

Ethereal

The Technology Firm

- **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



The screenshot displays the Wireshark interface with the following components:

- Packet List Pane:** Shows a list of captured packets. The first four packets are highlighted in yellow. The summary line for each packet is: `No. Time Source Destination Protocol Info`. For example, packet 23 at time 0.173433 from `10n.98:56:f6` to `NETBIOS-` is a `BROWSER Local Master Announcement` for `PC15897, workstation`.
- Protocol Tree Pane:** Shows a hierarchical view of the protocols in the selected packet. The tree includes: `Ethernet II`, `Logical Link Control`, `Internet Protocol Version 4`, `Internet Message Access Protocol`, `SMTP (Simple Mail Transfer Protocol)`, `Microsoft Windows Browser Protocol`, and `Microsoft Windows Browser Protocol`.
- Packet Bytes Pane:** Shows the raw bytes of the selected packet. The hex dump shows the first 10 bytes of the packet: `0000 ff ff ff ff ff ff 00 04 2c 98 56 f6 00 0c 00 00`.
- Hex Dump Pane:** Shows the ASCII representation of the hex dump. The first 10 bytes are: `.....V.....`.

The summary line, briefly describing what the packet is.

A protocol tree is shown, allowing you to drill down to exact protocol or field that you interested in.

a hex dump shows you exactly what the packet looks like when it goes over the wire.

Filename Of Current File