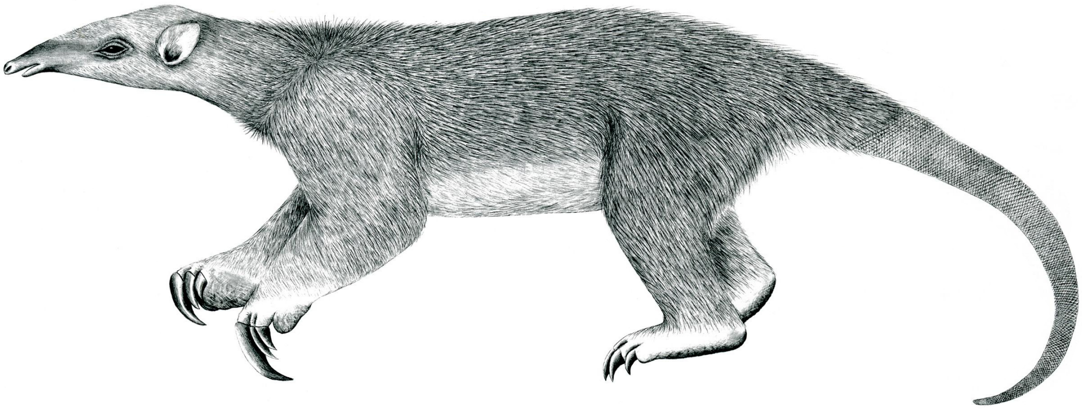
Tranalyzer2

jsonSink

JSON Output



Tranalyzer Development Team

Contents

1 jsonSink

1.1 Description

The jsonSink plugin generates JSON output in a file `PREFIX_flows.json`, where `PREFIX` is provided via Tranalyzer `-w` or `-W` option.

1.2 Dependencies

1.2.1 External Libraries

If gzip compression is activated (`JSON_GZ_COMPRESS=1`), then **zlib** must be installed.

		JSON_GZ_COMPRESS=1
Ubuntu:	`sudo apt-get install`	`zlib1g-dev`
Arch:	`sudo pacman -S`	`zlib`
Gentoo:	`sudo emerge`	`zlib`
openSUSE:	`sudo zypper install`	`zlib-devel`
Red Hat/Fedora[1]**:**	`sudo dnf install`	`zlib-devel`
macOS[2]**:**	`brew install`	`zlib`

1.2.2 Core Configuration

This plugin requires the following core configuration:

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

1.3 Configuration Flags

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

Name	**Default**	**Description**	**Flags**
`JSON_SOCKET_ON`	0	Output to a socket (1) or to a file (0)	
`JSON_SOCKET_ADDR`	`"127.0.0.1"`	Address of the socket	`JSON_SOCKET_ON=1`
`JSON_SOCKET_PORT`	5000	Port of the socket	`JSON_SOCKET_ON=1`
`JSON_GZ_COMPRESS`	0	Compress (gzip) the output	
`JSON_SPLIT`	1	Split the output file (Tranalyzer `-W` option)	`JSON_SOCKET_ON=0`
`JSON_ROOT_NODE`	0	Add a root node (array)	
`JSON_SUPPRESS_EMPTY_ARRAY`	1	Do not output empty fields	
`JSON_NO_SPACES`	1	Suppress unnecessary spaces	

[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
JSON_BUFFER_SIZE	1048576	Size of output buffer	
JSON_SELECT	0	Only output specific fields	
JSON_SELECT_FILE	"json-columns.txt"	Filename of the field selector (one column name per line)	JSON_SELECT=1
JSON_SUFFIX	"_flows.json"	Suffix for output file	JSON_SOCKET_ON=0

1.3.1 Environment Variable Configuration Flags

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

- JSON_BUFFER_SIZE
- JSON_SOCKET_ADDR (require JSON_SOCKET_ON=1)
- JSON_SOCKET_PORT (require JSON_SOCKET_ON=1)
- JSON_SUFFIX (require JSON_SOCKET_ON=0)
- JSON_SELECT_FILE

1.4 Plugin Report Output

The following information is reported:

- Number of flows discarded due to main buffer problems

1.5 Custom File Output

- PREFIX_flows.json: JSON representation of Tranalyzer output

1.6 Output Selected Fields Only

When JSON_SELECT=1, the columns to output can be customized with the help of JSON_SELECT_FILE. The filename defaults to json-columns.txt in the user plugin folder, e.g., *~/.tranalyzer/plugins*. The format of the file is simply one field name per line with lines starting with a '#' being ignored. For example, to only output source and destination addresses and ports, create the following file:

```
# Lines starting with a '#' are ignored and can be used to add comments
srcIP
srcPort
dstIP
dstPort
```

1.7 Example

To send compressed data over a socket (`JSON_SOCKET_ON=1` and `JSON_GZ_COMPRESS=1`):

1. `nc -l 127.0.0.1 5000 | gunzip`
2. `tranalyzer -r file.pcap`