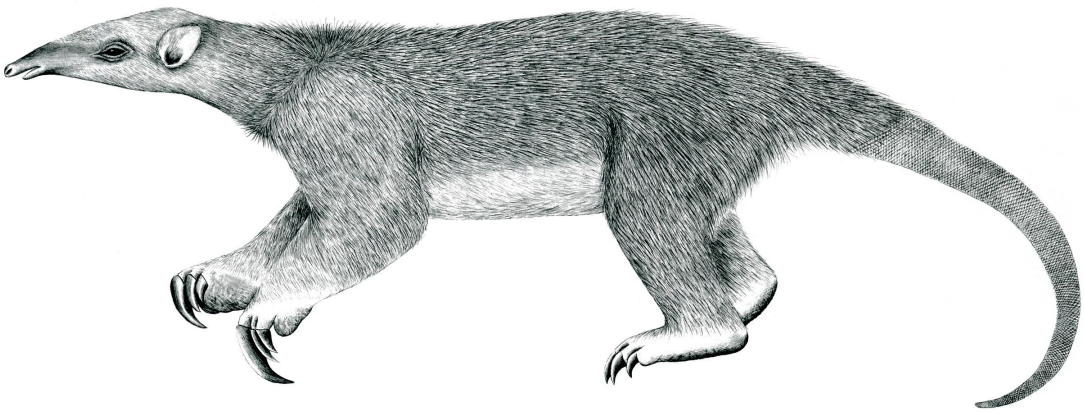
Tranalyzer2

bitForensic

Search packets for specific bits patterns



Tranalyzer Development Team

Contents

1 bitForensic

1.1 Description

The bitForensic plugin enables the user to search the packets for specific `uint8_t`, `uint16_t`, `uint32_t` and `uint64_t` patterns, combined with user-defined bit masks and nibble swap operations.

1.2 Dependencies

None.

1.2.1 Core Configuration

This plugin requires no special core configuration.

1.3 Configuration Flags

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

Name	Default	Description	Flags
`BF_PLEN`	0	0: Pattern search, 1: Length	
`BF_TOTLEN`	0	0: Residual length, 1: Total length	`BF_PLEN=1`
`BF_EXLEN`	2	Length excluded	`BF_PLEN=1`
`BF_PAT`	`0x0915`	Pattern: 1,2,4,8 bytes, defines `BF_PWDTH`	
`BF_MSK`	`0xffff`	Mask: 1,2,4,8 bytes, defines `BF_PWDTH`	
`BF_NETODR`	1	Search pattern network order	
`BF_NIBBLESWP`	0	Swap nibbles in search pattern (0-1)	
`BF_DNUM`	10	Max `bPDPos` flow storage	
`BF_SAVE_BCH`	0	Extract content: B/D info	
`BF_BSHIFT`	14	Start byte shift	`BF_SAVE_BCH=1`
`BF_RMDIR`	1	Empty `BF_V_PATH` before starting	`BF_SAVE_BCH=1`
`BF_V_PATH`	`"/tmp/BF/"`	Path for raw content	
`BF_FNAME`	`"bfnudel"`	Default content file name prefix	

1.3.1 Environment Variable Configuration Flags

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

- `BF_RMDIR`
- `BF_V_PATH`
- `BF_FNAME`

1.4 Flow File Output

The bitForensic plugin outputs the following columns:

Column	Type	Description	Flags
bfStat	H8	Status	
bfPDPos	R(U16)	Pattern Detect Position	

1.4.1 bfStat

The bfStat column is to be interpreted as follows:

bfStat	Description
0x01	Pattern found
0x02	Length byte, word found
0x04	—
0x08	Save content
0x10	BF_PWDTN0
0x20	BF_PWDTN1
0x40	BF_PWDTN2
0x80	—

1.5 Packet File Output

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

Column	Type	Description	Flags
bfStat	H8	Status	
bfPDPos	R(U16)	Pattern Detect Position	

1.6 Plugin Report Output

The following information is reported:

- Aggregated bfStat
- Number of bit patterns
- Max. number of file handles (BF_SAVE_BCH=1)