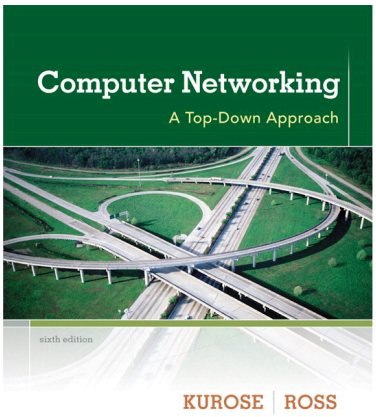
Wireshark Lab: Getting Started v6.0



Supplement to *Computer Networking: A Top-Down Approach, 6th ed.,* J.F. Kurose and K.W. Ross

"Tell me and I forget. Show me and I remember. Involve me and I understand." Chinese proverb

---

One's understanding of network protocols can often be greatly deepened by "seeing protocols in action" and by "playing around with protocols" – observing the sequence of messages exchanged between two protocol entities, delving down into the details of protocol operation, and causing protocols to perform certain actions and then observing these actions and their consequences. This can be done in simulated scenarios or in a "real" network environment such as the Internet. In the Wireshark labs you'll be doing in this course, you'll be running various network applications in different scenarios using your own computer (or you can borrow a friends; let me know if you don't have access to a computer where you can install/run Wireshark). You'll observe the network protocols in your computer "in action," interacting and exchanging messages with protocol entities executing elsewhere in the Internet. Thus, you and your computer will be an integral part of these "live" labs. You'll observe, and you'll learn, by doing.

In this first Wireshark lab, you'll get acquainted with Wireshark, and make some simple packet captures and observations.

The basic tool for observing the messages exchanged between executing protocol entities is called a **packet sniffer**. As the name suggests, a packet sniffer captures ("sniffs") messages being sent/received from/by your computer; it will also typically store and/or display the contents of the various protocol fields in these captured messages. A packet sniffer itself is passive. It observes messages being sent and received by applications and protocols running on your computer, but never sends packets itself. Similarly, received packets are never explicitly addressed to the packet sniffer. Instead, a packet sniffer receives a *copy* of packets that are sent/received from/by application and protocols executing on your machine.

Figure 1 shows the structure of a packet sniffer. At the right of Figure 1 are the protocols (in this case, Internet protocols) and applications (such as a web browser or ftp client) that normally run on your computer. The packet sniffer, shown within the dashed rectangle in Figure 1 is an addition to the usual software in your computer, and consists

of two parts. The **packet capture library** receives a copy of every link-layer frame that is sent from or received by your computer. Recall from the discussion from section 1.5 in the text (Figure 1.24[1]) that messages exchanged by higher layer protocols such as HTTP, FTP, TCP, UDP, DNS, or IP all are eventually encapsulated in link-layer frames that are transmitted over physical media such as an Ethernet cable. In Figure 1, the assumed physical media is an Ethernet, and so all upper-layer protocols are eventually encapsulated within an Ethernet frame. Capturing all link-layer frames thus gives you all messages sent/received from/by all protocols and applications executing in your computer.

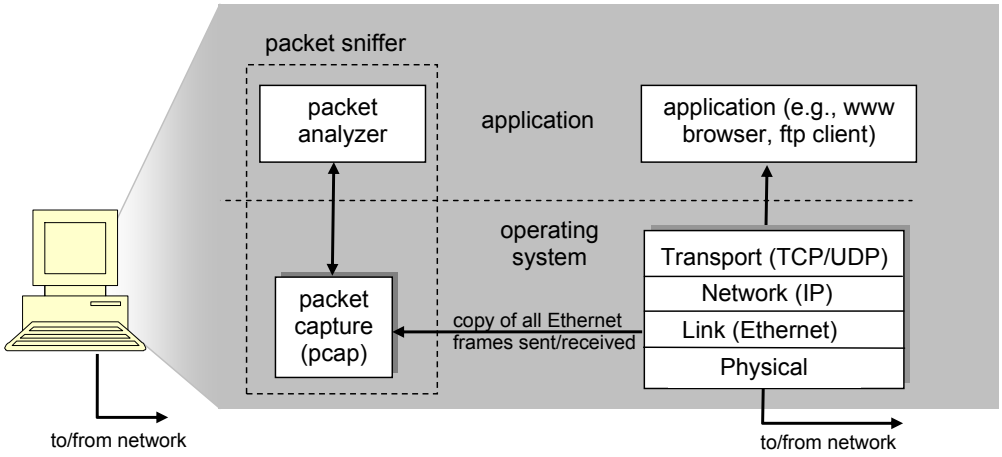


Figure 1: Packet sniffer structure

The second component of a packet sniffer is the **packet analyzer**, which displays the contents of all fields within a protocol message. In order to do so, the packet analyzer must "understand" the structure of all messages exchanged by protocols. For example, suppose we are interested in displaying the various fields in messages exchanged by the HTTP protocol in Figure 1. The packet analyzer understands the format of Ethernet frames, and so can identify the IP datagram within an Ethernet frame. It also understands the IP datagram format, so that it can extract the TCP segment within the IP datagram. Finally, it understands the TCP segment structure, so it can extract the HTTP message contained in the TCP segment. Finally, it understands the HTTP protocol and so, for example, knows that the first bytes of an HTTP message will contain the string "GET," "POST," or "HEAD," as shown in Figure 2.8 in the text.

We will be using the Wireshark packet sniffer [http://www.wireshark.org/] for these labs, allowing us to display the contents of messages being sent/received from/by protocols at different levels of the protocol stack. (Technically speaking, Wireshark is a packet analyzer that uses a packet capture library in your computer). Wireshark is a free network protocol analyzer that runs on Windows, Linux/Unix, and Mac computers. It's an ideal packet analyzer for our labs – it is stable, has a large user base and well-documented support that includes a user-guide (http://www.wireshark.org/docs/wsug_html_chunked/),

[1] References to figures and sections are for the 6th edition of our text, *Computer Networks, A Top-down Approach, 6th ed., J.F. Kurose and K.W. Ross, Addison-Wesley/Pearson, 2012.*

man pages (http://www.wireshark.org/docs/man-pages/), and a detailed FAQ (http://www.wireshark.org/faq.html), rich functionality that includes the capability to analyze hundreds of protocols, and a well-designed user interface. It operates in computers using Ethernet, serial (PPP and SLIP), 802.11 wireless LANs, and many other link-layer technologies (if the OS on which it's running allows Wireshark to do so).

Getting Wireshark

In order to run Wireshark, you will need to have access to a computer that supports both Wireshark and the *libpcap* or *WinPCap* packet capture library. The *libpcap* software will be installed for you, if it is not installed within your operating system, when you install Wireshark. See http://www.wireshark.org/download.html for a list of supported operating systems and download sites

Download and install the Wireshark software:

- Go to http://www.wireshark.org/download.html and download and install the Wireshark binary for your computer.

The Wireshark FAQ has a number of helpful hints and interesting tidbits of information, particularly if you have trouble installing or running Wireshark.

Running Wireshark

When you run the Wireshark program, you'll get a startup screen, as shown below:

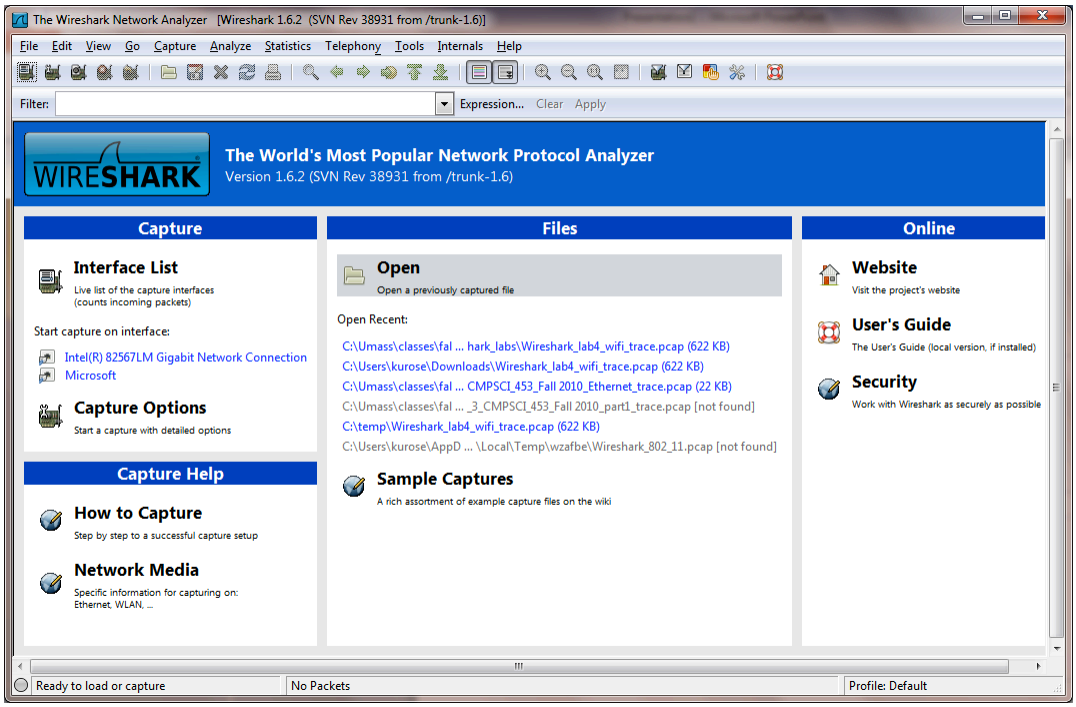


Figure 2: Initial Wireshark Screen

Take a look at the upper left hand side of the screen – you'll see an "Interface list". This is the list of network interfaces on your computer. Once you choose an interface, Wireshark will capture all packets on that interface. In the example above, there is an Ethernet interface (Gigabit network Connection) and a wireless interface ("Microsoft").

If you click on one of these interfaces to start packet capture (i.e., for Wireshark to begin capturing all packets being sent to/from that interface), a screen like the one below will be displayed, showing information about the packets being captured. Once you start packet capture, you can stop it by using the Capture pull down menu and selecting Stop.

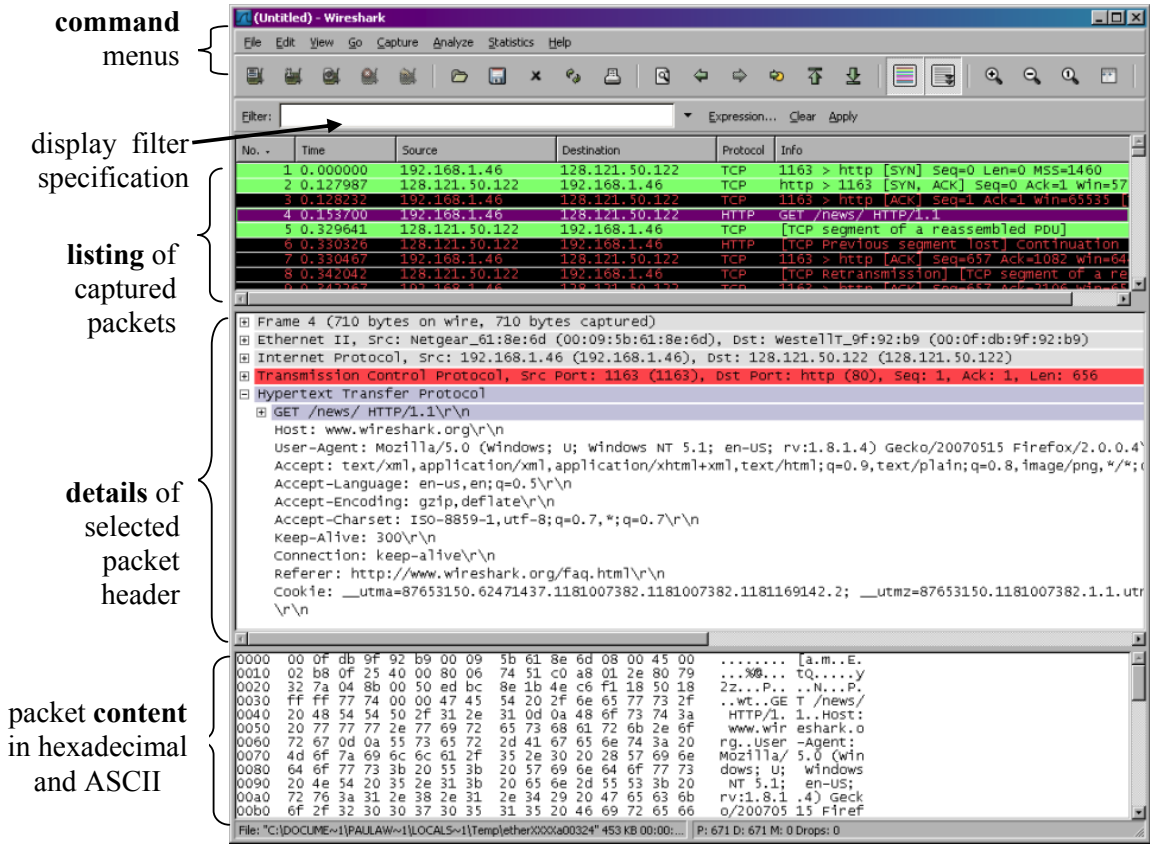


Figure 3: Wireshark Graphical User Interface, during packet capture and analysis

The Wireshark interface has five major components:

- The **command menus** are standard pulldown menus located at the top of the window. Of interest to us now are the File and Capture menus. The File menu allows you to save captured packet data or open a file containing previously captured packet data, and exit the Wireshark application. The Capture menu allows you to begin packet capture.

- The **packet-listing window** displays a one-line summary for each packet captured, including the packet number (assigned by Wireshark; this is *not* a packet number contained in any protocol's header), the time at which the packet was captured, the packet's source and destination addresses, the protocol type, and protocol-specific information contained in the packet. The packet listing can be sorted according to any of these categories by clicking on a column name. The protocol type field lists the highest-level protocol that sent or received this packet, i.e., the protocol that is the source or ultimate sink for this packet.
- The **packet-header details window** provides details about the packet selected (highlighted) in the packet-listing window. (To select a packet in the packet-listing window, place the cursor over the packet's one-line summary in the packet-listing window and click with the left mouse button.). These details include information about the Ethernet frame (assuming the packet was sent/received over an Ethernet interface) and IP datagram that contains this packet. The amount of Ethernet and IP-layer detail displayed can be expanded or minimized by clicking on the plus minus boxes to the left of the Ethernet frame or IP datagram line in the packet details window. If the packet has been carried over TCP or UDP, TCP or UDP details will also be displayed, which can similarly be expanded or minimized. Finally, details about the highest-level protocol that sent or received this packet are also provided.
- The **packet-contents window** displays the entire contents of the captured frame, in both ASCII and hexadecimal format.
- Towards the top of the Wireshark graphical user interface, is the **packet display filter field,** into which a protocol name or other information can be entered in order to filter the information displayed in the packet-listing window (and hence the packet-header and packet-contents windows). In the example below, we'll use the packet-display filter field to have Wireshark hide (not display) packets except those that correspond to HTTP messages.

ELECTRICAL SAFETY RULES FOR ELECTRICAL ENGINEERING LABORATORIES

(Safety Committee, Electrical Department UET Lahore)

1. For experiments where the voltages are 50 V AC (RMS)/DC or higher there should be at least two students in the laboratory and they must be supervised by either an instructor or a laboratory staff.
2. Switch off power by operating an associated switch or a circuit breaker before working on a circuit. It is a good practice to unplug the power cord from the source.
3. Complete your wiring, think about it, discuss it with your partners and re-check before switching power on. If unsure, ask an instructor or a laboratory staff.
4. Any alteration/modification in the circuit must only be done after the power to the circuit has been switched off (point 2).
5. When working with energised circuits, always use one hand: the other hand must be at your back. Think about this: it is absolutely important for your safety. It will save from possible electrocution.
6. After completing an experiment, switch off the power before dismantling the circuit.
7. Switch off power before checking or replacing a fuse. Identify and correct the cause of a blown-up fuse or a tripped circuit breaker before replacing the fuse or re-setting the circuit breaker.
8. Do not use damaged cords/leads, cords/leads which become hot or cords/leads with exposed wiring. Report to the laboratory staff if this happens.
9. If measurements must be made on live or energised circuits, use well-insulated meter probes. Remember: work with only one hand!
10. Use extension cords when necessary, and only on a temporary basis. Do not join leads together to make a longer lead/connection in a circuit.
11. Do not come to a laboratory wearing a chappal or slippers. The students working with electrical machines or with other rotating parts should not wear loose clothes.
12. Do not bring and consume edible items and drinks/beverages in a laboratory.
13. Avoid working with wet hands and clothing.
14. You should remove loose metallic bangles, bracelets, necklaces, ear rings and watchstraps before working on an electrical circuit. You should not have long loose hair as well!
15. Always check the electrical ratings of the equipment you work on and make sure you operate it within its ratings.
16. Never over-load an electrical circuit.
17. The fuses and circuit breakers must never be by-passed. Never replace a low-current fuse with a higher current rating fuse.
18. Make sure chassis or cabinets are grounded.
19. Safely discharge capacitors in equipment before working on a circuit.

Electrical Emergency Response

- It is the duty of a laboratory director, instructor and laboratory staff to make the students aware of the available Emergency Power-Off arrangement in their laboratory, and when and how they should operate it.

Dr. Muhammad Asghar Saqib
Convener, Department's Safety Committee

LABORATORY SAFETY RULES

(Safety Committee, Electrical Department UET Lahore)

The following general rules and safeguards should be followed always in the EED laboratories.

Administrative

1. Do not block access to these electrical panels/boards and shut-off switches.
2. Smoking is prohibited.
3. No food or drinks allowed.
4. Do not run or engage in reckless behavior.
5. Wear Personal Protective Equipment (PPE) if required.
6. Work space should be clear of unnecessary material such as extra books, papers, purses, and clothes.
7. Never wear rings, watches, bracelets, necklaces, or other electrically conductive jewelry.
8. No chatting or gaming is allowed
9. Inappropriate use of Internet (chatting, gaming and pornography etc.) is strictly prohibited.

Electrical safety

1. Working alone and unsupervised is forbidden unless getting permission from HSE incharge, security incharge, and safety officer.
2. When checking an operating circuit, keep one hand either in a pocket or behind your back to prevent current from passing through your chest cavity and injuring your heart.
3. Be familiar with the electrical hazards associated with your workplace.
4. Avoid contacting circuits with wet hands or wet materials.
5. Use electrical cords only if they are in good condition.
6. Avoid being grounded. Stay at least 6 inches away from all metal materials, walls, and water sources.
7. When unplugging a power cord, pull on the plug, not on the cable.
8. Follow lockout-tag out safety procedure.
9. Equipment found to be faulty in any way should be reported to the lab incharge immediately.
10. When attaching a high voltage power supply always switch off the supply.
11. When disassembling a circuit, first remove the source of power.

Emergency Response

1. Be familiar with emergency phones, fire alarm posters, emergency exit routes, first aid boxes, evacuation plans, eye wash, assembly points, and location of fire extinguishers.
2. Inform your lab instructor immediately after any incident, injury, fire or explosion.

Common Sense

1. It is better not to touch anything with which you are not familiar.
2. Your personal laboratory safety depends mostly on you.

Safety Committee Documents

Issued By: HSE Incharge

Approved By: Chairman