COEN 445
Lab 1

Introduction to Wireshark

Claude Fachkha

Outline

1. Introduction
2. Getting Wireshark
3. Running Wireshark
4. Trying Wireshark
5. Quiz

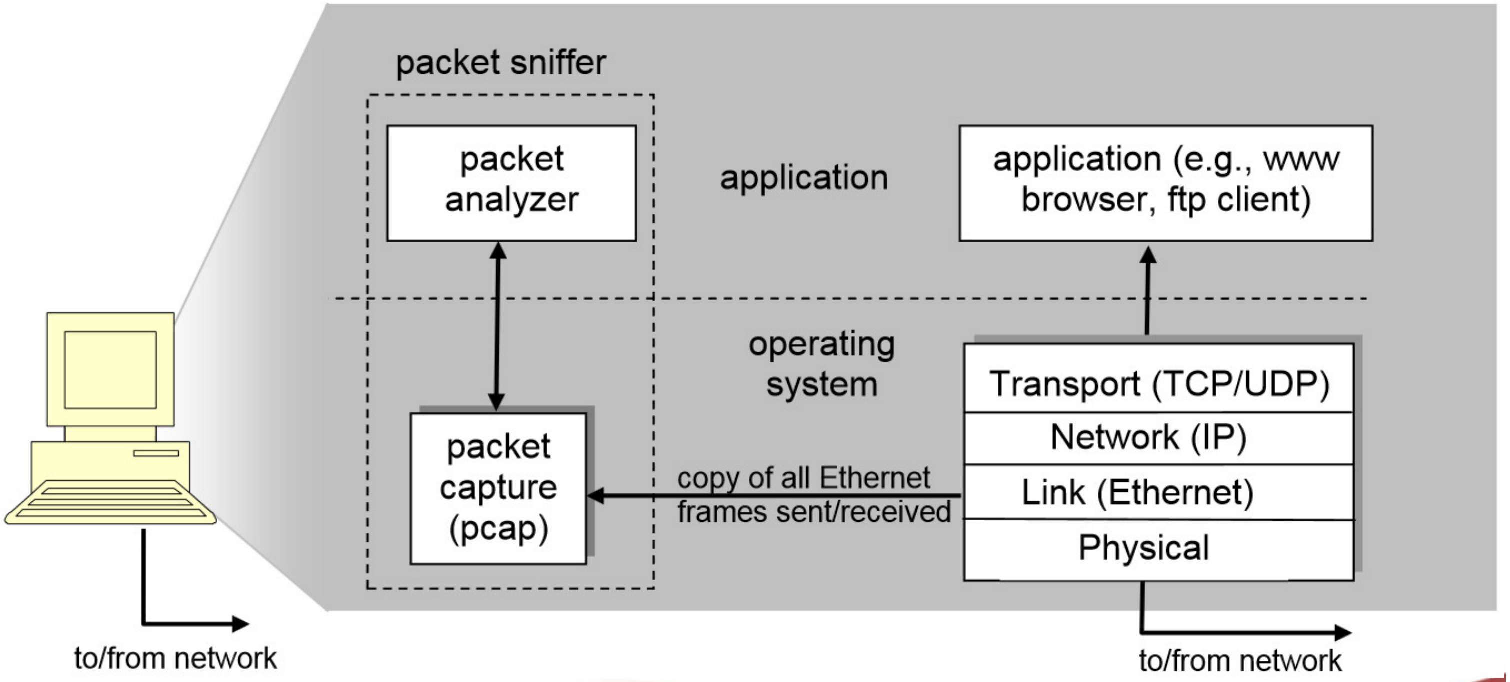
Introduction

The basic tool for observing the messages exchanged between executing protocol entities is called a **packet sniffer.**

The packet sniffer consists of 2 parts:

- The **packet capture** library receives a copy of every link layer frame that is sent from or received by your computer.

- The **packet analyzer** which displays the contents of all fields within a protocol message.

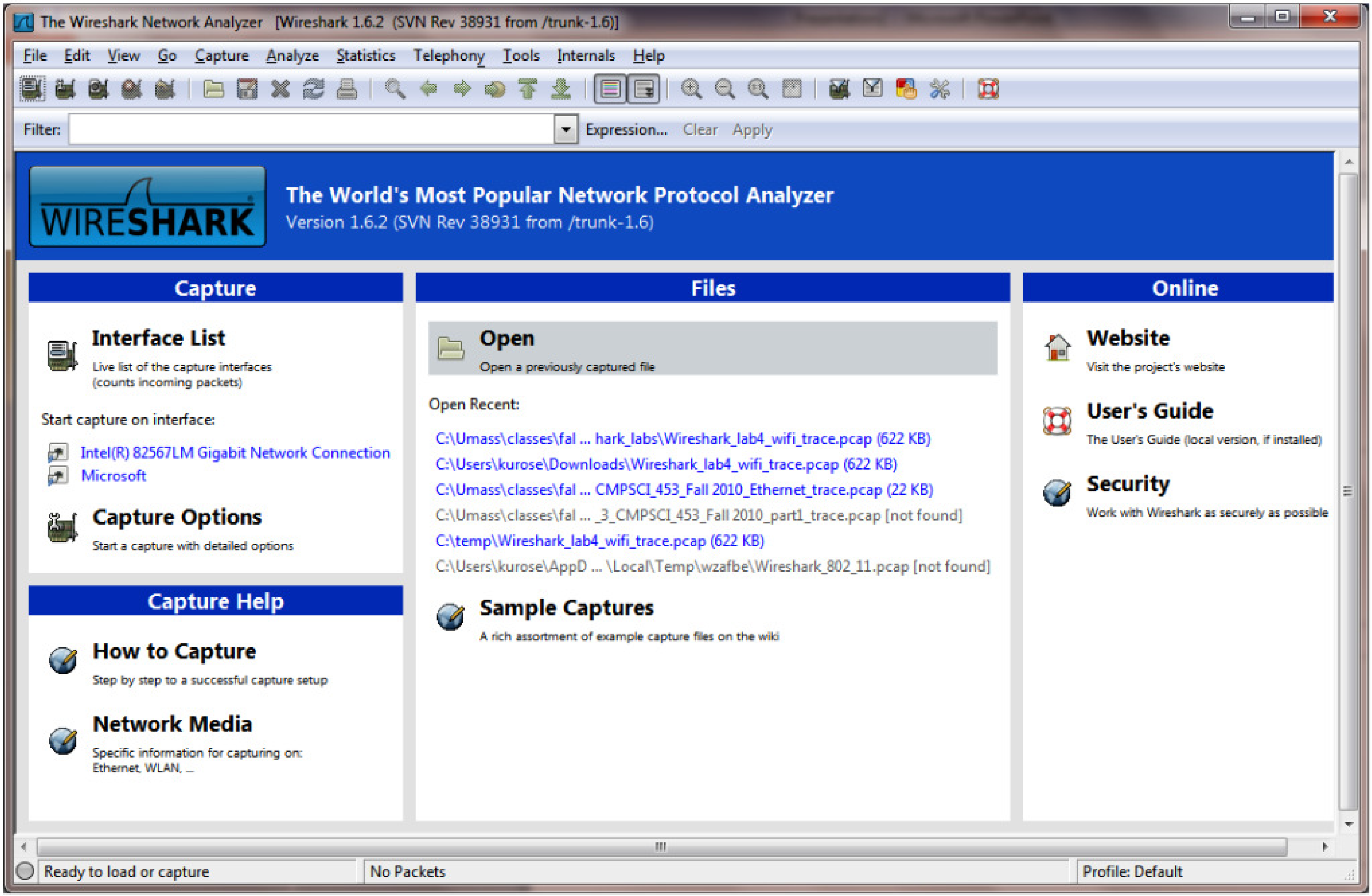


Getting Wireshark

- Wireshark is one of the best packet sniffer tools.

See http://www.wireshark.org/download.html

Running Wireshark



The Wireshark Network Analyzer [Wireshark 1.6.2 (SVN Rev 38931 from /trunk-1.6)]

WIRESHARK

The World's Most Popular Network Protocol Analyzer
Version 1.6.2 (SVN Rev 38931 from /trunk-1.6)

Capture

Interface List
Live list of the capture interfaces (counts incoming packets)

Start capture on interface:
Intel(R) 82567LM Gigabit Network Connection
Microsoft

Capture Options
Start a capture with detailed options

Capture Help

How to Capture
Step by step to a successful capture setup

Network Media
Specific information for capturing on: Ethernet, WLAN, ...

Files

Open
Open a previously captured file

Open Recent:
C:\Umass\classes\fal ... hark_labs\Wireshark_lab4_wifi_trace.pcap (622 KB)
C:\Users\kurose\Downloads\Wireshark_lab4_wifi_trace.pcap (622 KB)
C:\Umass\classes\fal ... CMPSCI_453_Fall 2010_Ethernet_trace.pcap (22 KB)
C:\Umass\classes\fal ... _3_CMPSCI_453_Fall 2010_part1_trace.pcap [not found]
C:\temp\Wireshark_lab4_wifi_trace.pcap (622 KB)
C:\Users\kurose\AppD ... \Local\Temp\wzafbe\Wireshark_802_11.pcap [not found]

Sample Captures
A rich assortment of example capture files on the wiki

Online

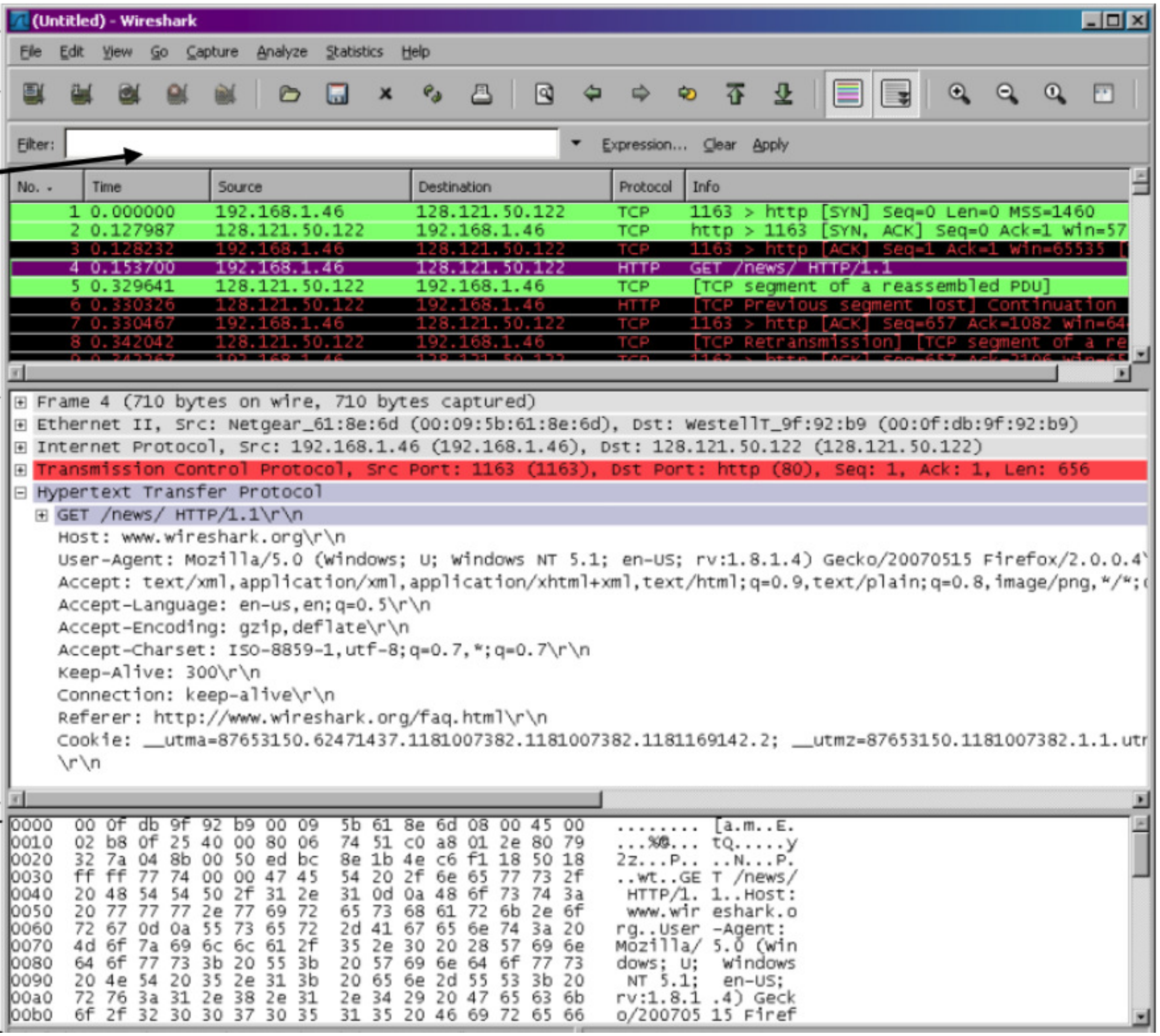
Website
Visit the project's website

User's Guide
The User's Guide (local version, if installed)

Security
Work with Wireshark as securely as possible

Ready to load or capture | No Packets | Profile: Default

Running Wireshark (cont.)


(Untitled) - Wireshark
File Edit View Go Capture Analyze Statistics Help
Filter:
Expression... Clear Apply

```
No. -  Time      Source          Destination     Protocol Info
  1 0.000000   192.168.1.46    128.121.50.122  TCP   1163 > http [SYN] Seq=0 Len=0 MSS=1460
  2 0.127987   128.121.50.122  192.168.1.46    TCP   http > 1163 [SYN, ACK] Seq=0 Ack=1 Win=57
  3 0.128232   192.168.1.46    128.121.50.122  TCP   1163 > http [ACK] Seq=1 Ack=1 Win=65535 [
  4 0.153700   192.168.1.46    128.121.50.122  HTTP  GET /news/ HTTP/1.1
  5 0.329641   128.121.50.122  192.168.1.46    TCP   [TCP segment of a reassembled PDU]
  6 0.330326   128.121.50.122  192.168.1.46    HTTP  [TCP Previous segment lost] Continuation
  7 0.330467   192.168.1.46    128.121.50.122  TCP   1163 > http [ACK] Seq=657 Ack=1082 Win=64
  8 0.342042   128.121.50.122  192.168.1.46    TCP   [TCP Retransmission] [TCP segment of a re
```

```
⊞ Frame 4 (710 bytes on wire, 710 bytes captured)
⊞ Ethernet II, Src: Netgear_61:8e:6d (00:09:5b:61:8e:6d), Dst: WestellT_9f:92:b9 (00:0f:db:9f:92:b9)
⊞ Internet Protocol, Src: 192.168.1.46 (192.168.1.46), Dst: 128.121.50.122 (128.121.50.122)
⊞ Transmission Control Protocol, Src Port: 1163 (1163), Dst Port: http (80), Seq: 1, Ack: 1, Len: 656
⊟ Hypertext Transfer Protocol
  ⊞ GET /news/ HTTP/1.1\r\n
    Host: www.wireshark.org\r\n
    User-Agent: Mozilla/5.0 (Windows; U; Windows NT 5.1; en-US; rv:1.8.1.4) Gecko/20070515 Firefox/2.0.0.4
    Accept: text/xml,application/xml,application/xhtml+xml,text/html;q=0.9,text/plain;q=0.8,image/png,*/*;
    Accept-Language: en-us,en;q=0.5\r\n
    Accept-Encoding: gzip,deflate\r\n
    Accept-Charset: ISO-8859-1,utf-8;q=0.7,*;q=0.7\r\n
    Keep-Alive: 300\r\n
    Connection: keep-alive\r\n
    Referer: http://www.wireshark.org/faq.html\r\n
    Cookie: __utma=87653150.62471437.1181007382.1181007382.1181169142.2; __utmz=87653150.1181007382.1.1.utr
    \r\n
```

```
0000  00 0f db 9f 92 b9 00 09  5b 61 8e 6d 08 00 45 00   ........ [a.m..E.
0010  02 b8 0f 25 40 00 80 06  74 51 c0 a8 01 2e 80 79   ...%@... tQ.....y
0020  32 7a 04 8b 00 50 ed bc  8e 1b 4e c6 f1 18 50 18   2z...P.. ..N...P.
0030  ff ff 77 74 00 00 47 45  54 20 2f 6e 65 77 73 2f   ..wt..GE T /news/
0040  20 48 54 54 50 2f 31 2e  31 0d 0a 48 6f 73 74 3a    HTTP/1. 1..Host:
0050  20 77 77 77 2e 77 69 72  65 73 68 61 72 6b 2e 6f    www.wir eshark.o
0060  72 67 0d 0a 55 73 65 72  2d 41 67 65 6e 74 3a 20   rg..User -Agent:
0070  4d 6f 7a 69 6c 6c 61 2f  35 2e 30 20 28 57 69 6e   Mozilla/ 5.0 (Win
0080  64 6f 77 73 3b 20 55 3b  20 57 69 6e 64 6f 77 73   dows; U;  Windows
0090  20 4e 54 20 35 2e 31 3b  20 65 6e 2d 55 53 3b 20    NT 5.1;  en-US;
00a0  72 76 3a 31 2e 38 2e 31  2e 34 29 20 47 65 63 6b   rv:1.8.1 .4) Geck
00b0  6f 2f 32 30 30 37 30 35  31 35 20 46 69 72 65 66   o/200705 15 Firef
```

command menus

display filter specification

listing of captured packets

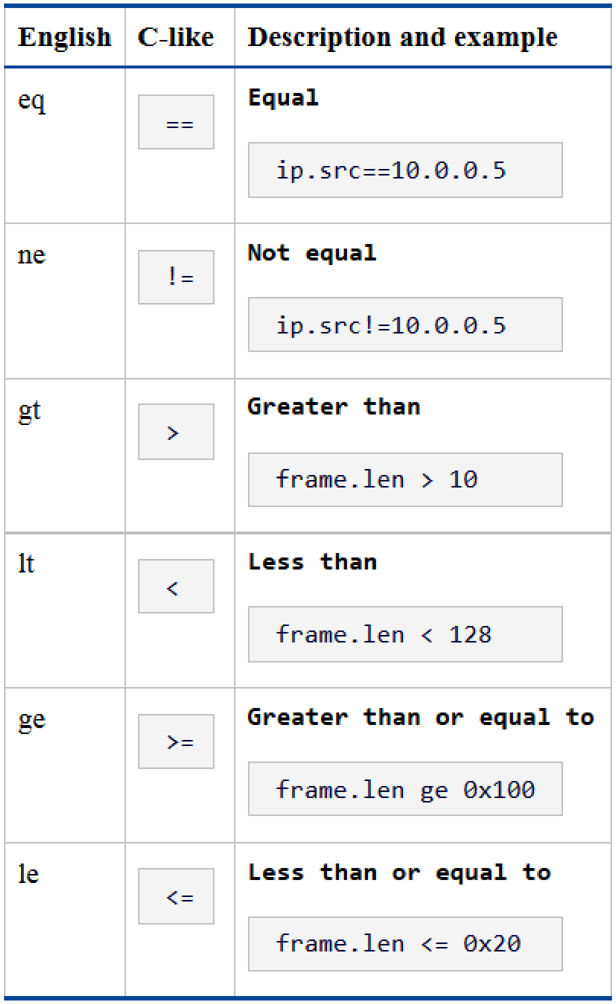
details of selected packet header

packet **content** in hexadecimal and ASCII

Running Wireshark (cont.)

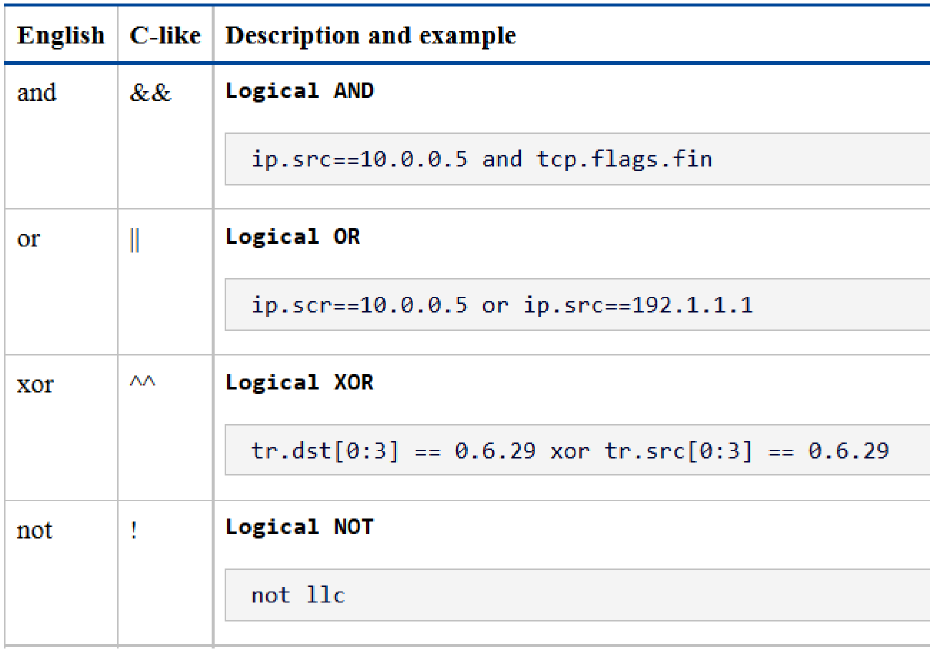
Filters

Table 6.4. Display Filter comparison operators



English	C-like	Description and example
eq	==	**Equal** `ip.src==10.0.0.5`
ne	!=	**Not equal** `ip.src!=10.0.0.5`
gt	>	**Greater than** `frame.len > 10`
lt	<	**Less than** `frame.len < 128`
ge	>=	**Greater than or equal to** `frame.len ge 0x100`
le	<=	**Less than or equal to** `frame.len <= 0x20`

Table 6.6. Display Filter Logical Operations



English	C-like	Description and example
and	&&	**Logical AND** `ip.src==10.0.0.5 and tcp.flags.fin`
or	||	**Logical OR** `ip.scr==10.0.0.5 or ip.src==192.1.1.1`
xor	^^	**Logical XOR** `tr.dst[0:3] == 0.6.29 xor tr.src[0:3] == 0.6.29`
not	!	**Logical NOT** `not llc`

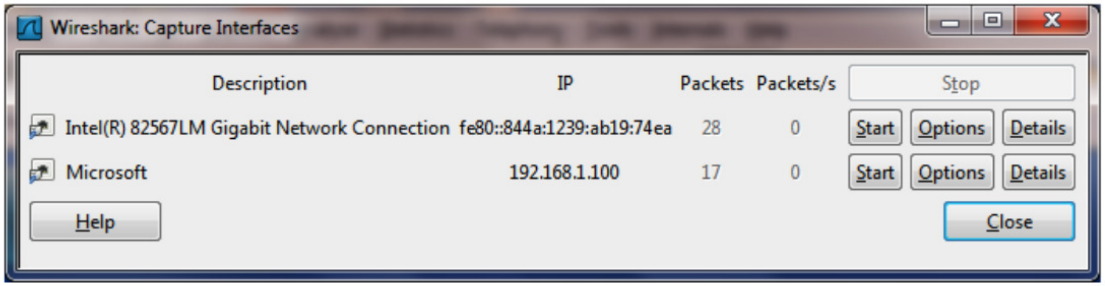
Check reference 1

Testing Wireshark

1. Start up your favorite web browser, which will display your selected homepage.

2. Start up the Wireshark software. You will initially see a window similar to that shown in slide 5. Wireshark has not yet begun capturing packets.

3. To begin packet capture, select the Capture pull down menu and select Interfaces. This will cause the “Wireshark: Capture Interfaces” window to be displayed, as shown in the figure below



Description	IP	Packets	Packets/s
Intel(R) 82567LM Gigabit Network Connection	fe80::844a:1239:ab19:74ea	28	0
Microsoft	192.168.1.100	17	0

Testing Wireshark (cont.)

4. Click on Start for the interface on which you want to begin packet capture (in the case, the Gigabit network Connection). Packet capture will now begin - Wireshark is now capturing all packets being sent/received from/by your computer.

5. By selecting Capture pulldown menu and selecting Stop, you can stop packet capture. But don’t stop packet capture yet. Let’s capture some interesting packets first.

6. While Wireshark is running, enter the URL: http://gaia.cs.umass.edu/wireshark-labs/INTRO-wireshark-file1.html and have that page displayed in your browser. In order to display this page, your browser will contact the HTTP server at gaia.cs.umass.edu and exchange HTTP messages with the server in order to download this page

Testing Wireshark (cont.)

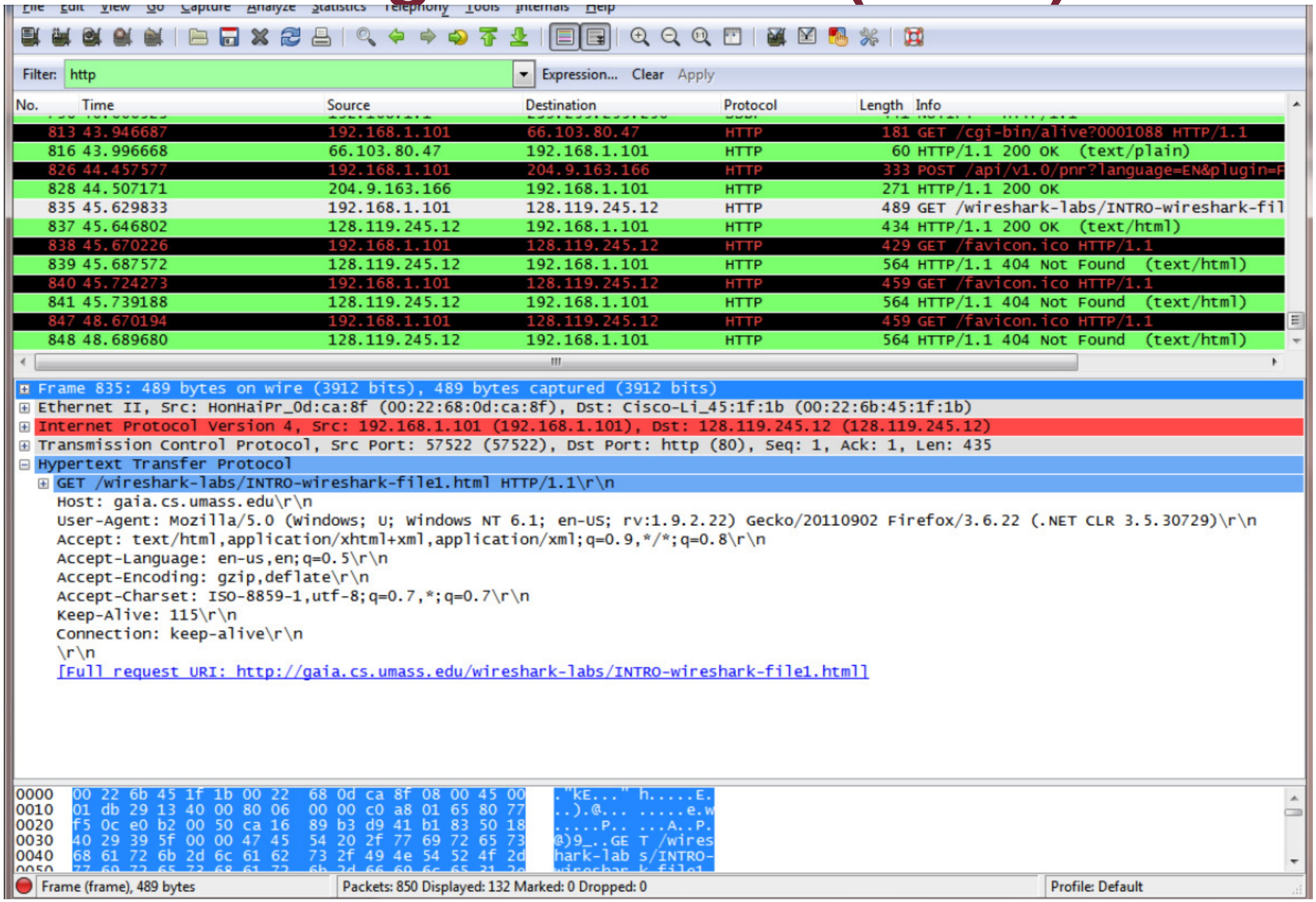
7. Stop Wireshark packet capture by selecting stop in the Wireshark capture window. You now have live packet data that contains all protocol messages exchanged between your computer and other network entities! The HTTP message exchanges with the gaia.cs.umass.edu web server should appear somewhere in the listing of packets captured.

8. Type in “http” (without the quotes, and in lower case - all protocol names are in lower case in Wireshark) into the display filter specification window at the top of the main Wireshark window. Then select Apply (to the right of where you entered “http”). This will cause only HTTP message to be displayed in the packet-listing window.

9. Find the HTTP GET message that was sent from your computer to the gaia.cs.umass.edu HTTP server. (Look for an HTTP GET message in the “listing of captured packets” portion of the Wireshark window (see Figure 3) that shows “GET” followed by the gaia.cs.umass.edu URL that you entered. When you select the HTTP GET message, the Ethernet frame, IP datagram, TCP segment, and HTTP message header information will be displayed in the packet-header window. By clicking on ‘+’ and ‘-‘ right-pointing and down-pointing arrowheads to the left side of the packet details window, minimize information displayed.

(you can refer to the picture in the next slide)

Testing Wireshark (cont.)


File Edit View Go Capture Analyze Statistics Telephony Tools Internals Help
Expression... Clear Apply

Filter: http

```
No.  Time       Source          Destination     Protocol Length Info
813 43.946687   192.168.1.101   66.103.80.47    HTTP     181 GET /cgi-bin/alive?0001088 HTTP/1.1
816 43.996668   66.103.80.47    192.168.1.101   HTTP      60 HTTP/1.1 200 OK  (text/plain)
826 44.457577   192.168.1.101   204.9.163.166   HTTP     333 POST /api/v1.0/pnr?language=EN&plugin=F
828 44.507171   204.9.163.166   192.168.1.101   HTTP     271 HTTP/1.1 200 OK
835 45.629833   192.168.1.101   128.119.245.12  HTTP     489 GET /wireshark-labs/INTRO-wireshark-fil
837 45.646802   128.119.245.12  192.168.1.101   HTTP     434 HTTP/1.1 200 OK  (text/html)
838 45.670226   192.168.1.101   128.119.245.12  HTTP     429 GET /favicon.ico HTTP/1.1
839 45.687572   128.119.245.12  192.168.1.101   HTTP     564 HTTP/1.1 404 Not Found  (text/html)
840 45.724273   192.168.1.101   128.119.245.12  HTTP     459 GET /favicon.ico HTTP/1.1
841 45.739188   128.119.245.12  192.168.1.101   HTTP     564 HTTP/1.1 404 Not Found  (text/html)
847 48.670194   192.168.1.101   128.119.245.12  HTTP     459 GET /favicon.ico HTTP/1.1
848 48.689680   128.119.245.12  192.168.1.101   HTTP     564 HTTP/1.1 404 Not Found  (text/html)
```

```
⊞ Frame 835: 489 bytes on wire (3912 bits), 489 bytes captured (3912 bits)
⊞ Ethernet II, Src: HonHaiPr_0d:ca:8f (00:22:68:0d:ca:8f), Dst: Cisco-Li_45:1f:1b (00:22:6b:45:1f:1b)
⊞ Internet Protocol Version 4, Src: 192.168.1.101 (192.168.1.101), Dst: 128.119.245.12 (128.119.245.12)
⊞ Transmission Control Protocol, Src Port: 57522 (57522), Dst Port: http (80), Seq: 1, Ack: 1, Len: 435
⊟ Hypertext Transfer Protocol
  ⊞ GET /wireshark-labs/INTRO-wireshark-file1.html HTTP/1.1\r\n
    Host: gaia.cs.umass.edu\r\n
    User-Agent: Mozilla/5.0 (Windows; U; Windows NT 6.1; en-US; rv:1.9.2.22) Gecko/20110902 Firefox/3.6.22 (.NET CLR 3.5.30729)\r\n
    Accept: text/html,application/xhtml+xml,application/xml;q=0.9,*/*;q=0.8\r\n
    Accept-Language: en-us,en;q=0.5\r\n
    Accept-Encoding: gzip,deflate\r\n
    Accept-Charset: ISO-8859-1,utf-8;q=0.7,*;q=0.7\r\n
    Keep-Alive: 115\r\n
    Connection: keep-alive\r\n
    \r\n
    [Full request URI: http://gaia.cs.umass.edu/wireshark-labs/INTRO-wireshark-file1.html]
```

```
0000  00 22 6b 45 1f 1b 00 22  68 0d ca 8f 08 00 45 00   ."kE..." h.....E.
0010  01 db 29 13 40 00 80 06  00 00 c0 a8 01 65 80 77   ..).@... .....e.w
0020  f5 0c e0 b2 00 50 ca 16  89 b3 d9 41 b1 83 50 18   .....P.. ...A..P.
0030  40 29 39 5f 00 00 47 45  54 20 2f 77 69 72 65 73   @)9_..GE T /wires
0040  68 61 72 6b 2d 6c 61 62  73 2f 49 4e 54 52 4f 2d   hark-lab s/INTRO-
```

Frame (frame), 489 bytes | Packets: 850 Displayed: 132 Marked: 0 Dropped: 0 | Profile: Default

Quiz
(Based on the previous experiment)

1. List 3 different protocols that appear in the protocol column in the unfiltered packet-listing window in step 7 above.

2. How long did it take from when the HTTP GET message was sent until the HTTP OK reply was received? (By default, the value of the Time column in the packet-listing window is the amount of time, in seconds, since Wireshark tracing began. To display the Time field in time-of-day format, select the Wireshark View pull down menu, then select Time Display Format , then select Time-of-day.)

3. What is the Internet address of the gaia.cs.umass.edu (also known as www-net.cs.umass.edu)? What is the Internet address of your computer?

4. Print the two HTTP messages (GET and OK) referred to in question 2 above. To do so, select Print from the Wireshark File command menu, and select the "Selected Packet Only" and "Print as displayed" radial buttons, and then click OK

References

1- **Wireshark: Display Filter Reference**
http://www.wireshark.org/docs/dfref/

2- **Wireshark: Building display filter expressions**
http://www.wireshark.org/docs/wsug_html_chunked/ChWorkBuildDisplayFilterSection.html

?

Claude Fachkha

c_fachkh@encs.concordia.ca