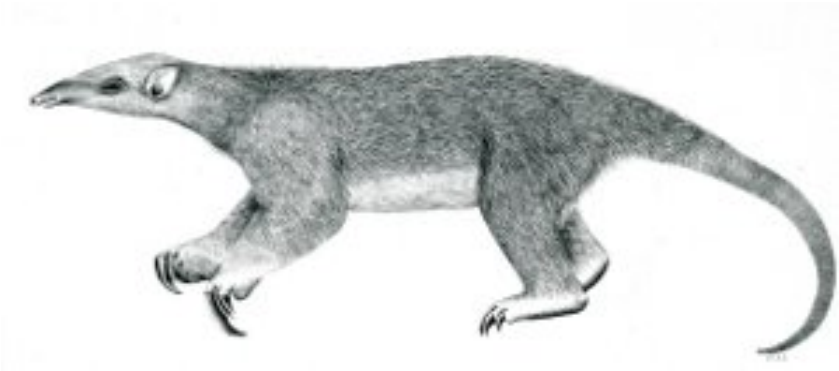
Tranalyzer2

basicStats

Basic Statistics



Tranalyzer Development Team

Contents

1 basicStats

1.1 Description

The basicStats plugin supplies basic layer four statistics for each flow.

1.2 Dependencies

1.2.1 Other Plugins

If the `basicFlow` plugin is loaded, then the country of the IPs with the most bytes and packets transmitted is displayed in the final report.

1.3 Configuration Flags

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

Name	Default	Description	Flags
`BS_AGGR_CNT`	0	1: add A+B counts, 0: A+B counts off	
`BS_REV_CNT`	1	1: add reverse counts from opposite flow, 0: native send counts	
`BS_STATS`	1	Output statistics (min, max, average, ...)	
`BS_PL_STATS`	1	1: Packet Length statistics	
`BS_IAT_STATS`	1	1: IAT statistics	
If `BS_STATS==1`, the following additional flags can be used:			
`BS_VAR`	0	Output the variance	
`BS_STDDEV`	1	Output the standard deviation	
`BS_XCLD`	0	0: do not exclude any value from statistics, 1: include (BS_XMIN,UINT16_MAX], 2: include [0,BS_XMAX), 3: include [BS_XMIN,BS_XMAX] 4: exclude (BS_XMIN,BS_XMAX)	
`BS_XMIN`	1	minimal included/excluded from statistics	`BS_XCLD>0`
`BS_XMAX`	65535	maximal included/excluded from statistics	`BS_XCLD>0`

1.4 Flow File Output

The basicStats plugin outputs the following fields:

Column	Type	Description	Flags
`numPktsSnt`	U64	Number of transmitted packets	
`numPktsRcvd`	U64	Number of received packets	`BS_REV_CNT=1`
`numPktsRTAggr`	U64	Number of received + transmitted packets	`BS_AGGR_CNT=1`
`numBytesSnt`	U64	Number of transmitted bytes	

Column	Type	Description	Flags
numBytesRcvd	U64	Number of received bytes	BS_REV_CNT=1
numBytesRTAggr	U64	Number of received + transmitted bytes	BS_AGGR_CNT=1
If BS_STATS=1, the following columns, whose value depends on BS_XCLD, are provided			
If BS_PL_STATS=1, the following five columns are displayed			
minPktSz	U16	Minimum layer 3 packet size	
maxPktSz	U16	Maximum layer 3 packet size	
avePktSize	F	Average layer 3 packet size	
varPktSize	F	Variance layer 3 packet size	BS_VAR=1
stdPktSize	F	Standard deviation layer 3 packet size	BS_STDDEV=1
If BS_IAT_STATS=1, the following five columns are displayed			
minIAT	F	Minimum IAT	
maxIAT	F	Maximum IAT	
aveIAT	F	Average IAT	
varIAT	F	Variance IAT	BS_VAR=1
stdIAT	F	Standard deviation IAT	BS_STDDEV=1
pktps	F	Sent packets per second	
bytps	F	Sent bytes per second	
pktAsm	F	Packet stream asymmetry	
bytAsm	F	Byte stream asymmetry	

1.5 Packet File Output

In packet mode (-s option), the basicFlow plugin outputs the following columns:

Column	Description
pktLen	Packet size on the wire
l7Len	L7 length

1.6 Plugin Report Output

The IP of biggest packets/bytes talker and packets/bytes counts are reported.