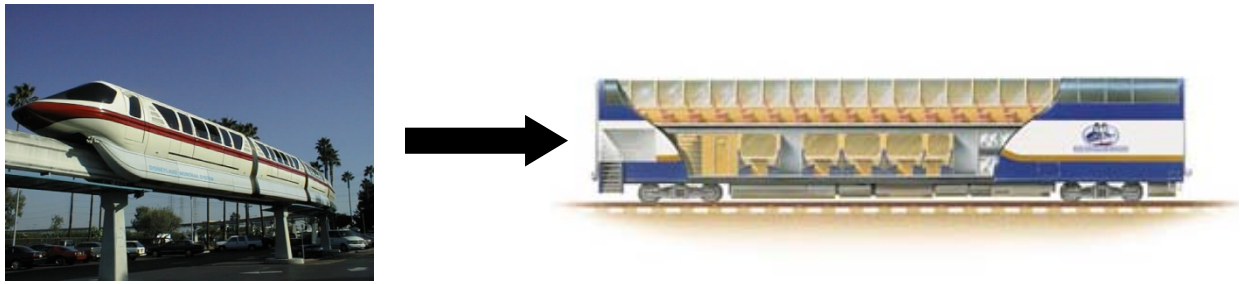
Packet Sniffing and Analysis

- Currently data just travels around your network like a train. With a packet sniffer, get the ability to capture the data and look inside the packets to see what is actually moving along the tracks.



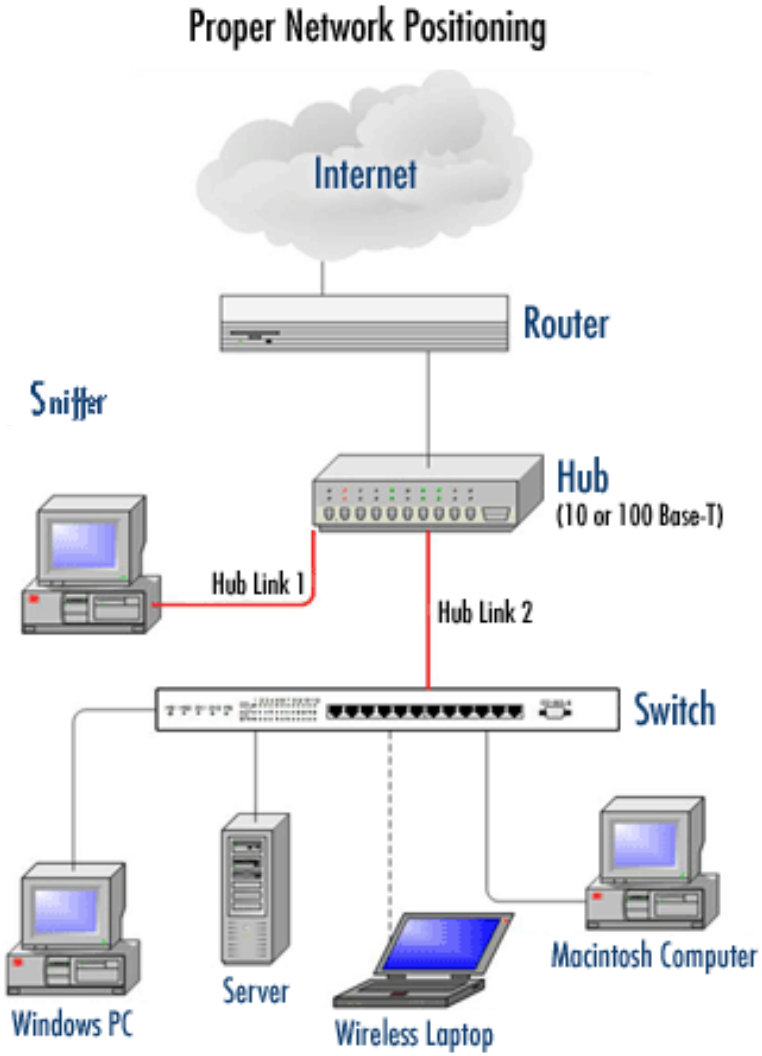
- Capture, decode, and analyze network traffic:
  - Why is the network slow
  - What is the network traffic pattern
  - How is the traffic being shared between nodes
- Known as traffic analysis, protocol analysis, sniffing, packet analysis, eavesdropping*, etc.

*Listen secretly to what is said in private!

Packet Sniffer and Analyzer

- Packet sniffer
  - A program that monitors the data traveling through the network *passively*
  - Receives a copy of packets that are sent/received from/by applications and protocols running on your machine
- Packet analyzer can decode and manipulate captured packets
  - Passive monitoring (detection) - Difficult to detect
  - Active (attack)
- Available both free and commercially
- Mainly software-based (utilizing OS and NIC)
- Common packet analyzers
  - **Wireshark**
  - Ethereal
  - Windump
  - And much more….

Sniffer Positioning



Who uses packet sniffers and analyzers?

- System administrators
  - Understand system problems and performance
  - Intrusion detection
- Malicious individuals (intruders)
  - Capture cleartext data (not encrypted/μη κρυπτογραφημένα)
  - Passively collect data on vulnerable protocols
    - FTP, POP3, IMAP, SMATP, rlogin, HTTP, etc.
    - Capture VoIP data
  - Mapping the target network
  - Traffic pattern discovery
  - Actively break into the network (backdoor techniques)

What is Wireshark?

- Formerly called ***Ethereal***
- An open source **packet analyzer**
  - free with many features
- Decodes over 750 protocols
- Compatible with many other sniffers
- Plenty of online resources are available
- Supports command-line and GUI interfaces
  - TSHARK (offers command line interface) has three components
    - Editcap
    - Mergecap
    - text2pcap

Remember: You must have a good understanding of the network before you use Sniffers effectively!

Packet Sniffer and Analyzer Structure

Wireshark – Application for Analyzing Packets

WinPcap – open source library for packet capture

Operating System – Windows & Unix/Linux

Network Card Drivers – Ethernet/WiFi Card

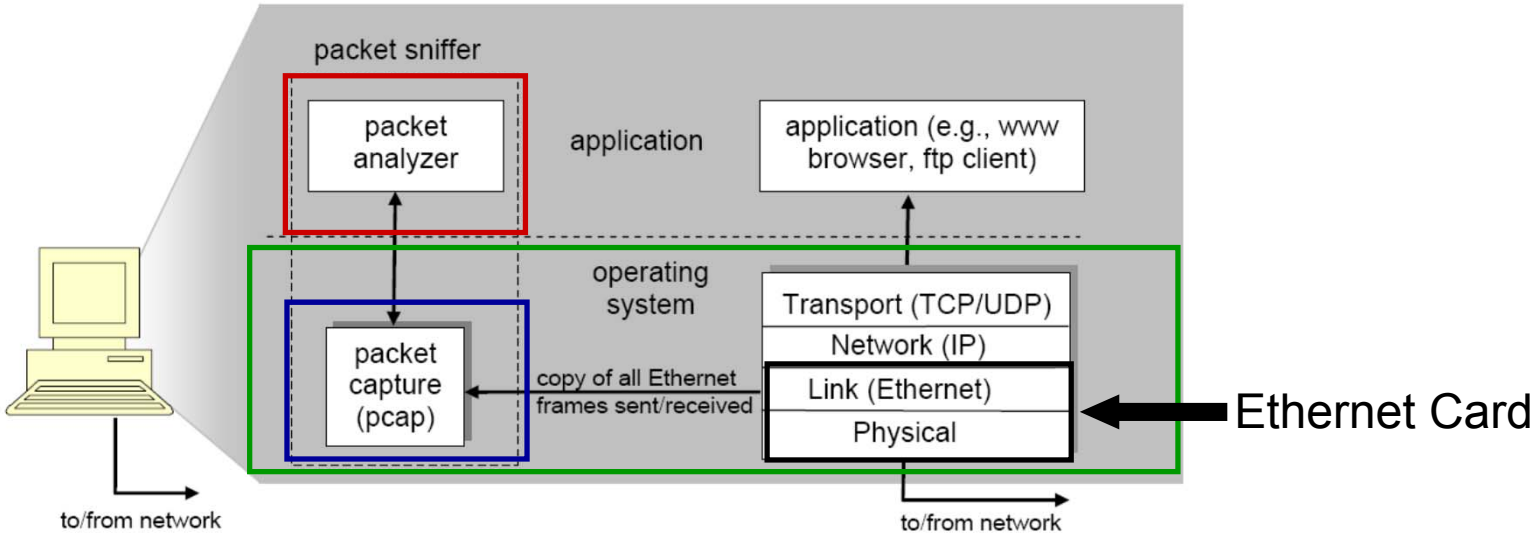
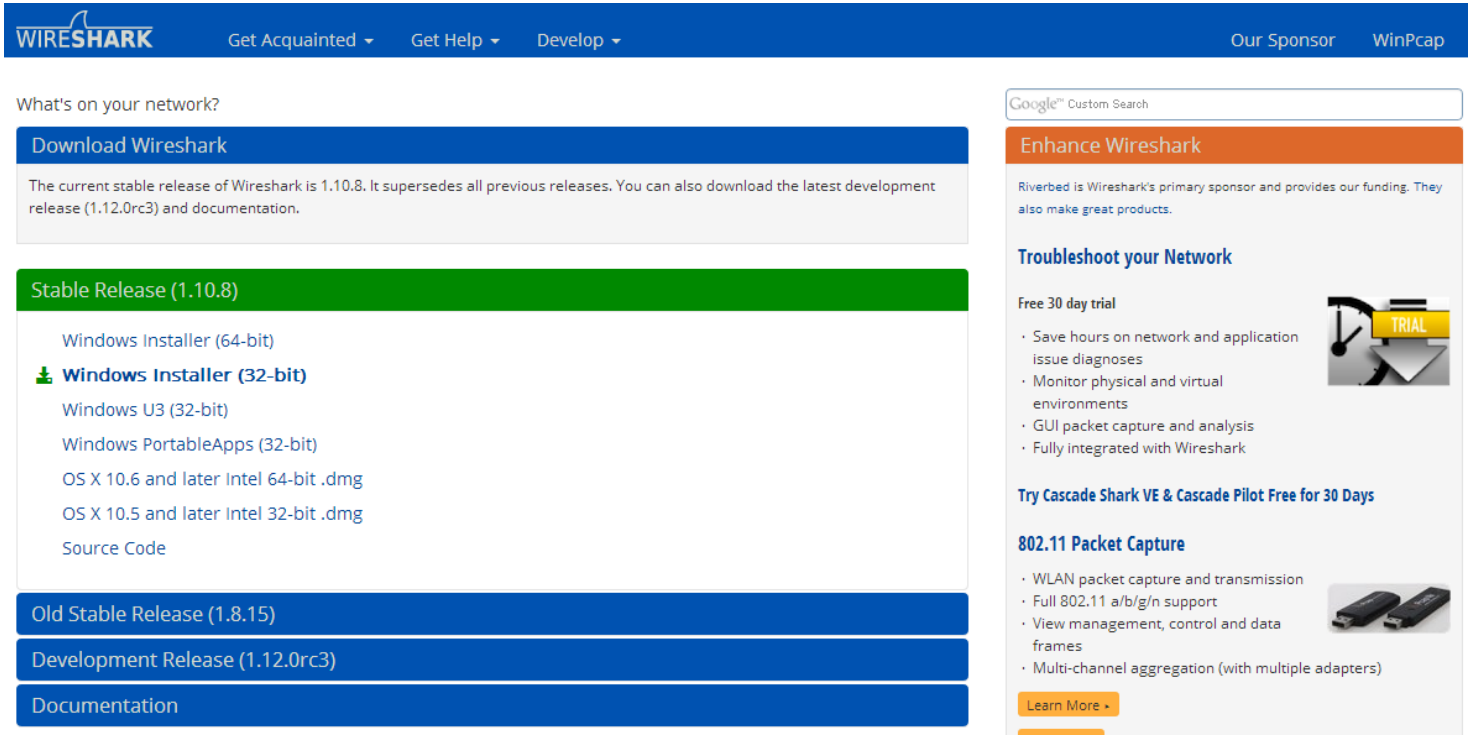


Figure 1: Packet sniffer structure

Getting Wireshark

- Download the program from
  - www.wireshark.org/download.html
- Requires to install capture drivers (monitor ports and capture all traveling packets)
  - Windows: winpcap (www.winpcap.org)
  - Linux: libpcap



Running Wireshark

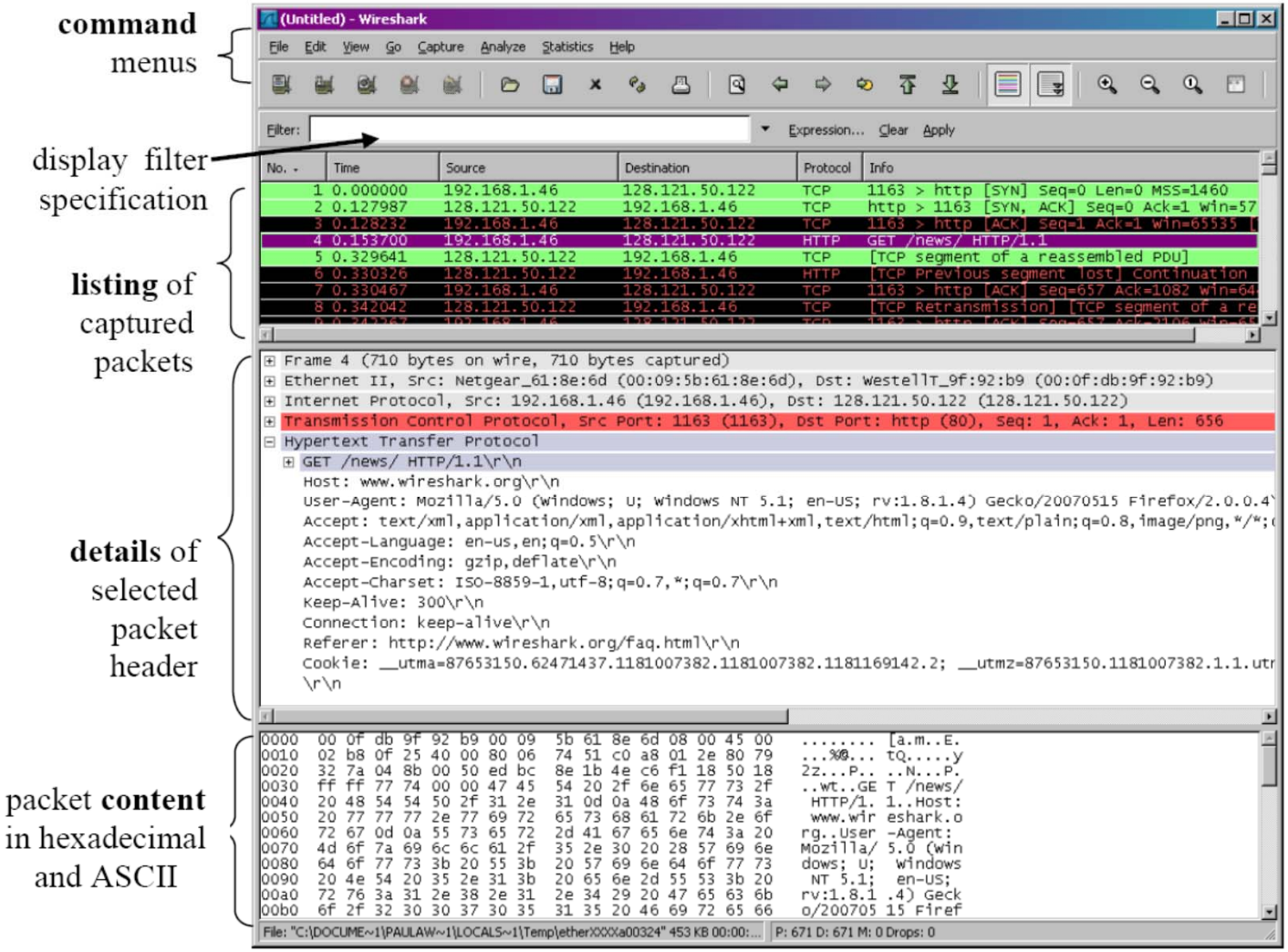
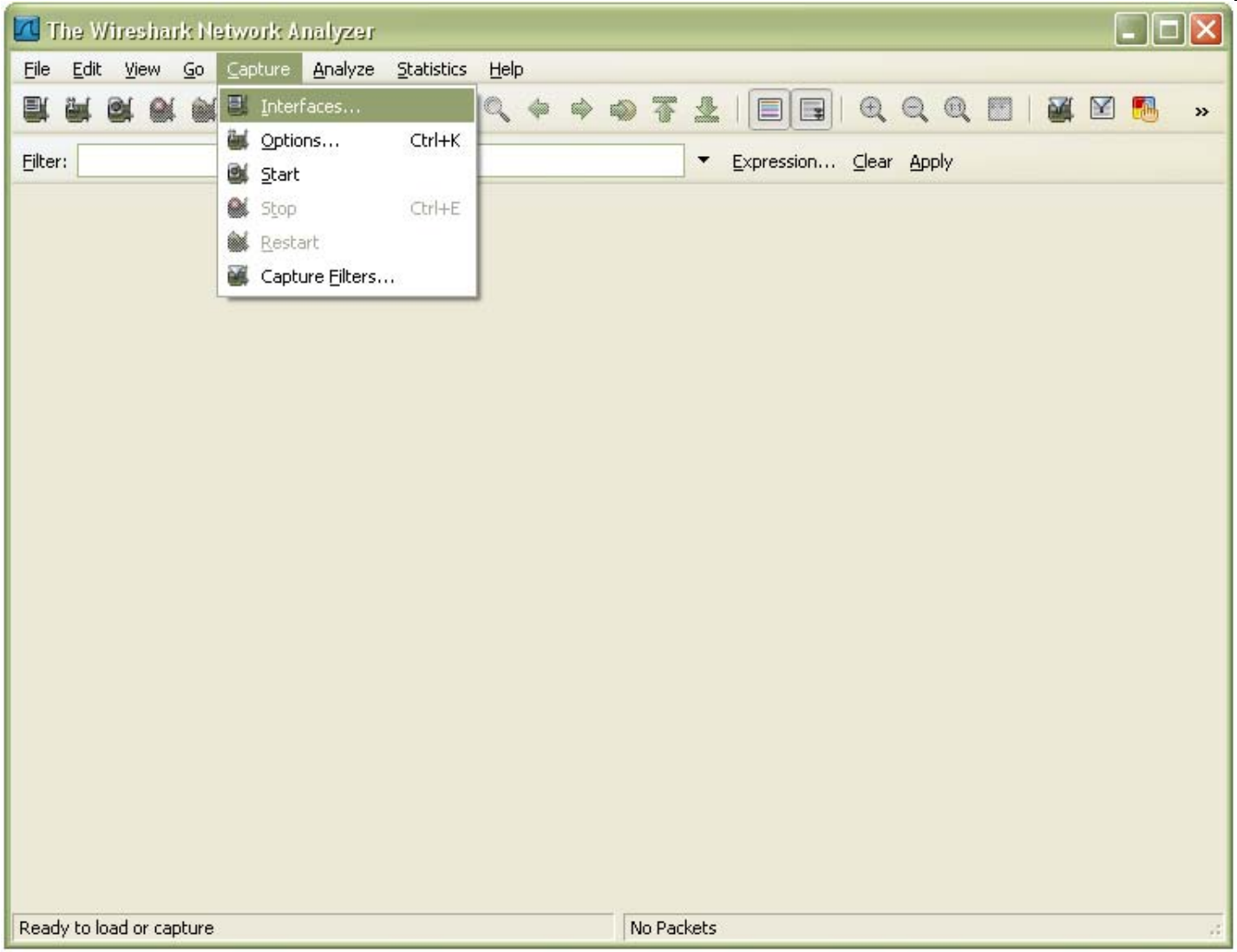
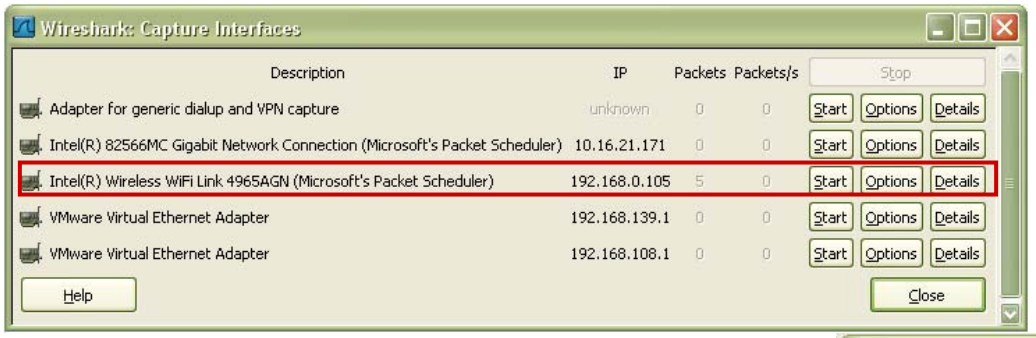


Figure 2: Wireshark Graphical User Interface

Running Wireshark (cnt'd)



Running Wireshark (cnt'd)

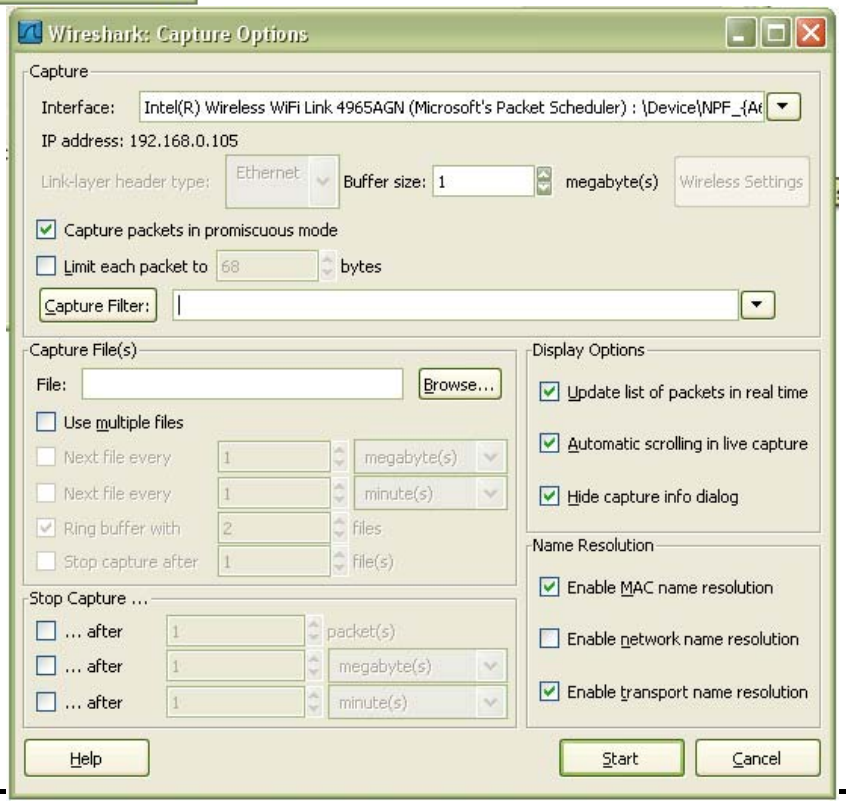


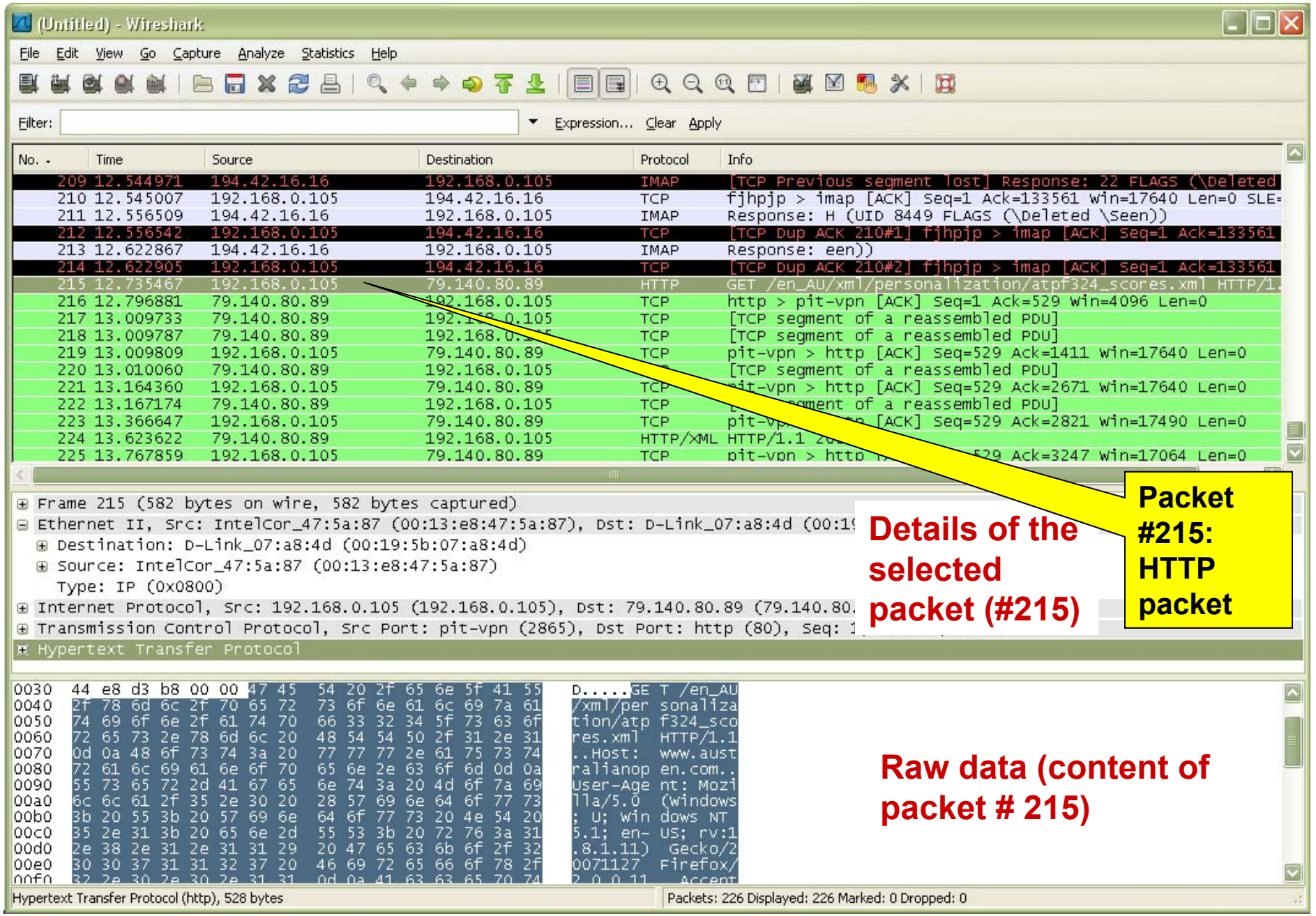
Choose a network interface card press Options

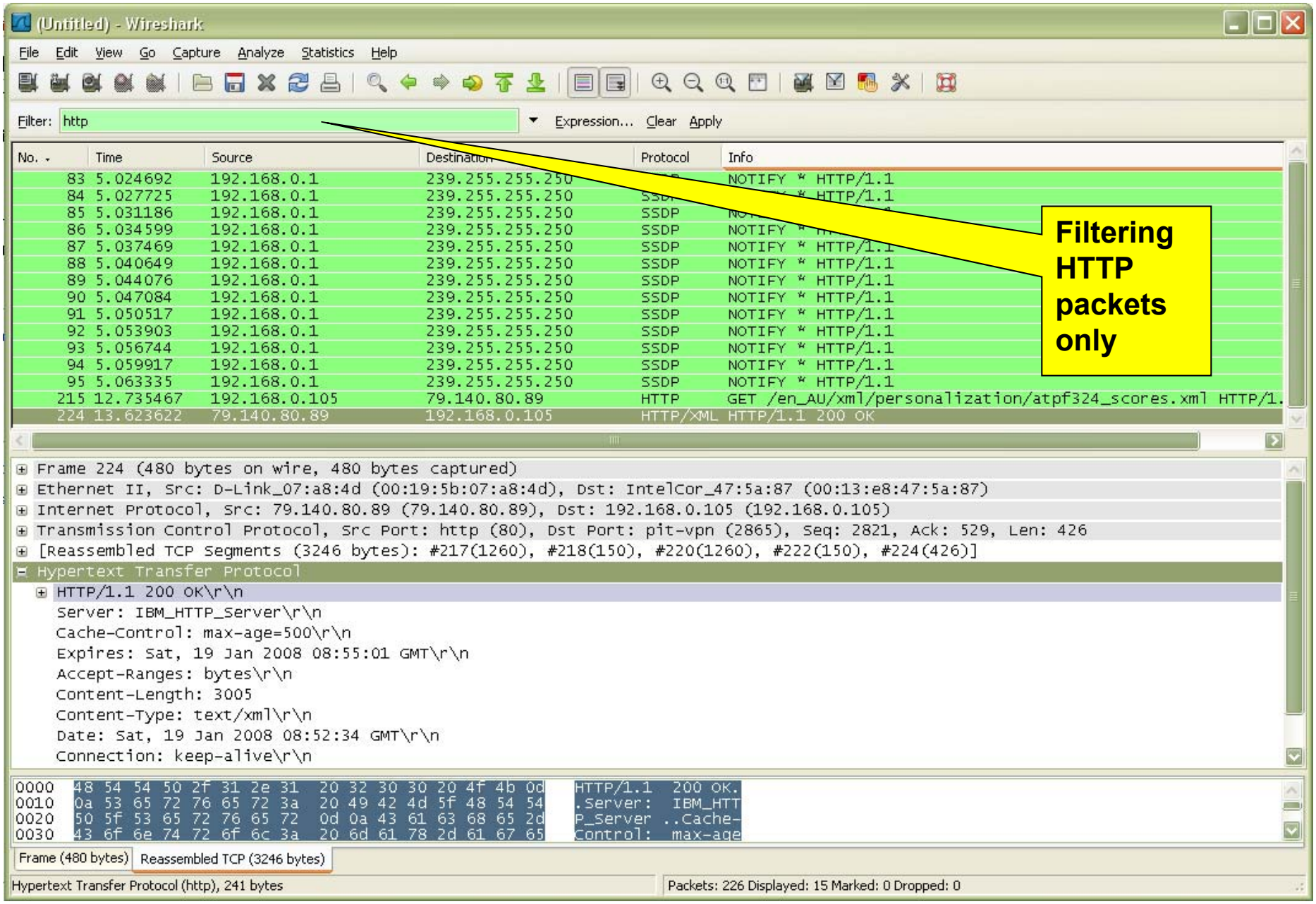
1

2

Sniffing parameters on the selected network interface card




(Untitled) - Wireshark
File Edit View Go Capture Analyze Statistics Help
Filter: Expression... Clear Apply
No. Time Source Destination Protocol Info
209 12.544971 194.42.16.16 192.168.0.105 IMAP [TCP Previous segment lost] Response: 22 FLAGS (\Deleted
210 12.545007 192.168.0.105 194.42.16.16 TCP fjhpjp > imap [ACK] Seq=1 Ack=133561 Win=17640 Len=0 SLE=
211 12.556509 194.42.16.16 192.168.0.105 IMAP Response: H (UID 8449 FLAGS (\Deleted \Seen))
212 12.556542 192.168.0.105 194.42.16.16 TCP [TCP Dup ACK 210#1] fjhpjp > imap [ACK] Seq=1 Ack=133561
213 12.622867 194.42.16.16 192.168.0.105 IMAP Response: een))
214 12.622905 192.168.0.105 194.42.16.16 TCP [TCP Dup ACK 210#2] fjhpjp > imap [ACK] Seq=1 Ack=133561
215 12.735467 192.168.0.105 79.140.80.89 HTTP GET /en_AU/xml/personalization/atpf324_scores.xml HTTP/1.
216 12.796881 79.140.80.89 192.168.0.105 TCP http > pit-vpn [ACK] Seq=1 Ack=529 Win=4096 Len=0
217 13.009733 79.140.80.89 192.168.0.105 TCP [TCP segment of a reassembled PDU]
218 13.009787 79.140.80.89 192.168.0.1 TCP [TCP segment of a reassembled PDU]
219 13.009809 192.168.0.105 79.140.80.89 TCP pit-vpn > http [ACK] Seq=529 Ack=1411 Win=17640 Len=0
220 13.010060 79.140.80.89 192.168.0.105 TCP [TCP segment of a reassembled PDU]
221 13.164360 192.168.0.105 79.140.80.89 TCP pit-vpn > http [ACK] Seq=529 Ack=2671 Win=17640 Len=0
222 13.167174 79.140.80.89 192.168.0.105 TCP [TCP segment of a reassembled PDU]
223 13.366647 192.168.0.105 79.140.80.89 TCP pit-vpn > http [ACK] Seq=529 Ack=2821 Win=17490 Len=0
224 13.623622 79.140.80.89 192.168.0.105 HTTP/XML HTTP/1.1
225 13.767859 192.168.0.105 79.140.80.89 TCP pit-vpn > http
Frame 215 (582 bytes on wire, 582 bytes captured)
Ethernet II, Src: IntelCor_47:5a:87 (00:13:e8:47:5a:87), Dst: D-Link_07:a8:4d (00:19
Destination: D-Link_07:a8:4d (00:19:5b:07:a8:4d)
Source: IntelCor_47:5a:87 (00:13:e8:47:5a:87)
Type: IP (0x0800)
Internet Protocol, Src: 192.168.0.105 (192.168.0.105), Dst: 79.140.80.89 (79.140.80.
Transmission Control Protocol, Src Port: pit-vpn (2865), Dst Port: http (80), Seq:
Hypertext Transfer Protocol
0030 44 e8 d3 b8 00 00 47 45 54 20 2f 65 6e 5f 41 55 D.....GE T /en_AU
0040 2f 78 6d 6c 2f 70 65 72 73 6f 6e 61 6c 69 7a 61 /xml/per sonaliza
0050 74 69 6f 6e 2f 61 74 70 66 33 32 34 5f 73 63 6f tion/atp f324_sco
0060 72 65 73 2e 78 6d 6c 20 48 54 54 50 2f 31 2e 31 res.xml HTTP/1.1
0070 0d 0a 48 6f 73 74 3a 20 77 77 77 2e 61 75 73 74 ..Host: www.aust
0080 72 61 6c 69 61 6e 6f 70 65 6e 2e 63 6f 6d 0d 0a ralianop en.com..
0090 55 73 65 72 2d 41 67 65 6e 74 3a 20 4d 6f 7a 69 User-Age nt: Mozi
00a0 6c 6c 61 2f 35 2e 30 20 28 57 69 6e 64 6f 77 73 lla/5.0 (Windows
00b0 3b 20 55 3b 20 57 69 6e 64 6f 77 73 20 4e 54 20 ; U; Win dows NT
00c0 35 2e 31 3b 20 65 6e 2d 55 53 3b 20 72 76 3a 31 5.1; en- US; rv:1
00d0 2e 38 2e 31 2e 31 31 29 20 47 65 63 6b 6f 2f 32 .8.1.11) Gecko/2
00e0 30 30 37 31 31 32 37 20 46 69 72 65 66 6f 78 2f 0071127 Firefox/
00f0 32 2e 30 2e 30 2e 31 31 0d 0a 41 63 63 65 70 74 2.0.0.11 Accept
Hypertext Transfer Protocol (http), 528 bytes
Packets: 226 Displayed: 226 Marked: 0 Dropped: 0
Details of the selected packet (#215)
Packet #215: HTTP packet
Raw data (content of packet # 215)


(Untitled) - Wireshark
File Edit View Go Capture Analyze Statistics Help
Filter: http
Expression... Clear Apply
No. Time Source Destination Protocol Info
83 5.024692 192.168.0.1 239.255.255.250 NOTIFY * HTTP/1.1
84 5.027725 192.168.0.1 239.255.255.250 NOTIFY * HTTP/1.1
85 5.031186 192.168.0.1 239.255.255.250 SSDP
86 5.034599 192.168.0.1 239.255.255.250 SSDP
87 5.037469 192.168.0.1 239.255.255.250 SSDP
88 5.040649 192.168.0.1 239.255.255.250 SSDP NOTIFY * HTTP/1.1
89 5.044076 192.168.0.1 239.255.255.250 SSDP NOTIFY * HTTP/1.1
90 5.047084 192.168.0.1 239.255.255.250 SSDP NOTIFY * HTTP/1.1
91 5.050517 192.168.0.1 239.255.255.250 SSDP NOTIFY * HTTP/1.1
92 5.053903 192.168.0.1 239.255.255.250 SSDP NOTIFY * HTTP/1.1
93 5.056744 192.168.0.1 239.255.255.250 SSDP NOTIFY * HTTP/1.1
94 5.059917 192.168.0.1 239.255.255.250 SSDP NOTIFY * HTTP/1.1
95 5.063335 192.168.0.1 239.255.255.250 SSDP NOTIFY * HTTP/1.1
215 12.735467 192.168.0.105 79.140.80.89 HTTP GET /en_AU/xml/personalization/atpf324_scores.xml HTTP/1.
224 13.623622 79.140.80.89 192.168.0.105 HTTP/XML HTTP/1.1 200 OK
Filtering HTTP packets only
Frame 224 (480 bytes on wire, 480 bytes captured)
Ethernet II, Src: D-Link_07:a8:4d (00:19:5b:07:a8:4d), Dst: IntelCor_47:5a:87 (00:13:e8:47:5a:87)
Internet Protocol, Src: 79.140.80.89 (79.140.80.89), Dst: 192.168.0.105 (192.168.0.105)
Transmission Control Protocol, Src Port: http (80), Dst Port: pit-vpn (2865), Seq: 2821, Ack: 529, Len: 426
[Reassembled TCP Segments (3246 bytes): #217(1260), #218(150), #220(1260), #222(150), #224(426)]
Hypertext Transfer Protocol
HTTP/1.1 200 OK\r\n
Server: IBM_HTTP_Server\r\n
Cache-Control: max-age=500\r\n
Expires: Sat, 19 Jan 2008 08:55:01 GMT\r\n
Accept-Ranges: bytes\r\n
Content-Length: 3005
Content-Type: text/xml\r\n
Date: Sat, 19 Jan 2008 08:52:34 GMT\r\n
Connection: keep-alive\r\n
0000 48 54 54 50 2f 31 2e 31 20 32 30 30 20 4f 4b 0d HTTP/1.1 200 OK.
0010 0a 53 65 72 76 65 72 3a 20 49 42 4d 5f 48 54 54 .Server: IBM_HTT
0020 50 5f 53 65 72 76 65 72 0d 0a 43 61 63 68 65 2d P_Server ..Cache-
0030 43 6f 6e 74 72 6f 6c 3a 20 6d 61 78 2d 61 67 65 Control: max-age
Frame (480 bytes) Reassembled TCP (3246 bytes)
Hypertext Transfer Protocol (http), 241 bytes
Packets: 226 Displayed: 15 Marked: 0 Dropped: 0