
Tranalyzer2

mqttDecode



MQ Telemetry Transport Protocol (MQTT)



Tranalyzer Development Team

Contents

1 mqttDecode 1

1.1 Description 1

1.2 Configuration Flags 1

1.3 Flow File Output 1

1.4 Packet File Output 3

1.5 Monitoring Output 3

1.6 Plugin Report Output 3

1.7 Additional Output 3

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 (ENVCTRL>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
0x02	—
0x04	—
0x08	—

mqttStat	Description
0x10	Reserved Control Packet Type (mqttCPT) (0 or 15) was used
0x20	—
0x40	—
0x80	Packet snapped

1.3.2 mqttCPT

The mqttCPT column is to be interpreted as follows:

mqttCPT	Description
2 ⁰ (=0x0001)	Reserved
2 ¹ (=0x0002)	Client request to connect to server
2 ² (=0x0004)	Connect acknowledgment
2 ³ (=0x0008)	Publish message
2 ⁴ (=0x0010)	Publish acknowledgment
2 ⁵ (=0x0020)	Publish complete (assured delivery part 1)
2 ⁶ (=0x0040)	Publish complete (assured delivery part 2)
2 ⁷ (=0x0080)	Publish complete (assured delivery part 3)
2 ⁸ (=0x0100)	Subscribe request
2 ⁹ (=0x0200)	Subscribe acknowledgment
2 ¹⁰ (=0x0400)	Unsubscribe request
2 ¹¹ (=0x0800)	Unsubscribe acknowledgment
2 ¹² (=0x1000)	PING request
2 ¹³ (=0x2000)	PING response
2 ¹⁴ (=0x4000)	Client is disconnecting
2 ¹⁵ (=0x8000)	Reserved

1.3.3 mqttConAck

The mqttConAck column is to be interpreted as follows:

mqttConAck	Description
2 ⁰ (=0x01)	Connection Accepted
2 ¹ (=0x02)	Connection Refused, unacceptable protocol version
2 ² (=0x04)	Connection Refused, identifier rejects
2 ³ (=0x08)	Connection Refused, Server unavailable
2 ⁴ (=0x10)	Connection Refused, bad user name or password
2 ⁵ (=0x20)	Connection Refused, not authorized

mqttConAck	Description
2 ⁶ (=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	