# 6. INTRODUCTION TO THE LABORATORY: SOFTWARE TOOLS

## 6.1. Wireshark – network sniffer

Wireshark (originally called Ethereal) is a freeware network sniffer. A sniffer investigates and analyzes network traffic. It gives administrators the opportunity to recognize weaknesses and vulnerabilities in the network and quickly find a way to resolve problems.

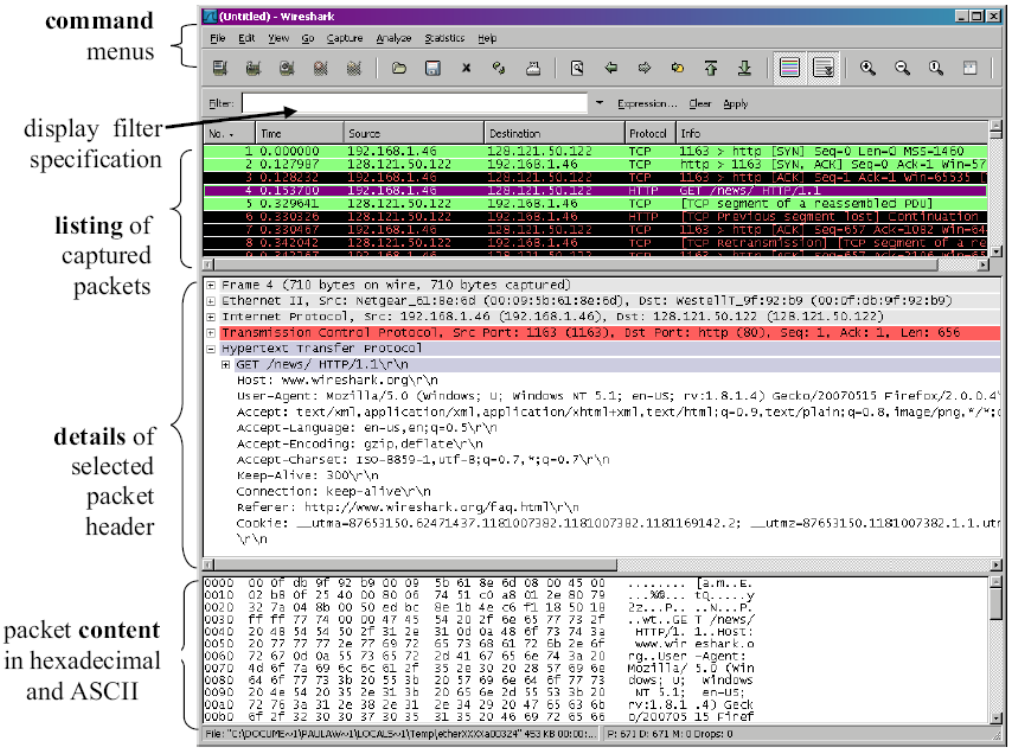


Fig. 6.1 Wireshark GUI

Wireshark is very similar to *tcpdump* (a common packet analyzer that runs from the command line), but Wireshark has a graphical front-end, and many more information sorting and filtering options. Wireshark allows the user to see all traffic being passed over the network by putting the network interface into promiscuous mode (configuration of a network card that makes the card pass all traffic it receives to the central processing unit rather than just frames addressed to it).

## 6.2. Wireshark features

Wireshark is software that "understands" the structure of different networking protocols. Thus, it is able to display the encapsulation and the fields, together with their meanings, of different packets specified by different networking protocols. Wireshark uses packet capture (pcap) to capture packets, so it can only capture the packets on the types of networks that pcap supports.

- Data can be captured "from the wire" from a live network connection or read from a file that has recorded already-captured packets.
- Live data can be read from a number of types of network, including Ethernet, IEEE 802.11, PPP, and loopback.
- Captured network data can be browsed via a GUI, or via the terminal (command line) version of the utility, tshark.
- Captured files can be programmatically edited or converted via command-line switches to the "editcap" program.
- Data display can be refined using a display filter.
- Plug-ins can be created for dissecting new protocols.
- VoIP calls in the captured traffic can be detected. If encoded in a compatible encoding the media flow can even be played.
- Raw USB traffic can be captured with Wireshark. This feature is currently available only under Linux.

## 6.3. Tutorial

1. Download and install the software. The latest version (1.4.1 at the time of writing) is available for downlad from the official site http://www.wireshark.org/download.html

2. Once Wireshark is installed, start it up and you'll be presented with the blank screen shown below in Figure 6.2.

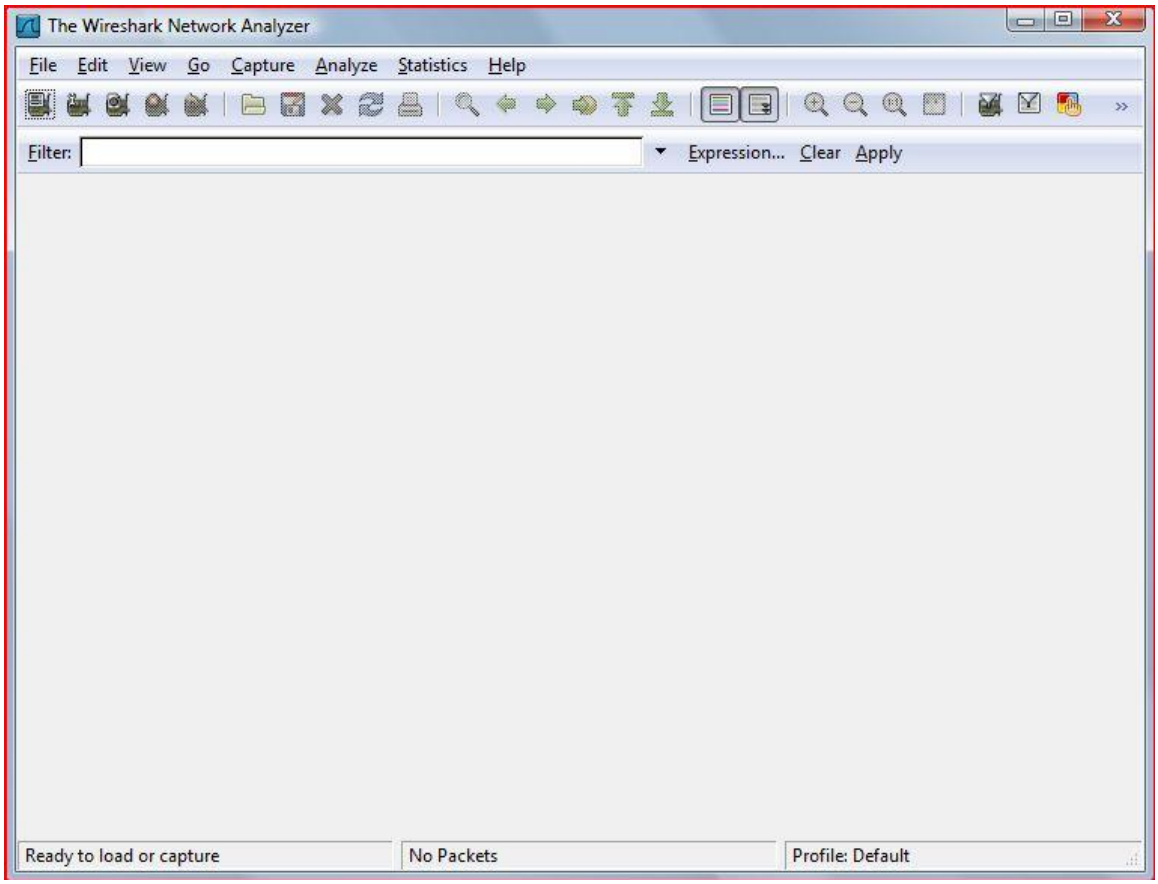


Fig. 6.2 The Wireshark screen after startup

3. To start scanning, choose Interfaces from the Capture menu. You'll see a pop-up window similar to the one below (Figure 6.3).

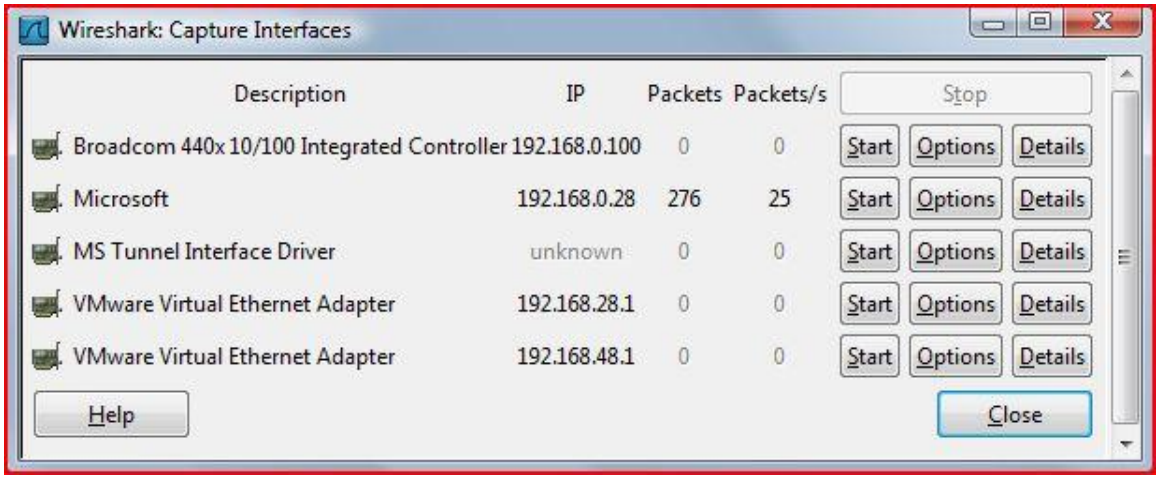


Fig. 6.3 The pop-up window

If you'd like to configure advanced options -- like capturing a file, resolving MAC addresses and DNS names, or limiting the time or size of the capture -- click the Options button corresponding to the interface you wish to configure. Many of these options can help to improve the performance of Wireshark. For example, you can adjust settings to avoid name-resolution issues, as they will otherwise slow down your capture system and generate large numbers of name queries. Time and size limits can also place limitations on unattended captures. Otherwise, simply click the Start button next to the name of the interface on which you wish to capture traffic.

4. The Wireshark screen will immediately begin filling up with traffic seen on the network interface, as shown below in Figure 6.4.

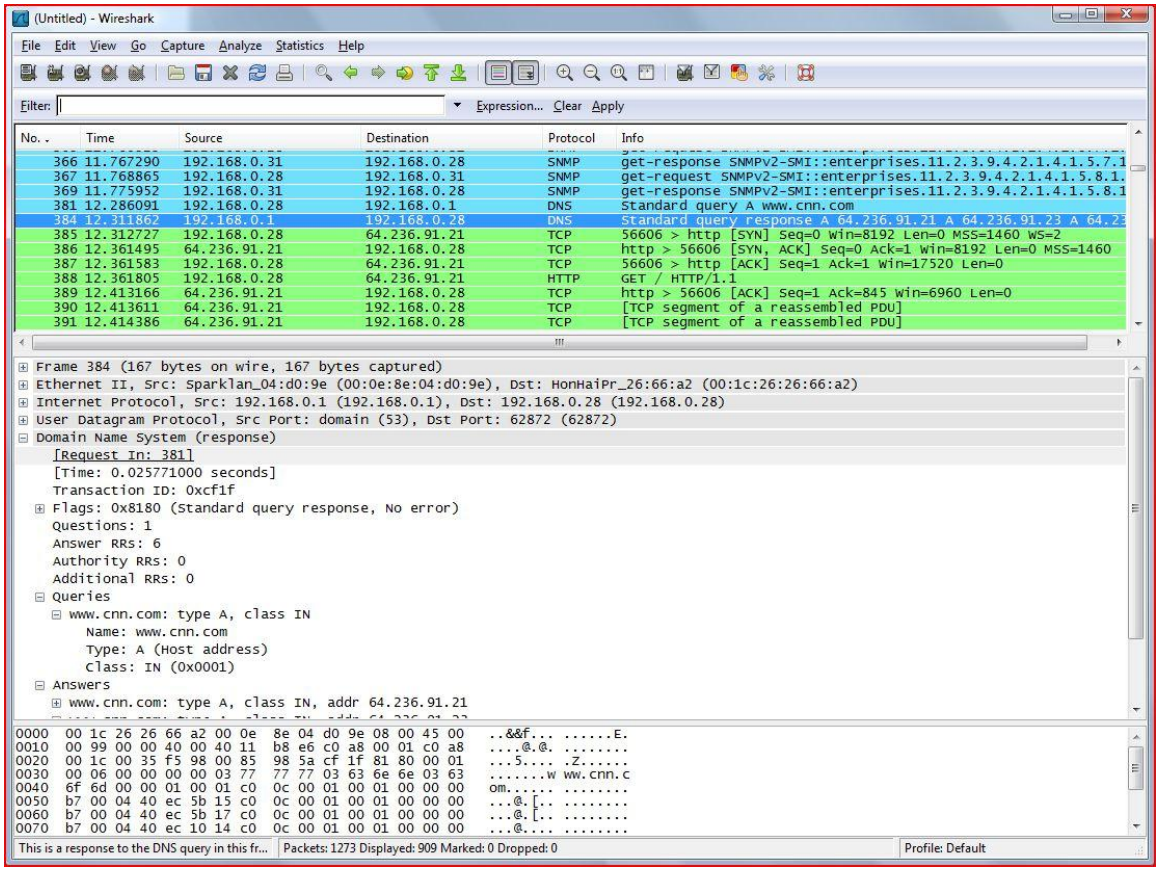


Fig. 6.4 The Wireshark interface showing network traffic

Each line in the top pane of the Wireshark window corresponds to a single packet seen on the network. The default display shows the time of the packet (relative to the initiation of the capture), the source and destination IP addresses, the protocol used and some information about the packet. You can drill down and obtain more information by clicking on a row. This causes the bottom two window panes to fill with information.

The middle pane contains drill-down details on the packet selected in the top frame. The "+" icons reveal varying levels of detail about each layer of information contained within the packet. In the example above a DNS response packet was selected. The DNS response (application layer) section of the packet is expanded to show that the original was requesting a DNS resolution for www.cnn.com, and this response is informing us that the available IP addresses include 64.236.91.21. The bottom window pane shows the contents of the packet in both hexadecimal and ASCII representations.

5. Color is your friend when analyzing packets with Wireshark. Notice in the example above that each row is color-coded. The darker blue rows correspond to DNS traffic, the lighter blue rows are UDP SNMP traffic, and the green rows signify HTTP traffic. Wireshark includes a complex color-coding scheme (which you can customize). Figure 6. 5 shows the default settings.

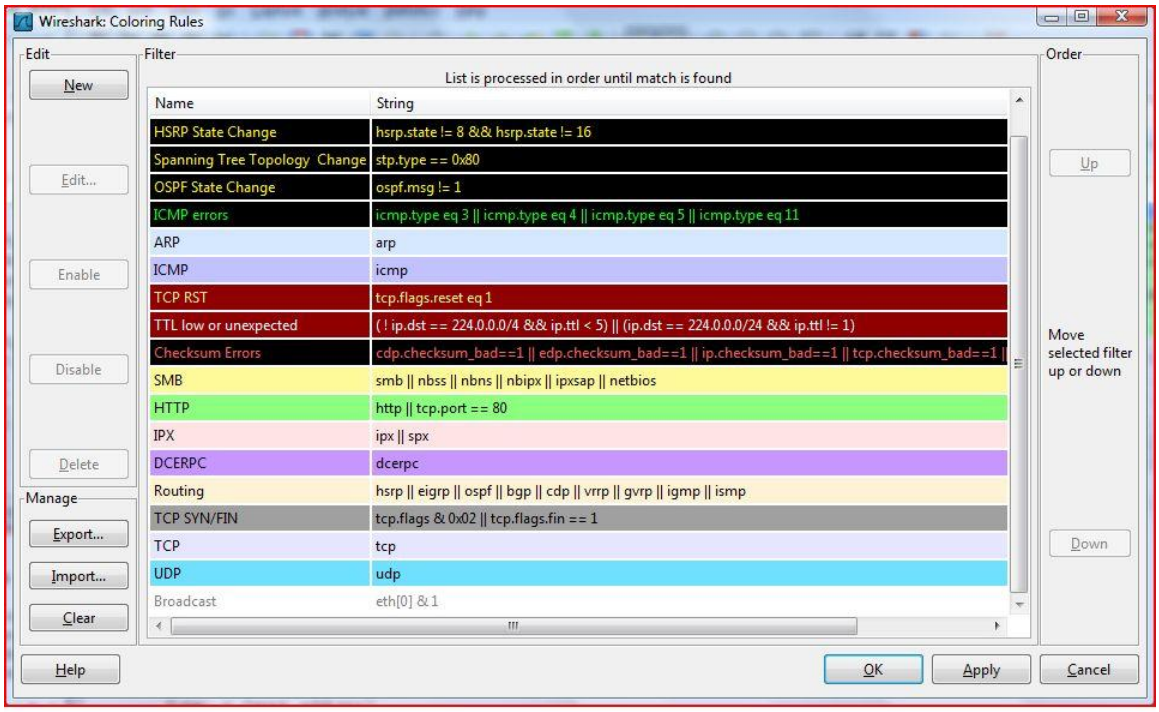


Fig. 6. 5 The Wireshark default settings

## 6.1. Further reading and references

I've put these in alphabetical order

Are they References or Further reading or Bibliography

If the date is the publication date it is usually enough just to put the year.

It isn't necessary to give the ISBN – although it helps.

Chappell, L. & Combs, G. (March 31, 2010). *Wireshark Network Analysis: The Official Wireshark Certified Network Analyst Study Guide*. Protocol Analysis Institute, dba

Chappell University. p. 800.  This means "page 800" If you want to say the book has 800 pages you need to write "pp. 800. ISBN 1893939995

Orebaugh, A., Ramirez, G. & Beale, J. (February 14, 2007). *Wireshark & Ethereal Network Protocol Analyzer Toolkit*. Syngress. p. 448.As above – pp. 448. Also who is the publisher? or is it available from the website you write below? ISBN 1597490733. http://www.syngress.com/hacking-and-penetration-testing/Wireshark-amp-Ethereal-Network-Protocol-Analyzer-Toolkit/

Sanders, C. (May 23, 2007). *Practical Packet Analysis: Using Wireshark to Solve Real-World Network Problems*. No Starch Press. p. 192. ISBN 1593271492. http://nostarch.com/packet.htm  As above.

**Author:** Tomasz Miklis