
Tranalyzer2

gquicDecode



Google Quick UDP Internet Connections (GQUIC)



Tranalyzer Development Team

Contents

1	gquicDecode	1
1.1	Description	1
1.2	Configuration Flags	1
1.3	Flow File Output	1
1.4	Packet File Output	2
1.5	Plugin Report Output	3
1.6	Known Bugs and Limitations	3

1 gquicDecode

1.1 Description

The gquicDecode plugin analyzes GQUIC traffic.

1.2 Configuration Flags

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

Name	Default	Description
GQUIC_SLEN	63	Max length for string columns, e.g., gquicSNI
GQUIC_DEBUG	0	0: do not print any debug messages 1: print warnings about unhandled cases 2: + print regular info about decoding status

1.3 Flow File Output

The gquicDecode plugin outputs the following columns:

Column	Type	Description	Flags
gquicStat	H8	Status	
gquicPubFlags	H8	Public Flags	
gquicFrameTypes	H16	Frame Types	
gquicCID	U64	Connection ID	
gquicSNI	S	Server Name Indication (SNI)	
gquicUAID	S	Client's User Agent ID	

1.3.1 gquicStat

The gquicStat column is to be interpreted as follows:

gquicStat	Description
0x01	Flow is GQUIC
0x02	Handshake (Stream number is 1)
0x04	Connection ID changed
0x08	—
0x10	—
0x20	—
0x40	Packet was snapped (t2buf failed)
0x80	Packet was malformed, e.g., covert channel

1.3.2 gquicPubFlags

The gquicPubFlags column is to be interpreted as follows:

gquicPubFlags	Description
0x01	Header contains a GQUIC Version
0x02	Public Reset packet
0x04	32 byte diversification nonce is present (version >= 33)
0x08	8 byte Connection ID is present (version >= 33)
0x0c	8 byte Connection ID is present (version < 33)
0x30	Number of low-order bytes of the packet number
0x40	Reserved for multipath use
0x80	Reserved (MUST be 0)

1.3.3 gquicFrameTypes

The gquicFrameTypes column is to be interpreted as follows:

gquicFrameTypes	Description
2 ⁰ (=0x0001)	PADDING
2 ¹ (=0x0002)	RST_STREAM
2 ² (=0x0004)	CONNECTION_CLOSE
2 ³ (=0x0008)	GOAWAY
2 ⁴ (=0x0010)	WINDOW_UPDATE
2 ⁵ (=0x0020)	BLOCKED
2 ⁶ (=0x0040)	STOP_WAITING
2 ⁷ (=0x0080)	PING
Special Frame Types:	
2 ¹⁴ (=0x4000)	ACK
2 ¹⁵ (=0x8000)	STREAM

1.4 Packet File Output

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

Column	Type	Description	Flags
gquicPubFlags	H8	Public Flags	
gquicVersion	SC	Version	
gquicPktNo	U64	Packet Number	
gquicCID	U64	Connection ID	

1.5 Plugin Report Output

The following information is reported:

- Aggregated `gquicStat`
- Number of GQUIC packets
- Number of GQUIC Client Hello packets
- Number of GQUIC Rejection packets
- Number of GQUIC Public Reset packets

1.6 Known Bugs and Limitations

- The `gquicDecode` plugin assumes every UDP packet on port 80 or 443 is GQUIC...