**Wireshark**

**Wireshark is a network packet analyzer. A network packet analyzer will try to capture network packets and tries to display that packet data as detailed as possible.** In the past, such tools were either very expensive, proprietary, or both. However, with the advent of Wireshark, all that has changed.

Wireshark is perhaps one of the best open source packet analyzers available today.

**Applications**

* **Network administrators use it to troubleshoot network problems**
* Network security engineers use it to **examine security problems**
* Developers use it to **debug protocol implementations**
* People use it to **learn network protocol** internals

**Features**

* Available for **UNIX** and **Windows**.
* **Capture** live packet data from a network interface.
* Display packets with **very detailed protocol information**.
* **Open and Save** packet data captured.
* **Import and Export** packet data from and to a lot of other capture programs.
* **Filter packets** on many criteria.
* **Search** for packets on many criteria.
* **Colorize** packet display based on filters.
* Create various **statistics**.

**Live capture from many different network media**

Wireshark can capture traffic from many different network media types - and despite its name - including wireless LAN as well. Which media types are supported, depends on many things like the operating system you are using.

**Import files from many other capture programs**

Wireshark can open packets captured from a large number of other capture programs.

The following file formats from other capture tools can be opened by Wireshark:

* libpcap - captures from *Wireshark*/*TShark*/*dumpcap*, *tcpdump*, and various other tools using libpcap's/tcpdump's capture format
* pcap-ng - "next-generation" successor to libpcap format
* Sun snoop and atmsnoop
* Shomiti/Finisar *Surveyor* captures
* Novell *LANalyzer* captures
* Microsoft Network Monitor captures
* AIX's iptrace captures
* Cinco Networks NetXray captures
* Network Associates Windows-based Sniffer and Sniffer Pro captures
* Network General/Network Associates DOS-based Sniffer (compressed or uncompressed) captures
* AG Group/WildPackets EtherPeek/TokenPeek/AiroPeek/EtherHelp/PacketGrabber captures
* RADCOM's WAN/LAN Analyzer captures
* Network Instruments Observer version 9 captures
* Lucent/Ascend router debug output
* HP-UX's nettl
* Toshiba's ISDN routers dump output
* ISDN4BSD *i4btrace* utility
* traces from the EyeSDN USB S0
* IPLog format from the Cisco Secure Intrusion Detection System
* pppd logs (pppdump format)
* the output from VMS's TCPIPtrace/TCPtrace/UCX$TRACE utilities
* the text output from the DBS Etherwatch VMS utility
* Visual Networks' Visual UpTime traffic capture
* the output from CoSine L2 debug
* the output from Accellent's 5Views LAN agents
* Endace Measurement Systems' ERF format captures
* Linux Bluez Bluetooth stack hcidump -w traces
* Catapult DCT2000 .out files
* Gammu generated text output from Nokia DCT3 phones in Netmonitor mode
* IBM Series (OS/400) Comm traces (ASCII & UNICODE)
* Juniper Netscreen snoop captures
* Symbian OS btsnoop captures
* Tamosoft CommView captures
* Textronix K12xx 32bit .rf5 format captures
* Textronix K12 text file format captures
* Apple PacketLogger captures
* Captures from Aethra Telecommunications' PC108 software for their test instruments

**Export files for many other capture programs**

Wireshark can save packets captured in a large number of formats of other capture programs.

The following file formats can be saved by Wireshark (with the known file extensions):

* libpcap, tcpdump and various other tools using tcpdump's capture format (\*.pcap,\*.cap,\*.dmp)
* Accellent 5Views (\*.5vw)
* HP-UX's nettl (\*.TRC0,\*.TRC1)
* Microsoft Network Monitor - NetMon (\*.cap)
* Network Associates Sniffer - DOS (\*.cap,\*.enc,\*.trc,\*fdc,\*.syc)
* Network Associates Sniffer - Windows (\*.cap)
* Network Instruments Observer version 9 (\*.bfr)
* Novell LANalyzer (\*.tr1)
* Sun snoop (\*.snoop,\*.cap)
* Visual Networks Visual UpTime traffic (\*.\*)
* new file formats are added from time to time

**Many protocol decoders**

There are protocol decoders (or dissectors, as they are known in Wireshark) for a great many protocols.

Wireshark distinguishes between protocols (e.g. tcp) and protocol fields (e.g. tcp.port).

**Open Source Software**

Wireshark is an open source software project, and is released under the [GNU General Public License](http://www.gnu.org/copyleft/gpl.html) (GPL). You can freely use Wireshark on any number of computers you like, without worrying about license keys or fees or such. In addition, all source code is freely available under the GPL. Because of that, it is very easy for people to add new protocols to Wireshark, either as plugins, or built into the source, and they often do!

**What Wireshark is not**

Here are some things Wireshark does not provide:

* Wireshark isn't an intrusion detection system. It will not warn you when someone does strange things on your network that he/she isn't allowed to do. However, if strange things happen, Wireshark might help you figure out what is really going on.
* Wireshark will not manipulate things on the network, it will only "measure" things from it. Wireshark doesn't send packets on the network or do other active things (except for name resolutions, but even that can be disabled).

**System Requirements**

**Microsoft Windows**

* Windows XP Home, XP Pro, XP Tablet PC, XP Media Center, Server 2003, Vista, 2008, 7, or 2008 R2
* Any modern 32-bit x86 or 64-bit AMD64/x86-64 processor.
* 128MB available RAM. Larger capture files require more RAM.
* 75MB available disk space. Capture files require additional disk space.
* 800\*600 (1280\*1024 or higher recommended) resolution with at least 65536 (16bit) colors (256 colors should work if Wireshark is installed with the "legacy GTK1" selection of the Wireshark 1.0.x releases)
* A supported network card for capturing:
* Ethernet: Any card supported by Windows should work. See the wiki pages on [Ethernet capture](http://wiki.wireshark.org/CaptureSetup/Ethernet) and [offloading](http://wiki.wireshark.org/CaptureSetup/Offloading) for issues that may affect your environment.
* 802.11: See the Wireshark wiki page