

Internet Traffic Monitoring and Analysis: Wireshark Tutorial

Dr.S.Geetha

School of Computer Science and Engineering

VIT, Chennai

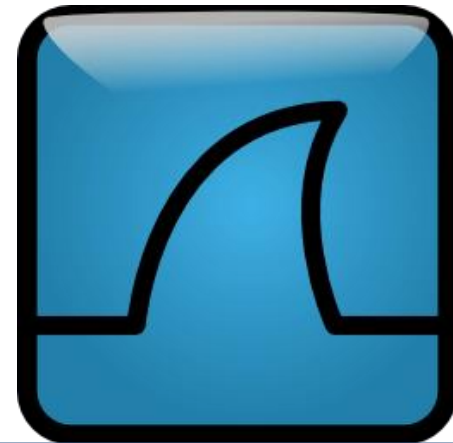
geetha.s@vit.ac.in

Outline

- What is Wireshark?
- Capturing Packets
- Analyzing Packets
- Filtering Packets
- Saving and Manipulating Packets
- Packet Statistics
- Colorizing Specific Packets
- References

What is Wireshark?

- The De-Facto Network Protocol Analyzer
 - Gerald Combs 1998
 - Open-Source (GNU Public License)
 - Multi-platform (Windows, Linux, OS X, Solaris, FreeBSD, NetBSD, and others)
 - Easily extensible
 - Large development group
- Previously Named “Ethereal”



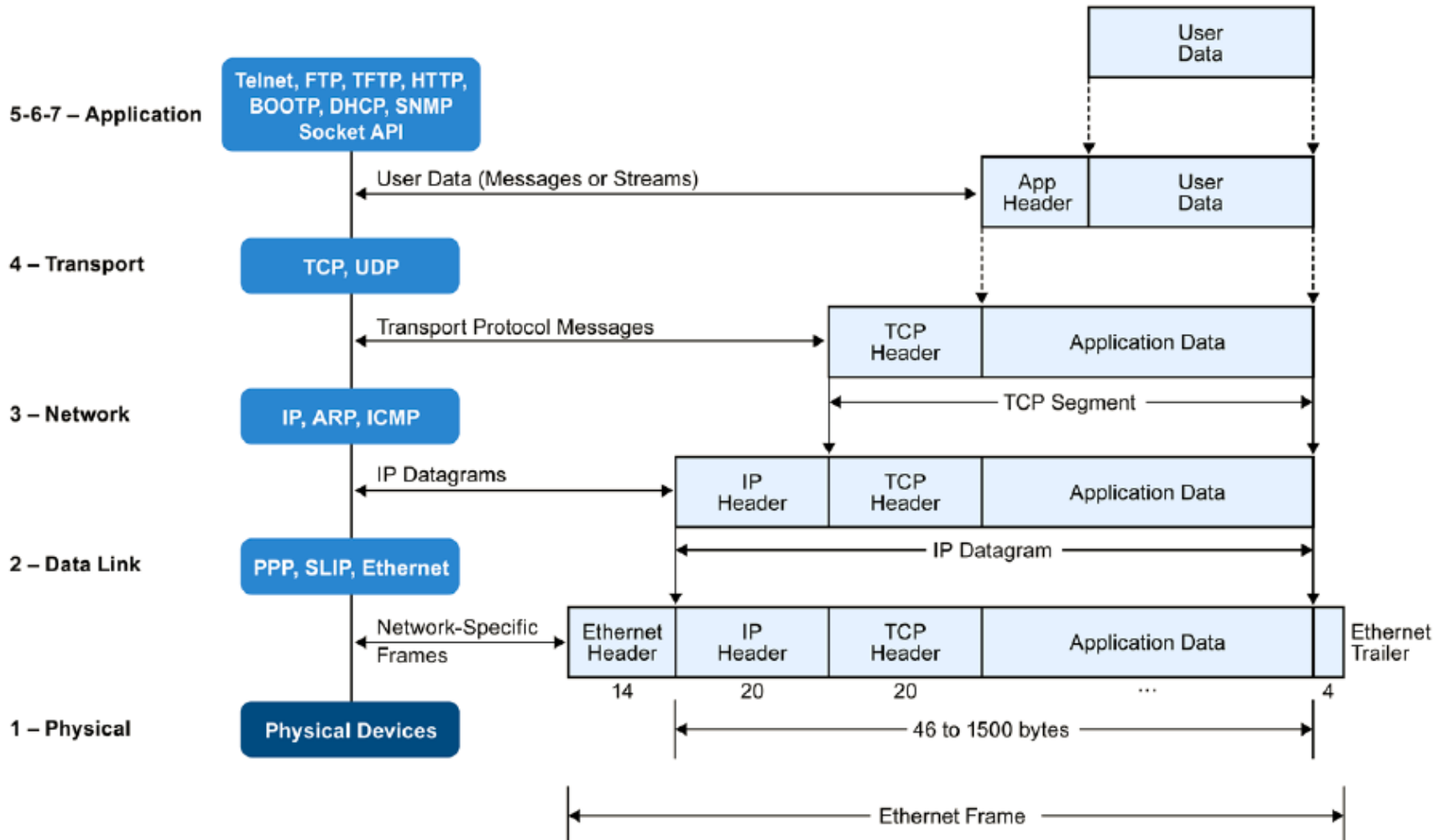
What is Wireshark?

- Features
 - Deep inspection of thousands of protocols
 - Powerful Packet Sniffer
 - Live capture and offline analysis
 - Standard three-pane packet browser
 - Captured network data can be browsed via a GUI, or via the TTY-mode TShark utility
 - The most powerful display filters in the industry
 - Rich VoIP analysis
 - Live data can be read from Ethernet, IEEE 802.11, PPP/HDLC, ATM, Bluetooth, USB, Token Ring, Frame Relay, FDDI, and others
 - Coloring rules can be applied to the packet list for quick, intuitive analysis
 - Output can be exported to XML, PostScript®, CSV, or plain text

What is Wireshark?

- What we can:
 - Capture network traffic
 - Decode packet protocols using dissectors
 - Define filters – capture and display
 - Watch smart statistics
 - Analyze problems
 - Interactively browse that traffic
- Some examples people use Wireshark for:
 - Network administrators: **troubleshoot network problems**
 - Network security engineers: **examine security problems**
 - Developers: **debug protocol implementations**
 - People: **learn network protocol internals**

TCP/IP Traffic



WIRESHARK

Interfaces

The image displays the Wireshark network protocol analyzer interface. The title bar indicates the active interface is 'Intel(R) PRO/Wireless 3945ABG Network Connection (Microsoft's Packet Scheduler) : Capturing - Wireshark'. The menu bar includes File, Edit, View, Go, Capture, Analyze, Statistics, Telephony, Tools, and Help. The toolbar contains icons for file operations, capture control, and analysis. A filter bar is present above the packet list.

Packet List

No.	Time	Source	Destination	Protocol	Info
64	36.858576	192.168.2.100	10.100.102.2	ICMP	Echo (ping) request
65	36.863613	10.100.102.2	192.168.2.100	ICMP	Echo (ping) response
66	44.406189	192.168.2.100	10.100.102.1	SNMP	get-request IF-MIB::ifOperS...
67	44.413024	10.100.102.1	192.168.2.100	SNMP	get-response IF-MIB::ifOper...
68	44.499055	Msi_d4:52:4d	Broadcast	ARP	Who has 1? Tell me
69	45.609033	192.168.2.100	10.40.41.2	ICMP	Echo (ping) request
70	47.797985	192.168.2.100	10.40.41.2	ICMP	Echo (ping) response
71	48.891533	192.168.2.100	10.100.102.1	SNMP	get-request IF-MIB::ifOperS...
72	48.897871	10.100.102.1	192.168.2.100	SNMP	get-response IF-MIB::ifOper...
73	49.989403	192.168.2.100	10.40.41.2	ICMP	Echo (ping) request
74	53.048866	192.168.2.100	255.255.255.255	UDP	Source port: 1027 Destination...

Packet Details

Frame 32 (86 bytes on wire, 86 bytes captured)

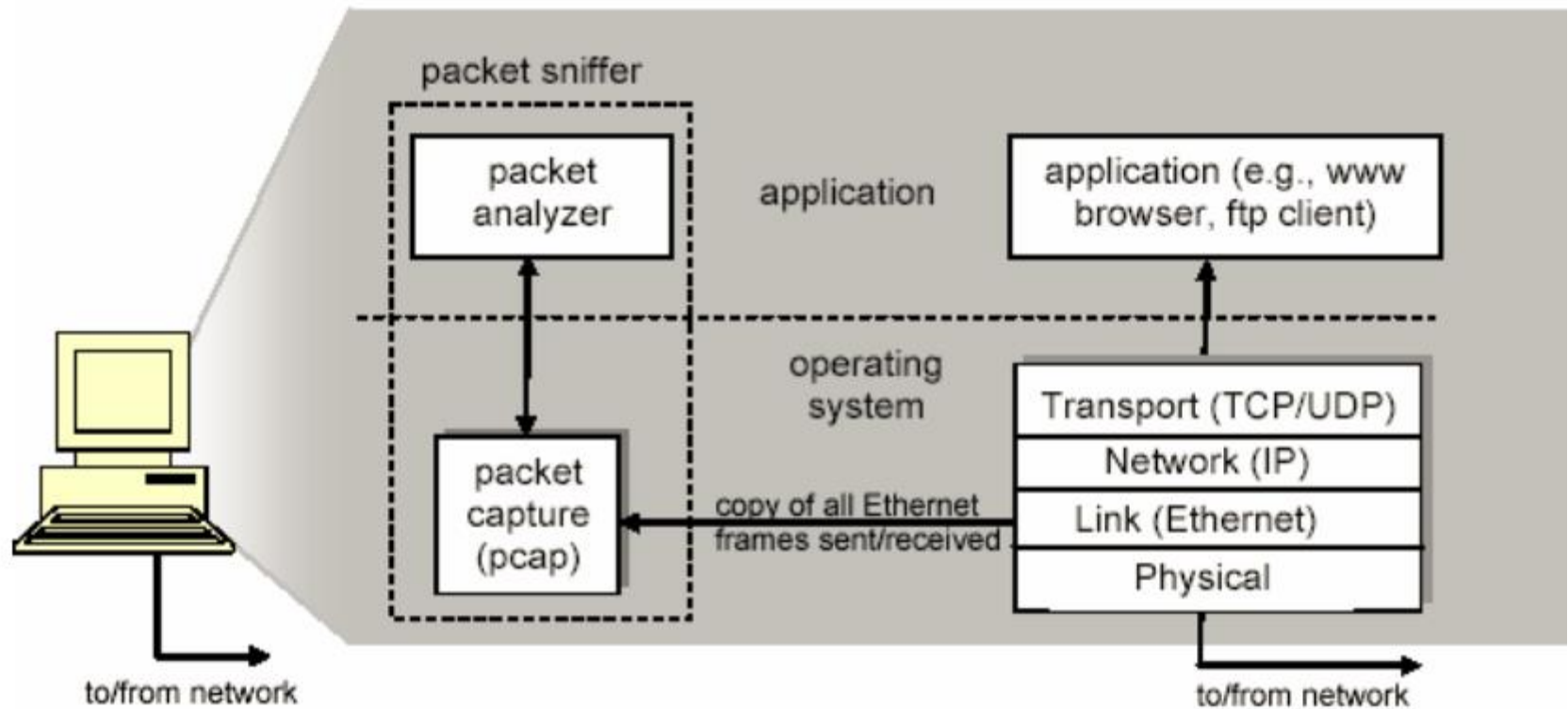
- Ethernet II, Src: IntelCor_a2:d8:9a (00:1c:bf:a2:d8:9a), Dst: EdimaxTe_6e:2f:7d (00:0e:2e:6e:2f:7d)
- Internet Protocol, Src: 192.168.2.100 (192.168.2.100), Dst: 10.100.102.1 (10.100.102.1)
- User Datagram Protocol, Src Port: solid-mux (1029), Dst Port: snmp (161)
 - Source port: solid-mux (1029)
 - Destination port: snmp (161)
 - Length: 52
 - Checksum: 0xa175 [validation disabled]
- Simple Network Management Protocol
 - version: version-1 (0)

Packet Bytes

Offset	Hex	ASCII
0000	00 0e 2e 6e 2f 7d 00 1c bf a2 d8 9a 08 00 45 00	...n/f... ..E..
0010	00 48 04 d4 00 00 80 11 02 60 c0 a8 02 64 0a 64	..H.....d..
0020	66 01 04 05 00 a1 00 34 a1 75 30 2a 02 01 00 04	f.....4..u0*..
0030	06 70 75 62 6c 69 63 a0 1d 02 03 00 e2 af 02 01	.public.....
0040	00 02 01 00 30 10 30 0e 06 0a 2b 06 01 02 01 020.0...+....
0050	02 01 08 05 05 00

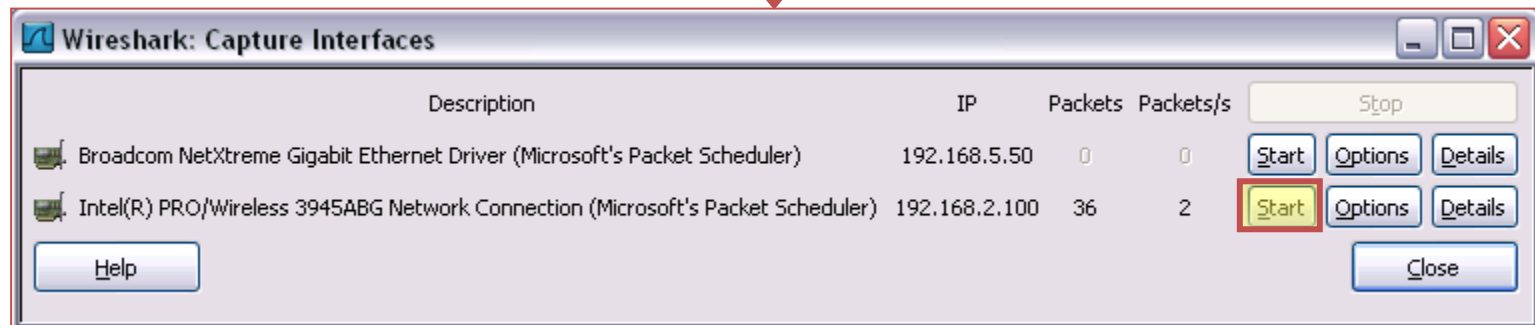
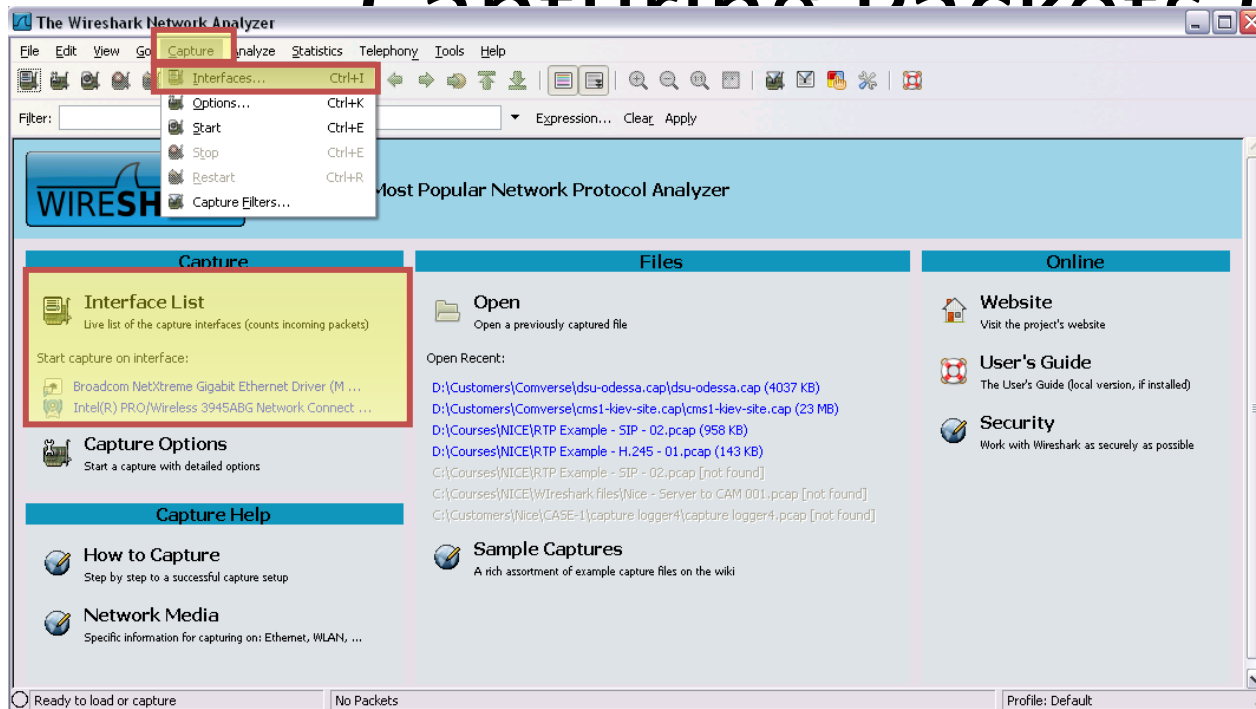
Frame (frame), 86 bytes | Packets: 74 Displayed: 74 Marked: 0 | Profile: Default

Packet Sniffer



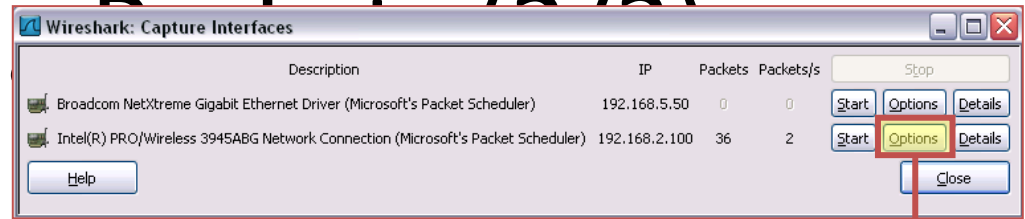
WIRESHARK

Capturing Packets (1/3)



WIRESHARK

Capturing Packets (1/2)



Capture all packets on the network

Buffer size – in order not to fill your laptop disk

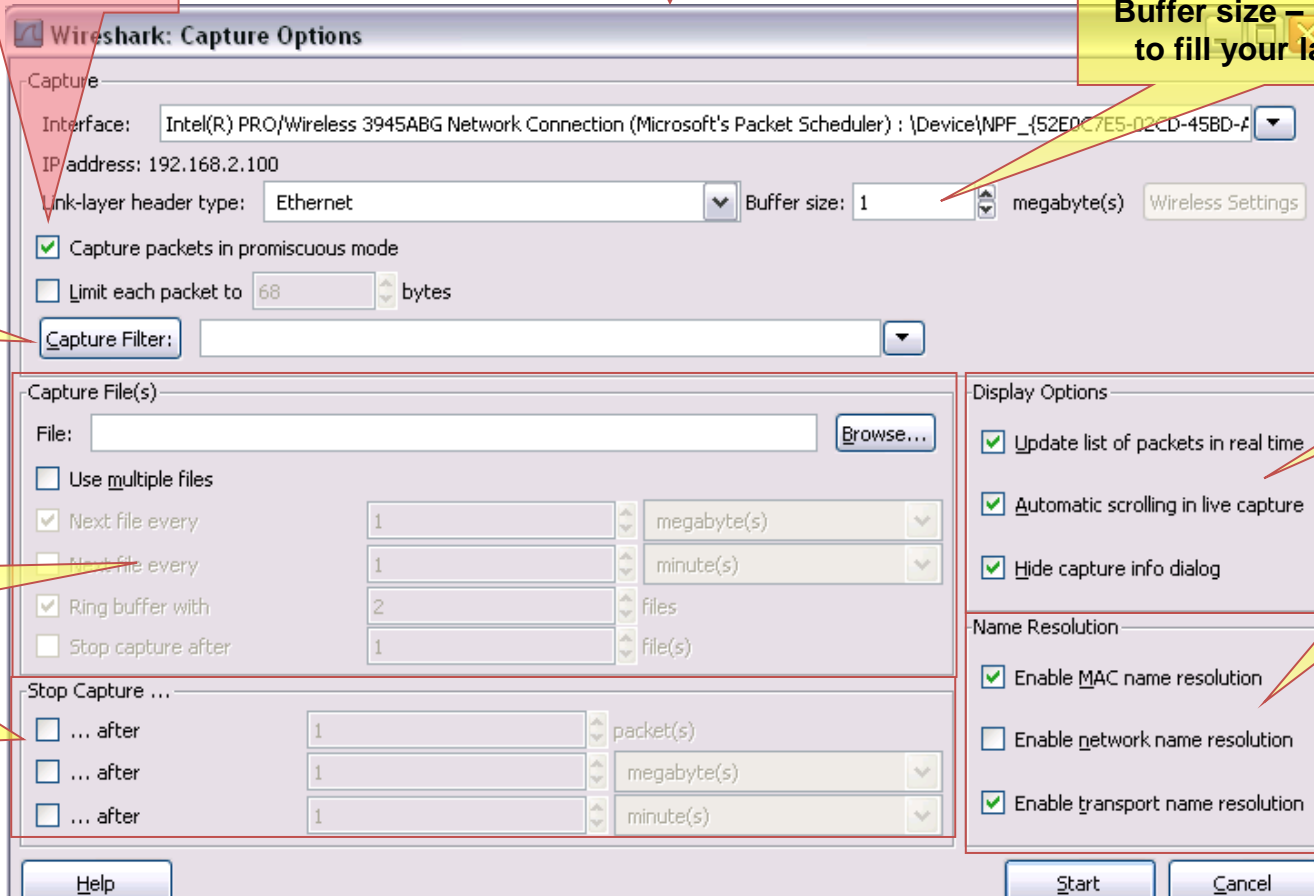
Capture filter

Display options

Capture in multiple files

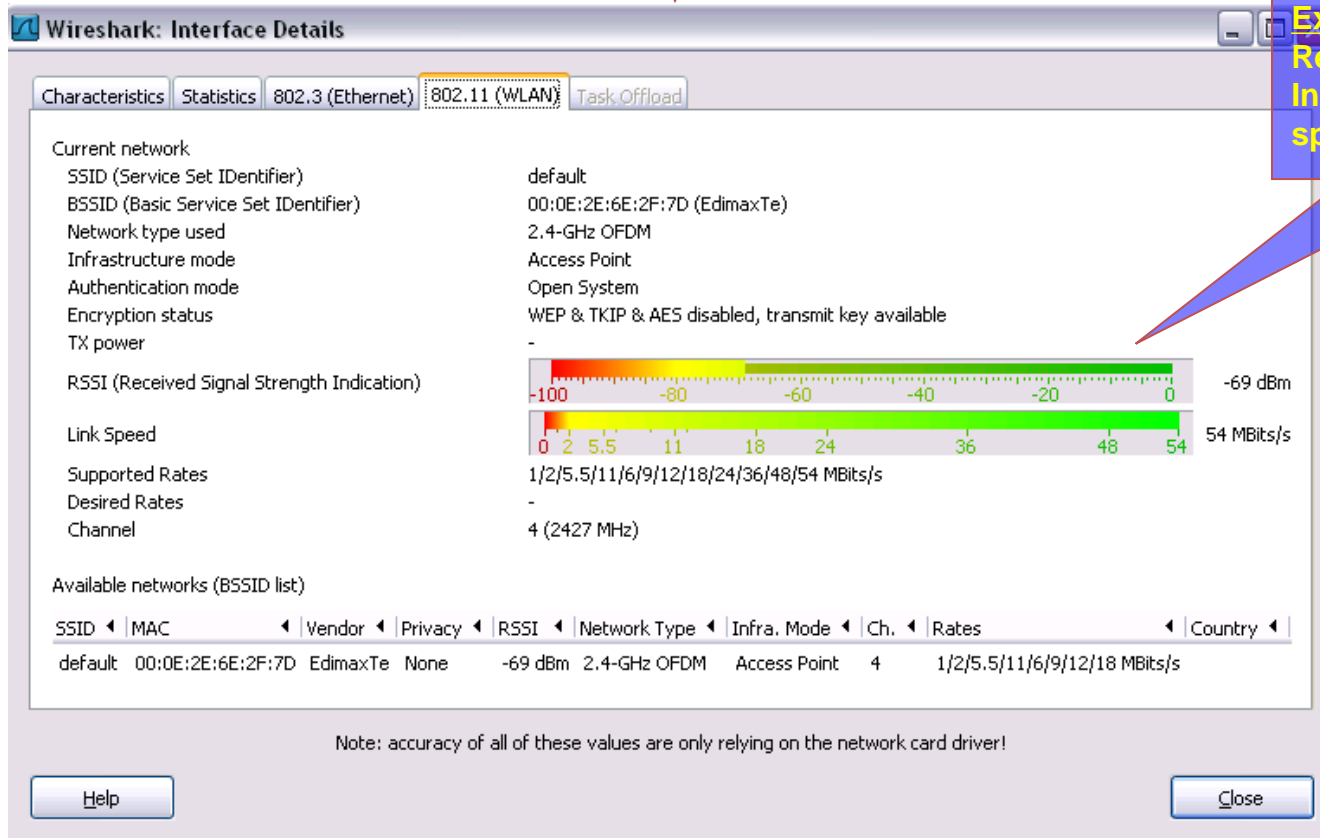
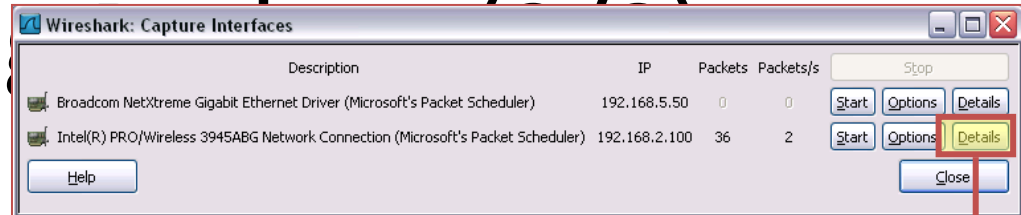
Name resolution options

When to automatically stop the capture



WIRESHARK

Capturing



Example (W-LAN):
Received Signal Strength
Indication (RSSI) and Link
speed (BW)

Analyzing Packets (1/9)

❖ Ethernet Frame Example

The image shows a Wireshark packet capture window. The top toolbar contains various icons for file operations, search, and display. Below the toolbar is a filter bar with a text input field and buttons for 'Expression...', 'Clear', and 'Apply'. The main packet list table displays the following data:

No.	Time	Source	Destination	Protocol	Info
4	23.227539	1.1.1.1	127.0.0.1	UDP	Source port: 55555 Destination...
5	23.838867	212.179.1.202	10.159.3.103	FTP	Response: 200 Type set to I.
6	23.857421	10.159.3.103	212.179.1.202	FTP	Request: SIZE upload1_1936
7	23.996093	212.179.1.202	10.159.3.103	FTP	Response: 213 11026917
8	24.012695	10.159.3.103	212.179.1.202	FTP	Request: MDTM upload1_1936
9	24.208984	212.179.1.202	10.159.3.103	FTP	Response: 213 20071202174050
10	24.266601	10.159.3.103	212.179.1.202	FTP	Request: PASV
11	24.391601	212.179.1.202	10.159.3.103	FTP	Response: 227 Entering Passi...

Below the packet list, the details pane shows the structure of the selected packet (Frame 10). The pane is organized into a tree view with expandable sections:

- Frame 10 (60 bytes on wire, 60 bytes captured)**
 - Arrival Time: Jan 13, 2008 11:44:18.844726000
 - [Time delta from previous captured frame: 0.057617000 seconds]
 - [Time delta from previous displayed frame: 0.057617000 seconds]
 - [Time since reference or first frame: 24.266601000 seconds]
 - Frame Number: 10
 - Frame Length: 60 bytes
 - Capture Length: 60 bytes
 - [Frame is marked: False]
 - [Protocols in frame: eth:ip:tcp:ftp]
 - [Coloring Rule Name: TCP]
 - [Coloring Rule String: tcp]
- Ethernet II, Src: Xerox_00:00:00 (01:00:01:00:00:00), Dst: d4:c8:20:00:01:00 (d4:c8:20:00:01:00)**
 - Destination: d4:c8:20:00:01:00 (d4:c8:20:00:01:00)**
 - Address: d4:c8:20:00:01:00 (d4:c8:20:00:01:00)
 - 0 = IG bit: Individual address (unicast)
 - 0. = LG bit: Globally unique address (factory default)
 - Source: Xerox_00:00:00 (01:00:01:00:00:00)**
 - Address: Xerox_00:00:00 (01:00:01:00:00:00)
 - 1 = IG bit: Group address (multicast/broadcast)
 - 0. = LG bit: Globally unique address (factory default)
 - Type: IP (0x0800)
- Internet Protocol, Src: 10.159.3.103 (10.159.3.103), Dst: 212.179.1.202 (212.179.1.202)**
- Transmission Control Protocol, Src Port: mps-raft (1700), Dst Port: ftp (21), Seq: 47, Ack: 55, Len: 6**
- File Transfer Protocol (FTP)**

Analyzing Packets (2/9)

No. ↓	Time	Source	Destination	Protocol	Info
4	23.227539	1.1.1.1	127.0.0.1	UDP	Source port: 33333 Destination
5	23.838867	212.179.1.202	10.159.3.103	FTP	Response: 200 Type set to I.
6	23.857421	10.159.3.103	212.179.1.202	FTP	Request: SIZE upload1_1936
7	23.996093	212.179.1.202	10.159.3.103	FTP	Response: 213 11026917
8	24.012695	10.159.3.103	212.179.1.202	FTP	Request: MDTM upload1_1936
9	24.208984	212.179.1.202	10.159.3.103	FTP	Response: 213 20071202174050
10	24.266601	10.159.3.103	212.179.1.202	FTP	Request: PASV

+

Frame 10 (60 bytes on wire, 60 bytes captured)

+

Ethernet II, Src: Xerox_00:00:00 (01:00:01:00:00:00), Dst: d4:c8:20:00:01:00 (d4:c8:20:00:01:00)

-

Internet Protocol, Src: 10.159.3.103 (10.159.3.103), Dst: 212.179.1.202 (212.179.1.202)

Version: 4

Header length: 20 bytes

-

Differentiated Services Field: 0x00 (DSCP 0x00: Default; ECN: 0x00)

0000 00.. = Differentiated Services Codepoint: Default (0x00)

.... ..0. = ECN-Capable Transport (ECT): 0

.... ...0 = ECN-CE: 0

Total Length: 46

Identification: 0x5f49 (24393)

-

Flags: 0x04 (Don't Fragment)

0... = Reserved bit: Not set

.1.. = Don't fragment: Set

..0. = More fragments: Not set

Fragment offset: 0

Time to live: 128

Protocol: TCP (0x06)

-

Header checksum: 0xb6fd [correct]

[Good: True]

[Bad : False]

Source: 10.159.3.103 (10.159.3.103)

Destination: 212.179.1.202 (212.179.1.202)

+

Transmission Control Protocol, Src Port: mps-raft (1700), Dst Port: ftp (21), Seq: 47, Ack: 55, Len: 6

-

File Transfer Protocol (FTP)

Analyzing Packets (3/9)

The image shows a Wireshark packet capture analysis of an FTP session. The top toolbar contains various icons for file operations, network analysis, and packet manipulation. Below the toolbar is a filter bar with a text input field and buttons for 'Expression...', 'Clear', and 'Apply'.

The packet list pane shows three packets:

No.	Time	Source	Destination	Protocol	Info
9	24.208984	212.179.1.202	10.159.3.103	FTP	Response: 213 200/1202174050
10	24.266601	10.159.3.103	212.179.1.202	FTP	Request: PASV
11	24.391601	212.179.1.202	10.159.3.103	FTP	Response: 227 Entering Passive

The packet details pane shows the structure of the selected packet (Frame 10):

- Frame 10 (60 bytes on wire, 60 bytes captured)
- Ethernet II, Src: Xerox_00:00:00 (01:00:01:00:00:00), Dst: d4:c8:20:00:01:00 (d4:c8:20:00:01:00)
- Internet Protocol, Src: 10.159.3.103 (10.159.3.103), Dst: 212.179.1.202 (212.179.1.202)
- Transmission Control Protocol, Src Port: mps-raft (1700), Dst Port: ftp (21), Seq: 47, Ack: 55, Len: 6
 - Source port: mps-raft (1700)
 - Destination port: ftp (21)
 - [Stream index: 1]
 - Sequence number: 47 (relative sequence number)
 - [Next sequence number: 53 (relative sequence number)]
 - Acknowledgement number: 55 (relative ack number)
 - Header length: 20 bytes
 - Flags: 0x18 (PSH, ACK)
 - 0... .. = Congestion Window Reduced (CWR): Not set
 - .0.. = ECN-Echo: Not set
 - ..0. = Urgent: Not set
 - ...1 = Acknowledgement: Set
 - 1... = Push: Set
 -0.. = Reset: Not set
 -0. = Syn: Not set
 -0 = Fin: Not set
 - Window size: 16945
 - Checksum: 0x8b8d [validation disabled]
 - [Good Checksum: False]
 - [Bad Checksum: False]
 - [SEQ/ACK analysis]
 - [\[This is an ACK to the segment in frame: 9\]](#)
 - [The RTT to ACK the segment was: 0.057617000 seconds]
 - [Number of bytes in flight: 6]

WIRESHARK

Analyzing Packets (4/9)

(Untitled) - Wireshark

File Edit View Go Capture Analyze Statistics Telephony Tools Help

Filter: Expression... Clear Apply

No.	Time	Source	Destination	Protocol	Info
1	0.000000	192.168.2.100	10.40.41.2	ICMP	Echo (ping) request
2	2.183304	192.168.2.100	10.40.41.2	ICMP	Echo (ping) request
3	3.430100	192.168.2.100	212.150.49.10	DNS	Standard query A www.ynet.co.il
4	3.457181	212.150.49.10	192.168.2.100	DNS	Standard query response CNAME ynet.co.il.d4p.net CNAME a39.g.
5	3.461602	192.168.2.100	212.150.49.10	DNS	Standard query A www.lenovo.com
6	3.623867	192.168.2.100	212.143.162.157	TCP	dzdaemon > http [SYN] Seq=0 Win=65535 Len=0 MSS=1460 WS=1 TSV
7	3.728385	212.143.162.157	192.168.2.100	TCP	http > dzdaemon [SYN, ACK] Seq=0 Ack=1 Win=5840 Len=0 MSS=145
8	3.728429	192.168.2.100	212.143.162.157	TCP	dzdaemon > http [ACK] Seq=1 Ack=1 Win=128480 Len=0
9	3.728839	192.168.2.100	212.143.162.157	HTTP	GET / HTTP/1.1
10	3.768896	212.143.162.157	192.168.2.100	TCP	http > dzdaemon [ACK] Seq=1 Ack=580 Win=6948 Len=0
11	3.770703	212.143.162.157	192.168.2.100	HTTP	HTTP/1.0 301 Moved Permanently
12	3.772411	192.168.2.100	212.143.162.157	HTTP	GET /home/0.7340.L-8.00.html HTTP/1.1

Frame 5 (74 bytes on wire, 74 bytes captured)

- Ethernet II, Src: IntelCor_a2:d8:9a (00:1c:bf:a2:d8:9a), Dst: EdimaxTe_6e:2f:7d (00:0e:2e:6e:2f:7d)
- Internet Protocol, Src: 192.168.2.100 (192.168.2.100), Dst: 212.150.49.10 (212.150.49.10)
- User Datagram Protocol, Src Port: natuslink (2895), Dst Port: domain (53)
- Domain Name System (query)

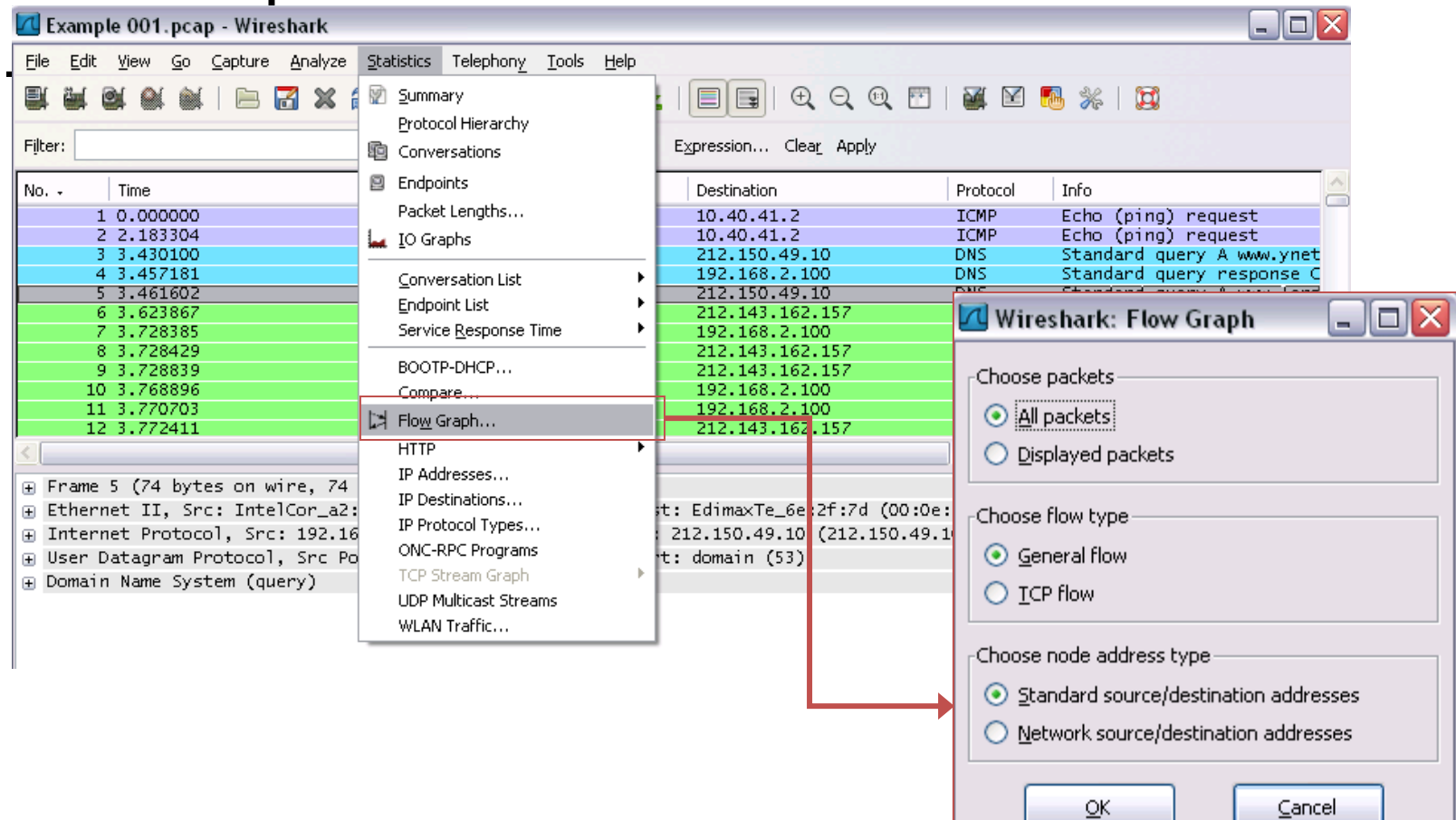
```

0000  00 0e 2e 6e 2f 7d 00 1c bf a2 d8 9a 08 00 45 00  ...n/}.. .....E.
0010  00 3c 7f ea 00 00 80 11 f2 19 c0 a8 02 64 d4 96  <..... .....d.
0020  31 0a 0b 4f 00 35 00 28 f5 df 9e d7 01 00 00 01  1..0.5.( .....
0030  00 00 00 00 00 00 03 77 77 77 06 6c 65 6e 6f 76  .....w ww.lenov
0040  6f 03 63 6f 6d 00 00 01 00 01  o.com... ..
  
```

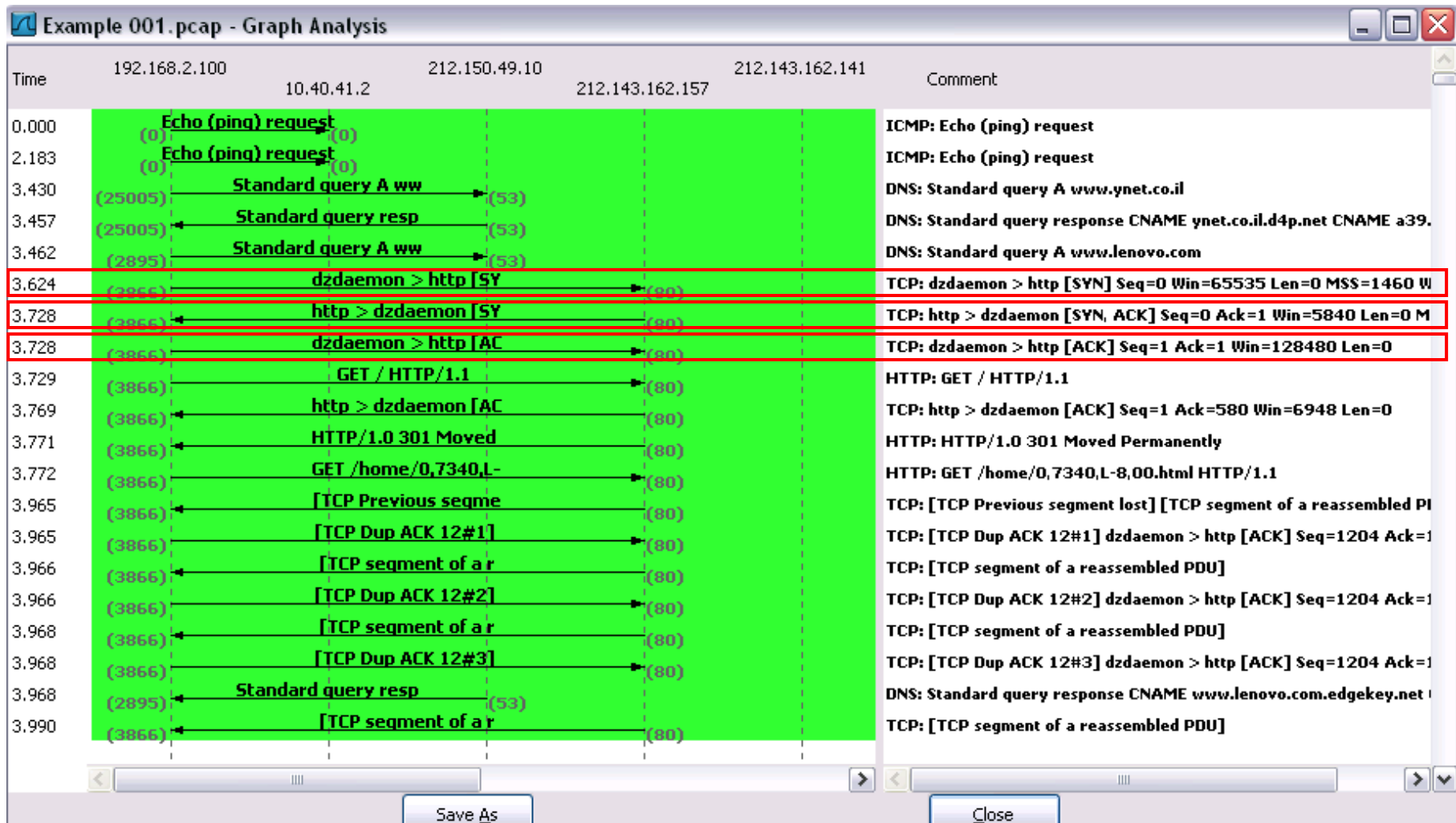
File: "C:\DOCUME~1\yoram\LOCALS~1\Temp\wi... Packets: 1303 Displayed: 1303 Marked: 0 Dropped: 0 Profile: Default

Analyzing Packets (5/9)

- Flow Graph



Analyzing Packets (6/9)



WIRESHARK

Analyzing Packets (7/9)

The image shows the Wireshark network protocol analyzer interface. The main window displays a list of captured packets. A context menu is open over packet 42, with the 'Follow TCP Stream' option highlighted. A red arrow points from this option to the 'Follow TCP Stream' sub-window.

Sniff2 --- HTTP Example.cap - Wireshark

File Edit View Go Capture Analyze Statistics Telephony Tools Help

Filter: Expression... Clear Apply

No.	Time	Source	Destination	Protocol	Info
38	10.031657	10.115.243.30	10.114.30.180	DNS	Standard query response CNAME toolbarqueries.l.google.
39	10.032397	10.114.30.180	64.233.183.99	TCP	peport > http [SYN] Seq=0 Win=65535 Len=0 MSS=1460 WS=
40	10.035182	64.233.183.99	10.114.30.180	TCP	http > peport [SYN, ACK] Seq=0 Ack=1 Win=32768 Len=0 M
41	10.035234	10.114.30.180	64.233.183.99	TCP	peport > http [ACK] Seq=1 Ack=1 Win=131400 Len=0 TSV=1
42	10.035443	10.114.30.180	64.233.183.99	HTTP	nt-auto&ch=6174981939&freshn
43	10.145399	64.233.183.99	10.114.30.180	TCP	Ack=447 Win=32768 Len=0 TSV=
44	10.312738	64.233.183.99	10.114.30.180	TCP	led PDU]
45	10.312814	64.233.183.99	10.114.30.180	HTTP	1)
46	10.312862	10.114.30.180	64.233.183.99	TCP	7 Ack=322 Win=131076 Len=0 T
47	10.399875	10.114.30.180	10.115.243.30	DNS	tcp.dc._msdcs.ndi.local
48	10.400571	10.115.243.30	10.114.30.180	DNS	o such name

Frame 42 (512 bytes on wire, 512 bytes captured)
Ethernet II, Src: Ibm_42:c2:4d (00:09:6b:42:c2:4d), Dst: LucentTe_cf:cd:2c (00:30:6d:cf:cd:2c)
Internet Protocol, Src: 10.114.30.180 (10.114.30.180), Dst: 64.233.183.99 (64.233.183.99)
Transmission Control Protocol, Src Port: peport (1449), Dst Port: http (80), Seq: 1, Ack: 1, L
Hypertext Transfer Protocol

0000 00 30 6d cf cd 2c 00 09 6b 42 c2 4d 08 00 45 00 .Om.... kB.M..E.
0010 01 f2 1a 79 40 00 80 06 bd 1a 0a 72 1e b4 40 e9 ...y@... ..r..@.
0020 b7 63 05 a9 00 50 f2 b3 c2 a3 34 52 27 7f 80 18 ..c...P...4R'...
0030 80 52 3a 66 00 00 01 01 08 0a 00 01 c7 f3 90 77 .R:f.... ..w
0040 be 82 47 45 54 20 2f 73 65 61 72 63 68 3f 63 6c ..GET /s earch?cl
0050 69 65 6e 74 3d 6e 61 76 63 6c 69 65 6e 74 2d 61 ient=nav client-a

File: "D:\Customers\Examples\Sniff2 --- HTTP Exa... Packets: 1648 Displayed: 1648 Marked: 0

Follow TCP Stream

Stream Content

```
GET /search?client=navclient-auto&ch=6174981939&freshness_check=4ilp-
GrPqKEx_r_lNxaYw&iqrn=q4&orig=0J&ie=UTF-8&oe=UTF-8&features=Rank&q=info:http%3A%2F%2Fwww%2Eynet%2Eeco%2Eil%2F
HTTP/1.1
User-Agent: Mozilla/4.0 (compatible; GoogleToolbar 2.0.114.9-big; Windows XP 5.1)
Host: toolbarqueries.google.com
Cache-Control: no-cache
Cookie: PREF=ID=1a18560743a17669;TB=2;CR=1;TM=1113765996;LM=1119978279;GM=1;S=7NmjkcGkIc845ngM; rememberme=false

HTTP/1.1 200 OK
Transfer-Encoding: chunked
Date: Mon, 11 Jul 2005 08:21:03 GMT
Content-Type: text/html
Cache-Control: private
Server: GWS/2.1
Via: 1.1 cache1 (NetCache NetApp/5.5R2D5), Version 2.0-Build_Linux_1336 $Date: 04/13/2005 15:53:0038$(IWSS), 1.1
cache1 (NetCache NetApp/5.5R2D5)

e
```

Find Save As Print Entire conversation (767 bytes) ASCII EBCDIC Hex Dump C Arrays Raw

Filter Out This Stream Close

WIRESHARK

Analyzing Packets (8/9)

Snif2 --- HTTP Example.cap - Wireshark

File Edit View Go Capture Analyze Statistics Telephony Tools Help

Filter: **(tcp.stream eq 5)** Expression... Clear Apply

No.	Time	Source	Destination	Protocol	Info
39	10.032397	10.114.30.180	64.233.183.99	TCP	peport > http [SYN] Seq=0 Win=65535 Len=0 MSS=1460 WS=
40	10.035182	64.233.183.99	10.114.30.180	TCP	http > peport [SYN, ACK] Seq=0 Ack=1 Win=32768 Len=0 M
41	10.035234	10.114.30.180	64.233.183.99	TCP	peport > http [ACK] Seq=1 Ack=1 Win=131400 Len=0 TSV=1
42	10.035443	10.114.30.180	64.233.183.99	HTTP	GET /search?client=navclient-auto&ch=6174981939&freshn
43	10.145399	64.233.183.99	10.114.30.180	TCP	http > peport [ACK] Seq=1 Ack=447 Win=32768 Len=0 TSV=
44	10.312738	64.233.183.99	10.114.30.180	TCP	[TCP segment of a reassembled PDU]
45	10.312814	64.233.183.99	10.114.30.180	HTTP	HTTP/1.1 200 OK (text/html)
46	10.312862	10.114.30.180	64.233.183.99	TCP	peport > http [ACK] Seq=447 Ack=322 Win=131076 Len=0 T
169	20.311539	64.233.183.99	10.114.30.180	TCP	http > peport [FIN, ACK] Seq=322 Ack=447 Win=32768 Len
170	20.311629	10.114.30.180	64.233.183.99	TCP	peport > http [ACK] Seq=447 Ack=323 Win=131076 Len=0 T
192	21.479689	10.114.30.180	64.233.183.99	TCP	peport > http [FIN, ACK] Seq=447 Ack=323 Win=131076 Le
194	21.480926	64.233.183.99	10.114.30.180	TCP	http > peport [ACK] Seq=323 Ack=448 Win=32768 Len=0 TS

+ Frame 39 (78 bytes on wire, 78 bytes captured)

+ Ethernet II, Src: IbmL42:c2:4d (00:09:6b:42:c2:4d), Dst: LucentTe_cf:cd:2c (00:30:6d:cf:cd:2c)

+ Internet Protocol, Src: 10.114.30.180 (10.114.30.180), Dst: 64.233.183.99 (64.233.183.99)

+ Transmission Control Protocol, Src Port: peport (1449), Dst Port: http (80), Seq: 0, Len: 0

0010 00 40 1a 77 40 00 80 06 be ce 0a 72 1e b4 40 e9 .@.w@... ..r..@.

0020 b7 63 05 a9 00 50 f2 b3 c2 a2 00 00 00 00 b0 02 .C...P.....

0030 ff ff 59 3d 00 00 02 04 05 b4 01 03 03 02 01 01 ..Y=.....

0040 08 0a 00 00 00 00 00 00 00 00 01 01 04 02

File: "D:\Customers\Examples\Snif2 --- HTTP Ex... Packets: 1648 Displayed: 12 Marked: 0 Profile: Default

WIRESHARK

Analyzing Packets (9/9)

The image displays the Wireshark network protocol analyzer interface. The main window shows a packet list on the left, a packet details pane in the middle, and a packet bytes pane at the bottom. The packet list shows a series of RTP packets. The packet details pane shows the selected packet's structure, including Ethernet II, Internet Protocol, User Datagram Protocol, and Real-time Transport Protocol. The RTP Stream Analysis window is open, showing a table of RTP packets with columns for Packet, Sequence, Delta(ms), Filtered Jitter(ms), Skew(ms), IP BW(kbps), Marker, and Status. The IP BW(kbps) column is highlighted, and a red arrow points to it from a green box labeled "Stable stream BW".

Stable stream BW

Wireshark: RTP Stream Analysis

Forward Direction | Reversed Direction

Analysing stream from 192.168.2.100 port 5004 to 78.136.29.109 port 6062 SSRC = 0x39FF6709

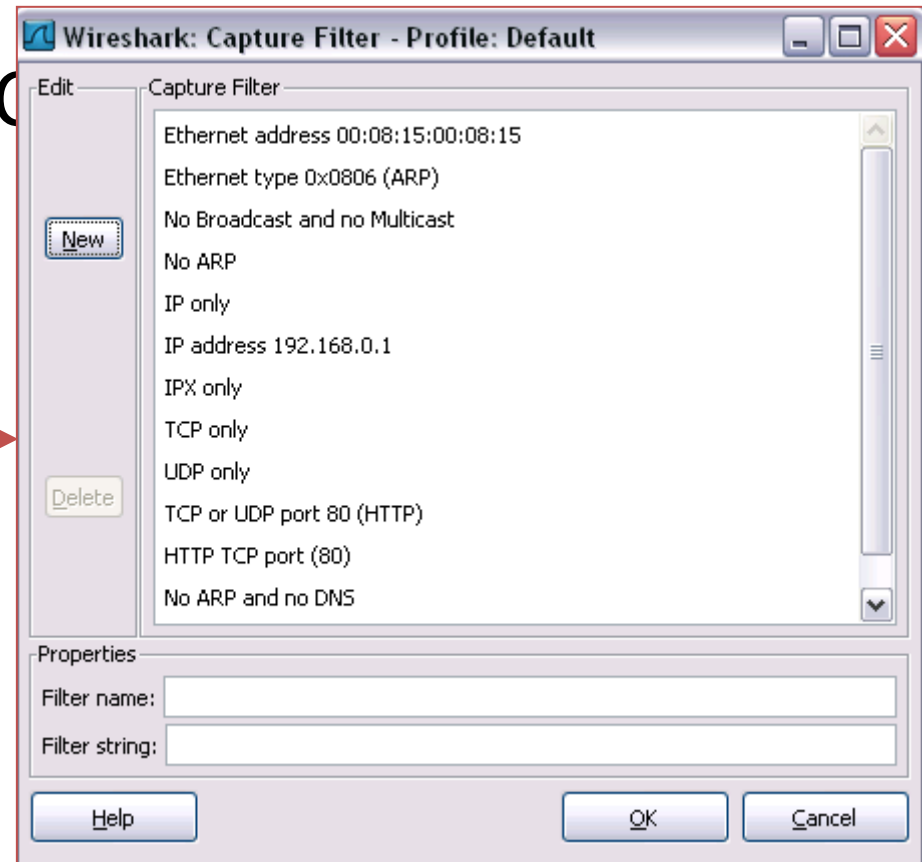
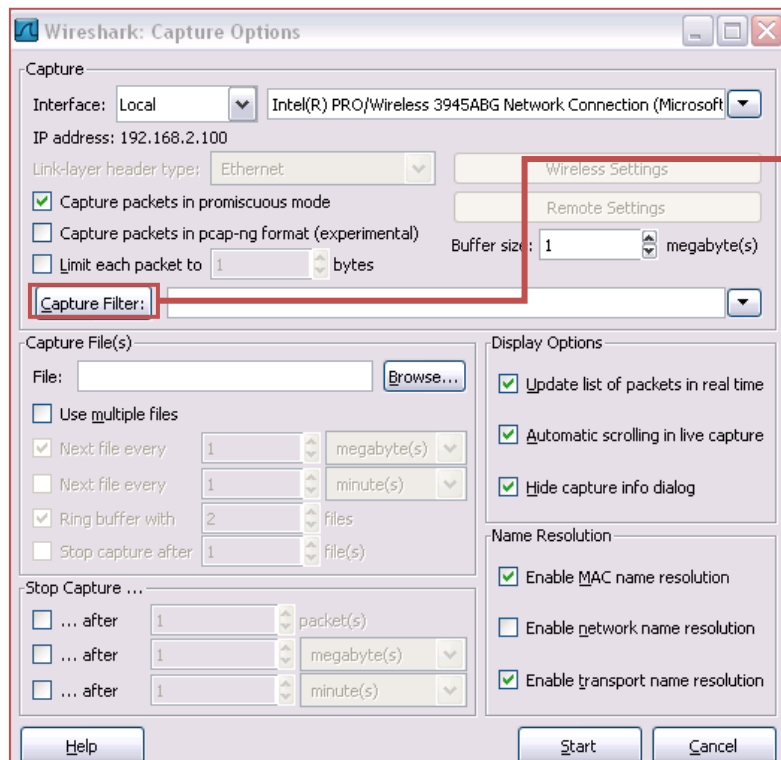
Packet	Sequence	Delta(ms)	Filtered Jitter(ms)	Skew(ms)	IP BW(kbps)	Marker	Status
1417	19063	0.00	0.00	0.00	24.48		[Ok]
1419	19064	0.00	0.00	0.00	24.48		[Ok]
1421	19065	0.00	0.00	0.00	24.48		[Ok]
1423	19066	0.00	0.00	0.00	24.48		[Ok]
1425	19067	0.00	0.00	0.00	24.48		[Ok]
1427	19068	0.00	0.00	0.00	24.48		[Ok]
1429	19069	0.00	0.00	0.00	24.48		[Ok]
1431	19070	0.00	0.00	0.00	24.48		[Ok]

Max delta = 0.00 ms at packet no. 0
Max jitter = 0.00 ms. Mean jitter = 0.00 ms.
Max skew = 0.00 ms.
Total RTP packets = 2098 (expected 2098) Lost RTP packets = 0 (0.00%) Sequence errors = 0
Duration 62.85 s (0 ms clock drift, corresponding to 1 Hz (+0.00%))

Save payload... Save as CSV... Refresh Jump to Graph Next non-Ok Close

Filtering Packets (1/4)

- Applying Filter when C
- Capture → Interfaces → Options:



WIRESHARK

Filtering Packets (2/4)

Example 003.pcap - Wireshark

File Edit View Go Capture Analyze Statistics Telephony Tools Help

Filter: Expression... Clear Apply

No.	Time	Source	Destination	Protocol	Info
485	47.639995	192.168.2.100	212.143.162.152	TCP	17231 → http [FIN, ACK] Seq=1409 Ack=380 Win=12810
486	47.649881	192.168.2.100	212.143.162.152	TCP	17241 → http [SYN] Seq=0 Win=65535 Len=0 MSS=1460
487	47.666485	212.143.162.152	192.168.2.100	TCP	http → 17237 [SYN, ACK] Seq=0 Ack=1 Win=5840 Len=0
488	47.666530	192.168.2.100	192.168.2.100		
489	47.666898	192.168.2.100	192.168.2.100		
490	47.667431	192.168.2.100	192.168.2.100		
491	47.675090	212.143.162.152	192.168.2.100		
492	47.675136	192.168.2.100	212.143.162.152		
493	47.677582	212.143.162.152	192.168.2.100		
494	47.677624	192.168.2.100	212.143.162.152		
495	47.677858	192.168.2.100	212.143.162.152		
496	47.695323	212.143.162.152	192.168.2.100		
497	47.697056	212.143.162.152	192.168.2.100		
498	47.737850	212.143.162.152	192.168.2.100		
499	47.739896	212.143.162.152	192.168.2.100		
500	47.788636	212.143.162.152	192.168.2.100		
501	47.797761	192.168.2.100	212.143.162.152		
502	47.826481	212.143.162.152	192.168.2.100		
503	47.826527	192.168.2.100	212.143.162.152		
504	47.826913	192.168.2.100	212.143.162.152		
505	47.839189	212.143.162.152	192.168.2.100		
506	47.841074	212.143.162.152	192.168.2.100		
507	47.856460	212.143.162.152	192.168.2.100		
508	47.858425	212.143.162.152	192.168.2.100		

Wireshark: Filter Expression - Profile: Default

Field name

- Mesh - Mesh Header
- message/http - Media Type: message/http
- Messenger - Microsoft Messenger Service
- MGCP - Media Gateway Control Protocol
- MGMT - DCE/RPC Remote Management
- MIKEY - Multimedia Internet KEYing
- MIME multipart - MIME Multipart Media Encapsulation
- MIOP - Unreliable Multicast Inter-ORB Protocol
- MIPv6 - Mobile IPv6 / Network Mobility
- MMS - MMS
- MMSE - MMS Message Encapsulation
- Mobile IP - Mobile IP
- Modbus/TCP - Modbus/TCP

Relation

- is present
- ==
- !=
- >
- <
- >=
- <=
- contains
- matches

Value (character string)

Predefined values:

Range (offset:length)

Frame 485 (54 bytes on wire, 54 bytes captured)

Ethernet II, Src: IntelCor_a2:d8:9a (00:1c:bf:a2:d8:9a), Dst: 08:00:27:2d:7d:00 (08:00:27:2d:7d:00)

Internet Protocol, Src: 192.168.2.100 (192.168.2.100), Dst: 212.143.162.152 (212.143.162.152)

Transmission Control Protocol, Src Port: 17231 (17231), Dst Port: 17237 (17237)

0000 00 0e 2e 6e 2f 7d 00 1c bf a2 d8 9a 08 00 45 00

0010 00 28 94 52 40 00 80 06 2c 49 c0 a8 02 64 d4 80

0020 a2 98 43 4f 00 50 b6 d6 a4 44 e9 7c 0f 5f 50 10

0030 fa 32 e3 d5 00 00

Filtering Packets (3/4)

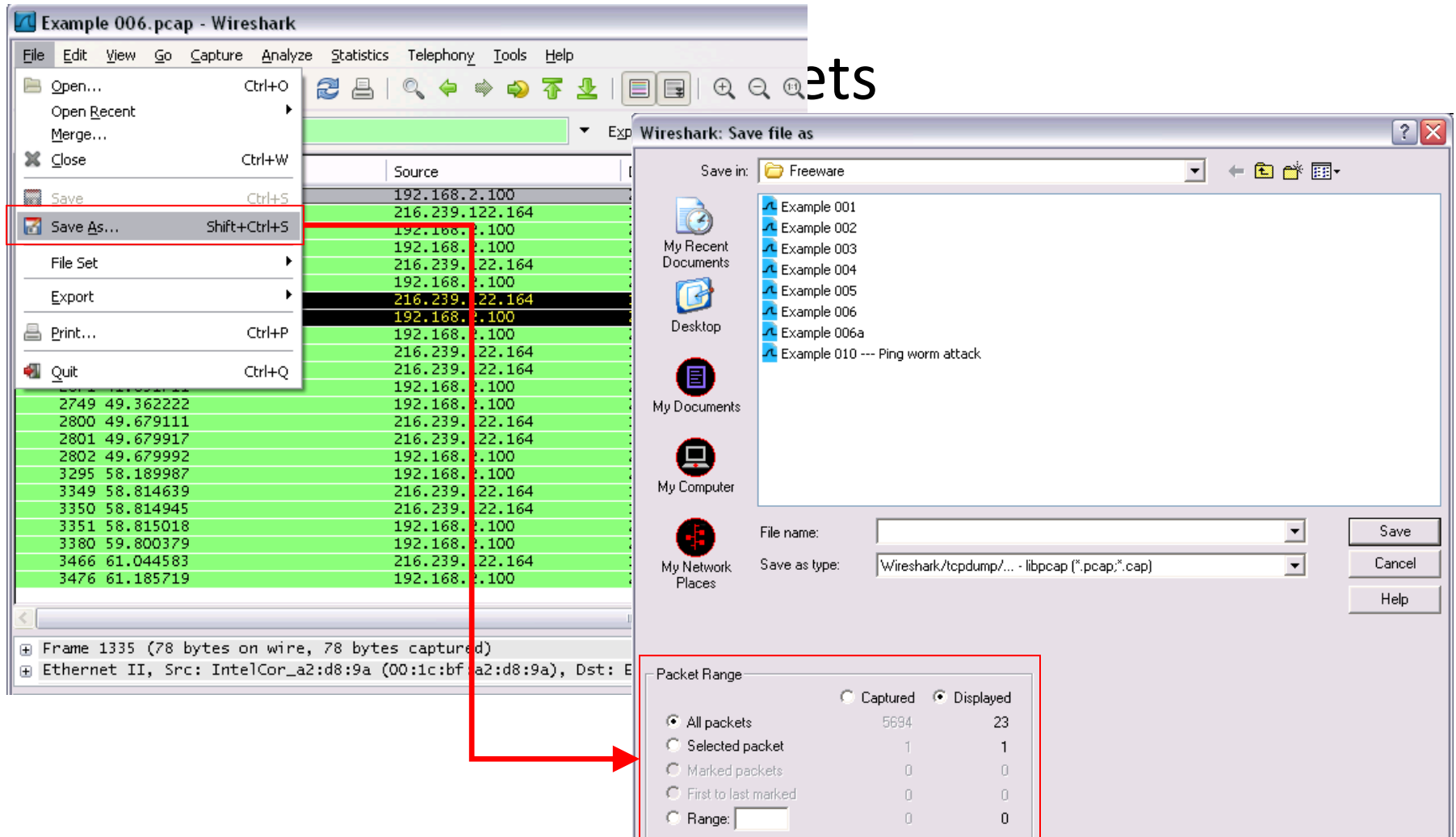
- Examples:
 - Capture only traffic to or from IP address 172.18.5.4
 - **host 172.18.5.4**
 - Capture traffic to or from a range of IP addresses
 - **net 192.168.0.0/24**
 - **net 192.168.0.0 mask 255.255.255.0**
 - Capture traffic from a range of IP addresses
 - **src net 192.168.0.0/24**
 - **src net 192.168.0.0 mask 255.255.255.0**
 - Capture traffic to a range of IP addresses
 - **dst net 192.168.0.0/24**
 - **dst net 192.168.0.0 mask 255.255.255.0**
 - Capture only DNS (port 53) traffic
 - **port 53**
 - Capture non-HTTP and non-SMTP traffic on your server
 - **host www.example.com and not (port 80 or port 25)**
 - **host www.example.com and not port 80 and not port 25**

Filtering Packets (4/4)

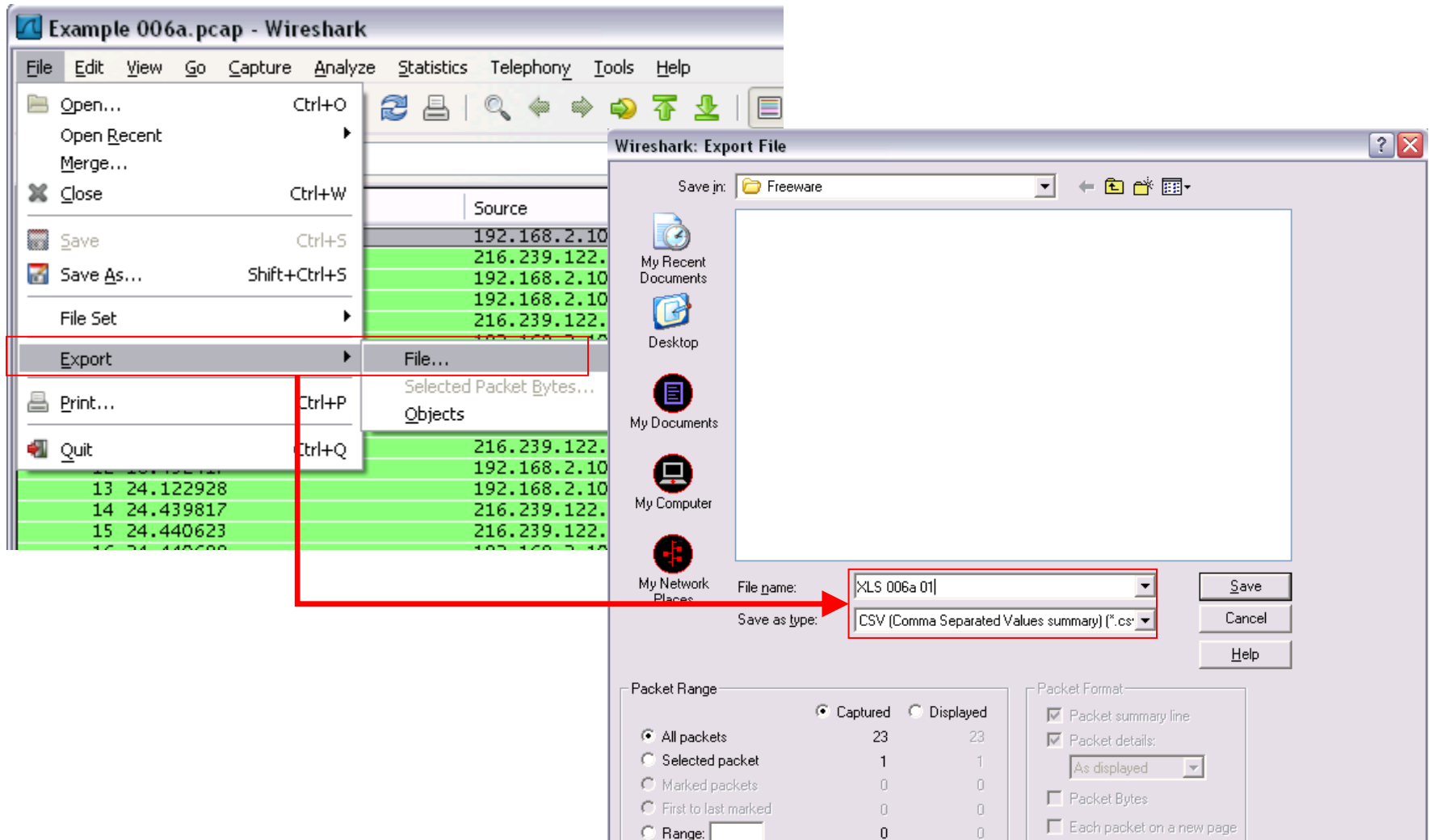
- Examples:
 - Capture except all ARP and DNS traffic
 - **port not 53 and not arp**
 - Capture traffic within a range of ports
 - **(tcp[2:2] > 1500 and tcp[2:2] < 1550) or (tcp[4:2] > 1500 and tcp[4:2] < 1550)**
 - **tcp portrange 1501-1549**
 - Capture only Ethernet type EAPOL
 - **ether proto 0x888e**
 - Capture only IP traffic
(the shortest filter, but sometimes very useful to get rid of lower layer protocols like ARP and STP)
 - **ip**
 - Capture only unicast traffic
(useful to get rid of noise on the network if you only want to see traffic to and from your machine, not, for example, broadcast and multicast announcements)
 - **not broadcast and not multicast**

WIRESHARK

Saving and Manipulating Packets (1/3)



Saving and Manipulating Packets (2/3)

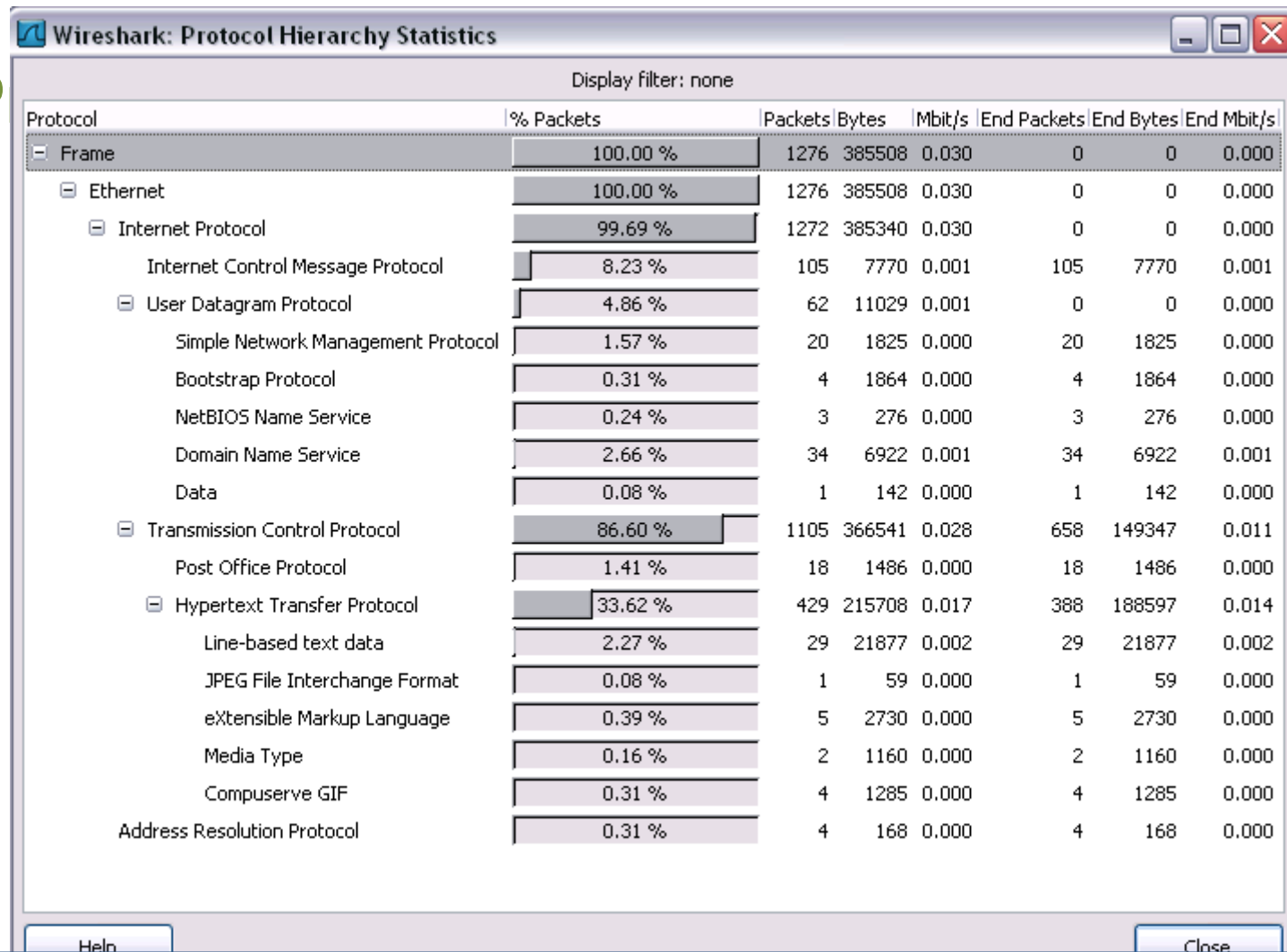


Saving and Manipulating Packets (3/3)

No.	Time	Time Variation	Source	Destination	Protocol	Info
1	0	0	192.168.2.100	216.239.122.164	TCP	27837 > http [SYN] Seq=0 Win=65535 Len=0 MSS=1460 WS=1 TSV=0 TSER=0
2	0.226724	0.226724	216.239.122.164	192.168.2.100	TCP	http > 27837 [SYN, ACK] Seq=0 Ack=1 Win=8190 Len=0 MSS=1380
3	0.226772	4.8E-05	192.168.2.100	216.239.122.164	TCP	27837 > http [ACK] Seq=1 Ack=1 Win=65535 Len=0
4	0.227146	0.227098	192.168.2.100	216.239.122.164	HTTP	GET /i/b.jpg HTTP/1.1
5	0.700674	0.473576	216.239.122.164	192.168.2.100	HTTP	HTTP/1.1 200 OK (JPEG JFIF image)
6	0.883533	0.409957	192.168.2.100	216.239.122.164	TCP	27837 > http [ACK] Seq=649 Ack=767 Win=64769 Len=0
7	1.161312	0.751355	216.239.122.164	192.168.2.100	HTTP	[TCP Retransmission] HTTP/1.1 200 OK (JPEG JFIF image)
8	1.161361	0.410006	192.168.2.100	216.239.122.164	TCP	[TCP Dup ACK 6#1] 27837 > http [ACK] Seq=649 Ack=767 Win=64769 Len=0
9	16.211468	15.801462	192.168.2.100	216.239.122.164	HTTP	GET /i/b.jpg HTTP/1.1
10	16.452024	0.650562	216.239.122.164	192.168.2.100	TCP	[TCP segment of a reassembled PDU]
11	16.452343	15.801781	216.239.122.164	192.168.2.100	HTTP	HTTP/1.1 200 OK (JPEG JFIF image)
12	16.452417	0.650636	192.168.2.100	216.239.122.164	TCP	27837 > http [ACK] Seq=1539 Ack=1533 Win=65535 Len=0
13	24.122928	23.472292	192.168.2.100	216.239.122.164	HTTP	GET /i/b.jpg HTTP/1.1
14	24.439817	0.967525	216.239.122.164	192.168.2.100	TCP	[TCP segment of a reassembled PDU]
15	24.440623	23.473098	216.239.122.164	192.168.2.100	HTTP	HTTP/1.1 200 OK (JPEG JFIF image)
16	24.440698	0.9676	192.168.2.100	216.239.122.164	TCP	27837 > http [ACK] Seq=2384 Ack=2299 Win=64769 Len=0
17	32.950693	31.983093	192.168.2.100	216.239.122.164	HTTP	GET /i/b.jpg HTTP/1.1
18	33.575345	1.592252	216.239.122.164	192.168.2.100	TCP	[TCP segment of a reassembled PDU]
19	33.575651	31.983399	216.239.122.164	192.168.2.100	HTTP	HTTP/1.1 200 OK (JPEG JFIF image)
20	33.575724	1.592325	192.168.2.100	216.239.122.164	TCP	27837 > http [ACK] Seq=3269 Ack=3065 Win=65535 Len=0
21	34.561085	32.96876	192.168.2.100	216.239.122.164	HTTP	GET /b.gif HTTP/1.1
22	35.805289	2.836529	216.239.122.164	192.168.2.100	HTTP	HTTP/1.1 200 OK (GIF89a)
23	35.946425	33.109896	192.168.2.100	216.239.122.164	TCP	27837 > http [ACK] Seq=4080 Ack=3567 Win=65033 Len=0

Packet Statistics (1/8)

• P



WIRESHARK

Packet Statistics (2/8)

Conversations: (Untitled)

Ethernet: 4 Fibre Channel FDMA **IPv4: 38** IXX JXTA NCP RSVP SCTP **TCP: 79** Token Ring **UDP: 23** USB WLAN

IPv4 Conversations

Address A	Address B	Packets	Bytes	Packets A->B	Bytes A->B	Packets A<-B	Bytes A<-B	Rel Start	Duration
192.168.2.100	255.255.255.255	1	142	1	142	0	0	96.384838000	0.0000
192.168.2.101	255.255.255.255	2	684	2	684	0	0	47.852757000	3.0721
192.168.2.1	255.255.255.255	2	1180	2	1180	0	0	47.857905000	3.0722
192.168.2.100	212.143.162.144	10	2194	6	815	4	1379	87.473054000	65.0878
192.168.2.100	212.179.31.90	10	1342	6	971	4	371	91.655266000	60.9113
62.90.102.31	192.168.2.100	10	1373	4	441	6	932	91.660203000	60.9174
192.168.2.100	212.150.22.226	10	1327	6	956	4	371	91.732692000	60.8200
192.168.2.100	212.150.236.220	10	1470	6	981	4	489	91.742363000	60.8122
192.168.2.100	212.179.58.84	10	1725	6	954	4	771	92.287214000	2.4984
82.80.238.109	192.168.2.100	11	1282	5	440	6	842	91.646648000	60.9214
10.12.44.2	192.168.2.100	12	888	6	444	6	444	31.421091000	164.384
10.10.10.2	192.168.2.100	12	888	6	444	6	444	31.531676000	164.804
10.12.20.2	192.168.2.100	12	888	6	444	6	444	5.250457000	164.523
10.31.68.1	192.168.2.100	12	888	6	444	6	444	5.578447000	164.631
10.100.102.2	192.168.2.100	12	888	6	444	6	444	17.858674000	164.363

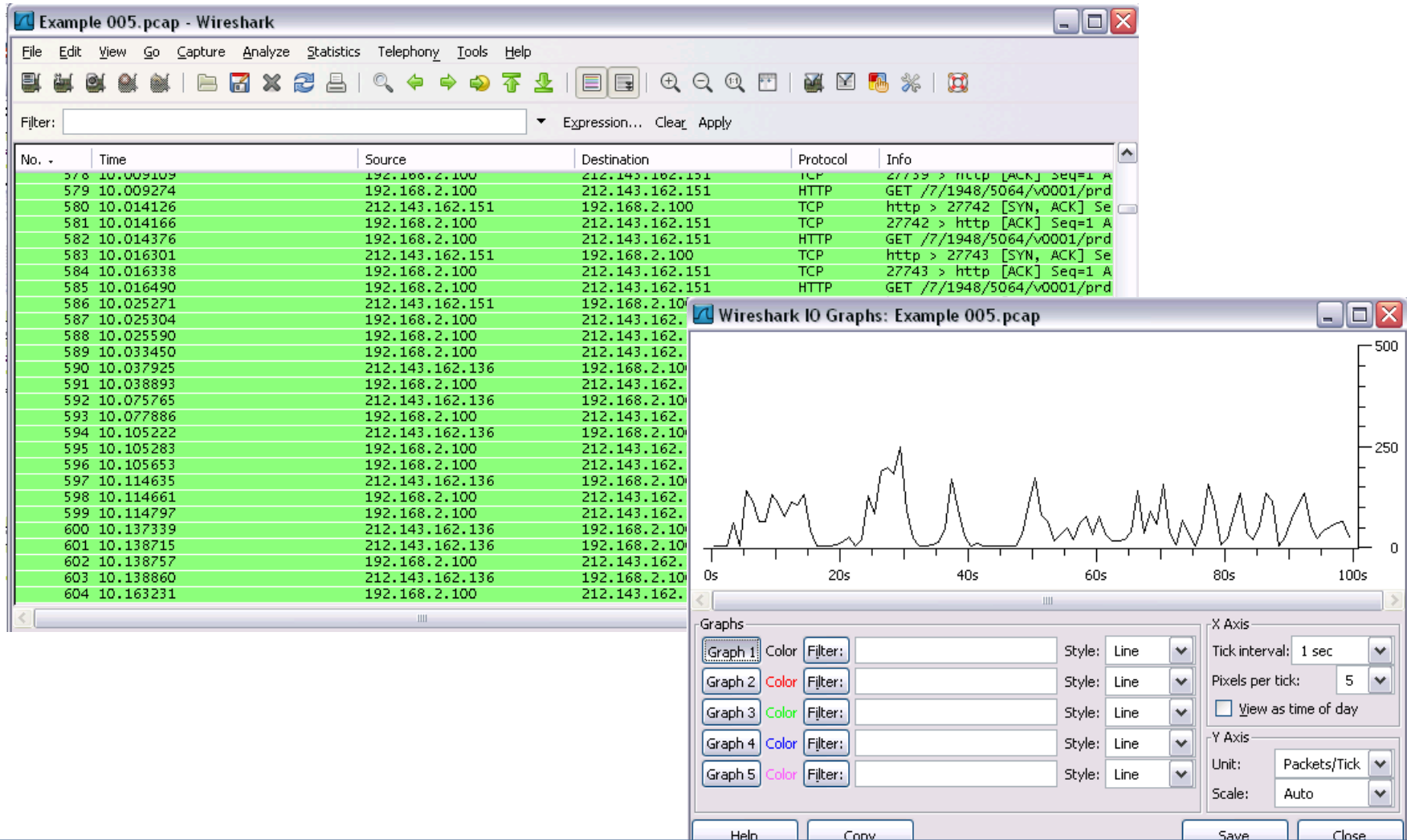
☒ Name resolution ☐ Limit to display filter

Help **Copy** **With some manipulation** Close

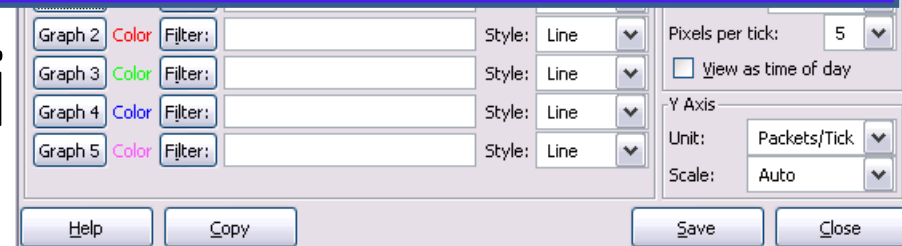
	A	B	C	D	E	F	G	H	I	J	K	L
1	Address A	Address B	Packets	Bytes	Packets A->B	Bytes A->B	Packets A<-B	Bytes A<-B	Rel Start	Duration	bps A->B	bps A<-B
2	10.10.10.1	10.159.3.103	2	124	0	0	2	124	0	42.0039	N/A	23.62
3	1.1.1.1	10.159.3.103	2	120	0	0	2	120	24.49414	1.1885	N/A	807.76

WIRESHARK

Packet Statistics (3/8)



Packet Stati



- Configurable Options
 - I/O Graphs
 - **Graph 1-5**: enable the specific graph 1-5 (graph 1 by default)
 - **Filter**: a display filter for this graph (only the packets that pass this filter will be taken into account for this graph)
 - **Style**: the style of the graph (Line/Impulse/FBar/Dot)
 - X Axis
 - **Tick interval**: an interval in x direction lasts (10/1 minutes or 10/1/0.1/0.01/0.001 seconds)
 - **Pixels per tick**: use 10/5/2/1 pixels per tick interval
 - **View as time of day**: option to view x direction labels as time of day instead of seconds or minutes since beginning of capture
 - Y Axis
 - **Unit**: the unit for the y direction (Packets/Tick, Bytes/Tick, Bits/Tick, Advanced...)
 - **Scale**: the scale for the y unit (Logarithmic, Auto, 10, 20, 50, 100, 200, ...)

Packet Statistics (5/8)

Sniff1 --- File copy from other side.cap - Wireshark

File Edit View Go Capture Analyze **Statistics** Telephony Tools Help

Filter: (tcp.stream eq 0)

Summary
Protocol Hierarchy
Conversations
Endpoints
Packet Lengths...
IO Graphs
Conversation List
Endpoint List
Service Response Time
BOOTP-DHCP...
Compare...
Flow Graph...
HTTP
IP Addresses...
IP Destinations...
IP Protocol Types...
ONC-RPC Programs
TCP Stream Graph
UDP Multicast Streams
WLAN Traffic...

Round Trip Time Graph
Throughput Graph
Time-Sequence Graph (Stevens)
Time-Sequence Graph (tcptrace)

No.	Time	Destination	Protocol	Info
762	0.132867	192.168.1.102	TCP	[TCP segment of a reassembled PDU]
763	0.132992	192.168.1.102	TCP	[TCP segment of a reassembled PDU]
764	0.133116	192.168.1.102	TCP	[TCP segment of a reassembled PDU]
766	0.133247	192.168.1.102	TCP	[TCP segment of a reassembled PDU]
767	0.133258	192.168.1.102	SMB	Read AndX Response, 61440 bytes
768	0.133265	192.168.104.77	TCP	paradym-31port > microsoft-ds [ACK] Seq=883 Ack=686944 Win=
769	0.133272	192.168.104.77	TCP	paradym-31port > microsoft-ds [ACK] Seq=883 Ack=689864 Win=
770	0.133281	192.168.104.77	TCP	paradym-31port > microsoft-ds [ACK] Seq=883 Ack=692784 Win=
771	0.134377	192.168.104.77	TCP	paradym-31port > microsoft-ds [ACK] Seq=883 Ack=695704 Win=
773	0.139299	192.168.104.77	SMB	Read AndX Request, FID: 0x8003, 61440 bytes at offset 1747
774	0.140539	192.168.1.102	TCP	[TCP segment of a reassembled PDU]
775	0.140661	192.168.1.102	TCP	[TCP segment of a reassembled PDU]
776	0.140785	192.168.1.102	TCP	[TCP segment of a reassembled PDU]
777	0.140909	192.168.1.102	TCP	[TCP segment of a reassembled PDU]
778	0.141033	192.168.1.102	TCP	[TCP segment of a reassembled PDU]
779	0.141155	192.168.1.102	TCP	[TCP segment of a reassembled PDU]
780	0.141282	192.168.1.102	TCP	[TCP segment of a reassembled PDU]
781	0.141293	192.168.104.77	TCP	paradym-31port > microsoft-ds [ACK] Seq=946 Ack=698807 Win=
782	0.141411	192.168.104.77	TCP	[TCP segment of a reassembled PDU]
783	0.141421	192.168.104.77	TCP	paradym-31port > microsoft-ds [ACK] Seq=946 Ack=701727 Win=
784	0.141538	192.168.1.102	TCP	[TCP segment of a reassembled PDU]
785	0.141663	192.168.1.102	TCP	[TCP segment of a reassembled PDU]
786	0.141783	192.168.1.102	TCP	[TCP segment of a reassembled PDU]
787	0.141908	192.168.1.102	TCP	[TCP segment of a reassembled PDU]
788	0.142035	192.168.104.77	TCP	[TCP segment of a reassembled PDU]
789	0.142046	192.168.1.102	TCP	paradym-31port > microsoft-ds [ACK] Seq=946 Ack=704647 Win=
790	0.142053	192.168.104.77	TCP	paradym-31port > microsoft-ds [ACK] Seq=946 Ack=707567 Win=
791	0.142059	192.168.1.102	TCP	paradym-31port > microsoft-ds [ACK] Seq=946 Ack=710487 Win=

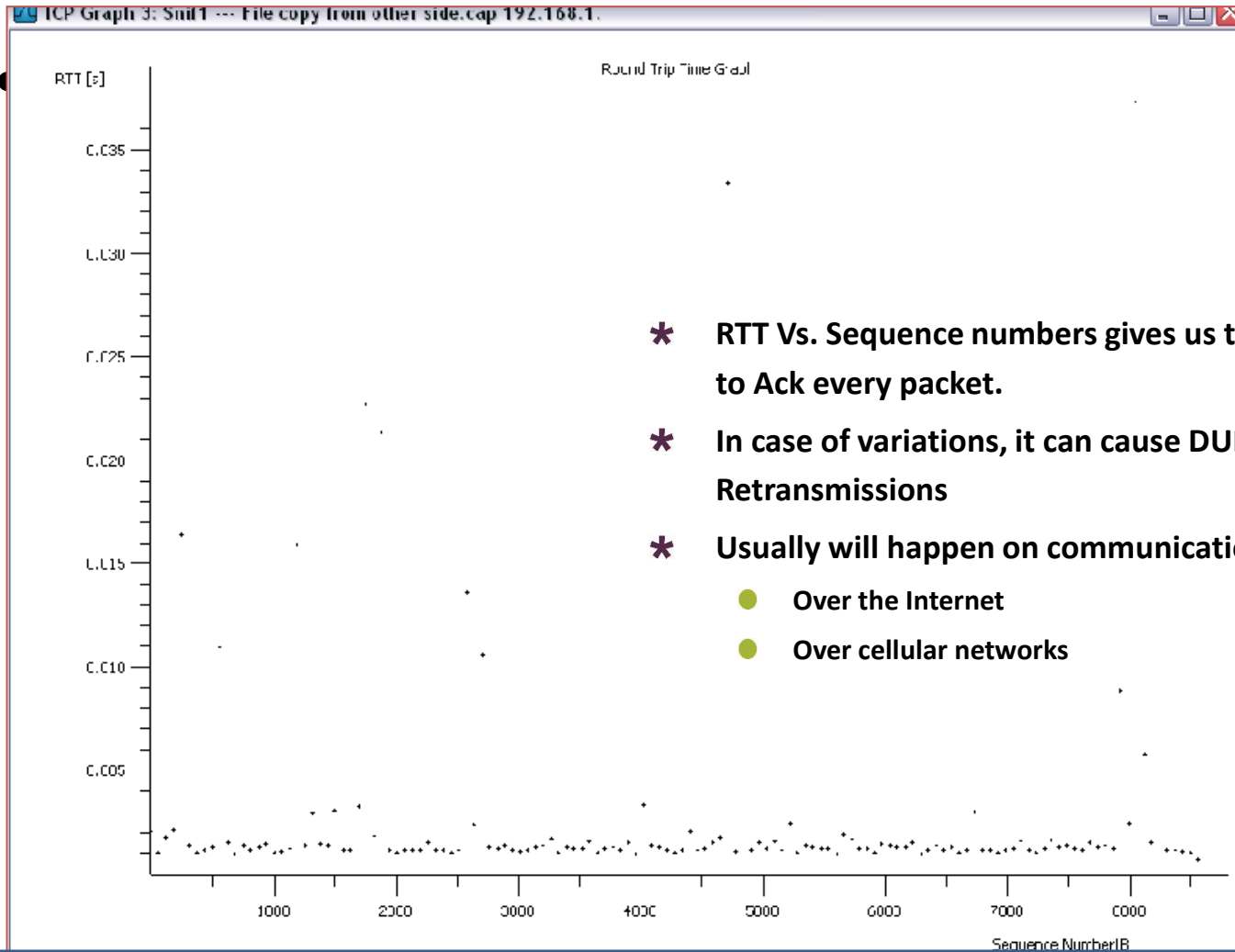
Frame 771 (60 bytes on wire, 60 bytes captured)

Ethernet II, Src: Intel_4c:cc:89 (00:d0:b7:4c:cc:89), Dst: Intel_2e:32:a9 (00:90:27:2e:32:a9)

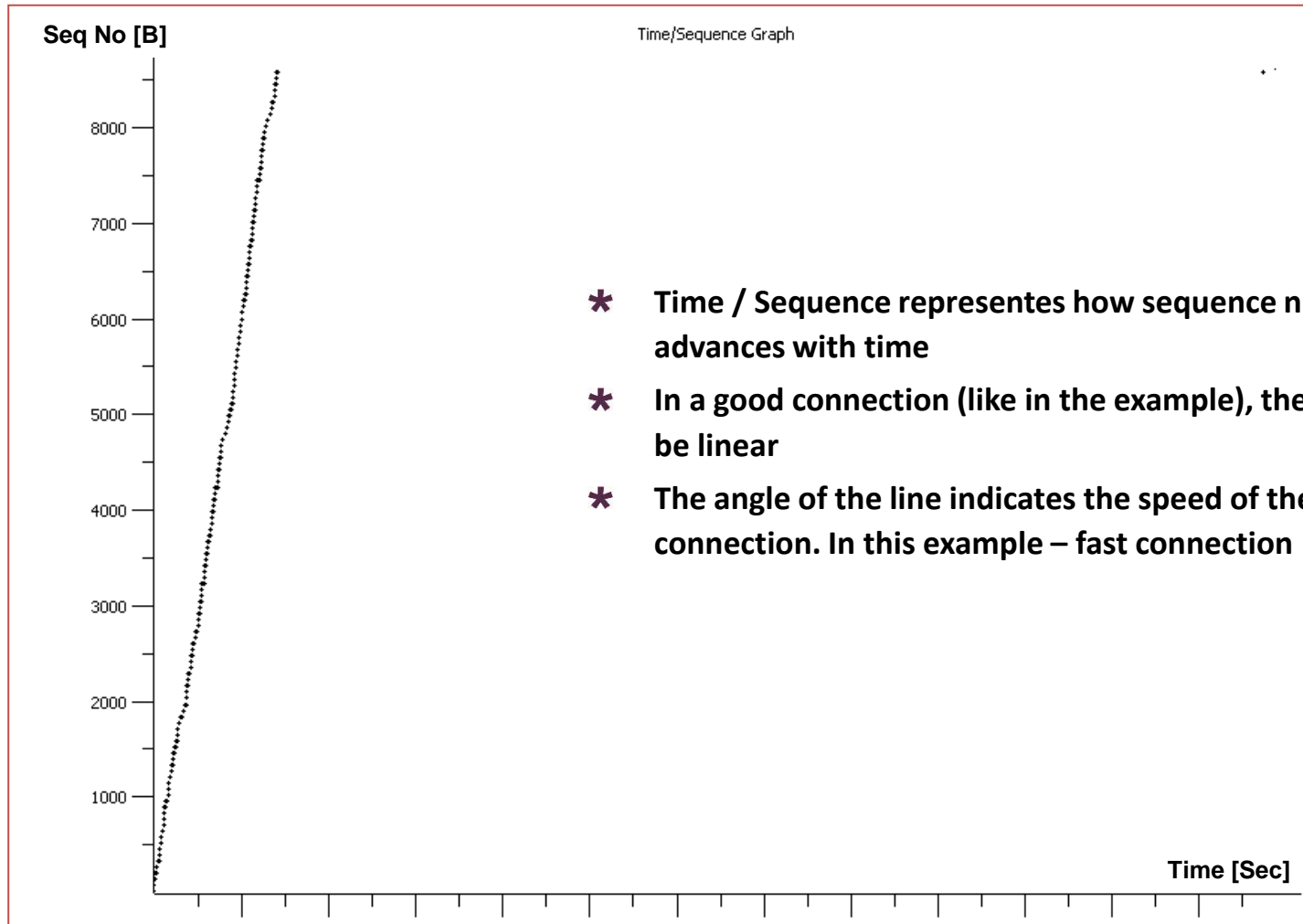
Internet Protocol, Src: 192.168.1.102 (192.168.1.102), Dst: 192.168.104.77 (192.168.104.77)

Transmission Control Protocol, Src Port: paradym-31port (1864), Dst Port: microsoft-ds (445), Seq: 883, Ack: 695704, Len: 0

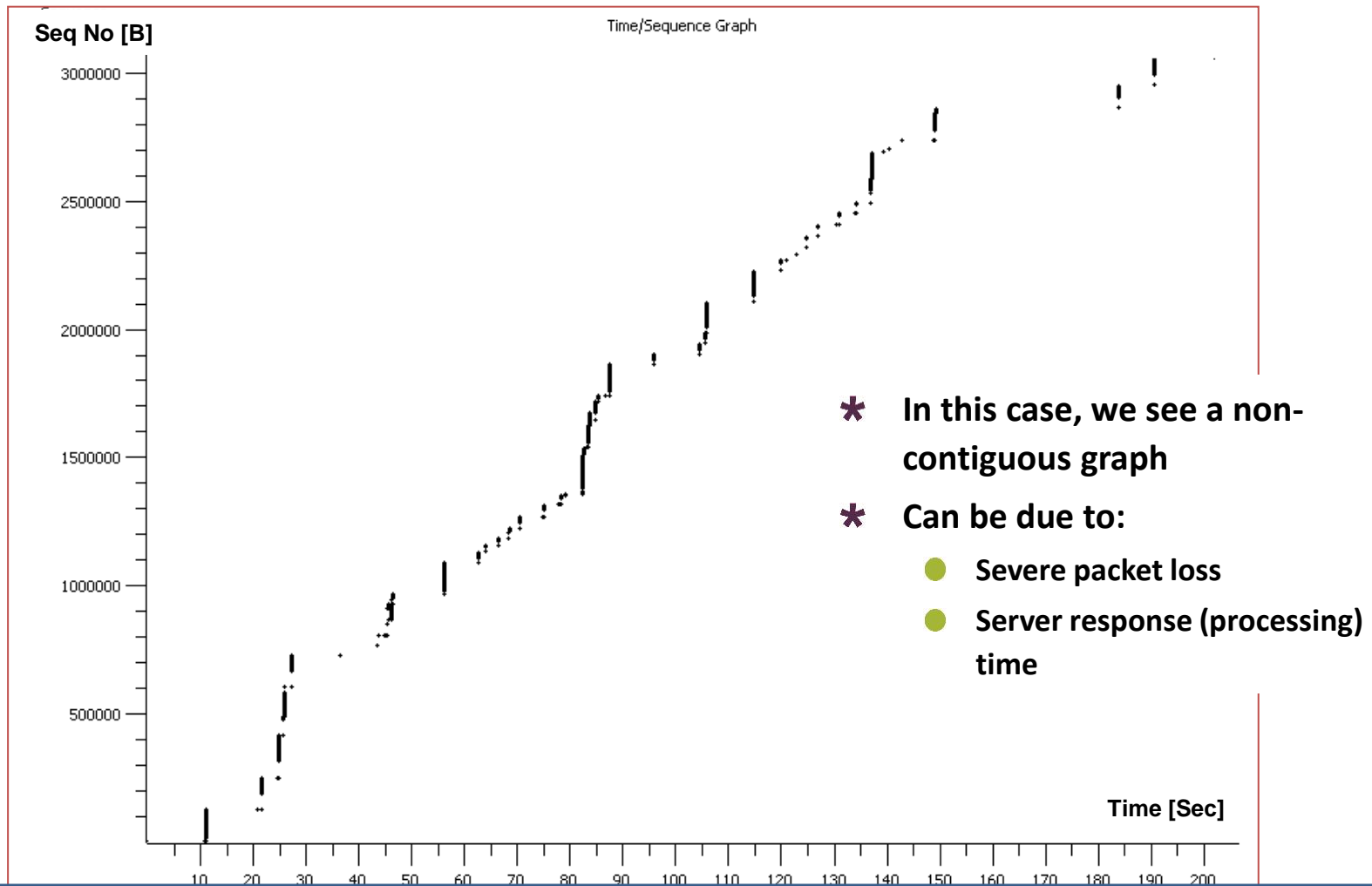
Packet Statistics (6/8)



Packet Statistics (7/8)



Packet Statistics (8/8)



Colorizing Specific Packets (1/4)

- Packet Colorization

- Colorize packets according to a filter
- Allow to emphasize the packets interested in
- A lot of Coloring Rule examples at the [Wireshark Wiki Coloring Rules page at](http://wiki.wireshark.org/ColoringRules)

We want to watch a specific protocol through out the capture file



No. ↓	Time	Source	Destination	Protocol	Info
1	0.000000	172.16.2.255	172.17.220.62	ICMP	Echo (ping) request
2	0.001075	172.16.3.14	172.16.1.224	DCERPC	Request: call_id: 395 opnum: 2 ctx_id: 0
3	0.002838	172.16.1.224	172.16.3.14	DCERPC	Response: call_id: 395 ctx_id: 0
4	0.004758	172.16.1.20	172.16.2.236	HTTP	Continuation or non-HTTP traffic
5	0.005001	172.16.2.236	172.16.1.20	TCP	netview-aix-12 > http-alt [ACK] Seq=1 Ack=1461 win=64240 Len=0
6	0.005134	172.16.1.20	172.16.2.236	HTTP	Continuation or non-HTTP traffic
7	0.005658	172.16.1.20	172.16.2.236	HTTP	Continuation or non-HTTP traffic
8	0.005790	172.16.1.20	172.16.2.236	HTTP	Continuation or non-HTTP traffic
9	0.005906	172.16.2.236	172.16.1.20	TCP	netview-aix-11 > http-alt [ACK] Seq=1 Ack=2049 win=64240 Len=0
10	0.006231	172.16.1.20	172.16.2.236	HTTP	Continuation or non-HTTP traffic
11	0.006253	172.16.1.20	172.16.2.236	HTTP	Continuation or non-HTTP traffic
12	0.006444	172.16.2.236	172.16.1.20	TCP	netview-aix-11 > http-alt [ACK] Seq=1 Ack=4097 win=64240 Len=0
13	0.006826	172.16.1.20	172.16.2.236	HTTP	Continuation or non-HTTP traffic
14	0.006962	172.16.1.20	172.16.2.236	HTTP	Continuation or non-HTTP traffic
15	0.007079	172.16.2.236	172.16.1.20	TCP	netview-aix-11 > http-alt [ACK] Seq=1 Ack=6145 win=64240 Len=0
16	0.007221	172.16.3.129	172.16.201.60	ICMP	Echo (ping) request
17	0.007951	172.16.1.20	172.16.2.236	HTTP	Continuation or non-HTTP traffic
18	0.007972	64.236.34.97	172.16.2.219	TCP	http > metasage [ACK] Seq=1 Ack=1 win=4096 Len=0
19	0.008068	172.16.1.20	172.16.2.236	HTTP	Continuation or non-HTTP traffic
20	0.008263	172.16.1.20	172.16.2.236	HTTP	Continuation or non-HTTP traffic
21	0.008279	172.16.1.40	172.16.2.5	TCP	qv-us > radmin-port [PSH, ACK] Seq=1 Ack=1 win=16306 Len=14

Colorizing Specific Packets (2/4)

The image shows the Wireshark network protocol analyzer interface. The main pane displays a list of captured packets. The 'Filter' field is empty. The 'Expression...' button is visible. The 'Colorize Conversation' menu item is highlighted, and the 'TCP' protocol is selected in the submenu. The 'Color 1' option is selected in the color selection dialog.

No.	Time	Source	Destination	Protocol	Info
1	0.000000	172.16.2.255	172.17.220.62	ICMP	Echo (ping) request
2	0.001075	172.16.3.14	172.16.1.224	DCERPC	Request: call_id: 395 numnum: 2 ctx_id: 0
3	0.002838	172.16.1.224	172.16.3.14	DCERPC	Mark Packet (toggle)
4	0.004758	172.16.1.20	172.16.2.236	HTTP	Set Time Reference (toggle)
5	0.005001	172.16.2.236	172.16.1.20	TCP	traffic
6	0.005134	172.16.1.20	172.16.2.236	HTTP	traffic
7	0.005658	172.16.1.20	172.16.2.236	HTTP	traffic
8	0.005790	172.16.1.20	172.16.2.236	HTTP	traffic
9	0.005906	172.16.2.236	172.16.1.20	TCP	traffic
10	0.006231	172.16.1.20	172.16.2.236	HTTP	traffic
11	0.006253	172.16.1.20	172.16.2.236	HTTP	traffic
12	0.006444	172.16.2.236	172.16.1.20	TCP	traffic
13	0.006826	172.16.1.20	172.16.2.236	HTTP	traffic
14	0.006962	172.16.1.20	172.16.2.236	HTTP	traffic
15	0.007079	172.16.2.236	172.16.1.20	TCP	traffic
16	0.007221	172.16.3.129	172.16.201.60	ICMP	traffic
17	0.007951	172.16.1.20	172.16.2.236	HTTP	traffic
18	0.007972	64.236.34.97	172.16.2.219	TCP	traffic
19	0.008068	172.16.1.20	172.16.2.236	HTTP	traffic
20	0.008263	172.16.1.20	172.16.2.236	HTTP	traffic
21	0.008279	172.16.1.40	172.16.2.5	TCP	traffic

Frame 2 (198 bytes on wire, 198 bytes captured)
Ethernet II, Src: 3com_74:5a:2b (00:50:da:74:5a:2b), Dst: Cisco_07:a2:b0 (00:0c:85:07:a2:b0)
Internet Protocol, Src: 172.16.3.14 (172.16.3.14), Dst: 172.16.1.224 (172.16.1.224)
Transmission Control Protocol, Src Port: writesrv (1334), Dst Port: alta-ana-lm (1346), Seq: 1, Ack: 1, Len: 1
DCE RPC Request, Fragment: Single, FragLen: 144, Call: 395 Ctx: 0

0000 00 0c 85 07 a2 b0 00 50 da 74 5a 2b 08 00 45 00P .tZ+..E.
0010 00 b8 58 74 40 00 80 06 44 bd ac 10 03 0e ac 10 ...Xt@... D.....
0020 01 e0 05 36 05 42 9a 8d a4 a2 49 a0 ce 05 50 18 ...6.B... ..I...P.
0030 fa 90 0f c3 00 00 05 00 00 03 10 00 00 00 90 00
0040 10 00 8b 01 00 00 52 00 00 00 00 00 02 00 00 00R.
0050 00 00 01 61 85 26 dd f2 6b 42 88 28 13 00 00 0d
File: "D:\Customers\Mivtachim\Sniff4 --- Center-... Packets: 11108 Displayed: 11108 Marked: 0 Profile: Default

Colorizing Specific Packets (3/4)

The image shows the Wireshark network protocol analyzer interface. The top menu bar includes File, Edit, View, Go, Capture, Analyze, Statistics, Telephony, Tools, and Help. Below the menu is a toolbar with various icons for file operations, capture, and analysis. A filter bar is present with a text input field and buttons for 'Expression...', 'Clear', and 'Apply'.

The main packet list pane displays 21 captured packets. Each row shows the packet number, time, source and destination IP addresses, protocol, and a brief description. The packets are color-coded: ICMP (blue), DCERPC (red), HTTP (green), and TCP (purple). The selected packet (No. 7) is highlighted in grey.

No.	Time	Source	Destination	Protocol	Info
1	0.000000	172.16.2.255	172.17.220.62	ICMP	Echo (ping) request
2	0.001075	172.16.3.14	172.16.1.224	DCERPC	Request: call_id: 395 opnum: 2 ctx_id: 0
3	0.002838	172.16.1.224	172.16.3.14	DCERPC	Response: call_id: 395 ctx_id: 0
4	0.004758	172.16.1.20	172.16.2.236	HTTP	Continuation or non-HTTP traffic
5	0.005001	172.16.2.236	172.16.1.20	TCP	netview-aix-12 > http-alt [ACK] Seq=1 Ack=1461 win=64240 Len=0
6	0.005134	172.16.1.20	172.16.2.236	HTTP	Continuation or non-HTTP traffic
7	0.005658	172.16.1.20	172.16.2.236	HTTP	Continuation or non-HTTP traffic
8	0.005790	172.16.1.20	172.16.2.236	HTTP	Continuation or non-HTTP traffic
9	0.005906	172.16.2.236	172.16.1.20	TCP	netview-aix-11 > http-alt [ACK] Seq=1 Ack=2049 win=64240 Len=0
10	0.006231	172.16.1.20	172.16.2.236	HTTP	Continuation or non-HTTP traffic
11	0.006253	172.16.1.20	172.16.2.236	HTTP	Continuation or non-HTTP traffic
12	0.006444	172.16.2.236	172.16.1.20	TCP	netview-aix-11 > http-alt [ACK] Seq=1 Ack=4097 win=64240 Len=0
13	0.006826	172.16.1.20	172.16.2.236	HTTP	Continuation or non-HTTP traffic
14	0.006962	172.16.1.20	172.16.2.236	HTTP	Continuation or non-HTTP traffic
15	0.007079	172.16.2.236	172.16.1.20	TCP	netview-aix-11 > http-alt [ACK] Seq=1 Ack=6145 win=64240 Len=0
16	0.007221	172.16.3.129	172.16.201.60	ICMP	Echo (ping) request
17	0.007951	172.16.1.20	172.16.2.236	HTTP	Continuation or non-HTTP traffic
18	0.007972	64.236.34.97	172.16.2.219	TCP	http > metasage [ACK] Seq=1 Ack=1 win=4096 Len=0
19	0.008068	172.16.1.20	172.16.2.236	HTTP	Continuation or non-HTTP traffic
20	0.008263	172.16.1.20	172.16.2.236	HTTP	Continuation or non-HTTP traffic
21	0.008279	172.16.1.40	172.16.2.5	TCP	av-us > radmin-port [PSH. ACK] Seq=1 Ack=1 win=16306 Len=14

Below the packet list, the packet details pane shows the structure of the selected packet (Frame 7):

- Frame 7 (1514 bytes on wire, 1514 bytes captured)
- Ethernet II, Src: Cisco_07:a2:b0 (00:0c:85:07:a2:b0), Dst: 3Com_21:5a:ee (00:04:76:21:5a:ee)
- Internet Protocol, Src: 172.16.1.20 (172.16.1.20), Dst: 172.16.2.236 (172.16.2.236)
- Transmission Control Protocol, Src Port: http-alt (8080), Dst Port: netview-aix-11 (1671), Seq: 1, Ack: 1, Len: 1460
- Hypertext Transfer Protocol

The packet bytes pane at the bottom shows the raw data in hexadecimal and ASCII:

```
0000  00 04 76 21 5a ee 00 0c 85 07 a2 b0 08 00 45 00  ..v!Z... ..E.
0010  05 dc da 91 40 00 7e 06 c0 69 ac 10 01 14 ac 10  ....@.. .i.....
0020  02 ec 1f 90 06 87 63 1c 76 33 75 66 1b 04 50 10  ....C. v3uf..P.
0030  ff ff c8 c0 00 00 09 09 09 09 09 3c 74 72 3e     ....<tr>
0040  3c 74 64 20 68 65 69 67 68 74 3d 22 33 22 3e 3c  <td heig ht="3"><
0050  7f 74 64 20 2c 2f 74 72 20 0d 02 00 00 00 00 00  (tds</tr> </td>
```

The status bar at the bottom indicates: File: "D:\Courses\Freeware\Example 016.cap" 4... Packets: 11108 Displayed: 11108 Marked: 0 Profile: Default

Colorizing Specific Packets (4/4)

Filter: Expression... Clear Apply

No. -	Time	Source	Destination	Protocol	Info
1	0.000000	192.168.2.100	198.65.166.131	UDP	Source port: 64064 Destination port: sip
2	1.708525	192.168.2.100	130.94.88.123	TCP	appworxsr > https [FIN, ACK] Seq=1 Ack=1 win=64240 Len=0
3	1.709469	192.168.2.100	130.94.88.123	TCP	lv-jc > https [SYN] Seq=0 win=65535 Len=0 MSS=1460 WS=1 TSV=0 TSER=
4	2.001023	130.94.88.123	192.168.2.100	TCP	https > lv-jc [SYN, ACK] Seq=0 Ack=1 win=5840 Len=0 MSS=1460 WS=2
5	2.001077	192.168.2.100	130.94.88.123	TCP	lv-jc > https [ACK] Seq=1 Ack=1 win=128480 Len=0
6	2.001180	130.94.88.123	192.168.2.100	TCP	https > appworxsr [ACK] Seq=1 Ack=2 win=3756 Len=0
7	2.001777	192.168.2.100	130.94.88.123	SSL	Client Hello
8	2.308152	130.94.88.123	192.168.2.100	TCP	https > lv-jc [ACK] Seq=1 Ack=103 win=5840 Len=0
9	2.308490	130.94.88.123	192.168.2.100	TLSv1	Server Hello,
10	2.309543	130.94.88.123	192.168.2.100	TCP	[TCP segment of a reassembled PDU]
11	2.309618	192.168.2.100	130.94.88.123	TCP	lv-jc > https [ACK] Seq=103 Ack=2705 win=128480 Len=0
12	2.617428	130.94.88.123	192.168.2.100	TCP	[TCP segment of a reassembled PDU]
13	2.619328	130.94.88.123	192.168.2.100	TLSv1	Certificate, Server Hello Done
14	2.619440	192.168.2.100	130.94.88.123	TCP	lv-jc > https [ACK] Seq=103 Ack=4549 win=128480 Len=0
15	2.620478	192.168.2.100	130.94.88.123	TLSv1	Client Key Exchange, Change Cipher Spec, Encrypted Handshake Message
16	2.922741	130.94.88.123	192.168.2.100	TLSv1	Change Cipher Spec, Encrypted Handshake Message
17	2.926069	192.168.2.100	130.94.88.123	TCP	[TCP segment of a reassembled PDU]
18	2.926211	192.168.2.100	130.94.88.123	TLSv1	Application Data
19	3.229909	130.94.88.123	192.168.2.100	TCP	https > lv-jc [ACK] Seq=4592 Ack=1782 win=12320 Len=0
20	3.234770	130.94.88.123	192.168.2.100	TCP	[TCP segment of a reassembled PDU]
21	3.235519	130.94.88.123	192.168.2.100	TLSv1	Application Data
22	3.235588	192.168.2.100	130.94.88.123	TCP	lv-jc > https [ACK] Seq=1782 Ack=6110 win=128480 Len=0
23	3.737122	192.168.2.100	130.94.88.123	TCP	[TCP segment of a reassembled PDU]
24	3.737295	192.168.2.100	130.94.88.123	TLSv1	Application Data
25	4.151556	130.94.88.123	192.168.2.100	TCP	https > lv-jc [ACK] Seq=6110 Ack=3261 win=15024 Len=0
26	4.151984	130.94.88.123	192.168.2.100	TCP	[TCP segment of a reassembled PDU]
27	4.152276	130.94.88.123	192.168.2.100	TLSv1	Application Data
28	4.152370	192.168.2.100	130.94.88.123	TCP	lv-jc > https [ACK] Seq=3261 Ack=7776 win=128480 Len=0
29	7.936331	192.168.2.100	212.150.49.10	DNS	Standard query A mail.barak.net.il
30	8.025917	212.150.49.10	192.168.2.100	DNS	Standard query response A 194.90.6.40
31	8.077161	192.168.2.100	194.90.6.40	TCP	dynamic3d > pop3 [SYN] Seq=0 win=65535 Len=0 MSS=1460 WS=1 TSV=0 TS
32	8.098732	194.90.6.40	192.168.2.100	TCP	pop3 > dynamic3d [SYN, ACK] Seq=0 Ack=1 win=49580 Len=0 TSV=8290107
33	8.098776	192.168.2.100	194.90.6.40	TCP	dynamic3d > pop3 [ACK] Seq=1 Ack=1 win=128480 Len=0 TSV=7813 TSER=8
34	8.118204	194.90.6.40	192.168.2.100	POP	S: +OK POP3 service
35	8.118745	192.168.2.100	194.90.6.40	POP	C: USER yoram-ndi.co.il
36	8.138633	194.90.6.40	192.168.2.100	TCP	pop3 > dynamic3d [ACK] Seq=19 Ack=23 win=49580 Len=0 TSV=829010732
37	8.140050	194.90.6.40	192.168.2.100	POP	S: +OK password required for user yoram-ndi.co.il

References

- Wireshark Website
 - <http://www.wireshark.org>
- Wireshark Documentation
 - <http://www.wireshark.org/docs/>
- Wireshark Wiki
 - <http://wiki.wireshark.org>
- Network analysis Using Wireshark Cookbook
 - <http://www.amazon.com/Network-Analysis-Using-Wireshark-Cookbook/dp/1849517649>

Q&A

