1. **Wireshark Lab: Exploring TCP**

In this lab, you’ll use your Web browser to access a file from a Web server. As in earlier Wireshark labs, you’ll use Wireshark to capture the packets arriving at your computer. You’ll *also* be able to download a Wireshark-readable packet trace from the Web server from which you downloaded the file. In this server trace, you’ll find the packets that were generated by your own access to the Web server. You’ll analyze the client- and server-side traces to explore aspects of TCP. In particular, you’ll evaluate the performance of the TCP connection between your computer and the Web server. You’ll trace TCP’s window behavior, and infer packet loss, retransmission, flow control, and congestion control behavior, and estimated roundtrip time.

As is the case with all Wireshark labs, the full description of this lab is available at this book’s Web site, http://www.awl.com/kurose-ross.

**Requirements:**

**Divide yourself into group of 10**

**1. Install Apache web server or any server of your choice in one of the computers**

**2. Install wireshark application in one of the computers**

**3. create a simple html form and store it in directory var / www / html of the apache server**

**4. create a network of computers by using hotspot or wired net, and share the ip of the computer with the apache web server**

**5. access the web server using the ip address shared**

**6. use wireshark to do the task**

1. **Wireshark Lab: Exploring UDP**

In this short lab, you’ll do a packet capture and analysis of your favorite application that uses UDP (for example, DNS or a multimedia application such as Skype). As we learned, UDP is a simple, no-frills transport protocol. In this lab, you’ll investigate the header fields in the UDP segment as well as the checksum calculation.

As is the case with all Wireshark labs, the full description of this lab is available at this book’s Web site, http://www.awl.com/kurose-ross.

**Requirements:**

**1. By using the same procedures above open wireshark and explore UDP by using drop down options to do the task**