

TLS handshake

Generated by Doxygen 1.8.12

Contents

1	Progetto di Advanced Programming of Cryptographic methods	1
2	Data Structure Index	3
2.1	Data Structures	3
3	File Index	5
3.1	File List	5
4	Data Structure Documentation	9
4.1	certificate_message Struct Reference	9
4.1.1	Detailed Description	9
4.1.2	Field Documentation	9
4.1.2.1	cert_length	9
4.1.2.2	X509_certificate	9
4.2	channel Struct Reference	9
4.2.1	Detailed Description	10
4.2.2	Field Documentation	10
4.2.2.1	channel_destination	10
4.2.2.2	channel_source	10
4.2.2.3	fd	10
4.2.2.4	fileName	10
4.2.2.5	isEnabled	10
4.2.2.6	mod	10
4.2.2.7	onPacketReceive	10
4.2.2.8	thread	11

4.3	cipher_suite_t Struct Reference	11
4.3.1	Detailed Description	11
4.3.2	Field Documentation	11
4.3.2.1	au	11
4.3.2.2	cipher_id	11
4.3.2.3	hash	11
4.3.2.4	key_size	11
4.3.2.5	kx	12
4.3.2.6	name	12
4.4	client_key_exchange Struct Reference	12
4.4.1	Detailed Description	12
4.4.2	Field Documentation	12
4.4.2.1	key	12
4.4.2.2	key_length	12
4.5	compression_methods_t Struct Reference	12
4.5.1	Detailed Description	13
4.5.2	Field Documentation	13
4.5.2.1	compression_id	13
4.5.2.2	length	13
4.6	DHE_server_key_exchange Struct Reference	13
4.6.1	Detailed Description	13
4.6.2	Field Documentation	14
4.6.2.1	g	14
4.6.2.2	p	14
4.6.2.3	pubKey	14
4.6.2.4	sign_hash_alg	14
4.6.2.5	signature	14
4.6.2.6	signature_length	14
4.7	ECDHE_server_key_exchange Struct Reference	14
4.7.1	Detailed Description	15

4.7.2	Field Documentation	15
4.7.2.1	named_curve	15
4.7.2.2	pub_key	15
4.7.2.3	sign_hash_alg	15
4.7.2.4	signature	15
4.7.2.5	signature_length	15
4.8	handshake Struct Reference	15
4.8.1	Detailed Description	16
4.8.2	Field Documentation	16
4.8.2.1	length	16
4.8.2.2	message	16
4.8.2.3	type	16
4.9	handshake_hello Struct Reference	16
4.9.1	Detailed Description	17
4.9.2	Field Documentation	17
4.9.2.1	cipher_suite_len	17
4.9.2.2	cipher_suites	17
4.9.2.3	compression_methods	17
4.9.2.4	random	17
4.9.2.5	session_id	17
4.9.2.6	TLS_version	17
4.10	packet_basic Struct Reference	17
4.10.1	Detailed Description	18
4.10.2	Field Documentation	18
4.10.2.1	destination	18
4.10.2.2	message	18
4.10.2.3	messageLen	18
4.10.2.4	source	18
4.11	random_data Struct Reference	18
4.11.1	Detailed Description	19

4.11.2	Field Documentation	19
4.11.2.1	random_bytes	19
4.11.2.2	UNIX_time	19
4.12	record Struct Reference	19
4.12.1	Detailed Description	19
4.12.2	Field Documentation	19
4.12.2.1	length	19
4.12.2.2	message	19
4.12.2.3	type	20
4.12.2.4	version	20
4.13	session_id_t Struct Reference	20
4.13.1	Detailed Description	20
4.13.2	Field Documentation	20
4.13.2.1	session_id	20
4.13.2.2	session_length	20
4.14	TLS_parameters Struct Reference	21
4.14.1	Detailed Description	21
4.14.2	Field Documentation	21
4.14.2.1	cipher_suite	21
4.14.2.2	client_random	21
4.14.2.3	handshake_messages	22
4.14.2.4	handshake_messages_len	22
4.14.2.5	master_secret	22
4.14.2.6	master_secret_len	22
4.14.2.7	previous_state	22
4.14.2.8	private_key	22
4.14.2.9	server_certificate	22
4.14.2.10	server_key_ex	22
4.14.2.11	server_random	22
4.14.2.12	tls_version	22

5	File Documentation	23
5.1	/Users/Darka/Dropbox/UNITN/AdvancedProgramming/Project/include/Crypto.h File Reference . . .	23
5.1.1	Function Documentation	24
5.1.1.1	PRF(const EVP_MD *hash, unsigned char *secret, int secret_len, char *label, unsigned char *seed, int seed_len, int result_len, unsigned char **result)	24
5.1.1.2	sign_DHE_server_key_ex(unsigned char *client_random, unsigned char *server_random, DHE_server_key_exchange *server_key_ex, authentication_↵_algorithm au)	24
5.1.1.3	sign_ECDHE_server_key_ex(unsigned char *client_random, unsigned char *server_random, ECDHE_server_key_exchange *server_key_ex, authentication_↵_algorithm au)	25
5.1.1.4	verify_DHE_server_key_ex_sign(X509 *certificate, unsigned char *client_↵_random, unsigned char *server_random, DHE_server_key_exchange *server_↵_key_ex, authentication_algorithm au)	25
5.1.1.5	verify_ECDHE_server_key_ex_sign(X509 *certificate, unsigned char *client_↵_random, unsigned char *server_random, ECDHE_server_key_exchange *server_key_ex, authentication_algorithm au)	26
5.2	/Users/Darka/Dropbox/UNITN/AdvancedProgramming/Project/include/handshakeConstants.h File Reference	26
5.2.1	Macro Definition Documentation	27
5.2.1.1	channel_mode_enum	27
5.2.1.2	enum_handshake_type	27
5.2.1.3	enum_record_version	27
5.2.1.4	REV16	28
5.2.1.5	REV32	28
5.2.2	Enumeration Type Documentation	28
5.2.2.1	anonymous enum	28
5.2.2.2	authentication_algorithm	28
5.2.2.3	channel_mode	28
5.2.2.4	hash_algorithm	29
5.2.2.5	key_exchange_algorithm	29
5.2.2.6	TLS_version	29
5.2.3	Function Documentation	29
5.2.3.1	get_cipher_suite(uint16_t id)	29
5.2.3.2	get_hash_function(hash_algorithm h)	30

5.3	/Users/Darka/Dropbox/UNITN/AdvancedProgramming/Project/include/HandshakeMessages/↵ Certificate.h File Reference	30
5.3.1	Function Documentation	31
5.3.1.1	deserialize_certificate_message(unsigned char *stream, uint32_t len)	31
5.3.1.2	free_certificate_message(certificate_message *cert)	32
5.3.1.3	make_certificate_message(char *cert_file_name)	32
5.3.1.4	serialize_certificate_message(certificate_message *cert, unsigned char **stream, uint32_t *len)	32
5.4	/Users/Darka/Dropbox/UNITN/AdvancedProgramming/Project/include/HandshakeMessages/↵ ServerClientHello.h File Reference	33
5.4.1	Typedef Documentation	34
5.4.1.1	compression_methods	34
5.4.1.2	session_id	34
5.4.2	Function Documentation	34
5.4.2.1	deserialize_client_server_hello(unsigned char *stream, uint32_t streamLen, channel_mode mode)	34
5.4.2.2	free_hello(handshake_hello *h)	35
5.4.2.3	make_hello(session_id session)	35
5.4.2.4	print_hello(handshake_hello *h)	36
5.4.2.5	serialize_client_server_hello(handshake_hello *hello, unsigned char **stream, uint32_t *streamLen, channel_mode mode)	36
5.5	/Users/Darka/Dropbox/UNITN/AdvancedProgramming/Project/include/HandshakeMessages/↵ ServerClientKeyExchange.h File Reference	36
5.5.1	Macro Definition Documentation	38
5.5.1.1	server_key_exchange_structs	38
5.5.2	Function Documentation	38
5.5.2.1	deserialize_client_key_exchange(uint32_t message_len, unsigned char *message)	38
5.5.2.2	deserialize_server_key_exchange(uint32_t message_len, unsigned char *message, key_exchange_algorithm kx)	38
5.5.2.3	free_server_key_exchange(void *server_key_ex, cipher_suite_t cipher_suite)	38
5.5.2.4	serialize_client_key_exchange(client_key_exchange *client_key_exchange, un- signed char **stream, uint32_t *streamLen)	39
5.5.2.5	serialize_server_key_exchange(void *server_key_exchange, unsigned char **stream, uint32_t *streamLen, key_exchange_algorithm kx)	39

5.6	/Users/Darka/Dropbox/UNITN/AdvancedProgramming/Project/include/ServerClientBasic.h File Reference	39
5.6.1	Macro Definition Documentation	40
5.6.1.1	DELAY_TIME	40
5.6.1.2	enum_mode	41
5.6.1.3	struct_channel	41
5.6.1.4	struct_packet	41
5.6.2	Typedef Documentation	41
5.6.2.1	channel	41
5.6.3	Enumeration Type Documentation	41
5.6.3.1	mode	41
5.6.4	Function Documentation	41
5.6.4.1	create_channel(char *fileName, char *channelFrom, char *channelTo, mode channelMode)	41
5.6.4.2	create_packet(char *from, char *to, unsigned char *message, uint32_t messageLen)	42
5.6.4.3	free_packet(packet_basic *p)	42
5.6.4.4	send_packet(channel *ch, packet_basic *p)	42
5.6.4.5	set_on_receive(channel *ch, void(*onPacketReceive)(channel *ch, packet_basic *p))	43
5.6.4.6	start_listener(channel *ch)	44
5.6.4.7	stop_channel(channel *ch)	44
5.6.4.8	wait_channel(channel *ch)	45
5.7	/Users/Darka/Dropbox/UNITN/AdvancedProgramming/Project/include/ServerClientHandshake Protocol.h File Reference	45
5.7.1	Function Documentation	46
5.7.1.1	deserialize_handshake(unsigned char *message, uint32_t messageLen)	46
5.7.1.2	free_handshake(handshake *h)	47
5.7.1.3	print_handshake(handshake *h)	47
5.7.1.4	send_handshake(channel *ch, handshake *h)	48
5.7.1.5	serialize_handshake(handshake *h, unsigned char **stream, uint32_t *streamLen)	48
5.8	/Users/Darka/Dropbox/UNITN/AdvancedProgramming/Project/include/ServerClientRecord Protocol.h File Reference	49

5.8.1	Macro Definition Documentation	50
5.8.1.1	enum_recordtype	50
5.8.1.2	REV16	50
5.8.1.3	struct_record	50
5.8.2	Typedef Documentation	50
5.8.2.1	record	50
5.8.3	Enumeration Type Documentation	50
5.8.3.1	recordType	50
5.8.4	Function Documentation	51
5.8.4.1	deserialize_record(unsigned char *message, uint32_t messageLen)	51
5.8.4.2	free_record(record *r)	51
5.8.4.3	print_record(record *r)	51
5.8.4.4	send_record(channel *ch, record *r)	52
5.8.4.5	serialize_record(record *r, unsigned char **message, uint16_t *messageLen)	52
5.9	/Users/Darka/Dropbox/UNITN/AdvancedProgramming/Project/include/TLS.h File Reference	53
5.9.1	Macro Definition Documentation	54
5.9.1.1	TLS_parameter_enum	54
5.9.2	Function Documentation	54
5.9.2.1	backup_handshake(TLS_parameters *TLS_param, handshake *h)	54
5.9.2.2	make_certificate(TLS_parameters *TLS_param)	55
5.9.2.3	make_change_cipher_spec()	55
5.9.2.4	make_client_hello(unsigned char *client_random)	56
5.9.2.5	make_client_key_exchange(TLS_parameters *TLS_param, uint16_t key_ex_alg)	56
5.9.2.6	make_DHE_server_key_exchange(TLS_parameters *TLS_param)	57
5.9.2.7	make_ECDHE_server_key_exchange(TLS_parameters *TLS_param)	58
5.9.2.8	make_finished_message(TLS_parameters *TLS_param)	58
5.9.2.9	make_server_hello(TLS_parameters *TLS_param, handshake_hello *client_hello)	59
5.9.2.10	make_server_hello_done()	60
5.9.2.11	make_server_key_exchange(TLS_parameters *TLS_param)	60
5.10	/Users/Darka/Dropbox/UNITN/AdvancedProgramming/Project/README.md File Reference	60

5.11 /Users/Darka/Dropbox/UNITN/AdvancedProgramming/Project/src/Crypto.c File Reference	61
5.11.1 Function Documentation	61
5.11.1.1 PRF(const EVP_MD *hash, unsigned char *secret, int secret_len, char *label, unsigned char *seed, int seed_len, int result_len, unsigned char **result)	61
5.11.1.2 sign_DHE_server_key_ex(unsigned char *client_random, unsigned char *server_random, DHE_server_key_exchange *server_key_ex, authentication←_algorithm au)	62
5.11.1.3 sign_ECDHE_server_key_ex(unsigned char *client_random, unsigned char *server_random, ECDHE_server_key_exchange *server_key_ex, authentication←_algorithm au)	62
5.11.1.4 sign_with_DSS(unsigned char **signature, unsigned int *signature_length, unsigned int to_sign_len, unsigned char *to_sign)	63
5.11.1.5 sign_with_ECDSA(unsigned char **signature, unsigned int *signature_length, unsigned int to_sign_len, unsigned char *to_sign)	63
5.11.1.6 sign_with_RSA(unsigned char **signature, unsigned int *signature_length, unsigned int to_sign_len, unsigned char *to_sign)	64
5.11.1.7 verify_DHE_server_key_ex_sign(X509 *certificate, unsigned char *client←_random, unsigned char *server_random, DHE_server_key_exchange *server←_key_ex, authentication_algorithm au)	64
5.11.1.8 verify_ECDHE_server_key_ex_sign(X509 *certificate, unsigned char *client←_random, unsigned char *server_random, ECDHE_server_key_exchange *server_key_ex, authentication_algorithm au)	64
5.12 /Users/Darka/Dropbox/UNITN/AdvancedProgramming/Project/src/handshakeConstants.c File Reference	65
5.12.1 Function Documentation	65
5.12.1.1 get_cipher_suite(uint16_t id)	65
5.12.1.2 get_hash_function(hash_algorithm h)	66
5.12.2 Variable Documentation	66
5.12.2.1 cipher_suite_len	66
5.12.2.2 cipher_suite_list	66
5.13 /Users/Darka/Dropbox/UNITN/AdvancedProgramming/Project/src/HandshakeMessages/Certificate.c File Reference	66
5.13.1 Function Documentation	67
5.13.1.1 deserialize_certificate_message(unsigned char *stream, uint32_t len)	67
5.13.1.2 free_certificate_message(certificate_message *cert)	67
5.13.1.3 make_certificate_message(char *cert_file_name)	68

5.13.1.4	serialize_certificate_message(certificate_message *cert, unsigned char **stream, uint32_t *len)	68
5.14	/Users/Darka/Dropbox/UNITN/AdvancedProgramming/Project/src/HandshakeMessages/Server↔ClientHello.c File Reference	68
5.14.1	Function Documentation	69
5.14.1.1	deserialize_client_server_hello(unsigned char *stream, uint32_t streamLen, channel_mode mode)	69
5.14.1.2	free_hello(handshake_hello *h)	69
5.14.1.3	make_hello(session_id session)	70
5.14.1.4	serialize_client_server_hello(handshake_hello *hello, unsigned char **stream, uint32_t *streamLen, channel_mode mode)	70
5.15	/Users/Darka/Dropbox/UNITN/AdvancedProgramming/Project/src/HandshakeMessages/Server↔ClientKeyExchange.c File Reference	71
5.15.1	Function Documentation	71
5.15.1.1	deserialize_client_key_exchange(uint32_t message_len, unsigned char *message)	71
5.15.1.2	deserialize_server_key_exchange(uint32_t message_len, unsigned char *message, key_exchange_algorithm kx)	72
5.15.1.3	free_server_key_exchange(void *server_key_ex, cipher_suite_t cipher_suite)	72
5.15.1.4	serialize_client_key_exchange(client_key_exchange *client_key_exchange, unsigned char **stream, uint32_t *streamLen)	72
5.15.1.5	serialize_server_key_exchange(void *server_key_exchange, unsigned char **stream, uint32_t *streamLen, key_exchange_algorithm kx)	73
5.16	/Users/Darka/Dropbox/UNITN/AdvancedProgramming/Project/src/ServerClientBasic.c File Reference	73
5.16.1	Function Documentation	74
5.16.1.1	create_channel(char *fileName, char *channelFrom, char *channelTo, mode channelMode)	74
5.16.1.2	create_packet(char *from, char *to, unsigned char *message, uint32_t↔t messageLen)	74
5.16.1.3	deserialize_packet(unsigned char *str, uint32_t fileLen)	74
5.16.1.4	free_packet(packet_basic *p)	75
5.16.1.5	get_file_size(int fd)	75
5.16.1.6	read_all_file(int fd, unsigned char **p)	76
5.16.1.7	reader(void *data)	76
5.16.1.8	send_packet(channel *ch, packet_basic *p)	77
5.16.1.9	serialize_packet(packet_basic *p, unsigned char **str, uint32_t *strLen)	77

5.16.1.10 set_on_receive(channel *ch, void(*onPacketReceive)(channel *ch, packet_basic *p))	78
5.16.1.11 start_listener(channel *ch)	79
5.16.1.12 stop_channel(channel *ch)	79
5.16.1.13 wait_channel(channel *ch)	80
5.17 /Users/Darka/Dropbox/UNITN/AdvancedProgramming/Project/src/ServerClientHandshake↵ Protocol.c File Reference	80
5.17.1 Function Documentation	80
5.17.1.1 deserialize_handshake(unsigned char *message, uint32_t messageLen)	80
5.17.1.2 free_handshake(handshake *h)	81
5.17.1.3 make_record(handshake *h)	81
5.17.1.4 print_handshake(handshake *h)	82
5.17.1.5 send_handshake(channel *ch, handshake *h)	82
5.17.1.6 serialize_handshake(handshake *h, unsigned char **stream, uint32_t *streamLen) 83	
5.18 /Users/Darka/Dropbox/UNITN/AdvancedProgramming/Project/src/ServerClientRecordProtocol.c File Reference	83
5.18.1 Function Documentation	84
5.18.1.1 deserialize_record(unsigned char *message, uint32_t messageLen)	84
5.18.1.2 free_record(record *r)	84
5.18.1.3 print_record(record *r)	85
5.18.1.4 send_record(channel *ch, record *r)	85
5.18.1.5 serialize_record(record *r, unsigned char **message, uint16_t *messageLen) .	86
5.19 /Users/Darka/Dropbox/UNITN/AdvancedProgramming/Project/src/Target/client.c File Reference . .	86
5.19.1 Function Documentation	87
5.19.1.1 main()	87
5.19.1.2 onPacketReceive(channel *ch, packet_basic *p)	88
5.19.1.3 print_master_secret()	88
5.19.1.4 print_random()	89
5.19.2 Variable Documentation	89
5.19.2.1 TLS_param	89
5.20 /Users/Darka/Dropbox/UNITN/AdvancedProgramming/Project/src/Target/server.c File Reference .	89
5.20.1 Function Documentation	90

5.20.1.1	compute_set_master_key_DH(client_key_exchange *client_public)	90
5.20.1.2	compute_set_master_key_ECDHE(client_key_exchange *client_public)	90
5.20.1.3	compute_set_master_key_RSA(client_key_exchange *client_key_exchange)	91
5.20.1.4	main()	91
5.20.1.5	onPacketReceive(channel *server2client, packet_basic *p)	92
5.20.1.6	print_master_secret()	93
5.20.1.7	print_random()	94
5.20.2	Variable Documentation	94
5.20.2.1	TLS_param	94
5.21	/Users/Darka/Dropbox/UNITN/AdvancedProgramming/Project/src/TLSClient.c File Reference	94
5.21.1	Function Documentation	95
5.21.1.1	backup_handshake(TLS_parameters *TLS_param, handshake *h)	95
5.21.1.2	make_change_cipher_spec()	95
5.21.1.3	make_client_hello(unsigned char *client_random)	96
5.21.1.4	make_client_key_exchange(TLS_parameters *TLS_param, uint16_t key_ex_alg)	96
5.21.1.5	make_finished_message(TLS_parameters *TLS_param)	97
5.22	/Users/Darka/Dropbox/UNITN/AdvancedProgramming/Project/src/TLSServer.c File Reference	98
5.22.1	Function Documentation	98
5.22.1.1	make_certificate(TLS_parameters *TLS_param)	98
5.22.1.2	make_DHE_server_key_exchange(TLS_parameters *TLS_param)	99
5.22.1.3	make_ECDHE_server_key_exchange(TLS_parameters *TLS_param)	100
5.22.1.4	make_server_hello(TLS_parameters *TLS_param, handshake_hello *client_hello)	100
5.22.1.5	make_server_hello_done()	101
5.22.1.6	make_server_key_exchange(TLS_parameters *TLS_param)	101
5.23	/Users/Darka/Dropbox/UNITN/AdvancedProgramming/Project/tests/clientBasic.c File Reference	102
5.23.1	Function Documentation	102
5.23.1.1	main(int argc, char **argv)	102
5.23.1.2	onPacketReceive(channel *ch, packet_basic *p)	103
5.24	/Users/Darka/Dropbox/UNITN/AdvancedProgramming/Project/tests/clientHandshake.c File Reference	104
5.24.1	Function Documentation	105

5.24.1.1	main()	105
5.25	/Users/Darka/Dropbox/UNITN/AdvancedProgramming/Project/tests/clientRecord.c File Reference	105
5.25.1	Function Documentation	106
5.25.1.1	main(int argc, const char *argv[])	106
5.25.1.2	onPacketReceive(channel *ch, packet_basic *p)	106
5.26	/Users/Darka/Dropbox/UNITN/AdvancedProgramming/Project/tests/serverBasic.c File Reference	107
5.26.1	Function Documentation	108
5.26.1.1	main(int argc, char **argv)	108
5.26.1.2	onPacketReceive(channel *ch, packet_basic *p)	108
5.27	/Users/Darka/Dropbox/UNITN/AdvancedProgramming/Project/tests/serverHandshake.c File Reference	109
5.27.1	Function Documentation	110
5.27.1.1	main()	110
5.27.1.2	onPacketReceive(channel *ch, packet_basic *p)	110
5.28	/Users/Darka/Dropbox/UNITN/AdvancedProgramming/Project/tests/serverRecord.c File Reference	111
5.28.1	Function Documentation	112
5.28.1.1	main(int argc, const char *argv[])	112
5.28.1.2	onPacketReceive(channel *ch, packet_basic *p)	113
5.29	/Users/Darka/Dropbox/UNITN/AdvancedProgramming/Project/tests/testCertificate.c File Reference	114
5.29.1	Function Documentation	114
5.29.1.1	main()	114
5.30	/Users/Darka/Dropbox/UNITN/AdvancedProgramming/Project/TLSProject/Build/Intermediates/TLSProject.build/Debug/StructTest.build/Objects-normal/x86_64/main.d File Reference	115
5.31	/Users/Darka/Dropbox/UNITN/AdvancedProgramming/Project/TLSProject/xcodeIntermediates/TLSProject.build/Debug/StructTest.build/Objects-normal/x86_64/main.d File Reference	115
5.32	/Users/Darka/Dropbox/UNITN/AdvancedProgramming/Project/TLSProject/Build/Intermediates/TLSProject.build/Debug/TLSClient.build/Objects-normal/x86_64/Certificate.d File Reference	115
5.33	/Users/Darka/Dropbox/UNITN/AdvancedProgramming/Project/TLSProject/Build/Intermediates/TLSProject.build/Debug/TLSClient.build/Objects-normal/x86_64/Certificate.d File Reference	115
5.34	/Users/Darka/Dropbox/UNITN/AdvancedProgramming/Project/TLSProject/xcodeIntermediates/TLSProject.build/Debug/TLSClient.build/Objects-normal/x86_64/Certificate.d File Reference	115
5.35	/Users/Darka/Dropbox/UNITN/AdvancedProgramming/Project/TLSProject/xcodeIntermediates/TLSProject.build/Debug/TLSClient.build/Objects-normal/x86_64/Certificate.d File Reference	116

5.36	/Users/Darka/Dropbox/UNITN/AdvancedProgramming/Project/TLSPProject/xcodeIntermediates/TLSPProject.build/Release/TLSCClient.build/Objects-normal/x86_64/Certificate.d File Reference	116
5.37	/Users/Darka/Dropbox/UNITN/AdvancedProgramming/Project/TLSPProject/xcodeIntermediates/TLSPProject.build/Release/TLSServer.build/Objects-normal/x86_64/Certificate.d File Reference . . .	116
5.38	/Users/Darka/Dropbox/UNITN/AdvancedProgramming/Project/TLSPProject/Build/Intermediates/TLSPProject.build/Debug/TLSCClient.build/Objects-normal/x86_64/client.d File Reference	116
5.39	/Users/Darka/Dropbox/UNITN/AdvancedProgramming/Project/TLSPProject/xcodeIntermediates/TLSPProject.build/Debug/TLSCClient.build/Objects-normal/x86_64/client.d File Reference	116
5.40	/Users/Darka/Dropbox/UNITN/AdvancedProgramming/Project/TLSPProject/xcodeIntermediates/TLSPProject.build/Release/TLSCClient.build/Objects-normal/x86_64/client.d File Reference	116
5.41	/Users/Darka/Dropbox/UNITN/AdvancedProgramming/Project/TLSPProject/Build/Intermediates/TLSPProject.build/Debug/TLSCClient.build/Objects-normal/x86_64/Crypto.d File Reference	116
5.42	/Users/Darka/Dropbox/UNITN/AdvancedProgramming/Project/TLSPProject/Build/Intermediates/TLSPProject.build/Debug/TLSServer.build/Objects-normal/x86_64/Crypto.d File Reference	116
5.43	/Users/Darka/Dropbox/UNITN/AdvancedProgramming/Project/TLSPProject/xcodeIntermediates/TLSPProject.build/Debug/TLSCClient.build/Objects-normal/x86_64/Crypto.d File Reference	116
5.44	/Users/Darka/Dropbox/UNITN/AdvancedProgramming/Project/TLSPProject/xcodeIntermediates/TLSPProject.build/Debug/TLSServer.build/Objects-normal/x86_64/Crypto.d File Reference	117
5.45	/Users/Darka/Dropbox/UNITN/AdvancedProgramming/Project/TLSPProject/xcodeIntermediates/TLSPProject.build/Release/TLSCClient.build/Objects-normal/x86_64/Crypto.d File Reference	117
5.46	/Users/Darka/Dropbox/UNITN/AdvancedProgramming/Project/TLSPProject/xcodeIntermediates/TLSPProject.build/Release/TLSServer.build/Objects-normal/x86_64/Crypto.d File Reference	117
5.47	/Users/Darka/Dropbox/UNITN/AdvancedProgramming/Project/TLSPProject/Build/Intermediates/TLSPProject.build/Debug/TLSCClient.build/Objects-normal/x86_64/handshakeConstants.d File Reference	117
5.48	/Users/Darka/Dropbox/UNITN/AdvancedProgramming/Project/TLSPProject/Build/Intermediates/TLSPProject.build/Debug/TLSServer.build/Objects-normal/x86_64/handshakeConstants.d File Reference	117
5.49	/Users/Darka/Dropbox/UNITN/AdvancedProgramming/Project/TLSPProject/xcodeIntermediates/TLSPProject.build/Debug/TLSCClient.build/Objects-normal/x86_64/handshakeConstants.d File Reference	117
5.50	/Users/Darka/Dropbox/UNITN/AdvancedProgramming/Project/TLSPProject/xcodeIntermediates/TLSPProject.build/Debug/TLSServer.build/Objects-normal/x86_64/handshakeConstants.d File Reference	117
5.51	/Users/Darka/Dropbox/UNITN/AdvancedProgramming/Project/TLSPProject/xcodeIntermediates/TLSPProject.build/Release/TLSCClient.build/Objects-normal/x86_64/handshakeConstants.d File Reference	117
5.52	/Users/Darka/Dropbox/UNITN/AdvancedProgramming/Project/TLSPProject/xcodeIntermediates/TLSPProject.build/Release/TLSServer.build/Objects-normal/x86_64/handshakeConstants.d File Reference	117
5.53	/Users/Darka/Dropbox/UNITN/AdvancedProgramming/Project/TLSPProject/Build/Intermediates/TLSPProject.build/Debug/TLSCClient.build/Objects-normal/x86_64/ServerClientBasic.d File Reference	118
5.54	/Users/Darka/Dropbox/UNITN/AdvancedProgramming/Project/TLSPProject/Build/Intermediates/TLSPProject.build/Debug/TLSServer.build/Objects-normal/x86_64/ServerClientBasic.d File Reference	118

5.55	/Users/Darka/Dropbox/UNITN/AdvancedProgramming/Project/TLSPProject/xcodeIntermediates/T↔ LSProject.build/Debug/TLSCClient.build/Objects-normal/x86_64/ServerClientBasic.d File Reference	118
5.56	/Users/Darka/Dropbox/UNITN/AdvancedProgramming/Project/TLSPProject/xcodeIntermediates/T↔ LSProject.build/Debug/TLSServer.build/Objects-normal/x86_64/ServerClientBasic.d File Reference	118
5.57	/Users/Darka/Dropbox/UNITN/AdvancedProgramming/Project/TLSPProject/xcodeIntermediates/T↔ LSProject.build/Release/TLSCClient.build/Objects-normal/x86_64/ServerClientBasic.d File Reference	118
5.58	/Users/Darka/Dropbox/UNITN/AdvancedProgramming/Project/TLSPProject/xcodeIntermediates/T↔ LSProject.build/Release/TLSServer.build/Objects-normal/x86_64/ServerClientBasic.d File Reference	118
5.59	/Users/Darka/Dropbox/UNITN/AdvancedProgramming/Project/TLSPProject/Build/Intermediates/T↔ LSProject.build/Debug/TLSCClient.build/Objects-normal/x86_64/ServerClientHandshakeProtocol.d File Reference	118
5.60	/Users/Darka/Dropbox/UNITN/AdvancedProgramming/Project/TLSPProject/Build/Intermediates/T↔ LSProject.build/Debug/TLSServer.build/Objects-normal/x86_64/ServerClientHandshakeProtocol.d File Reference	118
5.61	/Users/Darka/Dropbox/UNITN/AdvancedProgramming/Project/TLSPProject/xcodeIntermediates/T↔ LSProject.build/Debug/TLSCClient.build/Objects-normal/x86_64/ServerClientHandshakeProtocol.d File Reference	118
5.62	/Users/Darka/Dropbox/UNITN/AdvancedProgramming/Project/TLSPProject/xcodeIntermediates/T↔ LSProject.build/Debug/TLSServer.build/Objects-normal/x86_64/ServerClientHandshakeProtocol.d File Reference	119
5.63	/Users/Darka/Dropbox/UNITN/AdvancedProgramming/Project/TLSPProject/xcodeIntermediates/T↔ LSProject.build/Release/TLSCClient.build/Objects-normal/x86_64/ServerClientHandshakeProtocol.d File Reference	119
5.64	/Users/Darka/Dropbox/UNITN/AdvancedProgramming/Project/TLSPProject/xcodeIntermediates/↔ TLSPProject.build/Release/TLSServer.build/Objects-normal/x86_64/ServerClientHandshake↔ Protocol.d File Reference	119
5.65	/Users/Darka/Dropbox/UNITN/AdvancedProgramming/Project/TLSPProject/Build/Intermediates/TL↔ SProject.build/Debug/TLSCClient.build/Objects-normal/x86_64/ServerClientHello.d File Reference .	119
5.66	/Users/Darka/Dropbox/UNITN/AdvancedProgramming/Project/TLSPProject/Build/Intermediates/TL↔ SProject.build/Debug/TLSServer.build/Objects-normal/x86_64/ServerClientHello.d File Reference .	119
5.67	/Users/Darka/Dropbox/UNITN/AdvancedProgramming/Project/TLSPProject/xcodeIntermediates/T↔ LSProject.build/Debug/TLSCClient.build/Objects-normal/x86_64/ServerClientHello.d File Reference .	119
5.68	/Users/Darka/Dropbox/UNITN/AdvancedProgramming/Project/TLSPProject/xcodeIntermediates/T↔ LSProject.build/Debug/TLSServer.build/Objects-normal/x86_64/ServerClientHello.d File Reference	119
5.69	/Users/Darka/Dropbox/UNITN/AdvancedProgramming/Project/TLSPProject/xcodeIntermediates/T↔ LSProject.build/Release/TLSCClient.build/Objects-normal/x86_64/ServerClientHello.d File Reference	119
5.70	/Users/Darka/Dropbox/UNITN/AdvancedProgramming/Project/TLSPProject/xcodeIntermediates/T↔ LSProject.build/Release/TLSServer.build/Objects-normal/x86_64/ServerClientHello.d File Reference	119
5.71	/Users/Darka/Dropbox/UNITN/AdvancedProgramming/Project/TLSPProject/Build/Intermediates/↔ TLSPProject.build/Debug/TLSCClient.build/Objects-normal/x86_64/ServerClientKeyExchange.d File Reference	120

5.72	/Users/Darka/Dropbox/UNITN/AdvancedProgramming/Project/TLSPProject/Build/Intermediates/T↔ LSProject.build/Debug/TLSServer.build/Objects-normal/x86_64/ServerClientKeyExchange.d File Reference	120
5.73	/Users/Darka/Dropbox/UNITN/AdvancedProgramming/Project/TLSPProject/xcodeIntermediates/↔ TLSPProject.build/Debug/TLSCClient.build/Objects-normal/x86_64/ServerClientKeyExchange.d File Reference	120
5.74	/Users/Darka/Dropbox/UNITN/AdvancedProgramming/Project/TLSPProject/xcodeIntermediates/↔ TLSPProject.build/Debug/TLSServer.build/Objects-normal/x86_64/ServerClientKeyExchange.d File Reference	120
5.75	/Users/Darka/Dropbox/UNITN/AdvancedProgramming/Project/TLSPProject/xcodeIntermediates/T↔ LSProject.build/Release/TLSCClient.build/Objects-normal/x86_64/ServerClientKeyExchange.d File Reference	120
5.76	/Users/Darka/Dropbox/UNITN/AdvancedProgramming/Project/TLSPProject/xcodeIntermediates/T↔ LSProject.build/Release/TLSServer.build/Objects-normal/x86_64/ServerClientKeyExchange.d File Reference	120
5.77	/Users/Darka/Dropbox/UNITN/AdvancedProgramming/Project/TLSPProject/Build/Intermediates/T↔ LSProject.build/Debug/TLSCClient.build/Objects-normal/x86_64/ServerClientRecordProtocol.d File Reference	120
5.78	/Users/Darka/Dropbox/UNITN/AdvancedProgramming/Project/TLSPProject/Build/Intermediates/T↔ LSProject.build/Debug/TLSServer.build/Objects-normal/x86_64/ServerClientRecordProtocol.d File Reference	120
5.79	/Users/Darka/Dropbox/UNITN/AdvancedProgramming/Project/TLSPProject/xcodeIntermediates/T↔ LSProject.build/Debug/TLSCClient.build/Objects-normal/x86_64/ServerClientRecordProtocol.d File Reference	120
5.80	/Users/Darka/Dropbox/UNITN/AdvancedProgramming/Project/TLSPProject/xcodeIntermediates/T↔ LSProject.build/Debug/TLSServer.build/Objects-normal/x86_64/ServerClientRecordProtocol.d File Reference	121
5.81	/Users/Darka/Dropbox/UNITN/AdvancedProgramming/Project/TLSPProject/xcodeIntermediates/T↔ LSProject.build/Release/TLSCClient.build/Objects-normal/x86_64/ServerClientRecordProtocol.d File Reference	121
5.82	/Users/Darka/Dropbox/UNITN/AdvancedProgramming/Project/TLSPProject/xcodeIntermediates/↔ TLSPProject.build/Release/TLSServer.build/Objects-normal/x86_64/ServerClientRecordProtocol.d File Reference	121
5.83	/Users/Darka/Dropbox/UNITN/AdvancedProgramming/Project/TLSPProject/Build/Intermediates/TL↔ SProject.build/Debug/TLSCClient.build/Objects-normal/x86_64/TLSCClient.d File Reference	121
5.84	/Users/Darka/Dropbox/UNITN/AdvancedProgramming/Project/TLSPProject/Build/Intermediates/TL↔ SProject.build/Debug/TLSServer.build/Objects-normal/x86_64/TLSCClient.d File Reference	121
5.85	/Users/Darka/Dropbox/UNITN/AdvancedProgramming/Project/TLSPProject/xcodeIntermediates/T↔ LSProject.build/Debug/TLSCClient.build/Objects-normal/x86_64/TLSCClient.d File Reference	121
5.86	/Users/Darka/Dropbox/UNITN/AdvancedProgramming/Project/TLSPProject/xcodeIntermediates/T↔ LSProject.build/Debug/TLSServer.build/Objects-normal/x86_64/TLSCClient.d File Reference	121
5.87	/Users/Darka/Dropbox/UNITN/AdvancedProgramming/Project/TLSPProject/xcodeIntermediates/T↔ LSProject.build/Release/TLSCClient.build/Objects-normal/x86_64/TLSCClient.d File Reference	121

5.88	/Users/Darka/Dropbox/UNITN/AdvancedProgramming/Project/TLSPProject/xcodeIntermediates/TLSPProject.build/Release/TLSServer.build/Objects-normal/x86_64/TLSCClient.d File Reference	121
5.89	/Users/Darka/Dropbox/UNITN/AdvancedProgramming/Project/TLSPProject/Build/Intermediates/TLSPProject.build/Debug/TLSCClient.build/Objects-normal/x86_64/TLSServer.d File Reference	122
5.90	/Users/Darka/Dropbox/UNITN/AdvancedProgramming/Project/TLSPProject/Build/Intermediates/TLSPProject.build/Debug/TLSServer.build/Objects-normal/x86_64/TLSServer.d File Reference	122
5.91	/Users/Darka/Dropbox/UNITN/AdvancedProgramming/Project/TLSPProject/xcodeIntermediates/TLSPProject.build/Debug/TLSCClient.build/Objects-normal/x86_64/TLSServer.d File Reference	122
5.92	/Users/Darka/Dropbox/UNITN/AdvancedProgramming/Project/TLSPProject/xcodeIntermediates/TLSPProject.build/Debug/TLSServer.build/Objects-normal/x86_64/TLSServer.d File Reference	122
5.93	/Users/Darka/Dropbox/UNITN/AdvancedProgramming/Project/TLSPProject/xcodeIntermediates/TLSPProject.build/Release/TLSCClient.build/Objects-normal/x86_64/TLSServer.d File Reference	122
5.94	/Users/Darka/Dropbox/UNITN/AdvancedProgramming/Project/TLSPProject/xcodeIntermediates/TLSPProject.build/Release/TLSServer.build/Objects-normal/x86_64/TLSServer.d File Reference	122
5.95	/Users/Darka/Dropbox/UNITN/AdvancedProgramming/Project/TLSPProject/Build/Intermediates/TLSPProject.build/Debug/TLSServer.build/Objects-normal/x86_64/server.d File Reference	122
5.96	/Users/Darka/Dropbox/UNITN/AdvancedProgramming/Project/TLSPProject/xcodeIntermediates/TLSPProject.build/Debug/TLSServer.build/Objects-normal/x86_64/server.d File Reference	122
5.97	/Users/Darka/Dropbox/UNITN/AdvancedProgramming/Project/TLSPProject/xcodeIntermediates/TLSPProject.build/Release/TLSServer.build/Objects-normal/x86_64/server.d File Reference	122
5.98	/Users/Darka/Dropbox/UNITN/AdvancedProgramming/Project/TLSPProject/StructTest/main.c File Reference	123
5.98.1	Function Documentation	123
5.98.1.1	main(int argc, const char *argv[])	123
5.99	/Users/Darka/Dropbox/UNITN/AdvancedProgramming/Project/TLSPProject/xcodeIntermediates/TLSPProject.build/Debug/TLSCClient.build/Objects-normal/x86_64/TLSCClient-3E1448B75D6FF18F.d File Reference	123
5.100	/Users/Darka/Dropbox/UNITN/AdvancedProgramming/Project/TLSPProject/xcodeIntermediates/TLSPProject.build/Debug/TLSCClient.build/Objects-normal/x86_64/TLSCClient-BF9D49D9B0317373.d File Reference	123

Chapter 1

Progetto di Advanced Programming of Cryptographic methods

ToDo list

- SSL/TLS
- In particolare, lo schema di comunicazione client<->server
- In particolare, l'handshaking

hello client

- Tutta la comunicazione client<->server (senza socket)
- Il mezzo di comunicazione da usare sarà un file condiviso
- Ogni entità legge il file e lo ripulisce
- Nella comunicazione ci sarà un token
- 2 file: uno di comunicazione, l'altro con il token di chi deve parlare
- La comunicazione prosegue finché non si genera un master secret (la chiave condivisa)
- Per la generazione del master secret usare hash, md5, generatori random
- Si possono usare librerie già fatte
- Devono essere due programmi: Client e Server
- Il protocollo è diviso in 4 fasi, arrivare fino alla 4ª fase
- CI FERMIAMO AL SEGRETO COMUNE

PARAMETRI DI VALUTAZIONE:

- Funzionante
- Porcherie di programmazione
- La relazione che sarà una spiegazione di cosa abbiamo fatto
- Come lo abbiamo pensato ed implementato

Libro: William Stallings - Network Security Applications and Standards

Chapter 2

Data Structure Index

2.1 Data Structures

Here are the data structures with brief descriptions:

certificate_message	9
channel	9
cipher_suite_t	11
client_key_exchange	12
compression_methods_t	12
DHE_server_key_exchange	13
ECDHE_server_key_exchange	14
handshake	15
handshake_hello	16
packet_basic	17
random_data	18
record	19
session_id_t	20
TLS_parameters	21

Chapter 3

File Index

3.1 File List

Here is a list of all files with brief descriptions:

/Users/Darka/Dropbox/UNITN/AdvancedProgramming/Project/include/ Crypto.h	23
/Users/Darka/Dropbox/UNITN/AdvancedProgramming/Project/include/ handshakeConstants.h	26
/Users/Darka/Dropbox/UNITN/AdvancedProgramming/Project/include/ ServerClientBasic.h	39
/Users/Darka/Dropbox/UNITN/AdvancedProgramming/Project/include/ ServerClientHandshake ↔ Protocol.h	45
/Users/Darka/Dropbox/UNITN/AdvancedProgramming/Project/include/ ServerClientRecordProtocol.h	49
/Users/Darka/Dropbox/UNITN/AdvancedProgramming/Project/include/ TLS.h	53
/Users/Darka/Dropbox/UNITN/AdvancedProgramming/Project/include/HandshakeMessages/ Certificate ↔ h	30
/Users/Darka/Dropbox/UNITN/AdvancedProgramming/Project/include/HandshakeMessages/ Server ↔ ClientHello.h	33
/Users/Darka/Dropbox/UNITN/AdvancedProgramming/Project/include/HandshakeMessages/ Server ↔ ClientKeyExchange.h	36
/Users/Darka/Dropbox/UNITN/AdvancedProgramming/Project/src/ Crypto.c	61
/Users/Darka/Dropbox/UNITN/AdvancedProgramming/Project/src/ handshakeConstants.c	65
/Users/Darka/Dropbox/UNITN/AdvancedProgramming/Project/src/ ServerClientBasic.c	73
/Users/Darka/Dropbox/UNITN/AdvancedProgramming/Project/src/ ServerClientHandshakeProtocol.c	80
/Users/Darka/Dropbox/UNITN/AdvancedProgramming/Project/src/ ServerClientRecordProtocol.c	83
/Users/Darka/Dropbox/UNITN/AdvancedProgramming/Project/src/ TLSCClient.c	94
/Users/Darka/Dropbox/UNITN/AdvancedProgramming/Project/src/ TLSServer.c	98
/Users/Darka/Dropbox/UNITN/AdvancedProgramming/Project/src/HandshakeMessages/ Certificate.c	66
/Users/Darka/Dropbox/UNITN/AdvancedProgramming/Project/src/HandshakeMessages/ ServerClient ↔ Hello.c	68
/Users/Darka/Dropbox/UNITN/AdvancedProgramming/Project/src/HandshakeMessages/ ServerClient ↔ KeyExchange.c	71
/Users/Darka/Dropbox/UNITN/AdvancedProgramming/Project/src/Target/ client.c	86
/Users/Darka/Dropbox/UNITN/AdvancedProgramming/Project/src/Target/ server.c	89
/Users/Darka/Dropbox/UNITN/AdvancedProgramming/Project/tests/ clientBasic.c	102
/Users/Darka/Dropbox/UNITN/AdvancedProgramming/Project/tests/ clientHandshake.c	104
/Users/Darka/Dropbox/UNITN/AdvancedProgramming/Project/tests/ clientRecord.c	105
/Users/Darka/Dropbox/UNITN/AdvancedProgramming/Project/tests/ serverBasic.c	107
/Users/Darka/Dropbox/UNITN/AdvancedProgramming/Project/tests/ serverHandshake.c	109
/Users/Darka/Dropbox/UNITN/AdvancedProgramming/Project/tests/ serverRecord.c	111
/Users/Darka/Dropbox/UNITN/AdvancedProgramming/Project/tests/ testCertificate.c	114
/Users/Darka/Dropbox/UNITN/AdvancedProgramming/Project/TLSProject/Build/Intermediates/TLS↔ Project.build/Debug/StructTest.build/Objects-normal/x86_64/ main.d	115

/Users/Darka/Dropbox/UNITN/AdvancedProgramming/Project/TLSProject/xcodeIntermediates/TLS↔ Project.build/Debug/TLSClient.build/Objects-normal/x86_64/ ServerClientBasic.d	118
/Users/Darka/Dropbox/UNITN/AdvancedProgramming/Project/TLSProject/xcodeIntermediates/TLS↔ SProject.build/Debug/TLSClient.build/Objects-normal/x86_64/ ServerClientHandshake↔ Protocol.d	118
/Users/Darka/Dropbox/UNITN/AdvancedProgramming/Project/TLSProject/xcodeIntermediates/TLS↔ Project.build/Debug/TLSClient.build/Objects-normal/x86_64/ ServerClientHello.d	119
/Users/Darka/Dropbox/UNITN/AdvancedProgramming/Project/TLSProject/xcodeIntermediates/TLS↔ Project.build/Debug/TLSClient.build/Objects-normal/x86_64/ ServerClientKeyExchange.d	120
/Users/Darka/Dropbox/UNITN/AdvancedProgramming/Project/TLSProject/xcodeIntermediates/TLS↔ Project.build/Debug/TLSClient.build/Objects-normal/x86_64/ ServerClientRecordProtocol.d	120
/Users/Darka/Dropbox/UNITN/AdvancedProgramming/Project/TLSProject/xcodeIntermediates/TLS↔ Project.build/Debug/TLSClient.build/Objects-normal/x86_64/ TLSCClient-3E1448B75D6FF18↔ F.d	123
/Users/Darka/Dropbox/UNITN/AdvancedProgramming/Project/TLSProject/xcodeIntermediates/TLS↔ Project.build/Debug/TLSClient.build/Objects-normal/x86_64/ TLSCClient-BF9D49D9B0317373.↔ d	123
/Users/Darka/Dropbox/UNITN/AdvancedProgramming/Project/TLSProject/xcodeIntermediates/TLS↔ Project.build/Debug/TLSClient.build/Objects-normal/x86_64/ TLSCClient.d	121
/Users/Darka/Dropbox/UNITN/AdvancedProgramming/Project/TLSProject/xcodeIntermediates/TLS↔ Project.build/Debug/TLSClient.build/Objects-normal/x86_64/ TLSServer.d	122
/Users/Darka/Dropbox/UNITN/AdvancedProgramming/Project/TLSProject/xcodeIntermediates/TLS↔ Project.build/Debug/TLSServer.build/Objects-normal/x86_64/ Certificate.d	116
/Users/Darka/Dropbox/UNITN/AdvancedProgramming/Project/TLSProject/xcodeIntermediates/TLS↔ Project.build/Debug/TLSServer.build/Objects-normal/x86_64/ Crypto.d	117
/Users/Darka/Dropbox/UNITN/AdvancedProgramming/Project/TLSProject/xcodeIntermediates/TLS↔ Project.build/Debug/TLSServer.build/Objects-normal/x86_64/ handshakeConstants.d	117
/Users/Darka/Dropbox/UNITN/AdvancedProgramming/Project/TLSProject/xcodeIntermediates/TLS↔ Project.build/Debug/TLSServer.build/Objects-normal/x86_64/ server.d	122
/Users/Darka/Dropbox/UNITN/AdvancedProgramming/Project/TLSProject/xcodeIntermediates/TLS↔ Project.build/Debug/TLSServer.build/Objects-normal/x86_64/ ServerClientBasic.d	118
/Users/Darka/Dropbox/UNITN/AdvancedProgramming/Project/TLSProject/xcodeIntermediates/TLS↔ SProject.build/Debug/TLSServer.build/Objects-normal/x86_64/ ServerClientHandshake↔ Protocol.d	119
/Users/Darka/Dropbox/UNITN/AdvancedProgramming/Project/TLSProject/xcodeIntermediates/TLS↔ Project.build/Debug/TLSServer.build/Objects-normal/x86_64/ ServerClientHello.d	119
/Users/Darka/Dropbox/UNITN/AdvancedProgramming/Project/TLSProject/xcodeIntermediates/TLS↔ Project.build/Debug/TLSServer.build/Objects-normal/x86_64/ ServerClientKeyExchange.d	120
/Users/Darka/Dropbox/UNITN/AdvancedProgramming/Project/TLSProject/xcodeIntermediates/TLS↔ Project.build/Debug/TLSServer.build/Objects-normal/x86_64/ ServerClientRecordProtocol.d	121
/Users/Darka/Dropbox/UNITN/AdvancedProgramming/Project/TLSProject/xcodeIntermediates/TLS↔ Project.build/Debug/TLSServer.build/Objects-normal/x86_64/ TLSCClient.d	121
/Users/Darka/Dropbox/UNITN/AdvancedProgramming/Project/TLSProject/xcodeIntermediates/TLS↔ Project.build/Debug/TLSServer.build/Objects-normal/x86_64/ TLSServer.d	122
/Users/Darka/Dropbox/UNITN/AdvancedProgramming/Project/TLSProject/xcodeIntermediates/TLS↔ Project.build/Release/TLSCClient.build/Objects-normal/x86_64/ Certificate.d	116
/Users/Darka/Dropbox/UNITN/AdvancedProgramming/Project/TLSProject/xcodeIntermediates/TLS↔ Project.build/Release/TLSCClient.build/Objects-normal/x86_64/ client.d	116
/Users/Darka/Dropbox/UNITN/AdvancedProgramming/Project/TLSProject/xcodeIntermediates/TLS↔ Project.build/Release/TLSCClient.build/Objects-normal/x86_64/ Crypto.d	117
/Users/Darka/Dropbox/UNITN/AdvancedProgramming/Project/TLSProject/xcodeIntermediates/TLS↔ Project.build/Release/TLSCClient.build/Objects-normal/x86_64/ handshakeConstants.d	117
/Users/Darka/Dropbox/UNITN/AdvancedProgramming/Project/TLSProject/xcodeIntermediates/TLS↔ Project.build/Release/TLSCClient.build/Objects-normal/x86_64/ ServerClientBasic.d	118
/Users/Darka/Dropbox/UNITN/AdvancedProgramming/Project/TLSProject/xcodeIntermediates/TLS↔ SProject.build/Release/TLSCClient.build/Objects-normal/x86_64/ ServerClientHandshake↔ Protocol.d	119

/Users/Darka/Dropbox/UNITN/AdvancedProgramming/Project/TLSPProject/xcodeIntermediates/TLS↵ Project.build/Release/TLSCient.build/Objects-normal/x86_64/ ServerClientHello.d	119
/Users/Darka/Dropbox/UNITN/AdvancedProgramming/Project/TLSPProject/xcodeIntermediates/TLS↵ Project.build/Release/TLSCient.build/Objects-normal/x86_64/ ServerClientKeyExchange.d	120
/Users/Darka/Dropbox/UNITN/AdvancedProgramming/Project/TLSPProject/xcodeIntermediates/TLS↵ Project.build/Release/TLSCient.build/Objects-normal/x86_64/ ServerClientRecordProtocol.d	121
/Users/Darka/Dropbox/UNITN/AdvancedProgramming/Project/TLSPProject/xcodeIntermediates/TLS↵ Project.build/Release/TLSCient.build/Objects-normal/x86_64/ TLSCient.d	121
/Users/Darka/Dropbox/UNITN/AdvancedProgramming/Project/TLSPProject/xcodeIntermediates/TLS↵ Project.build/Release/TLSCient.build/Objects-normal/x86_64/ TLSServer.d	122
/Users/Darka/Dropbox/UNITN/AdvancedProgramming/Project/TLSPProject/xcodeIntermediates/TLS↵ Project.build/Release/TLSServer.build/Objects-normal/x86_64/ Certificate.d	116
/Users/Darka/Dropbox/UNITN/AdvancedProgramming/Project/TLSPProject/xcodeIntermediates/TLS↵ Project.build/Release/TLSServer.build/Objects-normal/x86_64/ Crypto.d	117
/Users/Darka/Dropbox/UNITN/AdvancedProgramming/Project/TLSPProject/xcodeIntermediates/TLS↵ Project.build/Release/TLSServer.build/Objects-normal/x86_64/ handshakeConstants.d	117
/Users/Darka/Dropbox/UNITN/AdvancedProgramming/Project/TLSPProject/xcodeIntermediates/TLS↵ Project.build/Release/TLSServer.build/Objects-normal/x86_64/ server.d	122
/Users/Darka/Dropbox/UNITN/AdvancedProgramming/Project/TLSPProject/xcodeIntermediates/TLS↵ Project.build/Release/TLSServer.build/Objects-normal/x86_64/ ServerClientBasic.d	118
/Users/Darka/Dropbox/UNITN/AdvancedProgramming/Project/TLSPProject/xcodeIntermediates/TLS↵ Project.build/Release/TLSServer.build/Objects-normal/x86_64/ ServerClientHandshake↵ Protocol.d	119
/Users/Darka/Dropbox/UNITN/AdvancedProgramming/Project/TLSPProject/xcodeIntermediates/TLS↵ Project.build/Release/TLSServer.build/Objects-normal/x86_64/ ServerClientHello.d	119
/Users/Darka/Dropbox/UNITN/AdvancedProgramming/Project/TLSPProject/xcodeIntermediates/TLS↵ Project.build/Release/TLSServer.build/Objects-normal/x86_64/ ServerClientKeyExchange.d	120
/Users/Darka/Dropbox/UNITN/AdvancedProgramming/Project/TLSPProject/xcodeIntermediates/T↵ LSProject.build/Release/TLSServer.build/Objects-normal/x86_64/ ServerClientRecord↵ Protocol.d	121
/Users/Darka/Dropbox/UNITN/AdvancedProgramming/Project/TLSPProject/xcodeIntermediates/TLS↵ Project.build/Release/TLSServer.build/Objects-normal/x86_64/ TLSCient.d	121
/Users/Darka/Dropbox/UNITN/AdvancedProgramming/Project/TLSPProject/xcodeIntermediates/TLS↵ Project.build/Release/TLSServer.build/Objects-normal/x86_64/ TLSServer.d	122

Chapter 4

Data Structure Documentation

4.1 certificate_message Struct Reference

```
#include <Certificate.h>
```

Data Fields

- uint32_t **cert_length**
- X509 * **X509_certificate**

4.1.1 Detailed Description

Definition at line 30 of file Certificate.h.

4.1.2 Field Documentation

4.1.2.1 uint32_t cert_length

Definition at line 31 of file Certificate.h.

4.1.2.2 X509* X509_certificate

Definition at line 32 of file Certificate.h.

The documentation for this struct was generated from the following file:

- /Users/Darka/Dropbox/UNITN/AdvancedProgramming/Project/include/HandshakeMessages/**Certificate.h**

4.2 channel Struct Reference

```
#include <ServerClientBasic.h>
```

Data Fields

- **mode** **mod**
- **char** * **channel_source**
- **char** * **channel_destination**
- **char** * **fileName**
- **int** **fd**
- **void**(* **onPacketReceive**)(struct **channel** *ch, **packet_basic** *p)
- **int** **isEnabled**
- **pthread_t** **thread**

4.2.1 Detailed Description

Definition at line 62 of file ServerClientBasic.h.

4.2.2 Field Documentation

4.2.2.1 **char*** **channel_destination**

Definition at line 68 of file ServerClientBasic.h.

4.2.2.2 **char*** **channel_source**

Definition at line 66 of file ServerClientBasic.h.

4.2.2.3 **int** **fd**

Definition at line 72 of file ServerClientBasic.h.

4.2.2.4 **char*** **fileName**

Definition at line 70 of file ServerClientBasic.h.

4.2.2.5 **int** **isEnabled**

Definition at line 76 of file ServerClientBasic.h.

4.2.2.6 **mode** **mod**

Definition at line 64 of file ServerClientBasic.h.

4.2.2.7 **void**(* **onPacketReceive**)(struct **channel** *ch, **packet_basic** *p)

Definition at line 74 of file ServerClientBasic.h.

4.2.2.8 pthread_t thread

Definition at line 78 of file ServerClientBasic.h.

The documentation for this struct was generated from the following file:

- /Users/Darka/Dropbox/UNITN/AdvancedProgramming/Project/include/**ServerClientBasic.h**

4.3 cipher_suite_t Struct Reference

```
#include <handshakeConstants.h>
```

Data Fields

- uint16_t **cipher_id**
- char * **name**
- **key_exchange_algorithm** kx
- **authentication_algorithm** au
- uint16_t **key_size**
- **hash_algorithm** hash

4.3.1 Detailed Description

Definition at line 45 of file handshakeConstants.h.

4.3.2 Field Documentation

4.3.2.1 authentication_algorithm au

Definition at line 49 of file handshakeConstants.h.

4.3.2.2 uint16_t cipher_id

Definition at line 46 of file handshakeConstants.h.

4.3.2.3 hash_algorithm hash

Definition at line 51 of file handshakeConstants.h.

4.3.2.4 uint16_t key_size

Definition at line 50 of file handshakeConstants.h.

4.3.2.5 `key_exchange_algorithm` kx

Definition at line 48 of file `handshakeConstants.h`.

4.3.2.6 `char* name`

Definition at line 47 of file `handshakeConstants.h`.

The documentation for this struct was generated from the following file:

- `/Users/Darka/Dropbox/UNITN/AdvancedProgramming/Project/include/handshakeConstants.h`

4.4 `client_key_exchange` Struct Reference

```
#include <ServerClientKeyExchange.h>
```

Data Fields

- `uint16_t key_length`
- `unsigned char * key`

4.4.1 Detailed Description

Definition at line 62 of file `ServerClientKeyExchange.h`.

4.4.2 Field Documentation

4.4.2.1 `unsigned char* key`

Definition at line 66 of file `ServerClientKeyExchange.h`.

4.4.2.2 `uint16_t key_length`

Definition at line 64 of file `ServerClientKeyExchange.h`.

The documentation for this struct was generated from the following file:

- `/Users/Darka/Dropbox/UNITN/AdvancedProgramming/Project/include/HandshakeMessages/ServerClientKeyExchange.h`

4.5 `compression_methods_t` Struct Reference

```
#include <ServerClientHello.h>
```


Data Fields

- uint16_t **length**
- uint8_t **compression_id**

4.5.1 Detailed Description

Definition at line 37 of file ServerClientHello.h.

4.5.2 Field Documentation

4.5.2.1 uint8_t compression_id

Definition at line 39 of file ServerClientHello.h.

4.5.2.2 uint16_t length

Definition at line 38 of file ServerClientHello.h.

The documentation for this struct was generated from the following file:

- /Users/Darka/Dropbox/UNITN/AdvancedProgramming/Project/include/HandshakeMessages/**ServerClientHello.h**

4.6 DHE_server_key_exchange Struct Reference

```
#include <ServerClientKeyExchange.h>
```

Data Fields

- BIGNUM * **p**
- BIGNUM * **g**
- BIGNUM * **pubKey**
- uint16_t **sign_hash_alg**
- unsigned int **signature_length**
- unsigned char * **signature**

4.6.1 Detailed Description

Definition at line 45 of file ServerClientKeyExchange.h.

4.6.2 Field Documentation

4.6.2.1 `BIGNUM* g`

Definition at line 49 of file `ServerClientKeyExchange.h`.

4.6.2.2 `BIGNUM* p`

Definition at line 47 of file `ServerClientKeyExchange.h`.

4.6.2.3 `BIGNUM* pubKey`

Definition at line 51 of file `ServerClientKeyExchange.h`.

4.6.2.4 `uint16_t sign_hash_alg`

Definition at line 54 of file `ServerClientKeyExchange.h`.

4.6.2.5 `unsigned char* signature`

Definition at line 58 of file `ServerClientKeyExchange.h`.

4.6.2.6 `unsigned int signature_length`

Definition at line 56 of file `ServerClientKeyExchange.h`.

The documentation for this struct was generated from the following file:

- `/Users/Darka/Dropbox/UNITN/AdvancedProgramming/Project/include/HandshakeMessages/ServerClientKeyExchange.h`

4.7 `ECDHE_server_key_exchange` Struct Reference

```
#include <ServerClientKeyExchange.h>
```

Data Fields

- `uint16_t named_curve`
- `BIGNUM * pub_key`
- `uint16_t sign_hash_alg`
- `unsigned int signature_length`
- `unsigned char * signature`

4.7.1 Detailed Description

Definition at line 32 of file ServerClientKeyExchange.h.

4.7.2 Field Documentation

4.7.2.1 uint16_t named_curve

Definition at line 33 of file ServerClientKeyExchange.h.

4.7.2.2 BIGNUM* pub_key

Definition at line 35 of file ServerClientKeyExchange.h.

4.7.2.3 uint16_t sign_hash_alg

Definition at line 37 of file ServerClientKeyExchange.h.

4.7.2.4 unsigned char* signature

Definition at line 41 of file ServerClientKeyExchange.h.

4.7.2.5 unsigned int signature_length

Definition at line 39 of file ServerClientKeyExchange.h.

The documentation for this struct was generated from the following file:

- /Users/Darka/Dropbox/UNITN/AdvancedProgramming/Project/include/HandshakeMessages/**ServerClientKeyExchange.h**

4.8 handshake Struct Reference

```
#include <ServerClientHandshakeProtocol.h>
```

Data Fields

- uint8_t **type**
- uint32_t **length**
- unsigned char * **message**

4.8.1 Detailed Description

Definition at line 36 of file ServerClientHandshakeProtocol.h.

4.8.2 Field Documentation

4.8.2.1 uint32_t length

Definition at line 38 of file ServerClientHandshakeProtocol.h.

4.8.2.2 unsigned char* message

Definition at line 39 of file ServerClientHandshakeProtocol.h.

4.8.2.3 uint8_t type

Definition at line 37 of file ServerClientHandshakeProtocol.h.

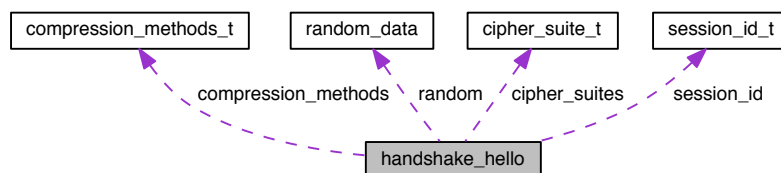
The documentation for this struct was generated from the following file:

- /Users/Darka/Dropbox/UNITN/AdvancedProgramming/Project/include/**ServerClientHandshakeProtocol.h**

4.9 handshake_hello Struct Reference

```
#include <ServerClientHello.h>
```

Collaboration diagram for handshake_hello:



Data Fields

- uint16_t **TLS_version**
- **random_data** random
- **session_id** session_id
- uint16_t **cipher_suite_len**
- **cipher_suite_t** * cipher_suites
- **compression_methods** compression_methods

4.9.1 Detailed Description

Definition at line 43 of file ServerClientHello.h.

4.9.2 Field Documentation

4.9.2.1 uint16_t cipher_suite_len

Definition at line 47 of file ServerClientHello.h.

4.9.2.2 cipher_suite_t* cipher_suites

Definition at line 48 of file ServerClientHello.h.

4.9.2.3 compression_methods compression_methods

Definition at line 49 of file ServerClientHello.h.

4.9.2.4 random_data random

Definition at line 45 of file ServerClientHello.h.

4.9.2.5 session_id session_id

Definition at line 46 of file ServerClientHello.h.

4.9.2.6 uint16_t TLS_version

Definition at line 44 of file ServerClientHello.h.

The documentation for this struct was generated from the following file:

- /Users/Darka/Dropbox/UNITN/AdvancedProgramming/Project/include/HandshakeMessages/**ServerClientHello.h**

4.10 packet_basic Struct Reference

```
#include <ServerClientBasic.h>
```

Data Fields

- char * **source**
- char * **destination**
- uint32_t **messageLen**
- unsigned char * **message**

4.10.1 Detailed Description

Definition at line 51 of file ServerClientBasic.h.

4.10.2 Field Documentation

4.10.2.1 char* destination

Definition at line 53 of file ServerClientBasic.h.

4.10.2.2 unsigned char* message

Definition at line 55 of file ServerClientBasic.h.

4.10.2.3 uint32_t messageLen

Definition at line 54 of file ServerClientBasic.h.

4.10.2.4 char* source

Definition at line 52 of file ServerClientBasic.h.

The documentation for this struct was generated from the following file:

- /Users/Darka/Dropbox/UNITN/AdvancedProgramming/Project/include/**ServerClientBasic.h**

4.11 random_data Struct Reference

```
#include <ServerClientHello.h>
```

Data Fields

- uint32_t **UNIX_time**
- uint8_t **random_bytes** [28]

4.11.1 Detailed Description

Definition at line 25 of file ServerClientHello.h.

4.11.2 Field Documentation

4.11.2.1 uint8_t random_bytes[28]

Definition at line 27 of file ServerClientHello.h.

4.11.2.2 uint32_t UNIX_time

Definition at line 26 of file ServerClientHello.h.

The documentation for this struct was generated from the following file:

- /Users/Darka/Dropbox/UNITN/AdvancedProgramming/Project/include/HandshakeMessages/**ServerClientHello.h**

4.12 record Struct Reference

```
#include <ServerClientRecordProtocol.h>
```

Data Fields

- uint8_t **type**
- uint16_t **version**
- uint16_t **length**
- unsigned char * **message**

4.12.1 Detailed Description

Definition at line 36 of file ServerClientRecordProtocol.h.

4.12.2 Field Documentation

4.12.2.1 uint16_t length

Definition at line 39 of file ServerClientRecordProtocol.h.

4.12.2.2 unsigned char* message

Definition at line 40 of file ServerClientRecordProtocol.h.

4.12.2.3 uint8_t type

Definition at line 37 of file ServerClientRecordProtocol.h.

4.12.2.4 uint16_t version

Definition at line 38 of file ServerClientRecordProtocol.h.

The documentation for this struct was generated from the following file:

- /Users/Darka/Dropbox/UNITN/AdvancedProgramming/Project/include/**ServerClientRecordProtocol.h**

4.13 session_id_t Struct Reference

```
#include <ServerClientHello.h>
```

Data Fields

- uint8_t **session_lenght**
- uint8_t * **session_id**

4.13.1 Detailed Description

Definition at line 31 of file ServerClientHello.h.

4.13.2 Field Documentation

4.13.2.1 uint8_t* session_id

Definition at line 33 of file ServerClientHello.h.

4.13.2.2 uint8_t session_lenght

Definition at line 32 of file ServerClientHello.h.

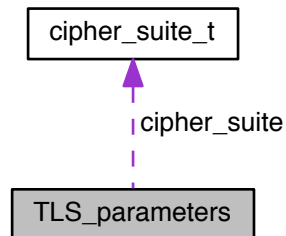
The documentation for this struct was generated from the following file:

- /Users/Darka/Dropbox/UNITN/AdvancedProgramming/Project/include/HandshakeMessages/**ServerClientHello.h**

4.14 TLS_parameters Struct Reference

```
#include <TLS.h>
```

Collaboration diagram for TLS_parameters:



Data Fields

- uint16_t **tls_version**
- uint16_t **previous_state**
- cipher_suite_t **cipher_suite**
- unsigned char **client_random** [32]
- unsigned char **server_random** [32]
- void * **server_key_ex**
- unsigned char * **master_secret**
- int **master_secret_len**
- int **handshake_messages_len**
- unsigned char * **handshake_messages**
- X509 * **server_certificate**
- BIGNUM * **private_key**

4.14.1 Detailed Description

Definition at line 21 of file TLS.h.

4.14.2 Field Documentation

4.14.2.1 cipher_suite_t cipher_suite

Definition at line 24 of file TLS.h.

4.14.2.2 unsigned char client_random[32]

Definition at line 26 of file TLS.h.

4.14.2.3 unsigned char* handshake_messages

Definition at line 35 of file TLS.h.

4.14.2.4 int handshake_messages_len

Definition at line 34 of file TLS.h.

4.14.2.5 unsigned char* master_secret

Definition at line 31 of file TLS.h.

4.14.2.6 int master_secret_len

Definition at line 32 of file TLS.h.

4.14.2.7 uint16_t previous_state

Definition at line 23 of file TLS.h.

4.14.2.8 BIGNUM* private_key

Definition at line 39 of file TLS.h.

4.14.2.9 X509* server_certificate

Definition at line 37 of file TLS.h.

4.14.2.10 void* server_key_ex

Definition at line 29 of file TLS.h.

4.14.2.11 unsigned char server_random[32]

Definition at line 27 of file TLS.h.

4.14.2.12 uint16_t tls_version

Definition at line 22 of file TLS.h.

The documentation for this struct was generated from the following file:

- /Users/Darka/Dropbox/UNITN/AdvancedProgramming/Project/include/**TLS.h**

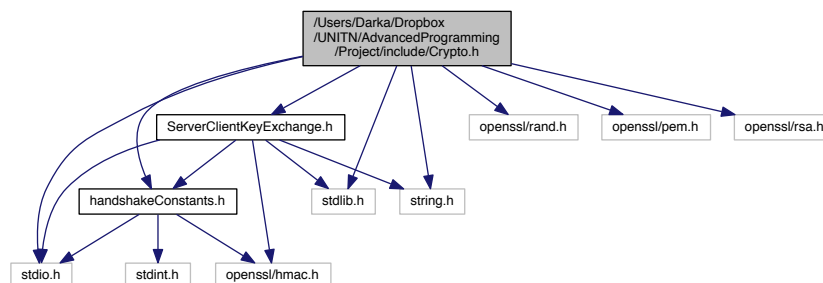
Chapter 5

File Documentation

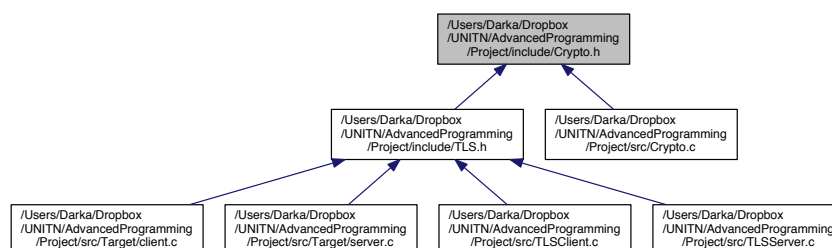
5.1 /Users/Darka/Dropbox/UNITN/AdvancedProgramming/Project/include/Crypto.h File Reference

```
#include <stdio.h>
#include <stdlib.h>
#include <string.h>
#include <openssl/rand.h>
#include <openssl/pem.h>
#include <openssl/rsa.h>
#include "handshakeConstants.h"
#include "ServerClientKeyExchange.h"
```

Include dependency graph for Crypto.h:



This graph shows which files directly or indirectly include this file:



Functions

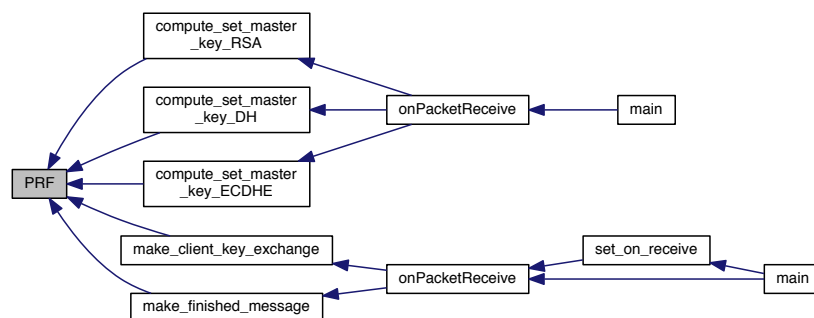
- void **PRF** (const EVP_MD *hash, unsigned char *secret, int secret_len, char *label, unsigned char *seed, int seed_len, int result_len, unsigned char **result)
- int **sign_DHE_server_key_ex** (unsigned char *client_random, unsigned char *server_random, **DHE_server_key_exchange** *server_key_ex, **authentication_algorithm** au)
- int **verify_DHE_server_key_ex_sign** (X509 *certificate, unsigned char *client_random, unsigned char *server_random, **DHE_server_key_exchange** *server_key_ex, **authentication_algorithm** au)
- int **sign_ECDHE_server_key_ex** (unsigned char *client_random, unsigned char *server_random, **ECDHE_server_key_exchange** *server_key_ex, **authentication_algorithm** au)
- int **verify_ECDHE_server_key_ex_sign** (X509 *certificate, unsigned char *client_random, unsigned char *server_random, **ECDHE_server_key_exchange** *server_key_ex, **authentication_algorithm** au)

5.1.1 Function Documentation

5.1.1.1 void PRF (const EVP_MD * *hash*, unsigned char * *secret*, int *secret_len*, char * *label*, unsigned char * *seed*, int *seed_len*, int *result_len*, unsigned char ** *result*)

Definition at line 15 of file Crypto.c.

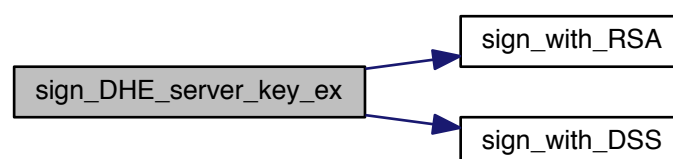
Here is the caller graph for this function:



5.1.1.2 int sign_DHE_server_key_ex (unsigned char * *client_random*, unsigned char * *server_random*, **DHE_server_key_exchange** * *server_key_ex*, **authentication_algorithm** *au*)

Definition at line 127 of file Crypto.c.

Here is the call graph for this function:



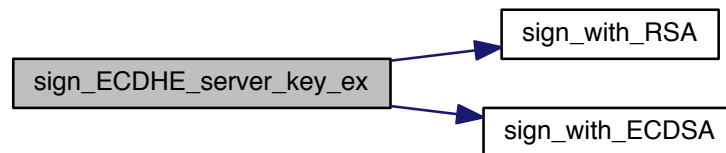
Here is the caller graph for this function:



5.1.1.3 `int sign_ECDHE_server_key_ex (unsigned char * client_random, unsigned char * server_random, ECDHE_server_key_exchange * server_key_ex, authentication_algorithm au)`

Definition at line 199 of file `Crypto.c`.

Here is the call graph for this function:



Here is the caller graph for this function:



5.1.1.4 `int verify_DHE_server_key_ex_sign (X509 * certificate, unsigned char * client_random, unsigned char * server_random, DHE_server_key_exchange * server_key_ex, authentication_algorithm au)`

Definition at line 42 of file `Crypto.c`.

Here is the caller graph for this function:



Data Structures

- struct **cipher_suite_t**

Macros

- **#define REV16(value)** `{{(value & 0x00FFU) << 8 | (value & 0xFF00U) >> 8;}}`
- **#define REV32(value)** `{{(value & 0x000000FFU) << 24 | (value & 0x0000FF00U) << 8 | (value & 0x00FF0000U) >> 8 | (value & 0xFF000000U) >> 24;}}`
- **#define channel_mode_enum**
- **#define enum_record_version**
- **#define enum_handshake_type**

Enumerations

- enum **key_exchange_algorithm** { **RSA_KX** = 1, **DHE_KX** = 2, **ECDHE_KX** = 3 }
- enum **authentication_algorithm** { **RSA_AU** = 1, **DSS_AU** = 2, **ECDSA_AU** = 3 }
- enum **hash_algorithm** {
 none = 0, **md5** = 1, **sha1** = 2, **sha224** = 3,
 sha256 = 4, **sha384** = 5, **sha512** = 6 }
- enum **channel_mode** { **SERVER_MODE**, **CLIENT_MODE** }
- enum **TLS_version** { **SSL3_0** = 0x0300, **TLS1_0** = 0x0301, **TLS1_1** = 0x0302, **TLS1_2** = 0x0303 }
- enum {
 HELLO_REQUEST = 0x00, **CLIENT_HELLO** = 0x01, **SERVER_HELLO** = 0x02, **CERTIFICATE** = 0x0B,
 SERVER_KEY_EXCHANGE = 0x0C, **CERTIFICATE_REQUEST** = 0x0D, **SERVER_DONE** = 0x0E, **CERTIFICATE_VERIFY** = 0x0F,
 CLIENT_KEY_EXCHANGE = 0x10, **FINISHED** = 0x14 }

Functions

- **cipher_suite_t get_cipher_suite** (uint16_t id)
- const EVP_MD * **get_hash_function** (hash_algorithm h)

5.2.1 Macro Definition Documentation

5.2.1.1 #define channel_mode_enum

Definition at line 58 of file handshakeConstants.h.

5.2.1.2 #define enum_handshake_type

Definition at line 90 of file handshakeConstants.h.

5.2.1.3 #define enum_record_version

Definition at line 77 of file handshakeConstants.h.

5.2.1.4 `#define REV16(value)(((value & 0x00FFU) << 8 | (value & 0xFF00U) >> 8;))`

Definition at line 18 of file handshakeConstants.h.

5.2.1.5 `#define REV32(value)(((value & 0x000000FFU) << 24 | (value & 0x0000FF00U) << 8 | (value & 0x00FF0000U) >> 8 | (value & 0xFF000000U) >> 24;))`

Definition at line 19 of file handshakeConstants.h.

5.2.2 Enumeration Type Documentation

5.2.2.1 anonymous enum

Enumerator

HELLO_REQUEST
CLIENT_HELLO
SERVER_HELLO
CERTIFICATE
SERVER_KEY_EXCHANGE
CERTIFICATE_REQUEST
SERVER_DONE
CERTIFICATE_VERIFY
CLIENT_KEY_EXCHANGE
FINISHED

Definition at line 91 of file handshakeConstants.h.

5.2.2.2 enum authentication_algorithm

Enumerator

RSA_AU
DSS_AU
ECDSA_AU

Definition at line 28 of file handshakeConstants.h.

5.2.2.3 enum channel_mode

Enumerator

SERVER_MODE
CLIENT_MODE

Definition at line 59 of file handshakeConstants.h.

5.2.2.4 enum hash_algorithm

Enumerator

none
md5
sha1
sha224
sha256
sha384
sha512

Definition at line 34 of file handshakeConstants.h.

5.2.2.5 enum key_exchange_algorithm

Enumerator

RSA_KX
DHE_KX
ECDHE_KX

Definition at line 22 of file handshakeConstants.h.

5.2.2.6 enum TLS_version

Enumerator

SSL3_0
TLS1_0
TLS1_1
TLS1_2

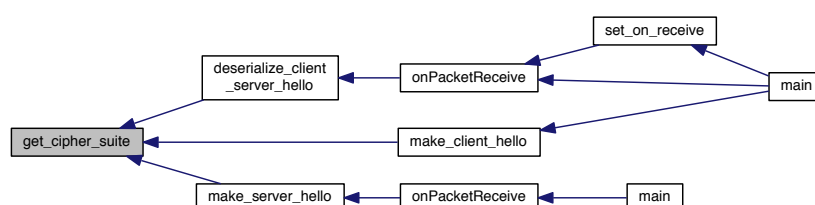
Definition at line 78 of file handshakeConstants.h.

5.2.3 Function Documentation

5.2.3.1 cipher_suite_t get_cipher_suite (uint16_t id)

Definition at line 103 of file handshakeConstants.c.

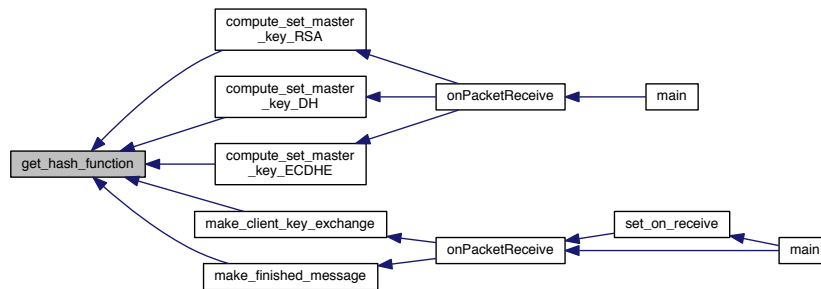
Here is the caller graph for this function:



5.2.3.2 `const EVP_MD* get_hash_function (hash_algorithm h)`

Definition at line 83 of file handshakeConstants.c.

Here is the caller graph for this function:



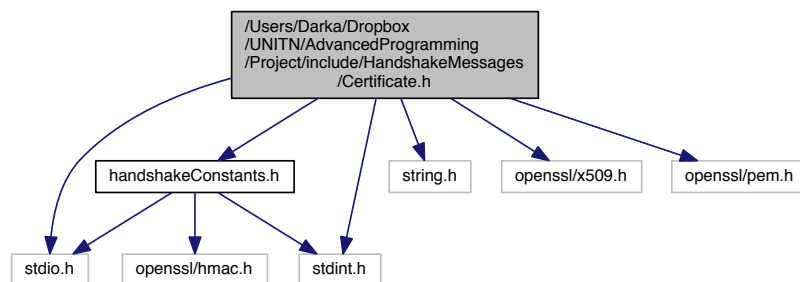
5.3 /Users/Darka/Dropbox/UNITN/AdvancedProgramming/Project/include/HandshakeMessages/Certificate.h File Reference

```

#include <stdio.h>
#include <stdint.h>
#include <string.h>
#include <openssl/x509.h>
#include <openssl/pem.h>
#include "handshakeConstants.h"

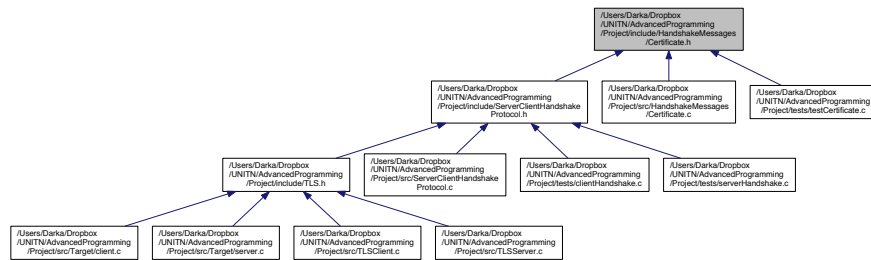
```

Include dependency graph for Certificate.h:



File Reference

This graph shows which files directly or indirectly include this file:



Data Structures

- struct **certificate_message**

Functions

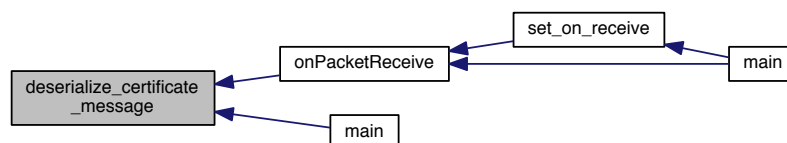
- **certificate_message * make_certificate_message** (char *cert_file_name)
- **void serialize_certificate_message** (certificate_message *cert, unsigned char **stream, uint32_t *len)
- **certificate_message * deserialize_certificate_message** (unsigned char *stream, uint32_t len)
- **void free_certificate_message** (certificate_message *cert)

5.3.1 Function Documentation

5.3.1.1 `certificate_message* deserialize_certificate_message (unsigned char * stream, uint32_t len)`

Definition at line 83 of file Certificate.c.

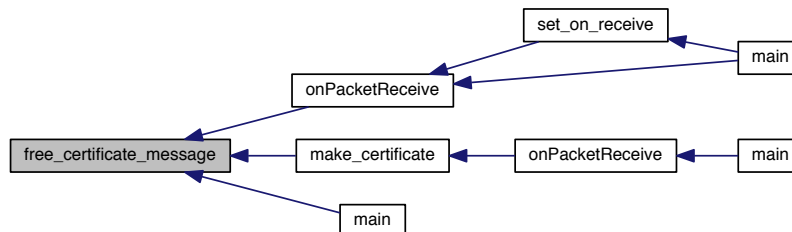
Here is the caller graph for this function:



5.3.1.2 void free_certificate_message (certificate_message * cert)

Definition at line 105 of file Certificate.c.

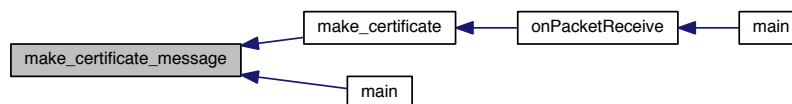
Here is the caller graph for this function:



5.3.1.3 certificate_message* make_certificate_message (char * cert_file_name)

Definition at line 16 of file Certificate.c.

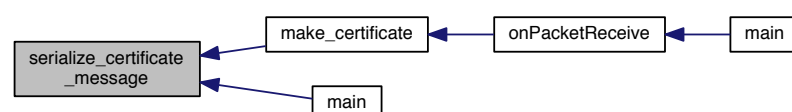
Here is the caller graph for this function:



5.3.1.4 void serialize_certificate_message (certificate_message * cert, unsigned char ** stream, uint32_t * len)

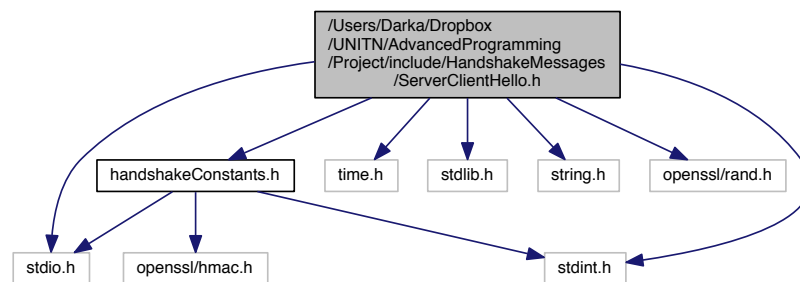
Definition at line 44 of file Certificate.c.

Here is the caller graph for this function:

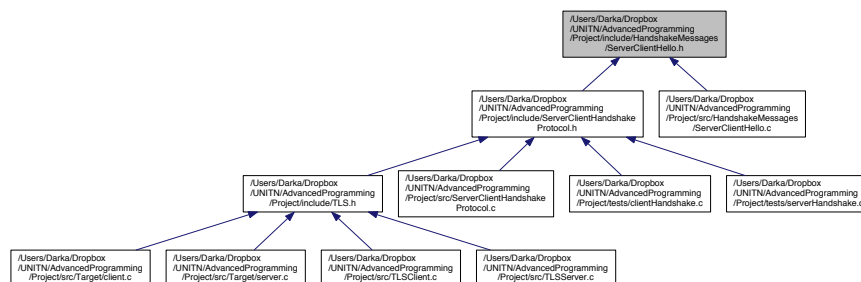


5.4 /Users/Darka/Dropbox/UNITN/AdvancedProgramming/Project/include/HandshakeMessages/ServerClientHello.h File Reference

```
#include <stdio.h>
#include <stdint.h>
#include <time.h>
#include <stdlib.h>
#include <string.h>
#include <openssl/rand.h>
#include "handshakeConstants.h"
Include dependency graph for ServerClientHello.h:
```



This graph shows which files directly or indirectly include this file:



Data Structures

- struct **random_data**
- struct **session_id_t**
- struct **compression_methods_t**
- struct **handshake_hello**

Typedefs

- typedef struct **session_id_t** session_id
- typedef struct **compression_methods_t** compression_methods

Functions

- **handshake_hello** * **make_hello** (**session_id** session)
- void **serialize_client_server_hello** (**handshake_hello** *hello, unsigned char **stream, uint32_t *streamLen, **channel_mode** mode)
- **handshake_hello** * **deserialize_client_server_hello** (unsigned char *stream, uint32_t streamLen, **channel_mode** mode)
- void **free_hello** (**handshake_hello** *h)
- void **print_hello** (**handshake_hello** *h)

5.4.1 Typedef Documentation

5.4.1.1 typedef struct **compression_methods_t** **compression_methods**

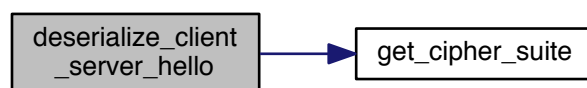
5.4.1.2 typedef struct **session_id_t** **session_id**

5.4.2 Function Documentation

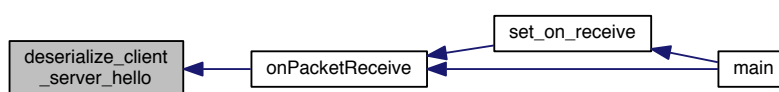
5.4.2.1 **handshake_hello*** **deserialize_client_server_hello** (unsigned char * *stream*, uint32_t *streamLen*, **channel_mode** *mode*)

Definition at line 106 of file ServerClientHello.c.

Here is the call graph for this function:



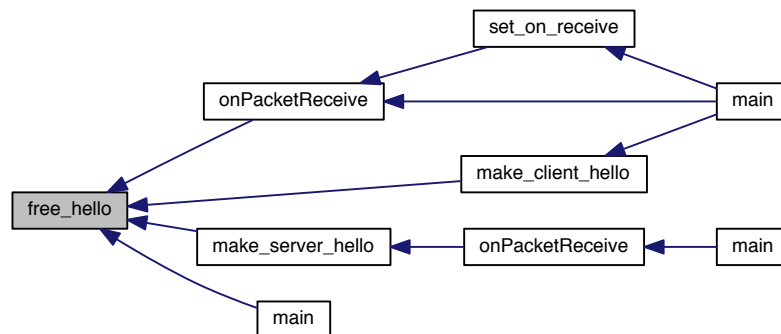
Here is the caller graph for this function:



5.4.2.2 void free_hello (handshake_hello * h)

Definition at line 209 of file ServerClientHello.c.

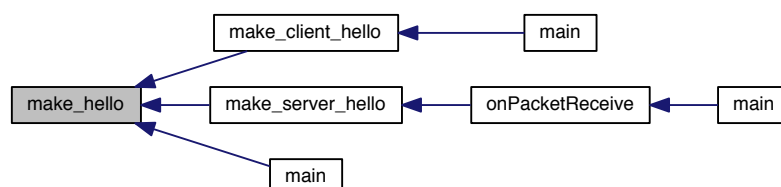
Here is the caller graph for this function:



5.4.2.3 handshake_hello* make_hello (session_id session)

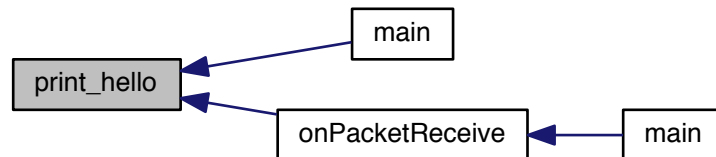
Definition at line 15 of file ServerClientHello.c.

Here is the caller graph for this function:



5.4.2.4 void print_hello (handshake_hello * h)

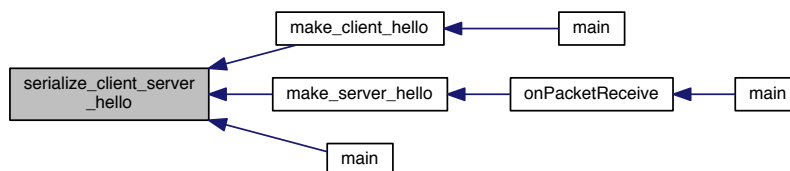
Here is the caller graph for this function:



5.4.2.5 void serialize_client_server_hello (handshake_hello * hello, unsigned char ** stream, uint32_t * streamLen, channel_mode mode)

Definition at line 37 of file ServerClientHello.c.

Here is the caller graph for this function:



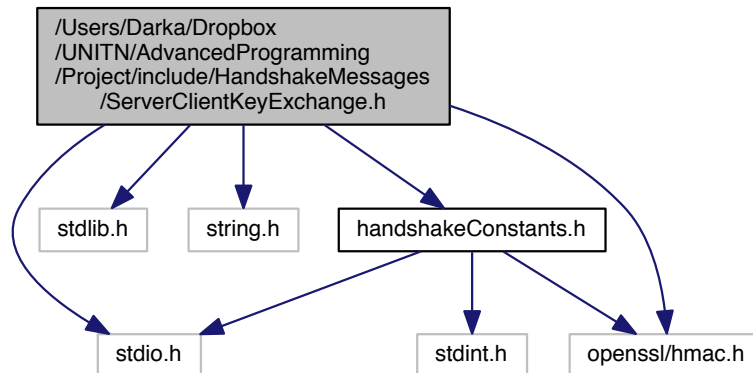
5.5 /Users/Darka/Dropbox/UNITN/AdvancedProgramming/Project/include/HandshakeMessages/ServerClientKeyExchange.h File Reference

```

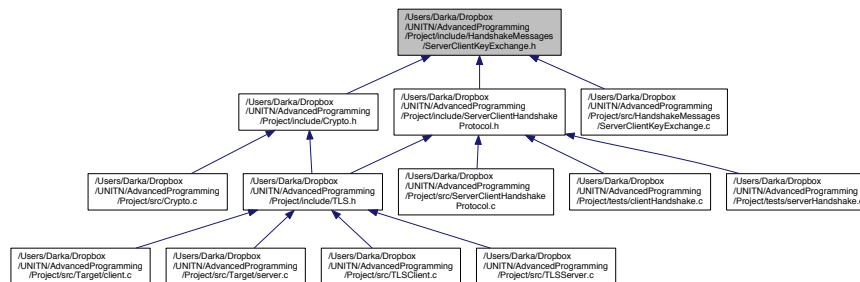
#include <stdio.h>
#include <stdlib.h>
#include <string.h>
#include <openssl/hmac.h>
#include "handshakeConstants.h"

```


Include dependency graph for ServerClientKeyExchange.h:



This graph shows which files directly or indirectly include this file:



Data Structures

- struct **ECDHE_server_key_exchange**
- struct **DHE_server_key_exchange**
- struct **client_key_exchange**

Macros

- #define **server_key_exchange_structs**

Functions

- void **serialize_server_key_exchange** (void *server_key_exchange, unsigned char **stream, uint32_t *streamLen, key_exchange_algorithm kx)
- void * **deserialize_server_key_exchange** (uint32_t message_len, unsigned char *message, key_exchange_algorithm kx)
- void **serialize_client_key_exchange** (client_key_exchange *client_key_exchange, unsigned char **stream, uint32_t *streamLen)
- void * **deserialize_client_key_exchange** (uint32_t message_len, unsigned char *message)
- void **free_server_key_exchange** (void *server_key_ex, cipher_suite_t cipher_suite)

5.5.1 Macro Definition Documentation

5.5.1.1 #define server_key_exchange_structs

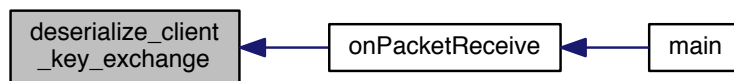
Definition at line 24 of file ServerClientKeyExchange.h.

5.5.2 Function Documentation

5.5.2.1 void* deserialize_client_key_exchange (uint32_t message_len, unsigned char * message)

Definition at line 185 of file ServerClientKeyExchange.c.

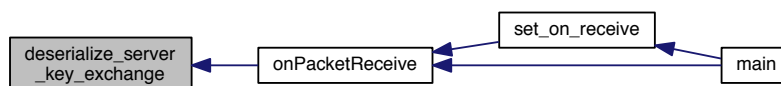
Here is the caller graph for this function:



5.5.2.2 void* deserialize_server_key_exchange (uint32_t message_len, unsigned char * message, key_exchange_algorithm kx)

Definition at line 104 of file ServerClientKeyExchange.c.

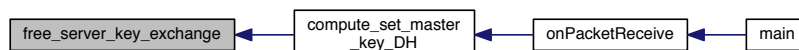
Here is the caller graph for this function:



5.5.2.3 void free_server_key_exchange (void * server_key_ex, cipher_suite_t cipher_suite)

Definition at line 199 of file ServerClientKeyExchange.c.

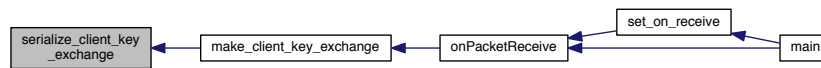
Here is the caller graph for this function:



5.5.2.4 void `serialize_client_key_exchange` (`client_key_exchange` * `client_key_exchange`, unsigned char ** `stream`, uint32_t * `streamLen`)

Definition at line 171 of file `ServerClientKeyExchange.c`.

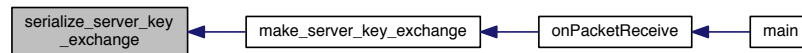
Here is the caller graph for this function:



5.5.2.5 void `serialize_server_key_exchange` (void * `server_key_exchange`, unsigned char ** `stream`, uint32_t * `streamLen`, `key_exchange_algorithm` `kx`)

Definition at line 15 of file `ServerClientKeyExchange.c`.

Here is the caller graph for this function:



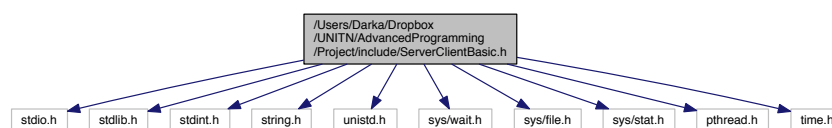
5.6 /Users/Darka/Dropbox/UNITN/AdvancedProgramming/Project/include/ServerClientBasic.h File Reference

```

#include <stdio.h>
#include <stdlib.h>
#include <stdint.h>
#include <string.h>
#include <unistd.h>
#include <sys/wait.h>
#include <sys/file.h>
#include <sys/stat.h>
#include <pthread.h>
#include <time.h>

```

Include dependency graph for `ServerClientBasic.h`:



5.6.1.2 `#define enum_mode`

Definition at line 42 of file ServerClientBasic.h.

5.6.1.3 `#define struct_channel`

Definition at line 61 of file ServerClientBasic.h.

5.6.1.4 `#define struct_packet`

Definition at line 49 of file ServerClientBasic.h.

5.6.2 Typedef Documentation

5.6.2.1 `typedef struct channel channel`

5.6.3 Enumeration Type Documentation

5.6.3.1 `enum mode`

Enumerator

SERVER

CLIENT

Definition at line 43 of file ServerClientBasic.h.

5.6.4 Function Documentation

5.6.4.1 `channel* create_channel (char * fileName, char * channelFrom, char * channelTo, mode channelMode)`

Definition at line 19 of file ServerClientBasic.c.

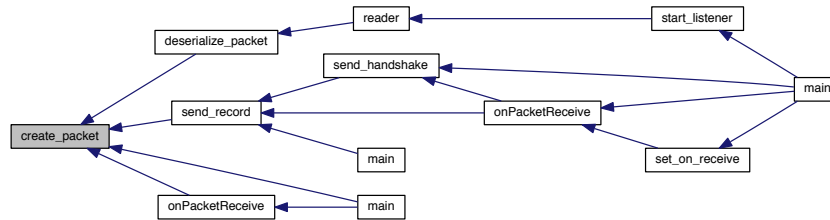
Here is the caller graph for this function:



5.6.4.2 `packet_basic* create_packet (char * from, char * to, unsigned char * message, uint32_t messageLen)`

Definition at line 131 of file ServerClientBasic.c.

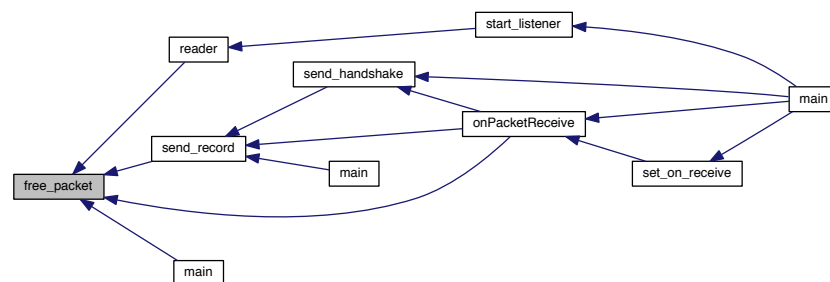
Here is the caller graph for this function:



5.6.4.3 `void free_packet (packet_basic * p)`

Definition at line 152 of file ServerClientBasic.c.

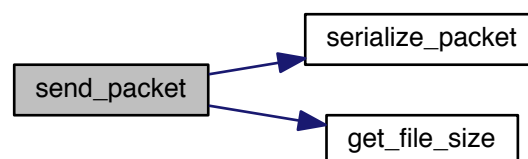
Here is the caller graph for this function:



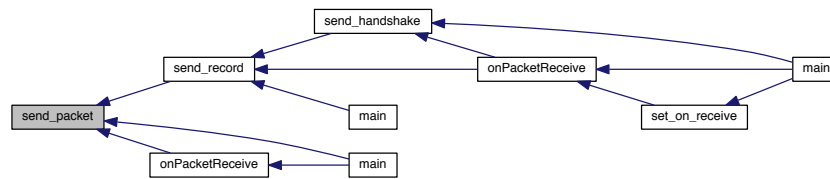
5.6.4.4 `int send_packet (channel * ch, packet_basic * p)`

Definition at line 41 of file ServerClientBasic.c.

Here is the call graph for this function:



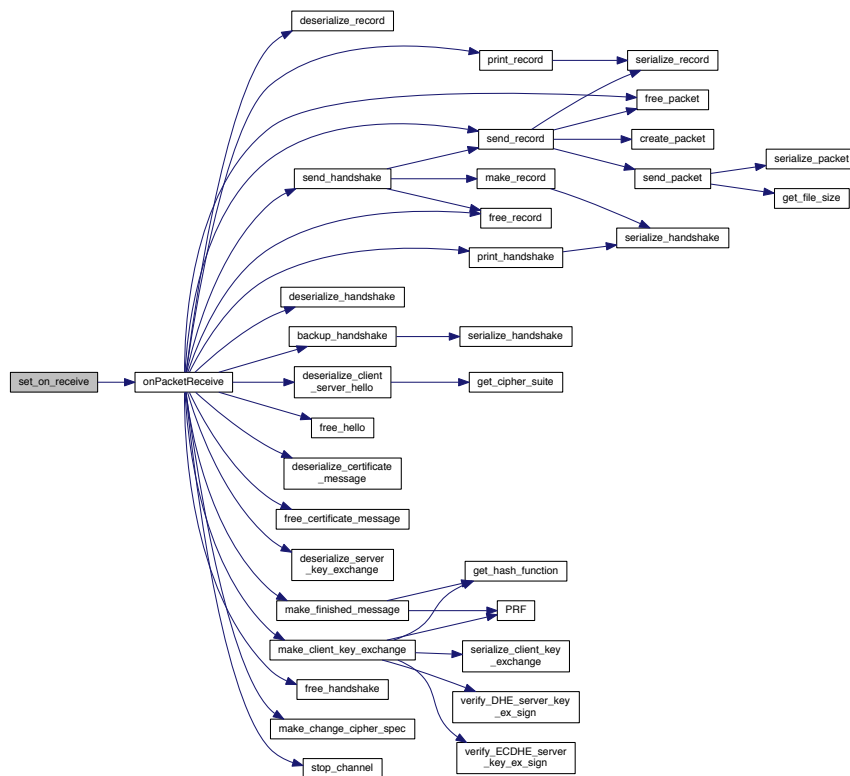
Here is the caller graph for this function:



5.6.4.5 `int set_on_receive (channel * ch, void(*) (channel *ch, packet_basic *p) onPacketReceive)`

Definition at line 32 of file `ServerClientBasic.c`.

Here is the call graph for this function:



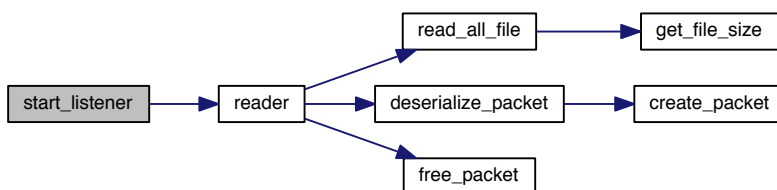
Here is the caller graph for this function:



5.6.4.6 `int start_listener (channel * ch)`

Definition at line 103 of file `ServerClientBasic.c`.

Here is the call graph for this function:



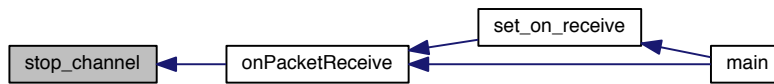
Here is the caller graph for this function:



5.6.4.7 `void stop_channel (channel * ch)`

Definition at line 121 of file `ServerClientBasic.c`.

Here is the caller graph for this function:



5.6.4.8 void wait_channel (channel * ch)

Definition at line 127 of file ServerClientBasic.c.

Here is the caller graph for this function:



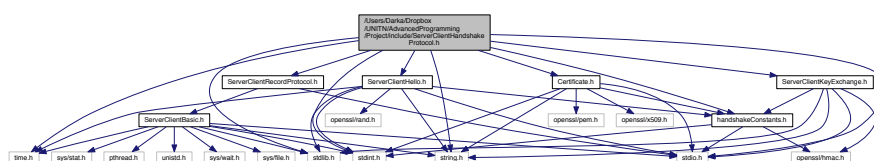
5.7 /Users/Darka/Dropbox/UNITN/AdvancedProgramming/Project/include/ServerClientHandshakeProtocol.h File Reference

```

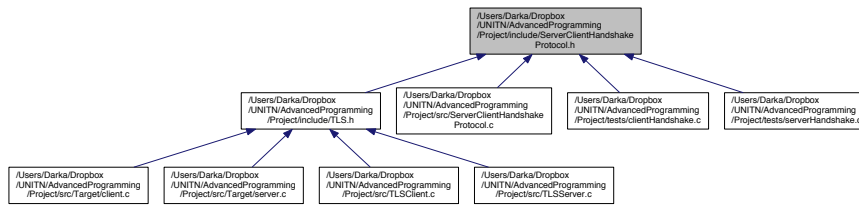
#include <stdio.h>
#include <stdint.h>
#include <time.h>
#include <stdlib.h>
#include <string.h>
#include "ServerClientRecordProtocol.h"
#include "handshakeConstants.h"
#include "ServerClientHello.h"
#include "Certificate.h"
#include "ServerClientKeyExchange.h"

```

Include dependency graph for ServerClientHandshakeProtocol.h:



This graph shows which files directly or indirectly include this file:



Data Structures

- struct **handshake**

Functions

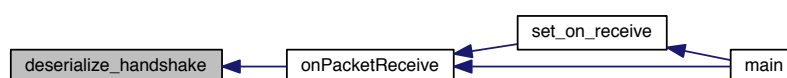
- int **send_handshake** (channel *ch, handshake *h)
- void **serialize_handshake** (handshake *h, unsigned char **stream, uint32_t *streamLen)
- handshake * **deserialize_handshake** (unsigned char *message, uint32_t messageLen)
- void **print_handshake** (handshake *h)
- void **free_handshake** (handshake *h)

5.7.1 Function Documentation

5.7.1.1 handshake* deserialize_handshake (unsigned char * message, uint32_t messageLen)

Definition at line 50 of file ServerClientHandshakeProtocol.c.

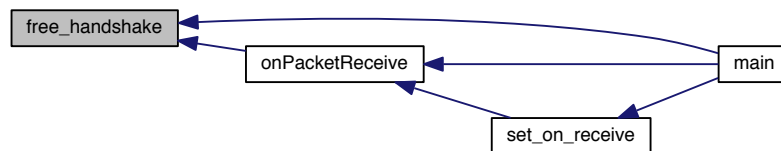
Here is the caller graph for this function:



5.7.1.2 void free_handshake (handshake * h)

Definition at line 66 of file ServerClientHandshakeProtocol.c.

Here is the caller graph for this function:



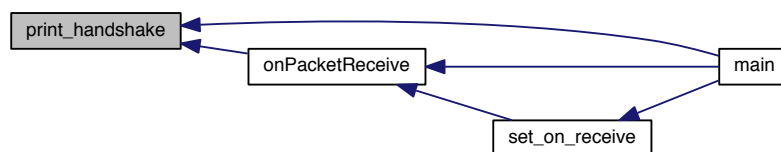
5.7.1.3 void print_handshake (handshake * h)

Definition at line 73 of file ServerClientHandshakeProtocol.c.

Here is the call graph for this function:



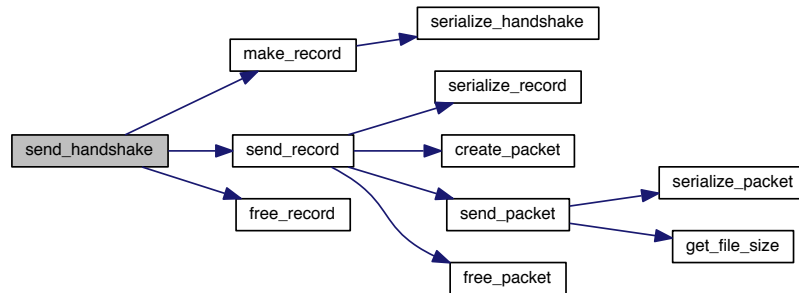
Here is the caller graph for this function:



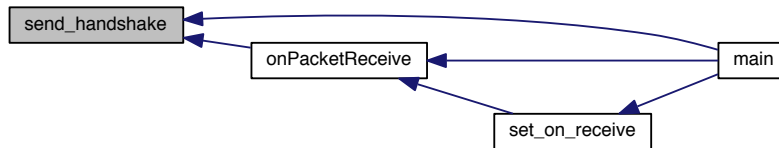
5.7.1.4 `int send_handshake (channel * ch, handshake * h)`

Definition at line 25 of file ServerClientHandshakeProtocol.c.

Here is the call graph for this function:



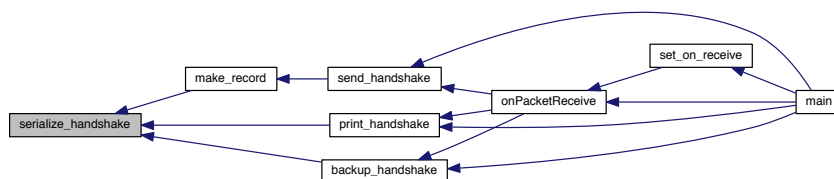
Here is the caller graph for this function:



5.7.1.5 `void serialize_handshake (handshake * h, unsigned char ** stream, uint32_t * streamLen)`

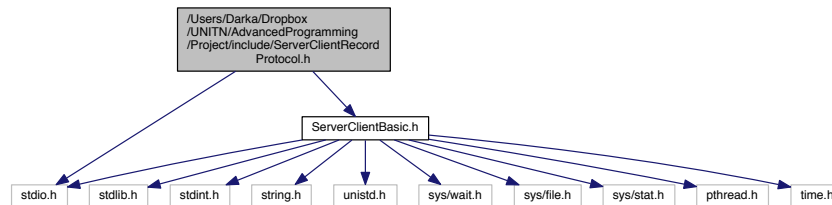
Definition at line 35 of file ServerClientHandshakeProtocol.c.

Here is the caller graph for this function:

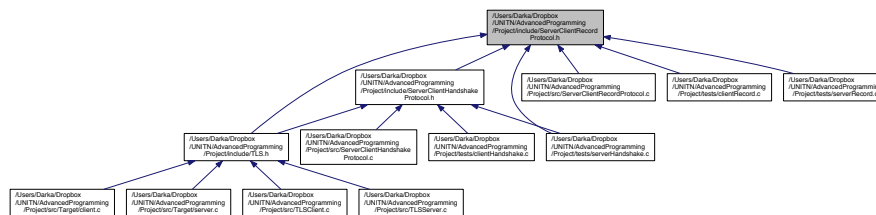


5.8 /Users/Darka/Dropbox/UNITN/AdvancedProgramming/Project/include/ServerClientRecordProtocol.h File Reference

```
#include <stdio.h>
#include "ServerClientBasic.h"
Include dependency graph for ServerClientRecordProtocol.h:
```



This graph shows which files directly or indirectly include this file:



Data Structures

- struct **record**

Macros

- #define **REV16**(value) (((value & 0x00FFU) << 8 | (value & 0xFF00U) >> 8;))
- #define **enum_recordtype**
- #define **struct_record**

Typedefs

- typedef struct **record** **record**

Enumerations

- enum **recordType** { **HANDSHAKE** = 0x16, **CHANGE_CIPHER_SPEC** = 0x14, **ALERT** = 0x15, **APPLICATION_DATA** = 0x17 }

Functions

- int **send_record** (channel *ch, record *r)
- record * **deserialize_record** (unsigned char *message, uint32_t messageLen)
- void **serialize_record** (record *r, unsigned char **message, uint16_t *messageLen)
Serialize record in a byte stream message and message length are used for return.
- void **print_record** (record *r)
- void **free_record** (record *r)

5.8.1 Macro Definition Documentation

5.8.1.1 #define enum_recordtype

Definition at line 22 of file ServerClientRecordProtocol.h.

5.8.1.2 #define REV16(value)({(value & 0x00FFU) << 8 | (value & 0xFF00U) >> 8;})

Definition at line 14 of file ServerClientRecordProtocol.h.

5.8.1.3 #define struct_record

Definition at line 35 of file ServerClientRecordProtocol.h.

5.8.2 Typedef Documentation

5.8.2.1 typedef struct record record

5.8.3 Enumeration Type Documentation

5.8.3.1 enum recordType

Enumerator

HANDSHAKE
CHANGE_CIPHER_SPEC
ALERT
APPLICATION_DATA

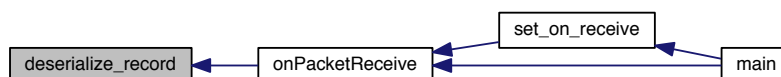
Definition at line 23 of file ServerClientRecordProtocol.h.

5.8.4 Function Documentation

5.8.4.1 `record* deserialize_record (unsigned char * message, uint32_t messageLen)`

Definition at line 22 of file `ServerClientRecordProtocol.c`.

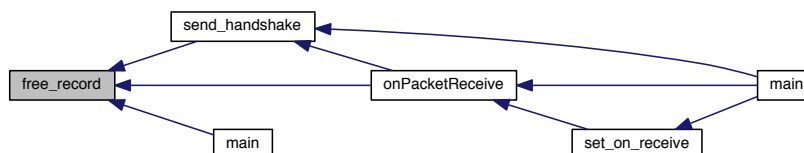
Here is the caller graph for this function:



5.8.4.2 `void free_record (record * r)`

Definition at line 68 of file `ServerClientRecordProtocol.c`.

Here is the caller graph for this function:



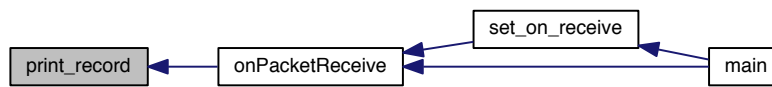
5.8.4.3 `void print_record (record * r)`

Definition at line 48 of file `ServerClientRecordProtocol.c`.

Here is the call graph for this function:



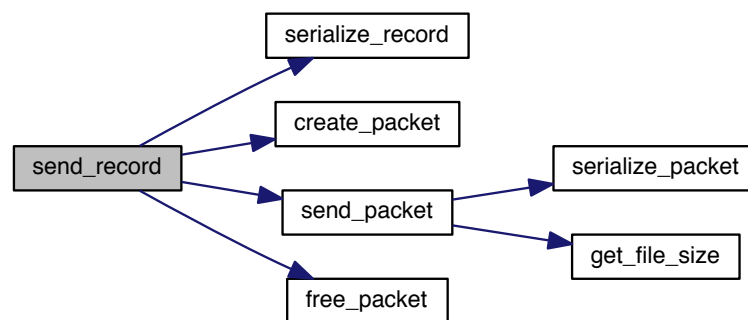
Here is the caller graph for this function:



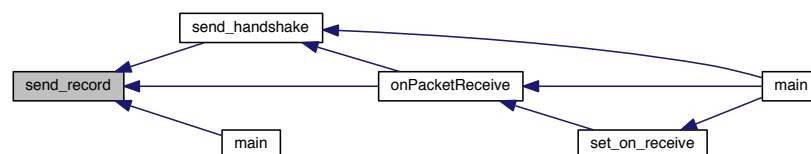
5.8.4.4 int send_record (channel * ch, record * r)

Definition at line 36 of file ServerClientRecordProtocol.c.

Here is the call graph for this function:



Here is the caller graph for this function:



5.8.4.5 void serialize_record (record * r, unsigned char ** message, uint16_t * messageLen)

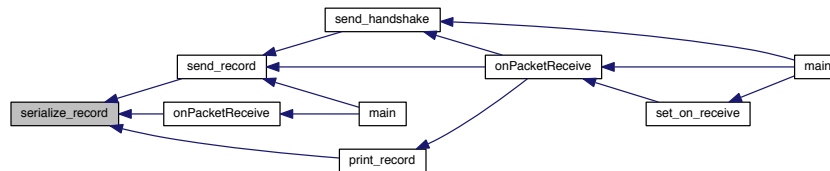
Serialize record in a byte stream message and message length are used for return.

Parameters

<i>message</i>	: pointer to null (the function allocate space for you)
<i>messageLen</i>	: pointer to integer (will contains the message length)

Definition at line 11 of file ServerClientRecordProtocol.c.

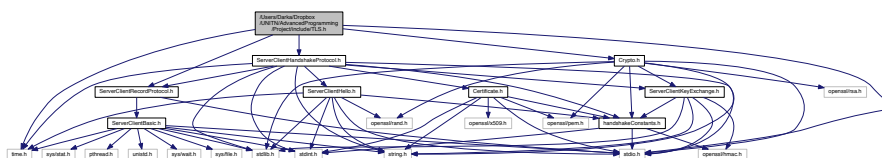
Here is the caller graph for this function:



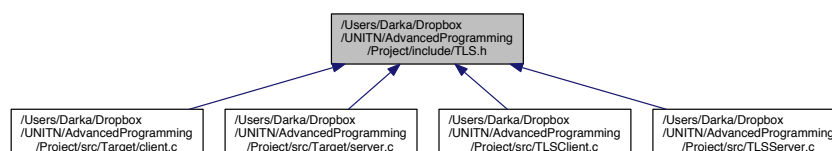
5.9 /Users/Darka/Dropbox/UNITN/AdvancedProgramming/Project/include/TLS.h File Reference

```
#include <stdio.h>
#include <time.h>
#include "ServerClientHandshakeProtocol.h"
#include "ServerClientRecordProtocol.h"
#include "Crypto.h"
```

Include dependency graph for TLS.h:



This graph shows which files directly or indirectly include this file:



Data Structures

- struct **TLS_parameters**

Macros

- `#define TLS_parameter_enum`

Functions

- `handshake * make_client_hello` (unsigned char *client_random)
- `handshake * make_client_key_exchange` (TLS_parameters *TLS_param, uint16_t key_ex_alg)
- `record * make_change_cipher_spec` ()
- `handshake * make_finished_message` (TLS_parameters *TLS_param)
- `handshake * make_server_hello` (TLS_parameters *TLS_param, handshake_hello *client_hello)
- `handshake * make_certificate` (TLS_parameters *TLS_param)
- `handshake * make_server_key_exchange` (TLS_parameters *TLS_param)
- `handshake * make_server_hello_done` ()
- `DHE_server_key_exchange * make_DHE_server_key_exchange` (TLS_parameters *TLS_param)
- `ECDHE_server_key_exchange * make_ECDHE_server_key_exchange` (TLS_parameters *TLS_param)
- `void backup_handshake` (TLS_parameters *TLS_param, handshake *h)

5.9.1 Macro Definition Documentation

5.9.1.1 #define TLS_parameter_enum

Definition at line 20 of file TLS.h.

5.9.2 Function Documentation

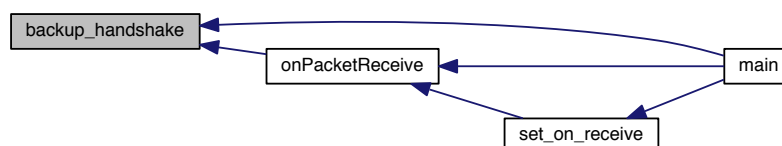
5.9.2.1 void backup_handshake (TLS_parameters * TLS_param, handshake * h)

Definition at line 13 of file TLSClient.c.

Here is the call graph for this function:



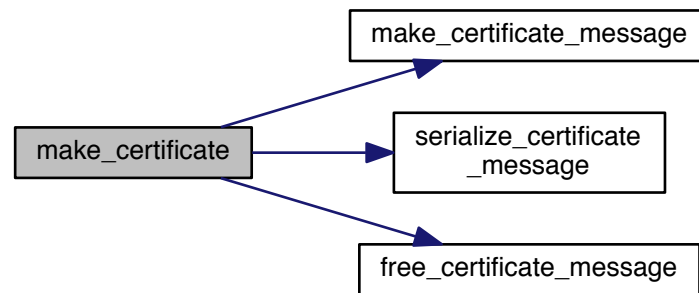
Here is the caller graph for this function:



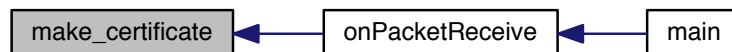
5.9.2.2 handshake* make_certificate (TLS_parameters * TLS_param)

Definition at line 48 of file TLSServer.c.

Here is the call graph for this function:



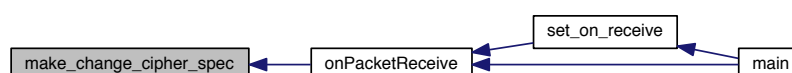
Here is the caller graph for this function:



5.9.2.3 record* make_change_cipher_spec ()

Definition at line 250 of file TLSClient.c.

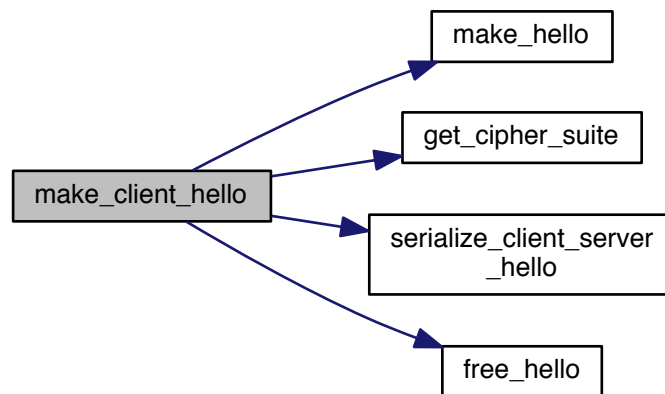
Here is the caller graph for this function:



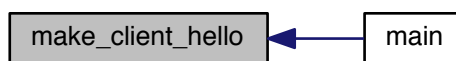
5.9.2.4 handshake* make_client_hello (unsigned char * *client_random*)

Definition at line 31 of file TLSClient.c.

Here is the call graph for this function:



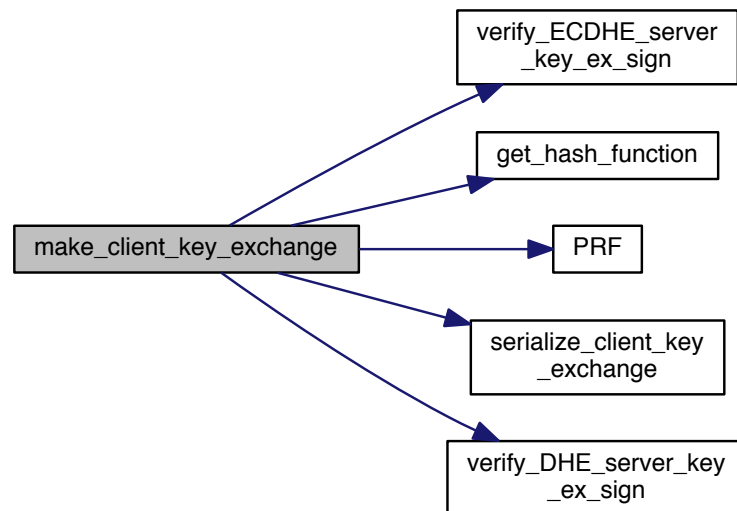
Here is the caller graph for this function:



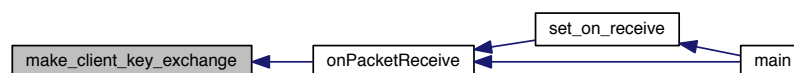
5.9.2.5 handshake* make_client_key_exchange (TLS_parameters * *TLS_param*, uint16_t *key_ex_alg*)

Definition at line 65 of file TLSClient.c.

Here is the call graph for this function:



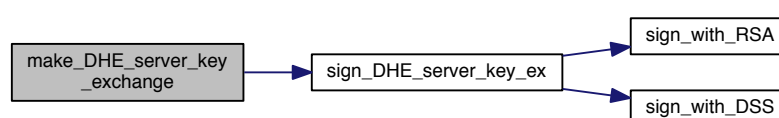
Here is the caller graph for this function:



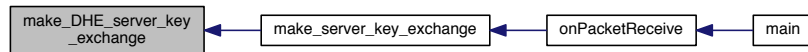
5.9.2.6 DHE_server_key_exchange* make_DHE_server_key_exchange (TLS_parameters * TLS_param)

Definition at line 113 of file TLSServer.c.

Here is the call graph for this function:



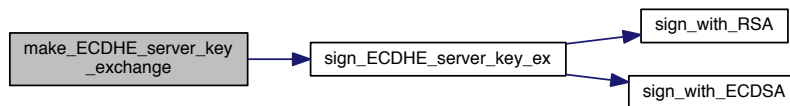
Here is the caller graph for this function:



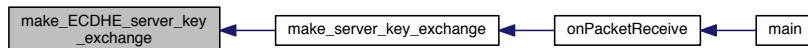
5.9.2.7 ECDHE_server_key_exchange* make_ECDHE_server_key_exchange (TLS_parameters * TLS_param)

Definition at line 153 of file TLSServer.c.

Here is the call graph for this function:



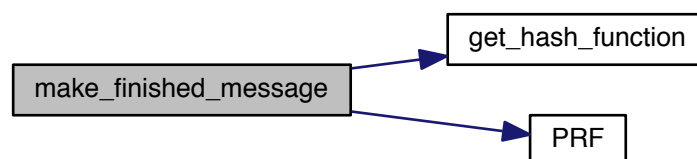
Here is the caller graph for this function:



5.9.2.8 handshake* make_finished_message (TLS_parameters * TLS_param)

Definition at line 262 of file TLSClient.c.

Here is the call graph for this function:



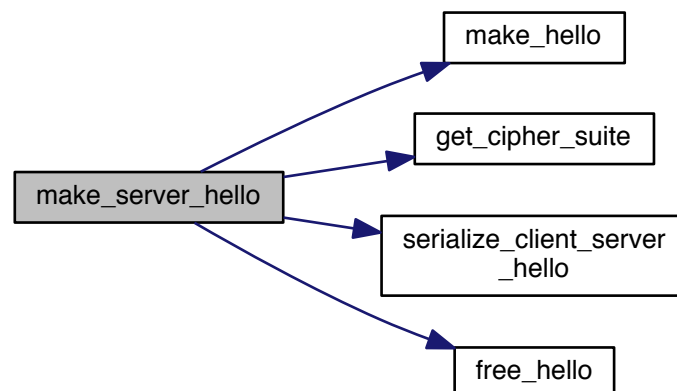
Here is the caller graph for this function:



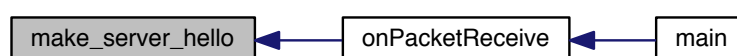
5.9.2.9 handshake* make_server_hello (TLS_parameters * TLS_param, handshake_hello * client_hello)

Definition at line 11 of file TLSServer.c.

Here is the call graph for this function:



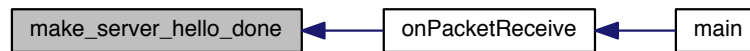
Here is the caller graph for this function:



5.9.2.10 handshake* make_server_hello_done ()

Definition at line 188 of file TLSServer.c.

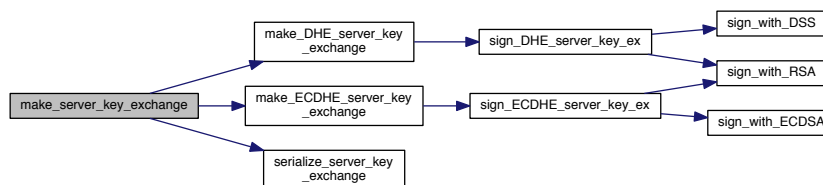
Here is the caller graph for this function:



5.9.2.11 handshake* make_server_key_exchange (TLS_parameters * TLS_param)

Definition at line 84 of file TLSServer.c.

Here is the call graph for this function:



Here is the caller graph for this function:

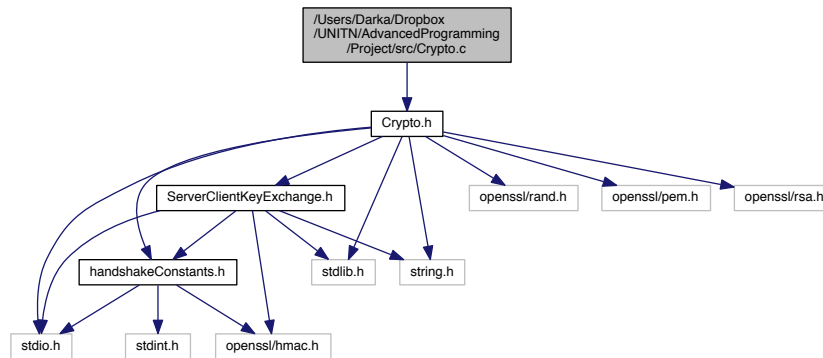


5.10 /Users/Darka/Dropbox/UNITN/AdvancedProgramming/Project/README.md File Reference

5.11 /Users/Darka/Dropbox/UNITN/AdvancedProgramming/Project/src/Crypto.c File Reference

```
#include "Crypto.h"
```

Include dependency graph for Crypto.c:



Functions

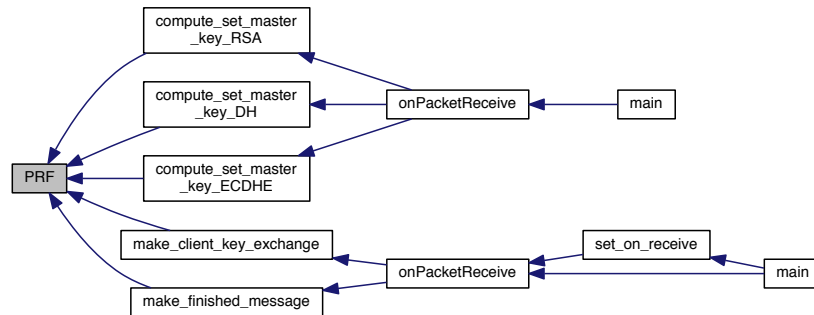
- int **sign_with_RSA** (unsigned char **signature, unsigned int *signature_length, unsigned int to_sign_len, unsigned char *to_sign)
- int **sign_with_DSS** (unsigned char **signature, unsigned int *signature_length, unsigned int to_sign_len, unsigned char *to_sign)
- int **sign_with_ECDSA** (unsigned char **signature, unsigned int *signature_length, unsigned int to_sign_len, unsigned char *to_sign)
- void **PRF** (const EVP_MD *hash, unsigned char *secret, int secret_len, char *label, unsigned char *seed, int seed_len, int result_len, unsigned char **result)
- int **verify_DHE_server_key_ex_sign** (X509 *certificate, unsigned char *client_random, unsigned char *server_random, **DHE_server_key_exchange** *server_key_ex, **authentication_algorithm** au)
- int **sign_DHE_server_key_ex** (unsigned char *client_random, unsigned char *server_random, **DHE_server_key_exchange** *server_key_ex, **authentication_algorithm** au)
- int **sign_ECDHE_server_key_ex** (unsigned char *client_random, unsigned char *server_random, **ECDHE_server_key_exchange** *server_key_ex, **authentication_algorithm** au)
- int **verify_ECDHE_server_key_ex_sign** (X509 *certificate, unsigned char *client_random, unsigned char *server_random, **ECDHE_server_key_exchange** *server_key_ex, **authentication_algorithm** au)

5.11.1 Function Documentation

- 5.11.1.1 void **PRF** (const EVP_MD * hash, unsigned char * secret, int secret_len, char * label, unsigned char * seed, int seed_len, int result_len, unsigned char ** result)

Definition at line 15 of file Crypto.c.

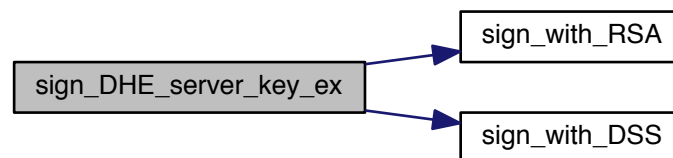
Here is the caller graph for this function:



5.11.1.2 `int sign_DHE_server_key_ex (unsigned char * client_random, unsigned char * server_random, DHE_server_key_exchange * server_key_ex, authentication_algorithm au)`

Definition at line 127 of file Crypto.c.

Here is the call graph for this function:



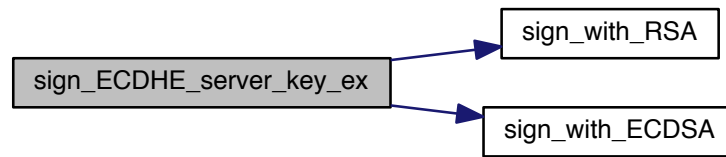
Here is the caller graph for this function:



5.11.1.3 `int sign_ECDHE_server_key_ex (unsigned char * client_random, unsigned char * server_random, ECDHE_server_key_exchange * server_key_ex, authentication_algorithm au)`

Definition at line 199 of file Crypto.c.

Here is the call graph for this function:



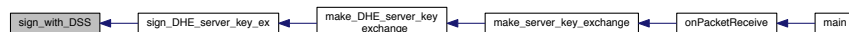
Here is the caller graph for this function:



5.11.1.4 `int sign_with_DSS (unsigned char ** signature, unsigned int * signature_length, unsigned int to_sign_len, unsigned char * to_sign)`

Definition at line 337 of file `Crypto.c`.

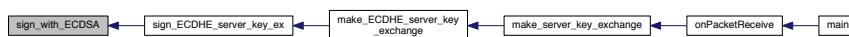
Here is the caller graph for this function:



5.11.1.5 `int sign_with_ECDSA (unsigned char ** signature, unsigned int * signature_length, unsigned int to_sign_len, unsigned char * to_sign)`

Definition at line 384 of file `Crypto.c`.

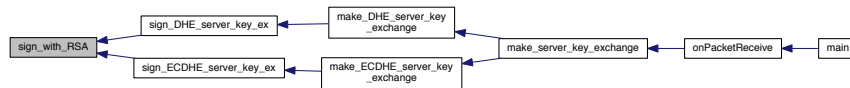
Here is the caller graph for this function:



5.11.1.6 `int sign_with_RSA (unsigned char ** signature, unsigned int * signature_length, unsigned int to_sign_len, unsigned char * to_sign)`

Definition at line 358 of file `Crypto.c`.

Here is the caller graph for this function:



5.11.1.7 `int verify_DHE_server_key_ex_sign (X509 * certificate, unsigned char * client_random, unsigned char * server_random, DHE_server_key_exchange * server_key_ex, authentication_algorithm au)`

Definition at line 42 of file `Crypto.c`.

Here is the caller graph for this function:



5.11.1.8 `int verify_ECDHE_server_key_ex_sign (X509 * certificate, unsigned char * client_random, unsigned char * server_random, ECDHE_server_key_exchange * server_key_ex, authentication_algorithm au)`

Definition at line 259 of file `Crypto.c`.

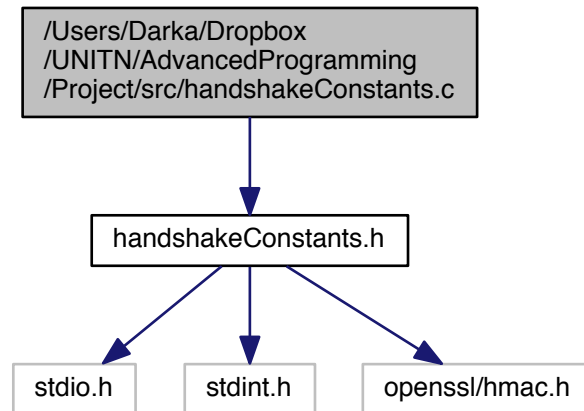
Here is the caller graph for this function:



5.12 /Users/Darka/Dropbox/UNITN/AdvancedProgramming/Project/src/handshakeConstants.c File Reference

```
#include "handshakeConstants.h"
```

Include dependency graph for handshakeConstants.c:



Functions

- `const EVP_MD * get_hash_function (hash_algorithm h)`
- `cipher_suite_t get_cipher_suite (uint16_t id)`

Variables

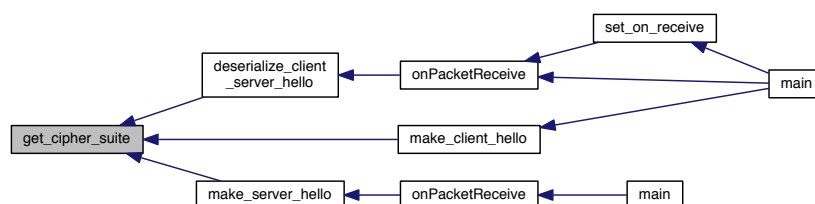
- `int cipher_suite_len = 61`
- `cipher_suite_t cipher_suite_list []`

5.12.1 Function Documentation

5.12.1.1 `cipher_suite_t get_cipher_suite (uint16_t id)`

Definition at line 103 of file `handshakeConstants.c`.

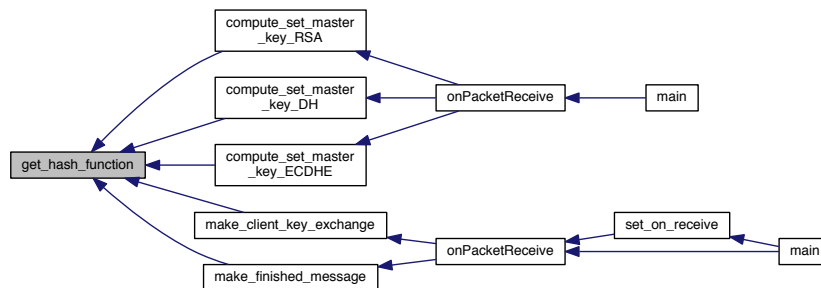
Here is the caller graph for this function:



5.12.1.2 `const EVP_MD* get_hash_function (hash_algorithm h)`

Definition at line 83 of file handshakeConstants.c.

Here is the caller graph for this function:



5.12.2 Variable Documentation

5.12.2.1 `int cipher_suite_len = 61`

Definition at line 11 of file handshakeConstants.c.

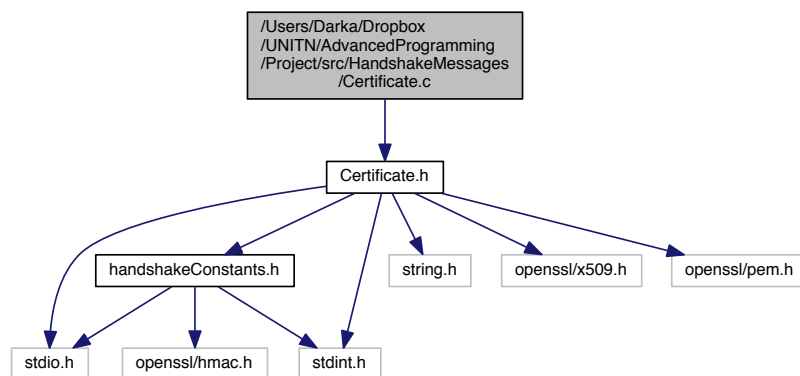
5.12.2.2 `cipher_suite_t cipher_suite_list[]`

Definition at line 13 of file handshakeConstants.c.

5.13 `/Users/Darka/Dropbox/UNITN/AdvancedProgramming/Project/src/HandshakeMessages/Certificate.c` File Reference

```
#include "Certificate.h"
```

Include dependency graph for `Certificate.c`:



Functions

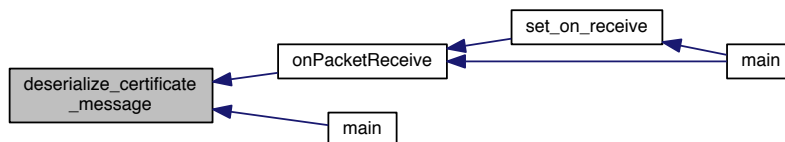
- **certificate_message * make_certificate_message** (char *cert_file_name)
- void **serialize_certificate_message** (certificate_message *cert, unsigned char **stream, uint32_t *len)
- **certificate_message * deserialize_certificate_message** (unsigned char *stream, uint32_t len)
- void **free_certificate_message** (certificate_message *cert)

5.13.1 Function Documentation

5.13.1.1 certificate_message* deserialize_certificate_message (unsigned char * stream, uint32_t len)

Definition at line 83 of file Certificate.c.

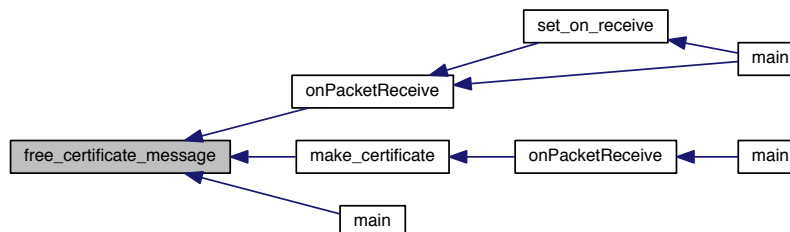
Here is the caller graph for this function:



5.13.1.2 void free_certificate_message (certificate_message * cert)

Definition at line 105 of file Certificate.c.

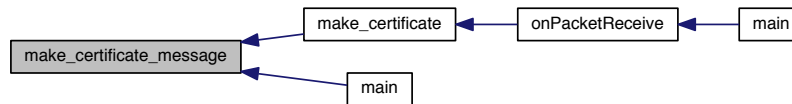
Here is the caller graph for this function:



5.13.1.3 `certificate_message* make_certificate_message (char * cert_file_name)`

Definition at line 16 of file Certificate.c.

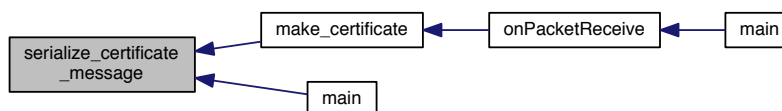
Here is the caller graph for this function:



5.13.1.4 `void serialize_certificate_message (certificate_message * cert, unsigned char ** stream, uint32_t * len)`

Definition at line 44 of file Certificate.c.

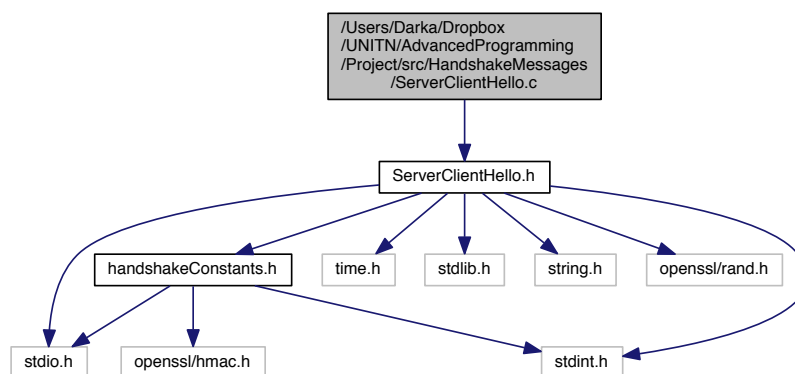
Here is the caller graph for this function:



5.14 `/Users/Darka/Dropbox/UNITN/AdvancedProgramming/Project/src/HandshakeMessages/ServerClientHello.c` File Reference

```
#include "ServerClientHello.h"
```

Include dependency graph for `ServerClientHello.c`:



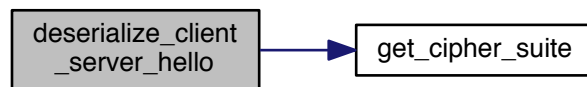
- **handshake_hello * make_hello** (**session_id** session)
- void **serialize_client_server_hello** (**handshake_hello** *hello, unsigned char **stream, uint32_t *streamLen, **channel_mode** mode)
- **handshake_hello * deserialize_client_server_hello** (unsigned char *stream, uint32_t streamLen, **channel_mode** mode)
- void **free_hello** (**handshake_hello** *h)

5.14.1 Function Documentation

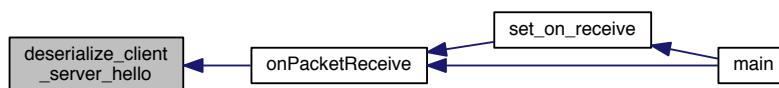
5.14.1.1 handshake_hello* deserialize_client_server_hello (unsigned char * *stream*, uint32_t *streamLen*, **channel_mode** *mode*)

Definition at line 106 of file ServerClientHello.c.

Here is the call graph for this function:



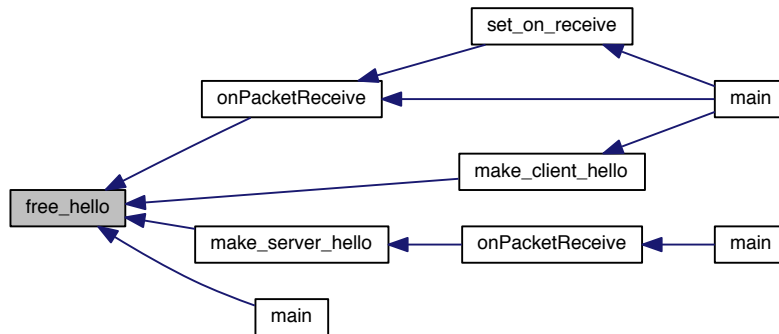
Here is the caller graph for this function:



5.14.1.2 void free_hello (handshake_hello * h)

Definition at line 209 of file ServerClientHello.c.

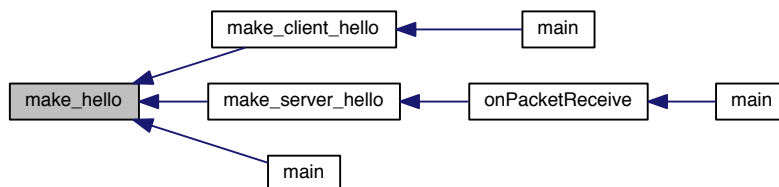
Here is the caller graph for this function:



5.14.1.3 `handshake_hello* make_hello (session_id session)`

Definition at line 15 of file `ServerClientHello.c`.

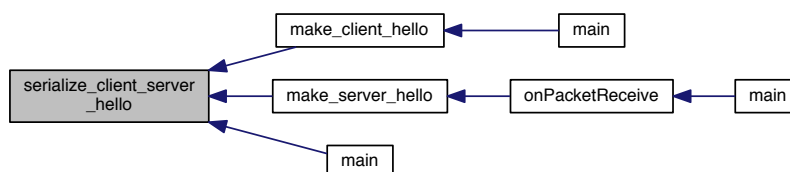
Here is the caller graph for this function:



5.14.1.4 `void serialize_client_server_hello (handshake_hello * hello, unsigned char ** stream, uint32_t * streamLen, channel_mode mode)`

Definition at line 37 of file `ServerClientHello.c`.

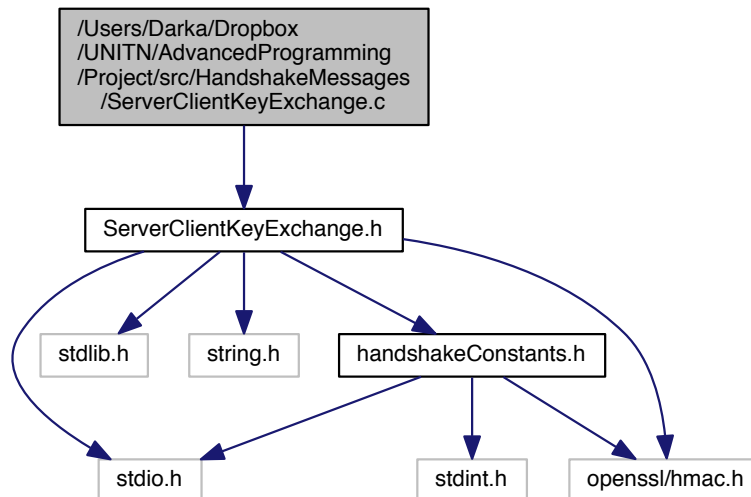
Here is the caller graph for this function:



5.15 /Users/Darka/Dropbox/UNITN/AdvancedProgramming/Project/src/HandshakeMessages/ServerClientKeyExchange.c File Reference

```
#include "ServerClientKeyExchange.h"
```

Include dependency graph for ServerClientKeyExchange.c:



Functions

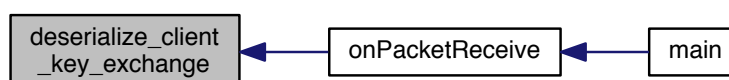
- void **serialize_server_key_exchange** (void *server_key_exchange, unsigned char **stream, uint32_t *streamLen, **key_exchange_algorithm** kx)
- void * **deserialize_server_key_exchange** (uint32_t message_len, unsigned char *message, **key_exchange_algorithm** kx)
- void **serialize_client_key_exchange** (**client_key_exchange** *client_key_exchange, unsigned char **stream, uint32_t *streamLen)
- void * **deserialize_client_key_exchange** (uint32_t message_len, unsigned char *message)
- void **free_server_key_exchange** (void *server_key_ex, **cipher_suite_t** cipher_suite)

5.15.1 Function Documentation

5.15.1.1 void* **deserialize_client_key_exchange** (uint32_t *message_len*, unsigned char * *message*)

Definition at line 185 of file `ServerClientKeyExchange.c`.

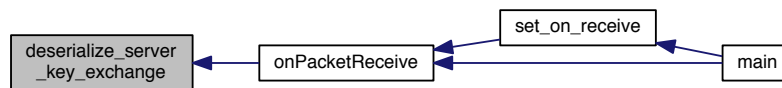
Here is the caller graph for this function:



5.15.1.2 `void* deserialize_server_key_exchange (uint32_t message_len, unsigned char * message, key_exchange_algorithm kx)`

Definition at line 104 of file ServerClientKeyExchange.c.

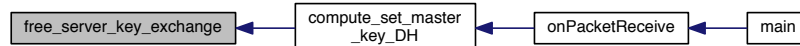
Here is the caller graph for this function:



5.15.1.3 `void free_server_key_exchange (void * server_key_ex, cipher_suite_t cipher_suite)`

Definition at line 199 of file ServerClientKeyExchange.c.

Here is the caller graph for this function:



5.15.1.4 `void serialize_client_key_exchange (client_key_exchange * client_key_exchange, unsigned char ** stream, uint32_t * streamLen)`

Definition at line 171 of file ServerClientKeyExchange.c.

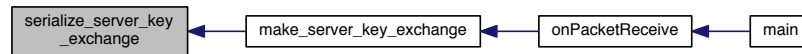
Here is the caller graph for this function:



5.15.1.5 void `serialize_server_key_exchange` (void * *server_key_exchange*, unsigned char ** *stream*, uint32_t * *streamLen*, key_exchange_algorithm *kx*)

Definition at line 15 of file `ServerClientKeyExchange.c`.

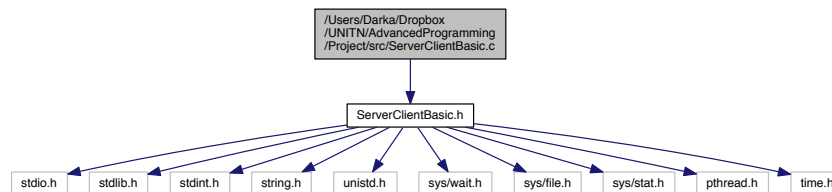
Here is the caller graph for this function:



5.16 /Users/Darka/Dropbox/UNITN/AdvancedProgramming/Project/src/ServerClientBasic.c File Reference

```
#include "ServerClientBasic.h"
```

Include dependency graph for `ServerClientBasic.c`:



Functions

- void **free_packet** (**packet_basic** *p)
- long long **get_file_size** (int fd)
- uint32_t **read_all_file** (int fd, unsigned char **p)
- **packet_basic** * **deserialize_packet** (unsigned char *str, uint32_t fileLen)
- void **serialize_packet** (**packet_basic** *p, unsigned char **str, uint32_t *strLen)
- **channel** * **create_channel** (char *fileName, char *channelFrom, char *channelTo, **mode** channelMode)
- int **set_on_receive** (**channel** *ch, void(***onPacketReceive**)(**channel** *ch, **packet_basic** *p))
- int **send_packet** (**channel** *ch, **packet_basic** *p)
- void **reader** (void *data)
- int **start_listener** (**channel** *ch)
- void **stop_channel** (**channel** *ch)
- void **wait_channel** (**channel** *ch)
- **packet_basic** * **create_packet** (char *from, char *to, unsigned char *message, uint32_t messageLen)

5.16.1 Function Documentation

5.16.1.1 `channel* create_channel (char * fileName, char * channelFrom, char * channelTo, mode channelMode)`

Definition at line 19 of file ServerClientBasic.c.

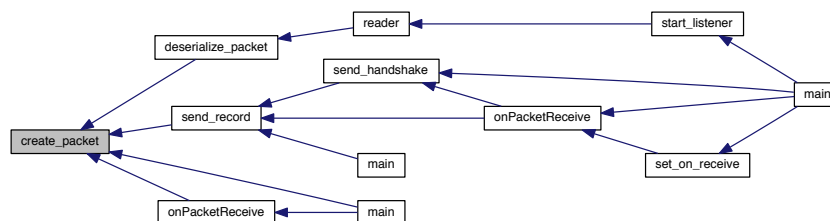
Here is the caller graph for this function:



5.16.1.2 `packet_basic* create_packet (char * from, char * to, unsigned char * message, uint32_t messageLen)`

Definition at line 131 of file ServerClientBasic.c.

Here is the caller graph for this function:



5.16.1.3 `packet_basic * deserialize_packet (unsigned char * str, uint32_t fileLen)`

Definition at line 205 of file ServerClientBasic.c.

Here is the call graph for this function:



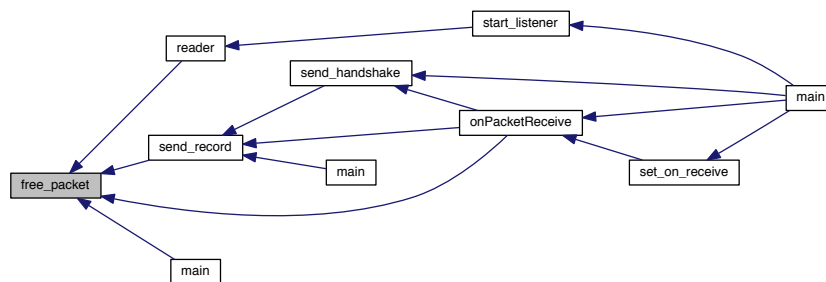
Here is the caller graph for this function:



5.16.1.4 void free_packet (packet_basic * p)

Definition at line 152 of file ServerClientBasic.c.

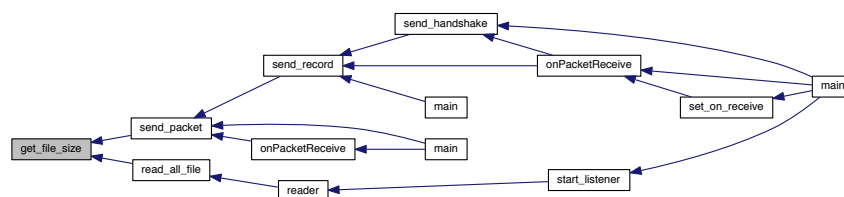
Here is the caller graph for this function:



5.16.1.5 long long get_file_size (int fd)

Definition at line 169 of file ServerClientBasic.c.

Here is the caller graph for this function:



5.16.1.6 `uint32_t read_all_file (int fd, unsigned char ** p)`

Definition at line 184 of file ServerClientBasic.c.

Here is the call graph for this function:



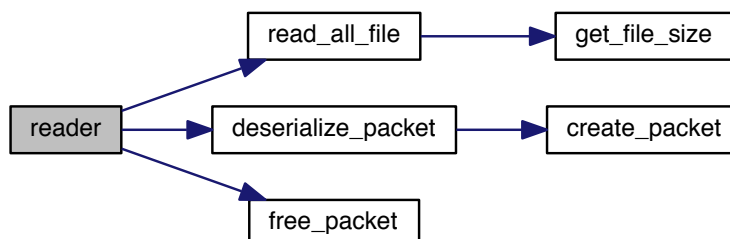
Here is the caller graph for this function:



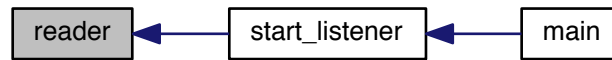
5.16.1.7 `void reader (void * data)`

Definition at line 77 of file ServerClientBasic.c.

Here is the call graph for this function:



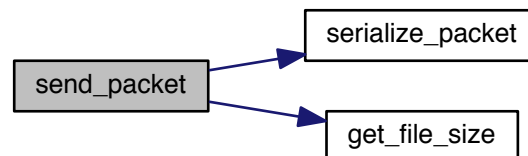
Here is the caller graph for this function:



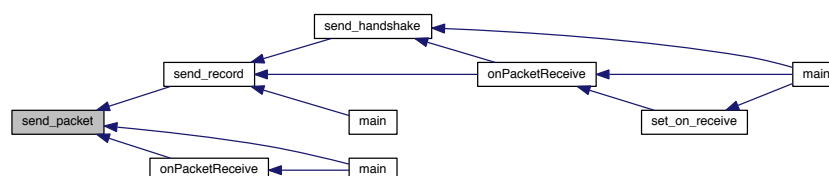
5.16.1.8 `int send_packet (channel * ch, packet_basic * p)`

Definition at line 41 of file `ServerClientBasic.c`.

Here is the call graph for this function:



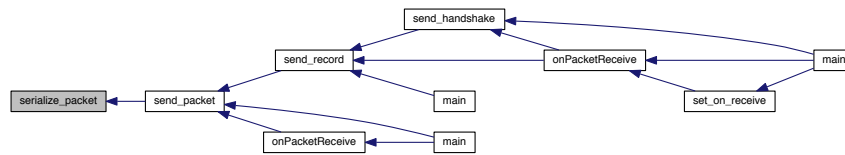
Here is the caller graph for this function:



5.16.1.9 `void serialize_packet (packet_basic * p, unsigned char ** str, uint32_t * strLen)`

Definition at line 241 of file `ServerClientBasic.c`.

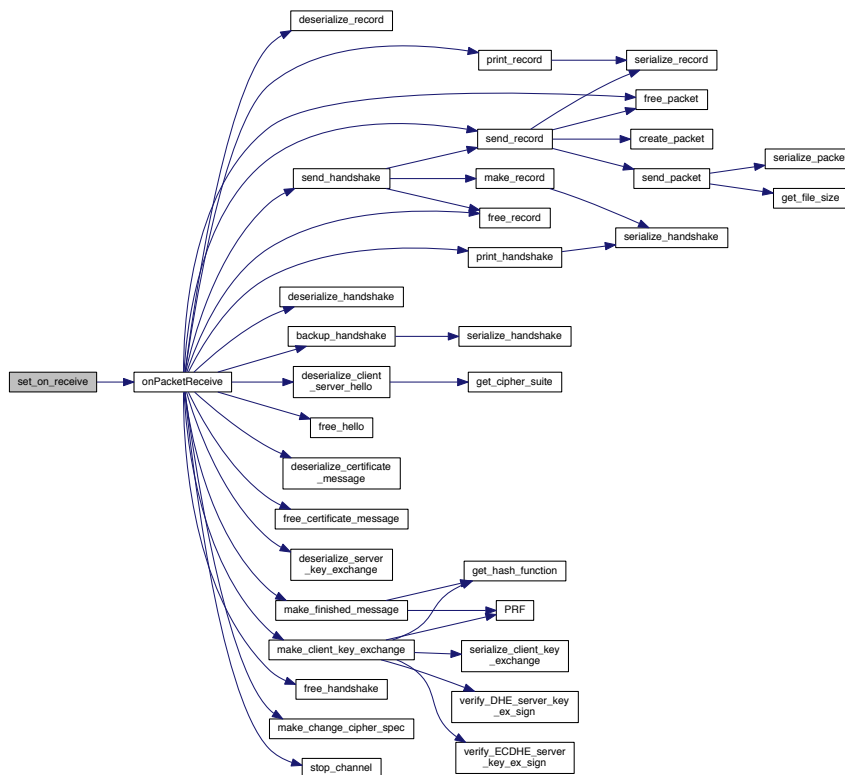
Here is the caller graph for this function:



5.16.1.10 `int set_on_receive (channel * ch, void(*) (channel *ch, packet_basic *p) onPacketReceive)`

Definition at line 32 of file ServerClientBasic.c.

Here is the call graph for this function:



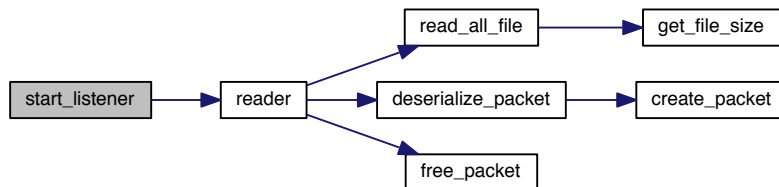
Here is the caller graph for this function:



5.16.1.11 int start_listener (channel * ch)

Definition at line 103 of file ServerClientBasic.c.

Here is the call graph for this function:



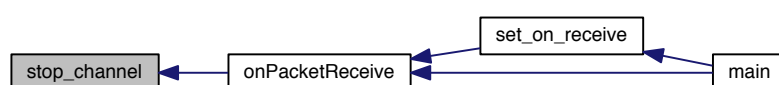
Here is the caller graph for this function:



5.16.1.12 void stop_channel (channel * ch)

Definition at line 121 of file ServerClientBasic.c.

Here is the caller graph for this function:



5.16.1.13 void wait_channel (channel * ch)

Definition at line 127 of file ServerClientBasic.c.

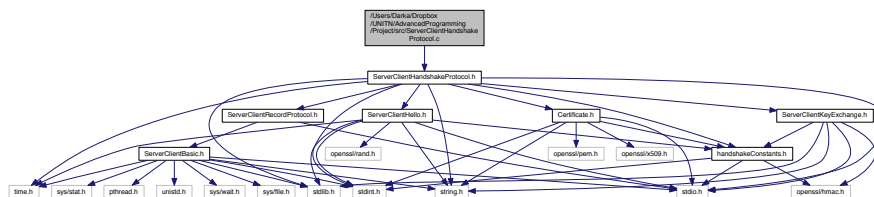
Here is the caller graph for this function:



5.17 /Users/Darka/Dropbox/UNITN/AdvancedProgramming/Project/src/ServerClientHandshakeProtocol.c File Reference

```
#include "ServerClientHandshakeProtocol.h"
```

Include dependency graph for ServerClientHandshakeProtocol.c:



Functions

- **record * make_record** (handshake *h)
- **int send_handshake** (channel *ch, handshake *h)
- **void serialize_handshake** (handshake *h, unsigned char **stream, uint32_t *streamLen)
- **handshake * deserialize_handshake** (unsigned char *message, uint32_t messageLen)
- **void free_handshake** (handshake *h)
- **void print_handshake** (handshake *h)

5.17.1 Function Documentation

5.17.1.1 handshake* deserialize_handshake (unsigned char * message, uint32_t messageLen)

Definition at line 50 of file ServerClientHandshakeProtocol.c.

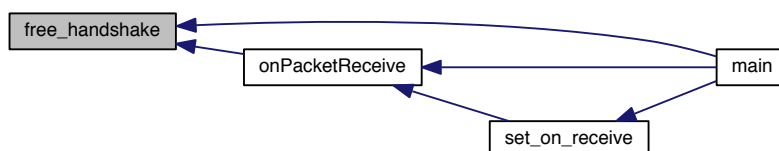
Here is the caller graph for this function:



5.17.1.2 void free_handshake (handshake * h)

Definition at line 66 of file ServerClientHandshakeProtocol.c.

Here is the caller graph for this function:



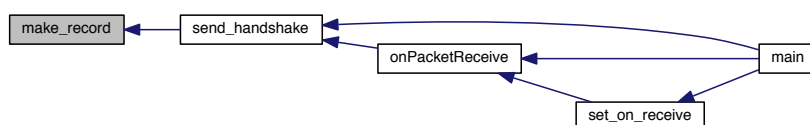
5.17.1.3 record* make_record (handshake * h)

Definition at line 11 of file ServerClientHandshakeProtocol.c.

Here is the call graph for this function:



Here is the caller graph for this function:



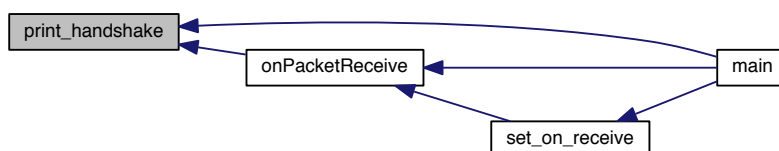
5.17.1.4 void print_handshake (handshake * h)

Definition at line 73 of file ServerClientHandshakeProtocol.c.

Here is the call graph for this function:



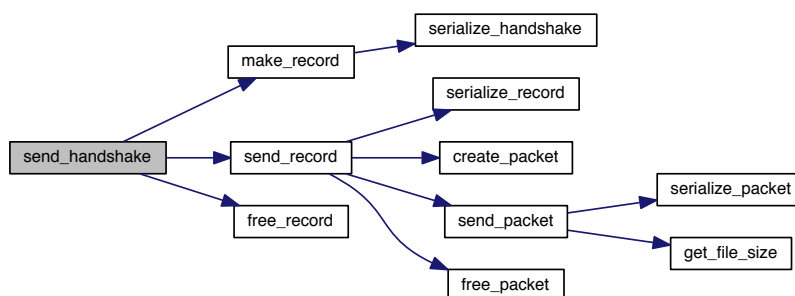
Here is the caller graph for this function:



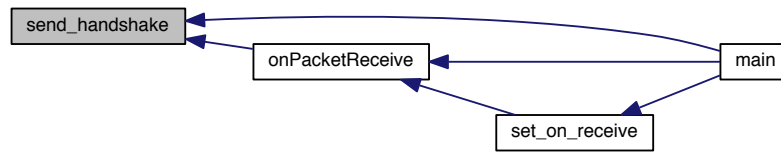
5.17.1.5 int send_handshake (channel * ch, handshake * h)

Definition at line 25 of file ServerClientHandshakeProtocol.c.

Here is the call graph for this function:



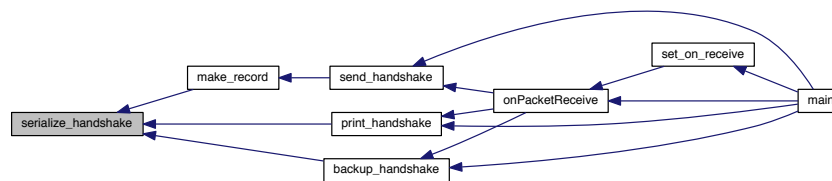
Here is the caller graph for this function:



5.17.1.6 `void serialize_handshake (handshake * h, unsigned char ** stream, uint32_t * streamLen)`

Definition at line 35 of file `ServerClientHandshakeProtocol.c`.

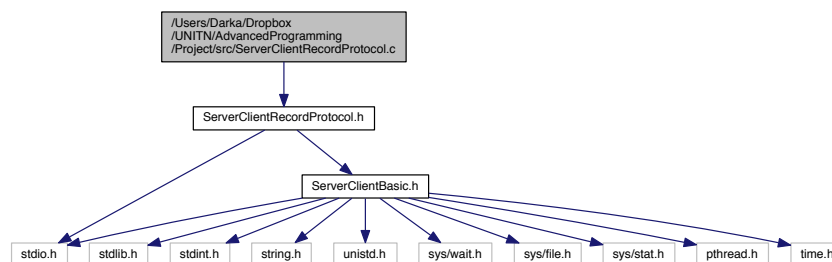
Here is the caller graph for this function:



5.18 /Users/Darka/Dropbox/UNITN/AdvancedProgramming/Project/src/ServerClientRecordProtocol.c File Reference

```
#include "ServerClientRecordProtocol.h"
```

Include dependency graph for `ServerClientRecordProtocol.c`:



Functions

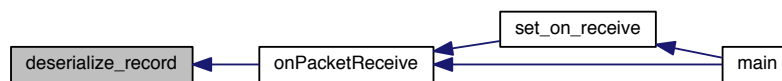
- void **serialize_record** (**record** *r, unsigned char **message, uint16_t *messageLen)
Serialize record in a byte stream message and message length are used for return.
- **record** * **deserialize_record** (unsigned char *message, uint32_t messageLen)
- int **send_record** (**channel** *ch, **record** *r)
- void **print_record** (**record** *r)
- void **free_record** (**record** *r)

5.18.1 Function Documentation

5.18.1.1 **record*** deserialize_record (unsigned char * message, uint32_t messageLen)

Definition at line 22 of file ServerClientRecordProtocol.c.

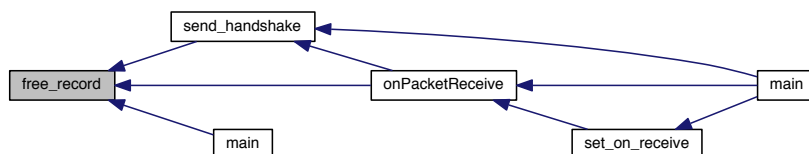
Here is the caller graph for this function:



5.18.1.2 void free_record (record * r)

Definition at line 68 of file ServerClientRecordProtocol.c.

Here is the caller graph for this function:



5.18.1.3 void print_record (record * r)

Definition at line 48 of file ServerClientRecordProtocol.c.

Here is the call graph for this function:



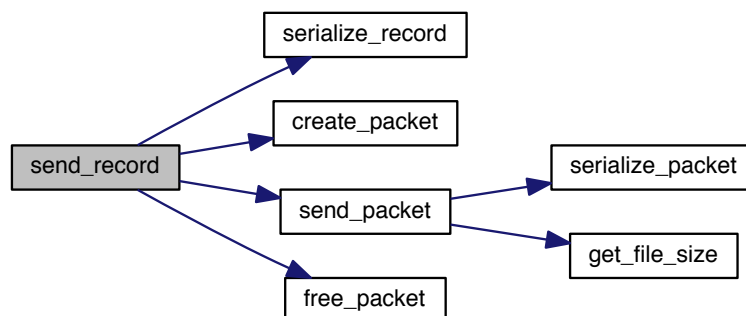
Here is the caller graph for this function:



5.18.1.4 int send_record (channel * ch, record * r)

Definition at line 36 of file ServerClientRecordProtocol.c.

Here is the call graph for this function:



Functions

- void **onPacketReceive** (channel *ch, packet_basic *p)
- void **print_master_secret** ()
- void **print_random** ()
- int **main** ()

Variables

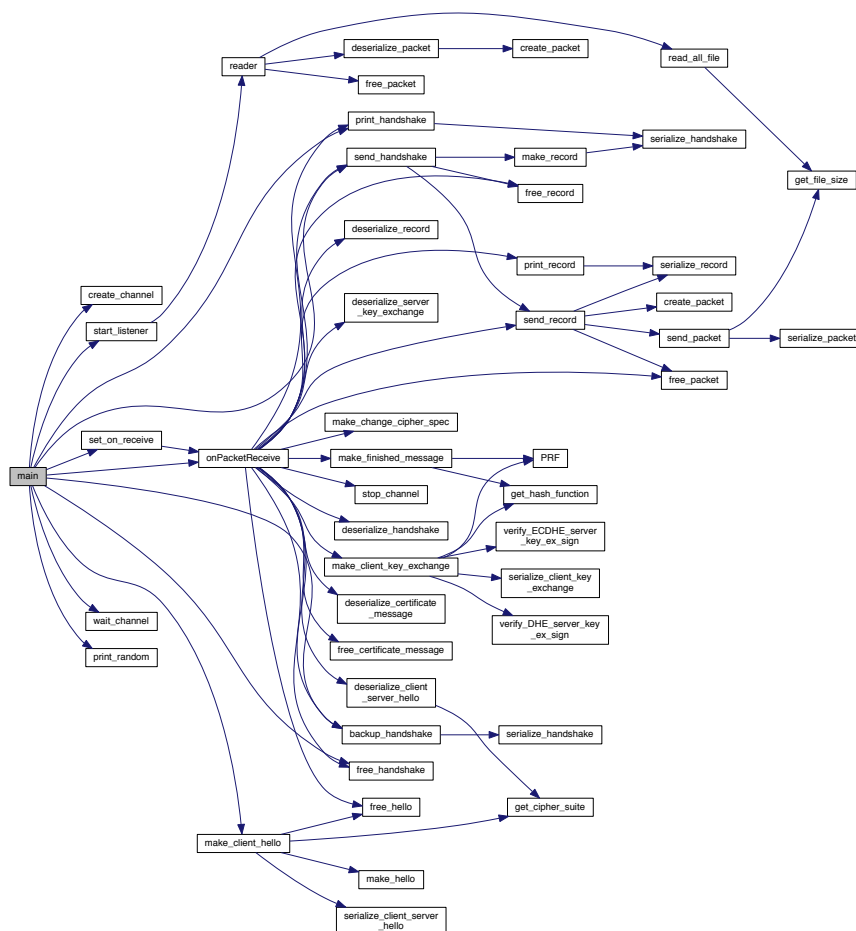
- TLS_parameters TLS_param

5.19.1 Function Documentation

5.19.1.1 int main ()

Definition at line 19 of file client.c.

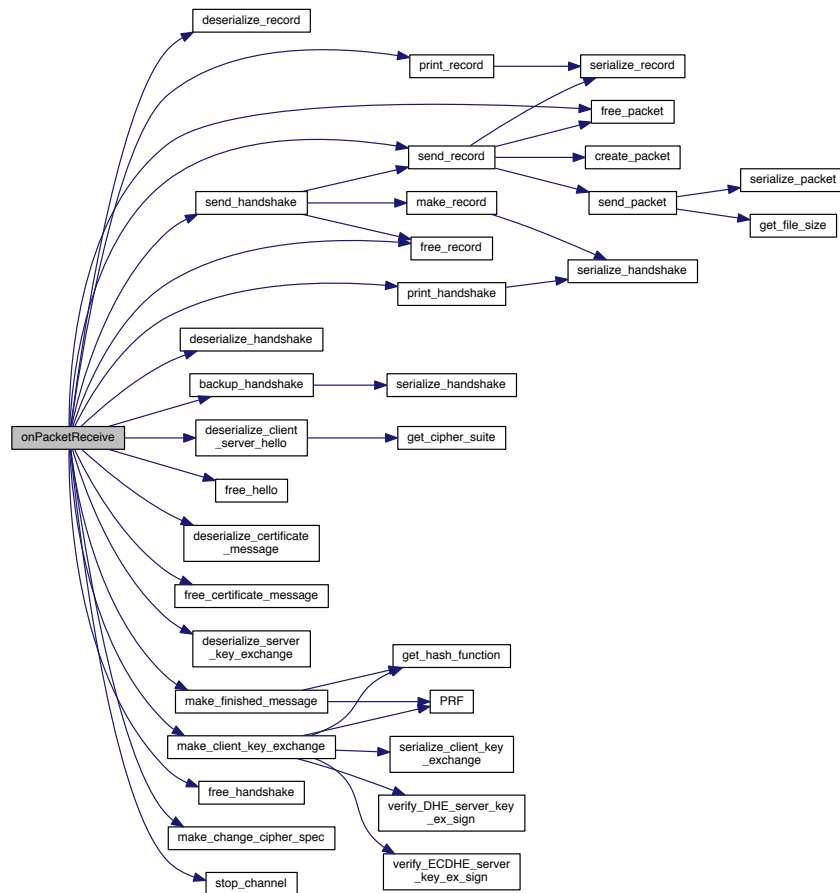
Here is the call graph for this function:



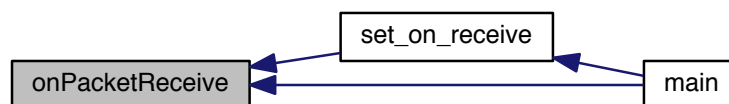
5.19.1.2 void onPacketReceive (channel * ch, packet_basic * p)

Definition at line 69 of file client.c.

Here is the call graph for this function:



Here is the caller graph for this function:



5.19.1.3 void print_master_secret ()

Definition at line 184 of file client.c.

5.19.1.4 void print_random ()

Definition at line 191 of file client.c.

Here is the caller graph for this function:



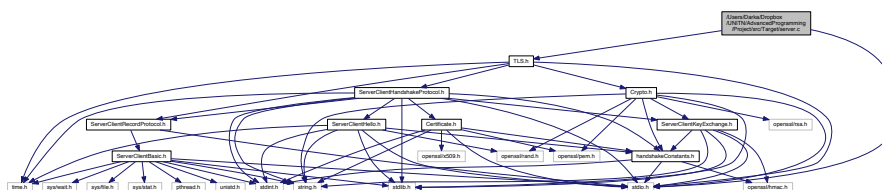
5.19.2 Variable Documentation

5.19.2.1 TLS_parameters TLS_param

Definition at line 17 of file client.c.

5.20 /Users/Darka/Dropbox/UNITN/AdvancedProgramming/Project/src/Target/server.c
File Reference

```
#include <stdio.h>
#include "TLS.h"
Include dependency graph for server.c:
```



Functions

- void **print_random** ()
- void **print_master_secret** ()
- void **compute_set_master_key_RSA** (client_key_exchange *client_key_exchange)
- void **compute_set_master_key_DH** (client_key_exchange *client_public)
- void **compute_set_master_key_ECDHE** (client_key_exchange *client_public)
- void **onPacketReceive** (channel *server2client, packet_basic *p)
- int **main** ()

Variables

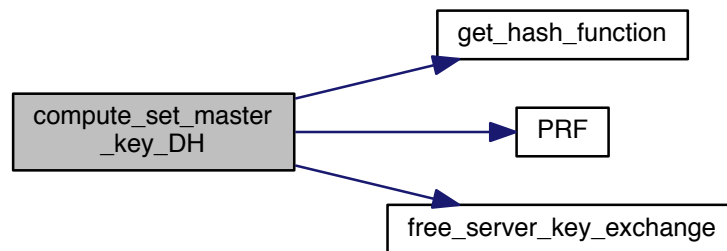
- `TLS_parameters TLS_param`

5.20.1 Function Documentation

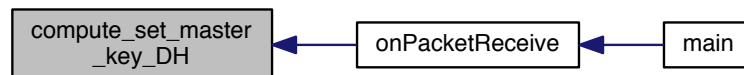
5.20.1.1 `void compute_set_master_key_DH (client_key_exchange * cliet_public)`

Definition at line 250 of file server.c.

Here is the call graph for this function:



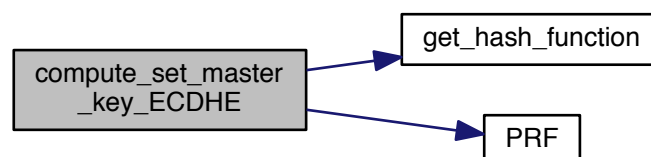
Here is the caller graph for this function:



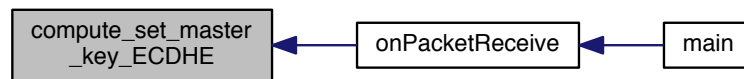
5.20.1.2 `void compute_set_master_key_ECDHE (client_key_exchange * cliet_public)`

Definition at line 279 of file server.c.

Here is the call graph for this function:



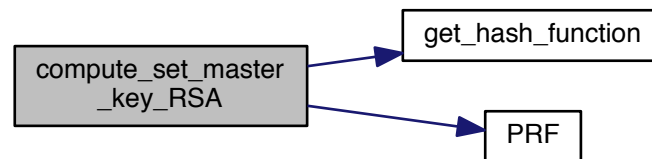
Here is the caller graph for this function:



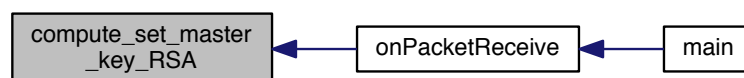
5.20.1.3 void compute_set_master_key_RSA (client_key_exchange * client_key_exchange)

Definition at line 213 of file server.c.

Here is the call graph for this function:



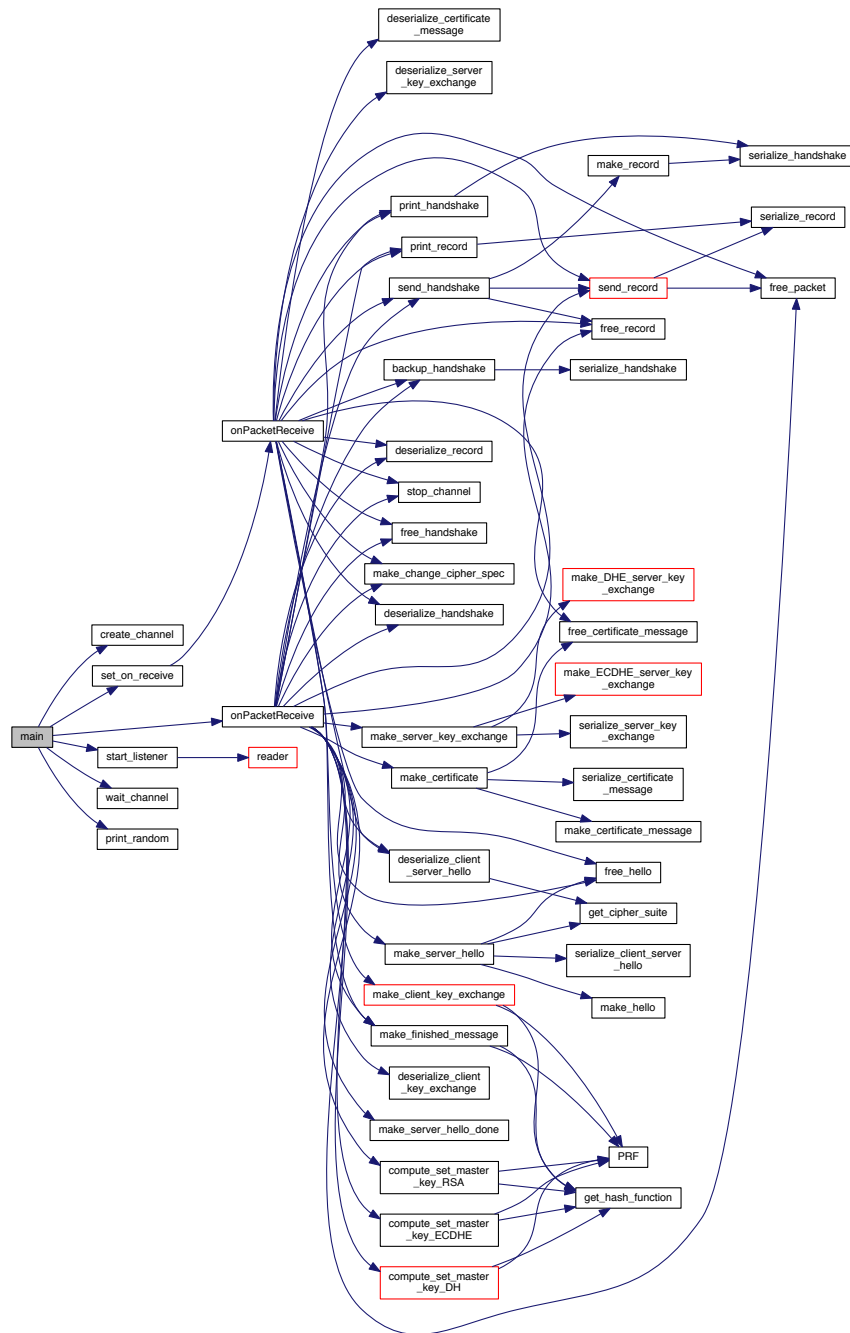
Here is the caller graph for this function:



5.20.1.4 int main ()

Definition at line 21 of file server.c.

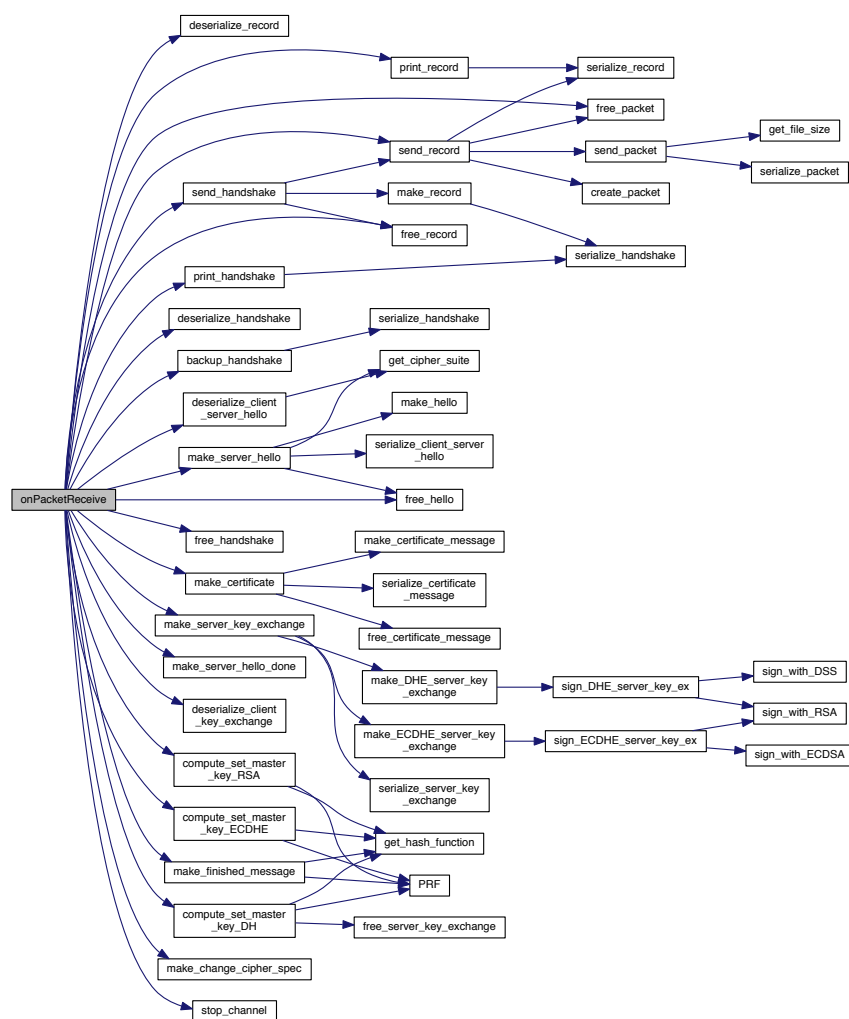
Here is the call graph for this function:



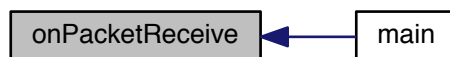
5.20.1.5 void onPacketReceive (channel * server2client, packet_basic * p)

Definition at line 58 of file server.c.

Here is the call graph for this function:



Here is the caller graph for this function:



5.20.1.6 void print_master_secret ()

Definition at line 205 of file server.c.

5.21.1 Function Documentation

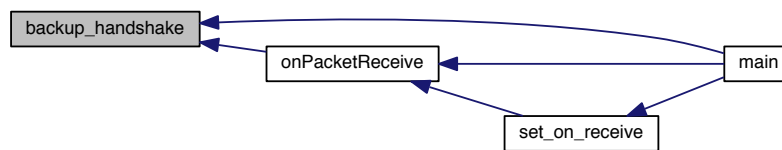
5.21.1.1 void backup_handshake (TLS_parameters * TLS_param, handshake * h)

Definition at line 13 of file TLSCClient.c.

Here is the call graph for this function:



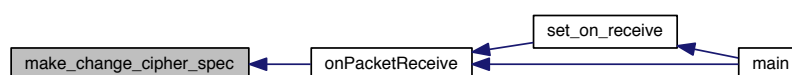
Here is the caller graph for this function:



5.21.1.2 record* make_change_cipher_spec ()

Definition at line 250 of file TLSCClient.c.

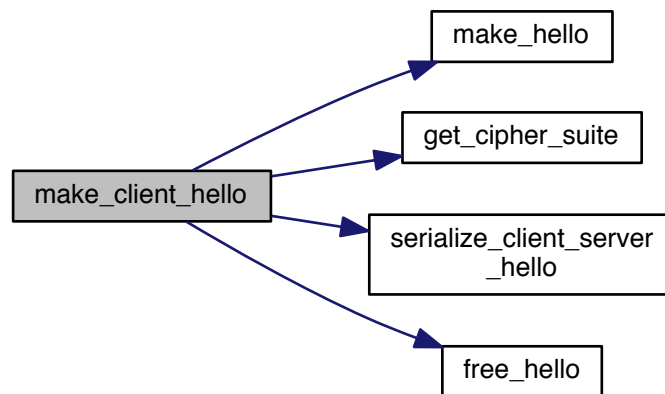
Here is the caller graph for this function:



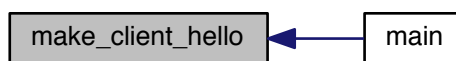
5.21.1.3 handshake* make_client_hello (unsigned char * client_random)

Definition at line 31 of file TLSClient.c.

Here is the call graph for this function:



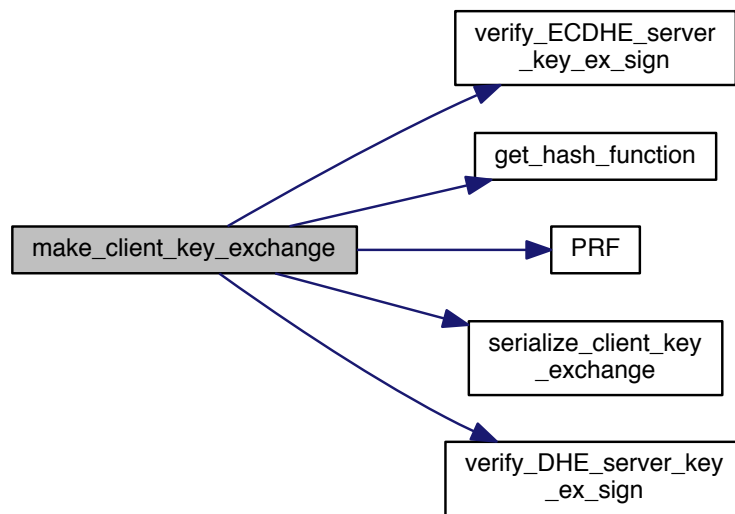
Here is the caller graph for this function:



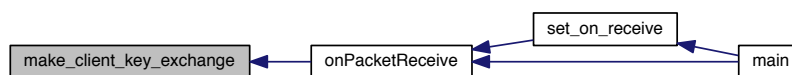
5.21.1.4 handshake* make_client_key_exchange (TLS_parameters * TLS_param, uint16_t key_ex_alg)

Definition at line 65 of file TLSClient.c.

Here is the call graph for this function:



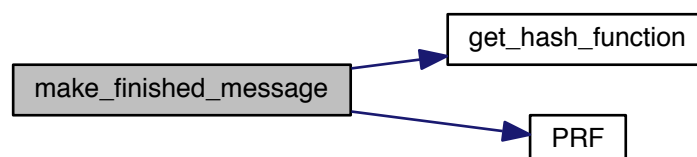
Here is the caller graph for this function:



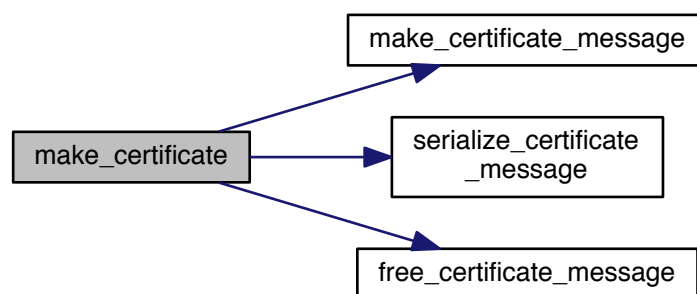
5.21.1.5 handshake* make_finished_message (TLS_parameters * TLS_param)

Definition at line 262 of file TLSClient.c.

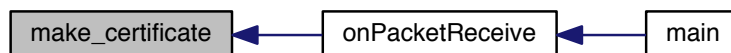
Here is the call graph for this function:



Here is the call graph for this function:



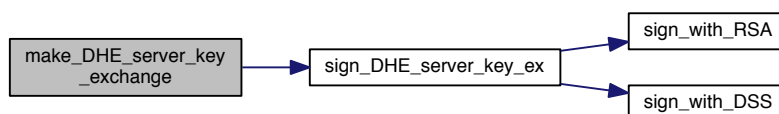
Here is the caller graph for this function:



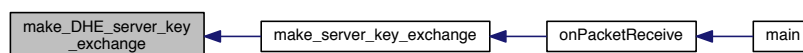
5.22.1.2 DHE_server_key_exchange* make_DHE_server_key_exchange (TLS_parameters * TLS_param)

Definition at line 113 of file TLSServer.c.

Here is the call graph for this function:



Here is the caller graph for this function:



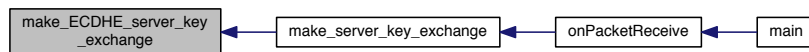
5.22.1.3 ECDHE_server_key_exchange* make_ECDHE_server_key_exchange (TLS_parameters * TLS_param)

Definition at line 153 of file TLSServer.c.

Here is the call graph for this function:



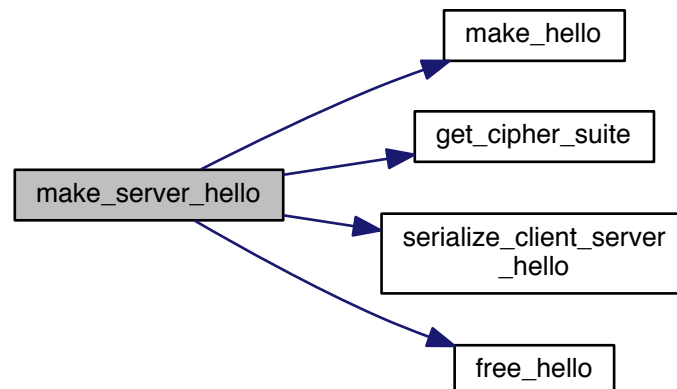
Here is the caller graph for this function:



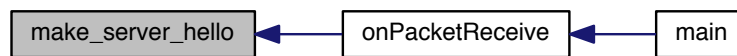
5.22.1.4 handshake* make_server_hello (TLS_parameters * TLS_param, handshake_hello * client_hello)

Definition at line 11 of file TLSServer.c.

Here is the call graph for this function:



Here is the caller graph for this function:



5.22.1.5 handshake* make_server_hello_done ()

Definition at line 188 of file `TLS_Server.c`.

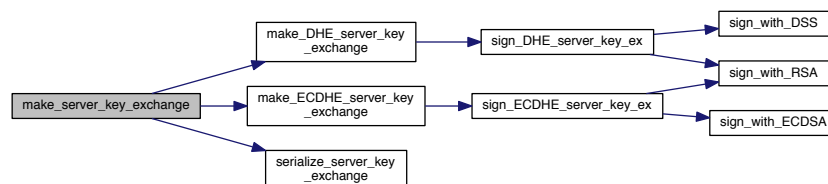
Here is the caller graph for this function:



5.22.1.6 handshake* make_server_key_exchange (TLS_parameters * TLS_param)

Definition at line 84 of file `TLS_Server.c`.

Here is the call graph for this function:



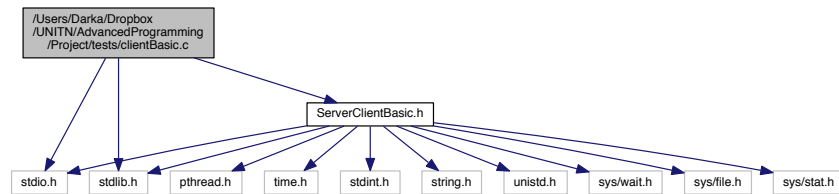
Here is the caller graph for this function:



5.23 /Users/Darka/Dropbox/UNITN/AdvancedProgramming/Project/tests/clientBasic.c

File Reference

```
#include <stdio.h>
#include <stdlib.h>
#include "ServerClientBasic.h"
Include dependency graph for clientBasic.c:
```



Functions

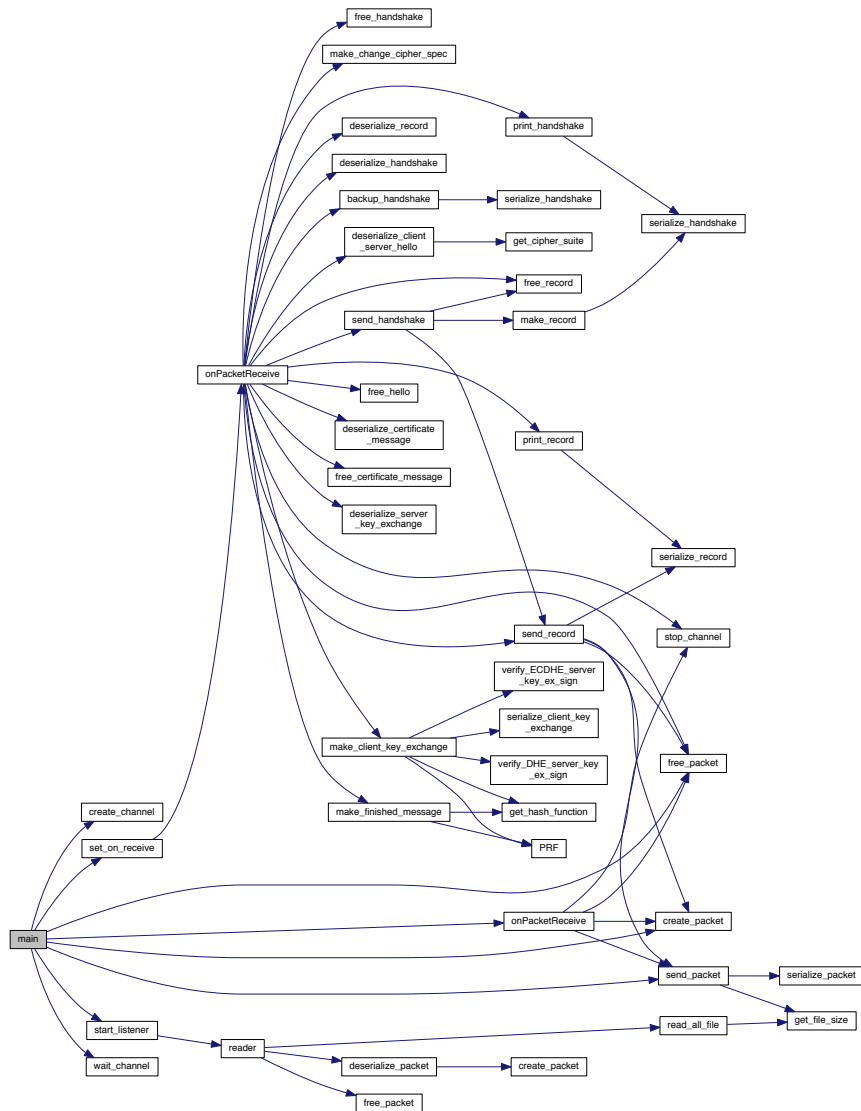
- void **onPacketReceive** (channel *ch, packet_basic *p)
- int **main** (int argc, char **argv)

5.23.1 Function Documentation

5.23.1.1 int main (int argc, char ** argv)

Definition at line 16 of file `clientBasic.c`.

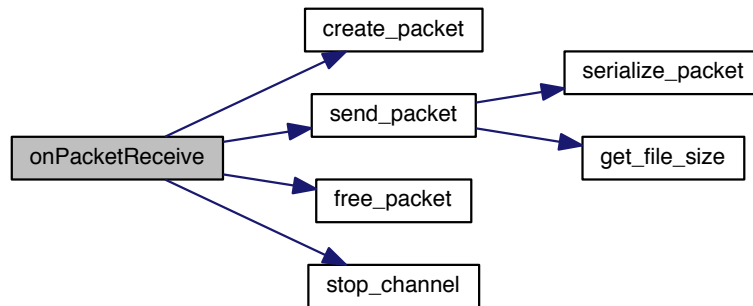
Here is the call graph for this function:



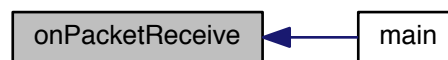
5.23.1.2 void onPacketReceive (channel * *ch*, packet_basic * *p*)

Definition at line 38 of file clientBasic.c.

Here is the call graph for this function:

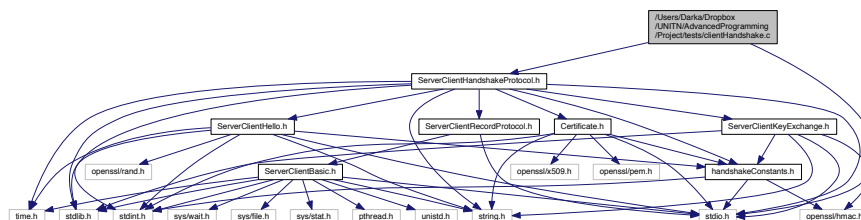


Here is the caller graph for this function:



5.24 /Users/Darka/Dropbox/UNITN/AdvancedProgramming/Project/tests/clientHandshake.c File Reference

```
#include <stdio.h>
#include "ServerClientHandshakeProtocol.h"
Include dependency graph for clientHandshake.c:
```



Functions

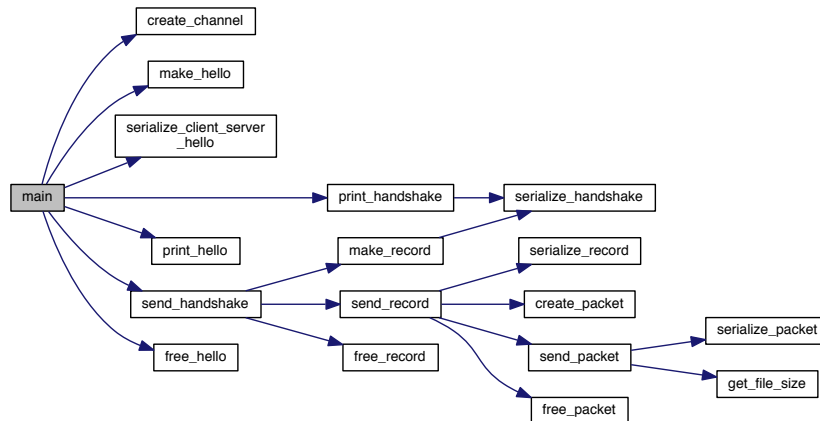
- `int main ()`

5.24.1 Function Documentation

5.24.1.1 int main ()

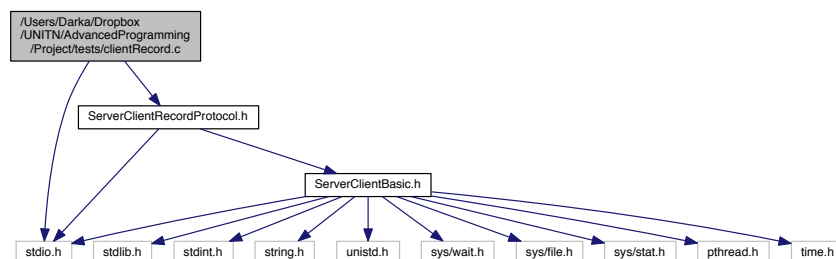
Definition at line 12 of file clientHandshake.c.

Here is the call graph for this function:



5.25 /Users/Darka/Dropbox/UNITN/AdvancedProgramming/Project/tests/clientRecord.c File Reference

```
#include <stdio.h>
#include "ServerClientRecordProtocol.h"
Include dependency graph for clientRecord.c:
```



Functions

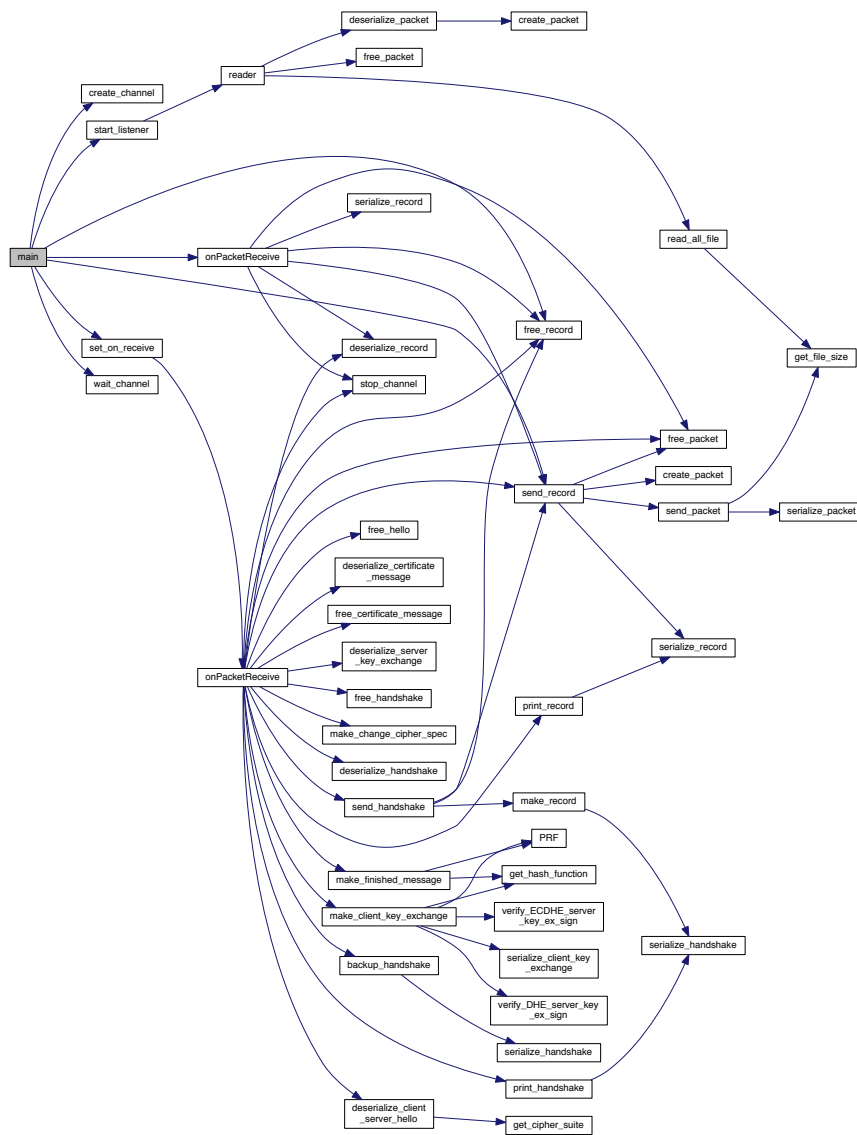
- void **onPacketReceive** (channel *ch, packet_basic *p)
- int **main** (int argc, const char *argv[])

5.25.1 Function Documentation

5.25.1.1 `int main (int argc, const char * argv[])`

Definition at line 15 of file clientRecord.c.

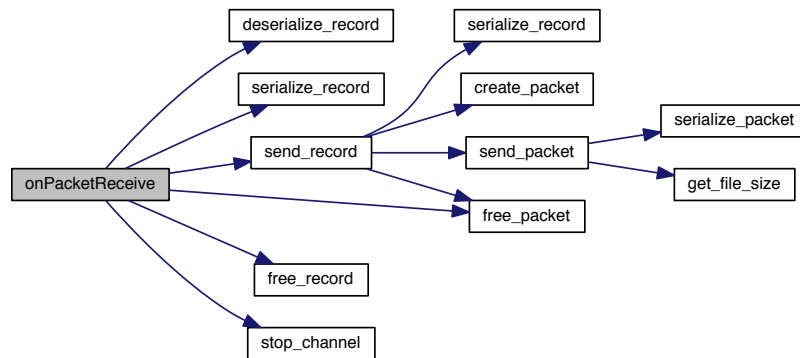
Here is the call graph for this function:



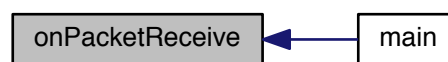
5.25.1.2 `void onPacketReceive (channel * ch, packet_basic * p)`

Definition at line 40 of file clientRecord.c.

Here is the call graph for this function:

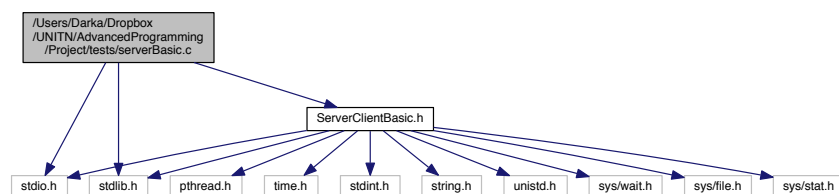


Here is the caller graph for this function:



5.26 /Users/Darka/Dropbox/UNITN/AdvancedProgramming/Project/tests/serverBasic.c File Reference

```
#include <stdio.h>
#include <stdlib.h>
#include "ServerClientBasic.h"
Include dependency graph for serverBasic.c:
```



Functions

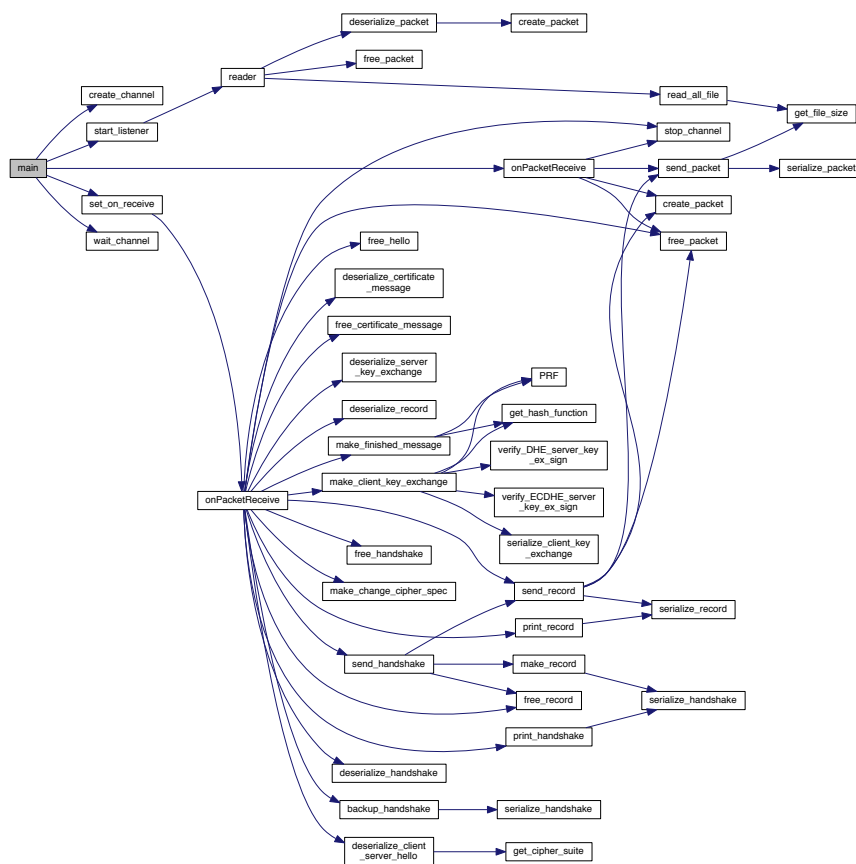
- void **onPacketReceive** (`channel *ch`, `packet_basic *p`)
- int **main** (`int argc`, `char **argv`)

5.26.1 Function Documentation

5.26.1.1 `int main (int argc, char ** argv)`

Definition at line 16 of file `serverBasic.c`.

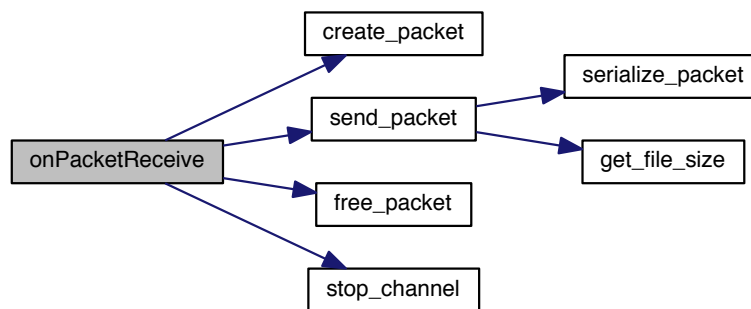
Here is the call graph for this function:



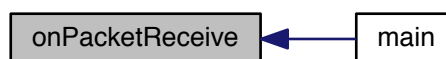
5.26.1.2 `void onPacketReceive (channel * ch, packet_basic * p)`

Definition at line 32 of file `serverBasic.c`.

Here is the call graph for this function:



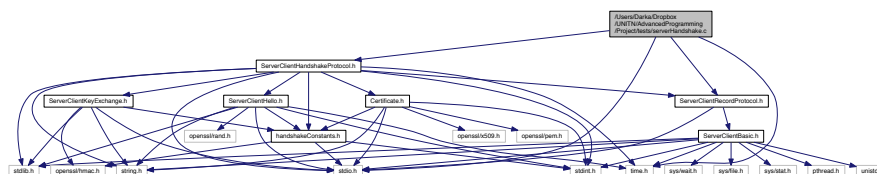
Here is the caller graph for this function:



5.27 /Users/Darka/Dropbox/UNITN/AdvancedProgramming/Project/tests/serverHandshake.c
File Reference

```
#include <stdio.h>
#include <time.h>
#include "ServerClientHandshakeProtocol.h"
#include "ServerClientRecordProtocol.h"
```

Include dependency graph for serverHandshake.c:



Functions

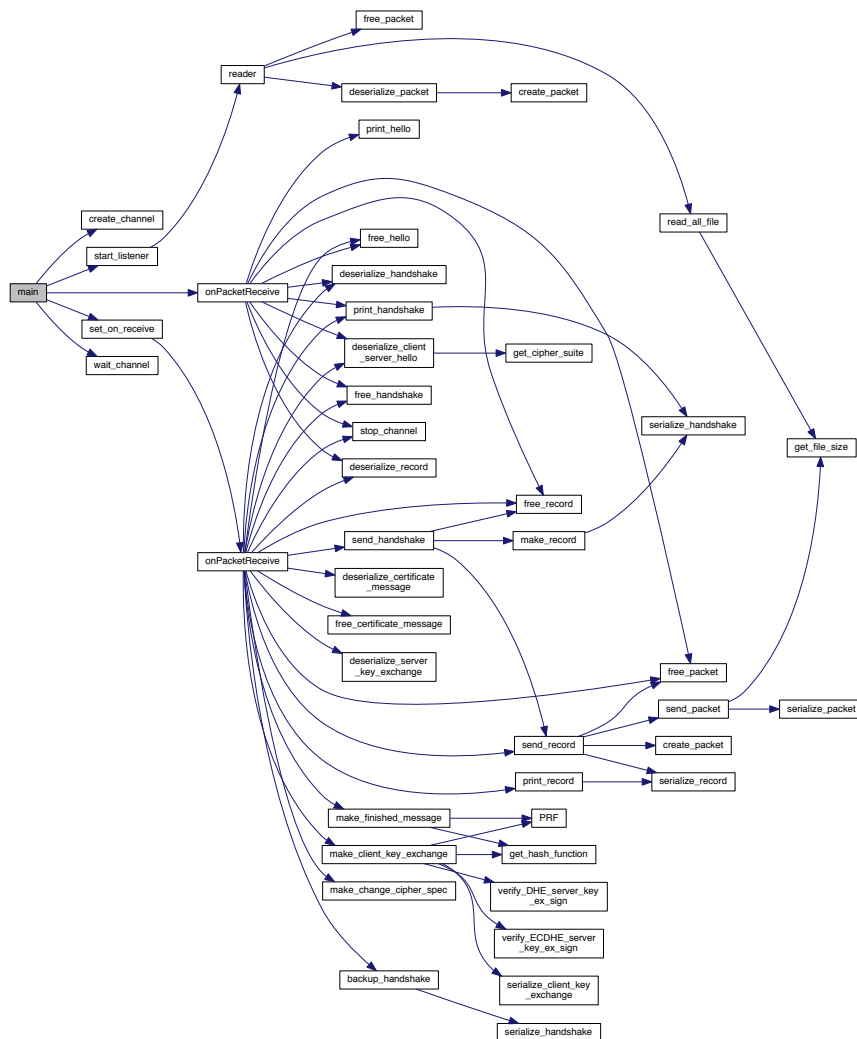
- void **onPacketReceive** (channel *ch, packet_basic *p)
- int **main** ()

5.27.1 Function Documentation

5.27.1.1 `int main ()`

Definition at line 18 of file `serverHandshake.c`.

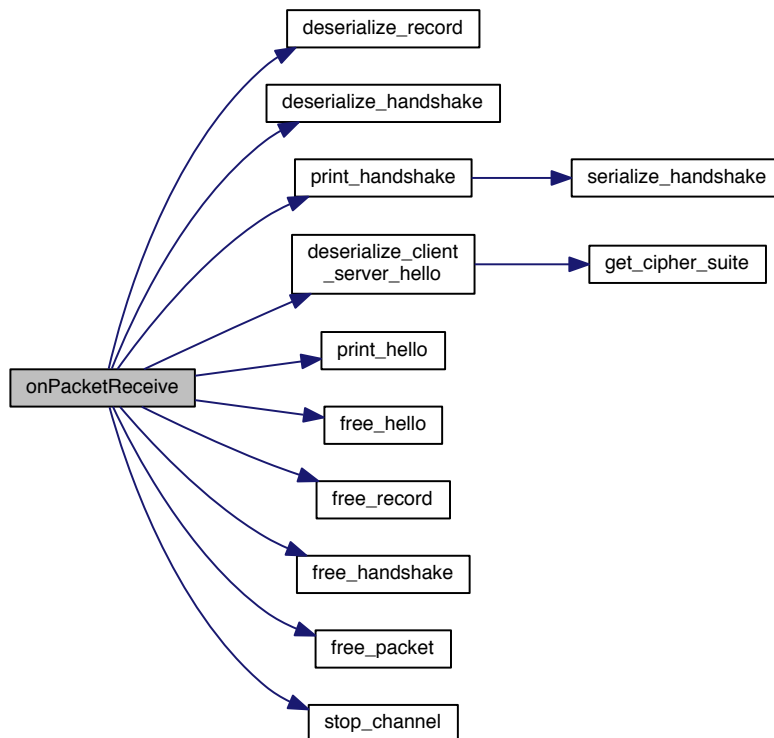
Here is the call graph for this function:



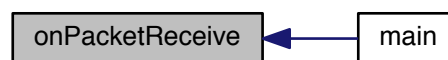
5.27.1.2 `void onPacketReceive (channel * ch, packet_basic * p)`

Definition at line 34 of file `serverHandshake.c`.

Here is the call graph for this function:



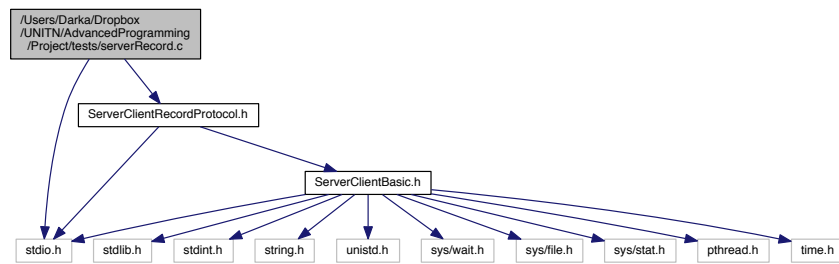
Here is the caller graph for this function:



5.28 /Users/Darka/Dropbox/UNITN/AdvancedProgramming/Project/tests/serverRecord.c File Reference

```
#include <stdio.h>
#include "ServerClientRecordProtocol.h"
```

Include dependency graph for serverRecord.c:



Functions

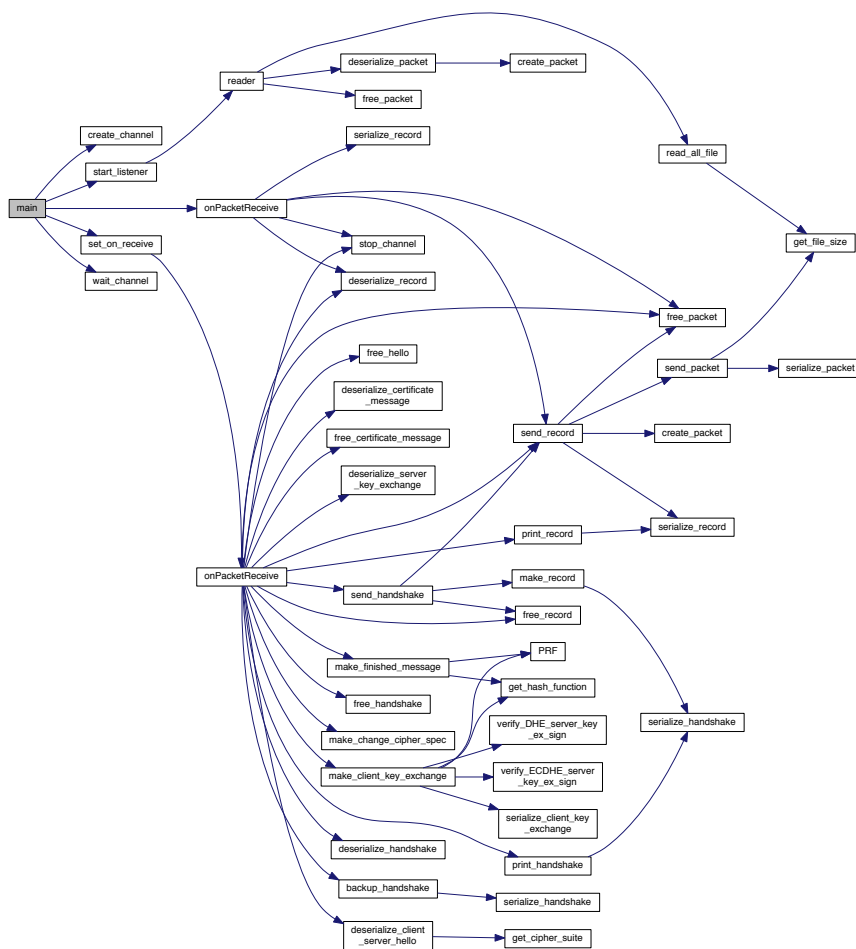
- void **onPacketReceive** (channel *ch, packet_basic *p)
- int **main** (int argc, const char *argv[])

5.28.1 Function Documentation

5.28.1.1 int main (int argc, const char * argv[])

Definition at line 15 of file serverRecord.c.

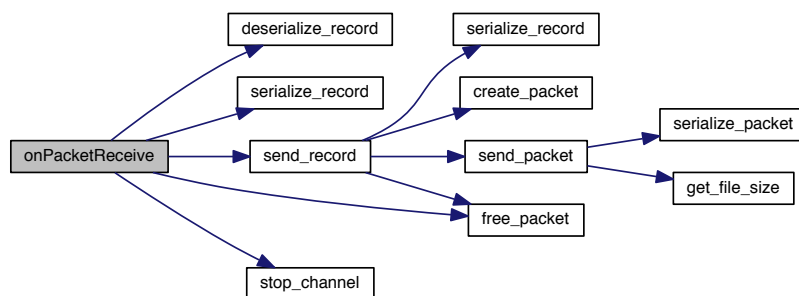
Here is the call graph for this function:



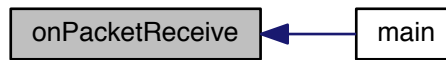
5.28.1.2 void onPacketReceive (channel * ch, packet_basic * p)

Definition at line 33 of file serverRecord.c.

Here is the call graph for this function:



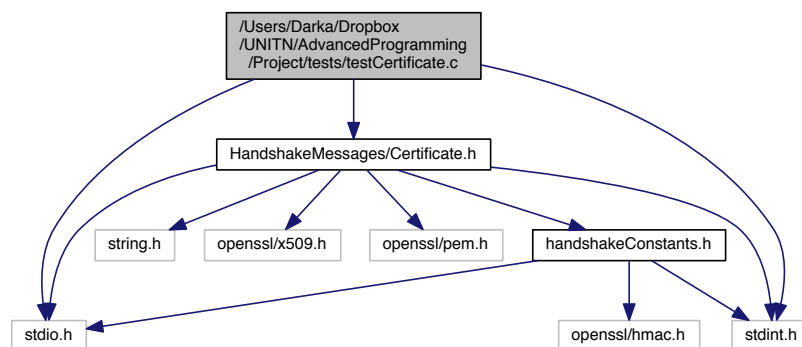
Here is the caller graph for this function:



5.29 /Users/Darka/Dropbox/UNITN/AdvancedProgramming/Project/tests/testCertificate.c File Reference

```
#include <stdio.h>
#include <stdint.h>
#include "HandshakeMessages/Certificate.h"
```

Include dependency graph for testCertificate.c:



Functions

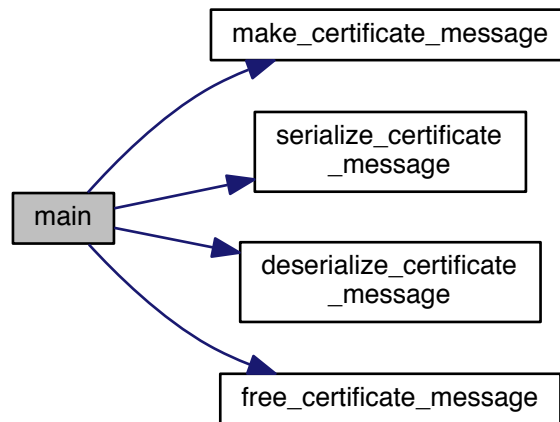
- `int main ()`

5.29.1 Function Documentation

5.29.1.1 `int main ()`

Definition at line 5 of file `testCertificate.c`.

Here is the call graph for this function:



5.30 /Users/Darka/Dropbox/UNITN/AdvancedProgramming/Project/TLSProject/Build/↵
Intermediates/TLSProject.build/Debug/StructTest.build/Objects-normal/x86_64/main.d
File Reference

5.31 /Users/Darka/Dropbox/UNITN/AdvancedProgramming/Project/TLSProject/xcode↵
Intermediates/TLSProject.build/Debug/StructTest.build/Objects-normal/x86_64/main.d
File Reference

5.32 /Users/Darka/Dropbox/UNITN/AdvancedProgramming/Project/TLSProject/Build/↵
Intermediates/TLSProject.build/Debug/TLSClient.build/Objects-normal/x86_64/↵
Certificate.d File Reference

5.33 /Users/Darka/Dropbox/UNITN/AdvancedProgramming/Project/TLSProject/Build/↵
Intermediates/TLSProject.build/Debug/TLSClient.build/Objects-normal/x86_64/↵
Certificate.d File Reference

5.34 /Users/Darka/Dropbox/UNITN/AdvancedProgramming/Project/TLSProject/xcode↵
Intermediates/TLSProject.build/Debug/TLSClient.build/Objects-normal/x86_64/↵
Certificate.d File Reference

- 5.35 `/Users/Darka/Dropbox/UNITN/AdvancedProgramming/Project/TLSProject/xcode↵
Intermediates/TLSProject.build/Debug/TLSServer.build/Objects-normal/x86_64/↵
Certificate.d` File Reference
- 5.36 `/Users/Darka/Dropbox/UNITN/AdvancedProgramming/Project/TLSProject/xcode↵
Intermediates/TLSProject.build/Release/TLSCient.build/Objects-normal/x86_64/↵
Certificate.d` File Reference
- 5.37 `/Users/Darka/Dropbox/UNITN/AdvancedProgramming/Project/TLSProject/xcode↵
Intermediates/TLSProject.build/Release/TLSServer.build/Objects-normal/x86_64/↵
Certificate.d` File Reference
- 5.38 `/Users/Darka/Dropbox/UNITN/AdvancedProgramming/Project/TLSProject/Build/↵
Intermediates/TLSProject.build/Debug/TLSCient.build/Objects-normal/x86_64/client.d`
File Reference
- 5.39 `/Users/Darka/Dropbox/UNITN/AdvancedProgramming/Project/TLSProject/xcode↵
Intermediates/TLSProject.build/Debug/TLSCient.build/Objects-normal/x86_64/client.d`
File Reference
- 5.40 `/Users/Darka/Dropbox/UNITN/AdvancedProgramming/Project/TLSProject/xcode↵
Intermediates/TLSProject.build/Release/TLSCient.build/Objects-normal/x86_↵
64/client.d` File Reference
- 5.41 `/Users/Darka/Dropbox/UNITN/AdvancedProgramming/Project/TLSProject/Build/↵
Intermediates/TLSProject.build/Debug/TLSCient.build/Objects-normal/x86_64/↵
Crypto.d` File Reference
- 5.42 `/Users/Darka/Dropbox/UNITN/AdvancedProgramming/Project/TLSProject/Build/↵
Intermediates/TLSProject.build/Debug/TLSServer.build/Objects-normal/x86_64/↵
Crypto.d` File Reference
- 5.43 `/Users/Darka/Dropbox/UNITN/AdvancedProgramming/Project/TLSProject/xcode↵
Intermediates/TLSProject.build/Debug/TLSCient.build/Objects-normal/x86_64/↵
Crypto.d` File Reference

5.44 /Users/Darka/Dropbox/UNITN/AdvancedProgramming/Project/TLSProject/xcodeIntermediates/TLSProject.build/Debug/TLSServer.build/Objects-normal/x86_64/Crypto.d File

Reference

117

5.44 /Users/Darka/Dropbox/UNITN/AdvancedProgramming/Project/TLSProject/xcodeIntermediates/TLSProject.build/Debug/TLSServer.build/Objects-normal/x86_64/Crypto.d File Reference

5.45 /Users/Darka/Dropbox/UNITN/AdvancedProgramming/Project/TLSProject/xcodeIntermediates/TLSProject.build/Release/TLSCClient.build/Objects-normal/x86_64/Crypto.d File Reference

5.46 /Users/Darka/Dropbox/UNITN/AdvancedProgramming/Project/TLSProject/xcodeIntermediates/TLSProject.build/Release/TLSServer.build/Objects-normal/x86_64/Crypto.d File Reference

5.47 /Users/Darka/Dropbox/UNITN/AdvancedProgramming/Project/TLSProject/Build/Intermediates/TLSProject.build/Debug/TLSCClient.build/Objects-normal/x86_64/handshakeConstants.d File Reference

5.48 /Users/Darka/Dropbox/UNITN/AdvancedProgramming/Project/TLSProject/Build/Intermediates/TLSProject.build/Debug/TLSServer.build/Objects-normal/x86_64/handshakeConstants.d File Reference

5.49 /Users/Darka/Dropbox/UNITN/AdvancedProgramming/Project/TLSProject/xcodeIntermediates/TLSProject.build/Debug/TLSCClient.build/Objects-normal/x86_64/handshakeConstants.d File Reference

5.50 /Users/Darka/Dropbox/UNITN/AdvancedProgramming/Project/TLSProject/xcodeIntermediates/TLSProject.build/Debug/TLSServer.build/Objects-normal/x86_64/handshakeConstants.d File Reference

5.51 /Users/Darka/Dropbox/UNITN/AdvancedProgramming/Project/TLSProject/xcodeIntermediates/TLSProject.build/Release/TLSCClient.build/Objects-normal/x86_64/handshakeConstants.d File Reference

5.52 /Users/Darka/Dropbox/UNITN/AdvancedProgramming/Project/TLSProject/xcodeIntermediates/TLSProject.build/Release/TLSServer.build/Objects-normal/x86_64/handshakeConstants.d File Reference

- 5.53 `/Users/Darka/Dropbox/UNITN/AdvancedProgramming/Project/TLSProject/Build/Intermediates/TLSProject.build/Debug/TLSClient.build/Objects-normal/x86_64/ServerClientBasic.d` File Reference
- 5.54 `/Users/Darka/Dropbox/UNITN/AdvancedProgramming/Project/TLSProject/Build/Intermediates/TLSProject.build/Debug/TLSClient.build/Objects-normal/x86_64/ServerClientBasic.d` File Reference
- 5.55 `/Users/Darka/Dropbox/UNITN/AdvancedProgramming/Project/TLSProject/Build/Intermediates/TLSProject.build/Debug/TLSClient.build/Objects-normal/x86_64/ServerClientBasic.d` File Reference
- 5.56 `/Users/Darka/Dropbox/UNITN/AdvancedProgramming/Project/TLSProject/Build/Intermediates/TLSProject.build/Debug/TLSClient.build/Objects-normal/x86_64/ServerClientBasic.d` File Reference
- 5.57 `/Users/Darka/Dropbox/UNITN/AdvancedProgramming/Project/TLSProject/Build/Intermediates/TLSProject.build/Release/TLSClient.build/Objects-normal/x86_64/ServerClientBasic.d` File Reference
- 5.58 `/Users/Darka/Dropbox/UNITN/AdvancedProgramming/Project/TLSProject/Build/Intermediates/TLSProject.build/Release/TLSClient.build/Objects-normal/x86_64/ServerClientBasic.d` File Reference
- 5.59 `/Users/Darka/Dropbox/UNITN/AdvancedProgramming/Project/TLSProject/Build/Intermediates/TLSProject.build/Debug/TLSClient.build/Objects-normal/x86_64/ServerClientHandshakeProtocol.d` File Reference
- 5.60 `/Users/Darka/Dropbox/UNITN/AdvancedProgramming/Project/TLSProject/Build/Intermediates/TLSProject.build/Debug/TLSClient.build/Objects-normal/x86_64/ServerClientHandshakeProtocol.d` File Reference
- 5.61 `/Users/Darka/Dropbox/UNITN/AdvancedProgramming/Project/TLSProject/Build/Intermediates/TLSProject.build/Debug/TLSClient.build/Objects-normal/x86_64/ServerClientHandshakeProtocol.d` File Reference

- 5.62 /Users/Darka/Dropbox/UNITN/AdvancedProgramming/Project/TLSProject/xcodeIntermediates/TLS↵
Project.build/Debug/TLSClient.build/Objects-normal/x86_64/ServerClientHandshakeProtocol.d File
Reference 119
- 5.62 /Users/Darka/Dropbox/UNITN/AdvancedProgramming/Project/TLSProject/xcode↵
Intermediates/TLSProject.build/Debug/TLSClient.build/Objects-normal/x86_64/↵
ServerClientHandshakeProtocol.d File Reference
- 5.63 /Users/Darka/Dropbox/UNITN/AdvancedProgramming/Project/TLSProject/xcode↵
Intermediates/TLSProject.build/Release/TLSClient.build/Objects-normal/x86_64/↵
ServerClientHandshakeProtocol.d File Reference
- 5.64 /Users/Darka/Dropbox/UNITN/AdvancedProgramming/Project/TLSProject/xcode↵
Intermediates/TLSProject.build/Release/TLSClient.build/Objects-normal/x86_64/↵
ServerClientHandshakeProtocol.d File Reference
- 5.65 /Users/Darka/Dropbox/UNITN/AdvancedProgramming/Project/TLSProject/Build/↵
Intermediates/TLSProject.build/Debug/TLSClient.build/Objects-normal/x86_64/↵
ServerClientHello.d File Reference
- 5.66 /Users/Darka/Dropbox/UNITN/AdvancedProgramming/Project/TLSProject/Build/↵
Intermediates/TLSProject.build/Debug/TLSClient.build/Objects-normal/x86_64/↵
ServerClientHello.d File Reference
- 5.67 /Users/Darka/Dropbox/UNITN/AdvancedProgramming/Project/TLSProject/xcode↵
Intermediates/TLSProject.build/Debug/TLSClient.build/Objects-normal/x86_64/↵
ServerClientHello.d File Reference
- 5.68 /Users/Darka/Dropbox/UNITN/AdvancedProgramming/Project/TLSProject/xcode↵
Intermediates/TLSProject.build/Debug/TLSClient.build/Objects-normal/x86_64/↵
ServerClientHello.d File Reference
- 5.69 /Users/Darka/Dropbox/UNITN/AdvancedProgramming/Project/TLSProject/xcode↵
Intermediates/TLSProject.build/Release/TLSClient.build/Objects-normal/x86_64/↵
ServerClientHello.d File Reference
- 5.70 /Users/Darka/Dropbox/UNITN/AdvancedProgramming/Project/TLSProject/xcode↵
Intermediates/TLSProject.build/Release/TLSClient.build/Objects-normal/x86_64/↵
ServerClientHello.d File Reference

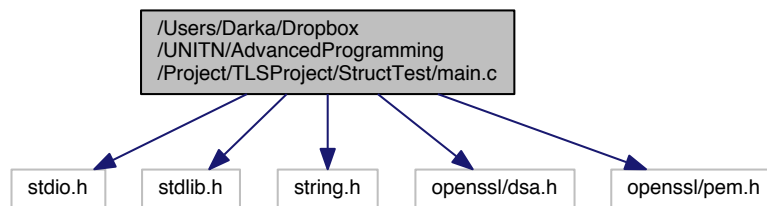
- 5.71 `/Users/Darka/Dropbox/UNITN/AdvancedProgramming/Project/TLSProject/Build/Intermediates/TLSProject.build/Debug/TLSClient.build/Objects-normal/x86_64/ServerClientKeyExchange.d` File Reference
- 5.72 `/Users/Darka/Dropbox/UNITN/AdvancedProgramming/Project/TLSProject/Build/Intermediates/TLSProject.build/Debug/TLSClient.build/Objects-normal/x86_64/ServerClientKeyExchange.d` File Reference
- 5.73 `/Users/Darka/Dropbox/UNITN/AdvancedProgramming/Project/TLSProject/xcodeIntermediates/TLSProject.build/Debug/TLSClient.build/Objects-normal/x86_64/ServerClientKeyExchange.d` File Reference
- 5.74 `/Users/Darka/Dropbox/UNITN/AdvancedProgramming/Project/TLSProject/xcodeIntermediates/TLSProject.build/Debug/TLSClient.build/Objects-normal/x86_64/ServerClientKeyExchange.d` File Reference
- 5.75 `/Users/Darka/Dropbox/UNITN/AdvancedProgramming/Project/TLSProject/xcodeIntermediates/TLSProject.build/Release/TLSClient.build/Objects-normal/x86_64/ServerClientKeyExchange.d` File Reference
- 5.76 `/Users/Darka/Dropbox/UNITN/AdvancedProgramming/Project/TLSProject/xcodeIntermediates/TLSProject.build/Release/TLSClient.build/Objects-normal/x86_64/ServerClientKeyExchange.d` File Reference
- 5.77 `/Users/Darka/Dropbox/UNITN/AdvancedProgramming/Project/TLSProject/Build/Intermediates/TLSProject.build/Debug/TLSClient.build/Objects-normal/x86_64/ServerClientRecordProtocol.d` File Reference
- 5.78 `/Users/Darka/Dropbox/UNITN/AdvancedProgramming/Project/TLSProject/Build/Intermediates/TLSProject.build/Debug/TLSClient.build/Objects-normal/x86_64/ServerClientRecordProtocol.d` File Reference
- 5.79 `/Users/Darka/Dropbox/UNITN/AdvancedProgramming/Project/TLSProject/xcodeIntermediates/TLSProject.build/Debug/TLSClient.build/Objects-normal/x86_64/ServerClientRecordProtocol.d` File Reference

- 5.80 /Users/Darka/Dropbox/UNITN/AdvancedProgramming/Project/TLSPProject/xcodeIntermediates/TLSPProject.build/Debug/TLSServer.build/Objects-normal/x86_64/ServerClientRecordProtocol.d File Reference 121
- 5.80 /Users/Darka/Dropbox/UNITN/AdvancedProgramming/Project/TLSPProject/xcodeIntermediates/TLSPProject.build/Debug/TLSServer.build/Objects-normal/x86_64/ServerClientRecordProtocol.d File Reference
- 5.81 /Users/Darka/Dropbox/UNITN/AdvancedProgramming/Project/TLSPProject/xcodeIntermediates/TLSPProject.build/Release/TLSCClient.build/Objects-normal/x86_64/ServerClientRecordProtocol.d File Reference
- 5.82 /Users/Darka/Dropbox/UNITN/AdvancedProgramming/Project/TLSPProject/xcodeIntermediates/TLSPProject.build/Release/TLSServer.build/Objects-normal/x86_64/ServerClientRecordProtocol.d File Reference
- 5.83 /Users/Darka/Dropbox/UNITN/AdvancedProgramming/Project/TLSPProject/Build/Intermediates/TLSPProject.build/Debug/TLSCClient.build/Objects-normal/x86_64/TLSCClient.d File Reference
- 5.84 /Users/Darka/Dropbox/UNITN/AdvancedProgramming/Project/TLSPProject/Build/Intermediates/TLSPProject.build/Debug/TLSServer.build/Objects-normal/x86_64/TLSCClient.d File Reference
- 5.85 /Users/Darka/Dropbox/UNITN/AdvancedProgramming/Project/TLSPProject/xcodeIntermediates/TLSPProject.build/Debug/TLSCClient.build/Objects-normal/x86_64/TLSCClient.d File Reference
- 5.86 /Users/Darka/Dropbox/UNITN/AdvancedProgramming/Project/TLSPProject/xcodeIntermediates/TLSPProject.build/Debug/TLSServer.build/Objects-normal/x86_64/TLSCClient.d File Reference
- 5.87 /Users/Darka/Dropbox/UNITN/AdvancedProgramming/Project/TLSPProject/xcodeIntermediates/TLSPProject.build/Release/TLSCClient.build/Objects-normal/x86_64/TLSCClient.d File Reference
- 5.88 /Users/Darka/Dropbox/UNITN/AdvancedProgramming/Project/TLSPProject/xcodeIntermediates/TLSPProject.build/Release/TLSServer.build/Objects-normal/x86_64/TLSCClient.d File Reference

- 5.89 `/Users/Darka/Dropbox/UNITN/AdvancedProgramming/Project/TLSPProject/Build/Intermediates/TLSPProject.build/Debug/TLSCClient.build/Objects-normal/x86_64/TLSSServer.d` File Reference
- 5.90 `/Users/Darka/Dropbox/UNITN/AdvancedProgramming/Project/TLSPProject/Build/Intermediates/TLSPProject.build/Debug/TLSSServer.build/Objects-normal/x86_64/TLSSServer.d` File Reference
- 5.91 `/Users/Darka/Dropbox/UNITN/AdvancedProgramming/Project/TLSPProject/xcodeIntermediates/TLSPProject.build/Debug/TLSCClient.build/Objects-normal/x86_64/TLSSServer.d` File Reference
- 5.92 `/Users/Darka/Dropbox/UNITN/AdvancedProgramming/Project/TLSPProject/xcodeIntermediates/TLSPProject.build/Debug/TLSSServer.build/Objects-normal/x86_64/TLSSServer.d` File Reference
- 5.93 `/Users/Darka/Dropbox/UNITN/AdvancedProgramming/Project/TLSPProject/xcodeIntermediates/TLSPProject.build/Release/TLSCClient.build/Objects-normal/x86_64/TLSSServer.d` File Reference
- 5.94 `/Users/Darka/Dropbox/UNITN/AdvancedProgramming/Project/TLSPProject/xcodeIntermediates/TLSPProject.build/Release/TLSSServer.build/Objects-normal/x86_64/TLSSServer.d` File Reference
- 5.95 `/Users/Darka/Dropbox/UNITN/AdvancedProgramming/Project/TLSPProject/Build/Intermediates/TLSPProject.build/Debug/TLSSServer.build/Objects-normal/x86_64/server.d` File Reference
- 5.96 `/Users/Darka/Dropbox/UNITN/AdvancedProgramming/Project/TLSPProject/xcodeIntermediates/TLSPProject.build/Debug/TLSSServer.build/Objects-normal/x86_64/server.d` File Reference
- 5.97 `/Users/Darka/Dropbox/UNITN/AdvancedProgramming/Project/TLSPProject/xcodeIntermediates/TLSPProject.build/Release/TLSSServer.build/Objects-normal/x86_64/server.d` File Reference

5.98 /Users/Darka/Dropbox/UNITN/AdvancedProgramming/Project/TLSProject/StructTest/main.c File Reference

```
#include <stdio.h>
#include <stdlib.h>
#include <string.h>
#include <openssl/dsa.h>
#include <openssl/pem.h>
Include dependency graph for main.c:
```



Functions

- `int main (int argc, const char *argv[])`

5.98.1 Function Documentation

5.98.1.1 `int main (int argc, const char * argv[])`

Definition at line 15 of file `main.c`.

5.99 /Users/Darka/Dropbox/UNITN/AdvancedProgramming/Project/TLSProject/xcodeIntermediates/TLSProject.build/Debug/TLSClient.build/Objects-normal/x86_64/TLSClient-3E1448B75D6FF18F.d File Reference

5.100 /Users/Darka/Dropbox/UNITN/AdvancedProgramming/Project/TLSProject/xcodeIntermediates/TLSProject.build/Debug/TLSClient.build/Objects-normal/x86_64/TLSClient-BF9D49D9B0317373.d File Reference

Index

/Users/Darka/Dropbox/UNITN/AdvancedProgramming/↵
Project/README.md, 60

/Users/Darka/Dropbox/UNITN/AdvancedProgramming/↵
Project/TLSProject/Build/Intermediates/↵
TLSProject.build/Debug/StructTest.build/↵
Objects-normal/x86_64/main.d, 115

/Users/Darka/Dropbox/UNITN/AdvancedProgramming/↵
Project/TLSProject/Build/Intermediates/↵
TLSProject.build/Debug/TLSCient.build/↵
Objects-normal/x86_64/Certificate.d, 115

/Users/Darka/Dropbox/UNITN/AdvancedProgramming/↵
Project/TLSProject/Build/Intermediates/↵
TLSProject.build/Debug/TLSCient.build/↵
Objects-normal/x86_64/Crypto.d, 116

/Users/Darka/Dropbox/UNITN/AdvancedProgramming/↵
Project/TLSProject/Build/Intermediates/↵
TLSProject.build/Debug/TLSCient.build/↵
Objects-normal/x86_64/ServerClientBasic.d,
118

/Users/Darka/Dropbox/UNITN/AdvancedProgramming/↵
Project/TLSProject/Build/Intermediates/↵
TLSProject.build/Debug/TLSCient.build/↵
Objects-normal/x86_64/ServerClient↵
HandshakeProtocol.d, 118

/Users/Darka/Dropbox/UNITN/AdvancedProgramming/↵
Project/TLSProject/Build/Intermediates/↵
TLSProject.build/Debug/TLSCient.build/↵
Objects-normal/x86_64/ServerClientHello.d,
119

/Users/Darka/Dropbox/UNITN/AdvancedProgramming/↵
Project/TLSProject/Build/Intermediates/↵
TLSProject.build/Debug/TLSCient.build/↵
Objects-normal/x86_64/ServerClientKey↵
Exchange.d, 120

/Users/Darka/Dropbox/UNITN/AdvancedProgramming/↵
Project/TLSProject/Build/Intermediates/↵
TLSProject.build/Debug/TLSCient.build/↵
Objects-normal/x86_64/ServerClient↵
RecordProtocol.d, 120

/Users/Darka/Dropbox/UNITN/AdvancedProgramming/↵
Project/TLSProject/Build/Intermediates/↵
TLSProject.build/Debug/TLSCient.build/↵
Objects-normal/x86_64/TLSCient.d, 121

/Users/Darka/Dropbox/UNITN/AdvancedProgramming/↵
Project/TLSProject/Build/Intermediates/↵
TLSProject.build/Debug/TLSCient.build/↵
Objects-normal/x86_64/TLSServer.d, 122

/Users/Darka/Dropbox/UNITN/AdvancedProgramming/↵
Project/TLSProject/Build/Intermediates/↵
TLSProject.build/Debug/TLSCient.build/↵
Objects-normal/x86_64/client.d, 116

/Users/Darka/Dropbox/UNITN/AdvancedProgramming/↵
Project/TLSProject/Build/Intermediates/↵
TLSProject.build/Debug/TLSCient.build/↵
Objects-normal/x86_64/handshakeConstants.↵
d, 117

/Users/Darka/Dropbox/UNITN/AdvancedProgramming/↵
Project/TLSProject/Build/Intermediates/↵
TLSProject.build/Debug/TLSServer.build/↵
Objects-normal/x86_64/Certificate.d, 115

/Users/Darka/Dropbox/UNITN/AdvancedProgramming/↵
Project/TLSProject/Build/Intermediates/↵
TLSProject.build/Debug/TLSServer.build/↵
Objects-normal/x86_64/Crypto.d, 116

/Users/Darka/Dropbox/UNITN/AdvancedProgramming/↵
Project/TLSProject/Build/Intermediates/↵
TLSProject.build/Debug/TLSServer.build/↵
Objects-normal/x86_64/ServerClientBasic.d,
118

/Users/Darka/Dropbox/UNITN/AdvancedProgramming/↵
Project/TLSProject/Build/Intermediates/T↵
LSProject.build/Debug/TLSServer.build/↵
Objects-normal/x86_64/ServerClient↵
HandshakeProtocol.d, 118

/Users/Darka/Dropbox/UNITN/AdvancedProgramming/↵
Project/TLSProject/Build/Intermediates/↵
TLSProject.build/Debug/TLSServer.build/↵
Objects-normal/x86_64/ServerClientHello.d,
119

/Users/Darka/Dropbox/UNITN/AdvancedProgramming/↵
Project/TLSProject/Build/Intermediates/T↵
LSProject.build/Debug/TLSServer.build/↵
Objects-normal/x86_64/ServerClientKey↵
Exchange.d, 120

/Users/Darka/Dropbox/UNITN/AdvancedProgramming/↵
Project/TLSProject/Build/Intermediates/T↵
LSProject.build/Debug/TLSServer.build/↵
Objects-normal/x86_64/ServerClient↵
RecordProtocol.d, 120

/Users/Darka/Dropbox/UNITN/AdvancedProgramming/↵
Project/TLSProject/Build/Intermediates/↵
TLSProject.build/Debug/TLSServer.build/↵
Objects-normal/x86_64/TLSCient.d, 121

/Users/Darka/Dropbox/UNITN/AdvancedProgramming/↵
Project/TLSProject/Build/Intermediates/↵
TLSProject.build/Debug/TLSServer.build/↵
Objects-normal/x86_64/TLSServer.d, 122

- /Users/Darka/Dropbox/UNITN/AdvancedProgramming/↔
Project/TLSPProject/Build/Intermediates/↔
TLSPProject.build/Debug/TLSServer.build/↔
Objects-normal/x86_64/handshakeConstants.↔
d, 117
- /Users/Darka/Dropbox/UNITN/AdvancedProgramming/↔
Project/TLSPProject/Build/Intermediates/↔
TLSPProject.build/Debug/TLSServer.build/↔
Objects-normal/x86_64/server.d, 122
- /Users/Darka/Dropbox/UNITN/AdvancedProgramming/↔
Project/TLSPProject/StructTest/main.c, 123
- /Users/Darka/Dropbox/UNITN/AdvancedProgramming/↔
Project/TLSPProject/xcodeIntermediates/↔
TLSPProject.build/Debug/StructTest.build/↔
Objects-normal/x86_64/main.d, 115
- /Users/Darka/Dropbox/UNITN/AdvancedProgramming/↔
Project/TLSPProject/xcodeIntermediates/↔
TLSPProject.build/Debug/TLSCClient.build/↔
Objects-normal/x86_64/Certificate.d, 115
- /Users/Darka/Dropbox/UNITN/AdvancedProgramming/↔
Project/TLSPProject/xcodeIntermediates/↔
TLSPProject.build/Debug/TLSCClient.build/↔
Objects-normal/x86_64/Crypto.d, 116
- /Users/Darka/Dropbox/UNITN/AdvancedProgramming/↔
Project/TLSPProject/xcodeIntermediates/↔
TLSPProject.build/Debug/TLSCClient.build/↔
Objects-normal/x86_64/ServerClientBasic.d,
118
- /Users/Darka/Dropbox/UNITN/AdvancedProgramming/↔
Project/TLSPProject/xcodeIntermediates/↔
TLSPProject.build/Debug/TLSCClient.build/↔
Objects-normal/x86_64/ServerClient↔
HandshakeProtocol.d, 118
- /Users/Darka/Dropbox/UNITN/AdvancedProgramming/↔
Project/TLSPProject/xcodeIntermediates/↔
TLSPProject.build/Debug/TLSCClient.build/↔
Objects-normal/x86_64/ServerClientHello.d,
119
- /Users/Darka/Dropbox/UNITN/AdvancedProgramming/↔
Project/TLSPProject/xcodeIntermediates/↔
TLSPProject.build/Debug/TLSCClient.build/↔
Objects-normal/x86_64/ServerClientKey↔
Exchange.d, 120
- /Users/Darka/Dropbox/UNITN/AdvancedProgramming/↔
Project/TLSPProject/xcodeIntermediates/↔
TLSPProject.build/Debug/TLSCClient.build/↔
Objects-normal/x86_64/ServerClient↔
RecordProtocol.d, 120
- /Users/Darka/Dropbox/UNITN/AdvancedProgramming/↔
Project/TLSPProject/xcodeIntermediates/↔
TLSPProject.build/Debug/TLSCClient.build/↔
Objects-normal/x86_64/TLSCClient-3E1448↔
B75D6FF18F.d, 123
- /Users/Darka/Dropbox/UNITN/AdvancedProgramming/↔
Project/TLSPProject/xcodeIntermediates/↔
TLSPProject.build/Debug/TLSCClient.build/↔
Objects-normal/x86_64/TLSCClient-BF9D49↔
D9B0317373.d, 123
- /Users/Darka/Dropbox/UNITN/AdvancedProgramming/↔
Project/TLSPProject/xcodeIntermediates/↔
TLSPProject.build/Debug/TLSCClient.build/↔
Objects-normal/x86_64/TLSCClient.d, 121
- /Users/Darka/Dropbox/UNITN/AdvancedProgramming/↔
Project/TLSPProject/xcodeIntermediates/↔
TLSPProject.build/Debug/TLSCClient.build/↔
Objects-normal/x86_64/TLSCClient.d, 121
- /Users/Darka/Dropbox/UNITN/AdvancedProgramming/↔
Project/TLSPProject/xcodeIntermediates/↔
TLSPProject.build/Debug/TLSCClient.build/↔
Objects-normal/x86_64/TLSServer.d, 122
- /Users/Darka/Dropbox/UNITN/AdvancedProgramming/↔
Project/TLSPProject/xcodeIntermediates/↔
TLSPProject.build/Debug/TLSCClient.build/↔
Objects-normal/x86_64/TLSServer.d, 122
- /Users/Darka/Dropbox/UNITN/AdvancedProgramming/↔
Project/TLSPProject/xcodeIntermediates/↔
TLSPProject.build/Debug/TLSCClient.build/↔
Objects-normal/x86_64/client.d, 116
- /Users/Darka/Dropbox/UNITN/AdvancedProgramming/↔
Project/TLSPProject/xcodeIntermediates/↔
TLSPProject.build/Debug/TLSCClient.build/↔
Objects-normal/x86_64/handshakeConstants.↔
d, 117
- /Users/Darka/Dropbox/UNITN/AdvancedProgramming/↔
Project/TLSPProject/xcodeIntermediates/↔
TLSPProject.build/Debug/TLSServer.build/↔
Objects-normal/x86_64/Certificate.d, 116
- /Users/Darka/Dropbox/UNITN/AdvancedProgramming/↔
Project/TLSPProject/xcodeIntermediates/↔
TLSPProject.build/Debug/TLSServer.build/↔
Objects-normal/x86_64/Crypto.d, 117
- /Users/Darka/Dropbox/UNITN/AdvancedProgramming/↔
Project/TLSPProject/xcodeIntermediates/↔
TLSPProject.build/Debug/TLSServer.build/↔
Objects-normal/x86_64/ServerClientBasic.d,
118
- /Users/Darka/Dropbox/UNITN/AdvancedProgramming/↔
Project/TLSPProject/xcodeIntermediates/↔
TLSPProject.build/Debug/TLSServer.build/↔
Objects-normal/x86_64/ServerClient↔
HandshakeProtocol.d, 119
- /Users/Darka/Dropbox/UNITN/AdvancedProgramming/↔
Project/TLSPProject/xcodeIntermediates/↔
TLSPProject.build/Debug/TLSServer.build/↔
Objects-normal/x86_64/ServerClientHello.d,
119
- /Users/Darka/Dropbox/UNITN/AdvancedProgramming/↔
Project/TLSPProject/xcodeIntermediates/↔
TLSPProject.build/Debug/TLSServer.build/↔
Objects-normal/x86_64/ServerClientKey↔
Exchange.d, 120
- /Users/Darka/Dropbox/UNITN/AdvancedProgramming/↔
Project/TLSPProject/xcodeIntermediates/↔
TLSPProject.build/Debug/TLSServer.build/↔
Objects-normal/x86_64/ServerClient↔
RecordProtocol.d, 121
- /Users/Darka/Dropbox/UNITN/AdvancedProgramming/↔
Project/TLSPProject/xcodeIntermediates/↔
TLSPProject.build/Debug/TLSServer.build/↔
Objects-normal/x86_64/TLSCClient.d, 121
- /Users/Darka/Dropbox/UNITN/AdvancedProgramming/↔
Project/TLSPProject/xcodeIntermediates/↔
TLSPProject.build/Debug/TLSServer.build/↔
Objects-normal/x86_64/TLSServer.d, 122

- /Users/Darka/Dropbox/UNITN/AdvancedProgramming/↵
 - Project/TLSPProject/xcodeIntermediates/↵
 - TLSPProject.build/Debug/TLSServer.build/↵
 - Objects-normal/x86_64/handshakeConstants.↵
 d, 117
- /Users/Darka/Dropbox/UNITN/AdvancedProgramming/↵
 - Project/TLSPProject/xcodeIntermediates/↵
 - TLSPProject.build/Debug/TLSServer.build/↵
 - Objects-normal/x86_64/server.d, 122
- /Users/Darka/Dropbox/UNITN/AdvancedProgramming/↵
 - Project/TLSPProject/xcodeIntermediates/T↵
 - LSProject.build/Release/TLSCClient.build/↵
 - Objects-normal/x86_64/Certificate.d, 116
- /Users/Darka/Dropbox/UNITN/AdvancedProgramming/↵
 - Project/TLSPProject/xcodeIntermediates/T↵
 - LSProject.build/Release/TLSCClient.build/↵
 - Objects-normal/x86_64/Crypto.d, 117
- /Users/Darka/Dropbox/UNITN/AdvancedProgramming/↵
 - Project/TLSPProject/xcodeIntermediates/T↵
 - LSProject.build/Release/TLSCClient.build/↵
 - Objects-normal/x86_64/ServerClientBasic.d, 118
- /Users/Darka/Dropbox/UNITN/AdvancedProgramming/↵
 - Project/TLSPProject/xcodeIntermediates/↵
 - TLSPProject.build/Release/TLSCClient.↵
 - build/Objects-normal/x86_64/ServerClient↵
 - HandshakeProtocol.d, 119
- /Users/Darka/Dropbox/UNITN/AdvancedProgramming/↵
 - Project/TLSPProject/xcodeIntermediates/T↵
 - LSProject.build/Release/TLSCClient.build/↵
 - Objects-normal/x86_64/ServerClientHello.d, 119
- /Users/Darka/Dropbox/UNITN/AdvancedProgramming/↵
 - Project/TLSPProject/xcodeIntermediates/T↵
 - LSProject.build/Release/TLSCClient.build/↵
 - Objects-normal/x86_64/ServerClientKey↵
 - Exchange.d, 120
- /Users/Darka/Dropbox/UNITN/AdvancedProgramming/↵
 - Project/TLSPProject/xcodeIntermediates/↵
 - TLSPProject.build/Release/TLSCClient.↵
 - build/Objects-normal/x86_64/ServerClient↵
 - RecordProtocol.d, 121
- /Users/Darka/Dropbox/UNITN/AdvancedProgramming/↵
 - Project/TLSPProject/xcodeIntermediates/T↵
 - LSProject.build/Release/TLSCClient.build/↵
 - Objects-normal/x86_64/TLSCClient.d, 121
- /Users/Darka/Dropbox/UNITN/AdvancedProgramming/↵
 - Project/TLSPProject/xcodeIntermediates/T↵
 - LSProject.build/Release/TLSCClient.build/↵
 - Objects-normal/x86_64/TLSServer.d, 122
- /Users/Darka/Dropbox/UNITN/AdvancedProgramming/↵
 - Project/TLSPProject/xcodeIntermediates/T↵
 - LSProject.build/Release/TLSCClient.build/↵
 - Objects-normal/x86_64/client.d, 116
- /Users/Darka/Dropbox/UNITN/AdvancedProgramming/↵
 - Project/TLSPProject/xcodeIntermediates/↵
 - TLSPProject.build/Release/TLSCClient.↵
 - build/Objects-normal/x86_64/handshake↵
 Constants.d, 117
- /Users/Darka/Dropbox/UNITN/AdvancedProgramming/↵
 - Project/TLSPProject/xcodeIntermediates/TL↵
 - SProject.build/Release/TLSServer.build/↵
 - Objects-normal/x86_64/Certificate.d, 116
- /Users/Darka/Dropbox/UNITN/AdvancedProgramming/↵
 - Project/TLSPProject/xcodeIntermediates/TL↵
 - SProject.build/Release/TLSServer.build/↵
 - Objects-normal/x86_64/Crypto.d, 117
- /Users/Darka/Dropbox/UNITN/AdvancedProgramming/↵
 - Project/TLSPProject/xcodeIntermediates/TL↵
 - SProject.build/Release/TLSServer.build/↵
 - Objects-normal/x86_64/ServerClientBasic.d, 118
- /Users/Darka/Dropbox/UNITN/AdvancedProgramming/↵
 - Project/TLSPProject/xcodeIntermediates/↵
 - TLSPProject.build/Release/TLSServer.↵
 - build/Objects-normal/x86_64/ServerClient↵
 - HandshakeProtocol.d, 119
- /Users/Darka/Dropbox/UNITN/AdvancedProgramming/↵
 - Project/TLSPProject/xcodeIntermediates/TL↵
 - SProject.build/Release/TLSServer.build/↵
 - Objects-normal/x86_64/ServerClientHello.d, 119
- /Users/Darka/Dropbox/UNITN/AdvancedProgramming/↵
 - Project/TLSPProject/xcodeIntermediates/TL↵
 - SProject.build/Release/TLSServer.build/↵
 - Objects-normal/x86_64/ServerClientKey↵
 - Exchange.d, 120
- /Users/Darka/Dropbox/UNITN/AdvancedProgramming/↵
 - Project/TLSPProject/xcodeIntermediates/↵
 - TLSPProject.build/Release/TLSServer.↵
 - build/Objects-normal/x86_64/ServerClient↵
 - RecordProtocol.d, 121
- /Users/Darka/Dropbox/UNITN/AdvancedProgramming/↵
 - Project/TLSPProject/xcodeIntermediates/TL↵
 - SProject.build/Release/TLSServer.build/↵
 - Objects-normal/x86_64/TLSCClient.d, 121
- /Users/Darka/Dropbox/UNITN/AdvancedProgramming/↵
 - Project/TLSPProject/xcodeIntermediates/TL↵
 - SProject.build/Release/TLSServer.build/↵
 - Objects-normal/x86_64/TLSServer.d, 122
- /Users/Darka/Dropbox/UNITN/AdvancedProgramming/↵
 - Project/TLSPProject/xcodeIntermediates/↵
 - TLSPProject.build/Release/TLSServer.↵
 - build/Objects-normal/x86_64/handshake↵
 Constants.d, 117
- /Users/Darka/Dropbox/UNITN/AdvancedProgramming/↵
 - Project/TLSPProject/xcodeIntermediates/TL↵
 - SProject.build/Release/TLSServer.build/↵
 - Objects-normal/x86_64/server.d, 122
- /Users/Darka/Dropbox/UNITN/AdvancedProgramming/↵
 - Project/include/Crypto.h, 23
- /Users/Darka/Dropbox/UNITN/AdvancedProgramming/↵
 - Project/include/HandshakeMessages/↵
 - Certificate.h, 30
- /Users/Darka/Dropbox/UNITN/AdvancedProgramming/↵
 - Project/include/HandshakeMessages/↵

- handshakeConstants.h, 27
- channel_source
 - channel, 10
- cipher_id
 - cipher_suite_t, 11
- cipher_suite
 - TLS_parameters, 21
- cipher_suite_len
 - handshake_hello, 17
 - handshakeConstants.c, 66
- cipher_suite_list
 - handshakeConstants.c, 66
- cipher_suite_t, 11
 - au, 11
 - cipher_id, 11
 - hash, 11
 - key_size, 11
 - kx, 11
 - name, 12
- cipher_suites
 - handshake_hello, 17
- client.c
 - main, 87
 - onPacketReceive, 87
 - print_master_secret, 88
 - print_random, 88
 - TLS_param, 89
- client_key_exchange, 12
 - key, 12
 - key_length, 12
- client_random
 - TLS_parameters, 21
- clientBasic.c
 - main, 102
 - onPacketReceive, 103
- clientHandshake.c
 - main, 105
- clientRecord.c
 - main, 106
 - onPacketReceive, 106
- compression_id
 - compression_methods_t, 13
- compression_methods
 - handshake_hello, 17
 - ServerClientHello.h, 34
- compression_methods_t, 12
 - compression_id, 13
 - length, 13
- compute_set_master_key_DH
 - server.c, 90
- compute_set_master_key_ECDHE
 - server.c, 90
- compute_set_master_key_RSA
 - server.c, 91
- create_channel
 - ServerClientBasic.c, 74
 - ServerClientBasic.h, 41
- create_packet
 - ServerClientBasic.c, 74
 - ServerClientBasic.h, 41
- Crypto.c
 - PRF, 61
 - sign_DHE_server_key_ex, 62
 - sign_ECDHE_server_key_ex, 62
 - sign_with_DSS, 63
 - sign_with_ECDSA, 63
 - sign_with_RSA, 63
 - verify_DHE_server_key_ex_sign, 64
 - verify_ECDHE_server_key_ex_sign, 64
- Crypto.h
 - PRF, 24
 - sign_DHE_server_key_ex, 24
 - sign_ECDHE_server_key_ex, 25
 - verify_DHE_server_key_ex_sign, 25
 - verify_ECDHE_server_key_ex_sign, 25
- DELAY_TIME
 - ServerClientBasic.h, 40
- DHE_KX
 - handshakeConstants.h, 29
- DHE_server_key_exchange, 13
 - g, 14
 - p, 14
 - pubKey, 14
 - sign_hash_alg, 14
 - signature, 14
 - signature_length, 14
- DSS_AU
 - handshakeConstants.h, 28
- deserialize_certificate_message
 - Certificate.c, 67
 - Certificate.h, 31
- deserialize_client_key_exchange
 - ServerClientKeyExchange.c, 71
 - ServerClientKeyExchange.h, 38
- deserialize_client_server_hello
 - ServerClientHello.c, 69
 - ServerClientHello.h, 34
- deserialize_handshake
 - ServerClientHandshakeProtocol.c, 80
 - ServerClientHandshakeProtocol.h, 46
- deserialize_packet
 - ServerClientBasic.c, 74
- deserialize_record
 - ServerClientRecordProtocol.c, 84
 - ServerClientRecordProtocol.h, 51
- deserialize_server_key_exchange
 - ServerClientKeyExchange.c, 72
 - ServerClientKeyExchange.h, 38
- destination
 - packet_basic, 18
- ECDHE_KX
 - handshakeConstants.h, 29
- ECDHE_server_key_exchange, 14
 - named_curve, 15
 - pub_key, 15

- sign_hash_alg, 15
- signature, 15
- signature_length, 15
- ECDSA_AU
 - handshakeConstants.h, 28
- enum_handshake_type
 - handshakeConstants.h, 27
- enum_mode
 - ServerClientBasic.h, 40
- enum_record_version
 - handshakeConstants.h, 27
- enum_recordtype
 - ServerClientRecordProtocol.h, 50
- FINISHED
 - handshakeConstants.h, 28
- fd
 - channel, 10
- fileName
 - channel, 10
- free_certificate_message
 - Certificate.c, 67
 - Certificate.h, 31
- free_handshake
 - ServerClientHandshakeProtocol.c, 80
 - ServerClientHandshakeProtocol.h, 46
- free_hello
 - ServerClientHello.c, 69
 - ServerClientHello.h, 34
- free_packet
 - ServerClientBasic.c, 75
 - ServerClientBasic.h, 42
- free_record
 - ServerClientRecordProtocol.c, 84
 - ServerClientRecordProtocol.h, 51
- free_server_key_exchange
 - ServerClientKeyExchange.c, 72
 - ServerClientKeyExchange.h, 38
- g
 - DHE_server_key_exchange, 14
- get_cipher_suite
 - handshakeConstants.c, 65
 - handshakeConstants.h, 29
- get_file_size
 - ServerClientBasic.c, 75
- get_hash_function
 - handshakeConstants.c, 65
 - handshakeConstants.h, 29
- HANDSHAKE
 - ServerClientRecordProtocol.h, 50
- HELLO_REQUEST
 - handshakeConstants.h, 28
- handshake, 15
 - length, 16
 - message, 16
 - type, 16
- handshake_hello, 16
 - cipher_suite_len, 17
 - cipher_suites, 17
 - compression_methods, 17
 - random, 17
 - session_id, 17
 - TLS_version, 17
- handshake_messages
 - TLS_parameters, 21
- handshake_messages_len
 - TLS_parameters, 22
- handshakeConstants.c
 - cipher_suite_len, 66
 - cipher_suite_list, 66
 - get_cipher_suite, 65
 - get_hash_function, 65
- handshakeConstants.h
 - authentication_algorithm, 28
 - CERTIFICATE_REQUEST, 28
 - CERTIFICATE_VERIFY, 28
 - CERTIFICATE, 28
 - CLIENT_HELLO, 28
 - CLIENT_KEY_EXCHANGE, 28
 - CLIENT_MODE, 28
 - channel_mode, 28
 - channel_mode_enum, 27
 - DHE_KX, 29
 - DSS_AU, 28
 - ECDHE_KX, 29
 - ECDSA_AU, 28
 - enum_handshake_type, 27
 - enum_record_version, 27
 - FINISHED, 28
 - get_cipher_suite, 29
 - get_hash_function, 29
 - HELLO_REQUEST, 28
 - hash_algorithm, 28
 - key_exchange_algorithm, 29
 - md5, 29
 - none, 29
 - REV16, 27
 - REV32, 28
 - RSA_AU, 28
 - RSA_KX, 29
 - SERVER_DONE, 28
 - SERVER_HELLO, 28
 - SERVER_KEY_EXCHANGE, 28
 - SERVER_MODE, 28
 - SSL3_0, 29
 - sha1, 29
 - sha224, 29
 - sha256, 29
 - sha384, 29
 - sha512, 29
 - TLS1_0, 29
 - TLS1_1, 29
 - TLS1_2, 29
 - TLS_version, 29
- hash

- cipher_suite_t, 11
- hash_algorithm
 - handshakeConstants.h, 28
- isEnabled
 - channel, 10
- key
 - client_key_exchange, 12
- key_exchange_algorithm
 - handshakeConstants.h, 29
- key_length
 - client_key_exchange, 12
- key_size
 - cipher_suite_t, 11
- kx
 - cipher_suite_t, 11
- length
 - record, 19
- length
 - compression_methods_t, 13
 - handshake, 16
- main
 - client.c, 87
 - clientBasic.c, 102
 - clientHandshake.c, 105
 - clientRecord.c, 106
 - main.c, 123
 - server.c, 91
 - serverBasic.c, 108
 - serverHandshake.c, 110
 - serverRecord.c, 112
 - testCertificate.c, 114
- main.c
 - main, 123
- make_DHE_server_key_exchange
 - TLS.h, 57
 - TLSServer.c, 99
- make_ECDHE_server_key_exchange
 - TLS.h, 58
 - TLSServer.c, 99
- make_certificate
 - TLS.h, 54
 - TLSServer.c, 98
- make_certificate_message
 - Certificate.c, 67
 - Certificate.h, 32
- make_change_cipher_spec
 - TLS.h, 55
 - TLSCClient.c, 95
- make_client_hello
 - TLS.h, 55
 - TLSCClient.c, 95
- make_client_key_exchange
 - TLS.h, 56
 - TLSCClient.c, 96
- make_finished_message
 - TLS.h, 58
 - TLSCClient.c, 97
- make_hello
 - ServerClientHello.c, 70
 - ServerClientHello.h, 35
- make_record
 - ServerClientHandshakeProtocol.c, 81
- make_server_hello
 - TLS.h, 59
 - TLSServer.c, 100
- make_server_hello_done
 - TLS.h, 59
 - TLSServer.c, 101
- make_server_key_exchange
 - TLS.h, 60
 - TLSServer.c, 101
- master_secret
 - TLS_parameters, 22
- master_secret_len
 - TLS_parameters, 22
- md5
 - handshakeConstants.h, 29
- message
 - handshake, 16
 - packet_basic, 18
 - record, 19
- messageLen
 - packet_basic, 18
- mod
 - channel, 10
- mode
 - ServerClientBasic.h, 41
- name
 - cipher_suite_t, 12
- named_curve
 - ECDHE_server_key_exchange, 15
- none
 - handshakeConstants.h, 29
- onPacketReceive
 - channel, 10
 - client.c, 87
 - clientBasic.c, 103
 - clientRecord.c, 106
 - server.c, 92
 - serverBasic.c, 108
 - serverHandshake.c, 110
 - serverRecord.c, 113
- p
 - DHE_server_key_exchange, 14
- PRF
 - Crypto.c, 61
 - Crypto.h, 24
- packet_basic, 17
 - destination, 18
 - message, 18
 - messageLen, 18

- source, 18
- previous_state
 - TLS_parameters, 22
- print_handshake
 - ServerClientHandshakeProtocol.c, 81
 - ServerClientHandshakeProtocol.h, 47
- print_hello
 - ServerClientHello.h, 35
- print_master_secret
 - client.c, 88
 - server.c, 93
- print_random
 - client.c, 88
 - server.c, 93
- print_record
 - ServerClientRecordProtocol.c, 84
 - ServerClientRecordProtocol.h, 51
- private_key
 - TLS_parameters, 22
- pub_key
 - ECDHE_server_key_exchange, 15
- pubKey
 - DHE_server_key_exchange, 14
- REV16
 - handshakeConstants.h, 27
 - ServerClientRecordProtocol.h, 50
- REV32
 - handshakeConstants.h, 28
- RSA_AU
 - handshakeConstants.h, 28
- RSA_KX
 - handshakeConstants.h, 29
- random
 - handshake_hello, 17
- random_bytes
 - random_data, 19
- random_data, 18
 - random_bytes, 19
 - UNIX_time, 19
- read_all_file
 - ServerClientBasic.c, 75
- reader
 - ServerClientBasic.c, 76
- record, 19
 - length, 19
 - message, 19
 - ServerClientRecordProtocol.h, 50
 - type, 19
 - version, 20
- recordType
 - ServerClientRecordProtocol.h, 50
- SERVER_DONE
 - handshakeConstants.h, 28
- SERVER_HELLO
 - handshakeConstants.h, 28
- SERVER_KEY_EXCHANGE
 - handshakeConstants.h, 28
- SERVER_MODE
 - handshakeConstants.h, 28
- SERVER
 - ServerClientBasic.h, 41
- SSL3_0
 - handshakeConstants.h, 29
- send_handshake
 - ServerClientHandshakeProtocol.c, 82
 - ServerClientHandshakeProtocol.h, 47
- send_packet
 - ServerClientBasic.c, 77
 - ServerClientBasic.h, 42
- send_record
 - ServerClientRecordProtocol.c, 85
 - ServerClientRecordProtocol.h, 52
- serialize_certificate_message
 - Certificate.c, 68
 - Certificate.h, 32
- serialize_client_key_exchange
 - ServerClientKeyExchange.c, 72
 - ServerClientKeyExchange.h, 38
- serialize_client_server_hello
 - ServerClientHello.c, 70
 - ServerClientHello.h, 36
- serialize_handshake
 - ServerClientHandshakeProtocol.c, 83
 - ServerClientHandshakeProtocol.h, 48
- serialize_packet
 - ServerClientBasic.c, 77
- serialize_record
 - ServerClientRecordProtocol.c, 86
 - ServerClientRecordProtocol.h, 52
- serialize_server_key_exchange
 - ServerClientKeyExchange.c, 72
 - ServerClientKeyExchange.h, 39
- server.c
 - compute_set_master_key_DH, 90
 - compute_set_master_key_ECDHE, 90
 - compute_set_master_key_RSA, 91
 - main, 91
 - onPacketReceive, 92
 - print_master_secret, 93
 - print_random, 93
 - TLS_param, 94
- server_certificate
 - TLS_parameters, 22
- server_key_ex
 - TLS_parameters, 22
- server_key_exchange_structs
 - ServerClientKeyExchange.h, 38
- server_random
 - TLS_parameters, 22
- serverBasic.c
 - main, 108
 - onPacketReceive, 108
- ServerClientBasic.c
 - create_channel, 74
 - create_packet, 74

- deserialize_packet, 74
- free_packet, 75
- get_file_size, 75
- read_all_file, 75
- reader, 76
- send_packet, 77
- serialize_packet, 77
- set_on_receive, 78
- start_listener, 79
- stop_channel, 79
- wait_channel, 79
- ServerClientBasic.h
 - CLIENT, 41
 - channel, 41
 - create_channel, 41
 - create_packet, 41
 - DELAY_TIME, 40
 - enum_mode, 40
 - free_packet, 42
 - mode, 41
 - SERVER, 41
 - send_packet, 42
 - set_on_receive, 43
 - start_listener, 44
 - stop_channel, 44
 - struct_channel, 41
 - struct_packet, 41
 - wait_channel, 45
- ServerClientHandshakeProtocol.c
 - deserialize_handshake, 80
 - free_handshake, 80
 - make_record, 81
 - print_handshake, 81
 - send_handshake, 82
 - serialize_handshake, 83
- ServerClientHandshakeProtocol.h
 - deserialize_handshake, 46
 - free_handshake, 46
 - print_handshake, 47
 - send_handshake, 47
 - serialize_handshake, 48
- ServerClientHello.c
 - deserialize_client_server_hello, 69
 - free_hello, 69
 - make_hello, 70
 - serialize_client_server_hello, 70
- ServerClientHello.h
 - compression_methods, 34
 - deserialize_client_server_hello, 34
 - free_hello, 34
 - make_hello, 35
 - print_hello, 35
 - serialize_client_server_hello, 36
 - session_id, 34
- ServerClientKeyExchange.c
 - deserialize_client_key_exchange, 71
 - deserialize_server_key_exchange, 72
 - free_server_key_exchange, 72
 - serialize_client_key_exchange, 72
 - serialize_server_key_exchange, 72
- ServerClientKeyExchange.h
 - deserialize_client_key_exchange, 38
 - deserialize_server_key_exchange, 38
 - free_server_key_exchange, 38
 - serialize_client_key_exchange, 38
 - serialize_server_key_exchange, 39
 - server_key_exchange_structs, 38
- ServerClientRecordProtocol.c
 - deserialize_record, 84
 - free_record, 84
 - print_record, 84
 - send_record, 85
 - serialize_record, 86
- ServerClientRecordProtocol.h
 - ALERT, 50
 - APPLICATION_DATA, 50
 - CHANGE_CIPHER_SPEC, 50
 - deserialize_record, 51
 - enum_recordtype, 50
 - free_record, 51
 - HANDSHAKE, 50
 - print_record, 51
 - REV16, 50
 - record, 50
 - recordType, 50
 - send_record, 52
 - serialize_record, 52
 - struct_record, 50
- serverHandshake.c
 - main, 110
 - onPacketReceive, 110
- serverRecord.c
 - main, 112
 - onPacketReceive, 113
- session_id
 - handshake_hello, 17
 - ServerClientHello.h, 34
 - session_id_t, 20
- session_id_t, 20
 - session_id, 20
 - session_lenght, 20
- session_lenght
 - session_id_t, 20
- set_on_receive
 - ServerClientBasic.c, 78
 - ServerClientBasic.h, 43
- sha1
 - handshakeConstants.h, 29
- sha224
 - handshakeConstants.h, 29
- sha256
 - handshakeConstants.h, 29
- sha384
 - handshakeConstants.h, 29
- sha512
 - handshakeConstants.h, 29

- sign_DHE_server_key_ex
 - Crypto.c, 62
 - Crypto.h, 24
- sign_ECDHE_server_key_ex
 - Crypto.c, 62
 - Crypto.h, 25
- sign_hash_alg
 - DHE_server_key_exchange, 14
 - ECDHE_server_key_exchange, 15
- sign_with_DSS
 - Crypto.c, 63
- sign_with_ECDSA
 - Crypto.c, 63
- sign_with_RSA
 - Crypto.c, 63
- signature
 - DHE_server_key_exchange, 14
 - ECDHE_server_key_exchange, 15
- signature_length
 - DHE_server_key_exchange, 14
 - ECDHE_server_key_exchange, 15
- source
 - packet_basic, 18
- start_listener
 - ServerClientBasic.c, 79
 - ServerClientBasic.h, 44
- stop_channel
 - ServerClientBasic.c, 79
 - ServerClientBasic.h, 44
- struct_channel
 - ServerClientBasic.h, 41
- struct_packet
 - ServerClientBasic.h, 41
- struct_record
 - ServerClientRecordProtocol.h, 50
- TLS.h
 - backup_handshake, 54
 - make_DHE_server_key_exchange, 57
 - make_ECDHE_server_key_exchange, 58
 - make_certificate, 54
 - make_change_cipher_spec, 55
 - make_client_hello, 55
 - make_client_key_exchange, 56
 - make_finished_message, 58
 - make_server_hello, 59
 - make_server_hello_done, 59
 - make_server_key_exchange, 60
 - TLS_parameter_enum, 54
- TLS1_0
 - handshakeConstants.h, 29
- TLS1_1
 - handshakeConstants.h, 29
- TLS1_2
 - handshakeConstants.h, 29
- TLS_param
 - client.c, 89
 - server.c, 94
- TLS_parameter_enum
 - TLS.h, 54
- TLS_parameters, 21
 - cipher_suite, 21
 - client_random, 21
 - handshake_messages, 21
 - handshake_messages_len, 22
 - master_secret, 22
 - master_secret_len, 22
 - previous_state, 22
 - private_key, 22
 - server_certificate, 22
 - server_key_ex, 22
 - server_random, 22
 - tls_version, 22
- TLS_version
 - handshake_hello, 17
 - handshakeConstants.h, 29
- TLSCClient.c
 - backup_handshake, 95
 - make_change_cipher_spec, 95
 - make_client_hello, 95
 - make_client_key_exchange, 96
 - make_finished_message, 97
- TLSServer.c
 - make_DHE_server_key_exchange, 99
 - make_ECDHE_server_key_exchange, 99
 - make_certificate, 98
 - make_server_hello, 100
 - make_server_hello_done, 101
 - make_server_key_exchange, 101
- testCertificate.c
 - main, 114
- thread
 - channel, 10
- tls_version
 - TLS_parameters, 22
- type
 - handshake, 16
 - record, 19
- UNIX_time
 - random_data, 19
- verify_DHE_server_key_ex_sign
 - Crypto.c, 64
 - Crypto.h, 25
- verify_ECDHE_server_key_ex_sign
 - Crypto.c, 64
 - Crypto.h, 25
- version
 - record, 20
- wait_channel
 - ServerClientBasic.c, 79
 - ServerClientBasic.h, 45
- X509_certificate
 - certificate_message, 9