D)/TEO	DVEET	2)/752	2)/772	Tours I I	
ВҮТЕО	BYTE1	BYTE2	BYTE3	CLIENT HELLO	
0x03	0x03	random0	random1		Protocol Legacy Version (0x0303)
random2	random3	0x00	0x13		Random data (4)
0x01	0x13	0x02	0x13		Cipher suites
0x03	0x13	0x04	0x13		Legacy compression method = 0x00
0x05	0x00	0x43	0x03		Extensions (supported versions, PSK, KEY_SHARE, OR BOTH for (EC) DHE)
0x04	0x03	0x03	0x03	_	Legacy session ID
0x01	UNUS	ONOS	UNUS .		Legacy Session is
ВҮТЕО	BYTE1	BYTE2	BYTE3	SERVER HELLO	
0x03	0x03	random0	random1	SERVERTIEEES	Protocol Legacy Version (0x0303)
random2	random3	0x00	0x13		Random data (4)
0x01	0x00	0x43	0x03		Selected Cipher suites
0x04					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		-		'	
ВҮТЕО	BYTE1	BYTE2	BYTE3	MAX_FRAGMENT_LEN	
0x01	DITE	51122	DITES	MAX_I IVAGINEIVI_LEIV	
0x01					
DVTEO	DVTF4	DVTF2	DVTF2	Tetatus producet	
BYTE0	BYTE1	BYTE2	BYTE3	STATUS_REQUEST	
0x05					
_				<b></b>	
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		
0x02	OVOI	UAU3	OVOI		
0x04					
DVTEO	DVTE4	DVTF2	DVTF3	TOUCHATURE ALCORITURAS	
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		0x0B	0x02	_	
	0x08		UXUZ		
0x01	0x02	0x03	I		
21772	D. (2004)	2,772	DV=50		
BYTE0	BYTE1	BYTE2	BYTE3	USE SRTP	
0x0E					
BYTE0	BYTE1	BYTE2	BYTE3	HEARTBEAT	
0x0F					
				<u></u>	
ВҮТЕО	BYTE1	BYTE2	BYTE3	APPLICATION_LAYER_PROTO	COL_NEGOTIATION
0x10				<del></del>	
BYTE0	BYTE1	BYTE2	BYTE3	SIGNED CERTIFICATE TIMESTA	AMP
0x12					
BYTE0	BYTE1	BYTE2	BYTE3	CLIENT CERTIFICATE TYPE	
DITEO	DITE	DITLE	DITES	- CLIENT CERTIFICATE THE	
0v12	CEPT TVDE	CEPT DATA OO	CEDT DATA NINI		
0x13	CERT_TYPE	CERT_DATA_00	CERT_DATA_NN		
				CEDVED CEDTIFICATE TYPE	
BYTE0	BYTE1	BYTE2	BYTE3	SERVER CERTIFICATE TYPE	
				SERVER CERTIFICATE TYPE	
<b>BYTE0</b> 0x14	BYTE1  CERT_TYPE	BYTE2  CERT_DATA_00	BYTE3  CERT_DATA_NN		
BYTE0 0x14 BYTE0	BYTE1	BYTE2	BYTE3	SERVER CERTIFICATE TYPE  PADDING	
<b>BYTE0</b> 0x14	BYTE1  CERT_TYPE	BYTE2  CERT_DATA_00	BYTE3  CERT_DATA_NN		
BYTE0 0x14 BYTE0	BYTE1  CERT_TYPE	BYTE2  CERT_DATA_00	BYTE3  CERT_DATA_NN		
BYTE0 0x14 BYTE0	BYTE1  CERT_TYPE	BYTE2  CERT_DATA_00	BYTE3  CERT_DATA_NN		
BYTE0 0x14 BYTE0	BYTE1  CERT_TYPE	BYTE2  CERT_DATA_00	BYTE3  CERT_DATA_NN		
BYTE0 0x14 BYTE0	BYTE1  CERT_TYPE	BYTE2  CERT_DATA_00	BYTE3  CERT_DATA_NN	PADDING	
BYTE0 0x14 BYTE0 0x15	BYTE1  CERT_TYPE  BYTE1  BYTE1	BYTE2  CERT_DATA_00  BYTE2	BYTE3  CERT_DATA_NN  BYTE3	PADDING   PRE_SHARED_KEY	
BYTE0 0x14  BYTE0 0x15  BYTE0 0x29	BYTE1  CERT_TYPE  BYTE1  BYTE1  0x00	BYTE2  CERT_DATA_00  BYTE2	BYTE3  CERT_DATA_NN  BYTE3	PADDING    PRE_SHARED_KEY PSK	
BYTE0 0x14  BYTE0 0x15  BYTE0	BYTE1  CERT_TYPE  BYTE1  BYTE1	BYTE2  CERT_DATA_00  BYTE2	BYTE3  CERT_DATA_NN  BYTE3	PADDING   PRE_SHARED_KEY	
BYTE0 0x14  BYTE0 0x15  BYTE0 0x29 0x29	BYTE1 CERT_TYPE  BYTE1  BYTE1  0x00 0x01	BYTE2  CERT_DATA_00  BYTE2  BYTE2	BYTE3  CERT_DATA_NN  BYTE3  BYTE3	PADDING  PRE_SHARED_KEY PSK PSK with EC(DHE)	
BYTE0 0x14  BYTE0 0x15  BYTE0 0x29 0x29 0x29  BYTE0	BYTE1  CERT_TYPE  BYTE1  0x00 0x01  BYTE1	BYTE2  CERT_DATA_00  BYTE2  BYTE2  BYTE2	BYTE3  CERT_DATA_NN  BYTE3  BYTE3	PADDING    PRE_SHARED_KEY PSK	
BYTE0 0x14  BYTE0 0x15  BYTE0 0x29 0x29  BYTE0 0x29	BYTE1 CERT_TYPE  BYTE1  Ox00 Ox01  BYTE1  SIZE0	BYTE2  CERT_DATA_00  BYTE2  BYTE2	BYTE3  CERT_DATA_NN  BYTE3  BYTE3  SIZE2	PADDING  PRE_SHARED_KEY PSK PSK with EC(DHE)	
BYTE0 0x14  BYTE0 0x15  BYTE0 0x29 0x29 0x29  BYTE0	BYTE1  CERT_TYPE  BYTE1  0x00 0x01  BYTE1	BYTE2  CERT_DATA_00  BYTE2  BYTE2  BYTE2	BYTE3  CERT_DATA_NN  BYTE3  BYTE3	PADDING  PRE_SHARED_KEY PSK PSK with EC(DHE)	
BYTE0 0x14  BYTE0 0x15  BYTE0 0x29 0x29 0x29  BYTE0 0x2A SIZE3	BYTE1 CERT_TYPE  BYTE1  0x00 0x01  BYTE1  SIZE0 EARLY_0	BYTE2  CERT_DATA_00  BYTE2  BYTE2  BYTE2  SIZE1	BYTE3  CERT_DATA_NN  BYTE3  BYTE3  BYTE3  SIZE2  EARLY_N	PADDING  PRE_SHARED_KEY PSK PSK with EC(DHE)  EARLY DATA	
BYTE0 0x14  BYTE0 0x15  BYTE0 0x29 0x29 0x29  BYTE0 0x2A SIZE3	BYTE1 CERT_TYPE  BYTE1  BYTE1  0x00 0x01  BYTE1  SIZE0 EARLY_0  BYTE1	BYTE2  CERT_DATA_00  BYTE2  BYTE2  SIZE1  BYTE2	BYTE3  CERT_DATA_NN  BYTE3  BYTE3  SIZE2  EARLY_N  BYTE3	PADDING  PRE_SHARED_KEY PSK PSK with EC(DHE)	
BYTE0 0x14  BYTE0 0x15  BYTE0 0x29 0x29 0x29  BYTE0 0x2A SIZE3	BYTE1 CERT_TYPE  BYTE1  0x00 0x01  BYTE1  SIZE0 EARLY_0	BYTE2  CERT_DATA_00  BYTE2  BYTE2  BYTE2  SIZE1	BYTE3  CERT_DATA_NN  BYTE3  BYTE3  BYTE3  SIZE2  EARLY_N	PADDING  PRE_SHARED_KEY PSK PSK with EC(DHE)  EARLY DATA	
BYTE0 0x14  BYTE0 0x15  BYTE0 0x29 0x29 0x29  BYTE0 0x2A SIZE3	BYTE1 CERT_TYPE  BYTE1  BYTE1  0x00 0x01  BYTE1  SIZE0 EARLY_0  BYTE1	BYTE2  CERT_DATA_00  BYTE2  BYTE2  SIZE1  BYTE2	BYTE3  CERT_DATA_NN  BYTE3  BYTE3  SIZE2  EARLY_N  BYTE3	PADDING  PRE_SHARED_KEY PSK PSK with EC(DHE)  EARLY DATA	
BYTE0 0x14  BYTE0 0x15  BYTE0 0x29 0x29 0x29  BYTE0 0x2A SIZE3  BYTE0 0x2B	BYTE1  CERT_TYPE  BYTE1  Ox00  Ox01  BYTE1  SIZE0  EARLY_0  BYTE1  Ox03	BYTE2  CERT_DATA_00  BYTE2  BYTE2  SIZE1   BYTE2  Ox04	BYTE3  CERT_DATA_NN  BYTE3  BYTE3  SIZE2  EARLY_N  BYTE3	PADDING  PRE_SHARED_KEY PSK PSK with EC(DHE)  EARLY DATA	
BYTE0 0x14  BYTE0 0x15  BYTE0 0x29 0x29 0x29  BYTE0 0x2A SIZE3  BYTE0 0x2B	BYTE1  CERT_TYPE  BYTE1  Ox00  Ox01  BYTE1  SIZE0  EARLY_0  BYTE1  Ox03	BYTE2  CERT_DATA_00  BYTE2  BYTE2  SIZE1   BYTE2  Ox04	BYTE3  CERT_DATA_NN  BYTE3  BYTE3  SIZE2  EARLY_N  BYTE3	PADDING  PRE_SHARED_KEY PSK PSK with EC(DHE)  EARLY DATA	
BYTEO 0x14  BYTEO 0x15  BYTEO 0x29 0x29  BYTEO 0x2A SIZE3  BYTEO 0x2B 0x03	BYTE1  CERT_TYPE  BYTE1  0x00 0x01  BYTE1  SIZE0 EARLY_0  BYTE1  0x03 0x03	BYTE2  CERT_DATA_00  BYTE2  BYTE2  SIZE1   BYTE2  Ox04  Ox02	BYTE3  CERT_DATA_NN  BYTE3  BYTE3  SIZE2  EARLY_N  BYTE3  Ox03	PADDING  PRE_SHARED_KEY PSK PSK with EC(DHE)  EARLY DATA  SUPPORTED VERSIONS	
BYTE0 0x14  BYTE0 0x15  BYTE0 0x29 0x29  BYTE0 0x2A SIZE3  BYTE0 0x2B 0x03	BYTE1  CERT_TYPE  BYTE1  BYTE1  0x00  0x01  BYTE1  SIZE0  EARLY_0  BYTE1  0x03  0x03  0x03	BYTE2  CERT_DATA_00  BYTE2  BYTE2  SIZE1   BYTE2  Ox04  Ox02	BYTE3  CERT_DATA_NN  BYTE3  BYTE3  SIZE2  EARLY_N  BYTE3  Ox03	PADDING  PRE_SHARED_KEY PSK PSK with EC(DHE)  EARLY DATA	
BYTEO 0x14  BYTEO 0x15  BYTEO 0x29 0x29  BYTEO 0x2A SIZE3  BYTEO 0x2B 0x03	BYTE1  CERT_TYPE  BYTE1  0x00 0x01  BYTE1  SIZE0 EARLY_0  BYTE1  0x03 0x03	BYTE2  CERT_DATA_00  BYTE2  BYTE2  SIZE1   BYTE2  Ox04  Ox02	BYTE3  CERT_DATA_NN  BYTE3  BYTE3  SIZE2  EARLY_N  BYTE3  Ox03	PADDING  PRE_SHARED_KEY PSK PSK with EC(DHE)  EARLY DATA  SUPPORTED VERSIONS	
BYTE0 0x14  BYTE0 0x15  BYTE0 0x29 0x29  BYTE0 0x2A SIZE3  BYTE0 0x2B 0x03	BYTE1  CERT_TYPE  BYTE1  BYTE1  0x00  0x01  BYTE1  SIZE0  EARLY_0  BYTE1  0x03  0x03  0x03	BYTE2  CERT_DATA_00  BYTE2  BYTE2  SIZE1   BYTE2  Ox04  Ox02	BYTE3  CERT_DATA_NN  BYTE3  BYTE3  SIZE2  EARLY_N  BYTE3  Ox03	PADDING  PRE_SHARED_KEY PSK PSK with EC(DHE)  EARLY DATA  SUPPORTED VERSIONS	
BYTE0 0x14  BYTE0 0x15  BYTE0 0x29 0x29  BYTE0 0x2A SIZE3  BYTE0 0x2B 0x03  BYTE0 0x2C	BYTE1  CERT_TYPE  BYTE1  0x00  0x01  BYTE1  SIZE0  EARLY_0  BYTE1  0x03  0x03  0x03  BYTE1  COOKIE_0	BYTE2 CERT_DATA_00  BYTE2  BYTE2  SIZE1   BYTE2  Ox04 Ox02  BYTE2	BYTE3  CERT_DATA_NN  BYTE3  BYTE3  SIZE2  EARLY_N  BYTE3  Ox03	PADDING  PRE_SHARED_KEY PSK PSK with EC(DHE)  EARLY DATA  SUPPORTED VERSIONS  COOKIE	
BYTEO 0x14  BYTEO 0x15  BYTEO 0x29 0x29  BYTEO 0x2A SIZE3  BYTEO 0x2B 0x03  BYTEO 0x2C	BYTE1  CERT_TYPE  BYTE1  BYTE1  0x00  0x01  BYTE1  SIZE0  EARLY_0  BYTE1  0x03  0x03  0x03	BYTE2  CERT_DATA_00  BYTE2  BYTE2  SIZE1   BYTE2  Ox04  Ox02	BYTE3  CERT_DATA_NN  BYTE3  BYTE3  SIZE2  EARLY_N  BYTE3  Ox03	PADDING  PRE_SHARED_KEY PSK PSK with EC(DHE)  EARLY DATA  SUPPORTED VERSIONS	
BYTE0 0x14  BYTE0 0x15  BYTE0 0x29 0x29  BYTE0 0x2A SIZE3  BYTE0 0x2B 0x03  BYTE0 0x2C	BYTE1  CERT_TYPE  BYTE1  0x00  0x01  BYTE1  SIZE0  EARLY_0  BYTE1  0x03  0x03  0x03  BYTE1  COOKIE_0	BYTE2 CERT_DATA_00  BYTE2  BYTE2  SIZE1   BYTE2  Ox04 Ox02  BYTE2	BYTE3  CERT_DATA_NN  BYTE3  BYTE3  SIZE2  EARLY_N  BYTE3  Ox03	PADDING  PRE_SHARED_KEY PSK PSK with EC(DHE)  EARLY DATA  SUPPORTED VERSIONS  COOKIE	
BYTEO 0x14  BYTEO 0x15  BYTEO 0x29 0x29  BYTEO 0x2A SIZE3  BYTEO 0x2B 0x03  BYTEO 0x2C  BYTEO 0x2C	BYTE1  CERT_TYPE  BYTE1  0x00 0x01  BYTE1  SIZE0 EARLY_0  BYTE1  0x03 0x03  0x03  BYTE1  COOKIE_0	BYTE2 CERT_DATA_00  BYTE2  BYTE2  SIZE1  BYTE2  Ox04 Ox02  BYTE2  BYTE2	BYTE3 CERT_DATA_NN  BYTE3  BYTE3  SIZE2 EARLY_N  BYTE3  Ox03  BYTE3  COOKIE_N	PADDING  PRE_SHARED_KEY PSK PSK with EC(DHE)  EARLY DATA  SUPPORTED VERSIONS  COOKIE  PSK KEY EXCHANGE MODES	
BYTEO 0x14  BYTEO 0x15  BYTEO 0x29 0x29  BYTEO 0x2A SIZE3  BYTEO 0x2B 0x03  BYTEO 0x2C	BYTE1  CERT_TYPE  BYTE1  0x00  0x01  BYTE1  SIZE0  EARLY_0  BYTE1  0x03  0x03  0x03  BYTE1  COOKIE_0	BYTE2 CERT_DATA_00  BYTE2  BYTE2  SIZE1   BYTE2  Ox04 Ox02  BYTE2	BYTE3  CERT_DATA_NN  BYTE3  BYTE3  SIZE2  EARLY_N  BYTE3  Ox03	PADDING  PRE_SHARED_KEY PSK PSK with EC(DHE)  EARLY DATA  SUPPORTED VERSIONS  COOKIE	
BYTEO 0x14  BYTEO 0x15  BYTEO 0x29 0x29  BYTEO 0x2A SIZE3  BYTEO 0x2B 0x03  BYTEO 0x2C  BYTEO 0x2C	BYTE1  CERT_TYPE  BYTE1  0x00 0x01  BYTE1  SIZE0 EARLY_0  BYTE1  0x03 0x03  0x03  BYTE1  COOKIE_0	BYTE2 CERT_DATA_00  BYTE2  BYTE2  SIZE1  BYTE2  Ox04 Ox02  BYTE2  BYTE2	BYTE3 CERT_DATA_NN  BYTE3  BYTE3  SIZE2 EARLY_N  BYTE3  Ox03  BYTE3  COOKIE_N	PADDING  PRE_SHARED_KEY PSK PSK with EC(DHE)  EARLY DATA  SUPPORTED VERSIONS  COOKIE  PSK KEY EXCHANGE MODES	
BYTEO	BYTE1  CERT_TYPE  BYTE1  BYTE1  0x00  0x01  BYTE1  SIZE0  EARLY_0  BYTE1  0x03  0x03  BYTE1  COOKIE_0  BYTE1  BYTE1	BYTE2 CERT_DATA_00  BYTE2  BYTE2  SIZE1   BYTE2  Ox04  Ox02  BYTE2   BYTE2  BYTE2  Ox04  Ox02	BYTE3  CERT_DATA_NN  BYTE3  BYTE3  SIZE2  EARLY_N  BYTE3  Ox03  BYTE3  COOKIE_N  BYTE3	PADDING  PRE_SHARED_KEY PSK PSK with EC(DHE)  EARLY DATA  SUPPORTED VERSIONS  COOKIE  PSK KEY EXCHANGE MODES	
BYTEO	BYTE1  CERT_TYPE  BYTE1  BYTE1  0x00  0x01  BYTE1  SIZE0  EARLY_0  BYTE1  0x03  0x03  BYTE1  COOKIE_0  BYTE1  BYTE1	BYTE2 CERT_DATA_00  BYTE2  BYTE2  SIZE1   BYTE2  Ox04  Ox02  BYTE2   BYTE2  BYTE2  Ox04  Ox02	BYTE3  CERT_DATA_NN  BYTE3  BYTE3  SIZE2  EARLY_N  BYTE3  Ox03  BYTE3  COOKIE_N  BYTE3	PADDING  PRE_SHARED_KEY PSK PSK with EC(DHE)  EARLY DATA  SUPPORTED VERSIONS  COOKIE  PSK KEY EXCHANGE MODES  CERTIFICATE AUTHORITIES	
BYTEO 0x14  BYTEO 0x15  BYTEO 0x29 0x29  BYTEO 0x2A SIZE3  BYTEO 0x2B 0x03  BYTEO 0x2C  BYTEO 0x2C	BYTE1  CERT_TYPE  BYTE1  0x00 0x01  BYTE1  SIZE0 EARLY_0  BYTE1  0x03 0x03  BYTE1  COOKIE_0  BYTE1  NAME_00	BYTE2 CERT_DATA_00  BYTE2  BYTE2  SIZE1   BYTE2  Ox04  Ox02  BYTE2   BYTE2  BYTE2  Ox04  Ox02	BYTE3  CERT_DATA_NN  BYTE3  BYTE3  SIZE2 EARLY_N  BYTE3  Ox03  BYTE3  COOKIE_N  BYTE3  NAME_NN	PADDING  PRE_SHARED_KEY PSK PSK with EC(DHE)  EARLY DATA  SUPPORTED VERSIONS  COOKIE  PSK KEY EXCHANGE MODES  CERTIFICATE AUTHORITIES	

BYTE0	BYTE1	BYTE2	BYTE3	POST HANDSHAKE AUTH
0x31				(contains no data)
BYTE0	BYTE1	BYTE2	BYTE3	SIGNATURE ALGORITHM CERT
0x32				
BYTE0	BYTE1	BYTE2	BYTE3	KEY SHARE (CLIENT)
0x33	GROUP_00	GROUP_01	PARAM_00	
PARAM_01	PARAM_02		PARAM_NN	
			1	
BYTE0	BYTE1	BYTE2	BYTE3	KEY SHARE (SERVER)
0x33	GROUP_00	GROUP_01		
			•	
BYTE0	BYTE1	BYTE2	BYTE3	APPLICATION RECORD
0x17	0x03	0x03	LEN_00	2^14 bytes maximum Plaintext
LEN_01	ENC_00	•••	ENC_NN	Encrypted
			ı	
DATA_00		DATA_NN	0x17	PLAINTEXT
PAD_00		PAD_NN	]	PADDING VARIABLE (MAY BE ZERO - USED FOR TRAFFIC SHAPING)
				MUST BE ALL ZERO
	212.22			
0x17	PAD_00		PAD_NN	ZERO LENGTH PLAINTEXT