PROTOCOL ANALYSIS INSTITUTE

Quick Reference Step-by-Step Lab 4 Instructions: Go Away Kid—You Bother Me!

Step-by-Step Instructions: **madclient.pdf**
Trace File: **madclient.dmp**
"Watch the Lab" File: ***madclient.avi (XviD codec) or madclient.wmv***

Step 1: Create an ***Ethereal Labs* directory** on your hard drive and **copy the trace files** from the LLK6 over to that directory.

Step 2: **Launch Ethereal**.

Step 3: Select **File > Open** on the Ethereal menu bar. Select **your local drive** off the drive list and double-click on the **Ethereal Labs directory** you created in Step 1. Double-click on the ***madclient.dmp*** trace file.

Step 4: This trace file contains the TCP setup process, the application's attempted setup, and the teardown process. Examine packets 1 through 3 – this is the handshake process using – port 2345. **Look this port up at www.iana.org**.

Step 5: Click on **View > Time Display Format > Seconds Since Previous Packet**.

Step 6: Now the time column displays the time between the SYN and the SYN ACK packets – it comes out to 0.000270 – that's 270 millionths of a second – 270 microseconds – wow! Blazingly fast! **Jot down the times between the following packets**:

Packet 8 and 9 (NBNS and ICMP): ____________________
Packet 10 and 11 (NBNS and ICMP): ____________________

Step 7: To streamline our trace, let's get rid of the NetBIOS Name Service and ICMP packets. In the Display Filter window, enter **!NBNS and !ICMP**. Click **Apply**.

Step 8: **Examine the data in packet 4** – it tells us what application is sending the traffic! What is the application?

Step 9: The server responded to packet 4 with an ACK. What did the server do next? **Look inside packet 12**. Why isn't this application working properly across this network?

If you'd like to be walked through this process, check out the *BYOL* section of LLKv6.
See the ***Laura Chappell Master Library (LCML)*** at www.packet-level.com for additional self-paced labs.