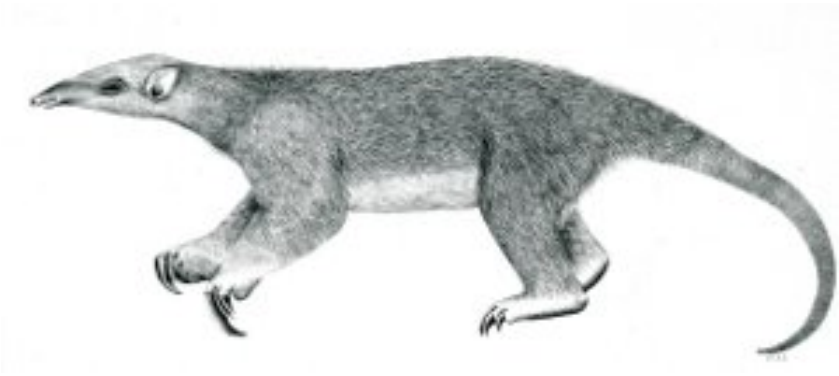
Tranalyzer2

descriptiveStats

Descriptive Statistics



Tranalyzer Development Team

Contents

1 descriptiveStats

1.1 Description

The descriptiveStats plugin calculates various statistics about a flow. Because the inter-arrival time of the first packet is per definition always zero, it is removed from the statistics. Therefore the inter-arrival time statistics values for flows with only one packet is set to zero.

1.2 Dependencies

1.2.1 Other Plugins

This plugin requires the `pktSIATHisto` plugin.

1.3 Configuration Flags

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

Name	Default	Description
ENABLE_PS_CALC	1	1: Enables / 0: Disables calculation of statistics for packet sizes
ENABLE_IAT_CALC	1	1: Enables / 0: Disables calculation of statistics for inter-arrival times

1.4 Flow File Output

The descriptiveStats plugin outputs the following columns:

Column	Type	Description	Flags
MinPl	F	Minimum packet length	ENABLE_PS_CALC=1
MaxPl	F	Maximum packet length	ENABLE_PS_CALC=1
MeanPl	F	Mean packet length	ENABLE_PS_CALC=1
LowQuartilePl	F	Lower quartile of packet lengths	ENABLE_PS_CALC=1
MedianPl	F	Median of packet lengths	ENABLE_PS_CALC=1
UppQuartilePl	F	Upper quartile of packet lengths	ENABLE_PS_CALC=1
IqdPl	F	Inter quartile distance of packet lengths	ENABLE_PS_CALC=1
ModePl	F	Mode of packet lengths	ENABLE_PS_CALC=1
RangePl	F	Range of packet lengths	ENABLE_PS_CALC=1
StdPl	F	Standard deviation of packet lengths	ENABLE_PS_CALC=1
RobStdPl	F	Robust standard deviation of packet lengths	ENABLE_PS_CALC=1
SkewPl	F	Skewness of packet lengths	ENABLE_PS_CALC=1
ExcPl	F	Excess of packet lengths	ENABLE_PS_CALC=1
MinIat	F	Minimum inter-arrival time	ENABLE_IAT_CALC=1
MaxIat	F	Maximum inter-arrival time	ENABLE_IAT_CALC=1
MeanIat	F	Mean inter-arrival time	ENABLE_IAT_CALC=1
LowQuartileIat	F	Lower quartile of inter-arrival times	ENABLE_IAT_CALC=1
MedianIat	F	Median of inter-arrival times	ENABLE_IAT_CALC=1
UppQuartileIat	F	Upper quartile of inter-arrival times	ENABLE_IAT_CALC=1

Column	Type	Description	Flags
IqdIat	F	Inter quartile distance of inter-arrival times	ENABLE_IAT_CALC=1
ModeIat	F	Mode of inter-arrival times	ENABLE_IAT_CALC=1
RangeIat	F	Range of inter-arrival times	ENABLE_IAT_CALC=1
StdIat	F	Standard deviation of inter-arrival times	ENABLE_IAT_CALC=1
RobStdIat	F	Robust standard deviation of inter-arrival times	ENABLE_IAT_CALC=1
SkewIat	F	Skewness of inter-arrival times	ENABLE_IAT_CALC=1
ExcIat	F	Excess of inter-arrival times	ENABLE_IAT_CALC=1

1.5 Known Bugs and Limitations

Because the packet length and inter-arrival time plugin stores the inter-arrival times in statistical bins the original time information is lost. Therefore the calculation of the inter-arrival times statistics is due to its logarithmic binning only a rough approximation of the original timing information. Nevertheless, this representation has shown to be useful in practical cases of anomaly and application classification.