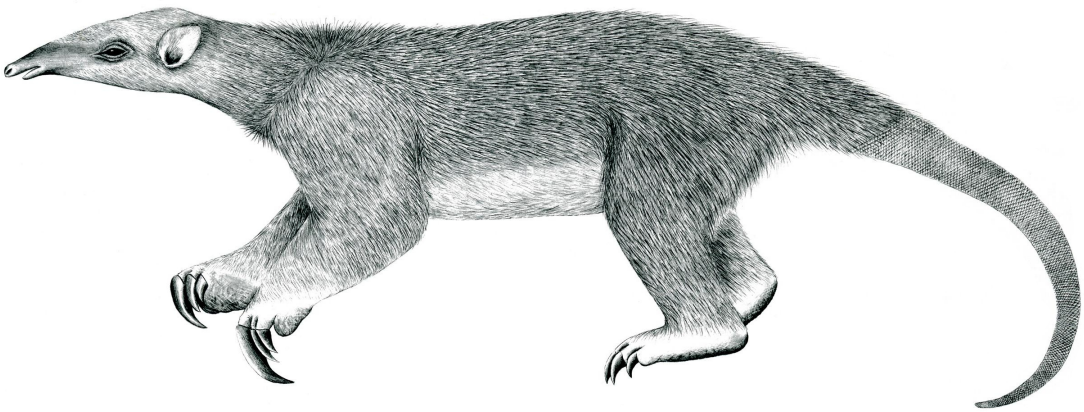
Tranalyzer2

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 Configuration Flags

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

Name	Default	Description	Flags
BS_AGGR_CNT	0	0: A+B counts off,	
	0	1: add A+B counts	
BS_REV_CNT	1	0: native send counts,	
		1: add reverse counts from opposite flow	
BS_MOD	0	> 1: modulo factor of packet length; else: off	
BS_PAD	1	1: Aggregated padding bytes	
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_SK	0	Skew/kurtosis calculation	BS_VAR=1
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	UINT16_MAX	maximal included/excluded from statistics	BS_XCLD>0

1.2.1 Environment Variable Configuration Flags

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

- BS_XMIN
- BS_XMAX

1.3 Flow File Output

The basicStats plugin outputs the following fields:

Column	Type	Description	Flags
pktsSnt	U64	Number of transmitted packets	
pktsRcvd	U64	Number of received packets	BS_REV_CNT=1
pktsRTAggr	U64	Number of received + transmitted packets	BS_AGGR_CNT=1
padBytesSnt	I64	Number of transmitted padding bytes	BS_PAD=1
l2-7BytesSnt	U64	Number of transmitted layer 2-7 bytes	
l2-7BytesRcvd	U64	Number of received layer 2-7 bytes	BS_REV_CNT=1
l2-7BytesRTAggr	U64	Number of received + transmitted layer 2-7 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			
minL2-7PktSz	U16	Minimum layer 2-7 packet size	
maxL2-7PktSz	U16	Maximum layer 2-7 packet size	
avgL2-7PktSz	F	Average layer 2-7 packet size	
stdL2-7PktSz	F	Standard deviation layer 2-7 packet size	BS_STDDEV=1
varL2-7PktSz	F	Variance layer 2-7 packet size	BS_VAR=1
skewL2-7PktSz	F	Skewness layer 2-7 packet size	BS_SK=1 && BS_VAR=1
kurL2-7PktSz	F	Kurtosis layer 2-7 packet size	BS_SK=1 && BS_VAR=1
If BS_IAT_STATS=1, the following five columns are displayed			
minIAT	F	Minimum IAT	
maxIAT	F	Maximum IAT	
avgIAT	F	Average IAT	
varIAT	F	Variance IAT	BS_VAR=1
stdIAT	F	Standard deviation IAT	BS_STDDEV=1
skewIAT	F	Skewness IAT	BS_SK=1 && BS_VAR=1
kurIAT	F	Kurtosis IAT	BS_SK=1 && BS_VAR=1
pktps	F	Sent packets per second	
bytps	F	Sent bytes per second	
pktAsm	F	Packet stream asymmetry	
bytAsm	F	Byte stream asymmetry	

1.3.1 Packet size

Packet sizes depend on `PACKETLENGTH` in *tranalyzer2/src/packetCapture.h*):

- `PACKETLENGTH=0`:
  - Output `*L2PktSz` and `*L2Bytes*` columns
  - Packet size include layer 2, 3 and 4 header
- `PACKETLENGTH=1`:
  - Output `*L3PktSz` and `*L3Bytes*` columns
  - Packet size include layer 3 and 4 header
- `PACKETLENGTH=2`:
  - Output `*L4PktSz` and `*L4Bytes*` columns
  - Packet size include layer 4 header
- `PACKETLENGTH=3`:
  - Output `*L7PktSz` and `*L7Bytes*` columns
  - Packet size include only layer 7

1.4 Packet File Output

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

Column	Type	Description	Flags
`pktLen`	U32	Packet size on the wire	
`udpLen`	U16	Length in UDP/UDP-Lite header	
`snapL4Len`	U16	Snapped layer 4 length	
`snapL7Len`	U16	Snapped layer 7 length	
`l7Len`	U16	Layer 7 length	
`pktLenMod`	U16	Modulo factor of packet length	`BS_MOD>1`
`padLen`	I64	Number of padding bytes	

1.5 Plugin Report Output

The following information is reported:

- MAC of biggest packets/bytes talker and packets/bytes counts
- IP of biggest packets/bytes talker and packets/bytes counts (`ANONYM_IP=0`)