

ĐẠI HỌC QUỐC GIA THÀNH PHỐ HỒ CHÍ MINH
TRƯỜNG ĐẠI HỌC CÔNG NGHỆ THÔNG TIN

KHOA MẠNG MÁY TÍNH VÀ TRUYỀN THÔNG



BÁO CÁO: LAB05 – BÀI TẬP TẠI LỚP
MÔN HỌC: MẬT MÃ HỌC

Giảng viên thực hành: ThS. NGUYỄN BÙI KIM NGÂN
Lớp: NT209.Q12.ANTT
Sinh viên thực hiện: NGUYỄN HOÀNG QUÝ – 24521494

Thành phố Hồ Chí Minh, tháng 11 năm 2025

Mục lục

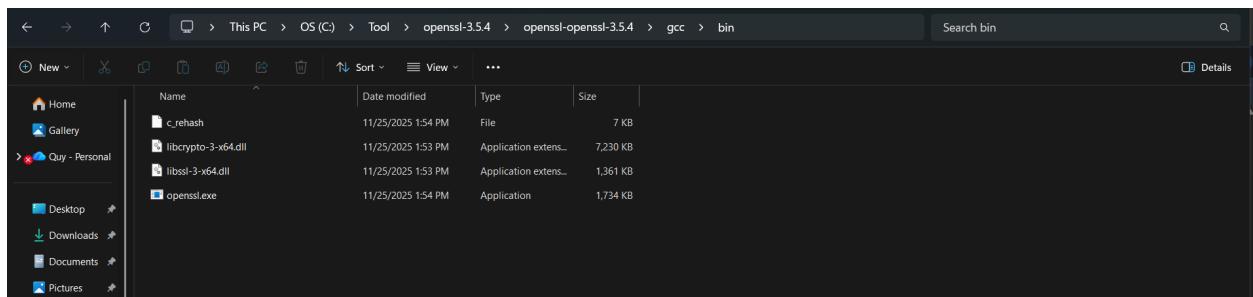
1	Compile OpenSSL	2
1.1	Target	2
1.2	GCC	2
1.3	Clang	2
1.4	MSVC	3
1.5	Ubuntu	3
2	Excute OpenSSL command	3
2.1	Target	3
2.2	Result	4
3	Apache Https Hosts	4
3.1	Target	4
3.2	Proof	5

1 Compile OpenSSL

1.1 Target

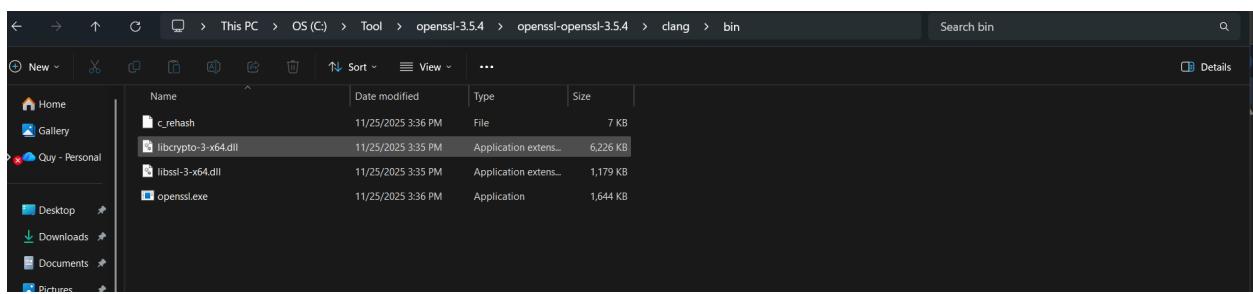
- Compile thành công thư viện OpenSSL trong các môi trường như gcc, clang, msvc, linux.
- Chụp ảnh minh chứng compile thành công.

1.2 GCC



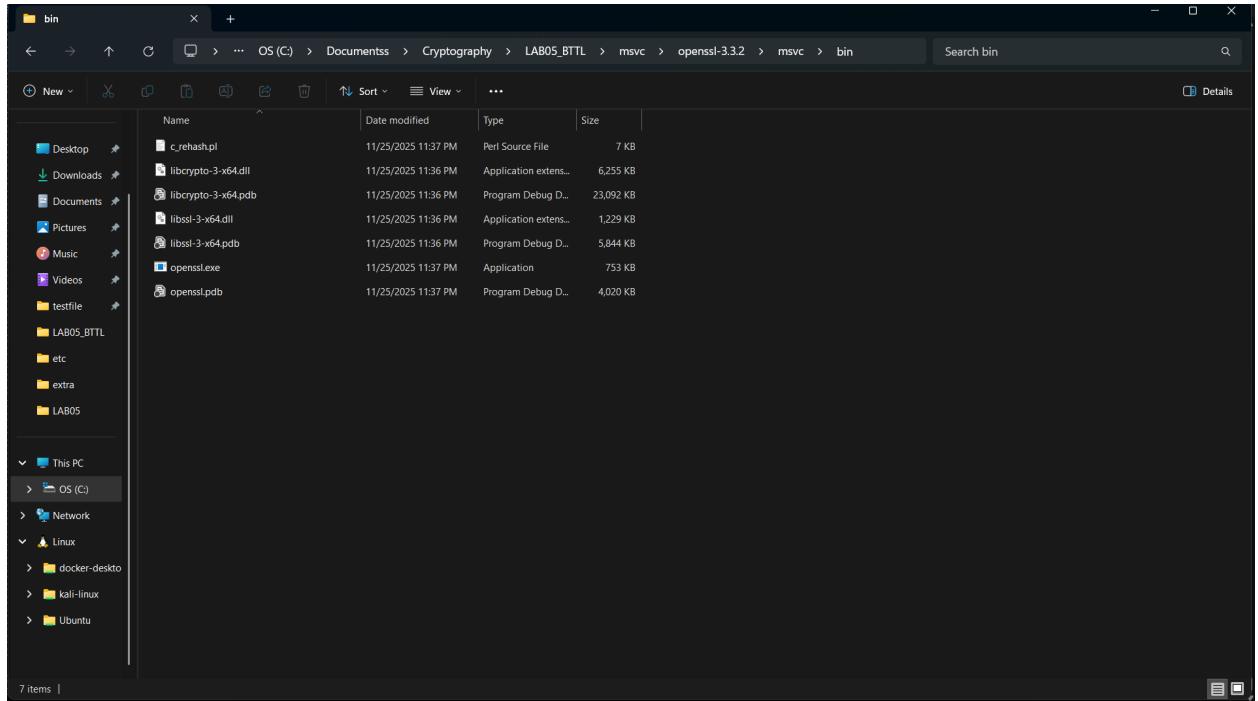
Hình 1: File openssl.exe được compile thành công trong thư mục gcc

1.3 Clang



Hình 2: File openssl.exe được compile thành công trong thư mục clang

1.4 MSVC



Hình 3: File openssl.exe được compile thành công trong thư mục msvc

1.5 Ubuntu

```
quy@quy-ASUS-TUF-Gaming-F15-FX507VV-FX507VV:~/openssl$ ls
openssl-3.2.1 openssl321 openssl-3.2.1.tar.gz
quy@quy-ASUS-TUF-Gaming-F15-FX507VV-FX507VV:~/openssl$ cd openssl321/
quy@quy-ASUS-TUF-Gaming-F15-FX507VV-FX507VV:~/openssl/openssl321$ ls
bin certs ct_log_list.cnf ct_log_list.cnf.dist include lib64 misc openssl.cnf openssl.cnf.dist private share
quy@quy-ASUS-TUF-Gaming-F15-FX507VV-FX507VV:~/openssl/openssl321$ ./openssl
c_rehash openssl
quy@quy-ASUS-TUF-Gaming-F15-FX507VV-FX507VV:~/openssl/openssl321$ file bin/openssl
bin/openssl: ELF 64-bit LSB pie executable, x86-64, version 1 (SYSV), dynamically linked, interpreter /lib64/ld-linux-x86-64.so.2, BuildID[sha1]=572323a0fb659e6b47e2cbc1474176b7342f025
8, for GNU/Linux 3.2.0, not stripped
quy@quy-ASUS-TUF-Gaming-F15-FX507VV-FX507VV:~/openssl/openssl321$
```

Hình 4: File openssl.exe được compile thành công trong thư mục ubuntu

2 Execute OpenSSL command

2.1 Target

- Thực thi thành công các câu lệnh trong file **4_x509-openssl.txt**
- Chụp ảnh minh chứng kết quả thực thi thành công.

2.2 Result

The screenshot shows a terminal window with the following content:

```
PS C:\Documents\.Cryptography\LAB05_BTTL\task4> C:\Tool\openssl-1.3.5A\openssl-1.3.5A\gcc\bin\openssl.exe eparam -list_curves
>> >> C:\Tool\openssl-1.3.5A\openssl-1.3.5A\gcc\bin\openssl.exe eparam -name prime256v1 -genkey -noout -out ec-private-key.pem
>> >> C:\Tool\openssl-1.3.5A\openssl-1.3.5A\gcc\bin\openssl.exe ec -in ec-private-key.pem -pubout -out ec-public-key.pem
secp128r1 : SEC/GWTLS curve over a 112 bit prime field
ln 44 Col 1 (113 selected) Spaces: 4 UTF-8 CRLF ( Plain Text Go Live Prettier
```

The terminal is running on Windows and executing OpenSSL commands. It lists curves, generates an EC private key, and creates an EC public key from it. The output includes the X509v3 Subject Key Identifier and Signature Algorithm.

Terminal Output (Continued):

```
X509v3 Subject Key Identifier:
E1:A7:33:5C:08:26:71:19:2C:43:69:7D:2B:86:CF:ED:65:1C:27:92
Signature Algorithm: sha256WithRSAEncryption
Signature Value:
33:de:3c:f3:25:5f:92:1a:db:95:a1:5c:7a:14:0b:01:12:d2:
6f:52:a4:ba:69:46:45:c9:ca:16:a5:01:11:35:61:91:06:46:
48:ed:09:b5:36:ed:a3:09:09:34:ae:4b:f5:f1:bc:c8:e4:ee:
d9:44:e9:ed:6e:af:b7:ff:f2:30:9b:0d:cd:72:f4:01:53:73:
5d:ac:5d:7d:16:ec:c1:01:3e:8b:29:b7:f3:3b:ce:f4:80:ae:
19:2a:ea:bd:fd:0f:ab:7a:96:98:ae:a2:bd:4d:3e:ca:3e:3f:
0b:5d:ba:f9:78:b3:cc:88:rd:2:e5:57:d4:36:92:24:fg:15:99:
46:9b:fa:66:xd:ad:fe:c1:09:33:69:d4:51:be:c5:eb:93:ea:
0c:53:bd:c8:ad:bc:bf:a9:dd:09:1a:7b:5d:c5:cd:be:2c:
65:ba:27:7f:b4:12:d1:3f:a8:7d:75:17:0e:a0:31:ca:8f:22:
04:a1:ec:06:ie:74:dd:b7:85:ca:9c:f1:25:27:a4:77:c7:81:
11:61:16:69:c3:8e:7a:b7:22:36:8d:df:2:40:8d:09:c2:74:
55:0b:3e:f2:a5:4b:3a:46:14:17:f1:6d:a1:fe:ff:c2:99:81:
5d:84:dd:8b:cb:0f:06:99:c0:eb:a9:b2:79:6e:4a:9e:f9:70:
2d:7e:ze:f1:11:97:e8:66:d0:bd:36:50:65:c7:dc:c2:04:9b:
10:94:03:fe:46:3e:4a:9f:9e:06:0b:a8:9c:7d:c6:62:27:39:
fa:83:41:c5:f0:b3:d0:36:13:4b:38:ad:ac:96:d3:30:51:21:
d9:9d:33:57:7d:66:d2:a3:05:68:33:3e:4e:42:63:72:21:06:
99:46:03:13:ff:f7:47:d7:ef:a2:f4:5d:a8:c3:6f:0f:25:fc:
98:51:8a:99:bb:68:c1:df:fe:a1:h2:02:54:17:05:f5:ed:8a:1a:5c:
91:73:31:ca:3f:10:75:32:85:0e:56:4b:50:f9:40:7c:af:
bd:a4:f9:98:7e:7b
```

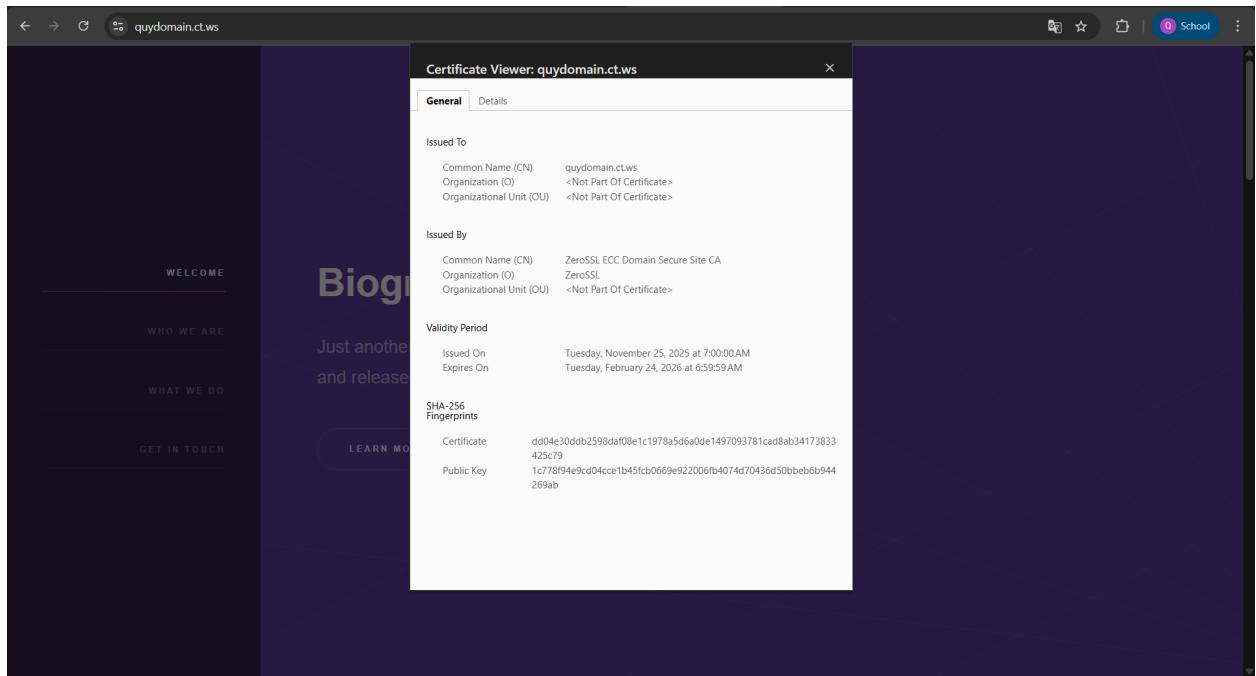
Hình 5: Minh chứng thực thi câu lệnh OpenSSL

3 Apache Https Hosts

3.1 Target

- Chụp ảnh minh chứng domain hosts bằng giao thức https.

3.2 Proof



Hình 6: Minh chứng domain sử dụng giao thức https