Snarfing Unified2 Data

In order to snarf unified2 data, I created a barnyard2 output plugin and a Java translator. You run barnyard2 using the output plugin, and pipe the output to the translator, and presto, you will get unified2 messages into your console.

1. Download the unified2_snarf.tar.gz file from Deep Node, gunzip, extract.

2. The files in the output-plugins-files directory are what I put into the barnyard2 src/output-plugins directory in my barnyard. “spo_shelli.c” and “spo_shelli.h” are the actual plugin; “Makefile”, “Makefile.am”, and “Makefile.in” contain modifications to include the new plugin. If you have already customized yours, use mine as an example and edit the ones you already have.

3. “plugbase.c” contains a modification to include the new plugin; this file goes into src/, or edit the one you have.

4. “barnyard2.conf” has my modifications to use the new plugin; please use as an example.

5. Compile “Uni2Trans.java” using javac. It’s the translator process. Or use the already compiled “Uni2Trans.class” and “Uni2Trans$TSSubnet.class” which I have included.

6. To run this stuff… here’s an example:

```
/home/arkowitz/barnyard2-1.9/src/barnyard2 -c /home/arkowitz/barnyard2-1.9/etc/barnyard2.conf -d
/var/log/snort -f uni2.log | java Uni2Trans
```