**Lab Exercise 1 Protocol Analysis**

This exercise is intended to deepen your understanding of the Internet protocols you are studying. You will examine real-world networks in action by recording packets as they are sent and received, and use a tool called a protocol analyzer to inspect the packets in detail.

**Objectives**

* Get familiar with Ethereal or Wireshark to analyze protocols.
* To learn how protocols and layering are represented in packets.

**Requirements**

* Capture a trace (to and from the computer) and explore the details of Ethernet frames and TCP/IP protocols, focusing on the packet format and encapsulation of Ethernet, IP, ARP, ICMP, UDP, TCP, and HTTP.
* Hand in trace file and exercise reports.

**Working through the Lab**

This lab exercise includes 10 labs. Each lab covers a different Internet protocol. We suggest you do them in the following order:

1. Ethernet.
2. IPv4.
3. ICMP.
4. ARP.
5. DHCP.
6. UDP.
7. TCP.
8. DNS.
9. HTTP.

However, the labs are relatively independent, and you may choose different orderings to suit your situation. They may also be taken “top down” instead of “bottom up” after the introductory lab.

**Tools**

All of the labs use the Ethereal or Wireshark network protocol analyzer to inspect packet traces.

Different labs also use different tools depending on their purpose. Each lab begins by listing the tools that it uses, a small number of which you may need to install. The tools include: wget/curl and your web browser to fetch web pages; ping and traceroute to probe network paths; operating system utilities such as ipconfig, ifconfig, arp, netstat and route to check and manipulate the state of your computer’s network interface; telnet to send and receive interactive traffic; and dig to examine the DNS.