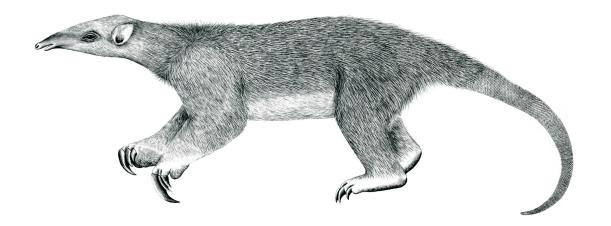
# Tranalyzer2

mqttDecode



MQ Telemetry Transport Protocol (MQTT)



Tranalyzer Development Team

CONTENTS

# **Contents**

1	mqt	tDecode .
	1.1	Description
	1.2	Configuration Flags
	1.3	Flow File Output
	1.4	Packet File Output
		Monitoring Output
	1.6	Plugin Report Output
		Additional Output

# 1 mqttDecode

### 1.1 Description

The mqttDecode plugin analyzes the MQ Telemetry Transport Protocol (MQTT).

## 1.2 Configuration Flags

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

Name	Default	Description	Flags
MQTT_TOPIC_MSG	1	save topics and messages in a separate file	
MQTT_PROTO_LEN	32	Max length for protocol name	
MQTT_CLIENT_ID_LEN	32	Max length for client ID	
MQTT_TOPIC_LEN	32	Max length for topic	
MQTT_TOPIC_MSG_SUFFIX	"_mqtt_msg.txt"	suffix to use for topics and messages file	MQTT_TOPIC_MSG=1

### 1.2.1 Environment Variable Configuration Flags

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

• MQTT\_TOPIC\_MSG\_SUFFIX (require MQTT\_TOPIC\_MSG=1)

## 1.3 Flow File Output

The mqttDecode plugin outputs the following columns:

Column	Type	Description	Flags
mqttStat	H8	Status	
mqttCPT	H16	Control packet types	
mqttProto	SC	Protocol name	
mqttProtoLevel	U8	Protocol level	
mqttClientID	SC	Client ID	
mqttConAck	H8	Connection status	
mqttTopic	S	Topics	

### 1.3.1 mqttStat

The mqttStat column is to be interpreted as follows:

mqttStat	Description
0x01	Flow is MQTT
$0 \times 02$	_
$0 \times 04$	_
0x08	_

1.3 Flow File Output 1 MQTTDECODE

mqttStat	Description
0x10	Reserved Control Packet Type (mqttCPT) (0 or 15) was used
0x20	_
0x40	_
0x <mark>8</mark> 0	Packet snapped

# 1.3.2 mqttCPT

The  $\mathtt{mqttCPT}$  column is to be interpreted as follows:

Description
Reserved
Client request to connect to server
Connect acknowledgment
Publish message
Publish acknowledgment
Publish complete (assured delivery part 1)
Publish complete (assured delivery part 2)
Publish complete (assured delivery part 3)
Subscribe request
Subscribe acknowledgment
Unsubscribe request
Unsubscribe acknowledgment
PING request
PING response
Client is disconnecting
Reserved

# 1.3.3 mqttConAck

The  ${\tt mqttConAck}$  column is to be interpreted as follows:

mqttConAck	Description
	Connection Accepted
	Connection Refused, unacceptable protocol version
	Connection Refused, identifier rejects
$2^3$ (=0x08)	Connection Refused, Server unavailable
	Connection Refused, bad user name or password
$2^5$ (=0x20)	Connection Refused, not authorized

1 MQTTDECODE 1.4 Packet File Output

mqttConAck	Description
2 <sup>6</sup> (=0x40)	_
$2^7$ (=0x80)	Return codes from $0x06$ to $0xff$ are reserved for future use

## **1.4** Packet File Output

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

Column	Type	Description	Flags
mqttStat	H8	Status	

# 1.5 Monitoring Output

In monitoring mode, the mqttDecode plugin outputs the following columns:

Column	Type	Description	Flags
mqttPkts	U64	Number of MQTT packets	

# 1.6 Plugin Report Output

The following information is reported:

- Aggregated mqttStat
- Number of MQTT packets
- Aggregated mqttCPT
- Aggregated mqttConAck

## 1.7 Additional Output

Non-standard output:

• PREFIX\_mqtt\_msg.txt: list of topics and messages

#### 1.7.1 \_mqtt\_msg.txt Output

Column	Type	Description	Flags
pktNo	U64	Packet number	
flowInd	U64	Flow index	
mqttTopic	S	Topic	
mqttMsg	S	Message	