

Lab 2a – Getting Started with Wireshark

Objectives:

- Familiarizing yourself with the network protocol analyzer
- To start gaining an deeper insight to protocols
- **Read the entire package and the instructions very clearly**

Background

Gerald Combs (a computer science graduate of the University of Missouri-Kansas City) started writing a program called Ethereal so that he could have a tool to capture and analyze packets

First version released in 1998

The name was changed to Wireshark in June, 2006, because Gerald Combs could not keep using the Ethereal trademark (which was then owned by his old employer, Network Integration Services) when he changed jobs (to CACE Technologies) – though he still held copyright on most of the source code

<http://www.wireshark.org/faq.html#q1.2>

Packet Sniffer and Packet Analyzer

- One's understanding of network protocols can often be greatly deepened by "seeing protocols in action" and by "playing around with protocols"
- 2 main components: packet sniffer, and packet analyzer
- 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. 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.
- The **packet analyzer** 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.

Submissions and Resources

What to hand in:

See packet (answer questions 1-4)

In addition

- Question 1: for the protocols with which you are not familiar, google it and at the very least write out the full name of the protocol
- Question 2: show the working out for this
- Question 3: self-explanatory
- Question 4: include these 2 print outs with your submission

Total: 20 points

Submit as follows:

Hand in at the beginning of class

Remember to use the standard format

<http://cs.millersville.edu/~csweb/lib/userfiles/AssignmentFormat.pdf>

- **The hard submission date for this lab is 9/17 at the beginning of class**