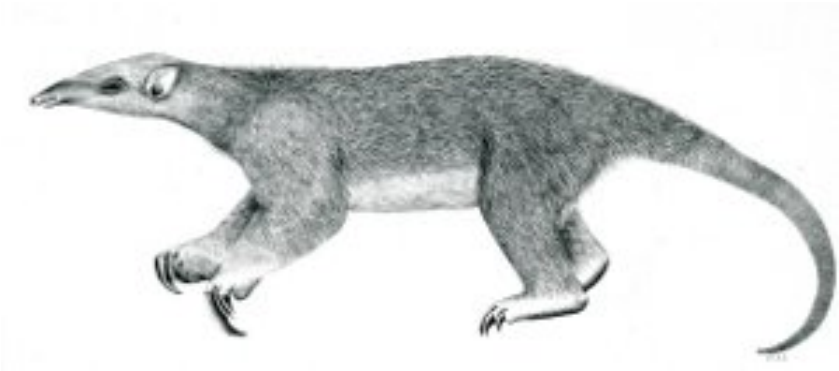
Tranalyzer2

macRecorder

MAC addresses



Tranalyzer Development Team

Contents

1 macRecorder

1.1 Description

The macRecorder plugin provides the source- and destination MAC address as well as the number of packets detected in the flow separated by an underscore. If there is more than one combination of MAC addresses, e.g., due to load balancing or router misconfiguration, the plugin prints all recognized MAC addresses separated by semicolons. The number of distinct source- and destination MAC addresses can be output by activating the `MR_NPAIRS` flag. The `MR_MANUF` flags controls the output of the manufacturers for the source and destination addresses. The representation of MAC addresses can be altered using the `MR_MAC_FMT` flag.

1.2 Dependencies

1.2.1 Required Files

The file `manuf.txt` is required if `MR_MANUF > 0` and file `maclbl.txt` is required if `MR_MACLBL > 0`.

1.3 Configuration Flags

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

Name	Default	Description
`MR_MAC_FMT`	1	Format for MAC addresses. 0: hex, 1: mac, 2: int
`MR_NPAIRS`	1	Whether (1) or not (0) to report number of distinct pairs
`MR_MANUF`	1	0: no manufacturers, 1: short names, 2: long names
`MR_MACLBL`	0	0: no mac label, 1: mac labeling
`MR_MAX_MAC`	16	max number of output MAC address per flow

1.4 Flow File Output

The macRecorder plugin outputs the following columns:

Column	Type	Description	Flags
`macPairs`	U32	Number of distinct src/dst MAC addresses pairs	`MR_NPAIRS=1`
`srcMac_dstMac_numP`	H64_H64_U64	Src/Dst MAC addresses, number of packets	`MR_MAC_FMT=0`
`srcMac_dstMac_numP`	MAC_MAC_U64	Src/Dst MAC addresses, number of packets	`MR_MAC_FMT=1`
`srcMac_dstMac_numP`	U64_U64_U64	Src/Dst MAC addresses, number of packets	`MR_MAC_FMT=2`
`srcManuf_dstManuf`	SC_SC	Src/Dst MAC manufacturers	`MR_MANUF=1`
`srcManuf_dstManuf`	S_S	Src/Dst MAC manufacturers	`MR_MANUF=2`
`srcLbl_dstLbl`	S_S	Src/Dst MAC label	`MR_MACLBL>0`

1.5 Packet File Output

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

Column	Description	Flags

Column	Description	Flags
srcManuf	Source MAC manufacturer	MR_MANUF=1
dstManuf	Destination MAC manufacturer	MR_MANUF=1

1.6 Example Output

Consider a host with MAC address aa:aa:aa:aa:aa:aa in a local network requesting a website from a public server. Due to load balancing, the opposite flow can be split and transmitted via two routers with MAC addresses bb:bb:bb:bb:bb:bb and cc:cc:cc:cc:cc:cc. The macRecorder plugin then produces the following output:

```
bb:bb:bb:bb:bb:bb_aa:aa:aa:aa:aa:aa_667;cc:cc:cc:cc:cc:cc_aa:aa:aa:aa:aa:aa_666
```