

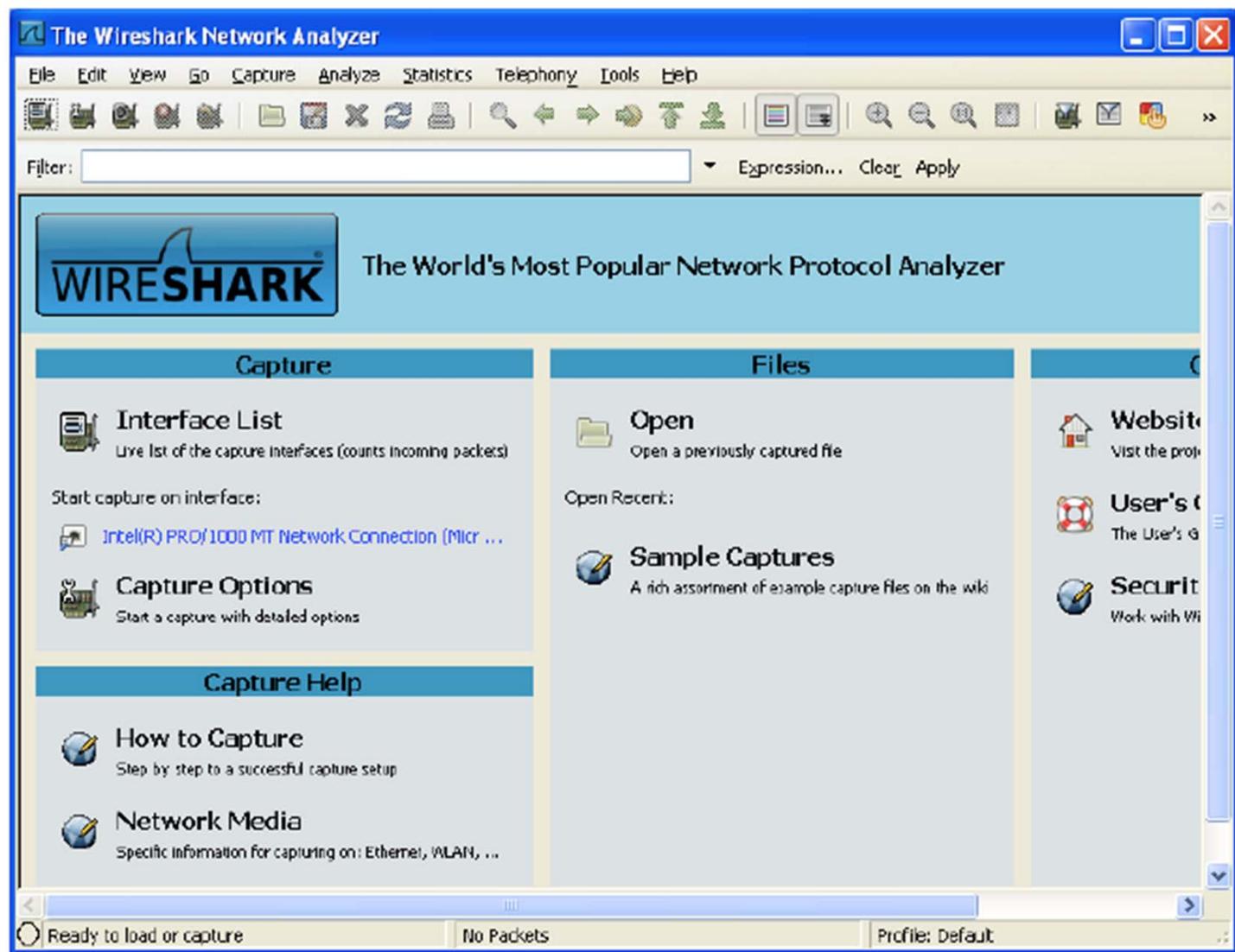
CSE 3214: Computer Network Protocols and Applications

—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

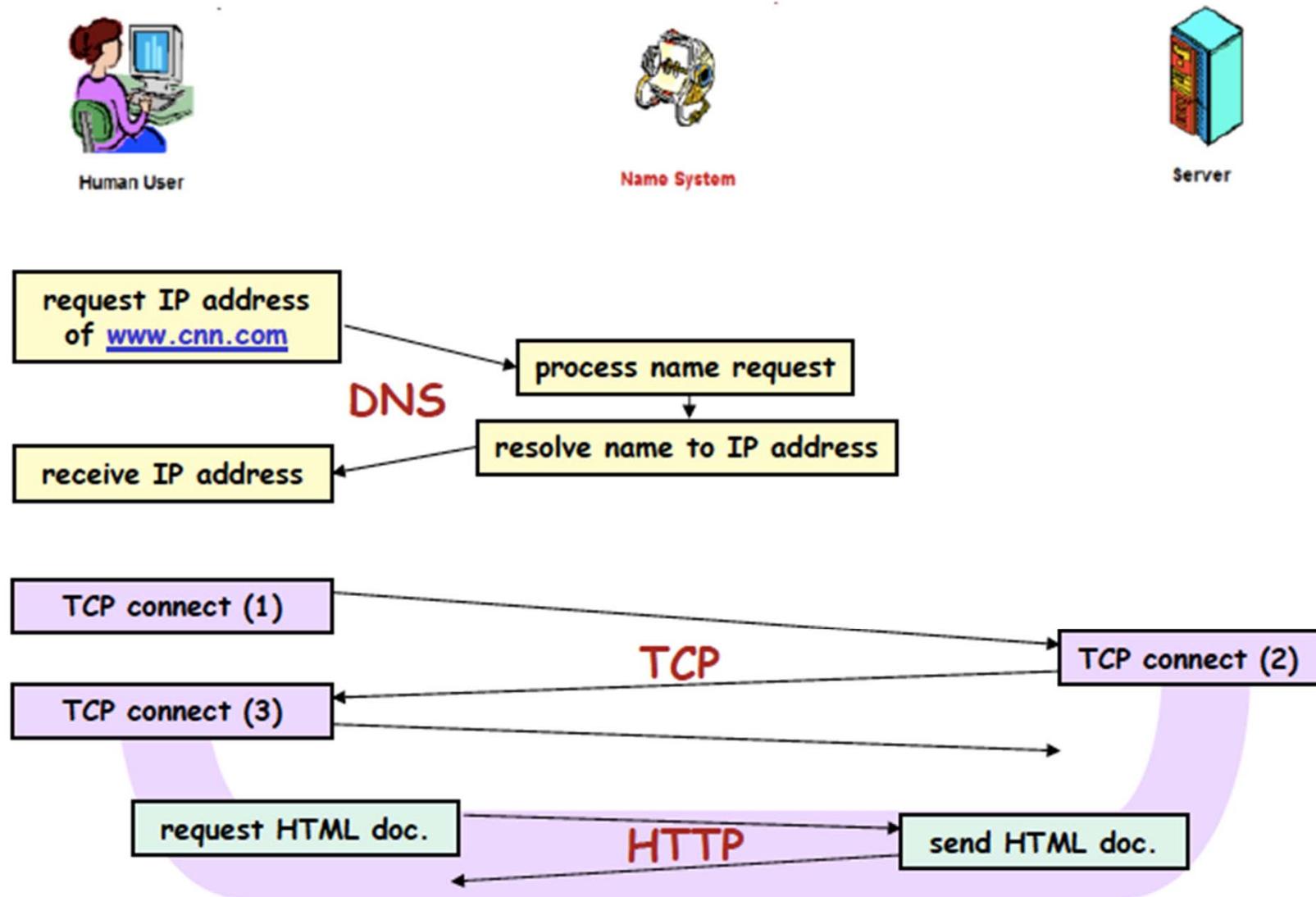
Common Network Analyzer

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

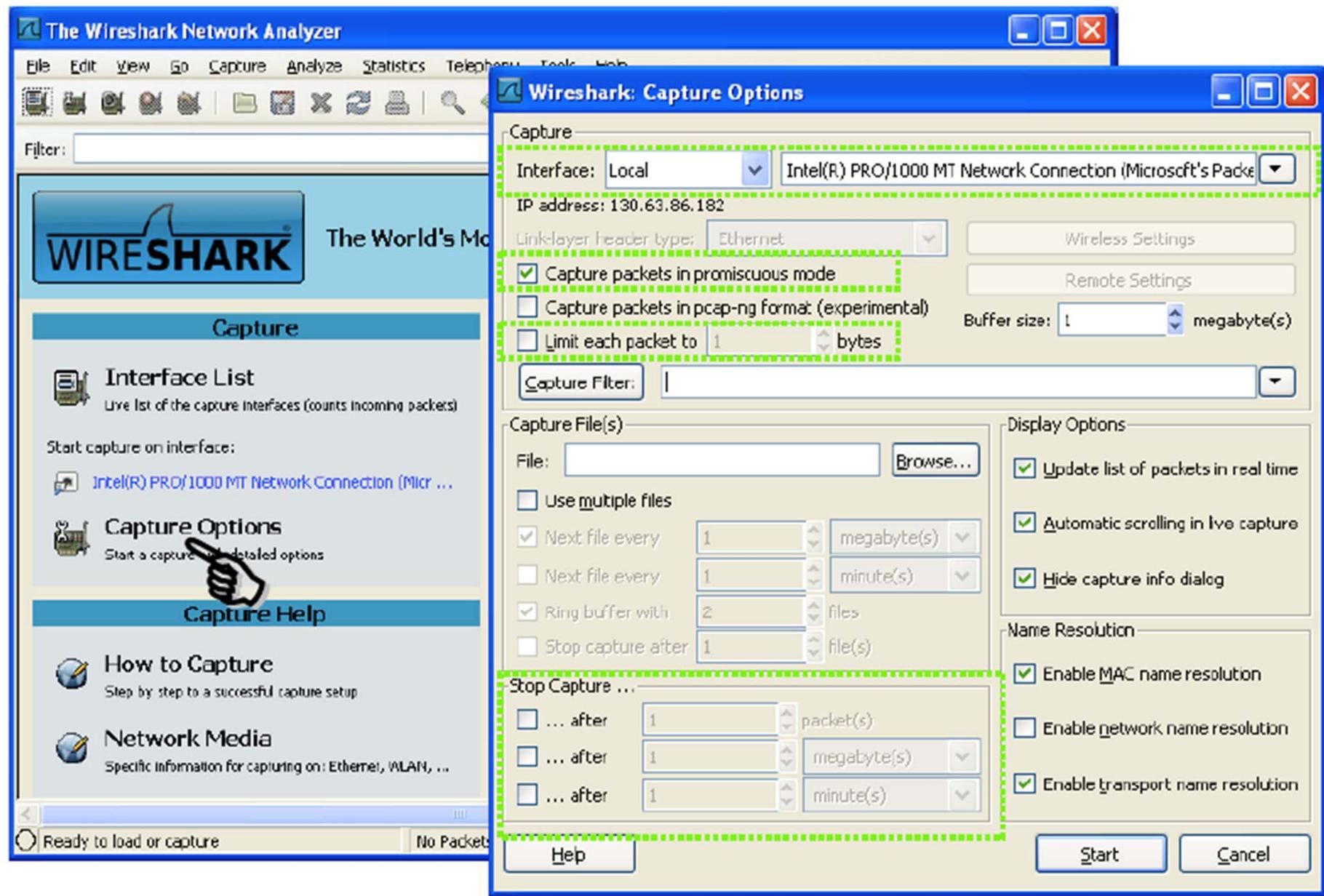


Wireshark Network Analyzer

Example: retrieval of www.cnn.com web page



Wireshark Network Analyzer



Wireshark Network Analyzer

Wireshark Display Window – captures traffic in three panes

The screenshot shows the Wireshark interface with three main panes:

- Summary Pane:** Shows a list of captured frames with columns for No., Time, Source, Destination, Protocol, and Info.
- Detail Pane:** Provides a detailed tree view of the selected frame's layers (Ethernet, IP, TCP, etc.) and their properties.
- Data Pane:** Displays the raw captured data in both hex and ASCII formats.

A callout line points from the "SUMMARY" section to the "Info" column in the summary table. Another callout line points from the "DETAIL" section to the tree view in the detail pane. A third callout line points from the "DATA" section to the hex/ASCII dump in the data pane.

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

The screenshot shows the Wireshark interface with a red underline highlighting the title bar. The main window displays a list of network packets captured on interface en0. A filter bar at the top is set to "http". The packet list table has columns: No., Time, Source, Destination, Protocol, Length, and Info. Several packets are selected, with the 267th packet highlighted in grey. The packet details pane below shows the HTTP response headers for this selected packet, including Date, Server, Set-Cookie, pragma, x-amz-id-1, p3p, cache-control, expires, x-amz-id-2, Vary, Content-Encoding, Content-Type, and multiple Set-cookie entries. The bytes pane at the bottom shows the raw hex and ASCII data for the selected frame.

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\nDate: Sun, 13 Jan 2013 20:31:03 GMT\r\nServer: Server\r\nSet-Cookie: skin=noskin; path=/; domain=.amazon.com; expires=Sun, 13-Jan-2013 20:31:03 GMT\r\npragma: no-cache\r\nx-amz-id-1: 113FFZG6RF65P6R9E2JX\r\np3p: policyref="http://www.amazon.com/w3c/p3p.xml", CP="CAO DSP LAW CUR ADM IVAo IVDo CONo OTPo OUR DELi PUBi\r\ncache-control: no-cache\r\nexpires: -1\r\nx-amz-id-2: qvDH+sYa4WnqaSw1/ZOJ8jjMPYAcebMeKALpNPR8xR+YP6kFF/UqiOS5dPfq3cpn\r\nVary: Accept-Encoding,User-Agent\r\nContent-Encoding: gzip\r\nContent-Type: text/html; charset=ISO-8859-1\r\nSet-cookie: x-wl-uid=1GXasEsIuzYmnZrBF0Z+jCs/N2dsX2UwWZxw34tcg+LSXTFcv9yQCcxImTg+WBHUJVtxBAuHhUt0=; path=/;\r\nSet-cookie: ubid-main=185-6430035-1464229; path=/; domain=.amazon.com; expires=Tue, 01-Jan-2036 08:00:01 GMT\r\nSet-cookie: session-id-time=2082787201l; path=/; domain=.amazon.com; expires=Tue, 01-Jan-2036 08:00:01 GMT\r\nSet-cookie: session-id=189-8166774-5048936; path=/; domain=.amazon.com; expires=Tue, 01-Jan-2036 08:00:01 GM

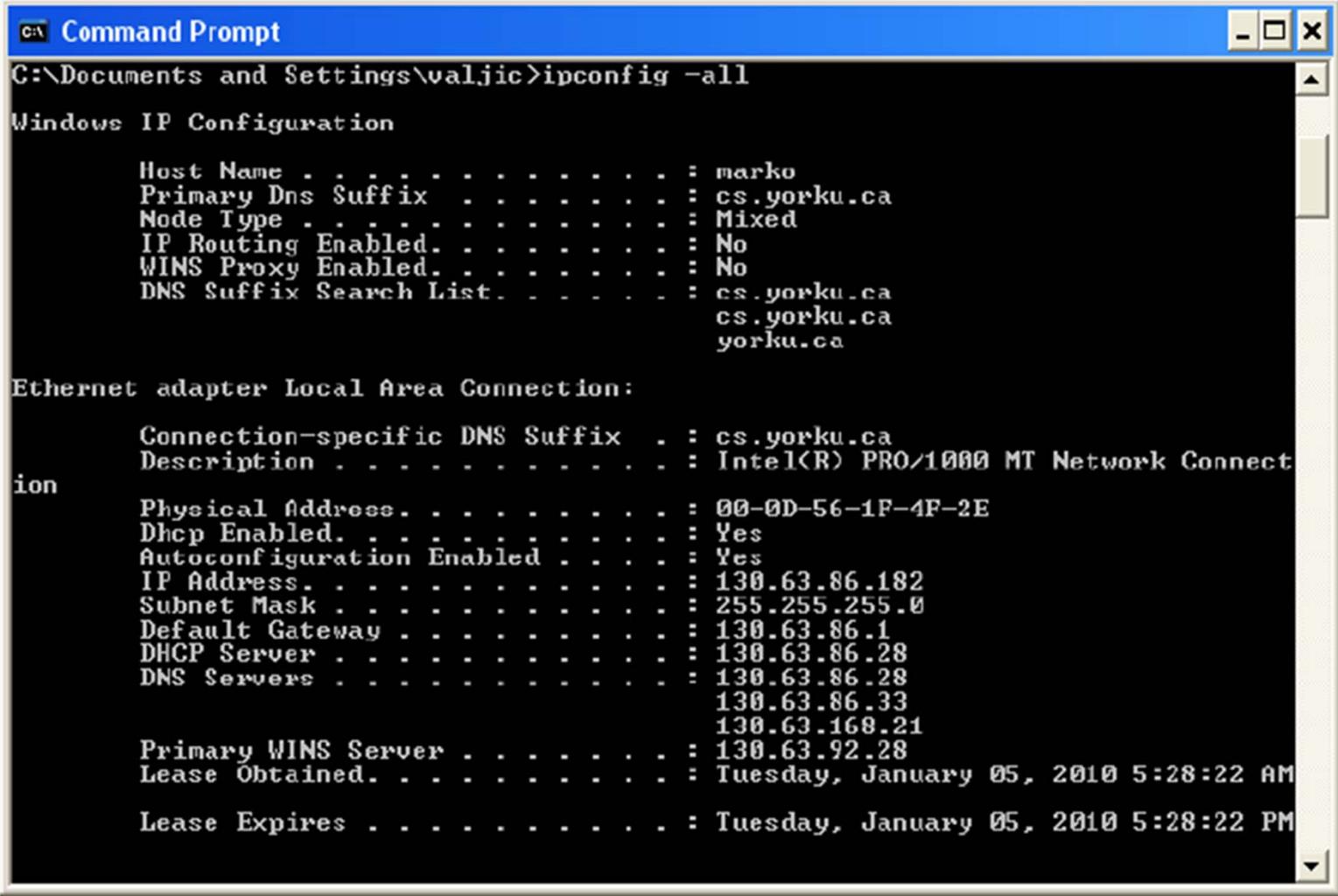
Frame	Length	Source	Destination	Protocol
0000	48 54 54 50 2f 31 2e 31 20 32 30 30 20 4f 4b 0d			HTTP/1.1 200 OK.
0010	0a 44 61 74 65 3a 20 53 75 6e 2c 20 31 33 20 4a			.Date: Sun, 13 J
0020	61 6e 20 32 30 31 33 20 32 30 3a 33 31 3a 30 33			an 2013 20:31:03

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

The image displays two instances of the Wireshark network analyzer interface. Both instances show a list of captured network packets in a table format with columns: No., Time, Source, Destination, Protocol, and Info.

Top Screenshot (DNS Filter):

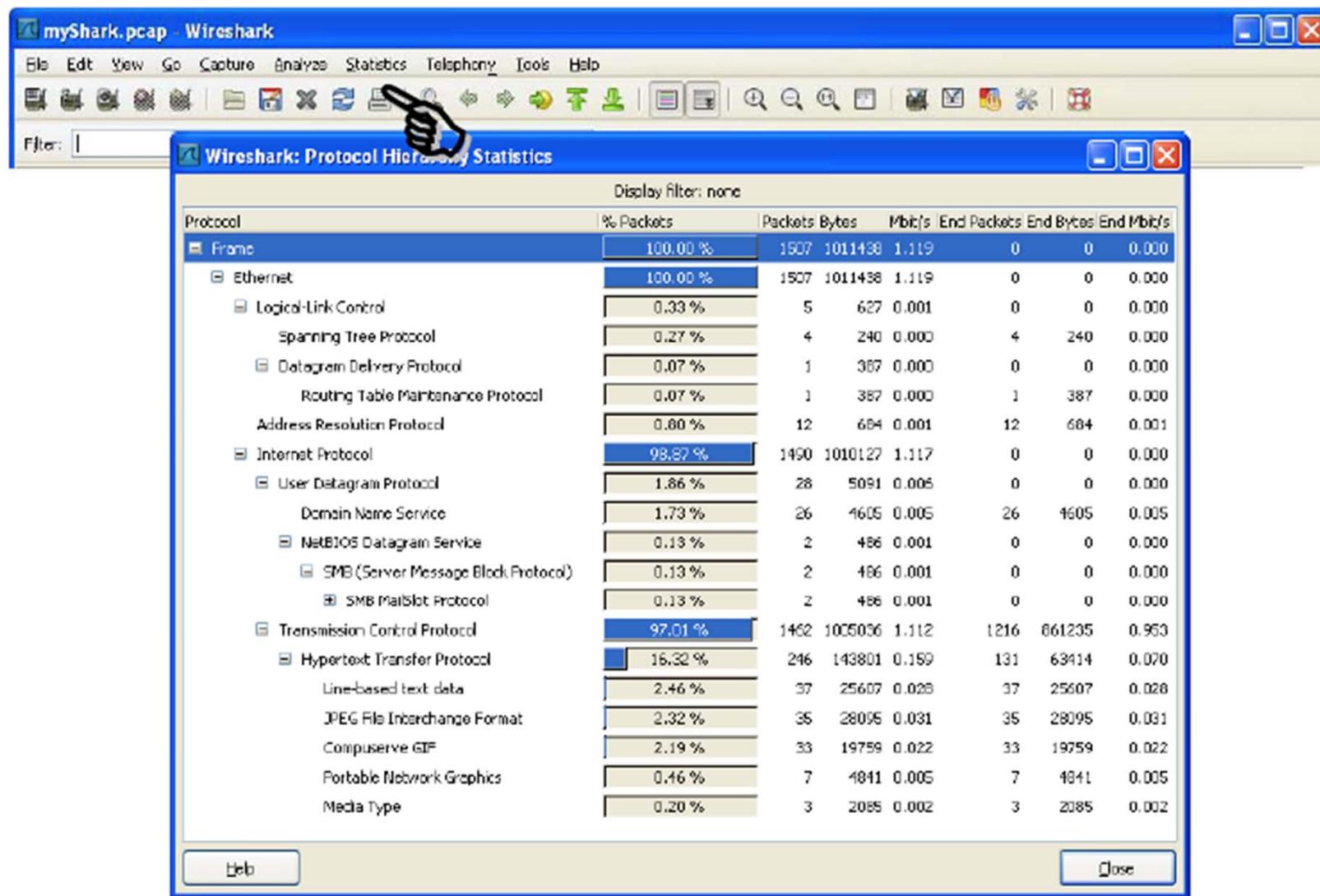
- Filter Bar:** Shows the filter expression `dns`.
- Table Data:** A list of DNS requests and responses. For example:
 - No. 4, Time 0.2417, Source 130.63.86.182, Destination 130.63.86.28, Protocol DNS, Info: Standard query A www.cnn.com
 - No. 5, Time 0.292557, Source 130.63.86.28, Destination 130.63.86.182, Protocol DNS, Info: Standard query response A 157.166.224.25 A 157.166.224.16 A

Bottom Screenshot (TCP Filter):

- Filter Bar:** Shows the filter expression `tcp`.
- Table Data:** A list of TCP connections. For example:
 - No. 6, Time 0.2417, Source 130.63.86.182, Destination 157.166.224.25, Protocol TCP, Info: 12m > http [SYN] Seq=0 Win=64240 Len=0 MSS=1460
 - No. 7, Time 0.337547, Source 157.166.224.25, Destination 130.63.86.182, Protocol TCP, Info: http > 12m [SYN, ACK] seq=0 Ack=1 win=1460 Len=0 MSS=1460

Wireshark Network Analyzer

Wireshark Statistics Summary Feature



Wireshark Installation

- www.wireshark.org

The screenshot shows the official Wireshark website at www.wireshark.org. The page features a blue header with the text "Wireshark - Go deep." and a navigation bar with links like YouTube, Apple, Yahoo!, Google Maps, Wikipedia, News, Popular, Google, INET @ RGS – Home, Reader, and a search bar. Below the header is a banner with the Wireshark logo and the tagline "the world's foremost network protocol analyzer". The main content area has three main sections: "Download Wireshark" with a "Get Started Now" button, "Learn Wireshark" with a "Resources and Documentation" button, and "Enhance Wireshark" with a "Riverbed Technology" button. At the bottom, there are three columns: "News and Events" (listing a "Wireshark Wiki Security Incident" from July 2012), "Wireshark Blog" (listing a post about "TCP's Nagle algorithm and delayed acknowledgement" from January 11, 2013), and "Enhance Wireshark" (listing a "Free 30 day trial" for Riverbed Technology).

Wireshark - Go deep.

Reader

YouTube Apple Yahoo! Google Maps Wikipedia News Popular Google INET @ RGS – Home

Wireshark - Go deep.

Packet Sniffer – EtherDetect TCP/IP Packet Sniffer

Riverbed Technology WinPcap IPv4 IPv6

WIRESHARK

the world's foremost network protocol analyzer

Wireshark | Get Help | Develop

Google™ Custom Search Search

Download Wireshark
Get Started Now

Learn Wireshark
Resources and Documentation

Enhance Wireshark
Riverbed Technology

News and Events

Wireshark Wiki Security Incident
On July 25, 2012 an intruder gained access to the server that hosts [wiki.wireshark.org](#), [blog.wireshark.org](#), and [ask.wireshark.org](#). This intrusion went undetected until January 8, 2013. Only the wiki appears to have been affected.
[Read more](#)

Troubleshooting the hidden dangers of TCP's Nagle algorithm and delayed acknowledgement
Jan 11 | By Hansang Bae

Wireshark Tutorial Series. Tips and tricks used by insiders and veterans

Enhance Wireshark

Troubleshoot your Network

Free 30 day trial

- Save hours on network and application issue diagnoses
- Monitor physical and virtual environments
- GUI packet capture and analysis
- Fully integrated with Wireshark