APPENDIX A

Introduction to tcpdump

Tcpdump is a packet capture tool. It can grab packets flowing on the network, match them to some criteria and then dump them on the screen or into a file. It is available on most of the UNIX platforms. On Linux machines, you need to be the root user to run tcpdump. If you save the captured data in a file, you can view the file later using tcpdump. Since Snort can also store data in the tcpdump format in files, it becomes an interesting tool for many people to view Snort files that have been created in the tcpdump format.

The typical output of the command when used on the command prompt without any argument is as follows:

```
[root@conformix]# tcpdump
Kernel filter, protocol ALL, TURBO mode (575 frames), datagram packet
  socket
tcpdump: listening on all devices
13:05:52.216049 eth0 < rr-laptop.6001 > dti414.1245: P
  1578894642:1578894674(32) ack 3347166818 win 63520
  <nop,nop,timestamp 453029 53292014> (DF)
13:05:52.216049 eth0 > dti414.1245 > rr-laptop.6001: . 1:1449(1448) ack
  32 win 63712 <nop,nop,timestamp 53292021 453029> (DF)
13:05:52.216049 eth0 > dti414.1245 > rr-laptop.6001: P 1449:2045(596)
  ack 32 win 63712 <nop,nop,timestamp 53292021 453029> (DF)
13:05:52.216049 eth0 < rr-laptop.6001 > dti414.1245: . 32:32(0) ack
  2045 win 64240 <nop,nop,timestamp 453029 53292021> (DF)
```

```
13:05:52.226049 eth0 > dti414.1245 > rr-laptop.6001: . 2045:3493(1448)
  ack 32 win 63712 <nop,nop,timestamp 53292022 453029> (DF)
13:05:52.226049 eth0 > dti414.1245 > rr-laptop.6001: P 3493:4089(596)
  ack 32 win 63712 <nop,nop,timestamp 53292022 453029> (DF)
13:05:52.226049 eth0 < rr-laptop.6001 > dti414.1245: . 32:32(0) ack
  4089 win 64240 <nop,nop,timestamp 453029 53292022> (DF)
```

You can use a number of command line switches with the command. A list of switches is available on the manual pages. The important switch to use with Snort is `-r <filename>`, where filename is the file containing Snort data. Simple Snort log files can't be used with this option. Only the files that are created in the tcpdump format can be read by the command.