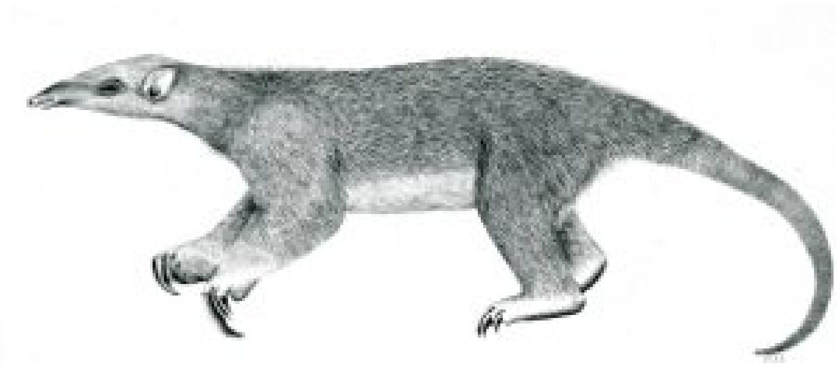
Tranalyzer2

syslogDecode

Syslog



Tranalyzer Development Team

Contents

1 syslogDecode

1.1 Description

The syslogDecode plugin analyzes Syslog traffic.

1.2 Configuration Flags

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

Name	Default	Description
No configuration options available		

1.3 Flow File Output

The syslogDecode plugin outputs the following columns:

Column	Type	Description
syslogStat	H8	Status
syslogMCnt	U32	message count
syslogSev_Fac_Cnt	RU8_U8_U16	Number of severity/facility messages

1.3.1 syslogStat

The syslogStat column is to be interpreted as follows:

syslogStat	Description
0x01	Syslog detected
0x80	Counter for facility/severity overflowed

1.4 TODO

- IPv6 tests

1.5 References

- https://tools.ietf.org/html/rfc5424