p2db : Normalizer for network packets

p2db is a fast tool to convert network packets to events for use with the semantic analysis framework. p2db is located under plugins/p2db.

Currently the following packets can be converted

- TCP
- UDP
- ICMP
- DNS
- IP

Tool Usage

```
$ p2db
Usage: p2db filename (outdb|"stats")

Options:
   filename    PCAP File to process.
   outdb       Sqlite database file for output.
   stats       Just display event stats.
```

Installation

Make sure all p2db dependencies are installed.

```
$ cd /path/to/SAF
$ cd plugins/p2db
$ make
$ make install
```