Звіт з виконання лабораторної роботи 1

ФІ-42мн Кістаєв Матвій
ФІ-42мн Бондар Петро

December 27, 2025

Огляд

Тема: Дослідження реалізацій протоколу SSL/TLS.

Мета: Дослідження особливостей реалізації криптографічних механізмів протоколу SSL/TLS

Задача: Розробити програмний засіб захисту логічного каналу зв'язку, що використовує протокол TLS (версія 1.3). Програмний засіб повинен мати хмарну архітектуру, в якій клієнт повинен бути орієнтованим на операційні системи та платформи для мобільних телефонів та планшетних комп'ютерів. Дозволяється використання бібліотеки OpenSSL або Crypto++ – реалізації з відкритим кодом.

Особливості реалізації

- Реалізовано програмний засіб із примітивним графічним інтерфейсом для платформи Windows.
- Програма дозволяє відігравати роль, як сервера, так і клієнта.

Figure 1: Скріншот із головного екрану програми

- Сервер та клієнт комунікують в межах локальної мережі по TCP.
- Використано мову програмування `Python` та бібліотеку для роботи з мережевими пакетами `Scapy`.

  Бібліотека дозволяє мати повний контроль над формуванням та відправкою пакетів.

  Шифрування, дешифрування та оновлення криптографічного контексту відбувається напівавтоматично.
- За допомогою бібліотеки `cryptography` реалізовано функцію для формування `X.509` сертифікатів (з вигаданим полем `issuer`).
- Реалізовано TLS версії 1.2. Кожне повідомлення рукостискання формується і надсилається «вручну». Всі криптографічні механізми працюють автоматично, спираючись на функціонал об'єкту сесії з бібліотеки `Scapy`, яка в свою чергу спирається на бібліотеку `cryptography` в `Python`.

```
        if "ECDHE" in controller.session.pwcs.ciphersuite.kx_alg.name:
            DHE_params = ServerECDHNamedCurveParams(tls_session=controller.session)
        else:
            DHE_params = ServerDHParams(tls_session=controller.session)

        DHE_params.fill_missing()

        ske_msg = TLSServerKeyExchange(params=DHE_params, tls_session=controller.session)

        ske_record = TLS(
            type=22,
            version=0x0303,
            msg=[ske_msg],
            tls_session=controller.session
        )
```

Figure 2: Приклад формування пакету `ServerKeyExchange`

```
        cs_codes = [ciphersuites[i].val for i in range(len(ciphersuites)) if check_vars[i].get() == 1]

        client_hello = TLSClientHello(
            version=0x0303,  # TLS 1.2
            gmt_unix_time=int(time.time()),
            random_bytes=os.urandom(28),
            sid=b'',
            ciphers=cs_codes,
            comp=[0],
            ext=[],
            tls_session=controller.session
        )

        client_hello_record = TLS(
            type=22,
            version=0x0303,
            msg=[client_hello],
            tls_session=controller.session
        )

        client_random = client_hello.gmt_unix_time.to_bytes(4, 'big') + client_hello.random_bytes
        controller.session.client_random = client_random
```

Figure 3: Приклад формування пакету `ClientHello`

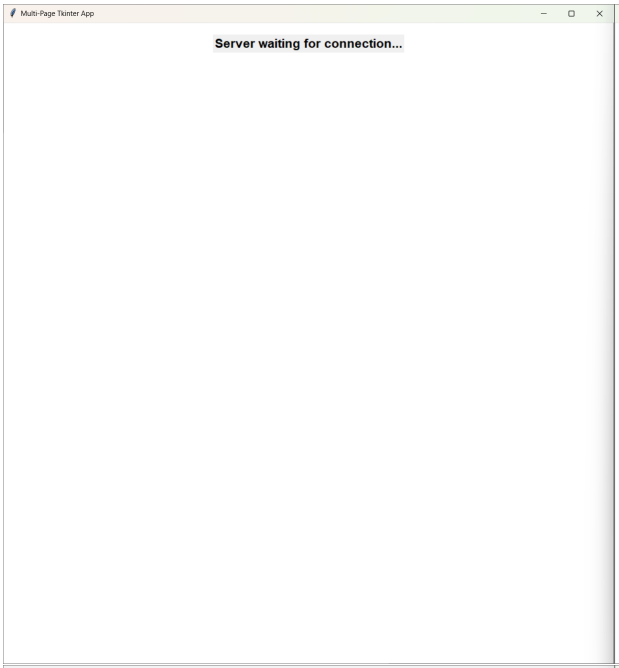
Демонстрація роботи програми

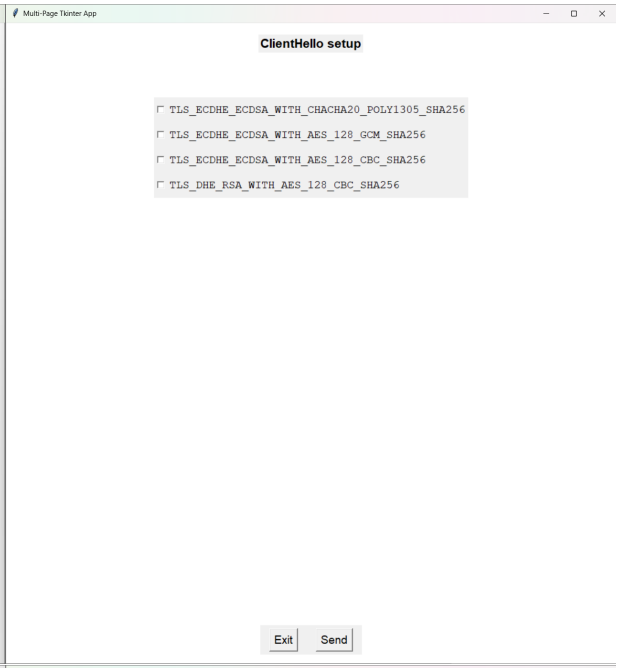
Далі наведемо кожен крок протоколу TLS, як це відображається в розробленій програмі.

З лівого боку знаходиться вікно сервера, з правого – клієнта.

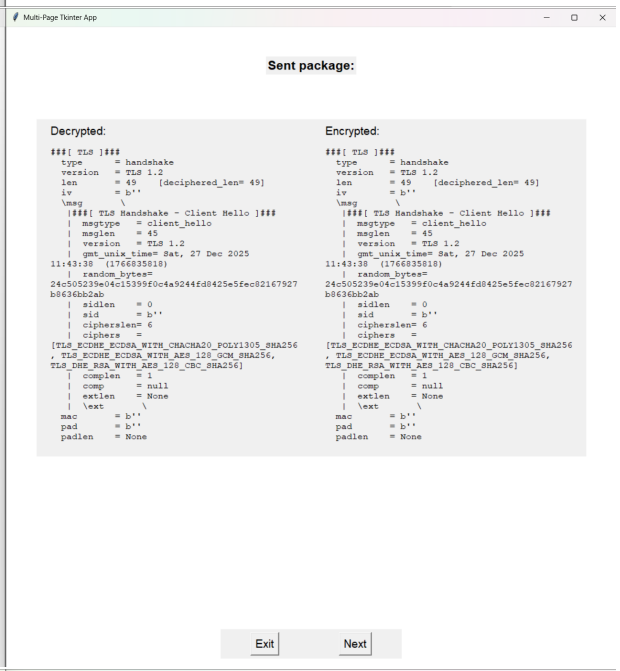
Кожен отриманий та надісланий пакет відображається у чистому вигляді (Enrcypted) та розшифрованому з урахуванням криптографічного контексту (Decrypted). Починаючи з `ClientHandshakeFinished`, коли повідомлення починають шифруватись, можна побачити різницю в цих двох колонках.

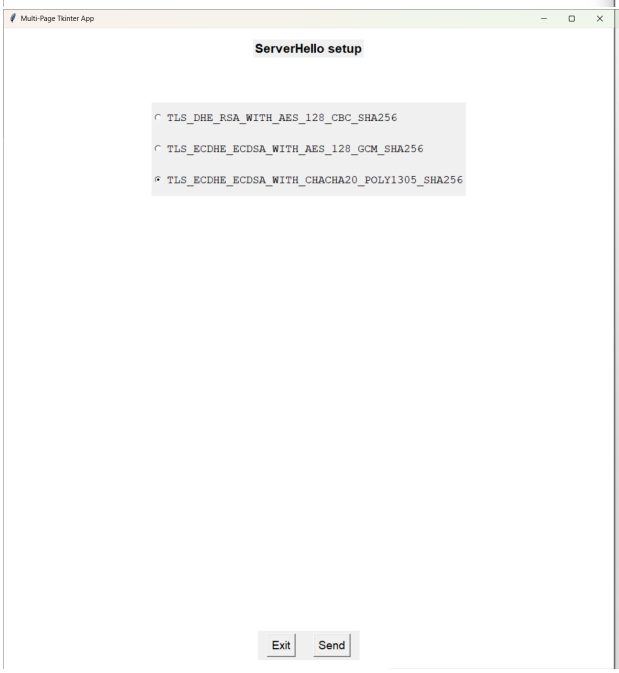
Також реалізовано базовий функціонал впливу на перебіг рукостискання – наприклад: ручний вибір наборів криптографічних алгоритмів, вибір довільного файлу сертифікату та публічного ключа для підпису сервера.


Multi-Page Tkinter App
Server waiting for connection...


Multi-Page Tkinter App
ClientHello setup
TLS_ECDHE_ECDSA_WITH_CHACHA20_POLY1305_SHA256
TLS_ECDHE_ECDSA_WITH_AES_128_GCM_SHA256
TLS_ECDHE_ECDSA_WITH_AES_128_CBC_SHA256
TLS_DHE_RSA_WITH_AES_128_CBC_SHA256
Exit
Send

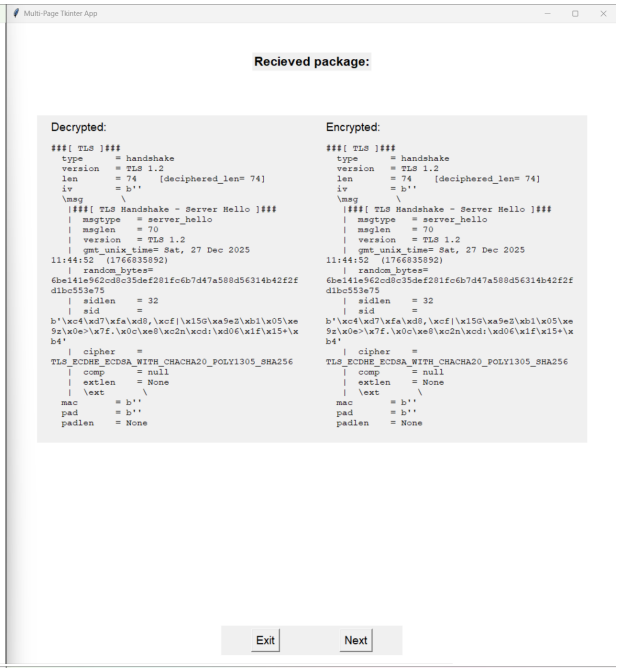

Multi-Page Tkinter App
Recieved package:
Decrypted:
Encrypted:
Exit
Next

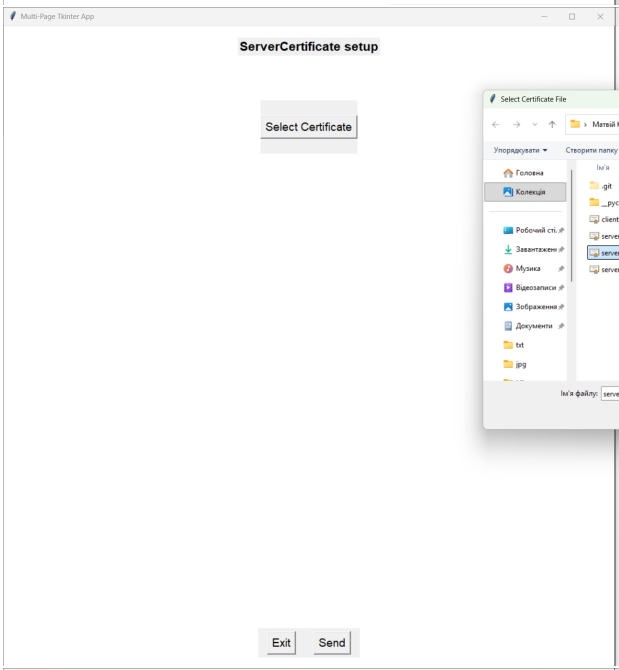

Multi-Page Tkinter App
Sent package:
Decrypted:
Encrypted:
Exit
Next

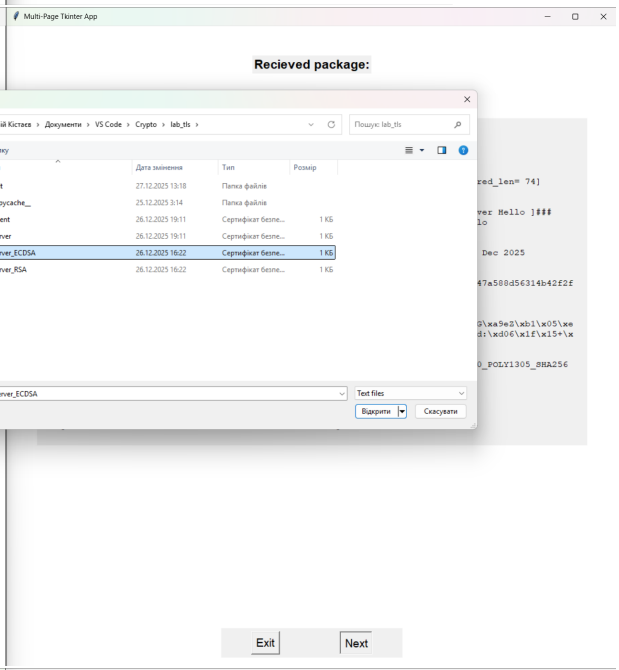

Multi-Page Tkinter App
ServerHello setup
TLS_DHE_RSA_WITH_AES_128_CBC_SHA256
TLS_ECDHE_ECDSA_WITH_AES_128_GCM_SHA256
TLS_ECDHE_ECDSA_WITH_CHACHA20_POLY1305_SHA256
Exit
Send


Multi-Page Tkinter App
Sent package:
Decrypted:
Encrypted:
Exit
Next

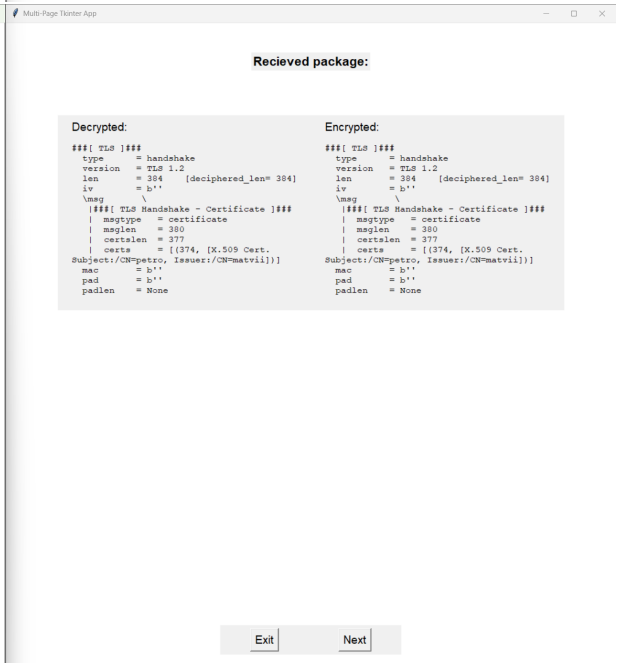

Multi-Page Tkinter App
Sent package:
Decrypted:
###[TLS]###
type = handshake
version = TLS 1.2
len = 74 [deciphered_len= 74]
iv = b''
\msg \
|###[TLS Handshake - Server Hello]###
| msgtype = server_hello
| msglen = 70
| version = TLS 1.2
| gmt_unix_time= Sat, 27 Dec 2025 11:44:52 (1766835892)
| random_bytes= 6be141e962cd8c35def281fc6b7d47a588d56314b42f2fd1bc553e75
| sidlen = 32
| sid = b'\xc4\xd7\xfa\xd8,\xcf|\x15G\xa9e2\xb1\x05\xe9z\x0e>\x7f.\x0c\xe8\xc2n\xcd:\xd06\x1f\x15+\xb4'
| cipher = TLS_ECDHE_ECDSA_WITH_CHACHA20_POLY1305_SHA256
| comp = null
| extlen = None
| \ext \
mac = b''
pad = b''
padlen = None
Encrypted:
###[TLS]###
type = handshake
version = TLS 1.2
len = 74 [deciphered_len= 74]
iv = b''
\msg \
|###[TLS Handshake - Server Hello]###
| msgtype = server_hello
| msglen = 70
| version = TLS 1.2
| gmt_unix_time= Sat, 27 Dec 2025 11:44:52 (1766835892)
| random_bytes= 6be141e962cd8c35def281fc6b7d47a588d56314b42f2fd1bc553e75
| sidlen = 32
| sid = b'\xc4\xd7\xfa\xd8,\xcf|\x15G\xa9e2\xb1\x05\xe9z\x0e>\x7f.\x0c\xe8\xc2n\xcd:\xd06\x1f\x15+\xb4'
| cipher = TLS_ECDHE_ECDSA_WITH_CHACHA20_POLY1305_SHA256
| comp = null
| extlen = None
| \ext \
mac = b''
pad = b''
padlen = None
Exit
Next


Multi-Page Tkinter App
Recieved package:
Decrypted:
###[TLS]###
type = handshake
version = TLS 1.2
len = 74 [deciphered_len= 74]
iv = b''
\msg \
|###[TLS Handshake - Server Hello]###
| msgtype = server_hello
| msglen = 70
| version = TLS 1.2
| gmt_unix_time= Sat, 27 Dec 2025 11:44:52 (1766835892)
| random_bytes= 6be141e962cd8c35def281fc6b7d47a588d56314b42f2fd1bc553e75
| sidlen = 32
| sid = b'\xc4\xd7\xfa\xd8,\xcf|\x15G\xa9e2\xb1\x05\xe9z\x0e>\x7f.\x0c\xe8\xc2n\xcd:\xd06\x1f\x15+\xb4'
| cipher = TLS_ECDHE_ECDSA_WITH_CHACHA20_POLY1305_SHA256
| comp = null
| extlen = None
| \ext \
mac = b''
pad = b''
padlen = None
Encrypted:
###[TLS]###
type = handshake
version = TLS 1.2
len = 74 [deciphered_len= 74]
iv = b''
\msg \
|###[TLS Handshake - Server Hello]###
| msgtype = server_hello
| msglen = 70
| version = TLS 1.2
| gmt_unix_time= Sat, 27 Dec 2025 11:44:52 (1766835892)
| random_bytes= 6be141e962cd8c35def281fc6b7d47a588d56314b42f2fd1bc553e75
| sidlen = 32
| sid = b'\xc4\xd7\xfa\xd8,\xcf|\x15G\xa9e2\xb1\x05\xe9z\x0e>\x7f.\x0c\xe8\xc2n\xcd:\xd06\x1f\x15+\xb4'
| cipher = TLS_ECDHE_ECDSA_WITH_CHACHA20_POLY1305_SHA256
| comp = null
| extlen = None
| \ext \
mac = b''
pad = b''
padlen = None
Exit
Next

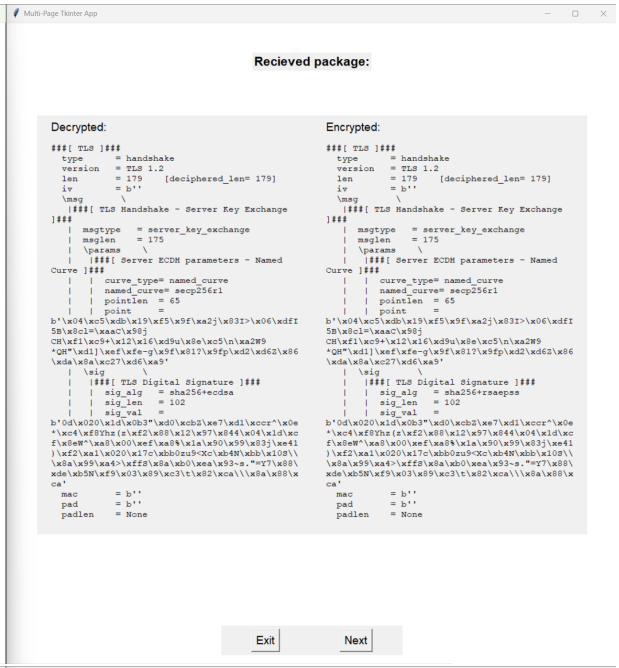

Multi-Page Tkinter App
ServerCertificate setup
Select Certificate
Exit
Send


Multi-Page Tkinter App
Recieved package:
Select Certificate File
server_ECDSA
server_RSA
Відкрити
Скасувати
Exit
Next

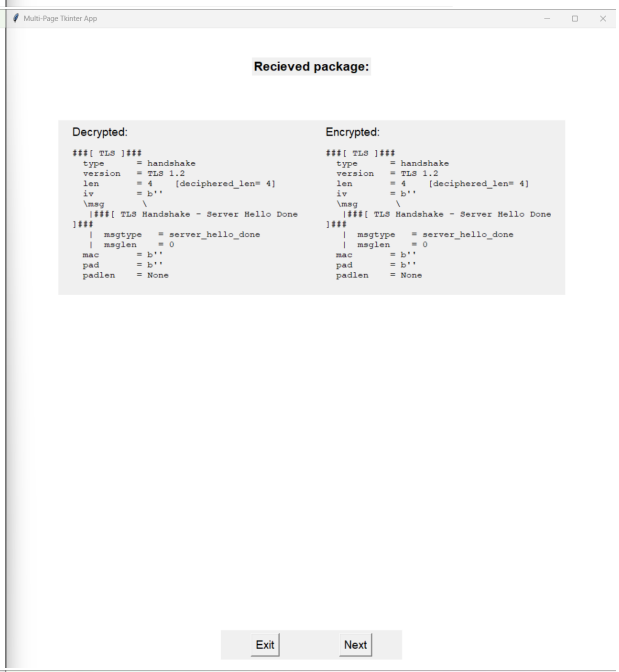

Multi-Page Tkinter App
Sent package:
Decrypted:
###[TLS]###
type = handshake
version = TLS 1.2
len = 384 [deciphered_len= 384]
iv = b''
\msg \
|###[TLS Handshake - Certificate]###
| msgtype = certificate
| msglen = 380
| certslen = 377
| certs = [<374, [X.509 Cert. Subject:/CN=petro, Issuer:/CN=matvii]>]
mac = b''
pad = b''
padlen = None
Encrypted:
###[TLS]###
type = handshake
version = TLS 1.2
len = 384 [deciphered_len= 384]
iv = b''
\msg \
|###[TLS Handshake - Certificate]###
| msgtype = certificate
| msglen = 380
| certslen = 377
| certs = [<374, [X.509 Cert. Subject:/CN=petro, Issuer:/CN=matvii]>]
mac = b''
pad = b''
padlen = None
Exit
Next


Multi-Page Tkinter App
Recieved package:
Decrypted:
###[TLS]###
type = handshake
version = TLS 1.2
len = 384 [deciphered_len= 384]
iv = b''
\msg \
|###[TLS Handshake - Certificate]###
| msgtype = certificate
| msglen = 380
| certslen = 377
| certs = [<374, [X.509 Cert. Subject:/CN=petro, Issuer:/CN=matvii]>]
mac = b''
pad = b''
padlen = None
Encrypted:
###[TLS]###
type = handshake
version = TLS 1.2
len = 384 [deciphered_len= 384]
iv = b''
\msg \
|###[TLS Handshake - Certificate]###
| msgtype = certificate
| msglen = 380
| certslen = 377
| certs = [<374, [X.509 Cert. Subject:/CN=petro, Issuer:/CN=matvii]>]
mac = b''
pad = b''
padlen = None
Exit
Next


Multi-Page Tkinter App
Sent package:
Decrypted:
###[TLS]###
type = handshake
version = TLS 1.2
len = 179 [deciphered_len= 179]
iv = b''
\msg \
|###[TLS Handshake - Server Key Exchange
]###
| msgtype = server_key_exchange
| msglen = 175
| \params \
| |###[Server ECDH parameters - Named
Curve]###
| | curve_type= named_curve
| | named_curve= secp256r1
| | pointlen = 65
| | point =
b'\x04\xc5\xdb\x19\xf5\x9f\xa2j\x83I>\x06\xdfI
5B\x8cl=\xaaC\x98j
CH\xf1\xc9+\x12\x16\xd9u\x8e\xc5\n\xa2W9
*QH"\xd1]\xef\xfe-g\x9f\x817\x9fp\xd2\xd62\x86
\xda\x8a\xc27\xd6\xa9'
| \sig \
| |###[TLS Digital Signature]###
| | sig_alg = sha256+ecdsa
| | sig_len = 102
| | sig_val =
b'0d\x020\x1d\x0b3"\xd0\xcb2\xe7\xd1\xccr^\x0e
*\xc4\xf8Yhz(\xf2\x88\x12\x97\x844\x04\x1d\xc
f\x8eW"\xa8\x00\xef\xa8%\x1a\x90\x99\x83j\xe41
)\xf2\xa1\x020\x17c\xbb0zu9<Xc\xb4M\xbb\x108\\
\x8a\x99\xa4>\xff8\x8a\xb0\xea\x93~s."Y7\88\
xde\xb5N\xf9\x03\x89\xc3\t\x82\xca\\\x8a\x88\x
ca'
mac = b''
pad = b''
padlen = None
Encrypted:
###[TLS]###
type = handshake
version = TLS 1.2
len = 179 [deciphered_len= 179]
iv = b''
\msg \
|###[TLS Handshake - Server Key Exchange
]###
| msgtype = server_key_exchange
| msglen = 175
| \params \
| |###[Server ECDH parameters - Named
Curve]###
| | curve_type= named_curve
| | named_curve= secp256r1
| | pointlen = 65
| | point =
b'\x04\xc5\xdb\x19\xf5\x9f\xa2j\x83I>\x06\xdfI
5B\x8cl=\xaaC\x98j
CH\xf1\xc9+\x12\x16\xd9u\x8e\xc5\n\xa2W9
*QH"\xd1]\xef\xfe-g\x9f\x817\x9fp\xd2\xd62\x86
\xda\x8a\xc27\xd6\xa9'
| \sig \
| |###[TLS Digital Signature]###
| | sig_alg = sha256+rsaepss
| | sig_len = 102
| | sig_val =
b'0d\x020\x1d\x0b3"\xd0\xcb2\xe7\xd1\xccr^\x0e
*\xc4\xf8Yhz(\xf2\x88\x12\x97\x844\x04\x1d\xc
f\x8eW"\xa8\x00\xef\xa8%\x1a\x90\x99\x83j\xe41
)\xf2\xa1\x020\x17c\xbb0zu9<Xc\xb4M\xbb\x108\\
\x8a\x99\xa4>\xff8\x8a\xb0\xea\x93~s."Y7\88\
xde\xb5N\xf9\x03\x89\xc3\t\x82\xca\\\x8a\x88\x
ca'
mac = b''
pad = b''
padlen = None
Exit
Next


Multi-Page Tkinter App
Recieved package:
Decrypted:
###[TLS]###
type = handshake
version = TLS 1.2
len = 179 [deciphered_len= 179]
iv = b''
\msg \
|###[TLS Handshake - Server Key Exchange
]###
| msgtype = server_key_exchange
| msglen = 175
| \params \
| |###[Server ECDH parameters - Named
Curve]###
| | curve_type= named_curve
| | named_curve= secp256r1
| | pointlen = 65
| | point =
b'\x04\xc5\xdb\x19\xf5\x9f\xa2j\x83I>\x06\xdfI
5B\x8cl=\xaaC\x98j
CH\xf1\xc9+\x12\x16\xd9u\x8e\xc5\n\xa2W9
*QH"\xd1]\xef\xfe-g\x9f\x817\x9fp\xd2\xd62\x86
\xda\x8a\xc27\xd6\xa9'
| \sig \
| |###[TLS Digital Signature]###
| | sig_alg = sha256+ecdsa
| | sig_len = 102
| | sig_val =
b'0d\x020\x1d\x0b3"\xd0\xcb2\xe7\xd1\xccr^\x0e
*\xc4\xf8Yhz(\xf2\x88\x12\x97\x844\x04\x1d\xc
f\x8eW"\xa8\x00\xef\xa8%\x1a\x90\x99\x83j\xe41
)\xf2\xa1\x020\x17c\xbb0zu9<Xc\xb4M\xbb\x108\\
\x8a\x99\xa4>\xff8\x8a\xb0\xea\x93~s."Y7\88\
xde\xb5N\xf9\x03\x89\xc3\t\x82\xca\\\x8a\x88\x
ca'
mac = b''
pad = b''
padlen = None
Encrypted:
###[TLS]###
type = handshake
version = TLS 1.2
len = 179 [deciphered_len= 179]
iv = b''
\msg \
|###[TLS Handshake - Server Key Exchange
]###
| msgtype = server_key_exchange
| msglen = 175
| \params \
| |###[Server ECDH parameters - Named
Curve]###
| | curve_type= named_curve
| | named_curve= secp256r1
| | pointlen = 65
| | point =
b'\x04\xc5\xdb\x19\xf5\x9f\xa2j\x83I>\x06\xdfI
5B\x8cl=\xaaC\x98j
CH\xf1\xc9+\x12\x16\xd9u\x8e\xc5\n\xa2W9
*QH"\xd1]\xef\xfe-g\x9f\x817\x9fp\xd2\xd62\x86
\xda\x8a\xc27\xd6\xa9'
| \sig \
| |###[TLS Digital Signature]###
| | sig_alg = sha256+rsaepss
| | sig_len = 102
| | sig_val =
b'0d\x020\x1d\x0b3"\xd0\xcb2\xe7\xd1\xccr^\x0e
*\xc4\xf8Yhz(\xf2\x88\x12\x97\x844\x04\x1d\xc
f\x8eW"\xa8\x00\xef\xa8%\x1a\x90\x99\x83j\xe41
)\xf2\xa1\x020\x17c\xbb0zu9<Xc\xb4M\xbb\x108\\
\x8a\x99\xa4>\xff8\x8a\xb0\xea\x93~s."Y7\88\
xde\xb5N\xf9\x03\x89\xc3\t\x82\xca\\\x8a\x88\x
ca'
mac = b''
pad = b''
padlen = None
Exit
Next


Multi-Page Tkinter App
Sent package:
Decrypted:
###[TLS]###
type = handshake
version = TLS 1.2
len = 4 [deciphered_len= 4]
iv = b''
\msg \
|###[TLS Handshake - Server Hello Done
]###
| msgtype = server_hello_done
| msglen = 0
mac = b''
pad = b''
padlen = None
Encrypted:
###[TLS]###
type = handshake
version = TLS 1.2
len = 4 [deciphered_len= 4]
iv = b''
\msg \
|###[TLS Handshake - Server Hello Done
]###
| msgtype = server_hello_done
| msglen = 0
mac = b''
pad = b''
padlen = None
Exit
Next


Multi-Page Tkinter App
Recieved package:
Decrypted:
###[TLS]###
type = handshake
version = TLS 1.2
len = 4 [deciphered_len= 4]
iv = b''
\msg \
|###[TLS Handshake - Server Hello Done
]###
| msgtype = server_hello_done
| msglen = 0
mac = b''
pad = b''
padlen = None
Encrypted:
###[TLS]###
type = handshake
version = TLS 1.2
len = 4 [deciphered_len= 4]
iv = b''
\msg \
|###[TLS Handshake - Server Hello Done
]###
| msgtype = server_hello_done
| msglen = 0
mac = b''
pad = b''
padlen = None
Exit
Next

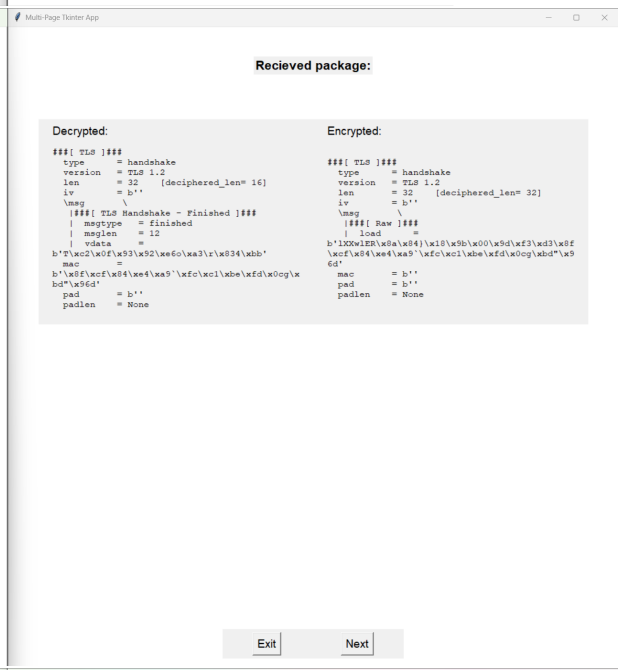

Multi-Page Tkinter App
Recieved package:
Decrypted:
###[TLS]###
type = handshake
version = TLS 1.2
len = 70 [deciphered_len= 70]
iv = b''
\msg \
|###[TLS Handshake - Client Key Exchange
]###
| msgtype = client_key_exchange
| msglen = 66
| \exchkeys \
| |###[Client ECDH Public Value]###
| | ecdh_Yclen= 65
| | ecdh_Yc =
b'\x04J\xb3(\xce\xc4\xd6Q\\\x05\xb9\x9f\xa79Pg
\xbep\x1c\x0en\xba%\xbbbC.\xe4\x8e\x9cXc\x1ff0
\\\xc2\xe3l#|\xf5\xb3\xb4f\xef\x80T\x93\xdcNe\
xdeK#\x03ci\xd2m\xbe\xbcx\x80s'
mac = b''
pad = b''
padlen = None
Encrypted:
###[TLS]###
type = handshake
version = TLS 1.2
len = 70 [deciphered_len= 70]
iv = b''
\msg \
|###[TLS Handshake - Client Key Exchange
]###
| msgtype = client_key_exchange
| msglen = 66
| \exchkeys \
| |###[Raw]###
| | load =
b'A\x04J\xb3(\xce\xc4\xd6Q\\\x05\xb9\x9f\xa79P
g\xbep\x1c\x0en\xba%\xbbbC.\xe4\x8e\x9cXc\x1ff
0\\\xc2\xe3l#|\xf5\xb3\xb4f\xef\x80T\x93\xdcNe
\xdeK#\x03ci\xd2m\xbe\xbcx\x80s'
mac = b''
pad = b''
padlen = None
Exit
Next


Multi-Page Tkinter App
Sent package:
Decrypted:
###[TLS]###
type = handshake
version = TLS 1.2
len = 70 [deciphered_len= 70]
iv = b''
\msg \
|###[TLS Handshake - Client Key Exchange
]###
| msgtype = client_key_exchange
| msglen = 66
| \exchkeys \
| |###[Client ECDH Public Value]###
| | ecdh_Yclen= 65
| | ecdh_Yc =
b'\x04J\xb3(\xce\xc4\xd6Q\\\x05\xb9\x9f\xa79Pg
\xbep\x1c\x0en\xba%\xbbbC.\xe4\x8e\x9cXc\x1ff0
\\\xc2\xe3l#|\xf5\xb3\xb4f\xef\x80T\x93\xdcNe\
xdeK#\x03ci\xd2m\xbe\xbcx\x80s'
mac = b''
pad = b''
padlen = None
Encrypted:
###[TLS]###
type = handshake
version = TLS 1.2
len = 70 [deciphered_len= 70]
iv = b''
\msg \
|###[TLS Handshake - Client Key Exchange
]###
| msgtype = client_key_exchange
| msglen = 66
| \exchkeys \
| |###[Raw]###
| | load =
b'A\x04J\xb3(\xce\xc4\xd6Q\\\x05\xb9\x9f\xa79P
g\xbep\x1c\x0en\xba%\xbbbC.\xe4\x8e\x9cXc\x1ff
0\\\xc2\xe3l#|\xf5\xb3\xb4f\xef\x80T\x93\xdcNe
\xdeK#\x03ci\xd2m\xbe\xbcx\x80s'
mac = b''
pad = b''
padlen = None
Exit
Next


Multi-Page Tkinter App
Recieved package:
Decrypted:
###[TLS]###
type = handshake
version = TLS 1.2
len = 32 [deciphered_len= 16]
iv = b''
\msg \
|###[TLS Handshake - Finished]###
| msgtype = finished
| msglen = 12
| vdata =
b'\x1c7\x80\x8a\xa7\xdch\x86\x7f2j\n'
mac =
b'\x059Y\x07\xa0*G\n8\xfb\x04\x03\x0ebG\xf8'
pad = b''
padlen = None
Encrypted:
###[TLS]###
type = handshake
version = TLS 1.2
len = 32 [deciphered_len= 32]
iv = b''
\msg \
|###[Raw]###
| load =
b'\\V\xb00\xae\xdd\x13ee)8x\xbeG\xce|\x059Y\x0
7\xa0*G\n8\xfb\x04\x03\x0ebG\xf8'
mac = b''
pad = b''
padlen = None
Exit
Next


Multi-Page Tkinter App
Sent package:
Decrypted:
###[TLS]###
type = handshake
version = TLS 1.2
len = 32 [deciphered_len= 16]
iv = b''
\msg \
|###[TLS Handshake - Finished]###
| msgtype = finished
| msglen = 12
| vdata =
b'1c7\x80\x8a\xa7\xdch\x86\x7f2j\n'
mac =
b'\x059Y\x07\xa0*G\n8\xfb\x04\x03\x0ebG\xf8'
pad = b''
padlen = None
Encrypted:
###[TLS]###
type = handshake
version = TLS 1.2
len = 32 [deciphered_len= 32]
iv = b''
\msg \
|###[Raw]###
| load =
b'\\V\xb00\xae\xdd\x13ee)8x\xbeG\xce|\x059Y\x0
7\xa0*G\n8\xfb\x04\x03\x0ebG\xf8'
mac = b''
pad = b''
padlen = None
Exit
Next


Multi-Page Tkinter App
Sent package:
Decrypted:
###[TLS]###
type = handshake
version = TLS 1.2
len = 32 [deciphered_len= 16]
iv = b''
\msg \
|###[TLS Handshake - Finished]###
| msgtype = finished
| msglen = 12
| vdata =
b'T\xc2\x0f\x93\x92\xe6o\xa3\r\x834\xbb'
mac =
b'\x8f\xcf\x84\xe4\xa9`\xfc\xc1\xbe\xfd\x0cg\x
bd"\x96d'
pad = b''
padlen = None
Encrypted:
###[TLS]###
type = handshake
version = TLS 1.2
len = 32 [deciphered_len= 32]
iv = b''
\msg \
|###[Raw]###
| load =
b'1XXwlER\x8a\x84)\x18\x9b\x00\x9d\xf3\xd3\x8f
\xcf\x84\xe4\xa9`\xfc\xc1\xbe\xfd\x0cg\xbd"\x9
6d'
mac = b''
pad = b''
padlen = None
Exit
Next


Multi-Page Tkinter App
Recieved package:
Decrypted:
###[TLS]###
type = handshake
version = TLS 1.2
len = 32 [deciphered_len= 16]
iv = b''
\msg \
|###[TLS Handshake - Finished]###
| msgtype = finished
| msglen = 12
| vdata =
b'T\xc2\x0f\x93\x92\xe6o\xa3\r\x834\xbb'
mac =
b'\x8f\xcf\x84\xe4\xa9`\xfc\xc1\xbe\xfd\x0cg\x
bd"\x96d'
pad = b''
padlen = None
Encrypted:
###[TLS]###
type = handshake
version = TLS 1.2
len = 32 [deciphered_len= 32]
iv = b''
\msg \
|###[Raw]###
| load =
b'1XXwlER\x8a\x84)\x18\x9b\x00\x9d\xf3\xd3\x8f
\xcf\x84\xe4\xa9`\xfc\xc1\xbe\xfd\x0cg\xbd"\x9
6d'
mac = b''
pad = b''
padlen = None
Exit
Next


Multi-Page Tkinter App
Sent package:
Decrypted:
###[TLS]###
type = handshake
version = TLS 1.2
len = 32 [deciphered_len= 16]
iv = b''
\msg \
|###[TLS Handshake - Finished]###
| msgtype = finished
| msglen = 12
| vdata =
b'T\xc2\x0f\x93\x92\xe6o\xa3\r\x834\xbb'
mac =
b'\x8f\xcf\x84\xe4\xa9`\xfc\xc1\xbe\xfd\x0cg\x
bd"\x96d'
pad = b''
padlen = None
Encrypted:
###[TLS]###
type = handshake
version = TLS 1.2
len = 32 [deciphered_len= 32]
iv = b''
\msg \
|###[Raw]###
| load =
b'1XXwlER\x8a\x84)\x18\x9b\x00\x9d\xf3\xd3\x8f
\xcf\x84\xe4\xa9`\xfc\xc1\xbe\xfd\x0cg\xbd"\x9
6d'
mac = b''
pad = b''
padlen = None
Exit
Next


Multi-Page Tkinter App
ClientApplicationData
Test client Application data
Exit
Send


Multi-Page Tkinter App
Recieved package:
Decrypted:
###[TLS]###
type = application_data
version = TLS 1.2
len = 44 [deciphered_len= 28]
iv = b''
\msg \
|###[TLS Application Data]###
| data = b'Test client Application data'
mac =
b'~\x05\x89]\x17x+\x0f\x9d\x88\xfe8\xeb\xd0\xa0\x8c'
pad = b''
padlen = None
Encrypted:
###[TLS]###
type = application_data
version = TLS 1.2
len = 44 [deciphered_len= 44]
iv = b''
\msg \
|###[TLS Application Data]###
| data =
b'\x19\x1a\x8bE0P\xbc\xbb\xfd\x14\x92\xdey/`\x91\x00\xb5\x19\x89\x11\xc8\x1c\xb9\xf2\xcb\xf9z~\x05\x89]\x17x+\x0f\x9d\x88\xfe8\xeb\xd0\xa0\x8c'
mac = b''
pad = b''
padlen = None
Exit
Next


Multi-Page Tkinter App
Sent package:
Decrypted:
###[TLS]###
type = application_data
version = TLS 1.2
len = 44 [deciphered_len= 28]
iv = b''
\msg \
|###[TLS Application Data]###
| data = b'Test client Application data'
mac =
b'~\x05\x89]\x17x+\x0f\x9d\x88\xfe8\xeb\xd0\xa0\x8c'
pad = b''
padlen = None
Encrypted:
###[TLS]###
type = application_data
version = TLS 1.2
len = 44 [deciphered_len= 44]
iv = b''
\msg \
|###[TLS Application Data]###
| data =
b'\x19\x1a\x8bE0P\xbc\xbb\xfd\x14\x92\xdey/`\x91\x00\xb5\x19\x89\x11\xc8\x1c\xb9\xf2\xcb\xf9z~\x05\x89]\x17x+\x0f\x9d\x88\xfe8\xeb\xd0\xa0\x8c'
mac = b''
pad = b''
padlen = None
Exit
Next


Multi-Page Tkinter App
ServerApplicationData
Test Server response data
Exit
Send


Multi-Page Tkinter App
Sent package:
Decrypted:
###[TLS]###
type = application_data
version = TLS 1.2
len = 44 [deciphered_len= 28]
iv = b''
\msg \
|###[TLS Application Data]###
| data = b'Test client Application data'
mac =
b'~\x05\x89]\x17x+\x0f\x9d\x88\xfe8\xeb\xd0\xa0\x8c'
pad = b''
padlen = None
Encrypted:
###[TLS]###
type = application_data
version = TLS 1.2
len = 44 [deciphered_len= 44]
iv = b''
\msg \
|###[TLS Application Data]###
| data =
b'\x19\x1a\x8bE0P\xbc\xbb\xfd\x14\x92\xdey/`\x91\x00\xb5\x19\x89\x11\xc8\x1c\xb9\xf2\xcb\xf9z~\x05\x89]\x17x+\x0f\x9d\x88\xfe8\xeb\xd0\xa0\x8c'
mac = b''
pad = b''
padlen = None
Exit
Next


Multi-Page Tkinter App
Sent package:
Decrypted:
###[TLS]###
type = application_data
version = TLS 1.2
len = 41 [deciphered_len= 25]
iv = b''
\msg \
|###[TLS Application Data]###
| data = b'Test Server response data'
mac =
b'ZWtK\xb1,oU\x1f\xfdQ\x00\x8a\x02\xae\xf3'
pad = b''
padlen = None
Encrypted:
###[TLS]###
type = application_data
version = TLS 1.2
len = 41 [deciphered_len= 41]
iv = b''
\msg \
|###[TLS Application Data]###
| data =
b'\xd2\x17-2\xdaA\x1aL\xc2\x03\x80\xc9\\\x92\xb5F\x18\xc1w\ru\x0f\x14g\xe0ZWtK\xb1,oU\x1f\xfdQ\x00\x8a\x02\xae\xf3'
mac = b''
pad = b''
padlen = None
Exit
Next


Multi-Page Tkinter App
Recieved package:
Decrypted:
###[TLS]###
type = application_data
version = TLS 1.2
len = 41 [deciphered_len= 25]
iv = b''
\msg \
|###[TLS Application Data]###
| data = b'Test Server response data'
mac =
b'ZWtK\xb1,oU\x1f\xfdQ\x00\x8a\x02\xae\xf3'
pad = b''
padlen = None
Encrypted:
###[TLS]###
type = application_data
version = TLS 1.2
len = 41 [deciphered_len= 41]
iv = b''
\msg \
|###[TLS Application Data]###
| data =
b'\xd2\x17-2\xdaA\x1aL\xc2\x03\x80\xc9\\\x92\xb5F\x18\xc1w\ru\x0f\x14g\xe0ZWtK\xb1,oU\x1f\xfdQ\x00\x8a\x02\xae\xf3'
mac = b''
pad = b''
padlen = None
Exit
Next

Перевірка за допомогою WireShark

За допомогою програми WireShark можна переконатись, що все відбувається чесно та коректно, і пакети з відповідним вмістом дійсно надсилаються в такій послідовності та в повному обсязі.

Наведемо так само скріншоти основних повідомлень рукостискання із WireShark:

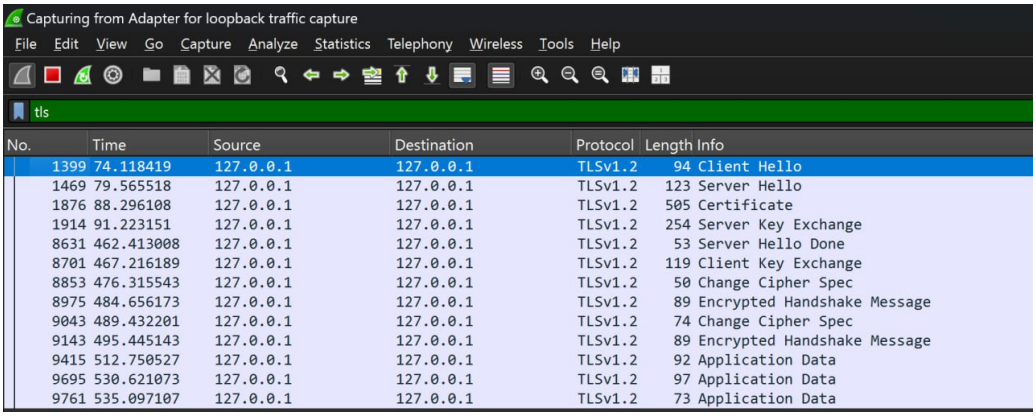
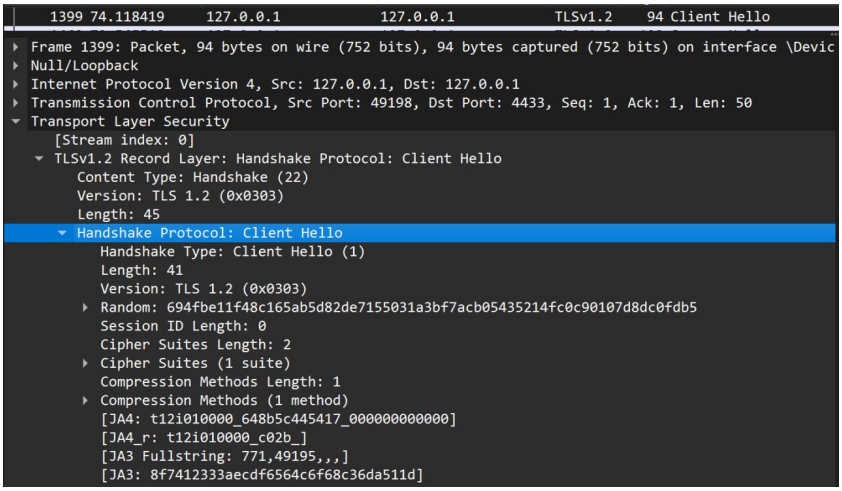
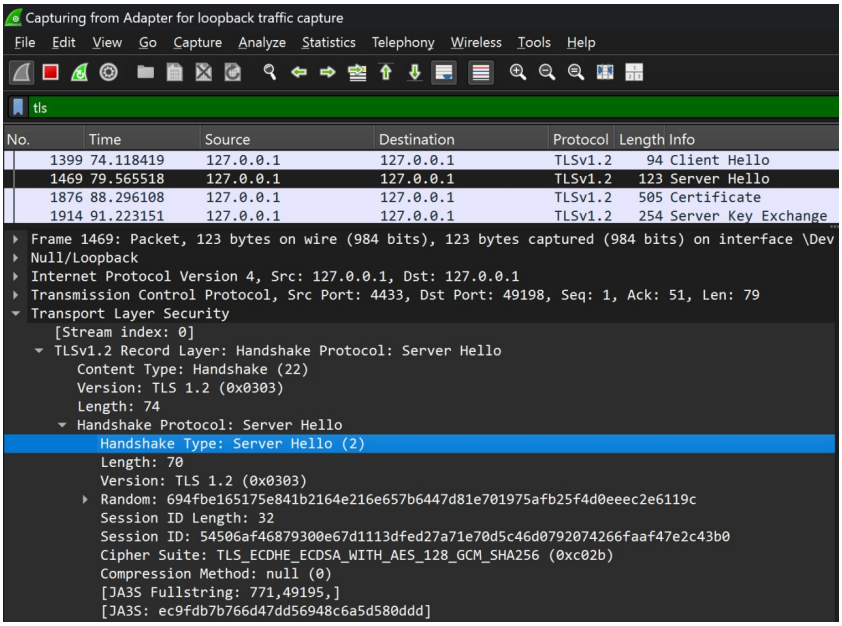
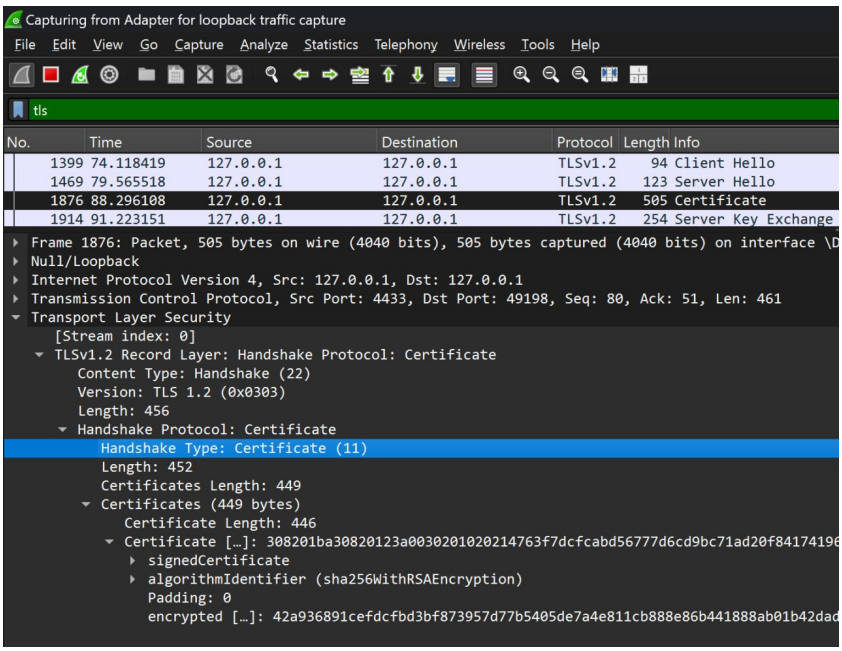
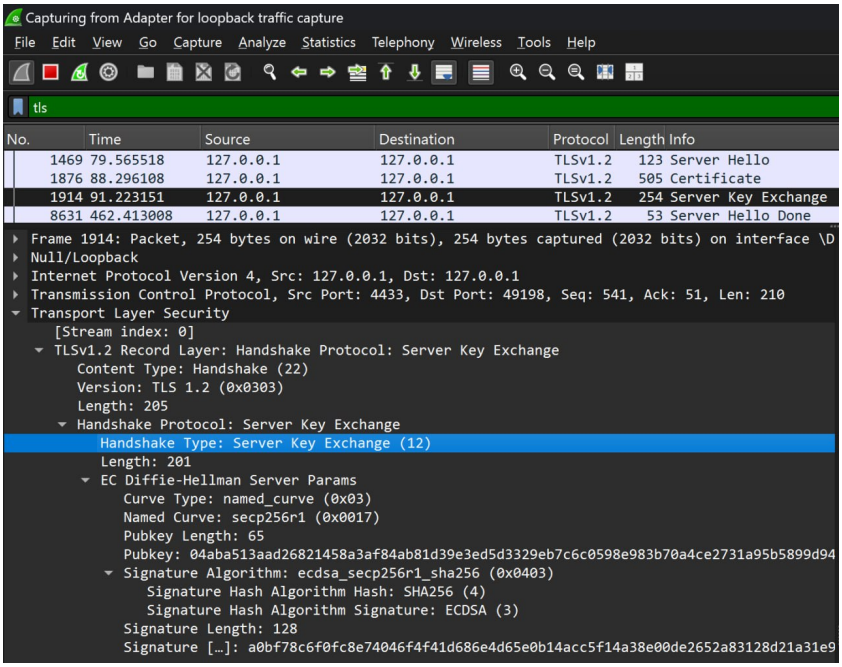


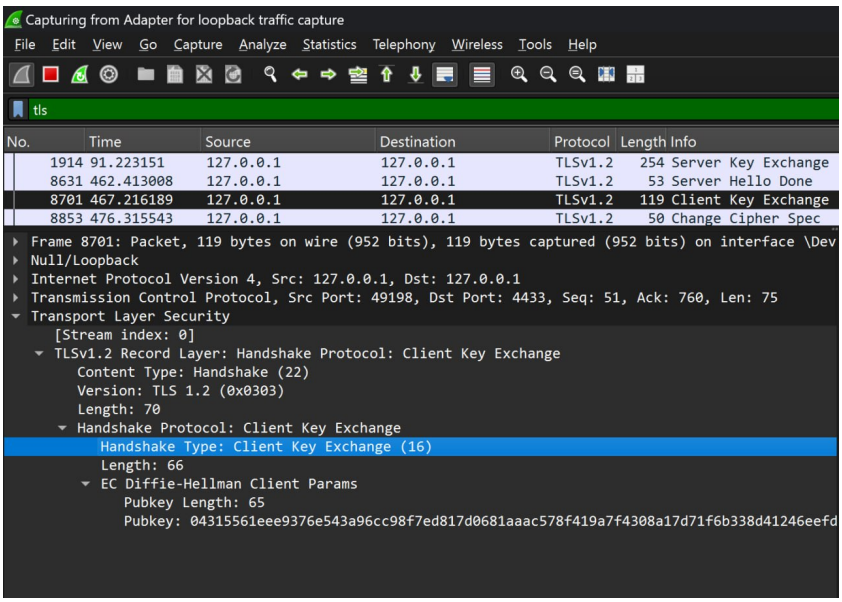
Figure 4: Загальний вигляд усіх надісланих пакетів






Capturing from Adapter for loopback traffic capture
File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help
tls
No. Time Source Destination Protocol Length Info
1399 74.118419 127.0.0.1 127.0.0.1 TLSv1.2 94 Client Hello
1469 79.565518 127.0.0.1 127.0.0.1 TLSv1.2 123 Server Hello
1876 88.296108 127.0.0.1 127.0.0.1 TLSv1.2 505 Certificate
1914 91.223151 127.0.0.1 127.0.0.1 TLSv1.2 254 Server Key Exchange
Frame 1876: Packet, 505 bytes on wire (4040 bits), 505 bytes captured (4040 bits) on interface \D
Null/Loopback
Internet Protocol Version 4, Src: 127.0.0.1, Dst: 127.0.0.1
Transmission Control Protocol, Src Port: 4433, Dst Port: 49198, Seq: 80, Ack: 51, Len: 461
Transport Layer Security
[Stream index: 0]
TLSv1.2 Record Layer: Handshake Protocol: Certificate
Content Type: Handshake (22)
Version: TLS 1.2 (0x0303)
Length: 456
Handshake Protocol: Certificate
Handshake Type: Certificate (11)
Length: 452
Certificates Length: 449
Certificates (449 bytes)
Certificate Length: 446
Certificate […]: 308201ba30820123a003020102021476 3f7dcfcabd56777d6cd9bc71ad20f8417419
signedCertificate
algorithmIdentifier (sha256WithRSAEncryption)
Padding: 0
encrypted […]: 42a936891cefdcfbd3bf873957d77b5405de7a4e811cb888e86b441888ab01b42dad


Capturing from Adapter for loopback traffic capture
File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help
tls
No. Time Source Destination Protocol Length Info
1469 79.565518 127.0.0.1 127.0.0.1 TLSv1.2 123 Server Hello
1876 88.296108 127.0.0.1 127.0.0.1 TLSv1.2 505 Certificate
1914 91.223151 127.0.0.1 127.0.0.1 TLSv1.2 254 Server Key Exchange
8631 462.413008 127.0.0.1 127.0.0.1 TLSv1.2 53 Server Hello Done
Frame 1914: Packet, 254 bytes on wire (2032 bits), 254 bytes captured (2032 bits) on interface \D
Null/Loopback
Internet Protocol Version 4, Src: 127.0.0.1, Dst: 127.0.0.1
Transmission Control Protocol, Src Port: 4433, Dst Port: 49198, Seq: 541, Ack: 51, Len: 210
Transport Layer Security
[Stream index: 0]
TLSv1.2 Record Layer: Handshake Protocol: Server Key Exchange
Content Type: Handshake (22)
Version: TLS 1.2 (0x0303)
Length: 205
Handshake Protocol: Server Key Exchange
Handshake Type: Server Key Exchange (12)
Length: 201
EC Diffie-Hellman Server Params
Curve Type: named_curve (0x03)
Named Curve: secp256r1 (0x0017)
Pubkey Length: 65
Pubkey: 04aba513aad26821458a3af84ab81d39e3ed5d3329eb7c6c0598e983b70a4ce2731a95b5899d94
Signature Algorithm: ecdsa_secp256r1_sha256 (0x0403)
Signature Hash Algorithm Hash: SHA256 (4)
Signature Hash Algorithm Signature: ECDSA (3)
Signature Length: 128
Signature […]: a0bf78c6f0fc8e74046f4f41d686e4d65e0b14acc5f14a38e00de2652a83128d21a31e9


Capturing from Adapter for loopback traffic capture
File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help
tls
No. Time Source Destination Protocol Length Info
1914 91.223151 127.0.0.1 127.0.0.1 TLSv1.2 254 Server Key Exchange
8631 462.413008 127.0.0.1 127.0.0.1 TLSv1.2 53 Server Hello Done
8701 467.216189 127.0.0.1 127.0.0.1 TLSv1.2 119 Client Key Exchange
8853 476.315543 127.0.0.1 127.0.0.1 TLSv1.2 50 Change Cipher Spec
Frame 8701: Packet, 119 bytes on wire (952 bits), 119 bytes captured (952 bits) on interface \Dev
Null/Loopback
Internet Protocol Version 4, Src: 127.0.0.1, Dst: 127.0.0.1
Transmission Control Protocol, Src Port: 49198, Dst Port: 4433, Seq: 51, Ack: 760, Len: 75
Transport Layer Security
[Stream index: 0]
TLSv1.2 Record Layer: Handshake Protocol: Client Key Exchange
Content Type: Handshake (22)
Version: TLS 1.2 (0x0303)
Length: 70
Handshake Protocol: Client Key Exchange
Handshake Type: Client Key Exchange (16)
Length: 66
EC Diffie-Hellman Client Params
Pubkey Length: 65
Pubkey: 04315561eee9376e543a96cc98f7ed817d0681aaac578f419a7f4308a17d71f6b338d41246eefd

Висновки

В даній роботі було розроблено додаток для симуляції захищеної комунікації сервера та клієнта по протоколу TLS версії 1.2. Було використано низькорівневу бібліотеку для роботи з мережевими пакетами, що дозволило ретельно дослідити особливості роботи протоколу TLS, включно із етапом рукостискання.

Також ми ретельно розібрались із внутрішньою організацією мережевої бібліотеки `Scapy` для `Python`, а також особливостями реалізації криптографічних механізмів в цій бібліотеці та `Python` в цілому.

Було отримано практичний досвід роботи із протоколом TLS, було ретельніше досліджено його документацію, а також особливості його імплементації.