feature



Wireshark Network Analyzer

Wireshark Statistics Summary Feature



Wireshark Installation

- www.wireshark.org

