

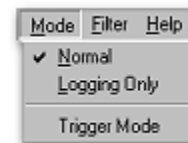
Sniff'em 1.01 Whitepaper

Generalities

Usage Modes

Normal Mode

Real-Time display of captured packets, incoming Network packets will be immediately decoded and added to the Packet list, this eats up a whole lot of resources, this is why we introduced the Logging only mode.



Logging Only

Logging only mode will disable the graphical display of incoming packets temporarily and capture the packets by logging them to the hard disc with a minimum of CPU usage, this is a real performance boost and recommended for heavy loaded networks.

Trigger mode

The Trigger mode is another nifty feature of Sniff'em™, it uses a predefined Filter to set it's Trigger event. As example: a Trigger filter is set to port 110 (POP3) and ASCII data "Password: superjemp", once such a packet is found (i.e. a user logs in) Sniff'em™ will start capturing subsequent traffic be it filtered or not.

Buffer Size Limits

The Buffer size can be adjusted in the Settings menu, it directly scales with free memory, when using Normal mode the display will be cleared once the limit set has been reached, if Logging Only mode is activated the Buffer Size is ignored. However when you open a saved Project which is bigger then Buffer size, a new Window will pop-up and give you the possibility to select the range of Packets to load into the Buffer. You may also change the Size of the Buffer to hold the whole Project.

