How To Capture from the Command Prompt with Wireshark

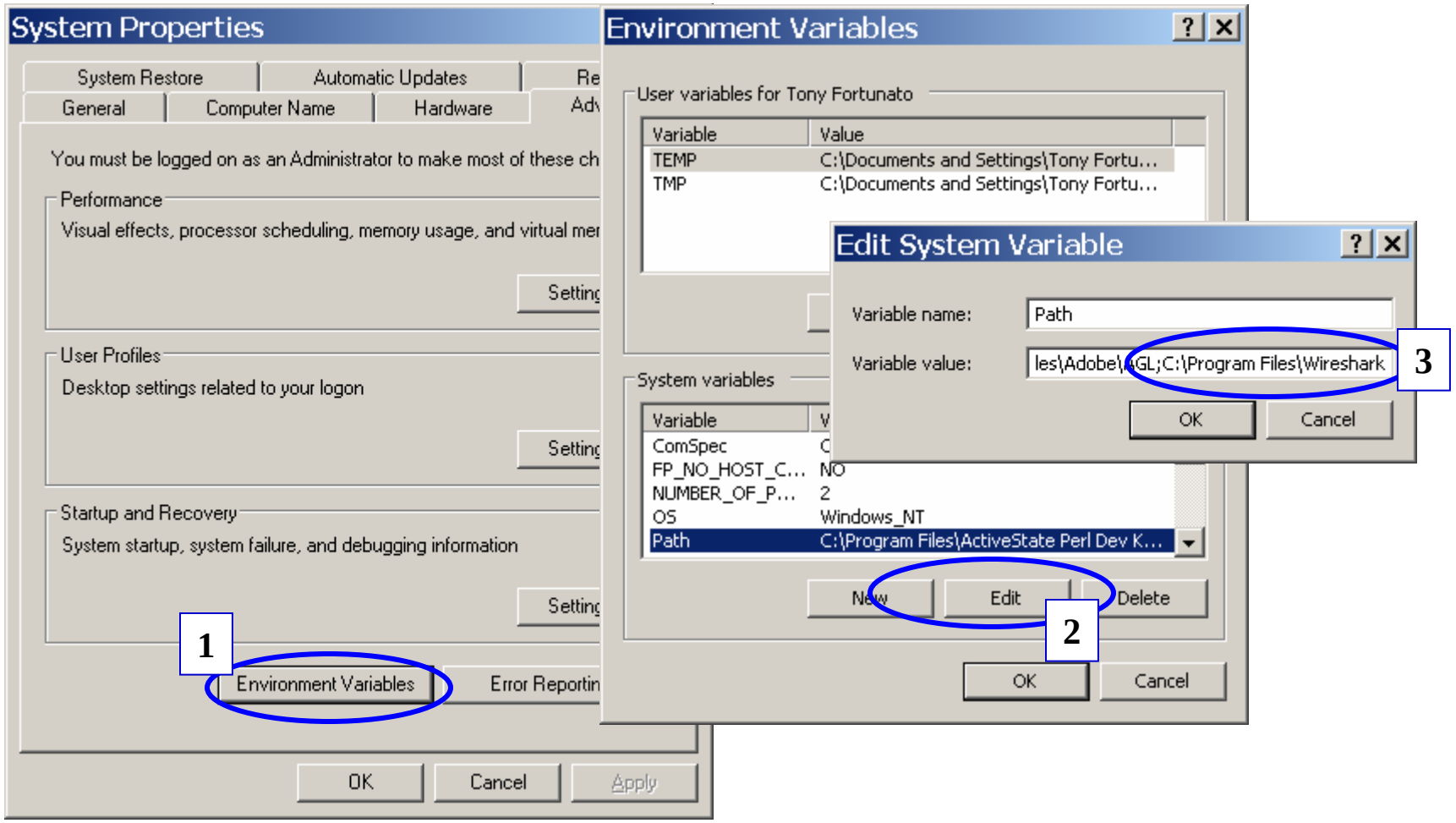
The Technology Firm

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): "mntC"
  -d <layer_type>==<selector>,<decode_as_protocol> ...
                           "Decode As", see the man page for details
                           Example: tcp.port==8888,http
```

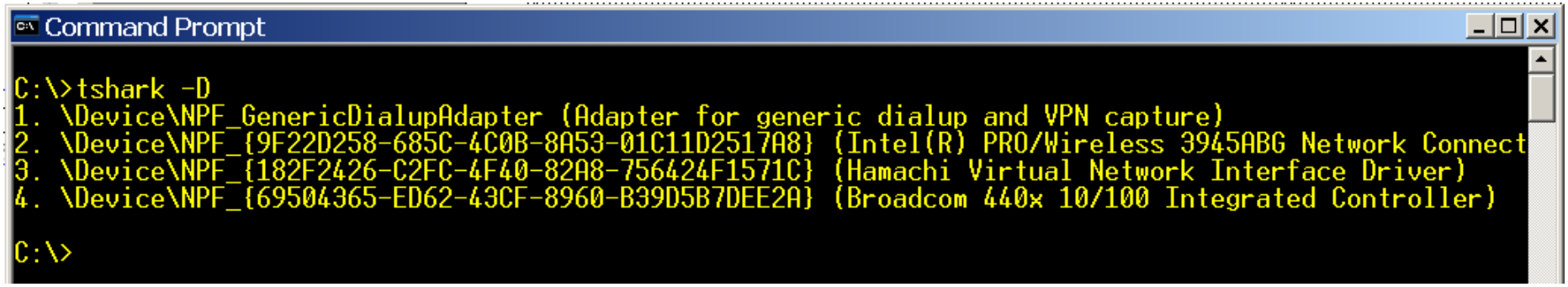
Tshark command syntax – Part 2

```
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

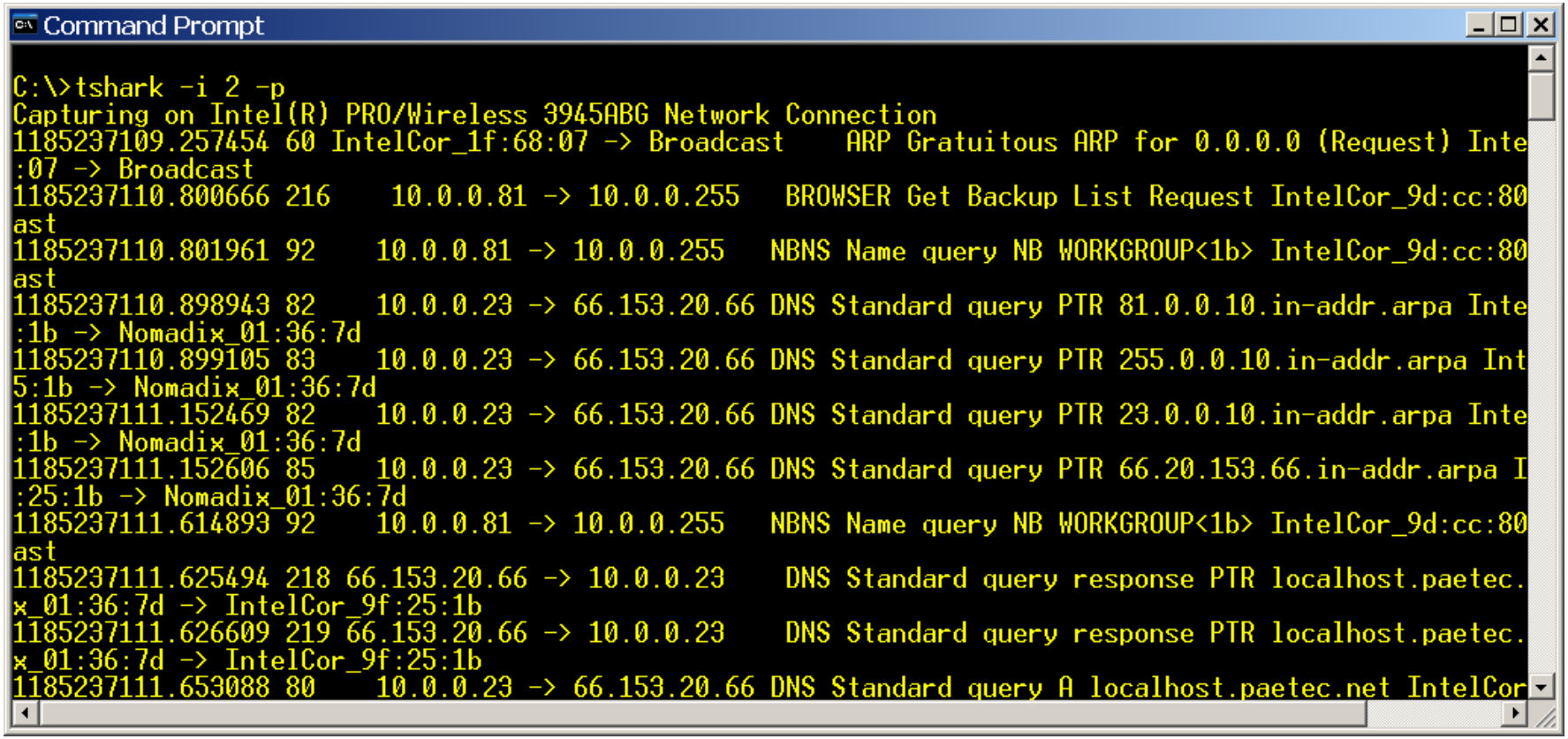
- From the command prompt type;
  - ✓ Tshark -D



- 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



Final command to capture

- 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
```