

Internet Traffic Monitoring and Analysis: Wireshark Tutorial

POSTECH CSED702D: Internet Traffic Monitoring and Analysis 1/39

Outline

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

POSTECH CSED702D: Internet Traffic Monitoring and Analysis 2/39

What is Wireshark?



❖ The De-Facto Network Protocol Analyzer

- Open-Source (GNU Public License)
- Multi-platform (Windows, Linux, OS X, Solaris, FreeBSD, NetBSD, and others)
- Easily extensible
- Large development group

❖ Previously Named “Ethereal”



POSTECH

CSED702D: Internet Traffic Monitoring and Analysis

3/39

What is Wireshark?



❖ Features

- Deep inspection of thousands of protocols
- 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

POSTECH

CSED702D: Internet Traffic Monitoring and Analysis

4/39

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**

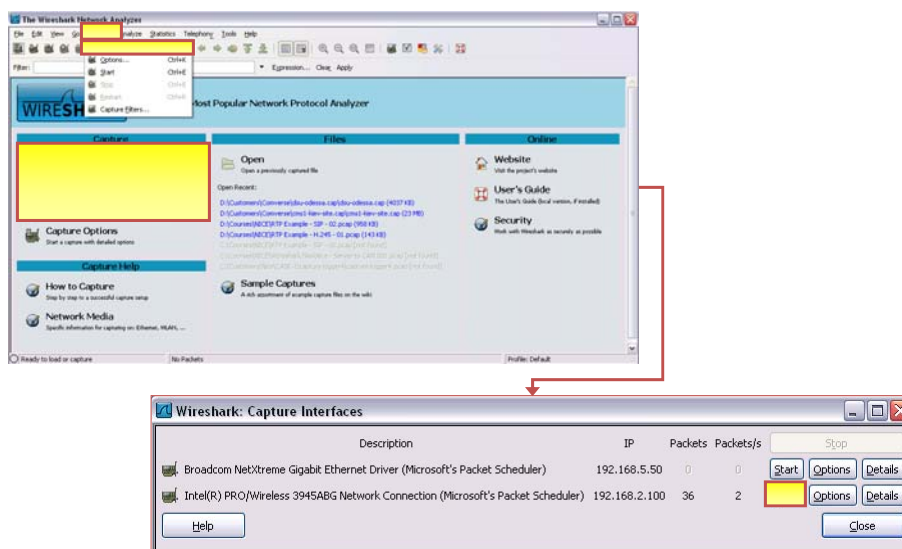
Interfaces



The screenshot shows the Wireshark interface with the following panes:

- Packet List:** A table of captured packets. The first packet is an Echo (ping) request from 192.168.2.100 to 10.100.102.2.
- Packet Details:** A hierarchical view of the selected packet's structure, showing Ethernet II, Internet Protocol, User Datagram Protocol, and Simple Network Management Protocol.
- Packet Bytes:** A hex dump and ASCII representation of the packet data.

Capturing Packets (1/3)

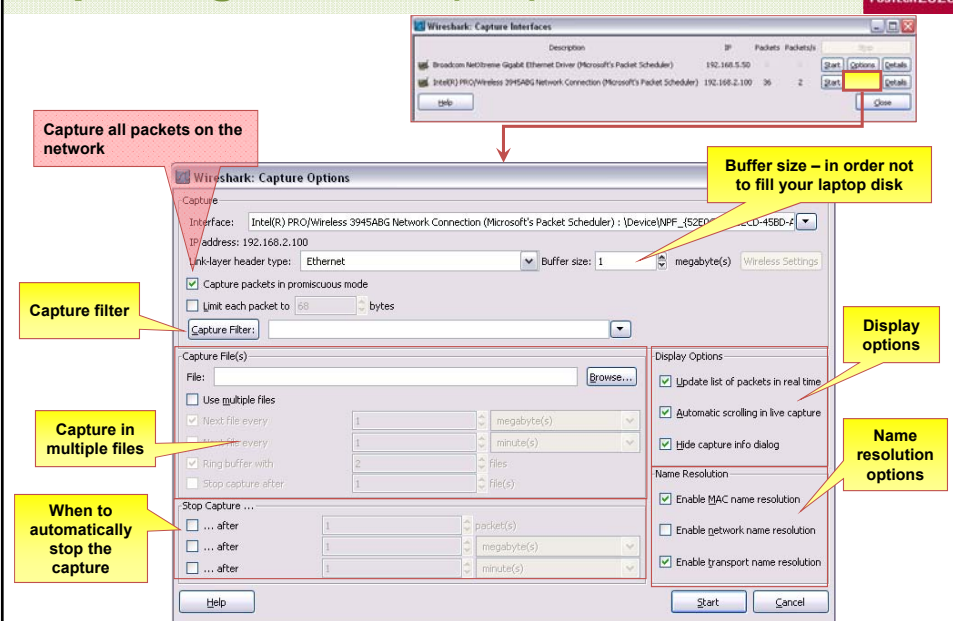


POSTECH

CSIED702D: Internet Traffic Monitoring and Analysis

7/39

Capturing Packets (2/3)



POSTECH

CSIED702D: Internet Traffic Monitoring and Analysis

8/39

Capturing Packets (3/3)



Wireshark: Capture Interfaces

Description	IP	Packets	Packet/s
Broadcom NetXtreme Gigabit Ethernet Driver (Microsoft's Packet Scheduler)	192.168.5.50		
Intel(R) PRO/Wireless 3945ABG Network Connection (Microsoft's Packet Scheduler)	192.168.2.100	36	2

Wireshark: Interface Details

Current network:

- SSID (Service Set Identifier): default
- BSSID (Basic Service Set Identifier): 00:0E:2E:6E:2F:7D (EdmaxTe)
- Network type used: 2.4-GHz OFDM
- Infrastructure mode: Access Point
- Authentication mode: Open System
- Encryption status: WEP & TKIP & AES disabled, transmit key available
- TX power: -

RSSI (Received Signal Strength Indication): -69 dBm

Link Speed: 54 MBits/s

Supported Rates: 1/2/5.5/11/6/9/12/18/24/36/48/54 MBits/s

Desired Rates: -

Channel: 4 (2427 MHz)

Available networks (BSSID list):

SSID	MAC	Vendor	Privacy	RSSI	Network Type	Infra. Mode	Ch.	Rates	Country
default	00:0E:2E:6E:2F:7D	EdmaxTe	None	-69 dBm	2.4-GHz OFDM	Access Point	4	1/2/5.5/11/6/9/12/18 MBits/s	

Note: accuracy of all of these values are only relying on the network card driver!

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

POSTECH

CSED702D: Internet Traffic Monitoring and Analysis

9/39

Analyzing Packets (1/9)



❖ Ethernet Frame Example

No. ·	Time	Source	Destination	Protocol	Info
4	23.847333	212.179.1.202	10.159.3.103	FTP	Source ports: 33333 destination
5	23.838867	10.159.3.103	212.179.1.202	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: MOTM upload1_1936
9	24.208994	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

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: ethip:tcp:ftp]

[Coloring Rule Name: TCP]

[Coloring Rule String: tcp]

Ethernet II, Src: Xerox_00:00:00:01:00:00 (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_00:00:00:01:00:00 (01:00:01:00:00:00)

Address: Xerox_00:00:00:01:00:00 (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)

POSTECH

CSED702D: Internet Traffic Monitoring and Analysis

10/39

Analyzing Packets (2/9)



❖ IP Packet Example

No. -	Time	Source	Destination	Protocol	Info
4	23.227539	1.1.1.1	127.0.0.1	UDP	Source port: 33333 Destination port: 33333
5	23.838867	212.179.1.202	10.159.3.103	FTP	Response: 200 Type set to 1
6	23.857421	10.159.3.103	212.179.1.202	FTP	Request: SIZE upload_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 upload_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)

POSTECH

CSED702D: Internet Traffic Monitoring and Analysis

11/39

Analyzing Packets (3/9)



❖ TCP Packet Example

No. -	Time	Source	Destination	Protocol	Info
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	24.301601	212.179.1.202	10.159.3.103	FTP	Response: 222 Entering Passive...

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: 16385
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]
File Transfer Protocol (FTP)

POSTECH

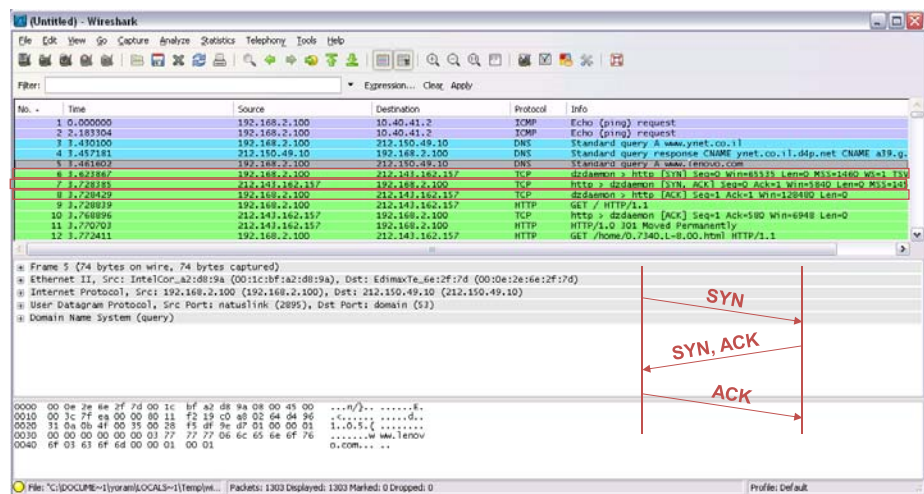
CSED702D: Internet Traffic Monitoring and Analysis

12/39

Analyzing Packets (4/9)



❖ TCP 3-way Handshake



POSTECH

CSED702D: Internet Traffic Monitoring and Analysis

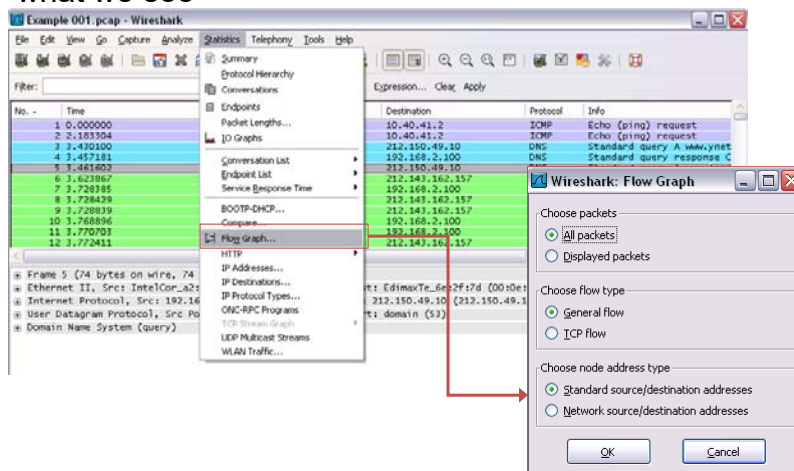
13/39

Analyzing Packets (5/9)



❖ Flow Graph

- Giving us a graphical flow, for better understanding of what we see



POSTECH

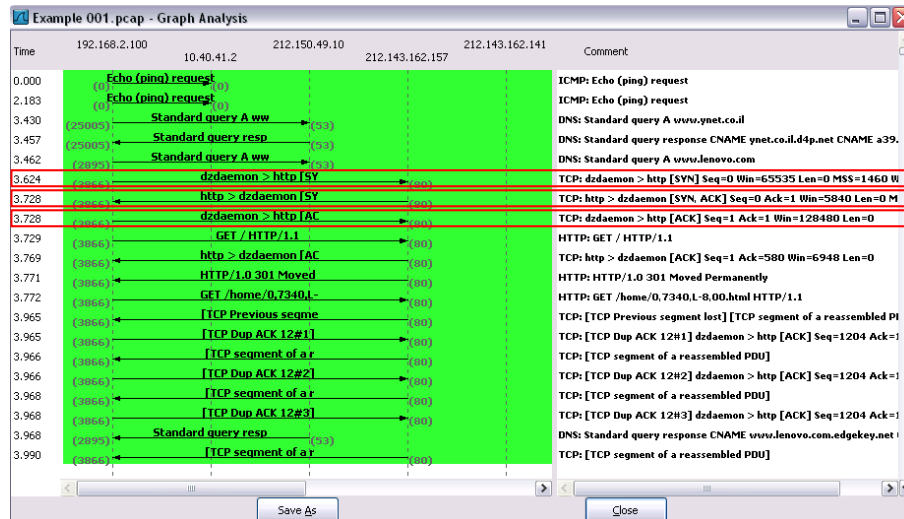
CSED702D: Internet Traffic Monitoring and Analysis

14/39

Analyzing Packets (6/9)



❖ Flow Graph



POSTECH

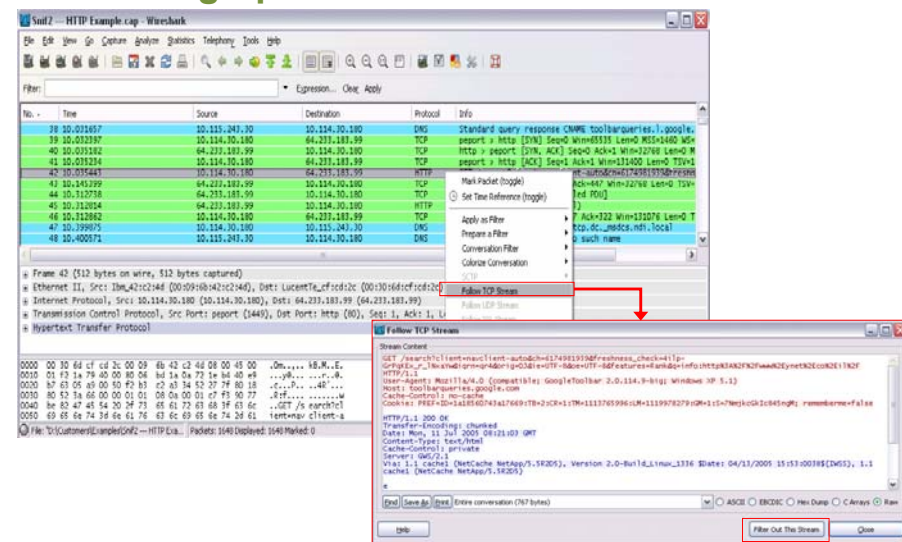
CSED702D: Internet Traffic Monitoring and Analysis

15/39

Analyzing Packets (7/9)



❖ Filtering Specific TCP Stream



POSTECH

CSED702D: Internet Traffic Monitoring and Analysis

16/39

Analyzing Packets (8/9)



❖ Filtering Specific TCP Stream

Wireshark interface showing packet filtering. The filter bar contains the expression `(tcp.stream eq 5)`. The packet list displays 19 packets, with the selected packet (No. 19) showing details for Ethernet II, Internet Protocol, and Transmission Control Protocol. The packet bytes pane shows the raw data in hexadecimal and ASCII.

POSTECH

CSIED702D: Internet Traffic Monitoring and Analysis

17/39

Analyzing Packets (9/9)



❖ RTP Stream Analysis

Wireshark interface showing RTP Stream Analysis. The packet list displays RTP packets. The RTP Stream Analysis window is open, displaying a table of RTP packets with columns for Sequence, Delta, Filtered, Skew, and Status. A red box highlights the text "Stable stream BW".

Packet	Sequence	Delta (ms)	Filtered	Skew (ms)	SP BW (bps)	Marker	Status
1417	19063	0.00	0.00	0.00	24.40		[Ok]
1419	19064	0.00	0.00	0.00	24.40		[Ok]
1421	19065	0.00	0.00	0.00	24.40		[Ok]
1423	19066	0.00	0.00	0.00	24.40		[Ok]
1425	19067	0.00	0.00	0.00	24.40		[Ok]
1427	19068	0.00	0.00	0.00	24.40		[Ok]
1429	19069	0.00	0.00	0.00	24.40		[Ok]
1431	19070	0.00	0.00	0.00	24.40		[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 = 2090 (expected 2090). Lost RTP packets = 0 (0.00%). Sequence errors = 0
 Duration 62.85 s (0 ms clock drift, corresponding to 1 Hz (+0.00%))

POSTECH

CSIED702D: Internet Traffic Monitoring and Analysis

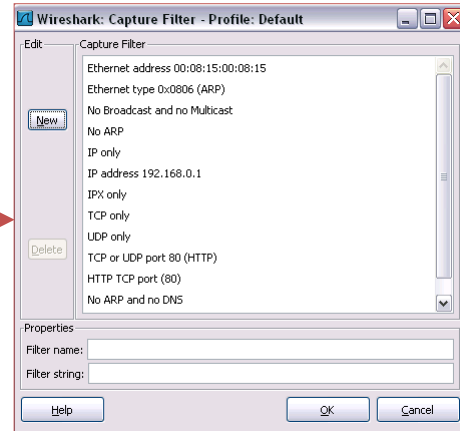
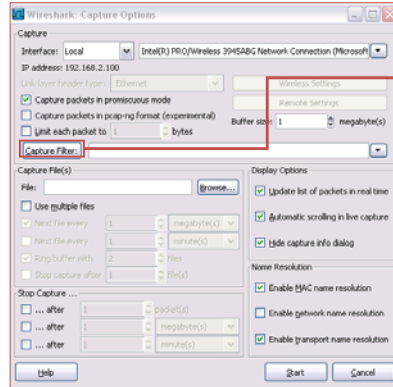
18/39

Filtering Packets (1/4)



❖ Applying Filter when Capturing Packets

Capture → Interfaces → Options:



POSTECH

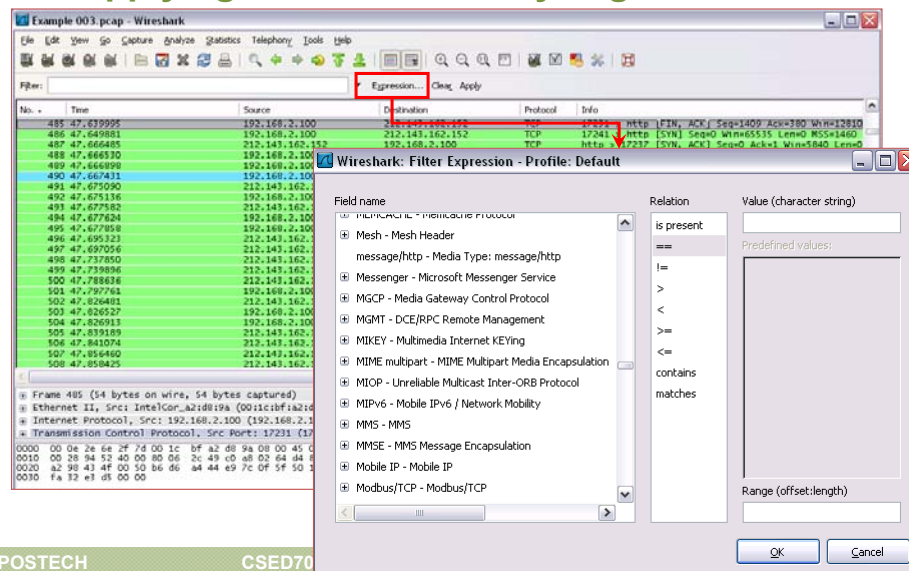
CSED702D: Internet Traffic Monitoring and Analysis

19/39

Filtering Packets (2/4)



❖ Applying Filter when Analyzing Packets



POSTECH

CSED70

9

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**

POSTECH

CSIED702D: Internet Traffic Monitoring and Analysis

21/39

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**

POSTECH

CSIED702D: Internet Traffic Monitoring and Analysis

22/39

Saving and Manipulating Packets (1/3)



❖ Save only displayed packets

POSTECH CSED702D: Internet Traffic Monitoring and Analysis 23/39

Saving and Manipulating Packets (2/3)



❖ Export to CSV file

POSTECH CSED702D: Internet Traffic Monitoring and Analysis 24/39

Saving and Manipulating Packets (3/3)



❖ Exported CSV File

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 /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 /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	24.12328	23.472292	192.168.2.100	216.239.122.164	HTTP	GET /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 /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	35.945425	33.109896	192.168.2.100	216.239.122.164	TCP	27837 > http [ACK] Seq=4080 Ack=3567 Win=65033 Len=0

POSTECH

CSED702D: Internet Traffic Monitoring and Analysis

25/39

Packet Statistics (1/8)



❖ Protocol Hierarchy

Wireshark: Protocol Hierarchy Statistics

Display filter: none

Protocol	% Packets	Packets: Bytes	Mbit/s	End Packets: End Bytes: End Mbit/s
Frame	100.00 %	1276 385508	0.030	0 0 0.000
Ethernet	100.00 %	1276 385508	0.030	0 0 0.000
Internet Protocol	99.69 %	1272 385340	0.030	0 0 0.000
Internet Control Message Protocol	8.23 %	105 7770	0.001	105 7770 0.001
User Datagram Protocol	4.86 %	62 11029	0.001	0 0 0.000
Simple Network Management Protocol	1.57 %	20 1825	0.000	20 1825 0.000
Bootstrap Protocol	0.31 %	4 1864	0.000	4 1864 0.000
NetBIOS Name Service	0.24 %	3 276	0.000	3 276 0.000
Domain Name Service	2.66 %	34 6922	0.001	34 6922 0.001
Data	0.08 %	1 142	0.000	1 142 0.000
Transmission Control Protocol	86.60 %	1105 366541	0.028	658 149347 0.011
Post Office Protocol	1.41 %	18 1486	0.000	18 1486 0.000
Hypertext Transfer Protocol	33.62 %	429 215708	0.017	388 188597 0.014
Line-based text data	2.27 %	29 21877	0.002	29 21877 0.002
JPEG File Interchange Format	0.08 %	1 59	0.000	1 59 0.000
extensible Markup Language	0.39 %	5 2730	0.000	5 2730 0.000
Media Type	0.16 %	2 1160	0.000	2 1160 0.000
CompuServe GIF	0.31 %	4 1285	0.000	4 1285 0.000
Address Resolution Protocol	0.31 %	4 168	0.000	4 168 0.000

POSTECH

CSED702D: Internet Traffic Monitoring and Analysis

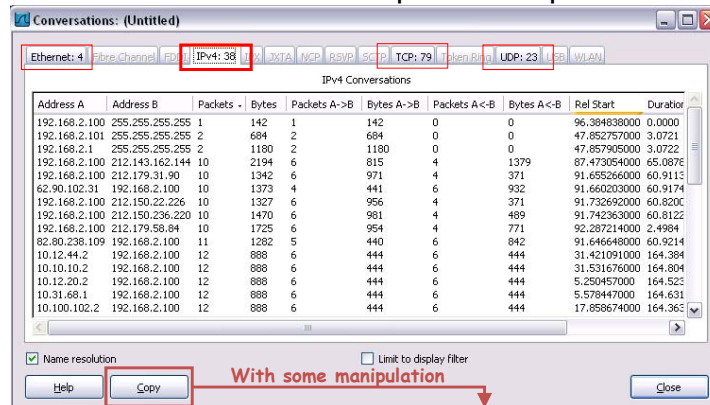
26/39

Packet Statistics (2/8)



❖ Conversation

- Traffic between two specific endpoints

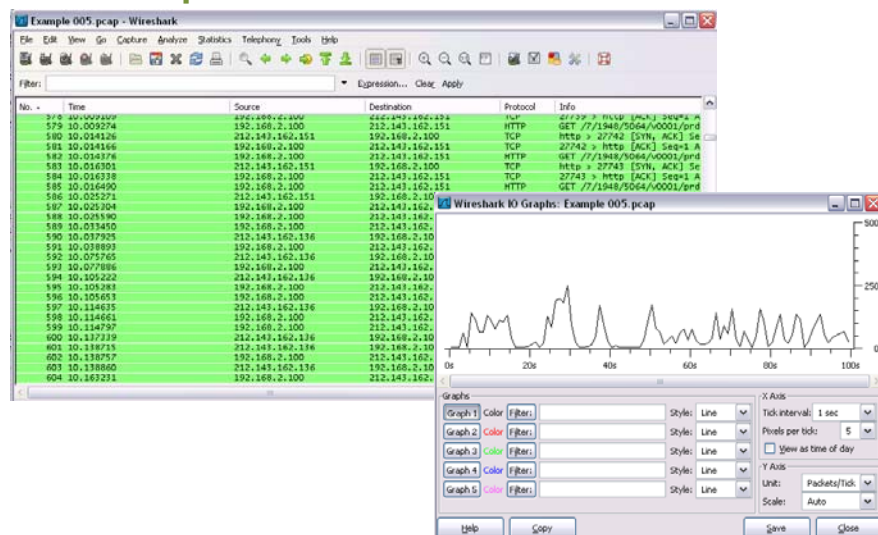


	A	B	C	D	E	F	G	H	I	J	K	L	
1	Address A	Address B	Packets	Bytes	Packets A->B	Bytes A->B	Packets A<-B	Bytes A<-B	Rel Start	Duration	bps A->B	bps A<-B	
2	10.10.10.1	10.159.3.103	2	124	0	0	2	124	0	42.0039	N/A	23.62	
3	1.1.1.1	10.159.3.103	2	120	0	0	2	120	24.49414	1.1885	N/A	807.76	
4	1.1.1.1	127.0.0.1	4	248	4	248	0	0	10.713867	14.9814	132.43	N/A	
5	10.159.3.103	212.179.1.202	491	458158	185	10643	306	447515	23.216796	15.4082	5525.89	232351.54	39

Packet Statistics (3/8)



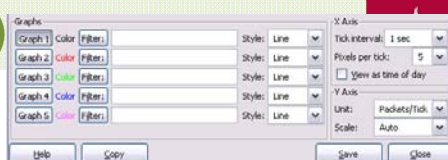
❖ I/O Graph



Packet Statistics (4/8)

❖ 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, ...)



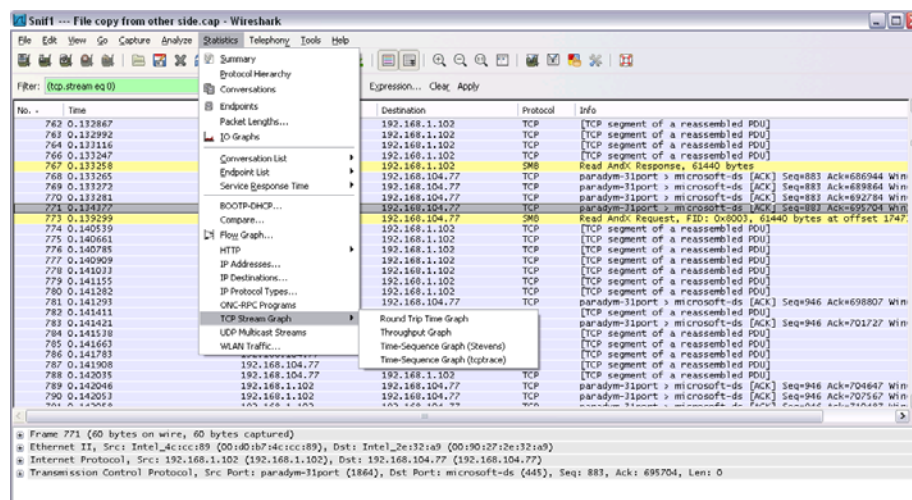
POSTECH

CS2ED702D: Internet Traffic Monitoring and Analysis

29/39

Packet Statistics (5/8)

❖ TCP Stream Graph



POSTECH

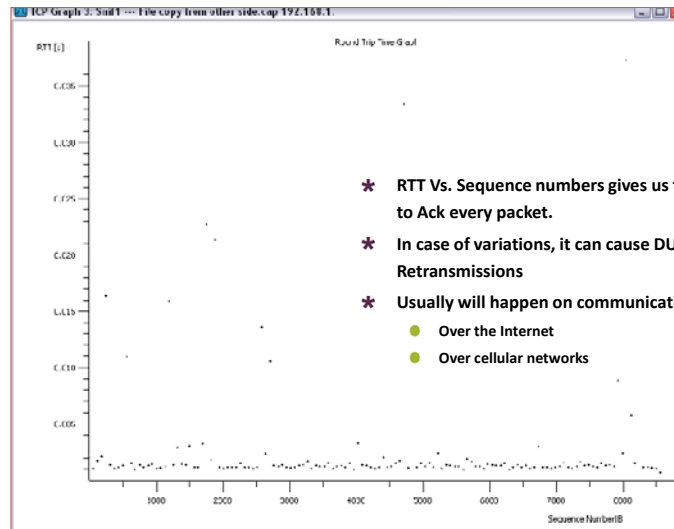
CS2ED702D: Internet Traffic Monitoring and Analysis

30/39

Packet Statistics (6/8)



❖ Round-Trip Time Graph



- * RTT Vs. Sequence numbers gives us the time that take to Ack every packet.
- * In case of variations, it can cause DUPACKs and even Retransmissions
- * Usually will happen on communications lines:
 - Over the Internet
 - Over cellular networks

POSTECH

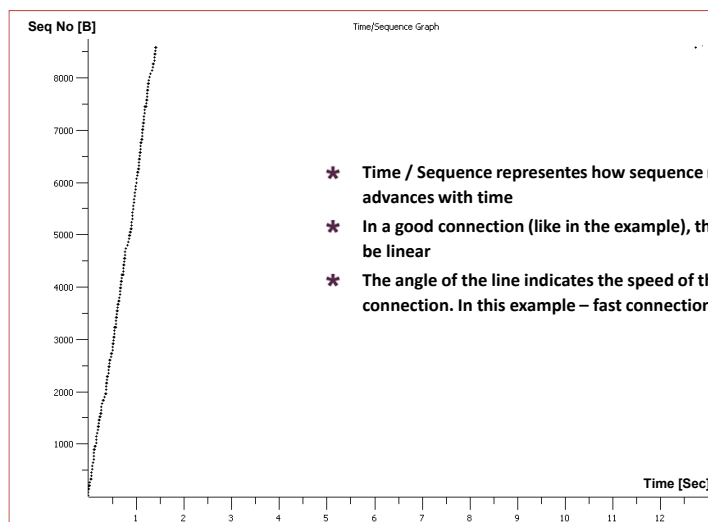
CSED702D: Internet Traffic Monitoring and Analysis

31/39

Packet Statistics (7/8)



❖ Time / Sequence Graph



- * Time / Sequence represents how sequence numbers advances with time
- * In a good connection (like in the example), the line will be linear
- * The angle of the line indicates the speed of the connection. In this example – fast connection

POSTECH

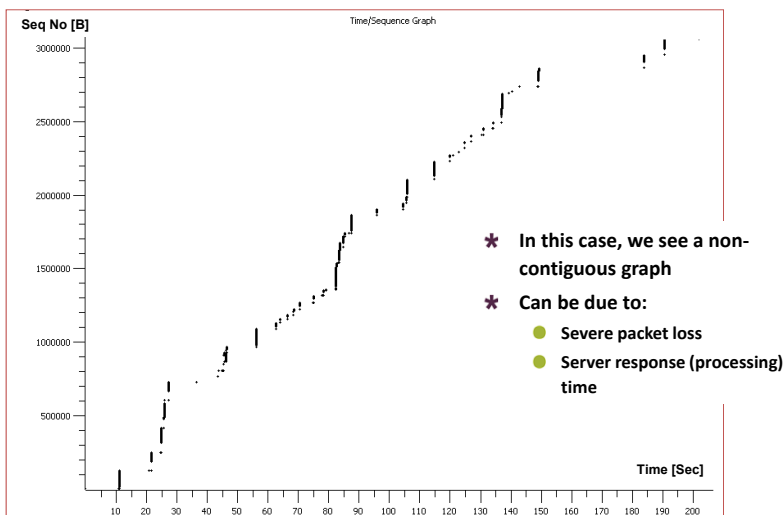
CSED702D: Internet Traffic Monitoring and Analysis

32/39

Packet Statistics (8/8)



❖ Time / Sequence Graph



POSTECH

CSIED702D: Internet Traffic Monitoring and Analysis

33/39

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	172.17.220.67	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	0.004728	172.16.2.236	172.16.1.20	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	0.005780	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 > metasploit [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	ov-us > radmin-port [PSH, ACK] Seq=1 Ack=1 win=16306 Len=14

POSTECH

CSIED702D: Internet Traffic Monitoring and Analysis

34/39

Colorizing Specific Packets (2/4)



The screenshot shows the Wireshark interface with the following details:

- Filter:** Expression... Clear Apply
- Packet List:**

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	0.005158	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	172.16.1.20	TCP	http > message [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	0.008268	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	ov-us > radin-port [PSH, ACK] Seq=1 Ack=1 win=16306 Len=14
- Packet Details:**
 - Frame 2 (108 bytes on wire, 108 bytes captured)
 - Ethernet II, Src: 3com:74:5a:12b (00:0c:85:07:a2:b0), 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: wntesrv (1334), Dst Port: alta-ana-lm (1346), Seq: 1, Ack: 1, Len: 1
 - DCE RPC Request, Fragment: Single, FragLen: 144, Call: 395 Ctx: 0
- Colorize Conversation:**
 - Color 1
 - Color 2
 - Color 3
 - Color 4
 - Color 5
 - Color 6
 - Color 7
 - Color 8
 - Color 9
 - Color 10
 - New Coloring Rule...

POSTECH

CSIED702D: Internet Traffic Monitoring and Analysis

35/39

Colorizing Specific Packets (3/4)



The screenshot shows the Wireshark interface with the following details:

- Filter:** Expression... Clear Apply
- Packet List:**

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	0.005158	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	172.16.1.20	TCP	http > message [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	0.008268	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	ov-us > radin-port [PSH, ACK] Seq=1 Ack=1 win=16306 Len=14
- Packet Details:**
 - 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
- Colorize Conversation:**
 - Color 1
 - Color 2
 - Color 3
 - Color 4
 - Color 5
 - Color 6
 - Color 7
 - Color 8
 - Color 9
 - Color 10
 - New Coloring Rule...

POSTECH

CSIED702D: Internet Traffic Monitoring and Analysis

36/39

Colorizing Specific Packets (4/4)



❖ TLS Connection Establishment

No.	Time	Source	Destination	Protocol	Info
1	0.000000	192.168.2.100	198.65.166.131	UDP	Source port: 64064 Destination port: 51p
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 > lv-jc [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	SSL	Server Hello
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	lv-jc > https [ACK] Seq=103 Ack=2705 Win=128480 Len=0
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	TLSv1	Certificate, Server Hello done
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=2705 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	2.927741	130.94.88.123	192.168.2.100	TLSv1	Change Cipher Spec, Encrypted Handshake Message
17	2.927669	192.168.2.100	130.94.88.123	TCP	lv-jc > https [ACK] Seq=4502 Ack=1782 Win=12320 Len=0
18	2.926211	192.168.2.100	130.94.88.123	TLSv1	Application data
19	2.229909	130.94.88.123	192.168.2.100	TCP	lv-jc > https [ACK] Seq=1782 Ack=6110 Win=128480 Len=0
20	3.234770	130.94.88.123	192.168.2.100	TCP	lv-jc > https [ACK] Seq=1782 Ack=6110 Win=128480 Len=0
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=6110 Ack=3261 Win=15024 Len=0
23	3.737122	192.168.2.100	130.94.88.123	TLSv1	Application data
24	3.737295	192.168.2.100	130.94.88.123	TLSv1	Application data
25	4.131556	130.94.88.123	192.168.2.100	TCP	lv-jc > https [ACK] Seq=3261 Ack=7776 Win=128480 Len=0
26	4.131984	130.94.88.123	192.168.2.100	TCP	lv-jc > https [ACK] Seq=3261 Ack=7776 Win=128480 Len=0
27	4.132276	130.94.88.123	192.168.2.100	TCP	lv-jc > https [ACK] Seq=3261 Ack=7776 Win=128480 Len=0
28	4.132370	192.168.2.100	130.94.88.123	TCP	lv-jc > https [ACK] Seq=3261 Ack=7776 Win=128480 Len=0
29	7.999952	192.168.2.100	212.150.49.10	DNS	Standard query request
30	8.025917	212.150.49.10	192.168.2.100	DNS	Standard query response
31	8.077161	192.168.2.100	194.90.6.40	TCP	dynamicid > pop3 [SYN] Seq=0 Win=65535 Len=0 MSS=1460 WS=1 TSv=0 TSEr=
32	8.098732	194.90.6.40	192.168.2.100	TCP	pop3 > dynamicid [SYN, ACK] Seq=0 Ack=1 Win=49580 Len=0 TSv=8290102
33	8.098776	192.168.2.100	194.90.6.40	TCP	dynamicid > pop3 [ACK] Seq=1 Ack=1 Win=128480 Len=0 TSv=7813 TSEr=
34	8.118204	194.90.6.40	192.168.2.100	POP	5: 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 > dynamicid [ACK] Seq=19 Ack=23 Win=49580 Len=0 TSv=829010732
37	8.140050	194.90.6.40	192.168.2.100	POP	5: OK password required for user yoram-ndi.co.il

POSTECH

CSIED702D: Internet Traffic Monitoring and Analysis

37/39

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>

POSTECH

CSIED702D: Internet Traffic Monitoring and Analysis

38/39

Q&A





POSTECH

CSED702D: Internet Traffic Monitoring and Analysis

39/39