Packet Analysis with Wireshark

EE4204: Computer Networks

Mehul Motani

motani@nus.edu.sg

* The material is adapted from J.F. Kurose & K.W. Ross, "*Computer Networking: A Top-Down Approach Featuring the Internet*", 4rd Edition.

Packet Capture & Analysis

- Currently data travels around the network like a train. With a packet sniffer, you can capture the data and look inside the packets to see what is actually moving around the network.
- Process of capturing, decoding, and analyzing network traffic
- Also known as traffic analysis, protocol analysis, sniffing, network analysis, eavesdropping, etc.
- Common packet analyzers
  - Wireshark, Ethereal
  - Tcpdump, Windump

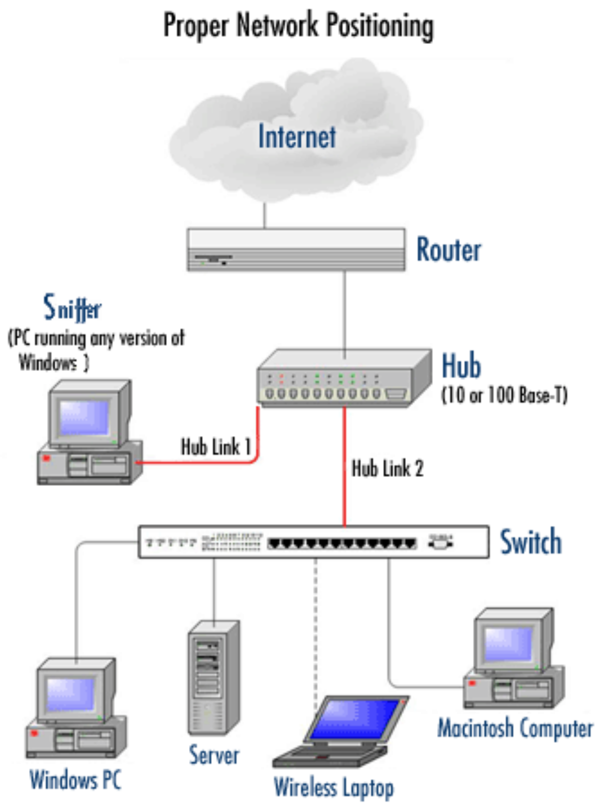
Who Uses Packet Analyzers

- System administrators
  - Understand system problems and performance
  - Intrusion detection
- Malicious individuals (intruders)
  - Capture cleartext data
  - 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)

Packet Capturer + Packet Analyzer

- Packet Sniffer = Packet Capturer + Packet Analyzer
- A combination of hardware and software tools what can detect, decode, and manipulate traffic on the network
- Packet Capture module
  - Receives a copy of every link-layer frame that is sent from or received by your computer
  - Libpcap (UNIX) and Winpcap (Windows)
- Packet Analyzer
  - Displays the contents of all fields within a protocol message
  - Understands the structure of all messages exchanged by protocols

Packet Sniffer in the Network



- Captures messages being sent/received
- Store and/or display the contents of the various protocol fields in these captured messages.
- A packet sniffer itself is passive.
- Packets are never explicitly addressed to the packet sniffer.

What is Wireshark?

- An free open source packet analyzer
- Captures network packets (link layer PDUs)
- Displays detailed PDU information
- Decodes over 750 protocols
- Compatible with many other sniffers
- Plenty of online resources are available
- Supports command-line and GUI interfaces
- Formerly called ***Ethereal***

Why use Wireshark ?

- Troubleshoot a network.
- Debug protocol implementations
- Detect network intrusion attempts.
- Monitor the network usage and filter for suspicious content
- Spy on other network users and collect their passwords. ← **Don't do this!**

Packet Analyzer

Is Wireshark a Packet Analyzer or Packet Capturer

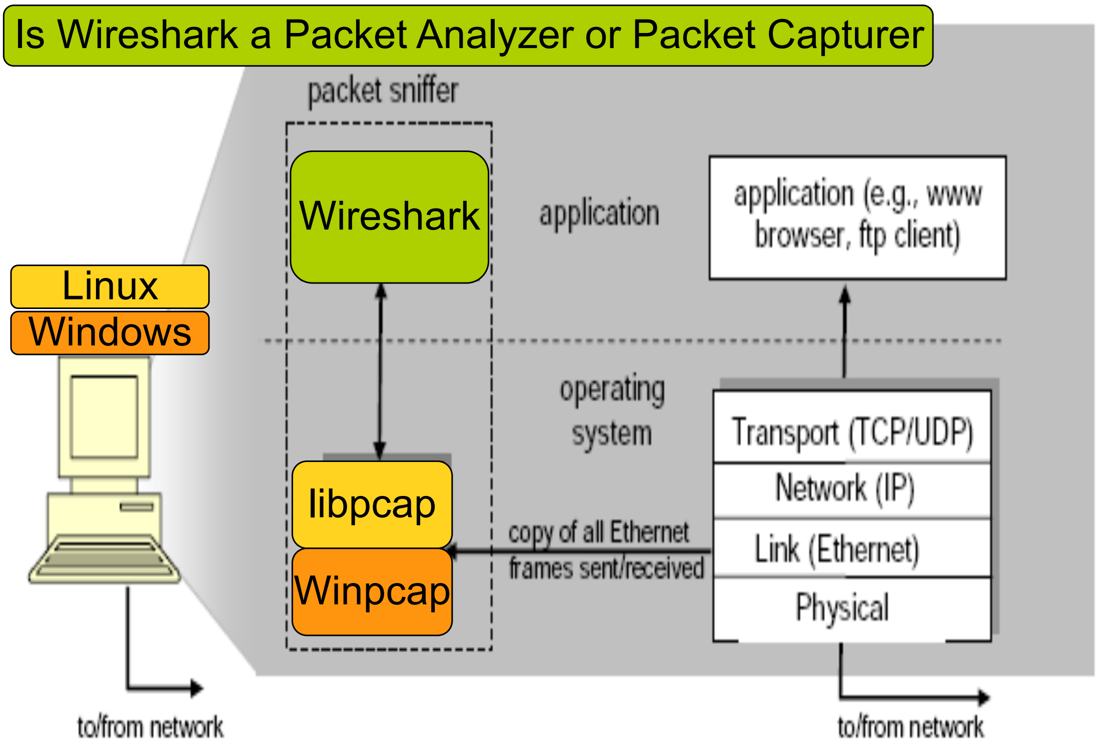
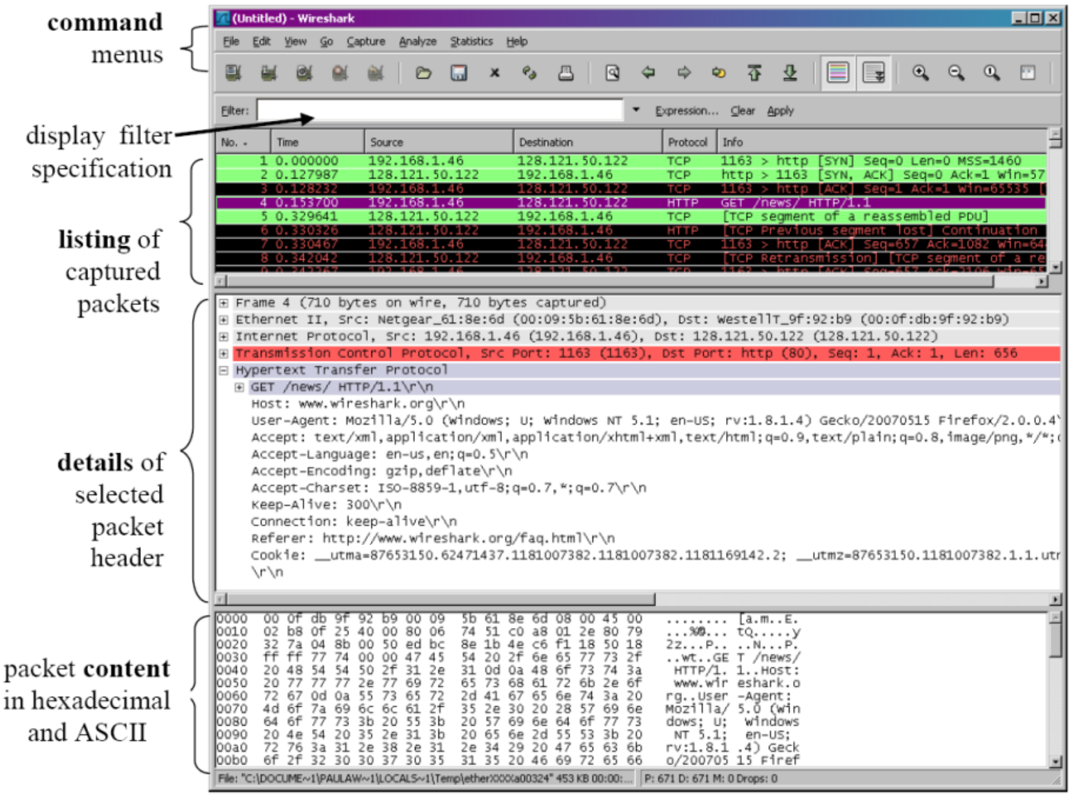


Figure 1: Packet sniffer structure

Wireshark User Interface


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
```

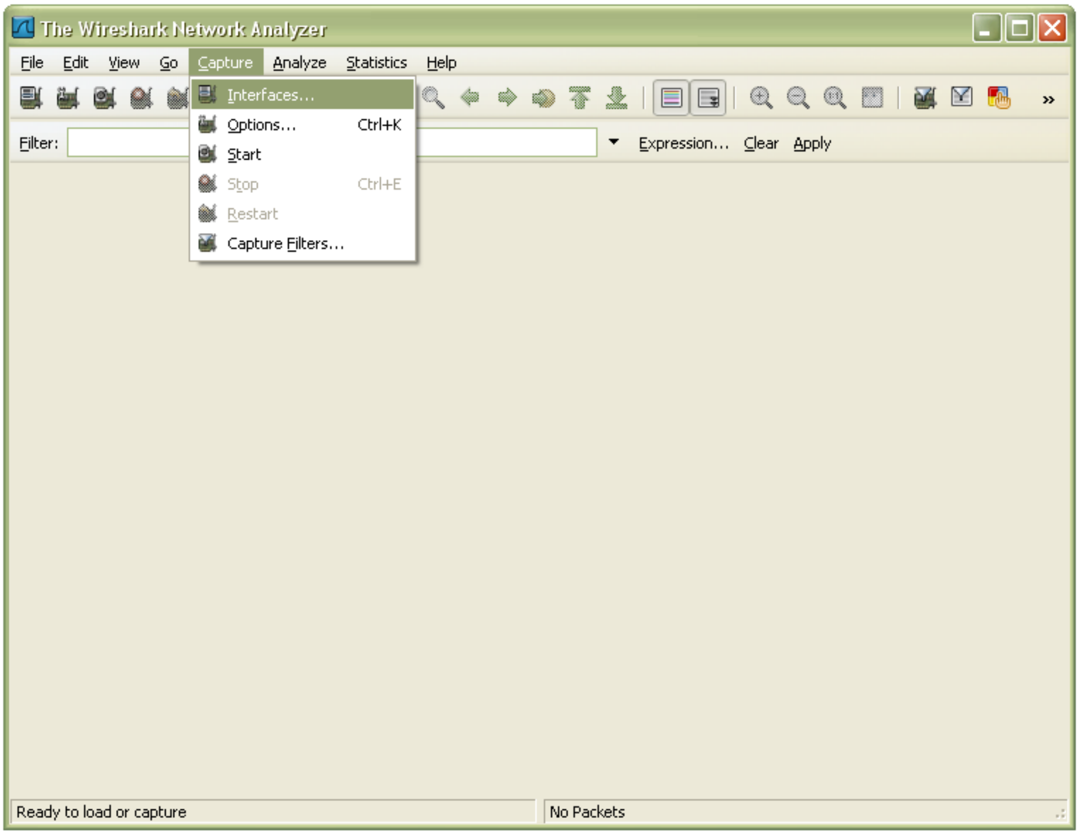
```
⊞ Frame 4 (710 bytes on wire, 710 bytes captured)
⊞ Ethernet II, Src: Netgear_61:8e:6d (00:09:5b:61:8e:6d), Dst: WestellT_9f:92:b9 (00:0f:db:9f:92:b9)
⊞ Internet Protocol, Src: 192.168.1.46 (192.168.1.46), Dst: 128.121.50.122 (128.121.50.122)
⊞ Transmission Control Protocol, Src Port: 1163 (1163), 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

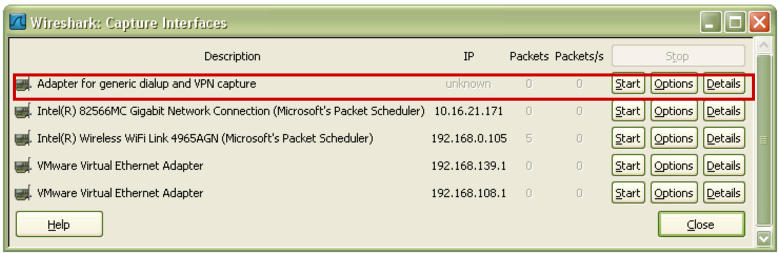
Figure 2: Wireshark Graphical User Interface

Running Wireshark


The Wireshark Network Analyzer
File Edit View Go Capture Analyze Statistics Help
Interfaces...
Options... Ctrl+K
Start
Stop Ctrl+E
Restart
Capture Filters...
Filter:
Expression... Clear Apply

Ready to load or capture No Packets

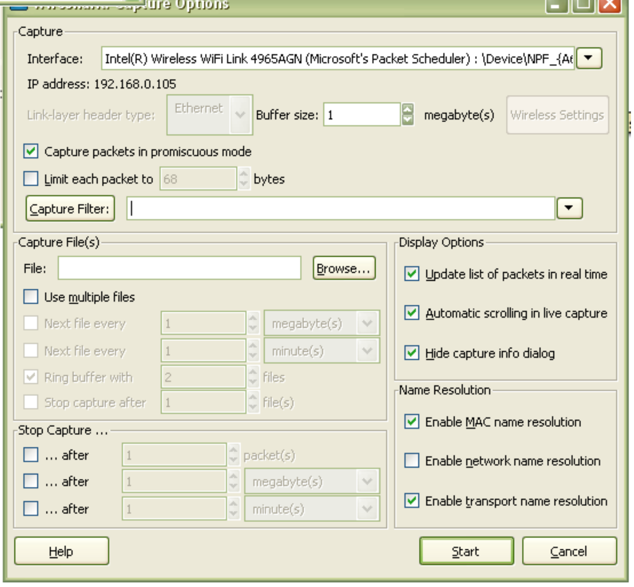
Running Wireshark



Wireshark: Capture Interfaces

	Description	IP	Packets	Packets/s	Stop		
	Adapter for generic dialup and VPN capture	unknown	0	0	Start	Options	Details
	Intel(R) 82566MC Gigabit Network Connection (Microsoft's Packet Scheduler)	10.16.21.171	0	0	Start	Options	Details
	Intel(R) Wireless WiFi Link 4965AGN (Microsoft's Packet Scheduler)	192.168.0.105	5	0	Start	Options	Details
	VMware Virtual Ethernet Adapter	192.168.139.1	0	0	Start	Options	Details
	VMware Virtual Ethernet Adapter	192.168.108.1	0	0	Start	Options	Details

- Choose a network interface card



...ure Options

Capture

Interface: Intel(R) Wireless WiFi Link 4965AGN (Microsoft's Packet Scheduler) : \Device\NPF_{A

IP address: 192.168.0.105

Link-layer header type: Ethernet Buffer size: 1 megabyte(s) Wireless Settings

☑ Capture packets in promiscuous mode

□ Limit each packet to 68 bytes

Capture Filter:

Capture File(s)

File: Browse...

□ Use multiple files

□ Next file every 1 megabyte(s)

□ Next file every 1 minute(s)

☑ Ring buffer with 2 files

□ Stop capture after 1 file(s)

Stop Capture ...

□ ... after 1 packet(s)

□ ... after 1 megabyte(s)

□ ... after 1 minute(s)

Display Options

☑ Update list of packets in real time

☑ Automatic scrolling in live capture

☑ Hide capture info dialog

Name Resolution

☑ Enable MAC name resolution

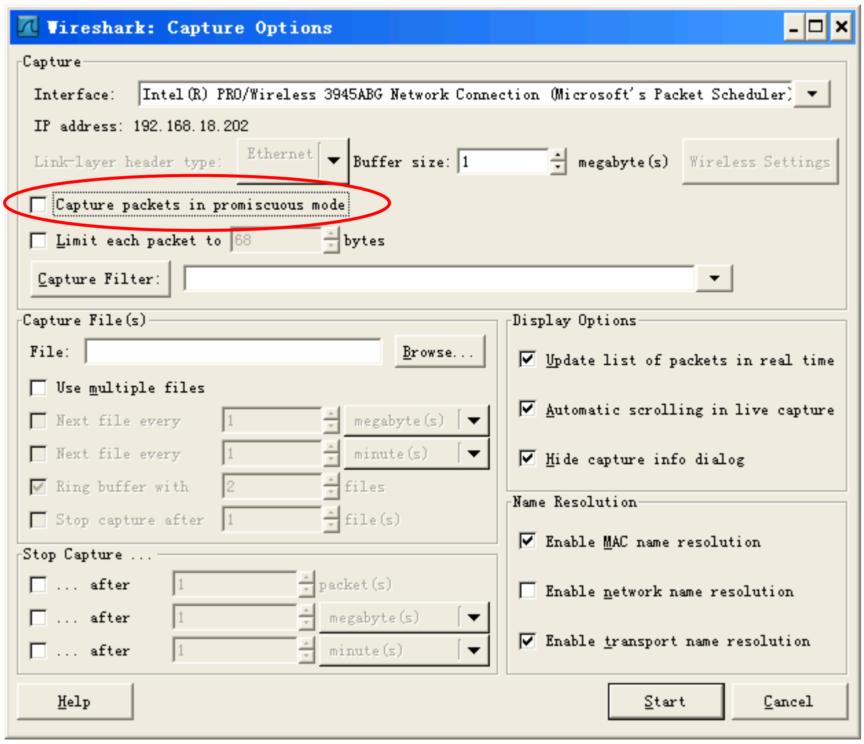
□ Enable network name resolution

☑ Enable transport name resolution

- Sniffing parameters on the selected network interface card

Promiscuous mode

This checkbox puts the interface in **promiscuous** mode when capturing, else Wireshark only captures packets going to or from your computer (not all packets on your LAN segment).



Wireshark: Capture Options

Capture

Interface: Intel(R) PRO/Wireless 3945ABG Network Connection (Microsoft's Packet Scheduler)

IP address: 192.168.18.202

Link-layer header type: Ethernet Buffer size: 1 megabyte(s) Wireless Settings

□ Capture packets in promiscuous mode

□ Limit each packet to 68 bytes

Capture Filter:

Capture File(s)

File: Browse...

□ Use multiple files

□ Next file every 1 megabyte(s)

□ Next file every 1 minute(s)

☑ Ring buffer with 2 files

□ Stop capture after 1 file(s)

Stop Capture ...

□ ... after 1 packet(s)

□ ... after 1 megabyte(s)

□ ... after 1 minute(s)

Display Options

☑ Update list of packets in real time

☑ Automatic scrolling in live capture

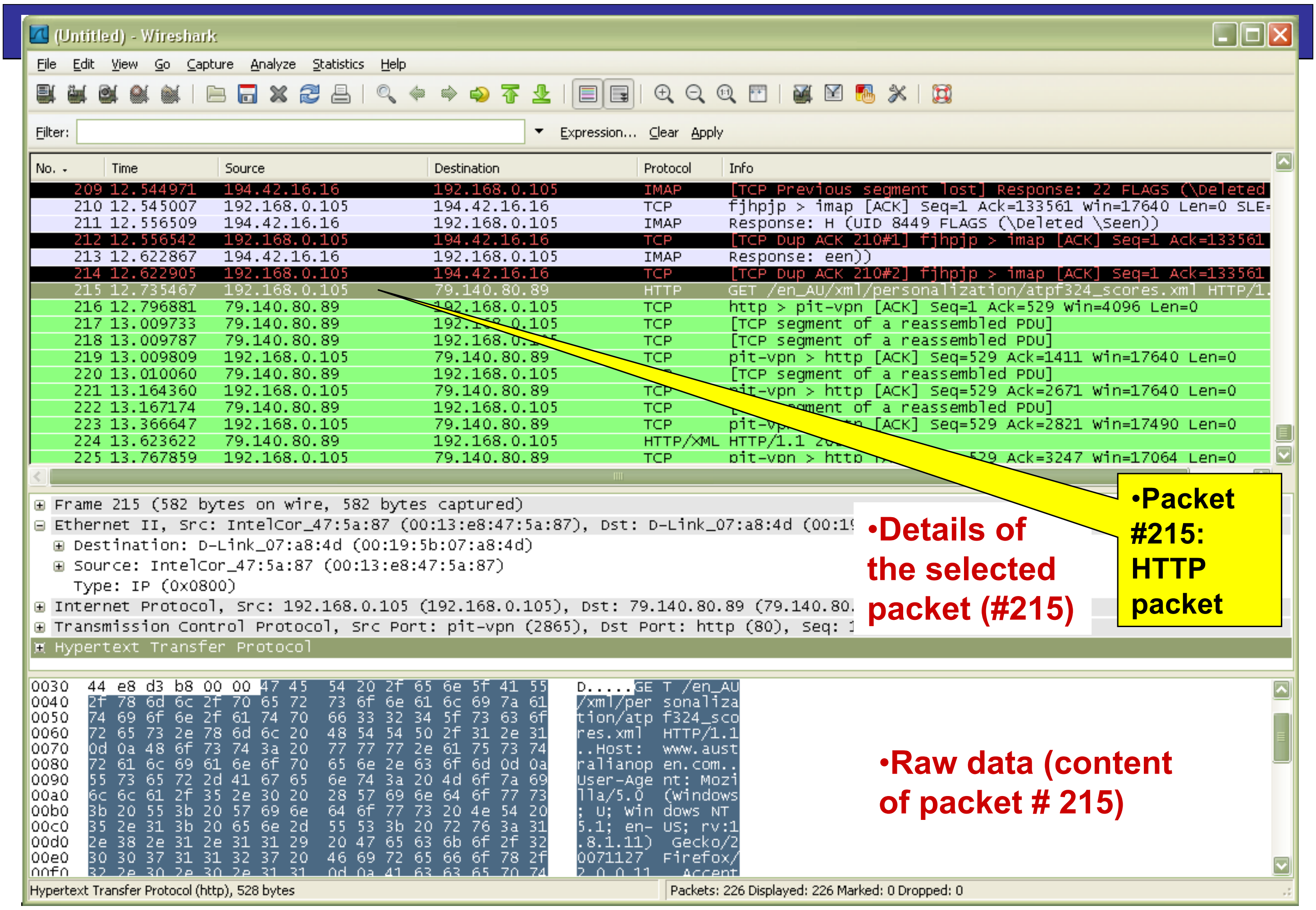
☑ Hide capture info dialog

Name Resolution

☑ Enable MAC name resolution

□ Enable network name resolution

☑ Enable transport name resolution



(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    192.168.0.105   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/1.1 200 OK
  225 13.767859  192.168.0.105   79.140.80.89    TCP       pit-vpn > http [ACK] Seq=529 Ack=3247 Win=17064 Len=0
```

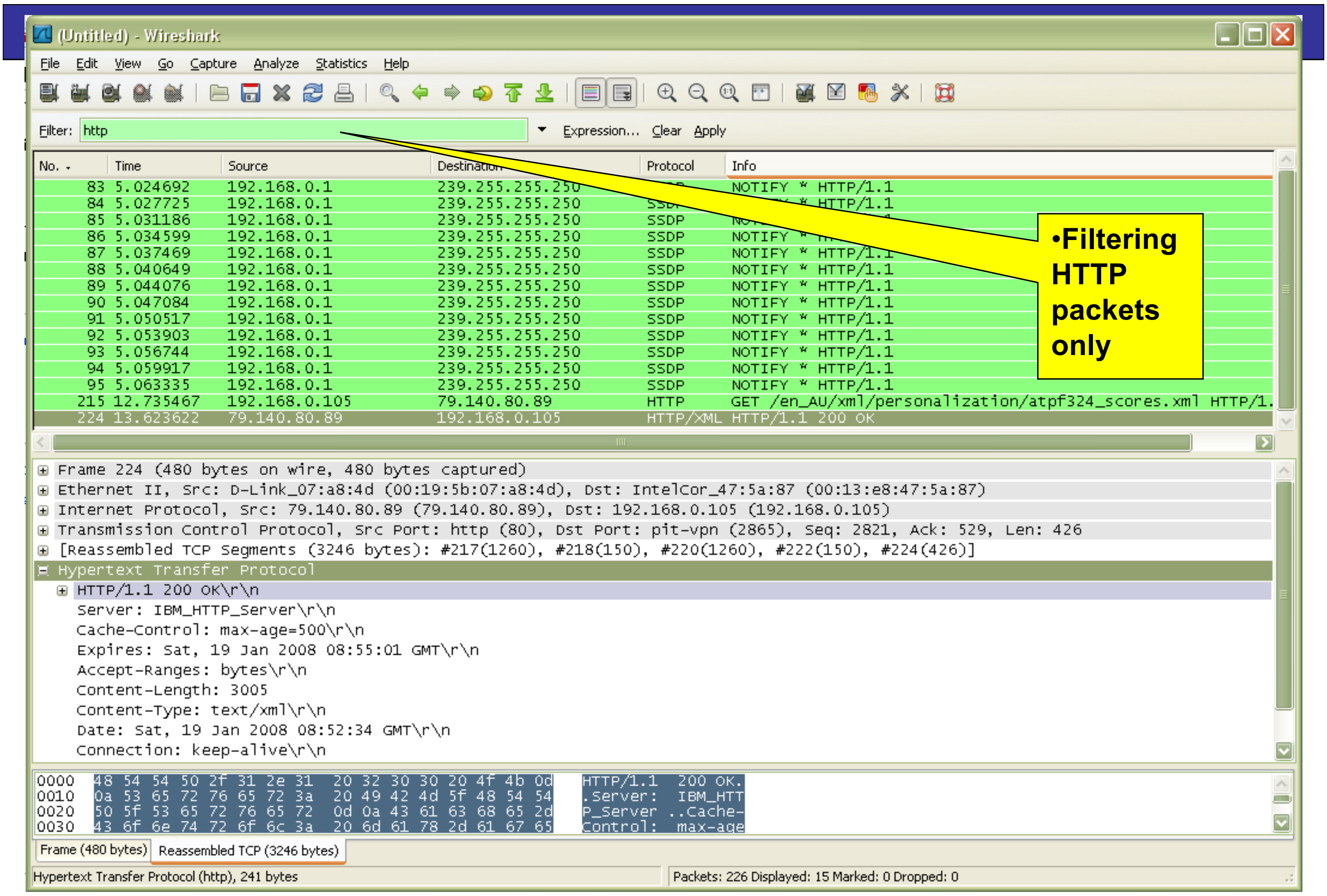
```
⊞ Frame 215 (582 bytes on wire, 582 bytes captured)
⊟ Ethernet II, Src: IntelCor_47:5a:87 (00:13:e8:47:5a:87), Dst: D-Link_07:a8:4d (00:1
    ⊞ Destination: D-Link_07:a8:4d (00:19:5b:07:a8:4d)
    ⊞ Source: IntelCor_47:5a:87 (00:13:e8:47:5a:87)
      Type: IP (0x0800)
⊞ Internet Protocol, Src: 192.168.0.105 (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: 1
⊞ 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

- **Packet #215: HTTP packet**
- **Details of the selected packet (#215)**
- **Raw data (content of packet # 215)**



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

Filter: http

```
No. -  Time       Source          Destination       Protocol  Info
   83 5.024692   192.168.0.1     239.255.255.250   SSDP      NOTIFY * HTTP/1.1
   84 5.027725   192.168.0.1     239.255.255.250   SSDP      NOTIFY * HTTP/1.1
   85 5.031186   192.168.0.1     239.255.255.250   SSDP      NOTIFY * HTTP/1.1
   86 5.034599   192.168.0.1     239.255.255.250   SSDP      NOTIFY * HTTP/1.1
   87 5.037469   192.168.0.1     239.255.255.250   SSDP      NOTIFY * HTTP/1.1
   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
```

```
⊞ 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

- **Filtering HTTP packets only**

Other features

- Filters can be setup to capture or display the packets of the desired patterns
- Captured packets can be stored in disk for later re-loading and analyzing
- Supported OS: Win32, Linux, FreeBSD, Solaris, Mac OS

Download and Installation

- Download Wireshark
  - http://www.wireshark.org/download.html
- Support
  - User's Guide: http://www.wireshark.org/docs/wsug_html_chunked/index.html
  - Wiki: http://wiki.wireshark.org/
- WinPcap – For reference only
  - Wireshark automatically installs WinPcap
  - http://www.winpcap.org/install/default.htm