Windows XP Sniffer Documentation

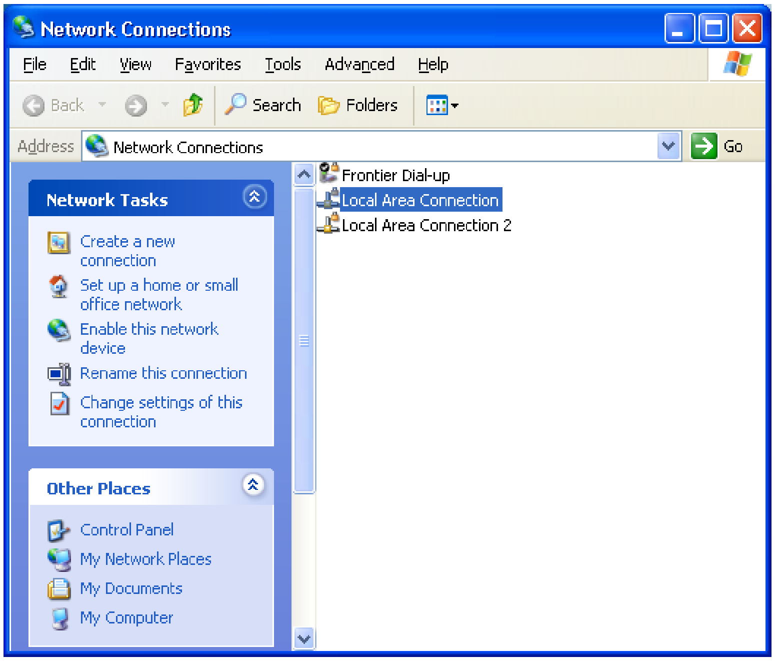
August 27, 2003

GV/WFL BOCES EduTech

Windows XP Sniffer Instructions
Activation

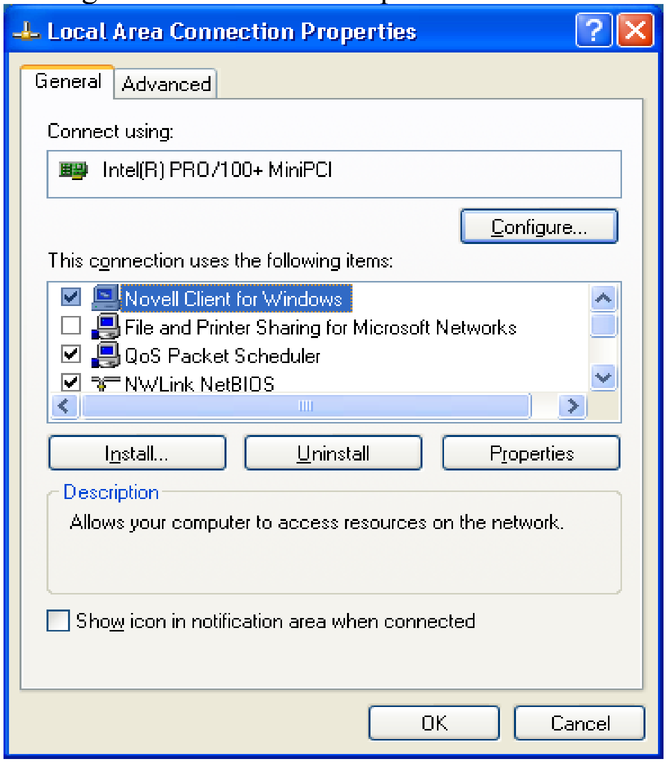
To turn on firewall logging, perform the following steps.

1. Right click on My Network Places and select Properties



2. Select Local Area Connection.

3. Right click and select Properties.



Connect using: Intel(R) PRO/100+ MiniPCI

This connection uses the following items:

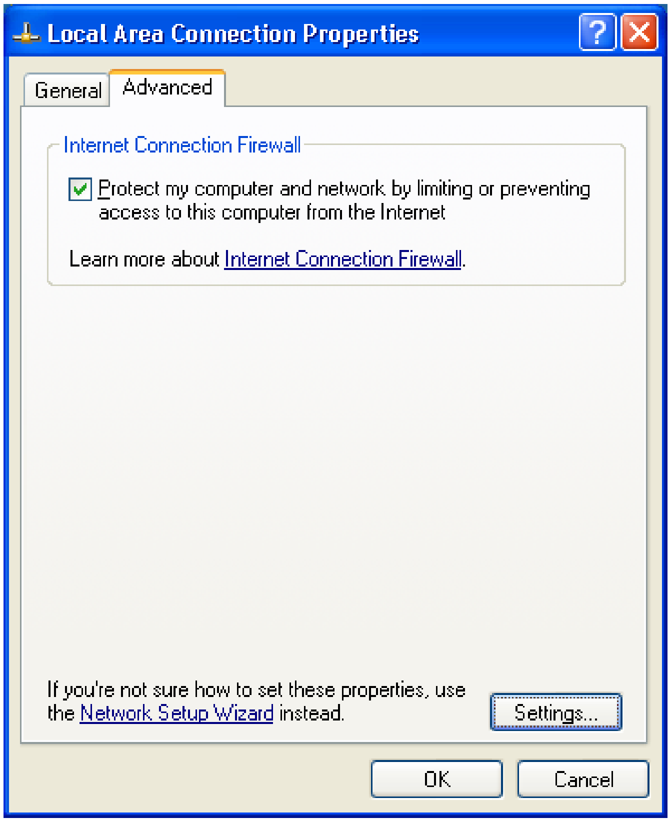
- ☑ Novell Client for Windows
- □ File and Printer Sharing for Microsoft Networks
- ☑ QoS Packet Scheduler
- ☑ NWLink NetBIOS

Description

Allows your computer to access resources on the network.

□ Show icon in notification area when connected

4. Select the Advanced Tab



Internet Connection Firewall

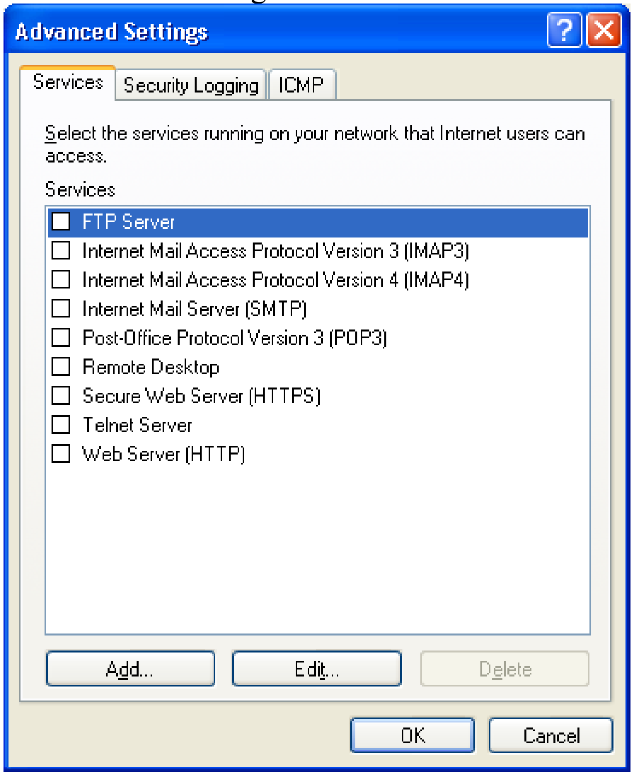
☑ Protect my computer and network by limiting or preventing access to this computer from the Internet

Learn more about Internet Connection Firewall.

If you're not sure how to set these properties, use the Network Setup Wizard instead.

5. Check the Protect my computer and network by limiting or preventing access to this computer from the Internet

6. Click the Settings button.

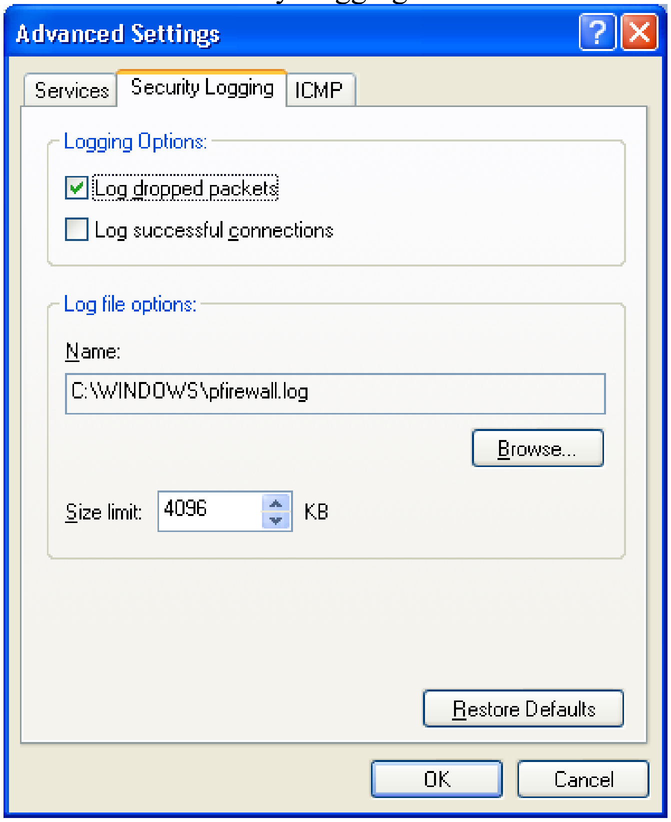


Select the services running on your network that Internet users can access.

Services

- □ FTP Server
- □ Internet Mail Access Protocol Version 3 (IMAP3)
- □ Internet Mail Access Protocol Version 4 (IMAP4)
- □ Internet Mail Server (SMTP)
- □ Post-Office Protocol Version 3 (POP3)
- □ Remote Desktop
- □ Secure Web Server (HTTPS)
- □ Telnet Server
- □ Web Server (HTTP)

7. Select the Security Logging Tab.



☑ Log dropped packets

□ Log successful connections

Name:

C:\WINDOWS\pfirewall.log

Size limit: 4096 KB

8. Under Logging Options, check the Log dropped packets option.

9. Make a note of the log file name (pfirewall.log) and path for future use.

10. Click Okay as needed to close the open windows.

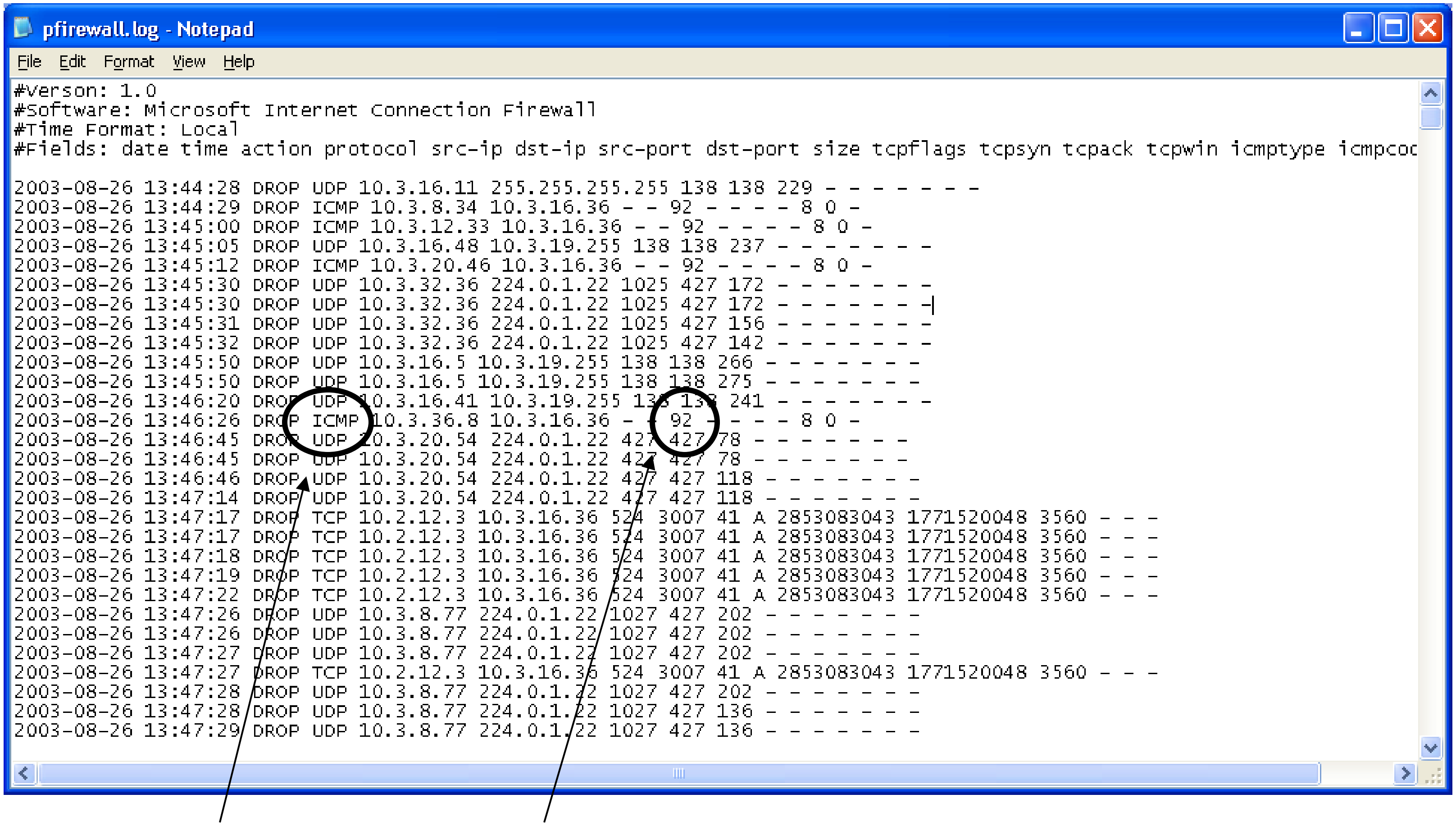
A log file will be created as a Microsoft Notepad file. To view the log file, follow the path that was specified in step 7 above. Using the path specified as an example, you might do the following.

- Open My Computer
- Select the C drive
- Open the WINDOWS folder
- Find the pfirewall.log file and open it.

The log file will continue to grow indefinitely unless the monitoring is halted. After a sufficient amount of data has been logged, turn off the logging utility by reversing the settings established in Steps 1 through 8 above.

Reading the Log File

The log file will look like this in Microsoft Notepad.



```
#Verson: 1.0
#Software: Microsoft Internet Connection Firewall
#Time Format: Local
#Fields: date time action protocol src-ip dst-ip src-port dst-port size tcpflags tcpsyn tcpack tcpwin icmptype icmpcoc

2003-08-26 13:44:28 DROP UDP 10.3.16.11 255.255.255.255 138 138 229 - - - - - - - -
2003-08-26 13:44:29 DROP ICMP 10.3.8.34 10.3.16.36 - - 92 - - - - 8 0 -
2003-08-26 13:45:00 DROP ICMP 10.3.12.33 10.3.16.36 - - 92 - - - - 8 0 -
2003-08-26 13:45:05 DROP UDP 10.3.16.48 10.3.19.255 138 138 237 - - - - - - - -
2003-08-26 13:45:12 DROP ICMP 10.3.20.46 10.3.16.36 - - 92 - - - - 8 0 -
2003-08-26 13:45:30 DROP UDP 10.3.32.36 224.0.1.22 1025 427 172 - - - - - - - -
2003-08-26 13:45:30 DROP UDP 10.3.32.36 224.0.1.22 1025 427 172 - - - - - - - -
2003-08-26 13:45:31 DROP UDP 10.3.32.36 224.0.1.22 1025 427 156 - - - - - - - -
2003-08-26 13:45:32 DROP UDP 10.3.32.36 224.0.1.22 1025 427 142 - - - - - - - -
2003-08-26 13:45:50 DROP UDP 10.3.16.5 10.3.19.255 138 138 266 - - - - - - - -
2003-08-26 13:45:50 DROP UDP 10.3.16.5 10.3.19.255 138 138 275 - - - - - - - -
2003-08-26 13:46:20 DROP UDP 10.3.16.41 10.3.19.255 138 138 241 - - - - - - - -
2003-08-26 13:46:26 DROP ICMP 10.3.36.8 10.3.16.36 - - 92 - - - - 8 0 -
2003-08-26 13:46:45 DROP UDP 10.3.20.54 224.0.1.22 427 427 78 - - - - - - - -
2003-08-26 13:46:45 DROP UDP 10.3.20.54 224.0.1.22 427 427 78 - - - - - - - -
2003-08-26 13:46:46 DROP UDP 10.3.20.54 224.0.1.22 427 427 118 - - - - - - - -
2003-08-26 13:47:14 DROP UDP 10.3.20.54 224.0.1.22 427 427 118 - - - - - - - -
2003-08-26 13:47:17 DROP TCP 10.2.12.3 10.3.16.36 524 3007 41 A 2853083043 1771520048 3560 - - -
2003-08-26 13:47:17 DROP TCP 10.2.12.3 10.3.16.36 524 3007 41 A 2853083043 1771520048 3560 - - -
2003-08-26 13:47:18 DROP TCP 10.2.12.3 10.3.16.36 524 3007 41 A 2853083043 1771520048 3560 - - -
2003-08-26 13:47:19 DROP TCP 10.2.12.3 10.3.16.36 524 3007 41 A 2853083043 1771520048 3560 - - -
2003-08-26 13:47:22 DROP TCP 10.2.12.3 10.3.16.36 524 3007 41 A 2853083043 1771520048 3560 - - -
2003-08-26 13:47:26 DROP UDP 10.3.8.77 224.0.1.22 1027 427 202 - - - - - - - -
2003-08-26 13:47:26 DROP UDP 10.3.8.77 224.0.1.22 1027 427 202 - - - - - - - -
2003-08-26 13:47:27 DROP UDP 10.3.8.77 224.0.1.22 1027 427 202 - - - - - - - -
2003-08-26 13:47:27 DROP TCP 10.2.12.3 10.3.16.36 524 3007 41 A 2853083043 1771520048 3560 - - -
2003-08-26 13:47:28 DROP UDP 10.3.8.77 224.0.1.22 1027 427 202 - - - - - - - -
2003-08-26 13:47:28 DROP UDP 10.3.8.77 224.0.1.22 1027 427 136 - - - - - - - -
2003-08-26 13:47:29 DROP UDP 10.3.8.77 224.0.1.22 1027 427 136 - - - - - - - -
```

Search for ICMP Protocol codes and a Size of 92. These are the field parameters that will indicate the possibility of the welchia virus running on a computer with the indicated src-ip.

Bringing the Data into Excel and Sorting

If the log file is large, you may wish to move the data into Microsoft Excel to use advanced sorting or filtering capabilities.

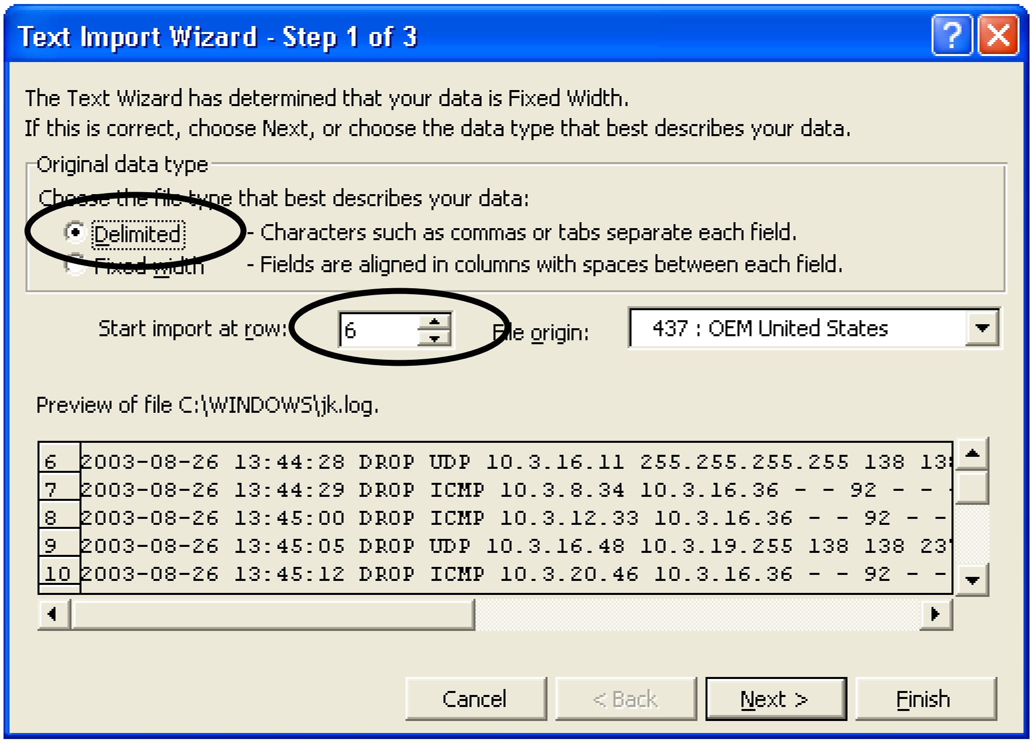
1. Open a blank spreadsheet.

2. Go to File and then select Open

3. At the bottom of the Open window, change the Files of Type dropdown window to read All Files (*.*)

4. Either enter the path and file name of the log file or use the browse features to find and select the file.

5. When Excel opens the file, it will recognize that it is not an Excel formatted file and give you the option of delineating the text with the Text Import Wizard.



Text Import Wizard - Step 1 of 3

The Text Wizard has determined that your data is Fixed Width.
If this is correct, choose Next, or choose the data type that best describes your data.

Original data type

Choose the file type that best describes your data:

● Delimited - Characters such as commas or tabs separate each field.
○ Fixed width - Fields are aligned in columns with spaces between each field.

Start import at row: 6

File origin: 437 : OEM United States

Preview of file C:\WINDOWS\jk.log.

```
6  2003-08-26 13:44:28 DROP UDP 10.3.16.11 255.255.255.255 138 13
7  2003-08-26 13:44:29 DROP ICMP 10.3.8.34 10.3.16.36 - - 92 - -
8  2003-08-26 13:45:00 DROP ICMP 10.3.12.33 10.3.16.36 - - 92 - -
9  2003-08-26 13:45:05 DROP UDP 10.3.16.48 10.3.19.255 138 138 23
10 2003-08-26 13:45:12 DROP ICMP 10.3.20.46 10.3.16.36 - - 92 - -
```

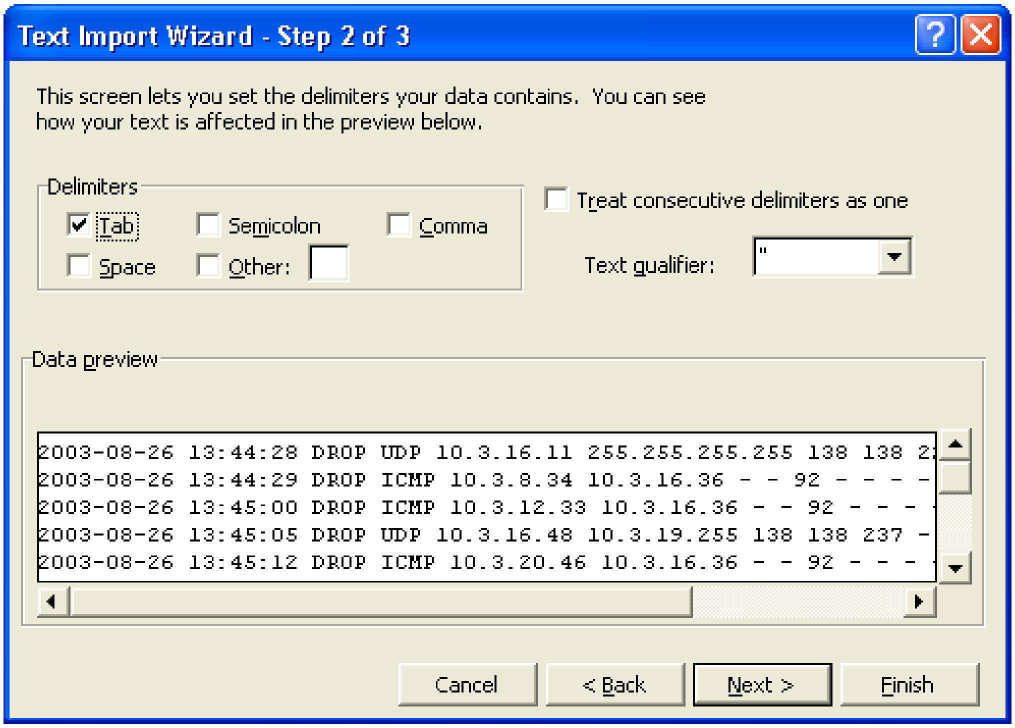
6. Choose the Delimited file type and Start the import at row 6 to avoid the header information.

   Note: If you want to retain the column headings, start the import at row 4 but remember that all names will be shifted to the right by one column because of the “#Fields:” in that line of text.

7. Click on Next

8. Now Change the Delimiters selection from Tab to Space

From This



Text Import Wizard - Step 2 of 3

This screen lets you set the delimiters your data contains. You can see how your text is affected in the preview below.

Delimiters

☑ Tab ☐ Semicolon ☐ Comma

☐ Space ☐ Other: □

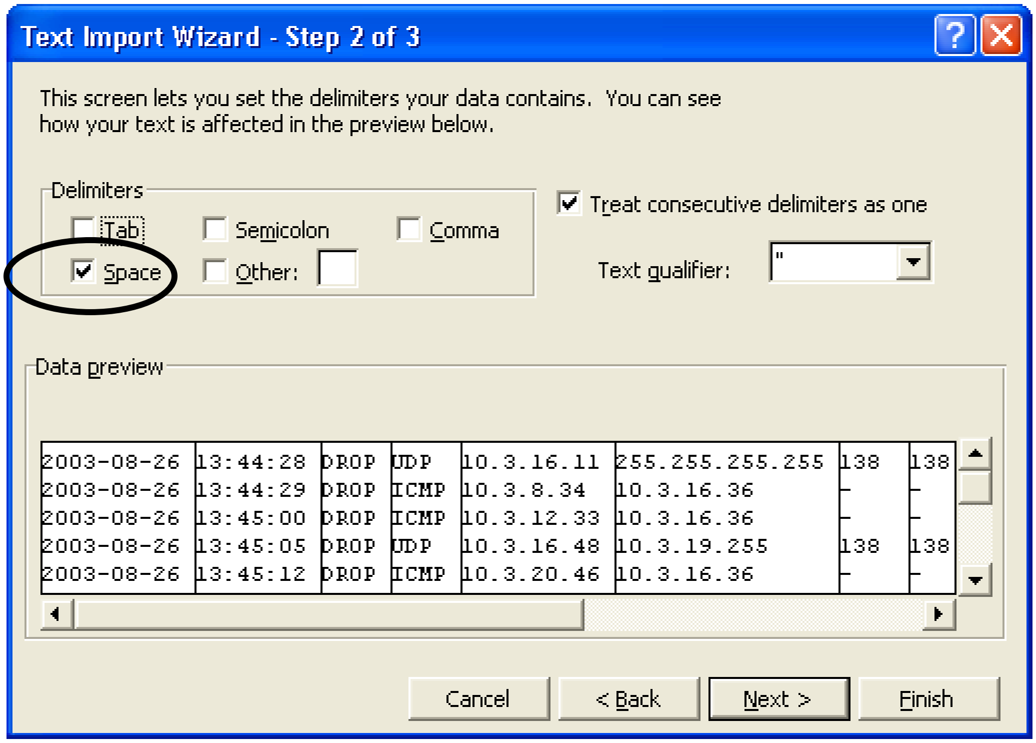
☐ Treat consecutive delimiters as one

Text qualifier: "

Data preview

```
2003-08-26 13:44:28 DROP UDP 10.3.16.11 255.255.255.255 138 138 2
2003-08-26 13:44:29 DROP ICMP 10.3.8.34 10.3.16.36 - - 92 - - - -
2003-08-26 13:45:00 DROP ICMP 10.3.12.33 10.3.16.36 - - 92 - - -
2003-08-26 13:45:05 DROP UDP 10.3.16.48 10.3.19.255 138 138 237 -
2003-08-26 13:45:12 DROP ICMP 10.3.20.46 10.3.16.36 - - 92 - - -
```

To This



Text Import Wizard - Step 2 of 3

This screen lets you set the delimiters your data contains. You can see how your text is affected in the preview below.

Delimiters

☐ Tab ☐ Semicolon ☐ Comma

☑ Space ☐ Other: □

☑ Treat consecutive delimiters as one

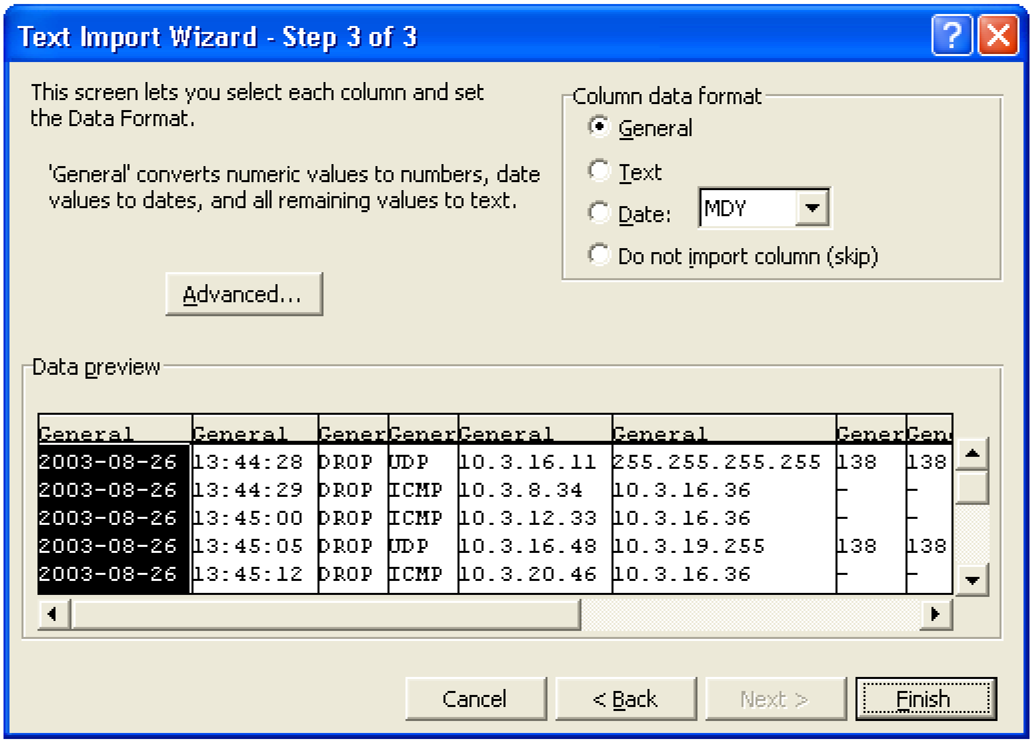
Text qualifier: "

Data preview

```
2003-08-26 13:44:28 DROP UDP  10.3.16.11 255.255.255.255 138 138
2003-08-26 13:44:29 DROP ICMP 10.3.8.34  10.3.16.36      -   -
2003-08-26 13:45:00 DROP ICMP 10.3.12.33 10.3.16.36      -   -
2003-08-26 13:45:05 DROP UDP  10.3.16.48 10.3.19.255     138 138
2003-08-26 13:45:12 DROP ICMP 10.3.20.46 10.3.16.36      -   -
```

9. Now click on Next again.

10. No need to change data formats as provided by step 3 of the Wizard. Just click Finish.



Text Import Wizard - Step 3 of 3

This screen lets you select each column and set the Data Format.

'General' converts numeric values to numbers, date values to dates, and all remaining values to text.

Column data format

● General

○ Text

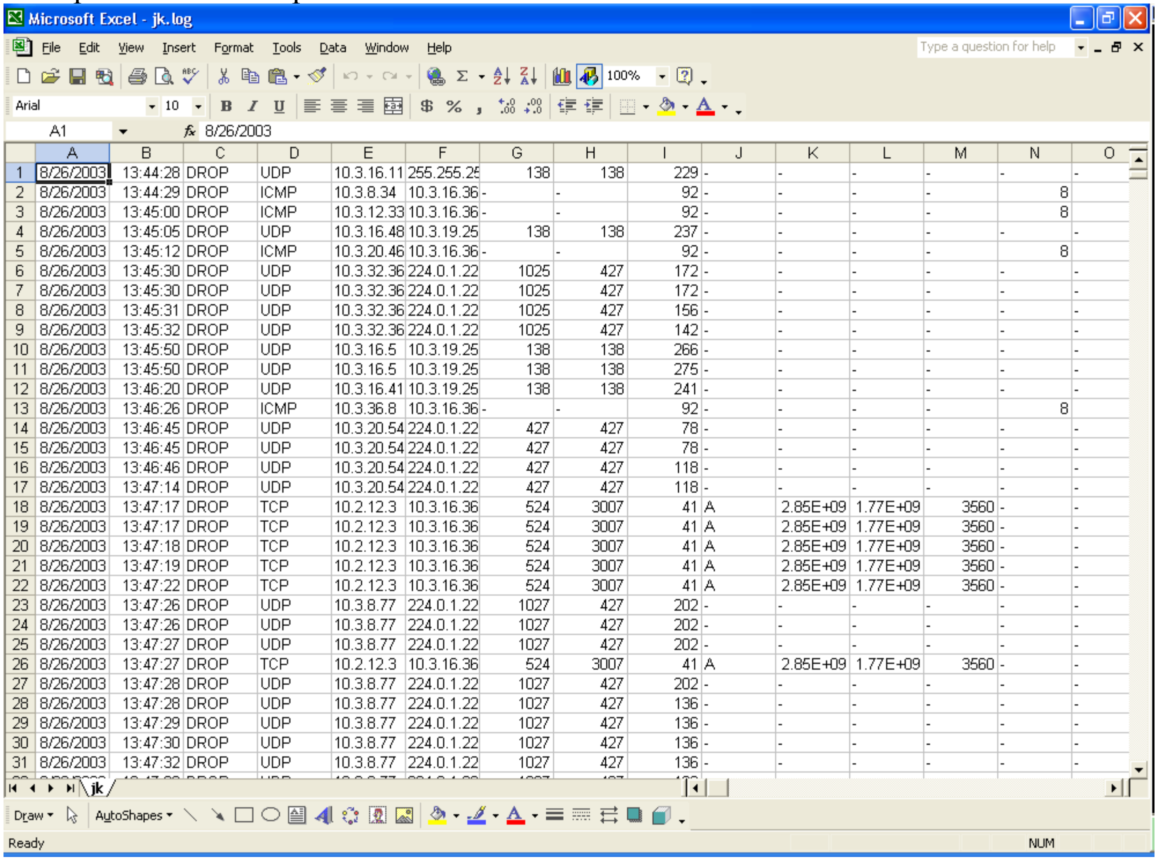
○ Date: MDY

○ Do not import column (skip)

Data preview

General	General	Gener	Gener	General	General	Gener	Gen
2003-08-26	13:44:28	DROP	UDP	10.3.16.11	255.255.255.255	138	138
2003-08-26	13:44:29	DROP	ICMP	10.3.8.34	10.3.16.36	-	-
2003-08-26	13:45:00	DROP	ICMP	10.3.12.33	10.3.16.36	-	-
2003-08-26	13:45:05	DROP	UDP	10.3.16.48	10.3.19.255	138	138
2003-08-26	13:45:12	DROP	ICMP	10.3.20.46	10.3.16.36	-	-

The spreadsheet will open as shown.



Microsoft Excel - jk.log

A1 fx 8/26/2003

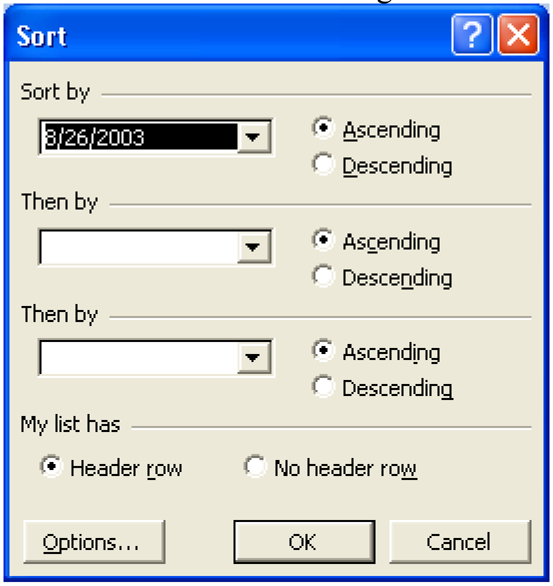
	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O
1	8/26/2003	13:44:28	DROP	UDP	10.3.16.11	255.255.25	138	138	229	-	-	-	-	-	-
2	8/26/2003	13:44:29	DROP	ICMP	10.3.8.34	10.3.16.36	-	-	92	-	-	-	-	8	
3	8/26/2003	13:45:00	DROP	ICMP	10.3.12.33	10.3.16.36	-	-	92	-	-	-	-	8	
4	8/26/2003	13:45:05	DROP	UDP	10.3.16.48	10.3.19.25	138	138	237	-	-	-	-	-	-
5	8/26/2003	13:45:12	DROP	ICMP	10.3.20.46	10.3.16.36	-	-	92	-	-	-	-	8	
6	8/26/2003	13:45:30	DROP	UDP	10.3.32.36	224.0.1.22	1025	427	172	-	-	-	-	-	-
7	8/26/2003	13:45:30	DROP	UDP	10.3.32.36	224.0.1.22	1025	427	172	-	-	-	-	-	-
8	8/26/2003	13:45:31	DROP	UDP	10.3.32.36	224.0.1.22	1025	427	156	-	-	-	-	-	-
9	8/26/2003	13:45:32	DROP	UDP	10.3.32.36	224.0.1.22	1025	427	142	-	-	-	-	-	-
10	8/26/2003	13:45:50	DROP	UDP	10.3.16.5	10.3.19.25	138	138	266	-	-	-	-	-	-
11	8/26/2003	13:45:50	DROP	UDP	10.3.16.5	10.3.19.25	138	138	275	-	-	-	-	-	-
12	8/26/2003	13:46:20	DROP	UDP	10.3.16.41	10.3.19.25	138	138	241	-	-	-	-	-	-
13	8/26/2003	13:46:26	DROP	ICMP	10.3.36.8	10.3.16.36	-	-	92	-	-	-	-	8	
14	8/26/2003	13:46:45	DROP	UDP	10.3.20.54	224.0.1.22	427	427	78	-	-	-	-	-	-
15	8/26/2003	13:46:45	DROP	UDP	10.3.20.54	224.0.1.22	427	427	78	-	-	-	-	-	-
16	8/26/2003	13:46:46	DROP	UDP	10.3.20.54	224.0.1.22	427	427	118	-	-	-	-	-	-
17	8/26/2003	13:47:14	DROP	UDP	10.3.20.54	224.0.1.22	427	427	118	-	-	-	-	-	-
18	8/26/2003	13:47:17	DROP	TCP	10.2.12.3	10.3.16.36	524	3007	41	A	2.85E+09	1.77E+09	3560	-	-
19	8/26/2003	13:47:17	DROP	TCP	10.2.12.3	10.3.16.36	524	3007	41	A	2.85E+09	1.77E+09	3560	-	-
20	8/26/2003	13:47:18	DROP	TCP	10.2.12.3	10.3.16.36	524	3007	41	A	2.85E+09	1.77E+09	3560	-	-
21	8/26/2003	13:47:19	DROP	TCP	10.2.12.3	10.3.16.36	524	3007	41	A	2.85E+09	1.77E+09	3560	-	-
22	8/26/2003	13:47:22	DROP	TCP	10.2.12.3	10.3.16.36	524	3007	41	A	2.85E+09	1.77E+09	3560	-	-
23	8/26/2003	13:47:26	DROP	UDP	10.3.8.77	224.0.1.22	1027	427	202	-	-	-	-	-	-
24	8/26/2003	13:47:26	DROP	UDP	10.3.8.77	224.0.1.22	1027	427	202	-	-	-	-	-	-
25	8/26/2003	13:47:27	DROP	UDP	10.3.8.77	224.0.1.22	1027	427	202	-	-	-	-	-	-
26	8/26/2003	13:47:27	DROP	TCP	10.2.12.3	10.3.16.36	524	3007	41	A	2.85E+09	1.77E+09	3560	-	-
27	8/26/2003	13:47:28	DROP	UDP	10.3.8.77	224.0.1.22	1027	427	202	-	-	-	-	-	-
28	8/26/2003	13:47:28	DROP	UDP	10.3.8.77	224.0.1.22	1027	427	136	-	-	-	-	-	-
29	8/26/2003	13:47:29	DROP	UDP	10.3.8.77	224.0.1.22	1027	427	136	-	-	-	-	-	-
30	8/26/2003	13:47:30	DROP	UDP	10.3.8.77	224.0.1.22	1027	427	136	-	-	-	-	-	-
31	8/26/2003	13:47:32	DROP	UDP	10.3.8.77	224.0.1.22	1027	427	136	-	-	-	-	-	-

To sort the data in Excel:

1. Select the entire spreadsheet by clicking in the upper left corner of the sheet.

2. Click on Data on the top menu and pull down to select Sort.

3. You will see the following window:



Sort

Sort by

8/26/2003 ● Ascending ○ Descending

Then by

● Ascending ○ Descending

Then by

● Ascending ○ Descending

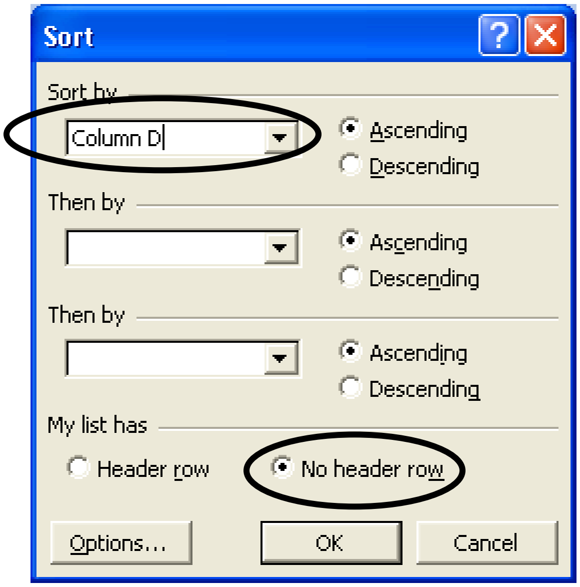
My list has

● Header row ○ No header row

4. First select My list has (No header row).

5. Now, the Sort by box will contain the column names. Select column D. This is where the Protocol data is located.

It will now look like this:



Sort

Sort by

Column D ● Ascending ○ Descending

Then by

● Ascending ○ Descending

Then by

● Ascending ○ Descending

My list has

○ Header row ● No header row

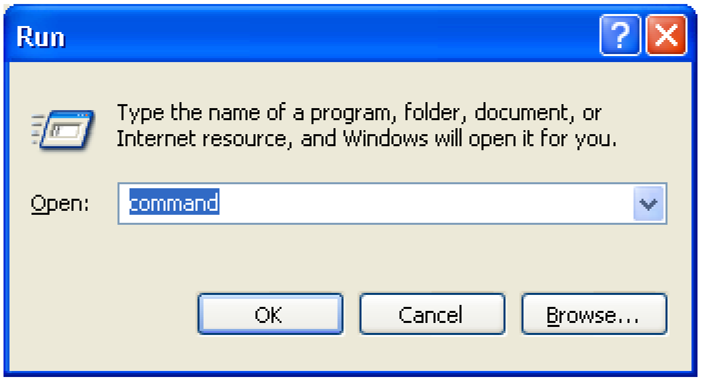
6. Click on OK.

7. The columns will now be sorted by Protocol and the ICMP designations will all be together for easy location and further analysis.

Tracing IP numbers

Once a suspected machine has been identified by the src-ip number provided by the log file, a trace route may be performed to obtain location information.

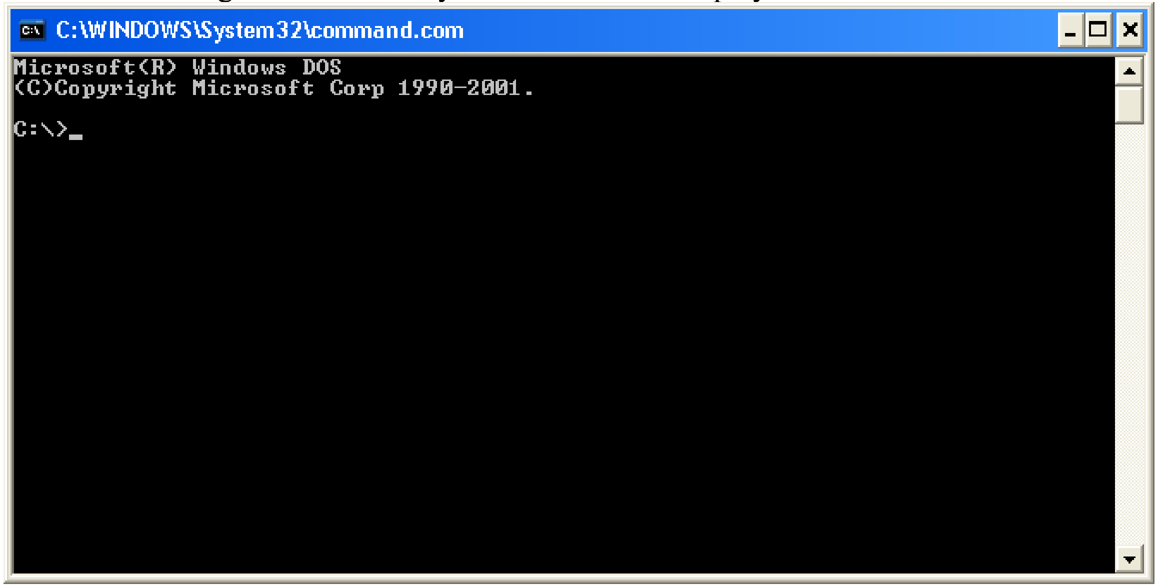
1. Click on the Start button and select Run.
2. In the space provided, enter Command as shown and click OK.



Type the name of a program, folder, document, or Internet resource, and Windows will open it for you.

Open: command

3. The following Command Entry Window will be displayed.



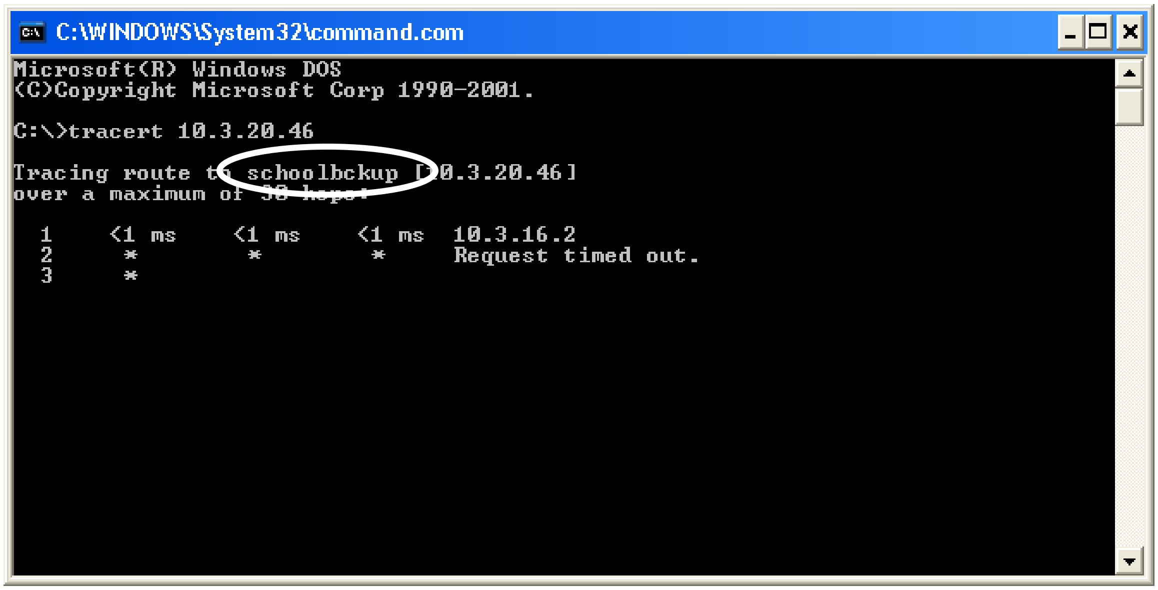
```
Microsoft(R) Windows DOS
(C)Copyright Microsoft Corp 1990-2001.

C:\>_
```

4. At the `C:\>` enter the trace route command (tracert) followed by the IP address you wish to trace. For example, to trace IP address 10.3.36.8, the command would look like this:

   ```
   C:\>tracert 10.3.36.8
   ```

5. Press enter and the trace will begin. Results will be displayed as shown on the next page.

Results of a tracert command on IP number 10.3.36.8



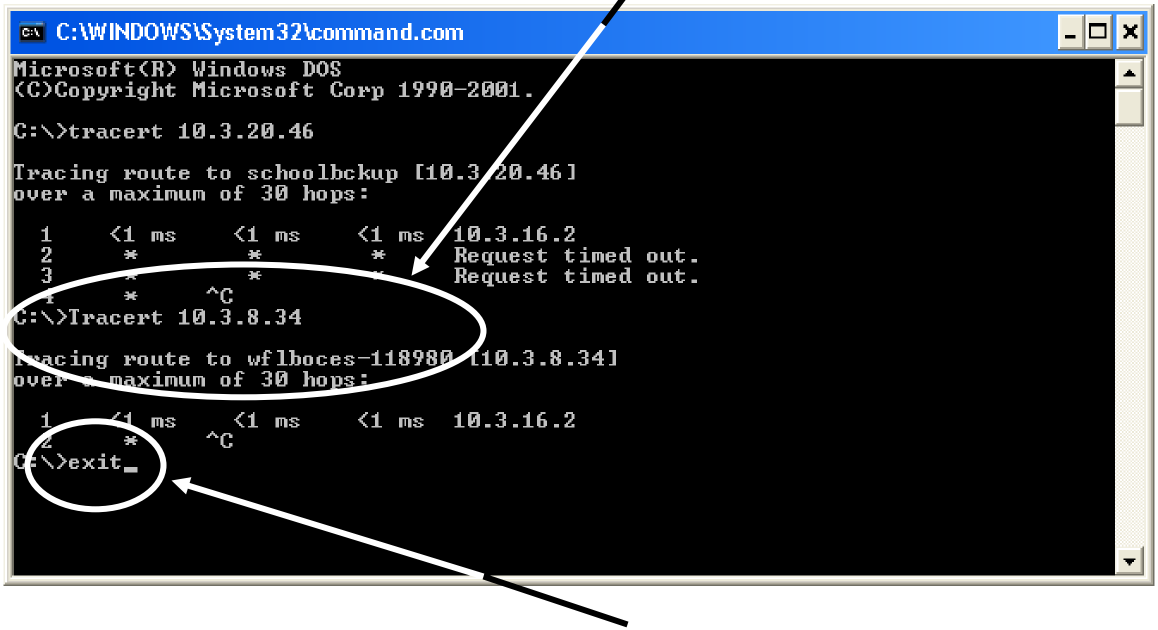
```
Microsoft(R) Windows DOS
(C)Copyright Microsoft Corp 1990-2001.

C:\>tracert 10.3.20.46

Tracing route to schoolbckup [10.3.20.46]
over a maximum of 30 hops:

  1    <1 ms    <1 ms    <1 ms  10.3.16.2
  2     *        *        *     Request timed out.
  3     *
```

The trace was able to provide the machine name, in this case, **schoolbckup**

The trace will continue to run for 30 hops.

To halt the process, press CTRL-Break.

In the screen shot below, the original trace was halted and another was initiated for IP 10.3.8.34 resulting in the computer named **wflboces-118980** being identified.



```
Microsoft(R) Windows DOS
(C)Copyright Microsoft Corp 1990-2001.

C:\>tracert 10.3.20.46

Tracing route to schoolbckup [10.3.20.46]
over a maximum of 30 hops:

  1    <1 ms    <1 ms    <1 ms  10.3.16.2
  2     *        *        *     Request timed out.
  3     *        *        *     Request timed out.
  4     *     ^C
C:\>Tracert 10.3.8.34

Tracing route to wflboces-118980 [10.3.8.34]
over a maximum of 30 hops:

  1    <1 ms    <1 ms    <1 ms  10.3.16.2
  2     *     ^C
C:\>exit_
```

Finally, as displayed above, you must issue an Exit command to close the window.