

date visited 9/17/12

IPv4 ✓ IPv6 ✗

## Wireshark

- [Riverbed Technology](#)
- [WinPcap](#)

the world's foremost network protocol analyzer

- [Wireshark »](#)
- [Get Help »](#)
- [Develop »](#)

 

Wireshark Frequently Asked Questions

## Index

### 1. General Questions:

[1.1 What is Wireshark?](#)

[1.2 What's up with the name change? Is Wireshark a fork?](#)

[1.3 Where can I get help?](#)

[1.4 What kind of shark is Wireshark?](#)

[1.5 How is Wireshark pronounced, spelled and capitalized?](#)

[1.6 How much does Wireshark cost?](#)

[1.7 But I just paid someone on eBay for a copy of Wireshark! Did I get ripped off?](#)

[1.8 Can I use Wireshark commercially?](#)

[1.9 Can I use Wireshark as part of my commercial product?](#)

[1.10 What protocols are currently supported?](#)

[1.11 Are there any plans to support {your favorite protocol}?](#)

[1.12 Can Wireshark read capture files from {your favorite network analyzer}?](#)

[1.13 What devices can Wireshark use to capture packets?](#)

[1.14 Does Wireshark work on Windows Vista or Windows Server 2008?](#)

### 2. Downloading Wireshark:

# date visited 9/17/12

[2.1 Why do I get an error when I try to run the Win32 installer?](#)

## **3. Installing Wireshark:**

[3.1 I installed the Wireshark RPM \(or other package\); why did it install TShark but not Wireshark?](#)

## **4. Building Wireshark:**

[4.1 I have libpcap installed; why did the configure script not find pcap.h or bpf.h?](#)

[4.2 Why do I get the error](#)

```
dfptest_DEPENDENCIES was already defined in condition TRUE, which implies  
condition HAVE_PLUGINS_TRUE
```

[when I try to build Wireshark from SVN or a SVN snapshot?](#)

[4.3 Why does the linker fail with a number of "Output line too long." messages followed by linker errors when I try to build Wireshark?](#)

[4.4 When I try to build Wireshark on Solaris, why does the link fail complaining that `plugin\_list` is undefined?](#)

[4.5 When I try to build Wireshark on Windows, why does the build fail because of conflicts between `winsock.h` and `winsock2.h`?](#)

## **5. Starting Wireshark:**

[5.1 Why does Wireshark crash with a Bus Error when I try to run it on Solaris 8?](#)

[5.2 When I run Wireshark on Windows NT, why does it die with a Dr. Watson error, reporting an "Integer division by zero" exception, when I start it?](#)

[5.3 When I try to run Wireshark, why does it complain about `sprint\_realloc\_objid` being undefined?](#)

[5.4 I've installed Wireshark from Fink on Mac OS X; why is it very slow to start up?](#)

## **6. Crashes and other fatal errors:**

[6.1 I have an XXX network card on my machine; if I try to capture on it, why does my machine crash or reset itself?](#)

[6.2 Why does my machine crash or reset itself when I select "Start" from the "Capture" menu or select "Preferences" from the "Edit" menu?](#)

## **7. Capturing packets:**

[7.1 When I use Wireshark to capture packets, why do I see only packets to and from my machine, or not see all the traffic I'm expecting to see from or to the machine I'm trying to monitor?](#)

[7.2 When I capture with Wireshark, why can't I see any TCP packets other than packets to and from my machine, even though another analyzer on the network sees those packets?](#)

# date visited 9/17/12

[7.3 Why am I only seeing ARP packets when I try to capture traffic?](#)

[7.4 Why am I not seeing any traffic when I try to capture traffic?](#)

[7.5 Can Wireshark capture on \(my T1/E1 line, SS7 links, etc.\)?](#)

[7.6 How do I put an interface into promiscuous mode?](#)

[7.7 I can set a display filter just fine; why don't capture filters work?](#)

[7.8 I'm entering valid capture filters; why do I still get "parse error" errors?](#)

[7.9 How can I capture packets with CRC errors?](#)

[7.10 How can I capture entire frames, including the FCS?](#)

[7.11 I'm capturing packets on a machine on a VLAN; why don't the packets I'm capturing have VLAN tags?](#)

[7.12 Why does Wireshark hang after I stop a capture?](#)

## **[8. Capturing packets on Windows:](#)**

[8.1 I'm running Wireshark on Windows; why does some network interface on my machine not show up in the list of interfaces in the "Interface:" field in the dialog box popped up by "Capture->Start", and/or why does Wireshark give me an error if I try to capture on that interface?](#)

[8.2 I'm running Wireshark on Windows; why do no network interfaces show up in the list of interfaces in the "Interface:" field in the dialog box popped up by "Capture->Start"?](#)

[8.3 I'm running Wireshark on Windows; why doesn't my serial port/ADSL modem/ISDN modem show up in the list of interfaces in the "Interface:" field in the dialog box popped up by "Capture->Start"?](#)

[8.4 I'm running Wireshark on Windows NT 4.0/Windows 2000/Windows XP/Windows Server 2003; my machine has a PPP \(dial-up POTS, ISDN, etc.\) interface, and it shows up in the "Interface" item in the "Capture Options" dialog box. Why can no packets be sent on or received from that network while I'm trying to capture traffic on that interface?](#)

[8.5 I'm running Wireshark on Windows; why am I not seeing any traffic being sent by the machine running Wireshark?](#)

[8.6 When I capture on Windows in promiscuous mode, I can see packets other than those sent to or from my machine; however, those packets show up with a "Short Frame" indication, unlike packets to or from my machine. What should I do to arrange that I see those packets in their entirety?](#)

[8.7 I'm trying to capture 802.11 traffic on Windows; why am I not seeing any packets?](#)

[8.8 I'm trying to capture 802.11 traffic on Windows; why am I seeing packets received by the machine on which I'm capturing traffic, but not packets sent by that machine?](#)

[8.9 I'm trying to capture Ethernet VLAN traffic on Windows, and I'm capturing on a "raw" Ethernet device rather than a "VLAN interface", so that I can see the VLAN headers; why am I seeing packets received by the machine on which I'm capturing traffic, but not packets sent by that machine?](#)

# date visited 9/17/12

## **9. Capturing packets on UN\*Xes:**

9.1 I'm running Wireshark on a UNIX-flavored OS; why does some network interface on my machine not show up in the list of interfaces in the "Interface:" field in the dialog box popped up by "Capture->Start", and/or why does Wireshark give me an error if I try to capture on that interface?

9.2 I'm running Wireshark on a UNIX-flavored OS; why do no network interfaces show up in the list of interfaces in the "Interface:" field in the dialog box popped up by "Capture->Start"?

9.3 I'm capturing packets on Linux; why do the time stamps have only 100ms resolution, rather than 1us resolution?

## **10. Capturing packets on wireless LANs:**

10.1 How can I capture raw 802.11 frames, including non-data (management, beacon) frames?

10.2 How do I capture on an 802.11 device in monitor mode?

## **11. Viewing traffic:**

11.1 Why am I seeing lots of packets with incorrect TCP checksums?

11.2 I've just installed Wireshark, and the traffic on my local LAN is boring. Where can I find more interesting captures?

11.3 Why doesn't Wireshark correctly identify RTP packets? It shows them only as UDP.

11.4 Why doesn't Wireshark show Yahoo Messenger packets in captures that contain Yahoo Messenger traffic?

## **12. Filtering traffic:**

12.1 I saved a filter and tried to use its name to filter the display; why do I get an "Unexpected end of filter string" error?

12.2 How can I search for, or filter, packets that have a particular string anywhere in them?

12.3 How do I filter a capture to see traffic for virus XXX?

## **1. General Questions**

Q 1.1: What is Wireshark?

A: Wireshark® is a network protocol analyzer. It lets you capture and interactively browse the traffic running on a computer network. It has a rich and powerful feature set and is world's most popular tool of its kind. It runs on most computing platforms including Windows, OS X, Linux, and UNIX. Network professionals, security experts, developers, and educators around the world use it regularly. It is freely available as open source, and is released under the GNU General Public License version 2.

It is developed and maintained by a global team of protocol experts, and it is an example of a [disruptive technology](#).

Wireshark used to be known as Ethereal®. See the next question for details about the name change. If you're

# date visited 9/17/12

still using Ethereal, it is [strongly recommended that you upgrade to Wireshark](#).

For more information, please see the [About Wireshark](#) page.

Q 1.2: What's up with the name change? Is Wireshark a fork?

A: In May of 2006, Gerald Combs (the original author of Ethereal) went to work for CACE Technologies (best known for WinPcap). Unfortunately, he had to leave the Ethereal trademarks behind.

This left the project in an awkward position. The only reasonable way to ensure the continued success of the project was to change the name. This is how Wireshark was born.

Wireshark is almost (but not quite) a fork. Normally a "fork" of an open source project results in two names, web sites, development teams, support infrastructures, etc. This is the case with Wireshark except for one notable exception -- every member of the core development team is now working on Wireshark. There has been no active development on Ethereal since the name change. Several parts of the Ethereal web site (such as the mailing lists, source code repository, and build farm) have gone offline.

More information on the name change can be found here:

- [Original press release](#)
- [NewsForge article](#)
- Many other articles in [our bibliography](#)

Q 1.3: Where can I get help?

A: Community support is available on the [Q&A site](#) and on the wireshark-users mailing list. Subscription information and archives for all of Wireshark's mailing lists can be found at <https://www.wireshark.org/mailman/listinfo>. An IRC channel dedicated to Wireshark can be found at <irc://irc.freenode.net/wireshark>. Self-paced and instructor-led training is available at [Wireshark University](#). Wireshark University also offers certification via the Wireshark Certified Network Analyst program.

Q 1.4: What kind of shark is Wireshark?

A: *carcharodon photoshopia*.

Q 1.5: How is Wireshark pronounced, spelled and capitalized?

A: Wireshark is pronounced as the word *wire* followed immediately by the word *shark*. Exact pronunciation and emphasis may vary depending on your locale (e.g. Arkansas).

It's spelled with a capital *W*, followed by a lower-case *reshark*. It is not a CamelCase word, i.e., *WireShark* is incorrect.

Q 1.6: How much does Wireshark cost?

A: Wireshark is "free software"; you can download it without paying any license fee. The version of Wireshark you download isn't a "demo" version, with limitations not present in a "full" version; it *is* the full version.

The license under which Wireshark is issued is [the GNU General Public License version 2](#). See [the GNU GPL FAQ](#) for some more information.

Q 1.7: But I just paid someone on eBay for a copy of Wireshark! Did I get ripped off?

A: That depends. Did they provide any sort of value-added product or service, such as installation support, installation media, training, trace file analysis, or funky-colored shark-themed socks? Probably not.

Wireshark is [available for anyone to download, absolutely free, at any time](#). Paying for a copy implies that you should get something for your money.

# date visited 9/17/12

Q 1.8: Can I use Wireshark commercially?

A: Yes, if, for example, you mean "I work for a commercial organization; can I use Wireshark to capture and analyze network traffic in our company's networks or in our customer's networks?"

If you mean "Can I use Wireshark as part of my commercial product?", see [the next entry in the FAQ](#).

Q 1.9: Can I use Wireshark as part of my commercial product?

A: As noted, Wireshark is licensed under [the GNU General Public License](#). The GPL imposes conditions on your use of GPL'ed code in your own products; you cannot, for example, make a "derived work" from Wireshark, by making modifications to it, and then sell the resulting derived work and not allow recipients to give away the resulting work. You must also make the changes you've made to the Wireshark source available to all recipients of your modified version; those changes must also be licensed under the terms of the GPL. See the [GPL FAQ](#) for more details; in particular, note the answer to [the question about modifying a GPLed program and selling it commercially](#), and [the question about linking GPLed code with other code to make a proprietary program](#).

You can combine a GPLed program such as Wireshark and a commercial program as long as they communicate "at arm's length", as per [this item in the GPL FAQ](#).

We recommend keeping Wireshark and your product completely separate, communicating over sockets or pipes. If you're loading any part of Wireshark as a DLL, you're probably doing it wrong.

Q 1.10: What protocols are currently supported?

A: There are currently hundreds of supported protocols and media. Details can be found in the [wireshark\(1\)](#) man page.

Q 1.11: Are there any plans to support {your favorite protocol}?

A: Support for particular protocols is added to Wireshark as a result of people contributing that support; no formal plans for adding support for particular protocols in particular future releases exist.

Q 1.12: Can Wireshark read capture files from {your favorite network analyzer}?

A: Support for particular capture file formats is added to Wireshark as a result of people contributing that support; no formal plans for adding support for particular capture file formats in particular future releases exist.

If a network analyzer writes out files in a format already supported by Wireshark (e.g., in libpcap format), Wireshark may already be able to read them, unless the analyzer has added its own proprietary extensions to that format.

If a network analyzer writes out files in its own format, or has added proprietary extensions to another format, in order to make Wireshark read captures from that network analyzer, we would either have to have a specification for the file format, or the extensions, sufficient to give us enough information to read the parts of the file relevant to Wireshark, or would need at least one capture file in that format **AND** a detailed textual analysis of the packets in that capture file (showing packet time stamps, packet lengths, and the top-level packet header) in order to reverse-engineer the file format.

Note that there is no guarantee that we will be able to reverse-engineer a capture file format.

Q 1.13: What devices can Wireshark use to capture packets?

A: Wireshark can read live data from Ethernet, Token-Ring, FDDI, serial (PPP and SLIP) (if the OS on which it's running allows Wireshark to do so), 802.11 wireless LAN (if the OS on which it's running allows Wireshark to do so), ATM connections (if the OS on which it's running allows Wireshark to do so), and the "any" device supported on Linux by recent versions of libpcap.