

Monitor traffic on a network for free with Ethereal

By David Davis

Takeaway

If you want to monitor traffic on your network, you can purchase a packet analyzer. However if your budget is tight, you don't have to spend any money at all. Here's how you can do so using Ethereal.

Ethereal

What is going on with the network? Why is the network running slow? Who is using all the bandwidth? Do you have unwanted traffic on the network? Why is my network application not working? These are all questions that can drive a network administrator crazy. These are also questions you can answer without breaking your budget with Ethereal.

What is it?

Ethereal is an open source protocol analyzer available for a variety of operating systems. As the source is freely available, it could, theoretically, be compiled on just about any operating system. You can run it on Windows, Linux/Unix, and Mac OS X.

Protocol Analyzers are commonly known as "packet sniffers." Many times they are also called just "sniffers." A Sniffer, however, is a specific brand of commercial (think expensive) protocol analyzer made by [Network General](#). Ethereal, on the other hand is completely free and offers most of the same features. Protocol analyzers are used to troubleshoot the network, analyze what is going on, understand protocol /traffic flow. If you are having a mysterious problem on the network, a protocol analyzer is your best tool. Ethereal is the most popular, freely available, protocol analyzer available.

At this point you may be asking "if this is such a critical tool, why does everyone doesn't have one installed on their PC"? The answer to that is that understanding what a protocol analyzer tells you can be difficult. Actually running the analyzer and clicking through the menus is not difficult. However, understanding the output is. For example, turning on debug mode in Windows might not be too hard but understanding the debug output is. The output you receive from Ethereal could be compared to "debug output."

In other words, Ethereal understands the packets and protocols that are sent across the network and can decode these into a readable, English format for a network administrator to analyze. Ethereal also provides its own intelligent analysis in many instances. This can be Live network data, as it is sent across the network or a saved file that you play back.

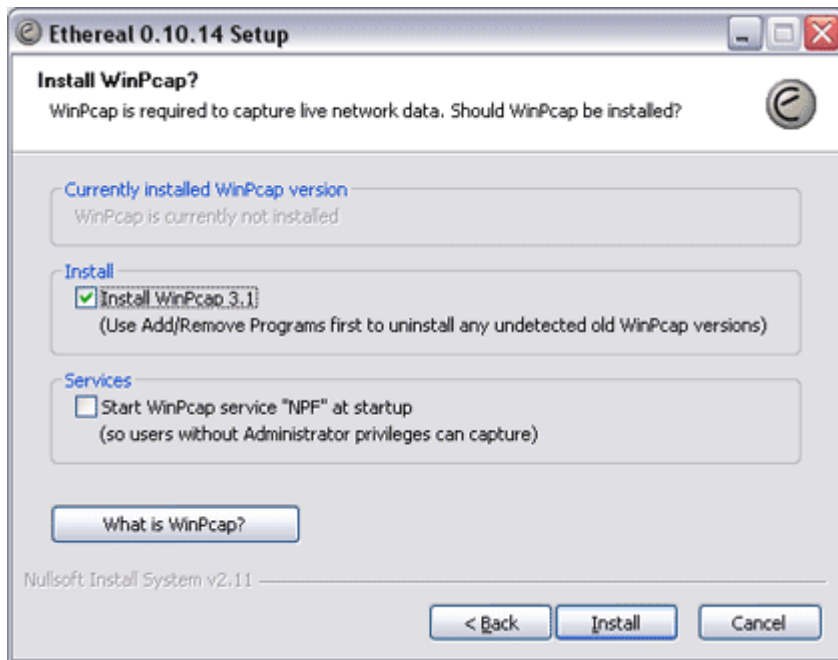
How do you get it?

To obtain a copy of Ethereal for your Windows PC, go to the [Ethereal Web site](#) and click on Download. As you can see, Ethereal can be downloaded in binary format for Windows, Solaris, and Red Hat from this Web site. You can also download the source code. On this same Webpage, there are links to other sites where you can download the binary version for operating systems like Mac OS X, Palm, HP-UX, IBM AIX, and other Linux variants.

Download Ethereal for Windows by clicking the Download button next to Windows. Once you have downloaded Ethereal, click Run, to begin the installation. The installation runs like most Windows Setup Wizards.

The first point where you have a decision to make is shown in **Figure A**. This screen asks you if you want winpcap installed.

Figure A



Deciding what you want to do about Winpcap.

[Winpcap](#) is a library that Ethereal uses for capturing packets without having to go through the operating system's protocol stack. Winpcap must be installed for Ethereal to be able to capture packets off of the network. Click Next to install Winpcap and Ethereal.

After copying files, the Winpcap window shown in **Figure B** will pop up over the Ethereal install window.

Figure B



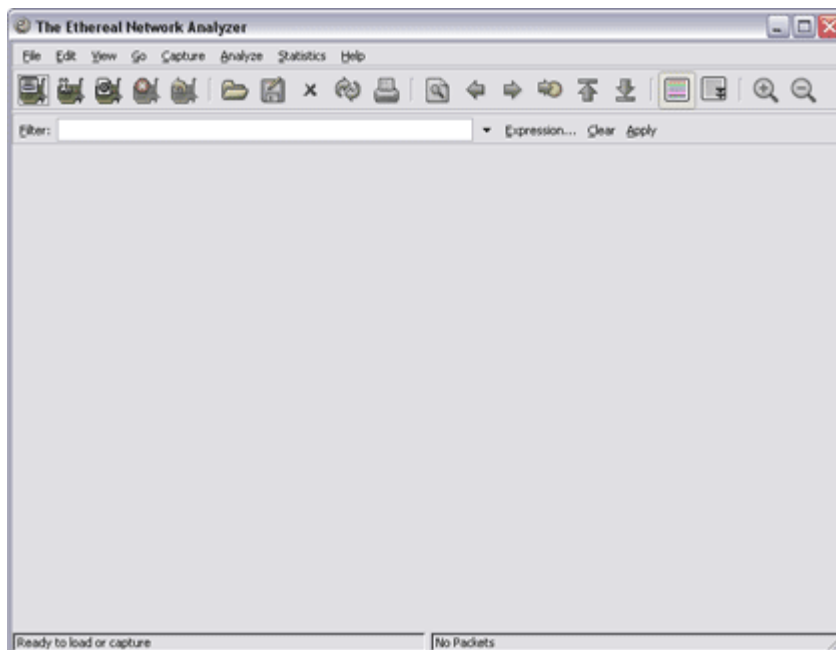
This window appears after you install Winpcap.

Click Next, then click Next, to agree to the license. Winpcap will be installed. When it is done, click Finish and you will be returned to the Ethereal Installation. The Ethereal install will complete by copying files. Click Next. Check the box that says Run Ethereal. Click Finish and the installation is done. Ethereal will now start.

How do you use it?

When Ethereal runs, you will see screen shown in **Figure C**.

Figure C



Ethereal's startup screen is rather plain.

From here, it isn't very obvious what to do. There are full week-long courses on Ethereal. Because of that, this article isn't meant to teach you fully how to use Ethereal. Instead, let me show you how to capture some basic packets off the network.

Keep in mind that a system will only see what packets are sent to it by the switch or hub that it is connected to. In the case of a switch, it is intelligent and only forwards traffic meant for the MAC address of your workstation and broadcast/multicast packets. If you had a hub, you would see all traffic on the network. So, proper placement of your workstation to capture the right amount of packets is critical. Many times, "port mirroring" is enabled on switches to mirror the port with the relevant traffic to your port. For example, you could mirror the core router's Ethernet port to your port.

To capture packets, first select the interface that you want to capture packets from. To do this, click the top left icon on the toolbar that says "List the available capture interfaces." You'll see a window that looks like the one in **Figure D**.

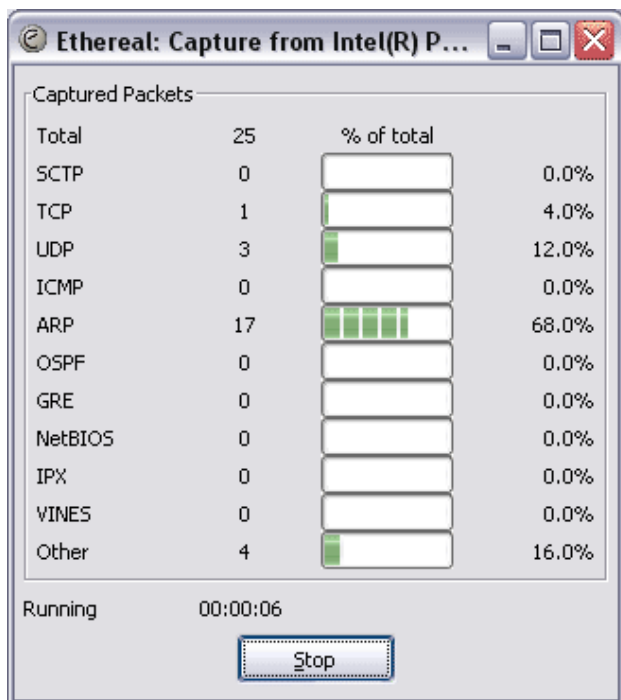
Figure D



Select where you want to capture packets from.

Notice that only one interface is seeing packets. That is because that is my primary network interface and also the interface I want to capture packets from. Click Capture and you'll see a window like the one in **Figure E** showing you the status of the capture.

Figure E

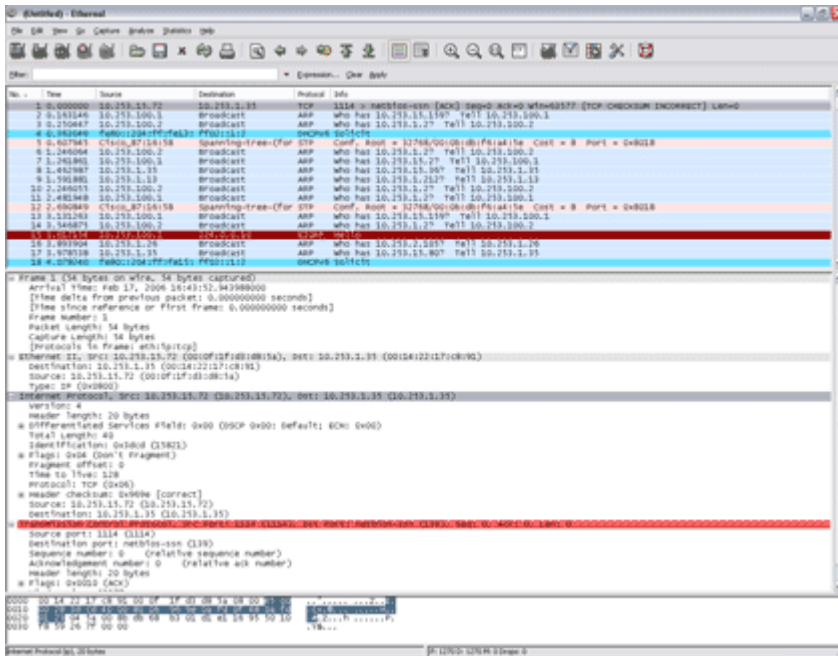


You can track the status of the captures as they go.

How do I: Monitor traffic on a network for free with Ethereal

Once you have some number of packets, click Stop. Your packets will be decoded and available for analysis as seen in **Figure F**.

Figure F



You can view all of the captures [here](#).

If you haven't used a protocol analyzer before, you will have to spend some time learning about them. Ethereal can do so many different things with the traffic. For example, you can see the actual conversation flow, as seen in **Figure G**.

Figure G



You can see many details of traffic, including conversation flow.

Free for all

Ethereal is a very powerful program with so many different uses. It is amazing with all its features and uses that it is still freely available to anyone.

Additional resources

- TechRepublic's [Downloads RSS Feed](#) **XML**
- Sign up for TechRepublic's [Downloads Weekly Update](#) newsletter
- Sign up for TechRepublic's [Network Administration NetNote](#) newsletter
- Check out all of TechRepublic's [free newsletters](#)
- Catch up with all the [How do I](#) articles on TechRepublic.

Version history

Version: 1.0

Published: November 9, 2006

Tell us what you think

TechRepublic downloads are designed to help you get your job done as painlessly and effectively as possible. Because we're continually looking for ways to improve the usefulness of these tools, we need your feedback. Please take a minute to [drop us a line](#) and tell us how well this download worked for you and offer your suggestions for improvement.

Thanks!

—The TechRepublic Downloads Team