Ethereal

The Technology Firm

What is Ethereal (From Docs.)

- **Ethereal** is a GUI network protocol analyzer. It lets you interactively browse packet data from a live network or from a previously saved capture file.
- **Ethereal** knows how to read **libpcap** capture files, including those of **tcpdump**, **snoop** (including **Shomiti**) and **atmsnoop**, **LanAlyzer**, **Sniffer** (compressed or uncompressed), Microsoft **Network Monitor**, AIX's **iptrace**, **NetXray**, **Sniffer Pro**, **Etherpeek**, **RADCOM's** WAN/LAN analyzer, **Lucent/Ascend** router debug output, HP-UX's **nettl**, the dump output from **Toshiba's** ISDN routers, the output from **i4btrace** from the ISDN4BSD project, the output in **IPLog** format from the Cisco Secure Intrusion Detection System, and **pppd logs** (pppdump format).
- Display filters in **Ethereal** are very powerful; more fields are filterable in **Ethereal** than in other protocol analyzers, and the syntax you can use to create your filters is richer. As **Ethereal** progresses, expect more and more protocol fields to be allowed in display filters.
- Packet capturing is performed with the pcap library. The capture filter syntax follows the rules of the pcap library. This syntax is different from the display filter syntax.

Ethereal Screen Layout