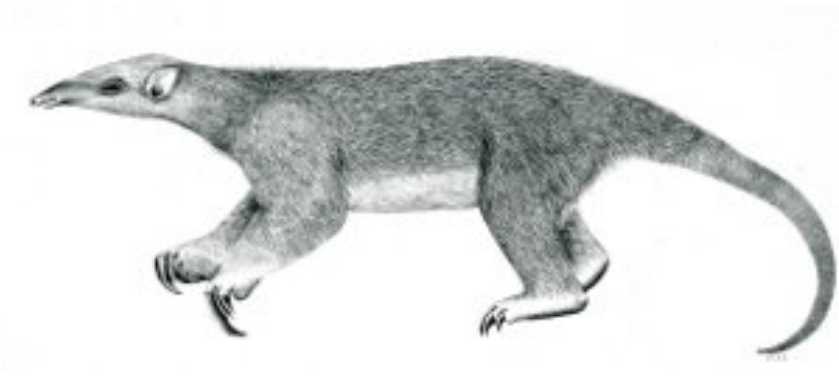
# Tranalyzer2

## 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 (`GZ_COMPRESS=1`), then **zlib** must be installed.

**Kali/Ubuntu:** `sudo apt-get install zlib1g-dev`

**Arch:** `sudo pacman -S zlib`

**Fedora/Red Hat:** `sudo yum install zlib-devel`

**Gentoo:** `sudo emerge zlib`

**OpenSUSE:** `sudo zypper install zlib-devel`

**Mac OS X:** `brew install zlib`[1]

## 1.3 Configuration Flags

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

| Name | Default | Description | Flags |
|---|---|---|---|
| SOCKET_ON | 0 | Whether to output to a socket (1) or to a file (0) | |
| SOCKET_ADDR | "127.0.0.1" | Address of the socket | SOCKET_ON=1 |
| SOCKET_PORT | 5000 | Port of the socket | SOCKET_ON=1 |
| GZ_COMPRESS | 0 | Compress (gzip) the output | |
| JSON_SPLIT | 1 | Split the output file (Tranalyzer -W option) | SOCKET_ON=0 |
| JSON_ROOT_NODE | 0 | Add a root node (array) | |
| SUPPRESS_EMPTY_ARRAY | 1 | Do not output empty fields | |
| JSON_NO_SPACES | 1 | Suppress unnecessary spaces | |
| JS_BUFFER_SIZE | 1024*1024 | Size of output buffer | |
| JSON_SUFFIX | "_flows.json" | Suffix for output file | SOCKET_ON=0 |

[1] Brew is a packet manager for Mac OS X that can be found here: https://brew.sh

## 1.4 Custom File Output

- `PREFIX_flows.json`: JSON representation of Tranalyzer output

## 1.5 Example

To send compressed data over a socket (`SOCKET_ON=1` and `GZ_COMPRESS=1`):

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