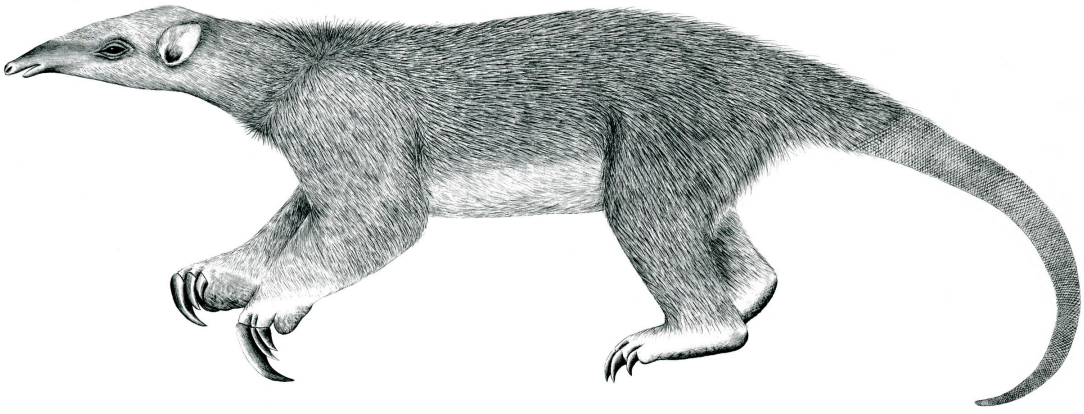
Tranalyzer2

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	Flags
`DS_PS_CALC`	1	Compute statistics for packet sizes	
`DS_IAT_CALC`	1	Compute statistics for inter-arrival times	
`DS_QUARTILES`	0	Quartiles calculation: 0: Use linear interpolation 1: Use the mean	`DS_PS_CALC=1`

1.4 Flow File Output

The descriptiveStats plugin outputs the following columns:

Column	Type	Description	Flags
`dsMinPl`	F	Minimum packet length	`DS_PS_CALC=1`
`dsMaxPl`	F	Maximum packet length	`DS_PS_CALC=1`
`dsMeanPl`	F	Mean packet length	`DS_PS_CALC=1`
`dsLowQuartilePl`	F	Lower quartile of packet lengths	`DS_PS_CALC=1`
`dsMedianPl`	F	Median of packet lengths	`DS_PS_CALC=1`
`dsUppQuartilePl`	F	Upper quartile of packet lengths	`DS_PS_CALC=1`
`dsIqdPl`	F	Inter quartile distance of packet lengths	`DS_PS_CALC=1`
`dsModePl`	F	Mode of packet lengths	`DS_PS_CALC=1`
`dsRangePl`	F	Range of packet lengths	`DS_PS_CALC=1`
`dsStdPl`	F	Standard deviation of packet lengths	`DS_PS_CALC=1`
`dsRobStdPl`	F	Robust standard deviation of packet lengths	`DS_PS_CALC=1`
`dsSkewPl`	F	Skewness of packet lengths	`DS_PS_CALC=1`
`dsExcPl`	F	Excess of packet lengths	`DS_PS_CALC=1`
`dsMinIat`	F	Minimum inter-arrival time	`DS_IAT_CALC=1`
`dsMaxIat`	F	Maximum inter-arrival time	`DS_IAT_CALC=1`
`dsMeanIat`	F	Mean inter-arrival time	`DS_IAT_CALC=1`

Column	Type	Description	Flags
dsLowQuartileIat	F	Lower quartile of inter-arrival times	DS_IAT_CALC=1
dsMedianIat	F	Median of inter-arrival times	DS_IAT_CALC=1
dsUppQuartileIat	F	Upper quartile of inter-arrival times	DS_IAT_CALC=1
dsIqdIat	F	Inter quartile distance of inter-arrival times	DS_IAT_CALC=1
dsModeIat	F	Mode of inter-arrival times	DS_IAT_CALC=1
dsRangeIat	F	Range of inter-arrival times	DS_IAT_CALC=1
dsStdIat	F	Standard deviation of inter-arrival times	DS_IAT_CALC=1
dsRobStdIat	F	Robust standard deviation of inter-arrival times	DS_IAT_CALC=1
dsSkewIat	F	Skewness of inter-arrival times	DS_IAT_CALC=1
dsExcIat	F	Excess of inter-arrival times	DS_IAT_CALC=1

1.5 Known Bugs and Limitations

Because the pktSIATHisto 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.