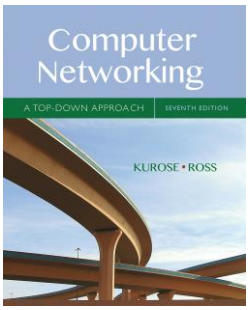

Supplements: Wireshark Labs

Computer Networking: A Top-Down Approach, 7th 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

---

A note on the use of these Wireshark Labs. We're making these Wireshark labs freely available to all (faculty, students, readers). They're available in both Word and PDF so you can add, modify, and delete content to suit your needs.
They obviously represent a ***lot*** of work on our part. In return for use, we only ask the following:

- If you use these labs (e.g., in a class) that you mention their source (after all, we'd like people to use our book!)
- If you post any labs on a www site, that you note that they are adapted from (or perhaps identical to) our labs,

and note our copyright of this material.

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 exchanges 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. The Java applets in the textbook Web site take the first approach. In these Wireshark labs, we'll take the latter approach. You'll be running various network applications in different scenarios using a computer on your desk, at home, or in a lab. 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.
The basic tool for observing the messages exchanged between executing protocol entities is called a packet sniffer. As the name suggests, a packet sniffer passively copies ("sniffs") messages being sent from and received by your computer; it will also display the contents of the various protocol fields of these captured messages. For these labs, we'll use the Wireshark packet sniffer. Wireshark is a free/shareware packet sniffer (a follow-on to the earlier Ethereal packet sniffer) that runs on Windows, Linux/Unix, and Mac computers. The Wireshark labs below will allow you to explore many of the Internet most important protocols.

Wireshark labs: click on the links below to download a Wireshark lab on the given topic.

- Getting Started, v7.0 (PDF, Word)
- HTTP, v7.0 (PDF, Word)
- DNS, v7.01 (PDF, Word)
- TCP, v7.0 (PDF, Word)
- UDP, v7.0 (PDF, Word)
- IP, v7.0 (PDF, Word)
- NAT, v7.0 (PDF, Word)
- ICMP, v7.0 (PDF, Word)
- Ethernet and ARP, v7.0 (PDF, Word)
- DHCP, v7.0 (PDF, Word)
- 802.11, v7.0 (PDF, Word)
- SSL, v7.0 (PDF, Word)
- trace files: wireshark-traces.zip

A zip file containing all of the PDF and Word documents above is here.

comments to kurose at cs.umass.edu