

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

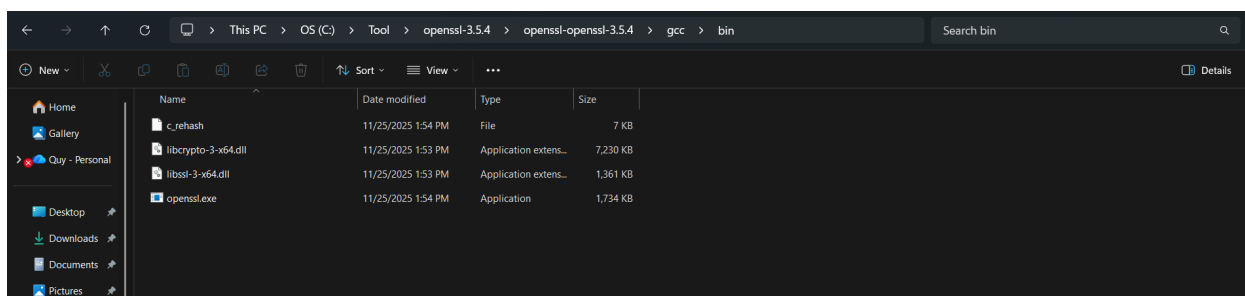
1	Compile OpenSSL	2
1.1	Target	2
1.2	GCC	2
1.3	Clang	2
1.4	MSVC	3
1.5	Ubuntu	3
2	Excute OpenSSL command	3
2.1	Target	3
2.2	Result	4
3	Apache Https Hosts	4
3.1	Target	4
3.2	Proof	5

1 Compile OpenSSL

1.1 Target

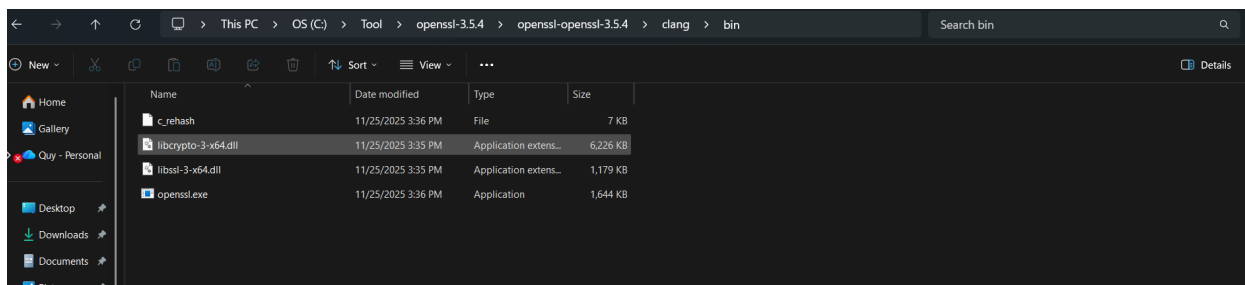
- Compile thành công thư viện OpenSSL trong các môi trường như gcc, clang, msvc, linux.
- Chụp ảnh minh chứng compile thành công.

1.2 GCC



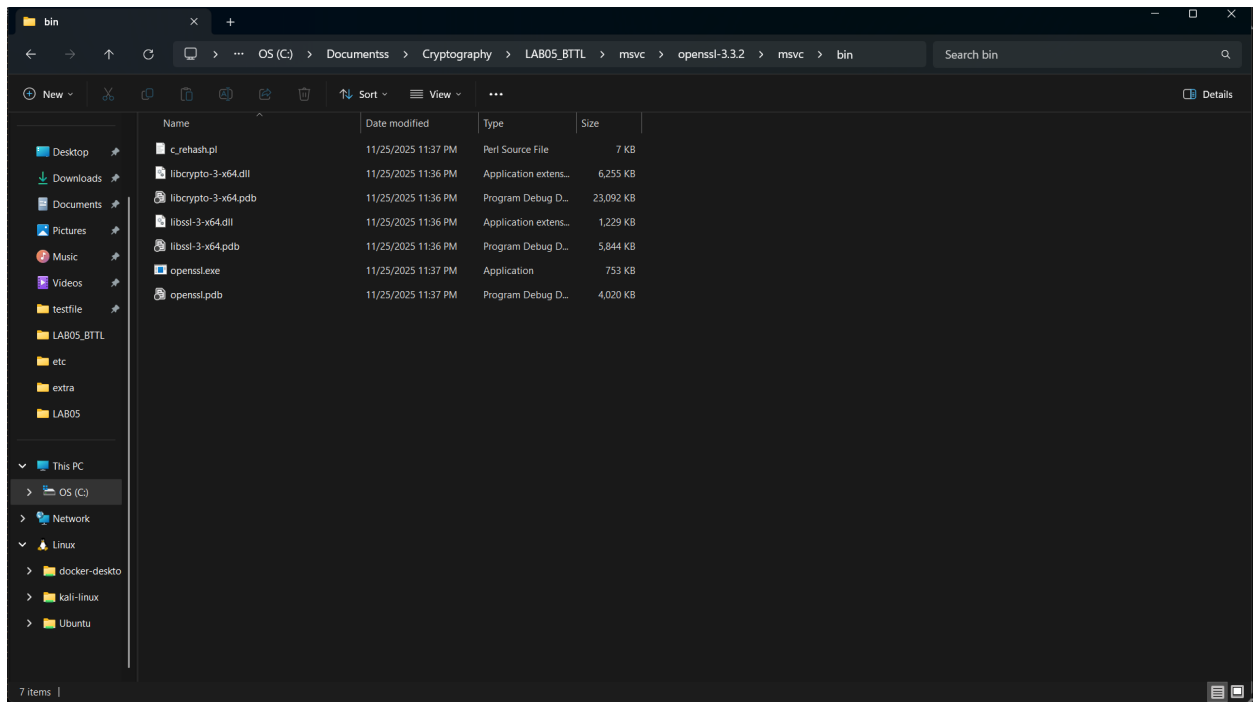
Hình 1: File openssl.exe được compile thành công trong thư mục gcc

1.3 Clang



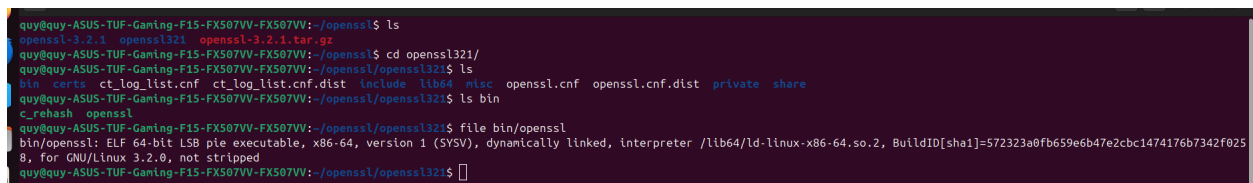
Hình 2: File openssl.exe được compile thành công trong thư mục clang

1.4 MSVC



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

1.5 Ubuntu



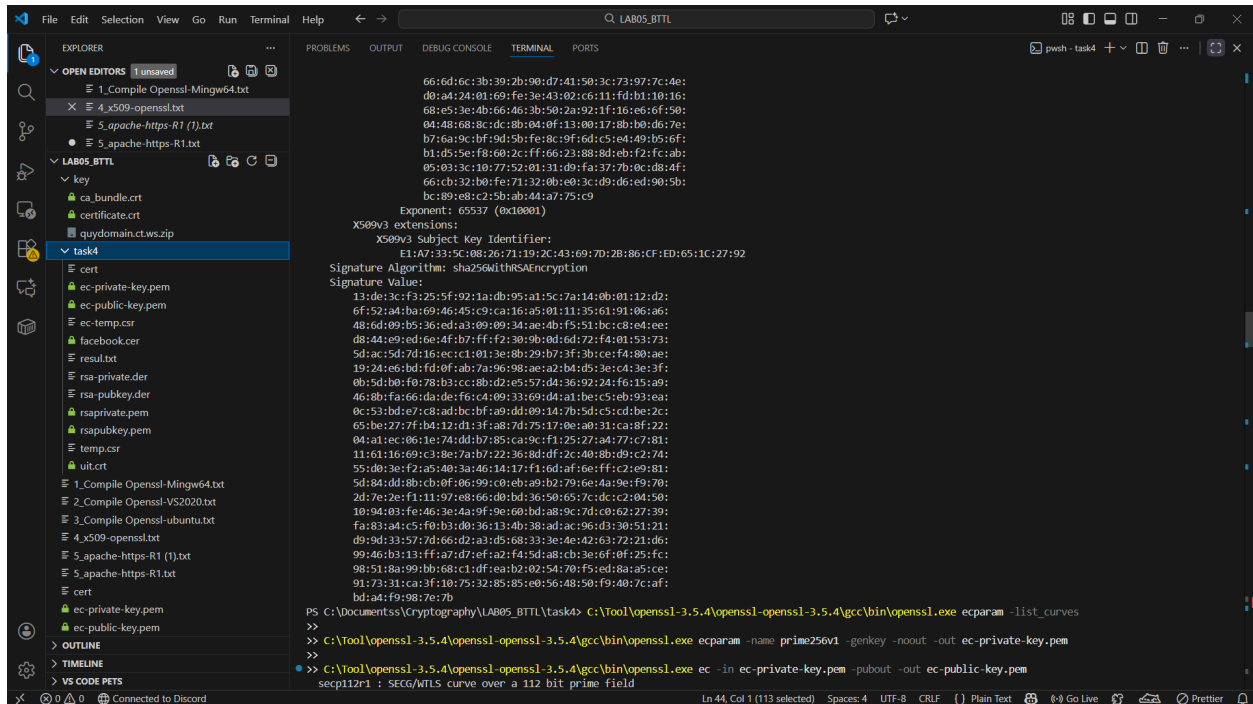
Hình 4: File openssl.exe được compile thành công trong thư mục ubuntu

2 Excute 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



```
66:6d:6c:3b:39:2b:90:d7:41:50:3c:73:97:7c:4e:
d0:a4:24:01:69:fe:3e:43:02:c6:11:fd:b1:10:16:
68:c5:3a:40:66:46:3b:50:2a:92:1f:16:eb:6f:50:
04:4b:68:8c:de:ab:04:0f:13:00:17:0b:1b:0d:7e:
b7:6a:9c:bf:9d:5b:fe:8c:9f:6d:c5:e4:49:b5:6f:
b1:d5:5e:f8:60:2c:ff:66:23:88:8d:eb:f2:fc:ab:
05:03:3c:10:77:52:01:31:d9:fa:37:7b:0c:d8:4f:
66:cb:32:b0:fe:71:32:0b:e0:3c:d9:de:ed:90:5b:
bc:89:e8:c2:5b:ab:44:a7:75:c9
Exponent: 65537 (0x10001)
X509v3 extensions:
X509v3 Subject Key Identifier:
E1:A7:33:5C:08:26:71:19:2C:43:69:7D:2B:86:CF:ED:05:1C:27:92
Signature Algorithm: sha256withSMAEncryption
Signature Value:
13:de:3c:fc: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:a6:
48:6d:09:b5:36:ed:a3:09:09:34:ae:4b:fs:51:bc:e4:ee:
d8:44:e9:ed:6e:4f:b7:ff:f2:30:9b:0d:6d:72:f4:01:53:73:
5d:ac:5d:7d:16:ec:c1:01:3e:8b:29:b7:3f:3b:ce:f4:80:ae:
19:24:e6:bd:fd:0f:ab:7a:96:98:ae:a2:b4:d5:3e:c4:3e:3f:
0b:5d:10:f9:78:b3:cc:e8:0d:05:57:d4:36:92:2a:fe:15:a9:
46:8b:fa:66:da:de:fe:c4:09:33:69:d4:a1:be:c5:eb:93:ea:
0c:53:bd:e7:c8:ad:bc:bf:a9:dd:09:14:7b:5d:c5:cd:be:2c:
65:be:27:7f:b4:12:d1:3f:a8:7d:75:17:0e:a0:31:ca:8f:22:
04:a1:ec:06:1e:74:dd:b7:85:ca:9c:f1:25:27:a4:77:c7:81:
11:61:16:69:c3:0e:7a:b7:22:36:8d:df:2c:40:8b:d9:c2:74:
55:d0:3e:f2:a5:40:3a:46:14:17:f1:6d:af:6e:ff:c2:e9:81:
5d:84:dd:8b:cb:0f:06:99:c0:eb:a9:b2:79:6e:4a:9e:f9:70:
2d:7e:2e:f1:11:97:e8:66:d0:bd:36:50:65:7c:dc:c2:04:50:
10:94:03:fe:46:3e:4a:9f:9e:60:bd:a8:9c:7d:c0:02:27:39:
fa:83:04:c5:f0:b3:d8:36:13:4b:38:ad:ae:96:d3:30:51:22:
d9:9d:33:57:7d:66:d2:a3:d5:68:23:3e:4e:42:6f:72:21:d6:
99:46:b3:13:ff:a7:d7:ef:a2:f4:5d:a8:cb:3e:ef:0f:25:fc:
98:51:8a:99:bb:68:c1:df:ea:b2:02:54:70:f5:ed:8a:a5:ce:
91:73:31:ca:3f:10:75:32:85:85:e0:56:48:50:f9:40:7c:af:
bd:a4:f9:98:7e:7b
PS C:\Documentss\Cryptography\LAB05_BTTL\task4> C:\Tool\openssl-3.5.4\openssl-3.5.4\bin\openssl.exe ecparam -list_curves
>>
>> C:\Tool\openssl-3.5.4\openssl-3.5.4\bin\openssl.exe ecparam -name prime256v1 -genkey -noout -out ec-private-key.pem
>>
>> C:\Tool\openssl-3.5.4\openssl-3.5.4\bin\openssl.exe ec -in ec-private-key.pem -pubout -out ec-public-key.pem
>>
secp112r1 : SECG/WTLS curve over a 112 bit prime field
```

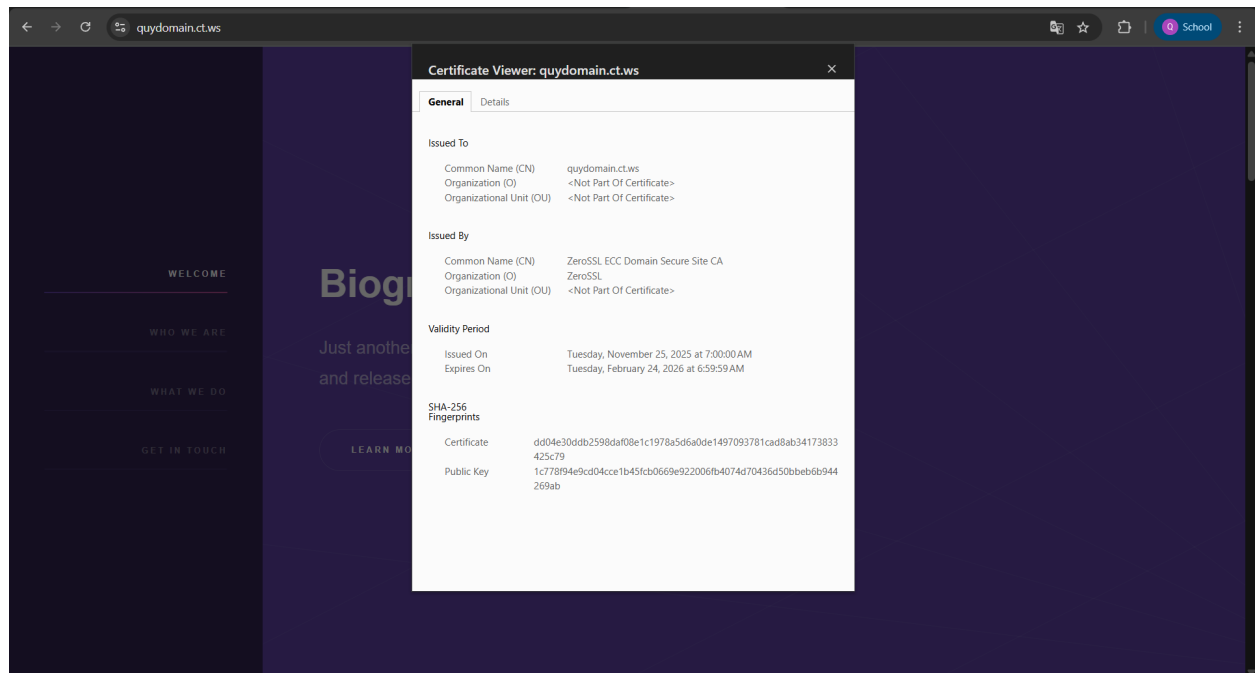
Hình 5: Minh chứng thực thi câu lệnh OpenSSL

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