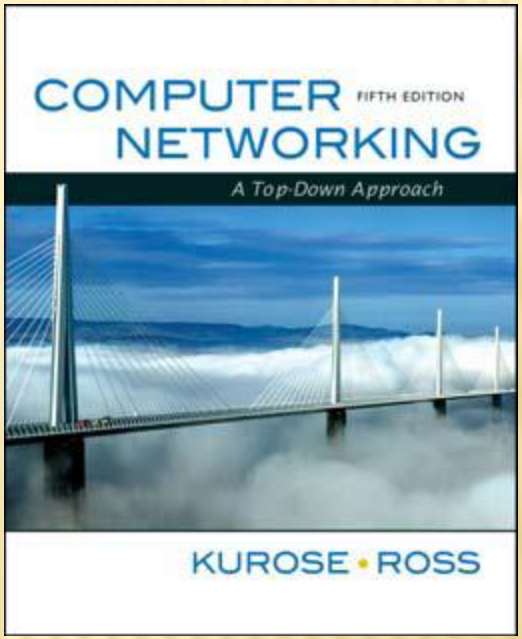


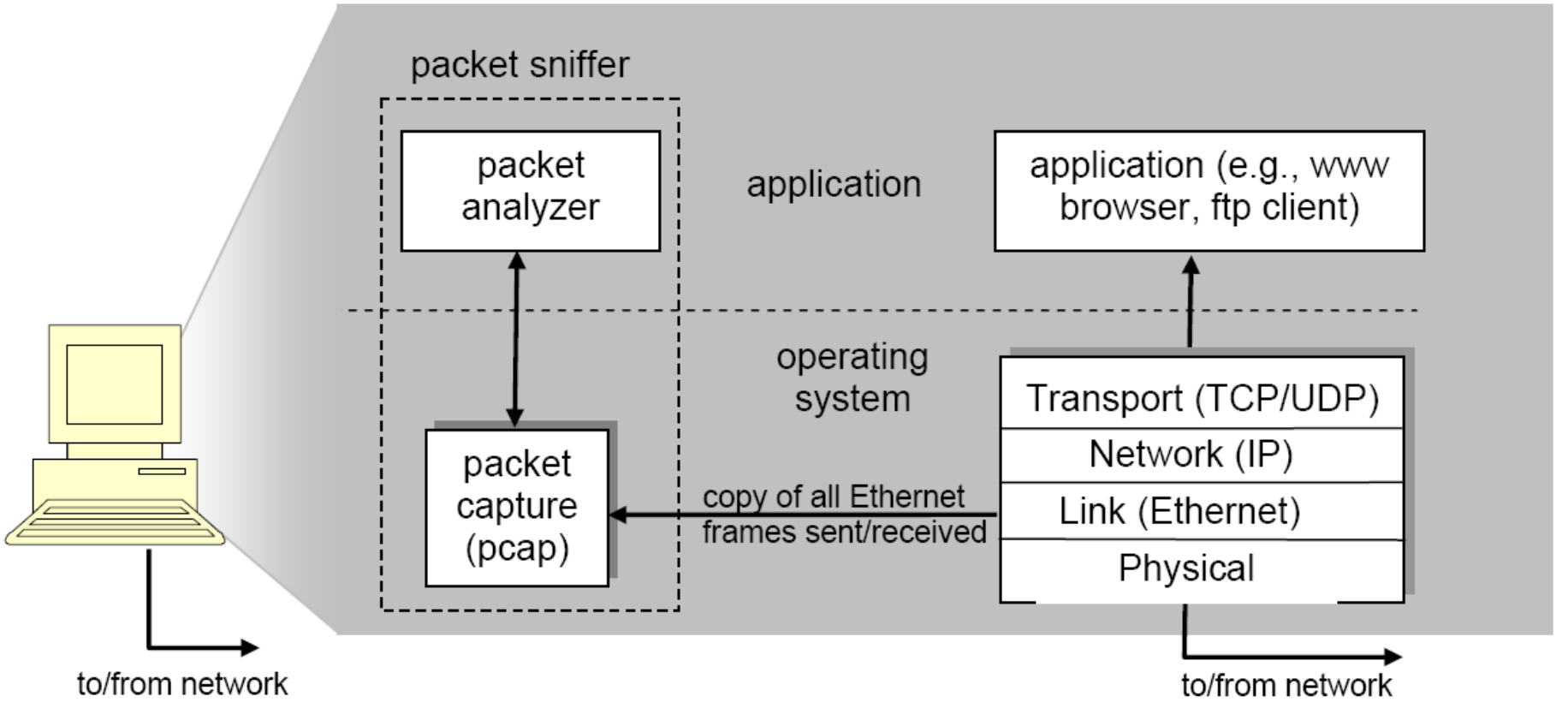
Computer Networking

LAB 1 – WIRESHARK INTRODUCTION

PACKET SNIFFERS

- The basic tool for observing the messages exchanged between executing protocol entities
- Captures (“sniffs”) messages being sent/received from/by your computer
- Store and/or display the contents of the various protocol fields in these captured messages

PACKET SNIFFER STRUCTURE

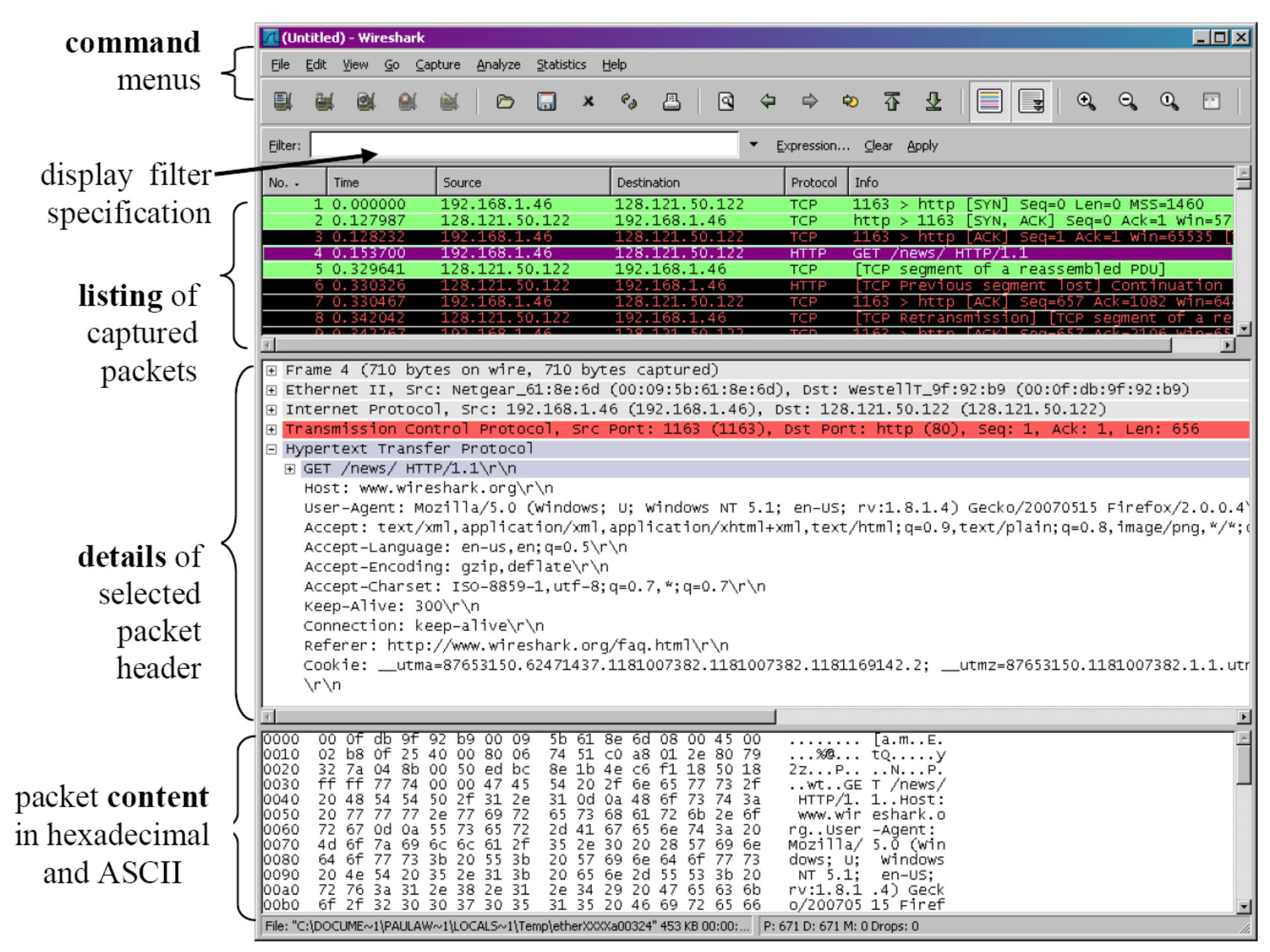


PACKET SNIFFER STRUCTURE

- The **packet capture library** receives a copy of every link-layer frame that is sent from or received by your computer.
- The **packet analyzer** displays the contents of all fields within a protocol message.

GETTING WIRESHARK

- Download and install the Wireshark software: http://www.wireshark.org/download.html
- Windows PortableApps (32-bit)


command menus
display filter specification
listing of captured packets
details of selected packet header
packet content in hexadecimal and ASCII
(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
File: "C:\DOCUME~1\PAULAW~1\LOCALS~1\Temp\etherXXXXa00324" 453 KB 00:00:...
P: 671 D: 671 M: 0 Drops: 0

TAKING WIRESHARK FOR A TEST RUN

1. Start up your favorite web browser
2. Start up the Wireshark software
3. To begin packet capture, select the Capture pull down menu and select *Options*
4. Select an interface that is being used to send and receive packets, click Start
5. Once you begin packet capture, a packet capture summary window will appear

TAKING WIRESHARK FOR A TEST RUN

6. Enter the URL: http://gaia.cs.umass.edu/wireshark-labs/INTRO-wireshark-file1.html
7. Stop Wireshark packet capture by selecting stop in the Wireshark capture window.
8. Type in “http” into the display filter specification window, then select *Apply*
9. Select the first http message shown in the packet-listing window

QUESTIONS

1. List the 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?
3. What is the Internet address of the gaia.cs.umass.edu? What is the Internet address of your computer?