BYTE0	BYTE1	BYTE2	BYTE3	CLIENT HELLO
0x03	0x03	random0	random1	
random2	random3	0x00	0x13	
0x01	0x13	0x02	0x13	
0x03	0x13	0x04	0x13	
0x05	0x00	0x43	0x03	
0x04	0x03	0x03	0x03	
0x01				

- Protocol Legacy Version (0x0303)
- Random data (4)
- Cipher suites
- Legacy compression method = 0x00
- Extensions (supported versions, PSK, KEY_SHARE, OR BOTH for (EC) DHE)
- Legacy session ID

BYTE0	BYTE1	BYTE2	BYTE3	SERVER HELLO
0x03	0x03	random0	random1	
random2	random3	0x00	0x13	
0x01	0x00	0x43	0x03	
0x04				

- Protocol Legacy Version (0x0303)
- Random data (4)
- Selected Cipher suites
- Legacy compression method = 0x00
- Extensions (supported versions, PSK, KEY_SHARE, OR BOTH for (EC) DHE)
- Legacy session ID

BYTE0	BYTE1	BYTE2	BYTE3	SERVER_NAME
0x00				

BYTE0	BYTE1	BYTE2	BYTE3	MAX_FRAGMENT_LEN
0x01				

BYTE0	BYTE1	BYTE2	BYTE3	STATUS_REQUEST
0x05				

BYTE0	BYTE1	BYTE2	BYTE3	SUPPORTED_GROUPS
0x0A	GROUP_00	GROUP_01		
0x0A	0x00	0x17	0x00	
0x18	0x00	0x19	0x00	
0x1D	0x00	0x1E	0x01	
0x00	0x01	0x01	0x01	
0x02	0x01	0x03	0x01	
0x04				

BYTE0	BYTE1	BYTE2	BYTE3	SIGNATURE_ALGORITHMS
0x0D	SIGSCHEME0	SIGSCHEME1		
0x0D	0x04	0x01	0x05	
0x01	0x06	0x01	0x04	
0x03	0x05	0x03	0x06	
0x03	0x08	0x04	0x08	
0x05	0x08	0x06	0x08	
0x07	0x08	0x08	0x08	
0x09	0x08	0x0B	0x02	
0x01	0x02	0x03		

BYTE0	BYTE1	BYTE2	BYTE3	USE SRTP
0x0E				

BYTE0	BYTE1	BYTE2	BYTE3	HEARTBEAT
0x0F				

BYTE0	BYTE1	BYTE2	BYTE3	APPLICATION_LAYER_PROTOCOL_NEGOTIATION
0x10				

BYTE0	BYTE1	BYTE2	BYTE3	SIGNED CERTIFICATE TIMESTAMP
0x12				

BYTE0	BYTE1	BYTE2	BYTE3	CLIENT CERTIFICATE TYPE
0x13	CERT_TYPE	CERT_DATA_00	CERT_DATA_NN	

BYTE0	BYTE1	BYTE2	BYTE3	SERVER CERTIFICATE TYPE
0x14	CERT_TYPE	CERT_DATA_00	CERT_DATA_NN	

BYTE0	BYTE1	BYTE2	BYTE3	PADDING
0x15				

BYTE0	BYTE1	BYTE2	BYTE3	PRE_SHARED_KEY
0x29	0x00			PSK
0x29	0x01			PSK with EC(DHE)

BYTE0	BYTE1	BYTE2	BYTE3	EARLY DATA
0x2A	SIZE0	SIZE1	SIZE2	
SIZE3	EARLY_0	...	EARLY_N	

BYTE0	BYTE1	BYTE2	BYTE3	SUPPORTED VERSIONS
0x2B	0x03	0x04	0x03	
0x03	0x03	0x02		

BYTE0	BYTE1	BYTE2	BYTE3	COOKIE
0x2C	COOKIE_0	...	COOKIE_N	

BYTE0	BYTE1	BYTE2	BYTE3	PSK KEY EXCHANGE MODES
0x2D				

BYTE0	BYTE1	BYTE2	BYTE3	CERTIFICATE AUTHORITIES
0x2F	NAME_00	...	NAME_NN	

BYTE0	BYTE1		BYTE3	OID FILTERS
0x30				

BYTE0	BYTE1	BYTE2	BYTE3
0x31			

POST HANDSHAKE AUTH
(contains no data)

BYTE0	BYTE1	BYTE2	BYTE3
0x32			

SIGNATURE ALGORITHM CERT

BYTE0	BYTE1	BYTE2	BYTE3
0x33	GROUP_00	GROUP_01	PARAM_00
PARAM_01	PARAM_02	…	PARAM_NN

KEY SHARE (CLIENT)

BYTE0	BYTE1	BYTE2	BYTE3
0x33	GROUP_00	GROUP_01	

KEY SHARE (SERVER)

BYTE0	BYTE1	BYTE2	BYTE3
0x17	**0x03**	**0x03**	**LEN_00**
LEN_01	**ENC_00**	**…**	**ENC_NN**

APPLICATION RECORD
2^14 bytes maximum

	Plaintext
	Encrypted

DATA_00	…	DATA_NN	0x17
PAD_00	…	PAD_NN	

PLAINTEXT
PADDING VARIABLE (MAY BE ZERO - USED FOR TRAFFIC SHAPING)
MUST BE ALL ZERO

0x17	PAD_00	…	PAD_NN

ZERO LENGTH PLAINTEXT