PROTOCOL ANALYSIS INSTITUTE

Quick Reference Step-by-Step Lab 1 Instructions: Spyware/Adware Process

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

Step 4: Scroll through the trace until you reach **packet 68**. Check out all those connection attempts!

Step 5: Look at **packets 68 and 69**—this makes us feel a bit better–she performs a DNS query to obtain the IP address of McAfee's VirusScan update server. Scroll through to **packet 93** which appears to be the end of this little dance.

Step 6: Look at **packets 94 and 95**. She is now ready to get the updated virus definitions.

Step 7: We are going to build and apply a filter to remove all traffic to and from the McAfee update server at 216.49.88.118. Click in the **filter window** above the trace file headings. **Enter !ip.addr==216.49.88.118**. Click **Apply**.

Step 8: Look inside **packets 147 and 148 -** we've got someone trying to send Linda a message using Microsoft's Messenger Service.

Step 9: Scroll through from **packet 208 to 349**. Ugly, ugly, ugly.

Step 10: Click on **Statistics > Conversations**. Click on **TCP tab** in the Conversations window. Click on the **Packets column** heading to sort it in ascending order. **Right mouse click on a conversation** to quickly build and apply a display filter based on the source and destination IP addresses and port numbers.

Step 11: Now let's go back to **packet 350**. Uh oh… we have someone making a connection to our client on port 1025. Look closely at **packets 357-359**. We wonder what this process is telling the client to do. We don't have to wait long to find out.

Step 12: Look at the client DNS query for updates.virtumonde.com. Do a **Google search on virtumonde**.

Step 13: Let's filter out traffic to and from this server to see what our client does. In the filter window, type in ***ip.addr==208.48.15.13*** and click **Apply**. Yipes! Look at **packet 386**!

Step 14: Click **Clear** to remove our filter so we can see what is happening next in the trace. Our client sends something up to a server using an HTTP POST command in **packet 405**. In response, the Virtumonde server sends our clients some new configuration information in packet 412.

Step 15: Scroll through the rest of the trace to look for other suspect communications.

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.