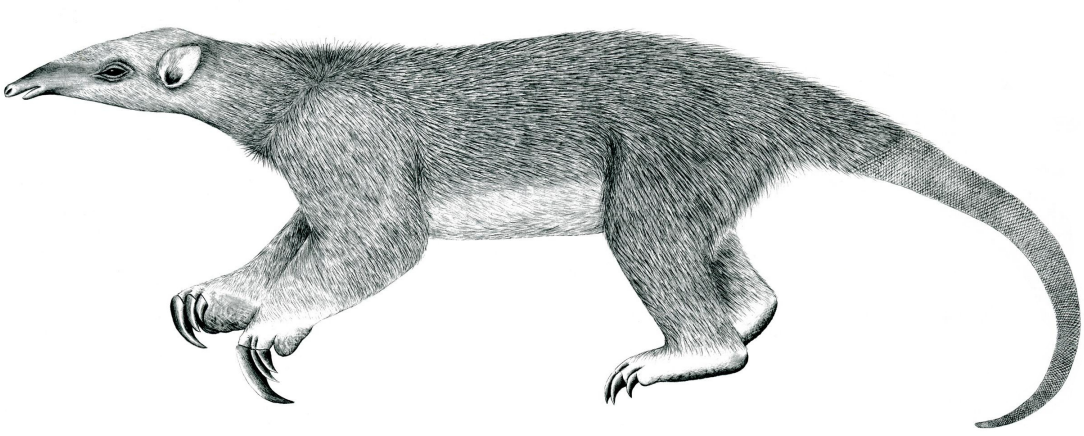
Tranalyzer2

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.

1.2 Configuration Flags

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

Name	Default	Description	Flags
POP_SAVE	0	Save content to POP_F_PATH	
POP_BTFLD	1	Enable bitfields output	
POP_MXNMLN	65	Maximal name length	
POP_MXUNM	5	Maximal number of users	
POP_MXPNM	5	Maximal number of passwords/parameters	
POP_MXCNM	10	Maximal number of content	
POP_RMDIR	1	Empty POP_F_PATH before starting	POP_SAVE=1
POP_F_PATH	"/tmp/POPFILES/"	Path for extracted content	POP_SAVE=1
POP_NONAME	"nudel"	No name file name	POP_SAVE=1

1.2.1 Environment Variable Configuration Flags

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

- POP_RMDIR
- POP_F_PATH
- POP_NONAME

1.3 Flow File Output

The popDecode plugin outputs the following columns:

Column	Type	Description	Flags
popStat	H16	Status	
popCBF	H16	POP command codes bitfield	POP_BTFLD=1
popCC	RSC	POP command codes	
popRM	RU16	POP response codes	
popUsrNum	U8	POP number of users	
popUsr	RS	POP users	
popPwNum	U8	POP number of passwords	
popPw	RS	POP passwords	
popCNum	U8	POP number of parameters	
popC	RS	POP content	

1.3.1 popStat

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

	popStat	Description	Flags
2^0	(=0x0001)	POP2 port found	
2^1	(=0x0002)	POP3 port found	
2^2	(=0x0004)	Response `+OK`	
2^3	(=0x0008)	Response `-ERR`	
2^4	(=0x0010)	Data storage exists	`POP_SAVE=1`
2^5	(=0x0020)	Data storage in progress	`POP_SAVE=1`
2^6	(=0x0040)	Response not valid or data	
2^7	(=0x0080)	Array overflow	
2^8	(=0x0100)	Authentication pending	
2^9	(=0x0200)	Return path pending	
2^{10}	(=0x0400)	—	
2^{11}	(=0x0800)	—	
2^{12}	(=0x1000)	—	
2^{13}	(=0x2000)	—	
2^{14}	(=0x4000)	—	
2^{15}	(=0x8000)	—	

1.3.2 popCBF

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

	popCBF	Description
2^0	(=0x0001)	Login with MD5 signature
2^1	(=0x0002)	Authentication request
2^2	(=0x0004)	Get a list of capabilities supported by the server
2^3	(=0x0008)	Mark the message as deleted
2^4	(=0x0010)	Get a scan listing of one or all messages
2^5	(=0x0020)	Return a `+OK` reply
2^6	(=0x0040)	Cleartext password entry
2^7	(=0x0080)	Exit session. Remove all deleted messages from the server
2^8	(=0x0100)	Retrieve the message
2^9	(=0x0200)	Remove the deletion marking from all messages
2^{10}	(=0x0400)	Get the drop listing
2^{11}	(=0x0800)	Begin a TLS negotiation
2^{12}	(=0x1000)	Get the top n lines of the message

	popCBF	Description
2^{13}	(=0x2000)	Get a unique-id listing for one or all messages
2^{14}	(=0x4000)	Mailbox login
2^{15}	(=0x8000)	

1.4 Packet File Output

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

Column	Type	Description	Flags
popStat	H16	Status	

1.5 Plugin Report Output

The following information is reported:

- POP status
- Number of POP packets
- Number of files extracted (`POP_SAVE=1`)

1.6 TODO

- fragmentation