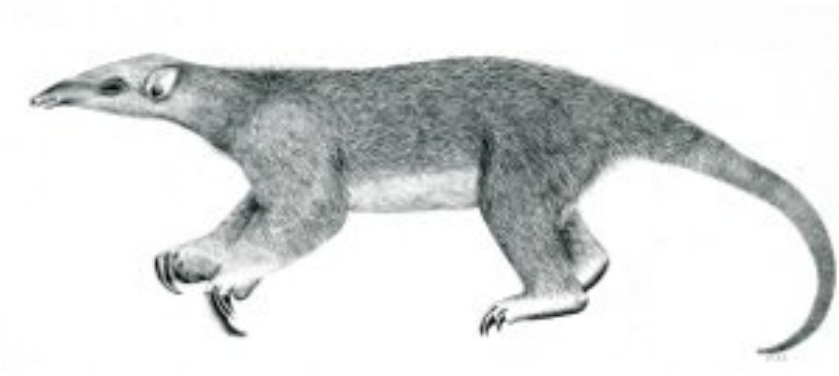
Tranalyzer2

popDecode

Post Office Protocol (POP)



Tranalyzer Development Team

Contents

1 popDecode

1.1 Description

The popDecode plugin processes MAIL header and content information of a flow. The idea is to identify certain pop mail features and save content. User defined compiler switches are in *popDecode.h*.

1.2 Configuration Flags

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

Name	Default	Description
POP_SAVE	0	save content to POP_F_PATH
MXNMLN	21	maximal name length
MXUNM	5	maximal number of users
MXPNM	5	maximal number of passwords/parameters
MXCNM	5	maximal number of content

1.3 Flow File Output

The popDecode plugin outputs the following columns:

Column	Type	Description
popStat	H8	Status bit field
popCBF	H16	POP command codes bit field
popCC	RSC	POP Command Codes
popRM	RU16	POP Response Codes
popUsrNum	U8	number of POP Users
popPwNum	U8	number of POP Passwords
popCNum	U8	number of POP parameters
popUsr	RS	POP Users
popPw	RS	POP Passwords
popC	RS	POP Content

1.3.1 popStat

The popStat column describes the errors encountered during the flow lifetime:

popStat	Name	Description
2^0 (=0x01)	POP2_INIT	pop2 port found
2^1 (=0x02)	POP3_INIT	pop3 port found
2^2 (=0x04)	POP_ROK	response +OK
2^3 (=0x08)	POP_RERR	response -ERR
2^4 (=0x10)	POP_DWF	data storage exists, POP_SAVE == 1
2^4 (=0x20)	POP_DTP	data storage in progress, POP_SAVE == 1
2^6 (=0x40)	POP_RNVL	response not valid or data

popStat	Name	Description
2^7 (=0x80)	POP_OVFL	array overflow

1.3.2 popCBF

The popCBF column describes the commands encountered during the flow lifetime:

popCBF	Name	Description
2^0 (=0x0001)	POP_APOP	Login with MD5 signature
2^1 (=0x0002)	POP_AUTH	Authentication request
2^2 (=0x0004)	POP_CAPA	Get a list of capabilities supported by the server
2^3 (=0x0008)	POP_DELE	Mark the message as deleted
2^4 (=0x0010)	POP_LIST	Get a scan listing of one or all messages
2^5 (=0x0020)	POP_NOOP	Return a +OK reply
2^6 (=0x0040)	POP_PASS	Cleartext password entry
2^7 (=0x0080)	POP_QUIT	Exit session. Remove all deleted messages from the server
2^8 (=0x0100)	POP_RETR	Retrieve the message
2^9 (=0x0200)	POP_RSET	Remove the deletion marking from all messages
2^{10} (=0x0400)	POP_STAT	Get the drop listing
2^{11} (=0x0800)	POP_STLS	Begin a TLS negotiation
2^{12} (=0x1000)	POP_TOP	Get the top n lines of the message
2^{13} (=0x2000)	POP_UIDL	Get a unique-id listing for one or all messages
2^{14} (=0x4000)	POP_USER	Mailbox login
2^{15} (=0x8000)	POP_XTND	

1.4 TODO

- IPv6
- fragmentation
- reply address extraction