Quick Reference Step-by-Step Lab 2 Instructions: The "Network is Slow"

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

Step 4: **Scroll through this trace quickly to get a feel for the traffic**. Lots of repetition and errors, eh? Not a very pretty trace. It looks like we can break down the trace file into three separate sections:

Packets 1–59	Invalid path
Packets 60-83	NetBIOS name failures
Packets 84-179	Failed search and ping

All three sections contain errors – which one of these (if any) might account for our client's complaints? We need to start measuring the amount of time used by each section.

Step 5: We will be working with time – let's ensure the time setting is correct. Click **View > Time Display Format > Seconds Since Beginning of Capture**.

Step 6: **Highlight packet 1**. **Right mouse click and select Time Reference > Set Time Reference (toggle)**. Packet 1 should now show up as the *REF* packet (in the time column). Highlight packet 59 which is the last packet in that first section. Write down the time column value.

Step 7: **Highlight packet 60**. **Right mouse click and select Time Reference > Set Time Reference (toggle)**. **Highlight packet 83** which is the last packet in that first section. Write down the time column value.

Step 8: Perform the **same steps** to reference packet 84 and write down the time column value on packet 179.

Step 9: Which section took the most time? Further review of this clients' traffic indicated that this was a constant problem throughout the day. The purpose of this lab is to focus on the importance of the time column in your analysis.

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.