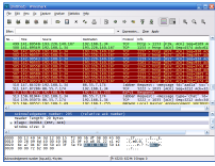


19 July 2006

By: Codrut Nistor, Editor, Software Reviews



Uncover Your Network's Secrets!

Wireshark can capture all your network traffic

All that belongs to the networking field was out of my reach for a long time, especially because I didn't have a home connection. After this problem was solved, I started to slowly gather information about computer networks terminology, but the greatest helpers have been programs like X-NetStat or Ethereal. Since I named Ethereal, I must say that this program is still around, but under a different cover. The former Ethereal is now known as Wireshark, it recently reached version 0.99.2 and it's my current target. The installation kit of this program is 12.5MB in size. During the setup process I advise you to pay attention to the hints displayed, since learning about WinPcap can't do you any harm. After the main setup process ends, WinPcap install program will start automatically, if you have chosen to install it, of course. Before getting to the program's interface and features, I must tell you more about what it does. Wireshark lets you interactively browse packet data from a live network or from a previously saved capture file. Network managers can use it for a lot of purposes, such as intrusion detection and traffic monitoring, while home users can use it for educational purposes, like getting to know network protocol internals. Even developers have their purpose in using this program, and that is to debug protocol implementations. The program's interface looks nice and up to date, while using it is not a child's play. The menus are well organized, and you can choose from six available interface layouts, but most of the terms that you meet inside Wireshark require some study. The resources from the official website are a great way to start, because the program's help is really basic, and doesn't clear things as it should. In order to display packets data, you have to capture it from one of your live network connections or load an existing capture file. This can be easily accomplished using the Capture menu's Start item. When you press the Stop button, the captured data is loaded into the program automatically. Each packet has its own structure, depending on the protocol it uses. Wireshark supports an impressive number of protocols and can also use (open and save) a large number of formats of other capture programs. Once the packets data is loaded, you can filter it using the filter toolbar and check the details displayed in the packet details and packet bytes panes. All you have to do is click the packet you're interested in from the packet list pane and you'll have the details loaded into the packet details area. In order to filter packed data you can use advanced filter expressions that can contain English language terms and C programming language operators. For each of the existing protocols you have different attributes that can be used to get the best out of this feature. Of course that filters can be saved and loaded as needed, this is a serious application, and if it misses something, apart from a good built in Help system, then this is up for the networking experts to decide... There are a lot of things to be said and done when talking about this subject, and all I can do now is recommend you to check out the online user guide, where you will get a lot of useful details and examples about it. Once you have captured some packets, you can find the desired ones using the Find Packet dialog box. Here you can enter manually filter expressions, and this feature can be seen as a stripped-down version of the mighty Filter Expression. Now let's check out some really advanced topics before drawing any conclusions. Yes, it's not a mistake, I wrote "really advanced", and what can be more advanced compared to the things done so far, this is what we have to see. The advanced features of Wireshark begin with Following TCP Streams and end with Name Resolution and Checksums. People who know already what these are about will be very pleased to find them here, while the others should read the user guide, while I get back to the last basic features of this program that need to be mentioned here. Graphics and statistics, how was I to forget about them? Wireshark doesn't involve

actively into your traffic, it acts only as an observer. The command center of the statistic features is the Statistics menu. Here you can get all the data you ever dreamed of, in numeric form, but you can also view highly customizable IO Graphs. This program is a real gem, and all I can do is bow down before the power of another excellent free application which proves once again that most good things in life are priceless. **The Good** Dissecting network traffic is never an easy task, but Wireshark makes it a little easier than usual. This program is extremely powerful, highly customizable and comes for free. **The Bad** From my point of view, the only bad thing about this program is its weak built in Help system, which may keep it away from some people. I also noticed some small latency from time to time when issuing commands, but it's not really bothering. **The Truth** I don't recommend this program to most beginners, but any computer user that will get his hands on Wireshark will find something new to learn. All you have to do is take on this challenge. Will you do it or not? *Here are some snapshots of the application in action:*