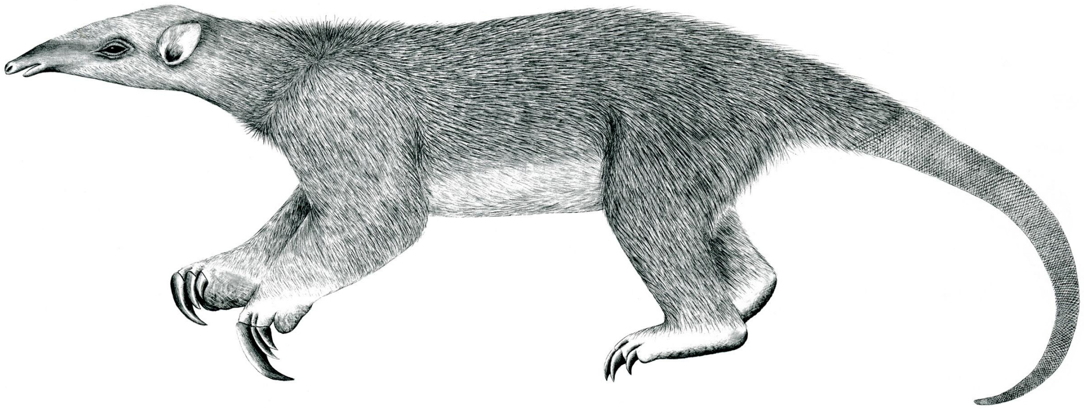
# Tranalyzer2

## smtpDecode

Simple Mail Transfer Protocol (SMTP)



Tranalyzer Development Team

# Contents

# 1 smtpDecode

## 1.1 Description

The smtpDecode plugin processes MAIL header and content information of a flow. The idea is to identify certain mail features and CNAMES.

## 1.2 Configuration Flags

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

| Name | Default | Description | Flags |
|---|---|---|---|
| SMTP_SAVE | 0 | 1: save content to SMTP_F_PATH | |
| SMTP_RMDIR | 1 | Empty SMTP_F_PATH before starting | SMTP_SAVE=1 |
| SMTP_BTFLD | 0 | 1: Bitfield coding of SMTP commands | |
| SMTP_RCTXT | 1 | 1: print response code text | |
| SMTP_MXNMLN | 70 | maximal name length | |
| SMTP_MXUNMLN | 25 | maximal user length | |
| SMTP_MXPNMLN | 15 | maximal PW length | |
| SMTP_MAXCNM | 8 | maximal number rec,trans codes | |
| SMTP_MAXUNM | 5 | maximal number server names | |
| SMTP_MAXPNM | 5 | maximal number server names | |
| SMTP_MAXSNM | 8 | maximal number of server addresses | |
| SMTP_MAXRNM | 8 | maximal number of rec EMail addresses | |
| SMTP_MAXTNM | 8 | maximal number of trans EMail addresses | |
| SMTP_F_PATH | "/tmp/SMTPFILES/" | Path for extracted content | |
| SMTP_NONAME | "nudel" | No name file name | |

### 1.2.1 Environment Variable Configuration Flags

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

- SMTP_RMDIR
- SMTP_F_PATH
- SMTP_NONAME

## 1.3 Flow File Output

The smtpDecode plugin outputs the following columns:

| Column | Type | Description | Flags |
|---|---|---|---|
| smtpStat | H8 | Status | |
| smtpCBF | H16 | Command codes bitfield | SMTP_BTFLD=1 |
| smtpCC | RSC | Command codes | |
| smtpRC | RU16 | Response codes | |
| smtpUsr | RS | Users | |

| Column | Type | Description | Flags |
|---|---|---|---|
| smtpPW | RS | Passwords | |
| smtpSANum | U8 | Number of server addresses | |
| smtpESANum | U8 | Number of email sender addresses | |
| smtpERANum | U8 | Number of email receiver addresses | |
| smtpSA | RS | Server send addresses | |
| smtpESA | RS | Email send addresses | |
| smtpERA | RS | Email receive addresses | |

### 1.3.1 smtpStat

The smtpStat column is to be interpreted as follows:

| smtpStat | | Description | Flags |
|---|---|---|---|
| $2^0$ | (=0x01) | SMTP ports found | |
| $2^1$ | (=0x02) | Authentication pending | |
| $2^2$ | (=0x04) | Data download pending | SMTP_SAVE=1 |
| $2^3$ | (=0x08) | User password pending | |
| $2^4$ | (=0x10) | flow write finished | SMTP_SAVE=1 |
| $2^5$ | (=0x20) | — | |
| $2^6$ | (=0x40) | File error | SMTP_SAVE=1 |
| $2^7$ | (=0x80) | Array overflow | |

### 1.3.2 smtpCBF

The smtpCBF column is to be interpreted as follows:

| smtpCBF | | Description |
|---|---|---|
| $2^0$ | (=0x0001) | HELO |
| $2^1$ | (=0x0002) | EHLO |
| $2^2$ | (=0x0004) | MAIL |
| $2^3$ | (=0x0008) | RCPT |
| $2^4$ | (=0x0010) | DATA |
| $2^5$ | (=0x0020) | RSET |
| $2^6$ | (=0x0040) | SEND |
| $2^7$ | (=0x0080) | SOML |

| smtpCBF | | Description |
|---|---|---|
| $2^8$ | (=0x0100) | SAML |
| $2^9$ | (=0x0200) | VRFY |
| $2^{10}$ | (=0x0400) | EXPN |
| $2^{11}$ | (=0x0800) | HELP |
| $2^{12}$ | (=0x1000) | NOOP |
| $2^{13}$ | (=0x2000) | QUIT |
| $2^{14}$ | (=0x4000) | TURN |
| $2^{15}$ | (=0x8000) | AUTH |

## 1.4 Packet File Output

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

| Column | Type | Description | Flags |
|---|---|---|---|
| smtpStat | H8 | Status | |

## 1.5 Plugin Report Output

The following information is reported:

- Aggregated smtpStat
- Number of SMTP packets
- Number of SMTP files

## 1.6 TODO

- fragmentation