
Wireshark Training

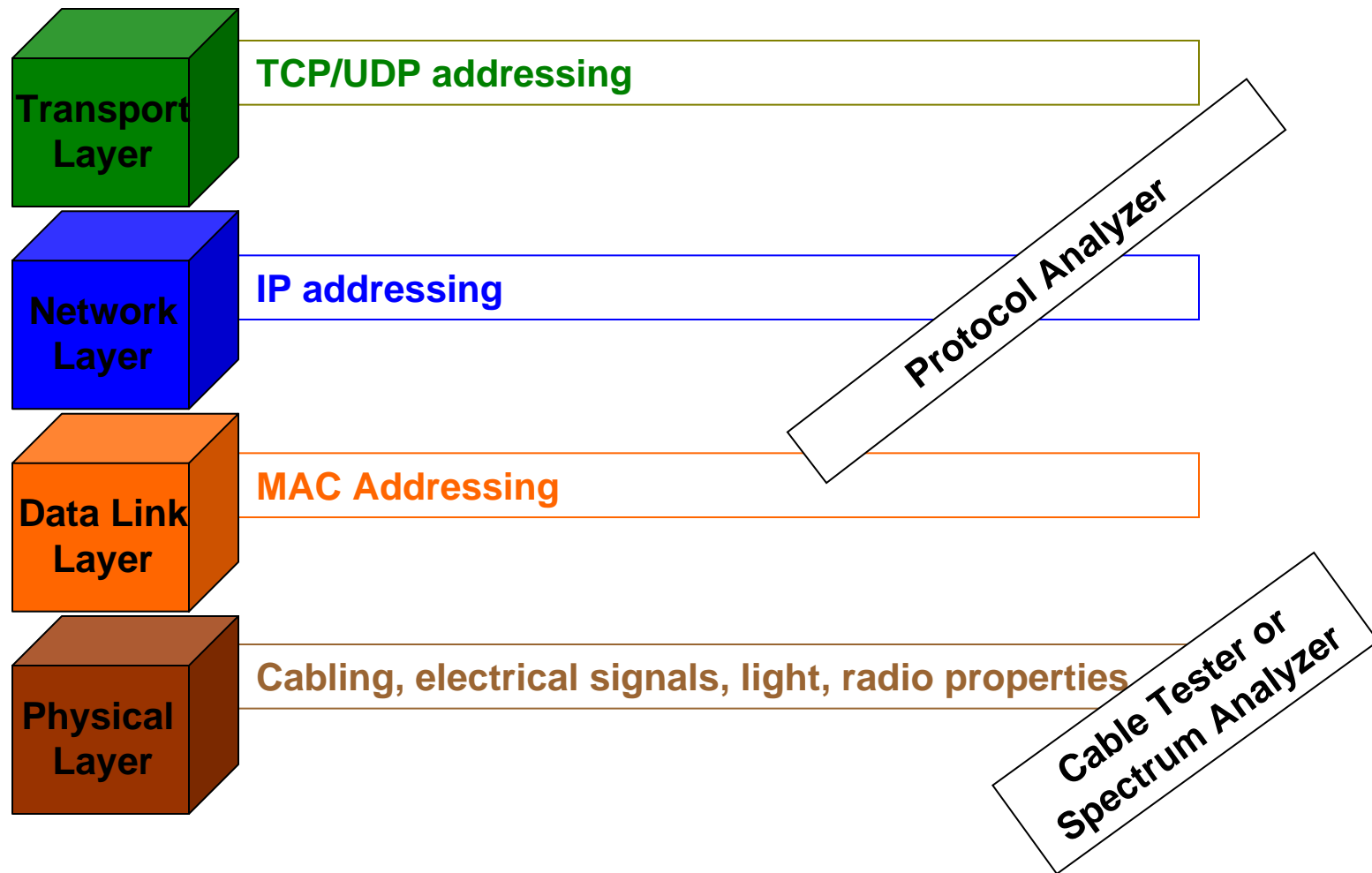


Tony Fortunato, The Technology Firm

Why use Wireshark?

- Wireshark can be used for the following tasks;
 - ✓ To determine how your applications behave on the wire
 - ✓ To identify application dependencies
 - ❖ For assistance in configuring firewalls
 - ❖ In understanding why your application is slow
 - ✓ To see if login or critical data is in clear text or not
 - ✓ Make sure your PC is configured optimally and it doesn't generate unnecessary traffic
 - ✓ Identify viruses, Trojans, worms or other uninstalled software
 - ✓ Monitor network for unwelcome applications like peer to peer applications

What is a Protocol Analyzer?



Windows Installation Command Line Option



- If you run the setup file with no, or incorrect options, you get the standard installer
- Helpful command line options;
 - ✓ /S runs the installer or uninstaller silently with default values.
 - ❖ Default values are *desktopicon=yes* and */quicklaunchicon=yes*
 - ❖ The silent installer option doesn't install WINPCAP!
 - ✓ /desktopicon installation of the desktop icon, =yes - force installation, =no - don't install, otherwise use defaults / user settings. This option can be useful for a silent installer.
 - ✓ /quicklaunchicon installation of the quick launch icon, =yes - force installation, =no - don't install, otherwise use defaults / user settings.
 - ✓ /D sets the default installation directory (\$INSTDIR), overriding InstallDir and InstallDirRegKey. It must be the last parameter used in the command line and must not contain any quotes, even if the path contains spaces.

Example:

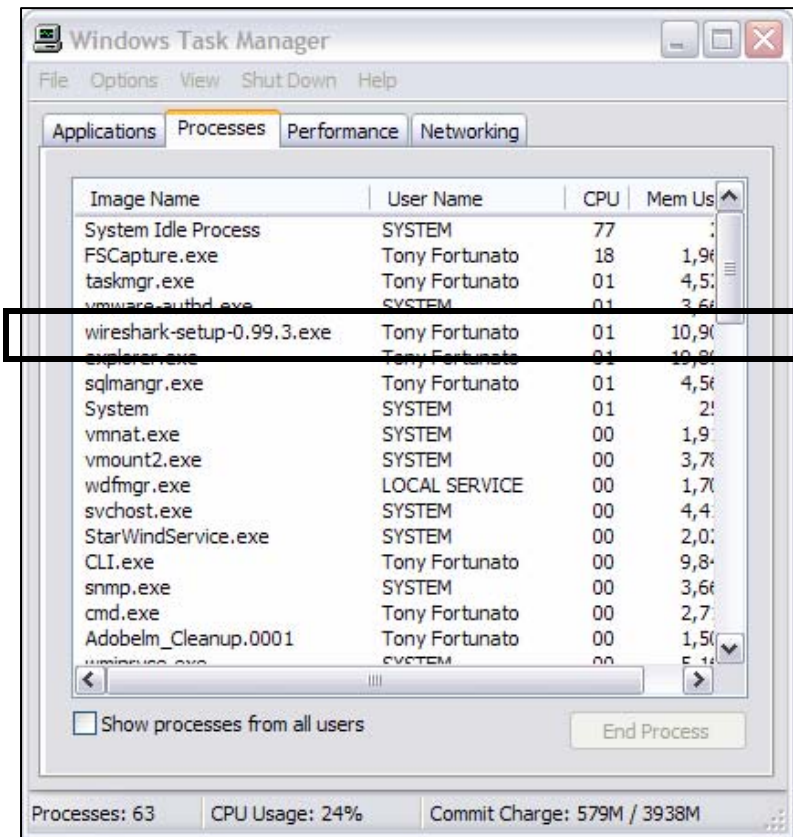
The following will silently install Wireshark without a *desktopicon* or *quicklaunchicon*;

- ✓ `wireshark-setup-0.99.3.exe /S /desktopicon=no /quicklaunchicon=no`

To Check Your Silent Install Progress



- The silent install is a real Catch-22
 - ✓ The good news is its silent, so you can get a customer to install it quickly, without prompts
 - ✓ The bad news is you really don't know when its done
 - ❖ To check the status of the install, use your Task Manager and sort by CPU. The Wireshark setup file will be near the top of the Processes list
 - ❖ Check your hard drive activity to get a sense if the software is being installed
 - ❖ Watch your Desktop and Quick Launch Toolbar for the Wireshark logo to appear



About your Wireshark



- To get information about your Wireshark installation go to Help -> About

WIRESHARK
Network Protocol Analyzer

Version 0.99.4 (SVN Rev 19757)

Copyright 1998-2006 Gerald Combs <gerald@wireshark.org>
This is free software; see the source for copying conditions. No warranty; not even for MERCHANTABILITY or FITNESS FOR A PARTICULAR PURPOSE.

Compiled with GTK+ 2.6.9, with GLib 2.6.6, with WinPcap 0.9.9, with libpcap 1.2.3, with libpcr 6.4, with Net-SNMP 5.3.1, with A GnuTLS 1.5.1, with Gcrypt 1.2.3, with MIT Kerberos, with AirPcap.

Running on Windows XP Service Pack 2, build 2600, with (packet.dll version 3, 1, 0, 27), based on libpcap version 0.9.9.4

Built using Microsoft Visual C++ 6.0 build 8804

Wireshark is Open Source Software released under the GPL

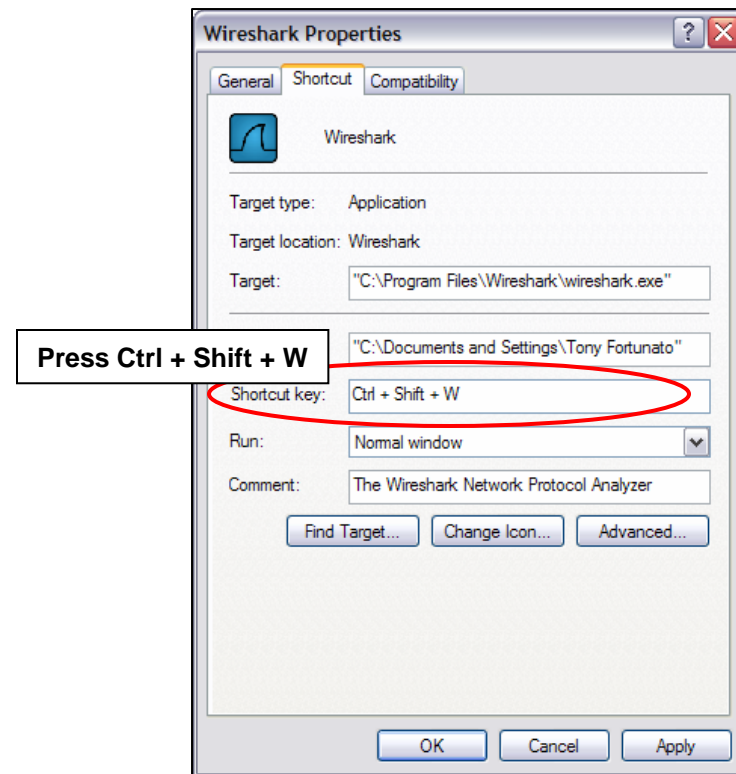
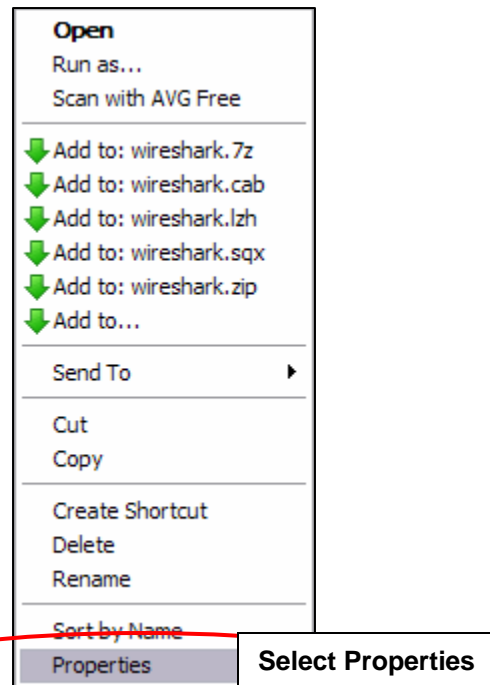
Check the man page and <http://www.wireshark.org> for more information

Name	Folder	Typical Files
"File" dialogs	C:\Documents and Settings\Tony Fortunato\Desktop\multiple files\	capture files
Global configuration	C:\Program Files\Wireshark	"dfilters", "preferences"
Global Plugins	C:\Program Files\Wireshark\plugins\0.99.4	dissector plugins
Personal configuration	C:\Documents and Settings\Tony Fortunato\Application Data\Wireshark\	"dfilters", "preferences"
Personal Plugins	C:\Documents and Settings\Tony Fortunato\Application Data\Wireshark\plugins	dissector plugins
Program	C:\Program Files\Wireshark	program files
System	C:\Program Files\Wireshark	"ethers", "ipxnets"
Temp	C:\DOCUME~1\TONYFO~1\LOCALS~1\Temp\	untitled capture files

Make It Easier To Launch Wireshark



- Add a “Shortcut key” to make Wireshark easier to get at.
- In this example, we assign Ctrl + Shift + W to Wireshark



Shortcut Keys

File Open	Ctrl + O	Mark Packet	Ctrl + M
File Close	Ctrl + W	Find Next Mark	Shift + Ctrl + N
File Save	Ctrl + S	Find Prev Mark	Shift + Ctrl + B
File Save As	Ctrl + Shift + S	Zoom In	Ctrl + +
File Quit	Ctrl + Q	Zoom Out	Ctrl + -
Preferences	Shift + Ctrl + P	Normal Size	Ctrl + =
Find Packet	Ctrl + F	Expand Protocol Tree	Ctrl + Right Arrow
Find Next	Ctrl + N	Collapse Protocol Tree	Ctrl + Left Arrow
Find Previous	Ctrl + B	Previous Packet	Ctrl + Pg Up
Set Time Reference	Ctrl + T	Next Packet	Ctrl + Down
Go to Packet No	Ctrl + G	Capture Options	Ctrl + K



How To Capture from the Command Prompt with Wireshark

The Technology Firm

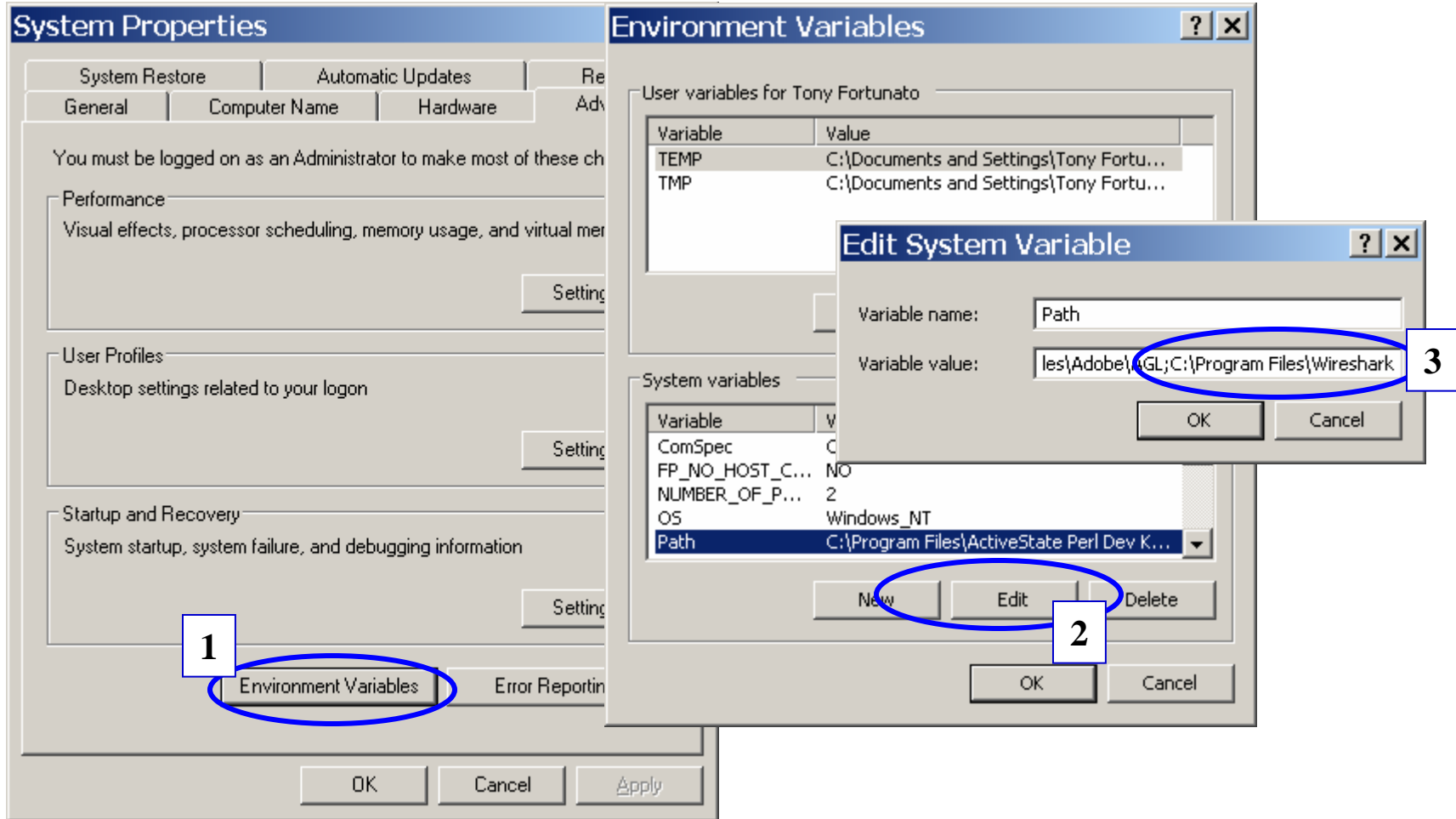


Things to do

1. Add Wireshark to your path
2. Determine which interface index maps to which NIC
3. Determine your capture parameters and location of your trace files
4. Test, check & go back to #2, if things don't work
5. Final command to capture

Add Wireshark to your path

- To make your Wireshark applications accessible from any directory, simply add Wireshark to your Windows path



Tshark command syntax – Part 1

Usage: tshark [options] ...

Capture interface:

- i <interface> name or idx of interface (def: first non-loopback)
- f <capture filter> packet filter in libpcap filter syntax
- s <snaplen> packet snapshot length (def: 65535)
- p don't capture in promiscuous mode
- B <buffer size> size of kernel buffer (def: 1MB)
- y <link type> link layer type (def: first appropriate)
- D print list of interfaces and exit
- L print list of link-layer types of iface and exit

Capture stop conditions:

- c <packet count> stop after n packets (def: infinite)
- a <autostop cond.> ... duration:NUM - stop after NUM seconds
filesize:NUM - stop this file after NUM KB
files:NUM - stop after NUM files

Capture output:

- b <ringbuffer opt.> ... duration:NUM - switch to next file after NUM secs
filesize:NUM - switch to next file after NUM KB
files:NUM - ringbuffer: replace after NUM files

Input file:

- r <infile> set the filename to read from (no pipes or stdin!)

Processing:

- R <read filter> packet filter in Wireshark display filter syntax
- n disable all name resolutions (def: all enabled)
- N <name resolve flags> enable specific name resolution(s): "mmtC"
- d <layer_type>==<selector>,<decode_as_protocol> ...
"Decode As", see the man page for details
Example: tcp.port==8888,http



Tshark command syntax – Part 2

Output:

- w <outfile|-> set the output filename (or '-' for stdout)
- F <output file type> set the output file type, default is libpcap an empty "-F" option will list the file types
- V add output of packet tree (Packet Details)
- S display packets even when writing to a file
- x add output of hex and ASCII dump (Packet Bytes)
- T pdml|ps|psml|text|fields
format of text output (def: text)
- e <field> field to print if -Tfields selected (e.g. tcp.port);
this option can be repeated to print multiple fields
- E<fieldsoption>=<value> set options for output when -Tfields selected:
 - header=y|n switch headers on and off
 - separator=/t|/s|<char> select tab, space, printable character as separator
 - quote=d|s|n select double, single, no quotes for values
- t ad|a|r|d|dd|e output format of time stamps (def: r: rel. to first)
- l flush output after each packet
- q be more quiet on stdout (e.g. when using statistics)
- X <key>:<value> eXtension options, see the man page for details
- z <statistics> various statistics, see the man page for details

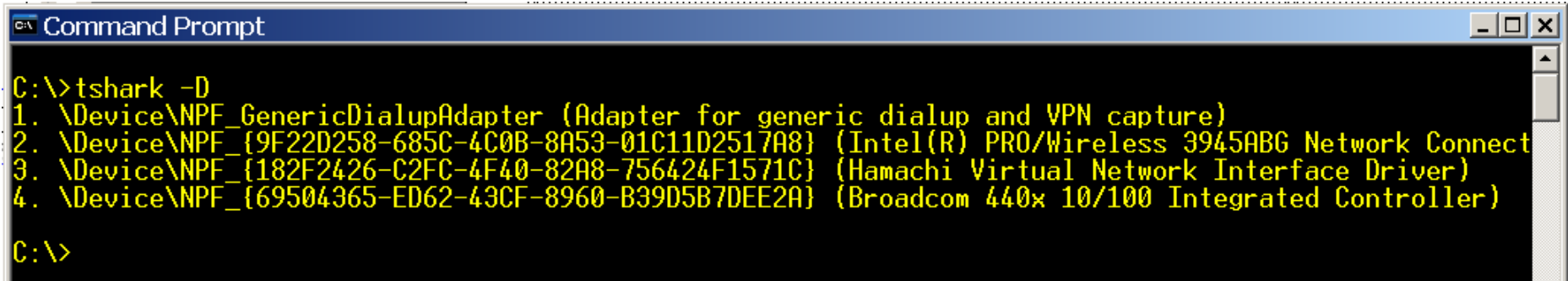
Miscellaneous:

- h display this help and exit
- v display version info and exit
- o <name>:<value> ... override preference setting



Determine which interface index maps to which NIC

- From the command prompt type;
 - ✓ Tshark -D

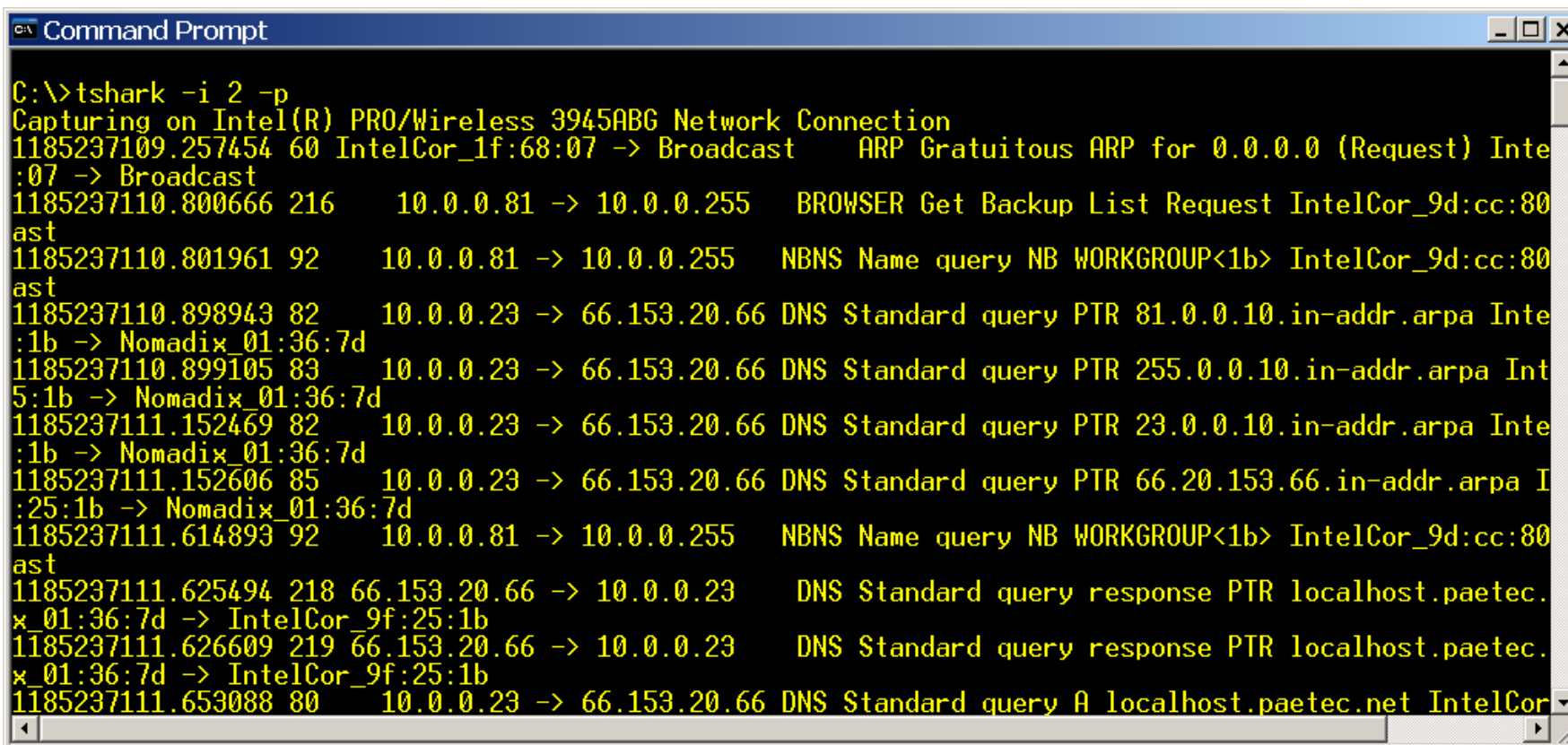


```
C:\>tshark -D
1. \Device\NPF_{Generic}Adapter (Adapter for generic dialup and VPN capture)
2. \Device\NPF_{9F22D258-685C-4C0B-8A53-01C11D2517A8} (Intel(R) PRO/Wireless 3945ABG Network Connect
3. \Device\NPF_{182F2426-C2FC-4F40-82A8-756424F1571C} (Hamachi Virtual Network Interface Driver)
4. \Device\NPF_{69504365-ED62-43CF-8960-B39D5B7DEE2A} (Broadcom 440x 10/100 Integrated Controller)
C:\>
```

- In this example I'll use my wireless card or index number 2

Test

- Since I will use my wireless I do not want to use promiscuous mode
- From the command prompt I will type the following, and should see some output
 - ✓ Tshark -i 2 -p



```
C:\>tshark -i 2 -p
Capturing on Intel(R) PRO/Wireless 3945ABG Network Connection
1185237109.257454 60 IntelCor_1f:68:07 -> Broadcast ARP Gratuitous ARP for 0.0.0.0 (Request) IntelCor_1f:68:07 -> Broadcast
1185237110.800666 216 10.0.0.81 -> 10.0.0.255 BROWSER Get Backup List Request IntelCor_9d:cc:80:ast
1185237110.801961 92 10.0.0.81 -> 10.0.0.255 NBNS Name query NB WORKGROUP<1b> IntelCor_9d:cc:80:ast
1185237110.898943 82 10.0.0.23 -> 66.153.20.66 DNS Standard query PTR 81.0.0.10.in-addr.arpa IntelCor_01:36:7d
1185237110.899105 83 10.0.0.23 -> 66.153.20.66 DNS Standard query PTR 255.0.0.10.in-addr.arpa IntelCor_05:1b -> Nomadix_01:36:7d
1185237111.152469 82 10.0.0.23 -> 66.153.20.66 DNS Standard query PTR 23.0.0.10.in-addr.arpa IntelCor_01:36:7d
1185237111.152606 85 10.0.0.23 -> 66.153.20.66 DNS Standard query PTR 66.20.153.66.in-addr.arpa IntelCor_025:1b -> Nomadix_01:36:7d
1185237111.614893 92 10.0.0.81 -> 10.0.0.255 NBNS Name query NB WORKGROUP<1b> IntelCor_9d:cc:80:ast
1185237111.625494 218 66.153.20.66 -> 10.0.0.23 DNS Standard query response PTR localhost.paetec.net IntelCor_01:36:7d -> IntelCor_9f:25:1b
1185237111.626609 219 66.153.20.66 -> 10.0.0.23 DNS Standard query response PTR localhost.paetec.net IntelCor_01:36:7d -> IntelCor_9f:25:1b
1185237111.653088 80 10.0.0.23 -> 66.153.20.66 DNS Standard query A localhost.paetec.net IntelCor_01:36:7d -> IntelCor_9f:25:1b
```

Command to capture 1 MB of data

- Now that I know everything works, I want to do the following;
 - ✓ -i 2 ;captures from my wireless
 - ✓ -p ;captures in non promiscuous mode
 - ✓ -a filesize:1000 ;captures 1 MB
 - ✓ -w 1MBcapture.pcap ; names the file
- As you capture, you will see the packet counter increase

```
C:\>tshark -i 2 -p -a filesize:1000 -w 1MBcapture.pcap
Capturing on Intel(R) PRO/Wireless 3945ABG Network Connection
47
```

- In this capture, I checked the file size to make sure it is 1 MB

```
C:\>tshark -i 2 -p -a filesize:1000 -w 1MBcapture.pcap
Capturing on Intel(R) PRO/Wireless 3945ABG Network Connection
1747

C:\>dir 1MBcapture.pcap
Volume in drive C has no label.
Volume Serial Number is A86A-A6B5

Directory of C:\

07/23/2007  08:46 PM                1,024,383 1MBcapture.pcap
             1 File(s)                1,024,383 bytes
             0 Dir(s)  44,738,777,088 bytes free
```

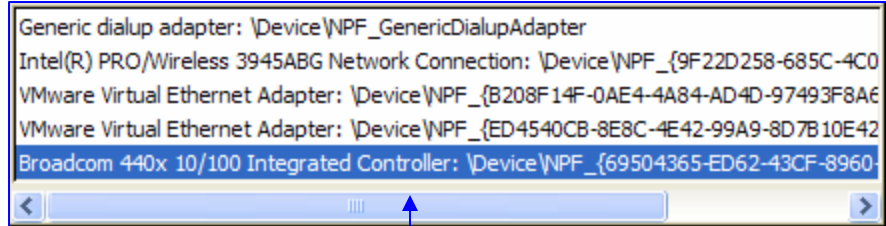
Command to Capture with a ip filter

- Tshark -i 4 -p host 10.44.10.1
 - ✓ -i 4 -p is specifically for my wireless interface
 - ✓ host 10.44.10.1 is the target of my capture filter

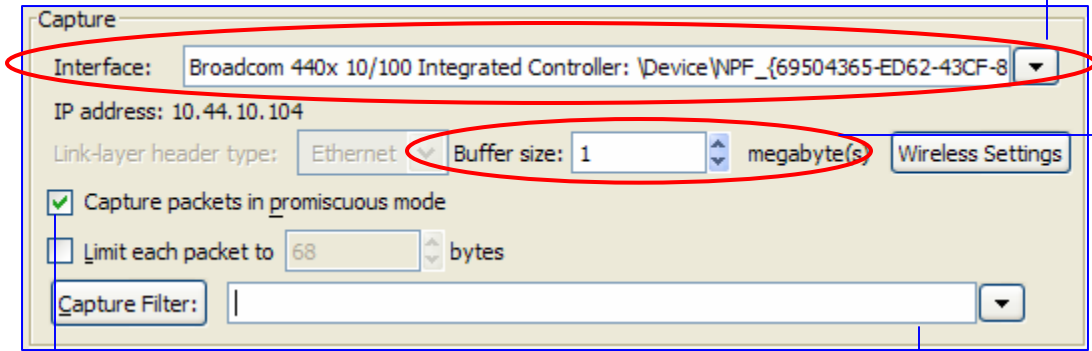
Command to Capture with a 100 Byte packet slice

- Tshark -i 4 -p host 10.44.10.1 -s 100
 - ✓ -i 4 -p is specifically for my wireless interface
 - ✓ host 10.44.10.1 is the target of my capture filter
 - ✓ Only capture the first 100 Bytes

Capture Options – Capture Frame



Used to show you which adapters are available for capturing.



8MB is fine

Check this for LAN captures, or you will only get frames to and from your adapter

- Common Capture Filters
- ether host *mac_address*
 - ip host *ip_address*
 - port *tcp_udp_port_no*



Filters are contained in this file
C:\Documents and \Application Data\Wireshark\filters
** Remember to leave the last line in this file blank..

Capture Filter Reference



Command	Description
ether host <i>MAC address</i>	Capture all packets to and from a <i>MAC address</i>
<i>IP Filters</i>	
host <i>ip address</i>	Capture all packets to and from an <i>ip address</i>
src host <i>ip address</i>	Capture all packets from an <i>ip address</i>
dst host <i>ip address</i>	Capture all packets to an <i>ip address</i>
<i>TCP/UDP Filters</i>	
port <i>port</i>	Capture all packets to and from a port number
src port <i>port</i>	Capture all packets from a port number
dst port <i>port</i>	Capture all packets to a port number
<i>IP Network Filters</i>	
net <i>net</i>	Capture all packets to and from a <i>net</i>
src net <i>net</i>	Capture all packets from a <i>net</i>
dst net <i>net</i>	Capture all packets to a <i>net</i>

Capture Filter Examples

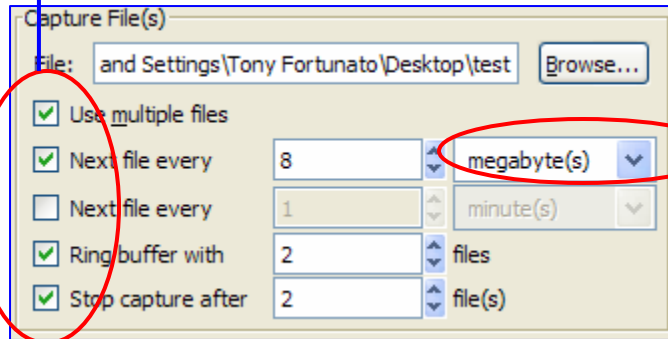


- Capture only DNS frames
 - ✓ port 53
- Capture HTTP and DNS frames
 - ✓ port 80 or port 53
- Capture all IP traffic
 - ✓ ip

Capture Options – Capture File(s) Frame



Creates files with the following syntax;
➤ *Filename_00001_yearmmddhhmmss*
for example *test_00001_20061102150628*
Capture Files will be in a **libpcap** format



Stay with size limits since you do not know how much data will be flowing at any given time.

Start Capture

Stop Capture

In this example, Wireshark will create 2-8MB files.



8MB

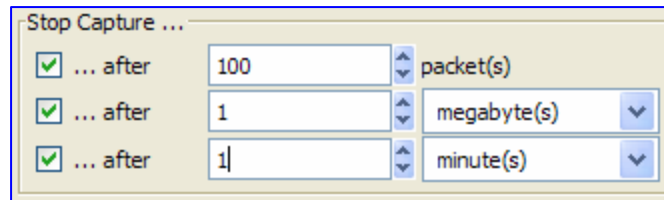


8MB



Capture Options – Stop Capture Frame

- This frame allows you to control when Wireshark will stop capturing.
- This will not save to a file.
- If multiple options are checked, the first condition it reaches, will stop the analyzer.



Filters are contained in this file
C:\Documents and \Application Data\Wireshark\filters
** If you choose to create your own cfilters file, remember to
leave the last line in this file blank.

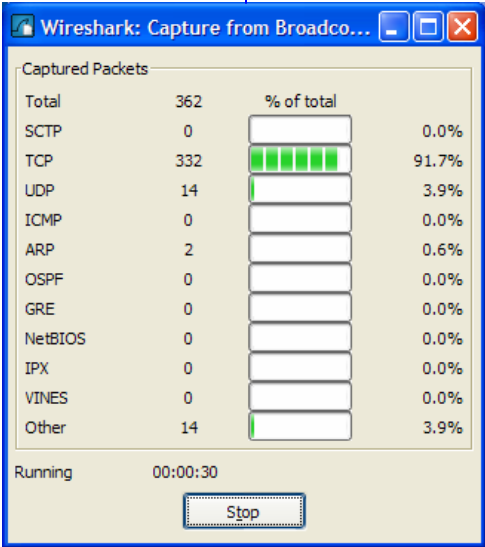
Display Options and Name Resolution

```
296 1.198039 04.007024 10.44.10.1 Spanning-tree-(for STP Conf. Root = 32768/00:0f:66:11:ea:10 Cost = 0
297 2.000208 66.007232 10.44.10.1 Spanning-tree-(for STP Conf. Root = 32768/00:0f:66:11:ea:16 Cost = 0
Broadcom 440x 10/100 Integrated Controller: <live capture in progress> File: C:\DOCUME~1\TONYF... |P: 297D: 297M: 0
```

- Helpful when troubleshooting real-time
- Only helpful with a Capture Filter or low-traffic network
- Helpful when the first 2 Display Options are not checked

Display Options

- Update list of packets in real time
- Automatic scrolling in live capture
- Hide capture info dialog



Capture Options – Name Resolution Frame

No. ↓	delta	Source	Destination	Protocol
1	0.00	00:0f:66:11:ea:17	01:80:c2:00:00:00	STP
2	2.00	00:0f:66:11:ea:17	01:80:c2:00:00:00	STP
3	2.00	00:0f:66:11:ea:17	01:80:c2:00:00:00	STP

No. ↓	delta	Source	Destination	Protocol
1	0.00	Cisco-Li_11:ea:17	spanning-tree-(for-bridges)_	STP
2	2.00	Cisco-Li_11:ea:17	spanning-tree-(for-bridges)_	STP
3	2.00	Cisco-Li_11:ea:17	spanning-tree-(for-bridges)_	STP

```
Info
3326 > http [SYN]
http > 3326 [SYN,
3326 > http [ACK]
```

```
Info
standard query re
3332 > 80 [SYN] S
80 > 3332 [SYN, A
3332 > 80 [ACK] S
```

Name Resolution

- Enable MAC name resolution
- Enable network name resolution
- Enable transport name resolution

Wireshark performs a reverse DNS lookup

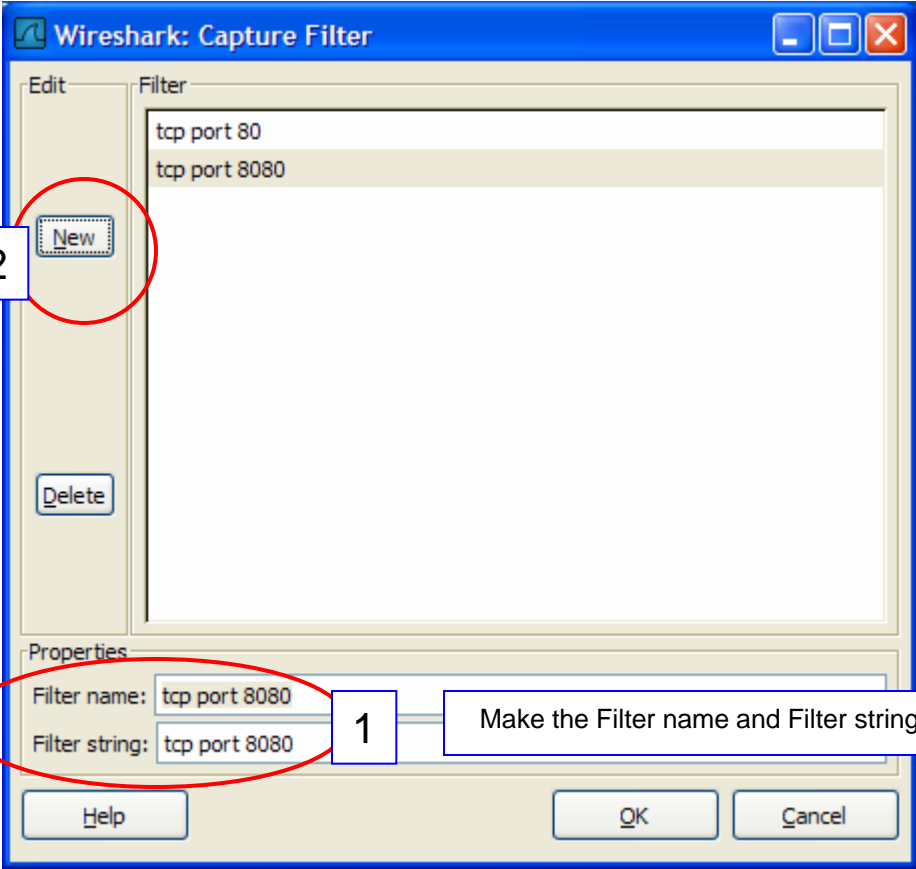
No. ↓	delta	Source	Destination
49	0.00	office.office	Spanning-tree-(for-bridg
50	0.80	new-host-2.office	www.thetechfirm.com
51	0.00	new-host-2.office	office.office
52	0.00	new-host-2.office	office.office
53	0.00	office.office	new-host-2.office

No. ↓	delta	Source	Destination
5	0.10	82.165.199.175	10.44.10.101
6	0.80	10.44.10.101	82.165.199.175
7	0.40	82.165.199.175	10.44.10.101




Capture – Capture Filters

- This screen allows you to Add or Delete Capture filters



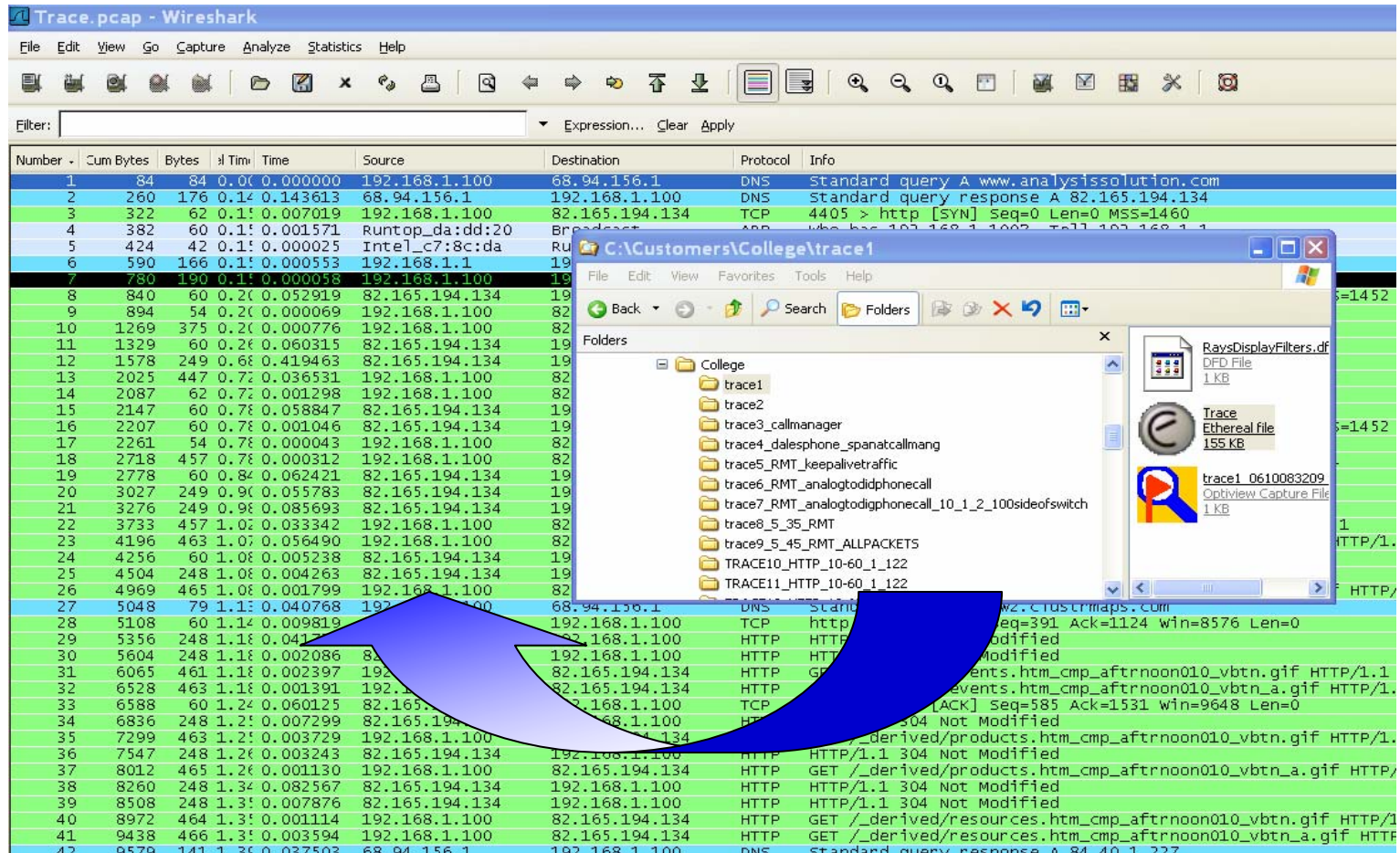
The image shows the 'Wireshark: Capture Filter' dialog box. It has a 'Filter' list containing 'tcp port 80' and 'tcp port 8080'. In the 'Edit' section, the 'New' button is circled in red with a box containing the number '2'. In the 'Properties' section, the 'Filter name' and 'Filter string' fields both contain 'tcp port 8080' and are circled in red with a box containing the number '1'. A callout box points to these fields with the text: 'Make the Filter name and Filter string the same to avoid confusion'. At the bottom, there are 'Help', 'OK', and 'Cancel' buttons. Below the dialog box, a text box contains the following information:

Filters are contained in this file
C:\Documents and \Application Data\Wireshark\filters
** Remember to leave the last line in this file blank..



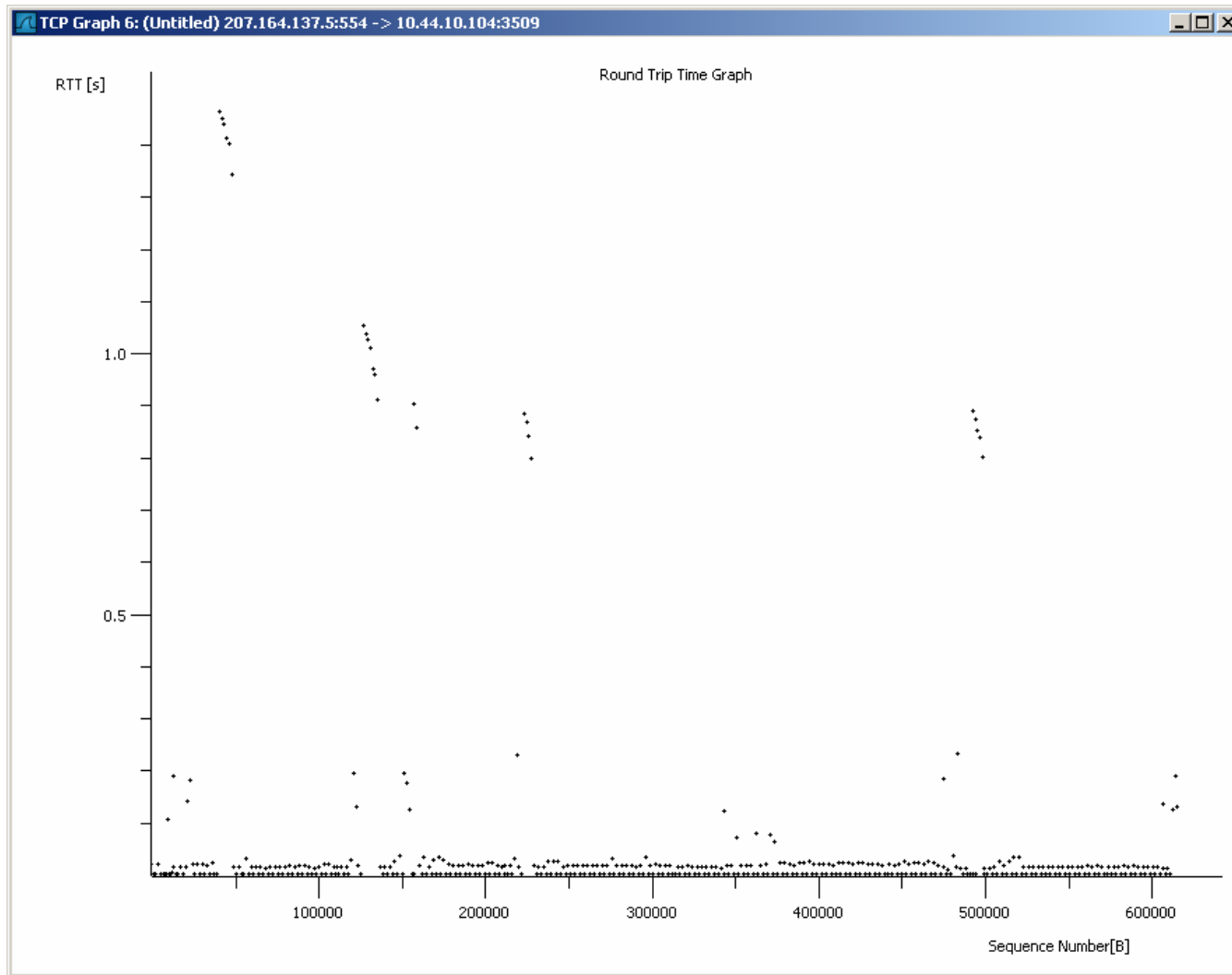
Neat Feature – ‘Drag and Drop’

- You can now drag and drop a file from Windows Explorer directly into Wireshark.



TCP Stream Graph - RTT

- Displays a graph of the round trip time (RTT) vs. the sequence number.



TCP Stream Graph - Throughput

- Displays a graph of throughput vs. time.

