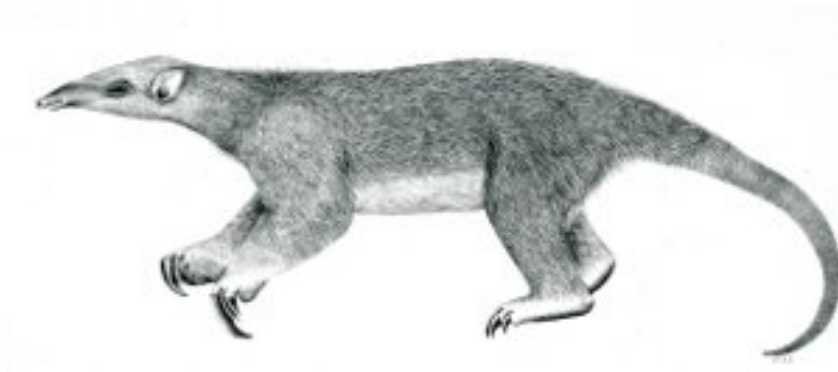

Tranalyzer2

protoStats



Protocol Statistics



Tranalyzer Development Team

Contents

1	protoStats	1
1.1	Description	1
1.2	Dependencies	1
1.3	Configuration Flags	1
1.4	Flow File Output	1
1.5	Additional Output	1
1.6	Post-Processing	1

1 protoStats

1.1 Description

The protoStats plugin provides protocol/port sorted frequency statistics about the observed OSI layer 4 protocols and ports to the file named `PREFIX_protocols`. Protocols numbers are decoded via a `proto.txt` file, automatically installed with the plugin.

1.2 Dependencies

1.2.1 Required Files

The file `proto.txt` is required.

1.3 Configuration Flags

The following flags can be used to control the output of the plugin:

Name	Default	Description
ETH_STAT	1	Output layer 2 statistics
SCTP_STAT	0	Output SCTP statistics
UDPLITE_STAT	0	Output UDP-Lite statistics

1.4 Flow File Output

None.

1.5 Additional Output

- `PREFIX_protocols.txt`: protocol statistics

1.6 Post-Processing

The `protStat` script can be used to sort the `PREFIX_protocols.txt` file for the most or least occurring protocols (in terms of number of packets or bytes). It can output the top or bottom *N* protocols or only those with at least a given percentage:

- list all the options: `protStat --help`
- sorted list of protocols (by packets): `protStat PREFIX_protocols.txt`
- sorted list of protocols (by bytes): `protStat PREFIX_protocols.txt -b`
- top 10 protocols (by packets): `protStat PREFIX_protocols.txt -n 10`
- bottom 5 protocols (by bytes): `protStat PREFIX_protocols.txt -n -5 -b`
- protocols with packets percentage greater than 20%: `protStat PREFIX_protocols.txt -p 20`
- protocols with bytes percentage smaller than 5%: `protStat PREFIX_protocols.txt -b -p -5`
- TCP and UDP statistics only: `protStat PREFIX_protocols.txt -udp -tcp`