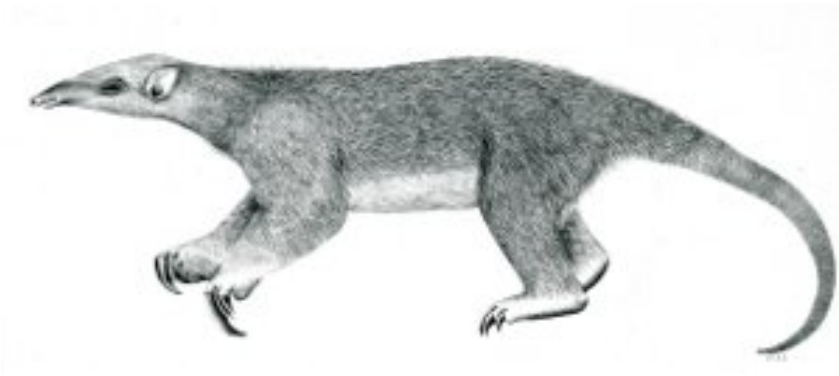
Tranalyzer2

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. User defined compiler switches are in *smtpDecode.h*.

1.2 Configuration Flags

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

Name	Default	Description
SMTP_SAVE	0	1: save content to SMTP_F_PATH
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
MAXCNM	8	maximal number rec,trans codes
MAXUNM	5	maxiaml number server names
MAXPNM	5	maxiaml number server names
MAXSNM	8	maximal number of server addresses
MAXRNM	8	maximal number of rec EMail addresses
MAXTNM	8	maximal number of trans EMail addresses

1.3 Flow File Output

The smtpDecode plugin outputs the following columns:

Column	Type	Description	Flags
smtpStat	H8	Status	
smtpCBF	H16	Command bit field	BITFIELD=1
smtpCC	RSC	Command Codes	
smtpRC	RI16	Response Codes	
smtpUsr	RS	SMTP Users	
smtpPW	RS	SMTP Passwords	
smtpSANum	I8	number of Server addresses	
smtpESANum	I8	number of email sender addresses	
smtpERANum	I8	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 describes the errors encountered during the flow lifetime:

smtpStat	Name	Description
2^0 (=0x01)	SMTP_INIT	SMTP ports found
2^1 (=0x02)	SMTP_AUTP	Authentication pending
2^2 (=0x04)	SMTP_DTP	data download pending, `SMTP_SAVE=1`
2^3 (=0x08)	PWSTATE	User PW pending
2^4 (=0x10)	SMTP_PWF	flow write finished, `SMTP_SAVE=1`
2^5 (=0x20)	—	—
2^6 (=0x40)	SMTP_FERR	File error, `SMTP_SAVE=1`
2^7 (=0x80)	SMTP_OVFL	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
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 TODO

- fragmentation