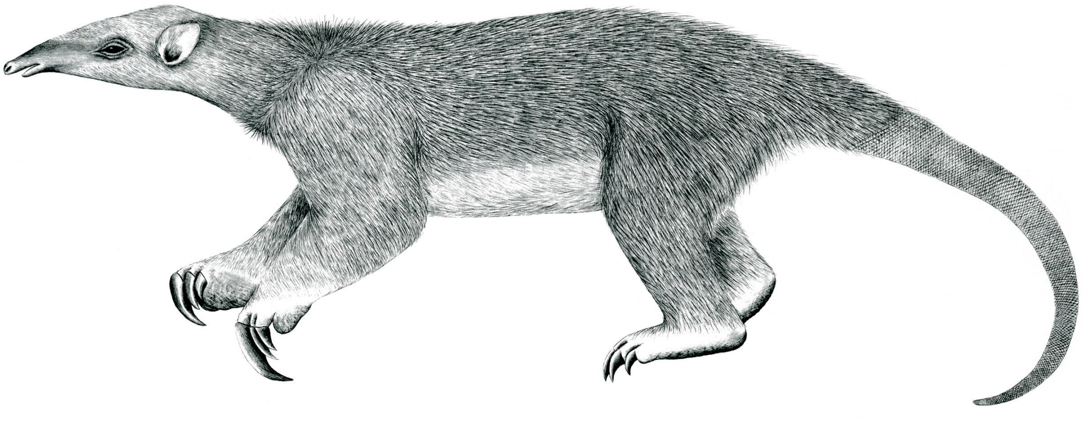
Tranalyzer2

t2PSkel

t2PSkel



Tranalyzer Development Team

Contents

1 t2PSkel

1.1 Description

The t2PSkel plugin analyzes ...

1.2 Dependencies

1.2.1 External Libraries

This plugin depends on the **XXX** library.

		OPT1=1	OPT2=1
Ubuntu:	`sudo apt-get install`	`libXXX-dev`	`libYYY-dev`
Arch:	`sudo pacman -S`	`libXXX`	`YYY`
Gentoo:	`sudo emerge`	`libXXX`	`YYY`
openSUSE:	`sudo zypper install`	`libXXX-devel`	`libYYY-devel`
Red Hat/Fedora[1]**:**	`sudo dnf install`	`libXXX-devel`	`YYY-devel`
macOS[2]**:**	`brew install`	`libXXX`	`YYY`

1.2.2 Core Configuration

This plugin requires the following core configuration:

- *$T2HOME/tranalyzer2/src/networkHeaders.h*:
  - `ETH_ACTIVATE>0`
- *$T2HOME/tranalyzer2/src/tranalyzer.h*:
  - `BLOCK_BUF=0`

1.2.3 Other Plugins

This plugin requires the `tcpFlags` and `tcpStates` plugins.

1.2.4 Required Files

The file `filename.txt` is required.

1.3 Configuration Flags

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

[1] If the `dnf` command could not be found, try with `yum` instead

[2] Brew is a packet manager for macOS that can be found here: https://brew.sh

Name	Default	Description	Flags
T2PSKEL_SAVE	0	Save content to T2PSKEL_F_PATH	
T2PSKEL_RMDIR	1	Empty T2PSKEL_F_PATH before starting	T2PSKEL_SAVE=1
T2PSKEL_STATS	0	Save statistics to baseFileName T2PSKEL_SUFFIX	
T2PSKEL_LOAD	0	Load T2PSKEL_FNAME	
T2PSKEL_VAR1	0	Output t2PSkelVar1	
T2PSKEL_IP	0	General description of T2PSKEL_IP 0: description of value 0 1: description of value 1 2: description of value 2	
T2PSKEL_VEC	0	Description of T2PSKEL_VEC	T2PSKEL_IP=1
T2PSKEL_ENV_NUM	0	Those variables can be overwritten at runtime	
T2PSKEL_ENV_STR	"str"	This variable can also be overwritten at runtime	
T2PSKEL_FNAME	"filename.txt"	File to load	T2PSKEL_LOAD=1
T2PSKEL_SUFFIX	"_suffix.txt"	Suffix for output file	T2PSKEL_STATS=1
T2PSKEL_F_PATH	"/tmp/t2PSkel_files"	Suffix for output file	T2PSKEL_STATS=1

1.3.1 Environment Variable Configuration Flags

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

- T2PSKEL_ENV_NUM
- T2PSKEL_ENV_STR

1.4 Flow File Output

The t2PSkel plugin outputs the following columns:

Column	Type	Description	Flags
t2PSkelStat	H8	Status	
t2PSkelText	S	describe t2PSkelText (string)	
t2PSkelVar1	U64	describe t2PSkelVar1 (uint64)	T2PSKEL_VAR1=1
t2PSkelIP	IP4	describe t2PSkelIP (IPv4)	T2PSKEL_IP=1
t2PSkelVar3_Var4	H32_H16	describe t2PSkelVar3_Var4	
If T2PSKEL_VEC=1, the following columns are displayed:			
t2PSkelVar5_Var6	R(U8_U8)	describe t2PSkelVar5_Var6	
t2PSkelVector	R(R(D))	describe t2PSkelVector	

1.4.1 t2PSkelStat

The t2PSkelStat column is to be interpreted as follows:

t2PSkelStat	Description
0x01	Flow is t2PSkel
0x02	—
0x04	—
0x08	—
0x10	—
0x20	—
0x40	—
0x80	—

1.4.2 t2PSkelVar1

The t2PSkelVar1 column is to be interpreted as follows:

t2PSkelVar1	Description
0x01	—
0x02	—
0x04	—
0x08	—

t2PSkelVar1	Description
0x10	—
0x20	—
0x40	—
0x80	—

1.5 Packet File Output

In packet mode (-s option), the t2PSkel plugin outputs the following columns:

Column	Type	Description	Flags
t2PSkelCol1	I8	describe col1	

1.6 Monitoring Output

In monitoring mode, the t2PSkel plugin outputs the following columns:

Column	Type	Description	Flags
t2PSkelCol1	I8	describe col1	

1.7 Plugin Report Output

The following information is reported:

- Aggregated t2PSkelStat
- Number of XXX packets

1.8 Additional Output

Non-standard output:

- PREFIX_suffix.txt: description

1.9 Post-Processing

1.10 Example Output

1.11 Known Bugs and Limitations

1.12 TODO

- TODO1
- TODO2

1.13 References

- RFCXXXX: Title
- `https://www.iana.org/assignments/`