IP Packet Sniffer

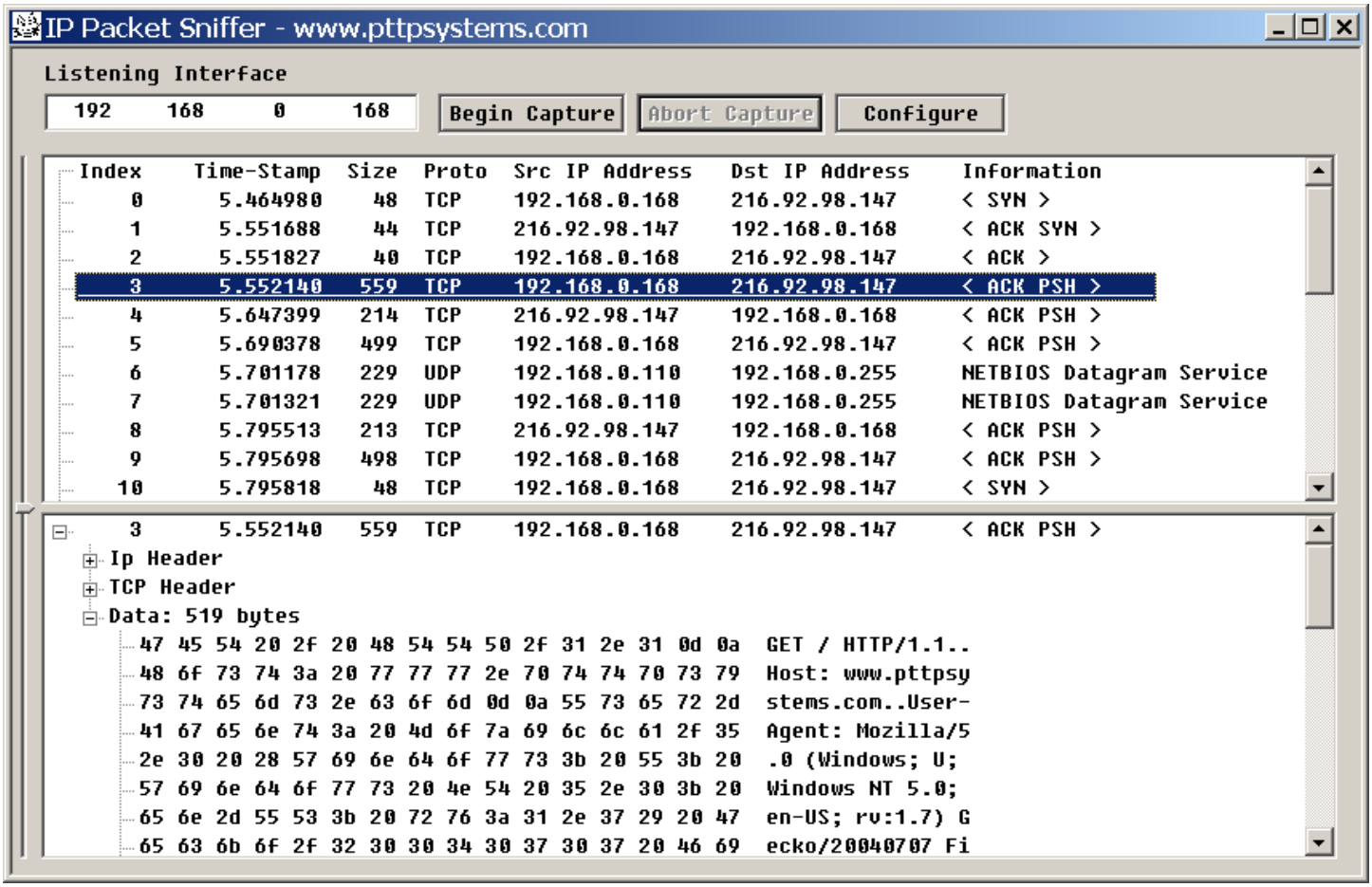
Summary

IP Packet Sniffer employs a “raw” socket to capture IP protocol packets traveling over your local network. These packets contain data and communications information traveling on your local network. The packets may originate from or be addressed to your computer. On the other hand, the data could be passing between computers that are not yours.

Note: *IP Packet Sniffer* does not have access to the Ethernet header for the IP packet.

Capture Dialog

The interface is shown below.



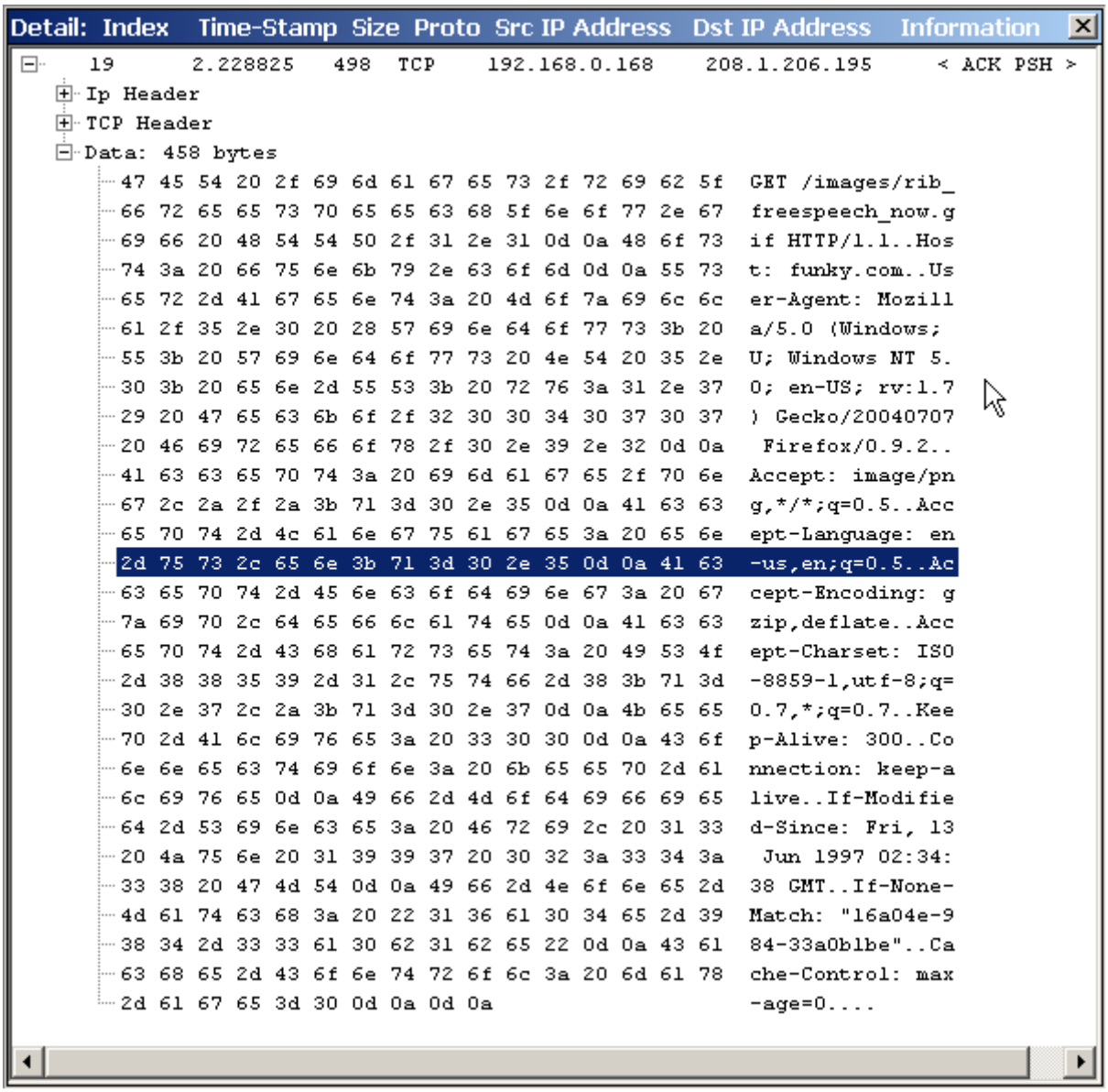
- The IP address in the upper left corner is the interface to which the program is currently listening.
- The “Begin Capture” button starts the capture process.
- The windows are cleared each time that a capture is initiated.
- A running capture can be terminated before the capture limits are reached using the “Abort Capture” button.
- The slider on the left controls the sizes of the two windows.
- The capture configuration panel can be accessed through the “Configure” button.

Captured Packet Window

The upper window shows a summary of the captured packets. The summary data include

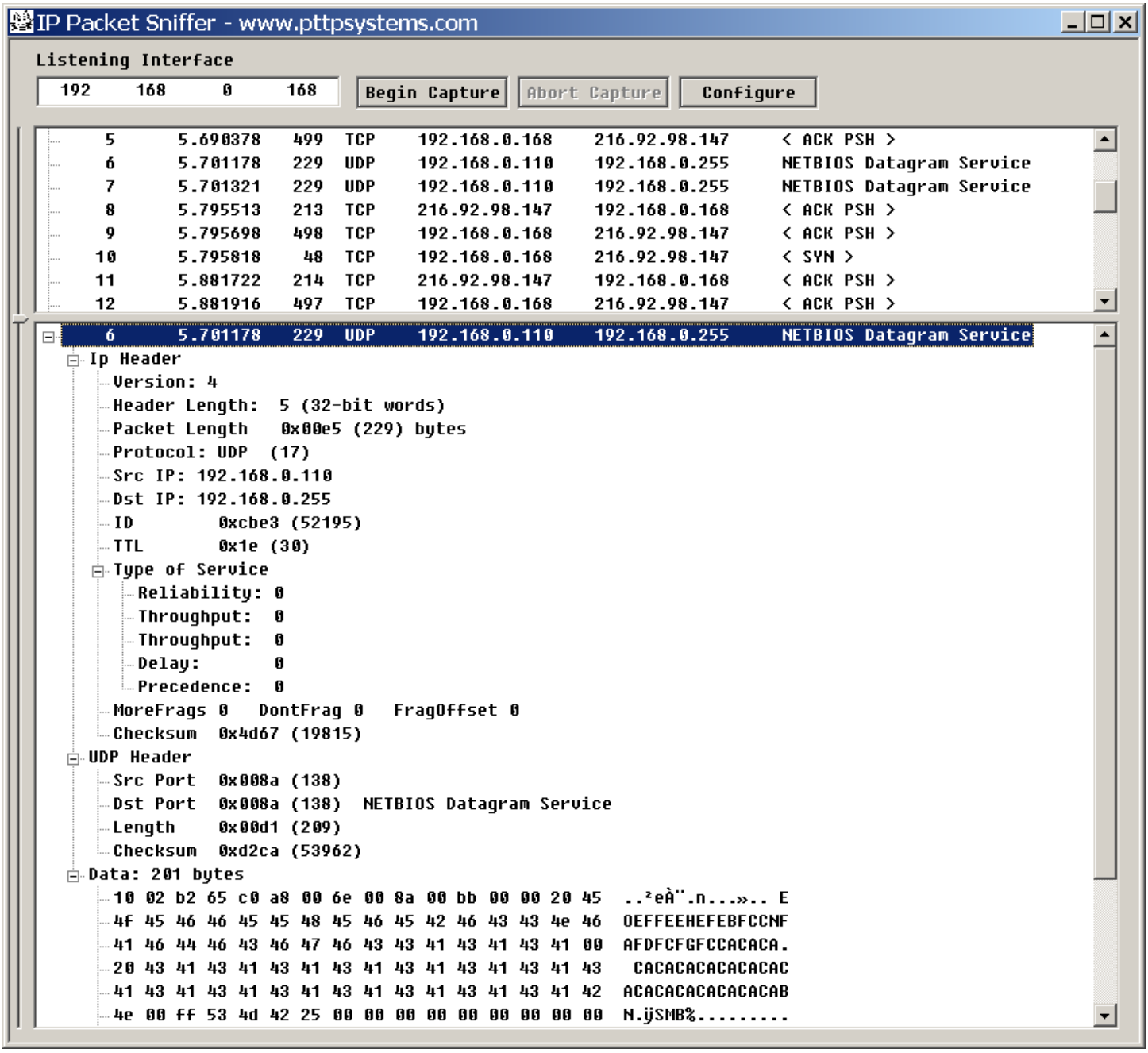
- packet number
- time elapsed since capture was initiated (with microsecond resolution)
- packet size
- packet type (protocol)
- source and destination IP addresses
- summary information about the IP packet

If you double-click an item in the captured packet window, you will create a snapshot in a floating, modeless window, as shown below. This window behaves in the same manner as the packet detail window discussed in the next section.



Packet Detail Window

The lower window on the main interface shows the details for any packet selected in the captured packet window.



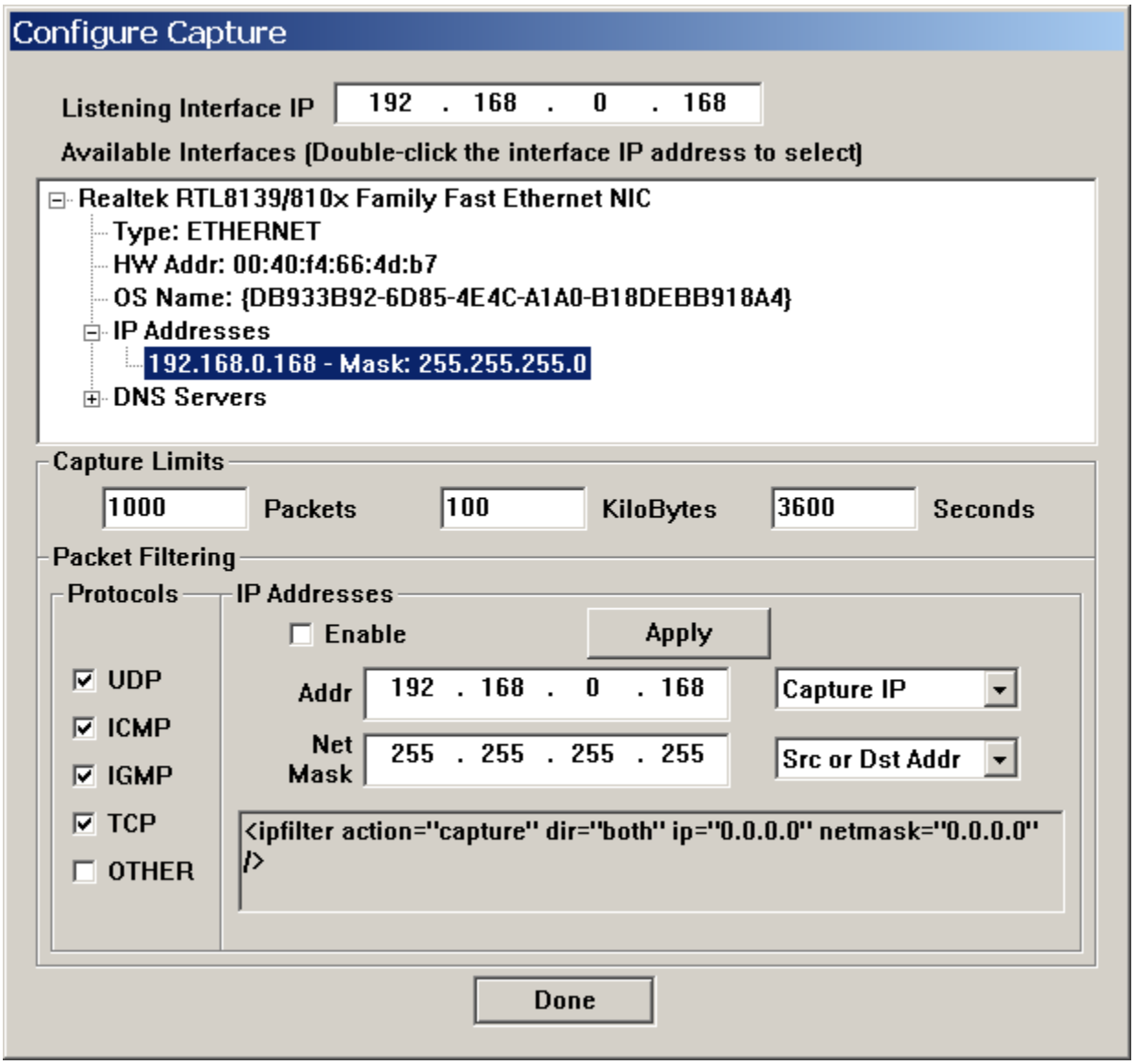
The packet details that may be shown include

- fields for the IP packet
- fields of the UDP, TCP, ICMP or IGMP portion of the packet
- packet payloads are also broken out for ICMP packets.
- data formats that are unknown, or just raw data are displayed using a combination of hexadecimal and ASCII text display.

Packet detail toggle states for the tree view are persistent.

Configuration Dialog

IP Packet Sniffer can be configured in number of ways to help you look at your network traffic. The interface is shown below.



Listening Interface

The IP address in the top middle of the window shows the IP address to which the listening socket is bound. *IP Packet Sniffer* can use any interface (Ethernet card) on your system that supports raw sockets.

At program startup the raw socket is bound to the first available interface. If that interface does not support either raw sockets or raw sockets in "promiscuous" mode, then an error message is displayed an you will need to go to the configuration dialog to select an interface.

Note: most, if not all, wireless cards do not support raw/promiscuous sockets.

Binding to an Interface

To bind to an interface that is not the default (first available) interface on your system, expand the "IP Addresses" section of the interface description of your choice then double-click the IP address of interest. If you have multiple IP addresses assigned to an interface, pick the appropriate IP address.

Capture Limits

IP Packet Sniffer can be configured to limit the packets captured to be less than the internal maximum values. The program currently only captures data to a 1024Kbyte memory buffer which can fill up very quickly when downloading, say, the front page of a busy website.

The limit parameters are:

- captured packet count (internal maximum of 8096)
- captured byte count in kilobytes (internal maximum of 1024Kb)
- capture time in seconds (unlimited)

Packet Filtering

IP Packet Sniffer can capture IP packets based on acceptance criteria so as to simplify searching for specific information. A busy network can produce a large amount of data, and who wants to sift through thousands of packets to find the needle in the haystack? ☺

Protocol, or Packet Type

The first and simplest filtering criterion is the type of IP packet. The packet types are grouped into five protocols categories: UDP, TCP, ICMP, IGMP, and OTHER. By default, UDP, TCP, ICMP, and IGMP packets are captured while OTHER packets are filtered out.

IP Addresses

The second criterion for IP packet filtering is the source and destination IP addresses in the IP packet. *IP Packet Sniffer* allows you to choose to either accept or ignore a single IP address or a single group of IP addresses on a single network based on the source IP, destination IP, or both. IP address filtering is disabled by default.

To enable this filter mechanism, enable the "Enable" check box.

To configure the IP filter, fill in the IP address or the network address and mask. Next, choose the appropriate capture/ignore and direction configurations using the drop-list menus on the right side of that section. Push the "Apply" button – a summary of the filter configuration will appear in the lower window.