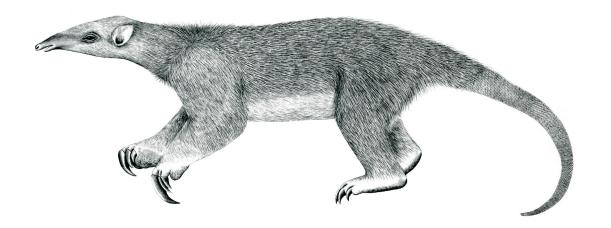
Tranalyzer2

gquicDecode



Google Quick UDP Internet Connections (GQUIC)



Tranalyzer Development Team

CONTENTS

Contents

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

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	Н8	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 ${\tt gquicStat}$ 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

1.4 Packet File Output 1 GQUICDECODE

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

gquicF	TrameTypes	Description		
2^{0}	(=0x0001)	PADDING		
2^{1}	(=0x0002)	RST_STREAM		
2^{2}	$(=0 \times 0 0 0 4)$	CONNECTION_CLOSE		
2^3	(=0x0008)	GOAWAY		
2^{4}	(=0x0010)	WINDOW_UPDATE		
	(=0x0020)	BLOCKED		
2^{6}	$(=0 \times 0040)$	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...