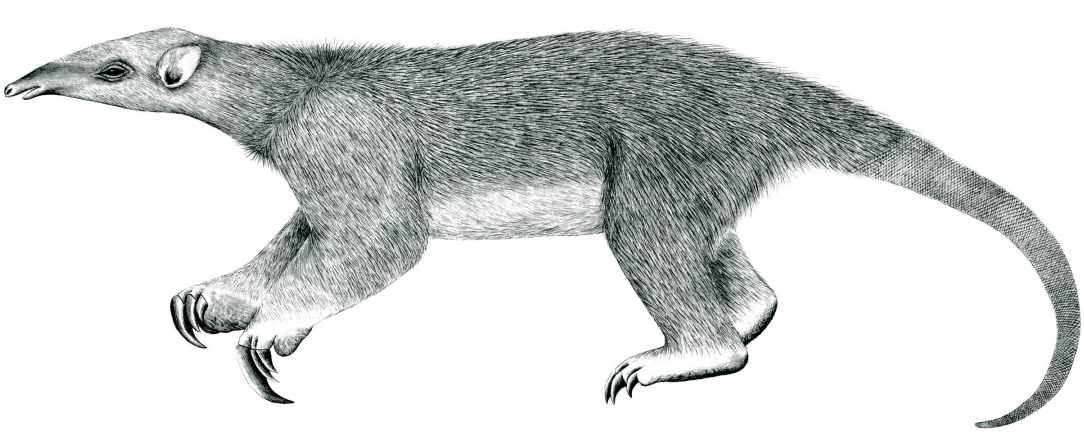
Tranalyzer2

regexHyperscan

Traffic pattern matching using the Hyperscan library.



Tranalyzer Development Team

Contents

1 regexHyperscan

1.1 Description

This plugin applies regexes on the network traffic using the Hyperscan library[1]. The regexes can be applied on the whole flow or per packet from layer 7.

1.2 Dependencies

1.2.1 External Libraries

This plugin depends on the Hyperscan library which is included in this plugin. In order to compile it, the following tools and libraries are needed.

Ubuntu:	`sudo apt-get install`	`cmake g++ libboost-dev ragel`
Arch:	`sudo pacman -S`	`boost cmake ragel`
Red Hat/Fedora[2]:	`sudo dnf install`	`boost-devel cmake gcc-c++ ragel`

1.2.2 Required Files

The file `hsregexes.txt` contains the regexes and their corresponding ID. The lines starting with `%` are comments. The other lines must contain two or three columns:

Column	Description
1	A string ID which will appear in the flow output if the flow matches the regex in column 2.
2	A regex in the Hyperscan format describe in Section 1.3.
3	Optional. Whether (1) to extract flows matching regex using the `liveXtr` plugin, or not (0).

1.3 Hyperscan regex format

Each regex must have the following format: `/pattern/flags`

The **pattern** use the PCRE syntax with some limitation explained in the Hyperscan documentation[3].

The **flags** are optional and are described in the Hyperscan documentation[4]. The following table provides a correspondence between the letters used in this plugin regex format and the values in the Hyperscan documentation.

Flag	Description
i	HS_FLAG_CASELESS
s	HS_FLAG_DOTALL
m	HS_FLAG_MULTILINE

[1] https://github.com/intel/hyperscan
[2] If the `dnf` command could not be found, try with `yum` instead
[3] https://intel.github.io/hyperscan/dev-reference/compilation.html#pattern-support
[4] https://intel.github.io/hyperscan/dev-reference/api_constants.html#pattern-flags

Flag	Description
H	HS_FLAG_SINGLEMATCH (enabled by default)
V	HS_FLAG_ALLOWEMPTY
8	HS_FLAG_UTF8
W	HS_FLAG_UCP

1.4 Configuration Flags

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

Name	Default	Description
RHS_STREAMING	1	1: Apply the regexes on the whole flow as a stream. 0: Apply the regexes per packet.
RHS_RELOADING	1	Automatically reload the regex file when modified.
RHS_EXTRACT_OPPOSITE	1	Also extract the opposite flow when regex match.
RHS_MAX_FLOW_MATCH	16	Max. number of regexes which can match on a flow.
RHS_REGEX_FILE	"hsregexes.txt"	The name of the file described in Section 1.2.2.

1.5 Flow File Output

The regexHyperscan plugin outputs the following columns:

Column	Type	Description
hsregexes	RS	IDs of all regexes matching this flow