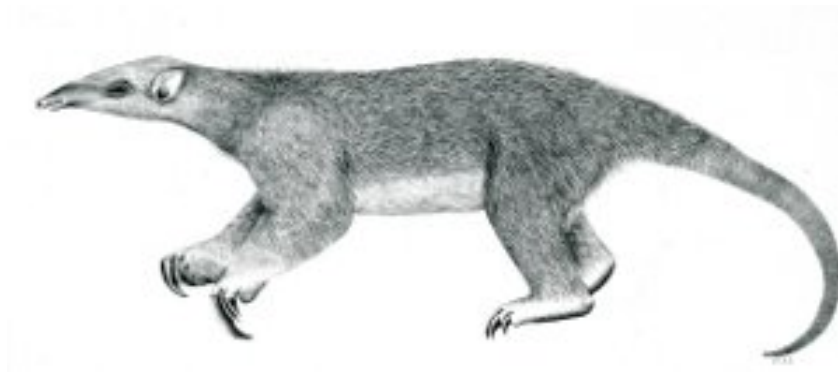

Tranalyzer2

nFrstPkts



Statistics Over the N First Packets



Tranalyzer Development Team

Contents

1	nFrstPkts	1
1.1	Description	1
1.2	Configuration Flags	1
1.3	Flow File Output	1
1.4	Post-Processing	2

1 nFrstPkts

1.1 Description

The nFrstPkts plugin supplies the Packet Length (PL) and Interarrival Times (IAT) of the N first packets per flow as a column. The default value for N is 20. It complements the packet mode (`-s` option) with flow based view for the N first packets signal. The plugin supplies several configuration options of how the resulting packet length signal should be represented. Using the `fpsGplt` script files are generated readily post processable by any command line tool (AWK, Perl), Excel or Data mining suit, such as SPSS. As outlined in the configuration below, Signals can be produced with IAT, or relative/absolute time. Also the aggregation of bursts into a single pulse can be configured via `NFRST_MINIAT`. `NFRST_MINPLAVE` controls the meaning of the PL value in puls aggregation mode. If 0 it corresponds to the BPP measure currently used in research for categorizing media content.

1.2 Configuration Flags

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

Name	Default	Description	Flags
NFRST_IAT	1	0: Time relative to flow start, 1: Interarrival Time, 2: Absolute Time	
NFRST_BCORR	0	0: A,B start at 0.0 1: B shift by flow start	NFRST_MINIATS=0
NFRST_MINIATS	0	0: Standard IAT Sequence 1: Minimal Pkt IAT s defining a pulse signal	
NFRST_MINIATU	0	0: Standard IAT Sequence, 1: Minimal Pkt IAT us defining a pulse signal	
NFRST_MINPLENFR	2	Minimal pulse length fraction	
NFRST_PLAVE	1	0: Sum PL (BPP), 1: Average PL	NFRST_MINIATS>0 NFRST_MINIATU>0
NFRST_PKT CNT	20	Number of packets to record	
NFRST_HDRINFO	0	add L3,L4 Header length	
NFRST_XCLD	0	0: include all, 1: include [NFRST_XMIN,NFRST_XMAX]	
NFRST_XMIN	1	min PL boundary	NFRST_XCLD=1
NFRST_XMAX	UINT16_MAX	max PL boundary	NFRST_XCLD=1

For the rest of this document, `NFRST_MINIAT` is used to represent `(NFRST_MINIATS>0 || NFRST_MINIATU>0)`.

1.3 Flow File Output

The nFrstPkts plugin outputs the following columns:

Column	Type	Description	Flags
nFpCnt	U32	Number of signal samples	
L2L3L4Pl_Iat	R(U16_UT)	L2/L3/L4 or payload length and inter-arrival times for the N first packets	NFRST_HDRINFO=0 && NFRST_MINIAT=0

Column	Type	Description	Flags
L2L3L4Pl_Iat_nP	R(U16_UT_UT)	L2/L3/L4 or payload length, inter-arrival times and pulse length for the N first packets	NFRST_HDRINFO=0&& NFRST_MINIAT>0
HD3l_HD4l_ L2L3L4Pl_Iat	R(U8_U8_ _U16_UT)	L3Hdr, L4Hdr, L2/L3/L4 or payload length and inter-arrival times for the N first packets	NFRST_HDRINFO=1&& NFRST_MINIAT=0
HD3l_HD4l_ L2L3L4Pl_Iat_nP	R(U8_U8_U16_ UT_UT)	L3Hdr, L4Hdr, L2/L3/L4 or payload length and inter-arrival times for the N first packets	NFRST_HDRINFO=1&& NFRST_MINIAT>0

1.4 Post-Processing

By invoking the script `fpsGplt` under *trunk/scripts* files are generated for the packet signal in a Gnuplot/Excel/SPSS readable column oriented format. It produces several signal variants which also can be used for signal processing and AI applications. S. traffic mining tutorial on our webpage

```
>fpsGplt -h
Usage:
    fpsGplt [OPTION...] <FILE>
```

Optional arguments:

```
-f          Flow index to extract, default: all flows
-d          Flow Direction: 0, 1; default both
-t          noTime: counts on x axis; default time on x axis
-i          invert B Flow PL
-s          time sorted

-h, --help  Show this help, then exit
```