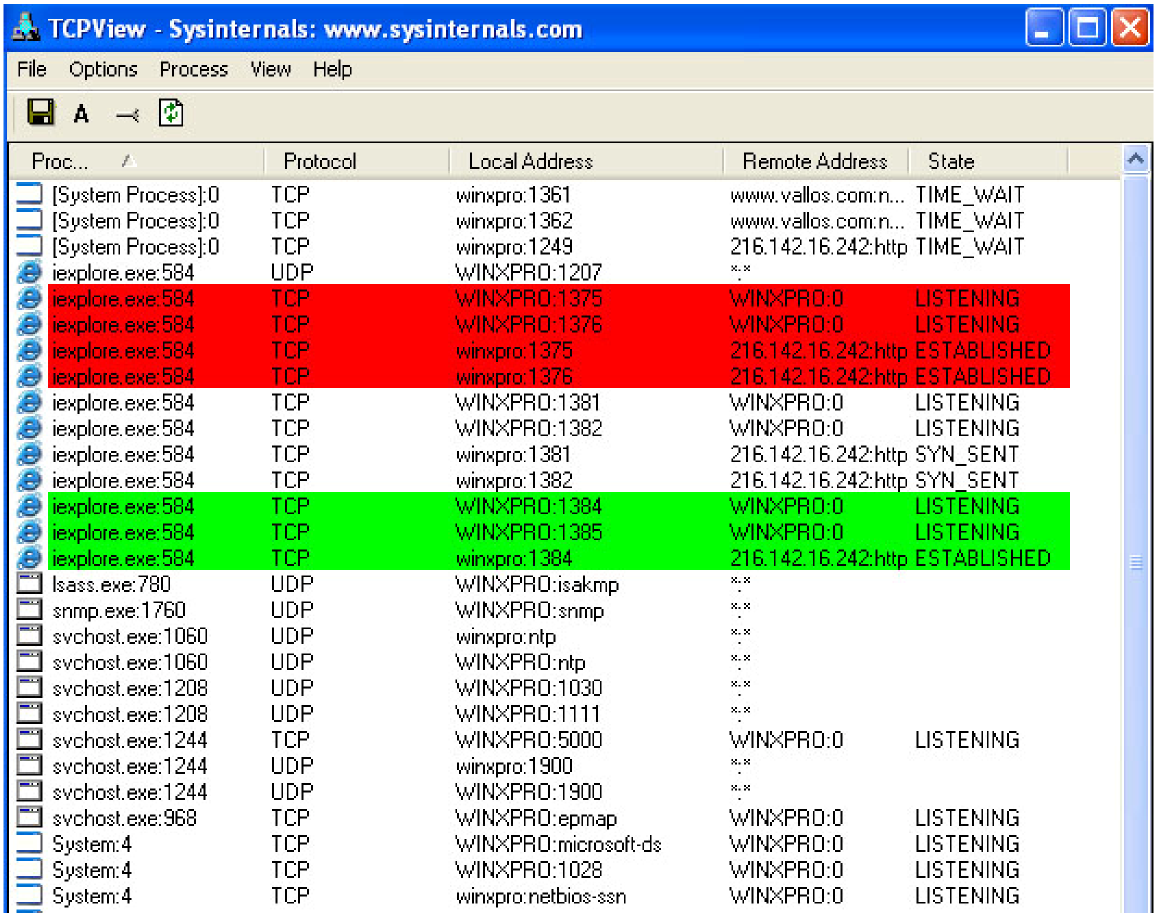
1.2.1

SOCKET MONITORING

TCPVIEW



Proc...	Protocol	Local Address	Remote Address	State
[System Process]:0	TCP	winxpro:1361	www.vallos.com:n...	TIME_WAIT
[System Process]:0	TCP	winxpro:1362	www.vallos.com:n...	TIME_WAIT
[System Process]:0	TCP	winxpro:1249	216.142.16.242:http	TIME_WAIT
iexplore.exe:584	UDP	WINXPRO:1207	*:*	
iexplore.exe:584	TCP	WINXPRO:1375	WINXPRO:0	LISTENING
iexplore.exe:584	TCP	WINXPRO:1376	WINXPRO:0	LISTENING
iexplore.exe:584	TCP	winxpro:1375	216.142.16.242:http	ESTABLISHED
iexplore.exe:584	TCP	winxpro:1376	216.142.16.242:http	ESTABLISHED
iexplore.exe:584	TCP	WINXPRO:1381	WINXPRO:0	LISTENING
iexplore.exe:584	TCP	WINXPRO:1382	WINXPRO:0	LISTENING
iexplore.exe:584	TCP	winxpro:1381	216.142.16.242:http	SYN_SENT
iexplore.exe:584	TCP	winxpro:1382	216.142.16.242:http	SYN_SENT
iexplore.exe:584	TCP	WINXPRO:1384	WINXPRO:0	LISTENING
iexplore.exe:584	TCP	WINXPRO:1385	WINXPRO:0	LISTENING
iexplore.exe:584	TCP	winxpro:1384	216.142.16.242:http	ESTABLISHED
lsass.exe:780	UDP	WINXPRO:isakmp	*:*	
snmp.exe:1760	UDP	WINXPRO:snmp	*:*	
svchost.exe:1060	UDP	winxpro:ntp	*:*	
svchost.exe:1060	UDP	WINXPRO:ntp	*:*	
svchost.exe:1208	UDP	WINXPRO:1030	*:*	
svchost.exe:1208	UDP	WINXPRO:1111	*:*	
svchost.exe:1244	TCP	WINXPRO:5000	WINXPRO:0	LISTENING
svchost.exe:1244	UDP	winxpro:1900	*:*	
svchost.exe:1244	UDP	WINXPRO:1900	*:*	
svchost.exe:968	TCP	WINXPRO:epmap	WINXPRO:0	LISTENING
System:4	TCP	WINXPRO:microsoft-ds	WINXPRO:0	LISTENING
System:4	TCP	WINXPRO:1028	WINXPRO:0	LISTENING
System:4	TCP	winxpro:netbios-ssn	WINXPRO:0	LISTENING

Objective

At the end of this lab students will be able to monitor Windows sockets. Students will be able to differentiate between Local and Remote end points, and the State of each end point.

Information for Laboratory

A. Students will utilize TCPView from Sysinternals, a freeware socket monitoring program.
B. Students will utilize Windows XP, and Netstat.

Student Preparation

The student will have completed requisite reading. The student will require paper for notes and should be prepared to discuss the exercises upon completion.

Instructor Preparation

Before class, the instructor or a lab assistant will ensure that TCPView has been downloaded, extracted, and copied to the desktop of each student workstation. Students must also have access to the windows utility netstat.

Estimated Completion Time

30 Minutes

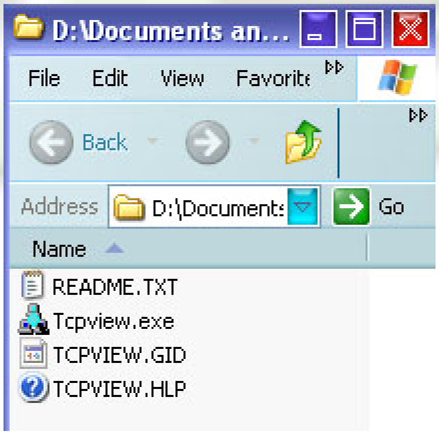
A socket is one end-point of a two-way communication link between two programs running on a network. A socket is notated as the IP Address, a colon (:), and the corresponding TCP port. An example would be 10.1.2.5:80, or www.domain.com:HTTP.

TCPView

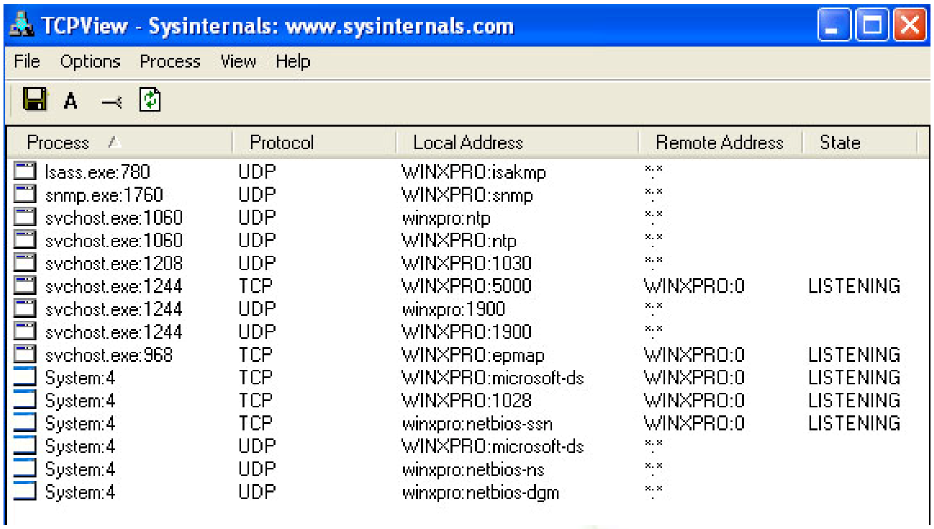
TCPView is a Windows program that will show you detailed listings of all TCP and UDP endpoints on your system, including the local and remote addresses and state of TCP connections. On Windows NT, 2000 and XP TCPView also reports the name of the process that owns the endpoint. TCPView provides a more informative and conveniently presented subset of the Netstat program that ships with Windows.

Step 1: Viewing active Windows sockets

From your desktop, locate and launch the TCPView program by double clicking on the Tcpview.exe file.



README.TXT
Tcpview.exe
TCPVIEW.GID
TCPVIEW.HLP

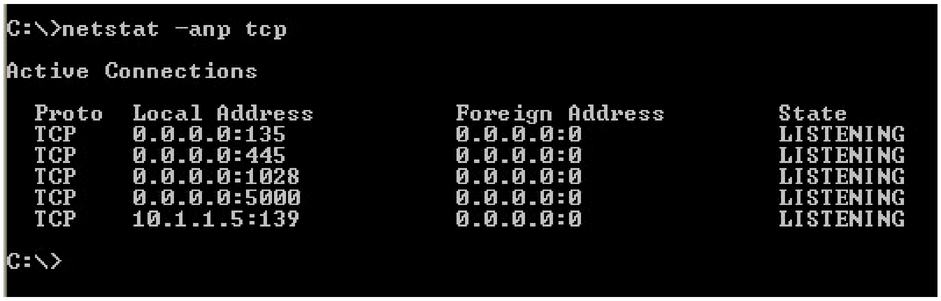

TCPView - Sysinternals: www.sysinternals.com
File Options Process View Help

Process	Protocol	Local Address	Remote Address	State
lsass.exe:780	UDP	WINXPRO:isakmp	*:*	
snmp.exe:1760	UDP	WINXPRO:snmp	*:*	
svchost.exe:1060	UDP	winxpro:ntp	*:*	
svchost.exe:1060	UDP	WINXPRO:ntp	*:*	
svchost.exe:1208	UDP	WINXPRO:1030	*:*	
svchost.exe:1244	TCP	WINXPRO:5000	WINXPRO:0	LISTENING
svchost.exe:1244	UDP	winxpro:1900	*:*	
svchost.exe:1244	UDP	WINXPRO:1900	*:*	
svchost.exe:968	TCP	WINXPRO:epmap	WINXPRO:0	LISTENING
System:4	TCP	WINXPRO:microsoft-ds	WINXPRO:0	LISTENING
System:4	TCP	WINXPRO:1028	WINXPRO:0	LISTENING
System:4	TCP	winxpro:netbios-ssn	WINXPRO:0	LISTENING
System:4	UDP	WINXPRO:microsoft-ds	*:*	
System:4	UDP	winxpro:netbios-ns	*:*	
System:4	UDP	winxpro:netbios-dgm	*:*	

TCPView lists all Windows Processes and the associated protocol, either TCP or UDP. The Local Address is listed with the used TCP or UDP port number. The Remote address is listed with the used TCP or UDP port number. The State is listed as either Listening, Established, or Time_wait. The state shows what connections are currently in use, and what they are doing. If a connection is listening, it is waiting for a remote connection to be established. If a connection is established, the Local and Remote end points are connected, and transferring data between each other.

To verify the accuracy of the TCPView program, a Windows netstat command can be run and compared to the output of TCPView.

From START, Run, type ‘cmd’ and press enter. From the C:\> prompt type ‘netstat –anp tcp’ and press enter.

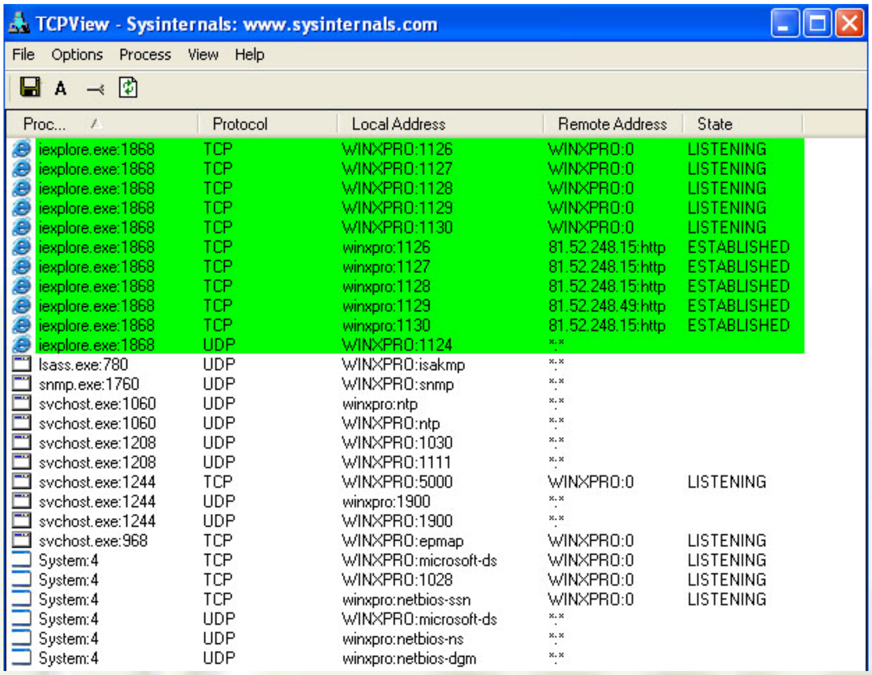


```
C:\>netstat -anp tcp

Active Connections

  Proto  Local Address          Foreign Address        State
  TCP    0.0.0.0:135            0.0.0.0:0              LISTENING
  TCP    0.0.0.0:445            0.0.0.0:0              LISTENING
  TCP    0.0.0.0:1028           0.0.0.0:0              LISTENING
  TCP    0.0.0.0:5000           0.0.0.0:0              LISTENING
  TCP    10.1.1.5:139           0.0.0.0:0              LISTENING

C:\>
```

Notice that there are 5 listening TCP ports on both the Windows netstat output, and from TCPView.

Step 2: Viewing new connections

Keep TCPView open and viewable on the desktop. Open Internet Explorer and watch the output from TCPView.

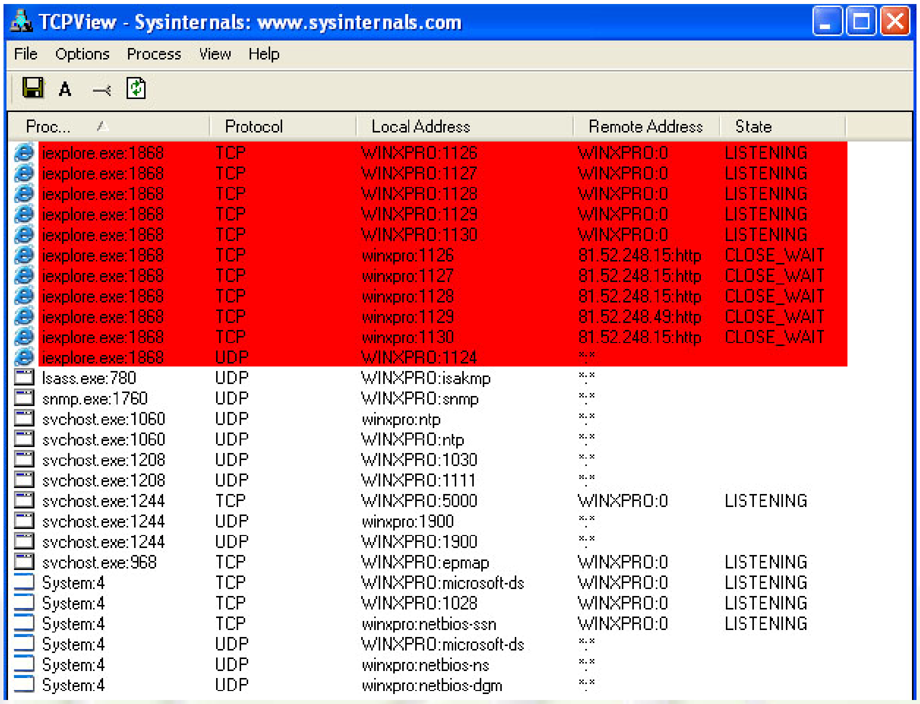


Proc...	Protocol	Local Address	Remote Address	State
iexplore.exe:1868	TCP	WINXPRO:1126	WINXPRO:0	LISTENING
iexplore.exe:1868	TCP	WINXPRO:1127	WINXPRO:0	LISTENING
iexplore.exe:1868	TCP	WINXPRO:1128	WINXPRO:0	LISTENING
iexplore.exe:1868	TCP	WINXPRO:1129	WINXPRO:0	LISTENING
iexplore.exe:1868	TCP	WINXPRO:1130	WINXPRO:0	LISTENING
iexplore.exe:1868	TCP	winxpro:1126	81.52.248.15:http	ESTABLISHED
iexplore.exe:1868	TCP	winxpro:1127	81.52.248.15:http	ESTABLISHED
iexplore.exe:1868	TCP	winxpro:1128	81.52.248.15:http	ESTABLISHED
iexplore.exe:1868	TCP	winxpro:1129	81.52.248.49:http	ESTABLISHED
iexplore.exe:1868	TCP	winxpro:1130	81.52.248.15:http	ESTABLISHED
iexplore.exe:1868	UDP	WINXPRO:1124	*:*	
lsass.exe:780	UDP	WINXPRO:isakmp	*:*	
snmp.exe:1760	UDP	WINXPRO:snmp	*:*	
svchost.exe:1060	UDP	winxpro:ntp	*:*	
svchost.exe:1060	UDP	WINXPRO:ntp	*:*	
svchost.exe:1208	UDP	WINXPRO:1030	*:*	
svchost.exe:1208	UDP	WINXPRO:1111	*:*	
svchost.exe:1244	TCP	WINXPRO:5000	WINXPRO:0	LISTENING
svchost.exe:1244	UDP	winxpro:1900	*:*	
svchost.exe:1244	UDP	WINXPRO:1900	*:*	
svchost.exe:968	TCP	WINXPRO:epmap	WINXPRO:0	LISTENING
System:4	TCP	WINXPRO:microsoft-ds	WINXPRO:0	LISTENING
System:4	TCP	WINXPRO:1028	WINXPRO:0	LISTENING
System:4	TCP	winxpro:netbios-ssn	WINXPRO:0	LISTENING
System:4	UDP	WINXPRO:microsoft-ds	*:*	
System:4	UDP	winxpro:netbios-ns	*:*	
System:4	UDP	winxpro:netbios-dgm	*:*	

Notice that as soon as you open Internet Explorer, the process is listed in TCPView, and highlighted green. TCPView automatically shows all new connections highlighted green.

Notice that for the Internet Explorer process, The end point Remote Address:HTTP is showing an Established connection to a remote web server on port 80, HTTP.

Step 3: Viewing Closing connections



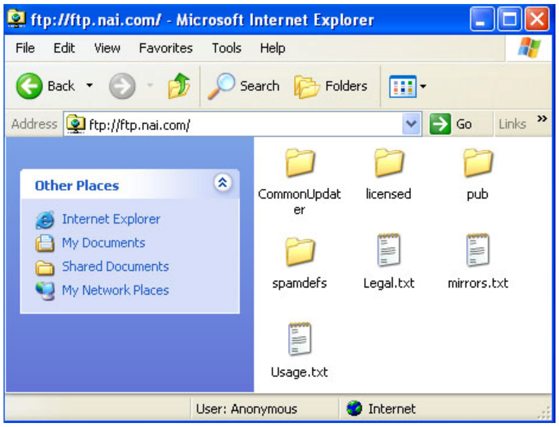
Proc...	Protocol	Local Address	Remote Address	State
iexplore.exe:1868	TCP	WINXPRO:1126	WINXPRO:0	LISTENING
iexplore.exe:1868	TCP	WINXPRO:1127	WINXPRO:0	LISTENING
iexplore.exe:1868	TCP	WINXPRO:1128	WINXPRO:0	LISTENING
iexplore.exe:1868	TCP	WINXPRO:1129	WINXPRO:0	LISTENING
iexplore.exe:1868	TCP	WINXPRO:1130	WINXPRO:0	LISTENING
iexplore.exe:1868	TCP	winxpro:1126	81.52.248.15:http	CLOSE_WAIT
iexplore.exe:1868	TCP	winxpro:1127	81.52.248.15:http	CLOSE_WAIT
iexplore.exe:1868	TCP	winxpro:1128	81.52.248.15:http	CLOSE_WAIT
iexplore.exe:1868	TCP	winxpro:1129	81.52.248.49:http	CLOSE_WAIT
iexplore.exe:1868	TCP	winxpro:1130	81.52.248.15:http	CLOSE_WAIT
iexplore.exe:1868	UDP	WINXPRO:1124	*:*	
lsass.exe:780	UDP	WINXPRO:isakmp	*:*	
snmp.exe:1760	UDP	WINXPRO:snmp	*:*	
svchost.exe:1060	UDP	winxpro:ntp	*:*	
svchost.exe:1060	UDP	WINXPRO:ntp	*:*	
svchost.exe:1208	UDP	WINXPRO:1030	*:*	
svchost.exe:1208	UDP	WINXPRO:1111	*:*	
svchost.exe:1244	TCP	WINXPRO:5000	WINXPRO:0	LISTENING
svchost.exe:1244	UDP	winxpro:1900	*:*	
svchost.exe:1244	UDP	WINXPRO:1900	*:*	
svchost.exe:968	TCP	WINXPRO:epmap	WINXPRO:0	LISTENING
System:4	TCP	WINXPRO:microsoft-ds	WINXPRO:0	LISTENING
System:4	TCP	WINXPRO:1028	WINXPRO:0	LISTENING
System:4	TCP	winxpro:netbios-ssn	WINXPRO:0	LISTENING
System:4	UDP	WINXPRO:microsoft-ds	*:*	
System:4	UDP	winxpro:netbios-ns	*:*	
System:4	UDP	winxpro:netbios-dgm	*:*	

Notice that as soon as you close Internet Explorer, the process listed in TCPView is highlighted in red. TCPView automatically shows all closing connections highlighted green.

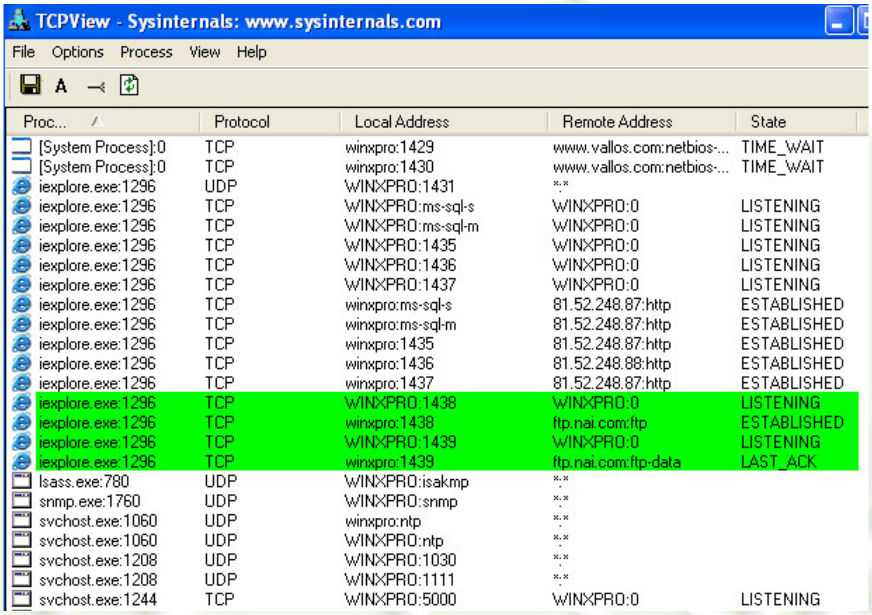
Step 4: Viewing Connections

Keep TCPView open and watch as the output changes as you do the next step.

Open another instance of Internet Explorer, and enter ‘ftp://ftp.nai.com’ in the address bar and press enter. You should be connect to the FTP site as below.



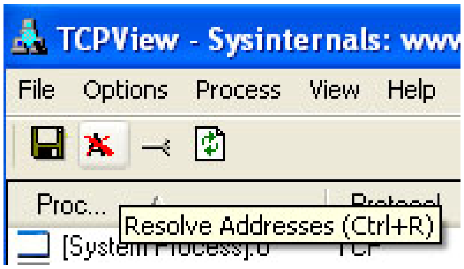
Notice the output from TCPView as below.


TCPView - Sysinternals: www.sysinternals.com
File Options Process View Help

Proc...	Protocol	Local Address	Remote Address	State
[System Process]:0	TCP	winxpro:1429	www.vallos.com:netbios-...	TIME_WAIT
[System Process]:0	TCP	winxpro:1430	www.vallos.com:netbios-...	TIME_WAIT
iexplore.exe:1296	UDP	WINXPRO:1431	*:*	
iexplore.exe:1296	TCP	WINXPRO:ms-sql-s	WINXPRO:0	LISTENING
iexplore.exe:1296	TCP	WINXPRO:ms-sql-m	WINXPRO:0	LISTENING
iexplore.exe:1296	TCP	WINXPRO:1435	WINXPRO:0	LISTENING
iexplore.exe:1296	TCP	WINXPRO:1436	WINXPRO:0	LISTENING
iexplore.exe:1296	TCP	WINXPRO:1437	WINXPRO:0	LISTENING
iexplore.exe:1296	TCP	winxpro:ms-sql-s	81.52.248.87:http	ESTABLISHED
iexplore.exe:1296	TCP	winxpro:ms-sql-m	81.52.248.87:http	ESTABLISHED
iexplore.exe:1296	TCP	winxpro:1435	81.52.248.87:http	ESTABLISHED
iexplore.exe:1296	TCP	winxpro:1436	81.52.248.88:http	ESTABLISHED
iexplore.exe:1296	TCP	winxpro:1437	81.52.248.87:http	ESTABLISHED
iexplore.exe:1296	TCP	WINXPRO:1438	WINXPRO:0	LISTENING
iexplore.exe:1296	TCP	winxpro:1438	ftp.nai.com:ftp	ESTABLISHED
iexplore.exe:1296	TCP	WINXPRO:1439	WINXPRO:0	LISTENING
iexplore.exe:1296	TCP	winxpro:1439	ftp.nai.com:ftp-data	LAST_ACK
lsass.exe:780	UDP	WINXPRO:isakmp	*:*	
snmp.exe:1760	UDP	WINXPRO:snmp	*:*	
svchost.exe:1060	UDP	winxpro:ntp	*:*	
svchost.exe:1060	UDP	WINXPRO:ntp	*:*	
svchost.exe:1208	UDP	WINXPRO:1030	*:*	
svchost.exe:1208	UDP	WINXPRO:1111	*:*	
svchost.exe:1244	TCP	WINXPRO:5000	WINXPRO:0	LISTENING

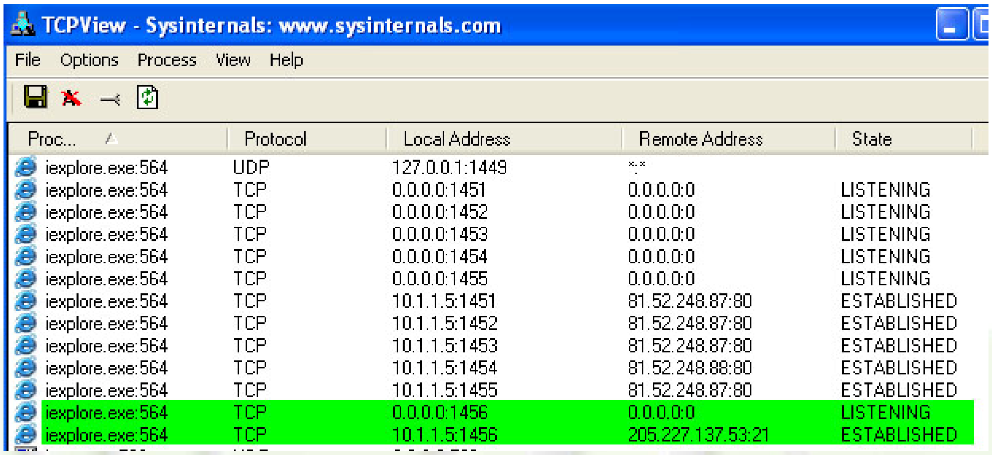
Notice that the Remote Address end point shows the active sockets ftp.nai.com:ftp, and ftp.nai.com:ftp-data.

From the toolbar on TCPView, click the A button to disable name resolution, or press Ctrl+R.


TCPView - Sysinternals: www
File Options Process View Help
Proc...
Protocol
Resolve Addresses (Ctrl+R)
[System Process]:0
TCP

Close all instances of Internet Explorer. Open Internet Explorer, and enter ‘ftp://ftp.nai.com’ in the address bar and press enter. You should be connected again to the FTP site.

Notice that the output from TCPView changes when name resolution has been shut off. TCPView now shows the socket as 205.227.137.53:21 instead of ftp.nai.com:ftp.



Proc...	Protocol	Local Address	Remote Address	State
iexplore.exe:564	UDP	127.0.0.1:1449	*:*	
iexplore.exe:564	TCP	0.0.0.0:1451	0.0.0.0:0	LISTENING
iexplore.exe:564	TCP	0.0.0.0:1452	0.0.0.0:0	LISTENING
iexplore.exe:564	TCP	0.0.0.0:1453	0.0.0.0:0	LISTENING
iexplore.exe:564	TCP	0.0.0.0:1454	0.0.0.0:0	LISTENING
iexplore.exe:564	TCP	0.0.0.0:1455	0.0.0.0:0	LISTENING
iexplore.exe:564	TCP	10.1.1.5:1451	81.52.248.87:80	ESTABLISHED
iexplore.exe:564	TCP	10.1.1.5:1452	81.52.248.87:80	ESTABLISHED
iexplore.exe:564	TCP	10.1.1.5:1453	81.52.248.87:80	ESTABLISHED
iexplore.exe:564	TCP	10.1.1.5:1454	81.52.248.88:80	ESTABLISHED
iexplore.exe:564	TCP	10.1.1.5:1455	81.52.248.87:80	ESTABLISHED
iexplore.exe:564	TCP	0.0.0.0:1456	0.0.0.0:0	LISTENING
iexplore.exe:564	TCP	10.1.1.5:1456	205.227.137.53:21	ESTABLISHED

Analysis

1) For which applications is TCPView best suited?

2) After working with these utilities, what about TCP/IP sockets do you feel you should study further? Why?

3) What are the benefits of using TCPView instead of Netstat?

Summary Discussion

A classroom discussion should follow the lab. Review the lab questions and your analyses as a group. Share your experiences and knowledge with the class.

Appendix

TCPView version 2.34 from Sysinternals, running on a Windows XP with Service Pack 1, was used to perform this lab.