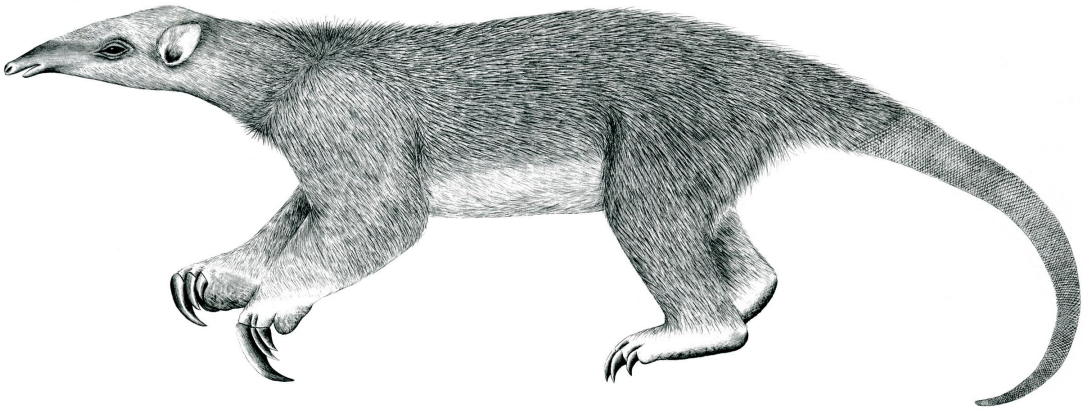
Tranalyzer2

entropy

Entropy



Tranalyzer Development Team

Contents

1 entropy

1.1 Description

The entropy plugin estimates the entropy of the snapped IP payload distribution. The number of bits of the alphabet can be 1,2,4,8. Default 8 bit, hence an alphabet of 256 symbols. The calculation of the entropy demands a certain minimum number of elements per flow. Two other key parameters, a binary and text based ratio, in combination with the entropy serve as input for AI for content and application classification. The character and binary ratio denote the degree of text or binary content respectively. All is experimental and described in detail in the Entropy et al tutorial on https://www.tranalyzer.com.

1.2 Configuration Flags

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

Name	Default	Description
ENT_NORM	1	0: # bits 1: Normalized entropy
ENT_NBITS	8	N bit word, vocabulary: 2^N
ENT_HPKTIG	0	Ignore first N packets
ENT_HEAD	0	Start word of entropy calc in payload
ENT_TAIL	1500	Position until entropy is calculated
ENT_THRESL	8	Threshold for minimal payload length
ENT_THRESH	8192	Threshold for maximal payload length
ENT_ALPHAD	0	Print alphabet distribution in flow file

1.2.1 Environment Variable Configuration Flags

The following configuration flags can also be configured with environment variables (ENVCNTRL>0):

- ENT_HPKTIG
- ENT_HEAD
- ENT_TAIL
- ENT_THRESL
- ENT_THRESH

1.3 Flow File Output

The entropy plugin outputs the following columns:

Column	Type	Description	Flags
PyldEntropy	F	Payload entropy[1]	
PyldChRatio	F	Payload character ratio	

[1] A value of -1 indicates that no entropy was calculated

Column	Type	Description	Flags
PyldBinRatio	F	Payload binary ratio	
NumBin0	U32	Number of 0 count bins	ENT_ALPHAD=1
Corr	F	entropy correction	ENT_ALPHAD=1
PyldLen	U32	Payload length	ENT_ALPHAD=1
PyldHisto	R(U32)	Payload histogram	ENT_ALPHAD=1

1.4 Plugin Report Output

The following information is reported:

- NValFlows, Min, Average, Max entropy