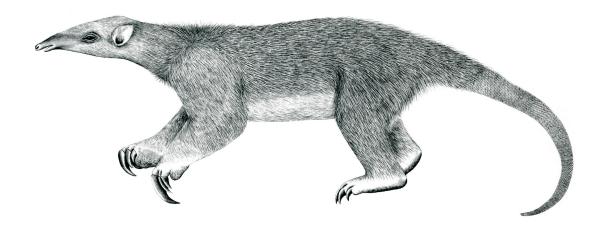
Tranalyzer2

igmpDecode



Internet Group Management Protocol (IGMP)



Tranalyzer Development Team

CONTENTS

Contents

1	igmj	oDecode .
	1.1	Description
	1.2	Required Files
	1.3	Configuration Flags
	1.4	Flow File Output
	1.5	Plugin Report Output
	1.6	Additional Output
		Post-Processing

1 igmpDecode

1.1 Description

This plugin analyzes IGMP traffic and provides absolute and relative statistics to the PREFIX_igmpStats.txt file.

1.2 Required Files

None

1.3 Configuration Flags

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

Name	Default	Description
IGMP_STATFILE	1	Print IGMP statistics in a separate file
IGMP_NOCODE	"_"	Symbol to use to represent the absence of a code
IGMP_SUFFIX	"_igmpStats.txt"	Suffix for output file

1.3.1 Environment Variable Configuration Flags

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

- IGMP_NOCODE
- IGMP_SUFFIX

1.4 Flow File Output

The igmpDecode plugin outputs the following columns:

Column	Type	Description	Flags
igmpStat	H8	Status	
igmpVersion	RI8	Version	
igmpAType	H32	Aggregated type	
igmpMCastAddr	IP4	Multicast address	
igmpNRec	U16	Number of records	

1.4.1 igmpStat

The igmpStat column is to be interpreted as follows:

igmpStat	Description
2^0 (=0x01)	IGMP message had invalid length
2^1 (=0x02)	IGMP message had invalid checksum
2^2 (=0x04)	IGMP message had invalid TTL ($\neq 1$)

igmpStat	Description
2^3 (=0x08)	IGMP message was invalid for other reasons

1.5 Plugin Report Output

The following information is reported:

- Aggregated igmpStat
- Number of IGMP packets
- Number of IGMP queries
- Number of IGMP reports
- IGMP query / report ratio

1.6 Additional Output

The plugin exports global statistics about IGMP traffic in the PREFIX_igmpStats.txt file. Note that the default suffix of "_igmpStats.txt" can be changed by editing the IGMP_SUFFIX flag.

1.7 Post-Processing

The protStat script can be used to sort the PREFIX_igmpStats.txt file for the most or least occurring types and codes. It can output the top or bottom N protocols or only those with at least a given percentage:

- list all the options: protStat --help
- for better readability, use protStat with tcol: protStat ... | tcol
- sorted list of types (by packets): protStat PREFIX_igmpStats.txt
- top 10 IGMP types and codes (by packets): protStat PREFIX_igmpStats.txt -n 10
- bottom 5 IGMP types and codes (by packets): protStat PREFIX_igmpStats.txt -n -5
- IGMP types and codes with packets percentage greater than 20%: protStat PREFIX_igmpStats.txt -p 20
- IGMP types and codes with packets percentage smaller than 5%: protStat PREFIX_igmpStats.txt -p -5