REPORT FOR LAB5-6 CRYPTOGRAPHY

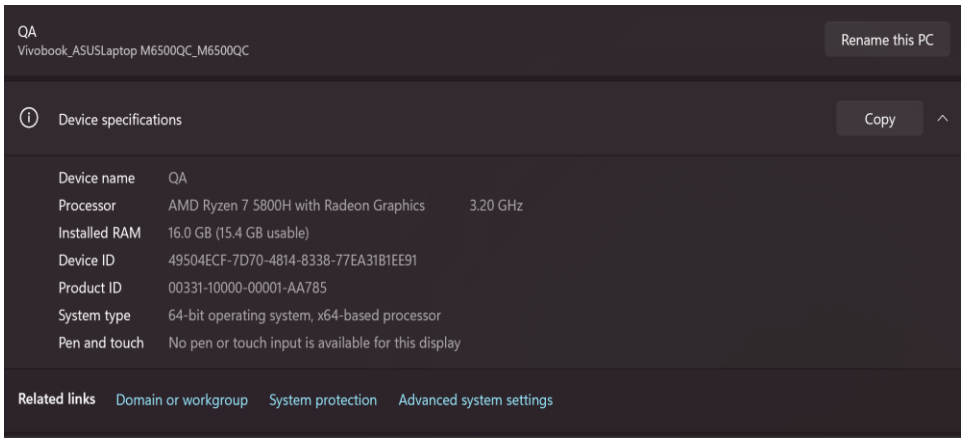
MSSV: 22520064

Name: Nguyễn Thị Quỳnh Anh

Lecturer: Nguyễn Ngọc Tự

I. Hardware resources

1. Windows

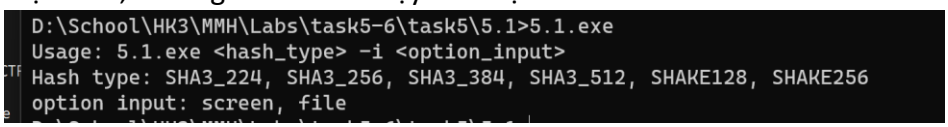


2. Linux

3. Báo cáo chi tiết.

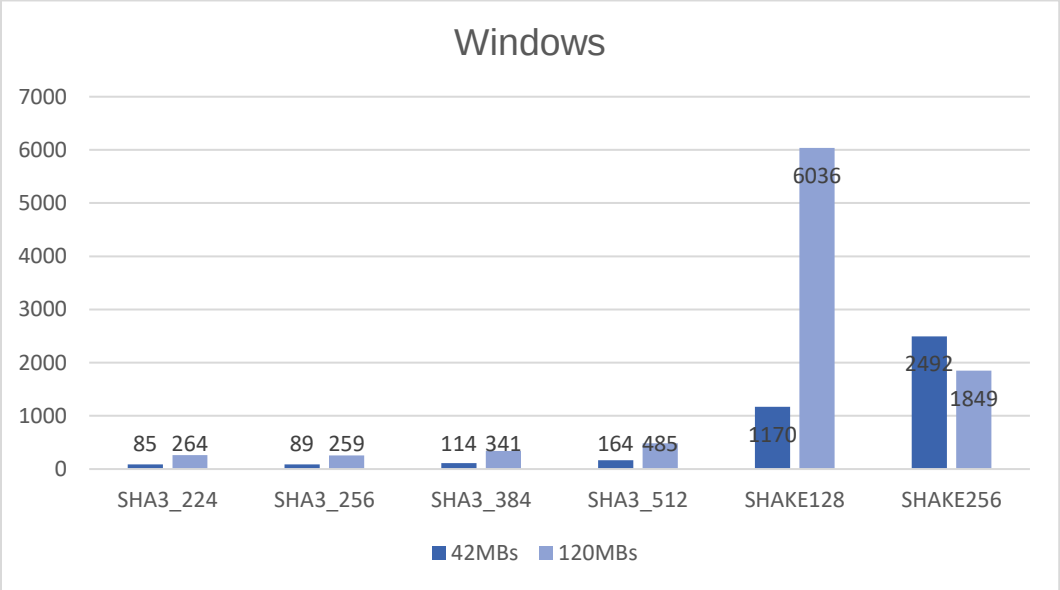
1. Task 5.1

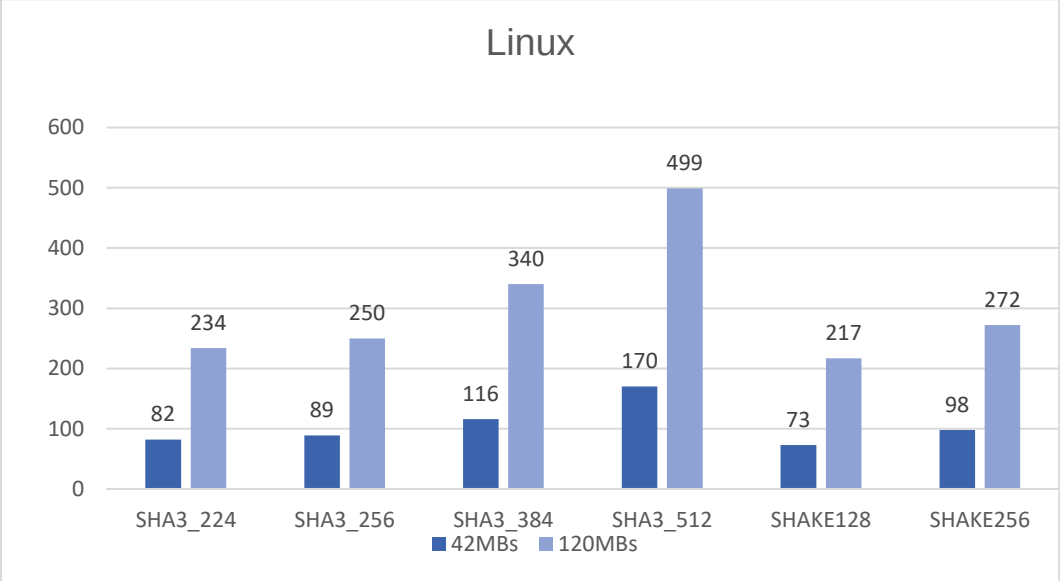
- Xây dựng chương trình thực hiện chức năng hash, cho người dùng lựa chọn các loại hash, các argument khi chạy file thực thi như sau:



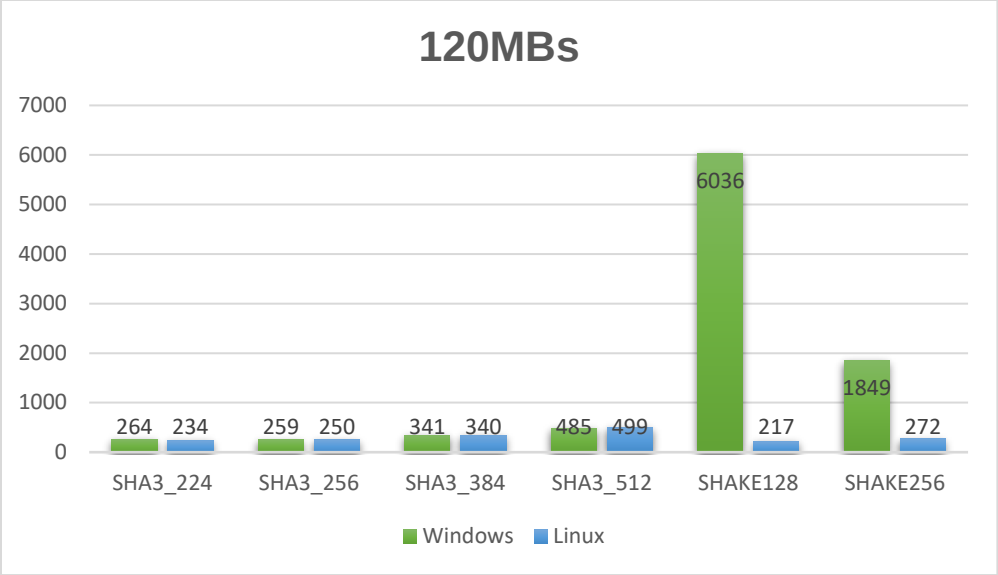
-

- Em dùng 2 input file để đo thời gian thực thi, so sánh giữa linux và windows, cũng như giữa các loại hash khác nhau.
- Đây là thống kê của em về thời gian băm (đ/v milliseconds)





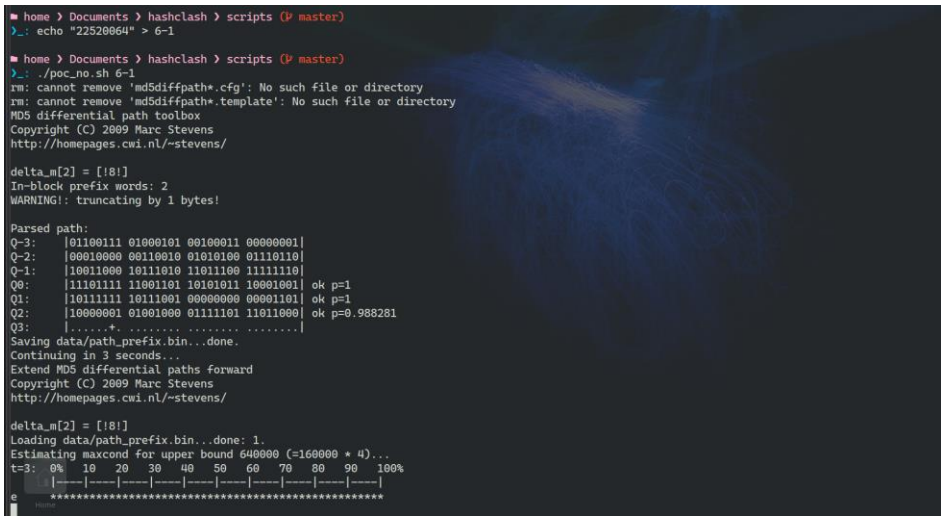
- Từ hai biểu đồ trên, có thể thấy, file có độ lớn càng lớn, thời gian băm càng lâu. Nhưng nếu xét một file có độ lớn nhất định, ở bên linux hai hàm băm SHAKE chạy hanh hơn nhiều so với hàm SHA thì bên Windows ngược lại, hàm SHA nhanh hơn nhiều so với SHAKE.



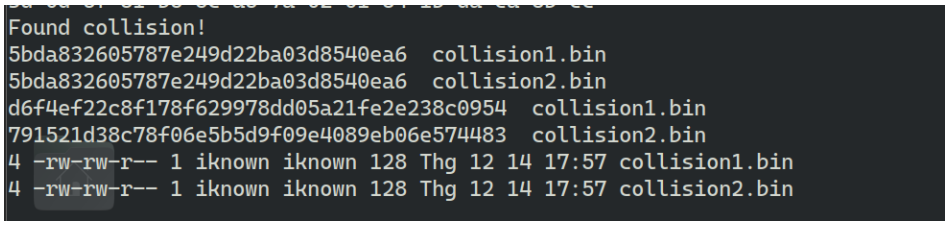
- Từ biểu đồ trên có thể thấy, thời gian không chênh lệch giữa windows và linux của các thuật toán SHA3. Những hàm băm SHAKE lại có chênh lệch lớn, thời gian chạy trên Windows lớn hơn nhiều lần so với chạy trên Linux.

2. Task 6

- **6.1a : Two collision messages have the same prefix string**
  - Sau khi install hashclash tool. Dùng script **poc_no.sh.**



  - Đợi sau khi chạy xong, em có được 2 file có cùng hash MD5



  - In ra hexdump của 2 file này:

```
home ❯ Documents ❯ hashclash ❯ scripts (master)
❯_: xxd collision1.bin
00000000: 3232 3532 3030 3634 9f00 2527 0bf8 cb63  22520064..%'...c
00000010: 8e23 a73c cb56 b6a8 7f11 9f5f 586f 2062  .#.<.V....._Xo b
00000020: 0533 780c 067b 4b11 8a28 de64 c66d f103  .3x..{K..(.d.m..
00000030: b746 9f6b 4f8c aaa1 f346 2b81 f379 0636  .F.kO....F+..y.6
00000040: 9c9d f25b 459c ed31 c0da 628b 9bf4 709f  ...[E..1..b...p.
00000050: 7649 8c5b 6880 464c ab1d 40cc c560 3d92  vI.[h.FL..@..`=.
00000060: 42fe 91e0 110f 8baa 294e 53ab 5192 c933  B.......)NS.Q..3
00000070: 3d0d 6f81 b55c a67a 0201 841b daea 8bec  =.o..\.z........

home ❯ Documents ❯ hashclash ❯ scripts (master)
❯_: xxd collision2.bin
00000000: 3232 3532 3030 3634 9f01 2527 0bf8 cb63  22520064..%'...c
00000010: 8e23 a73c cb56 b6a8 7f11 9f5f 586f 2062  .#.<.V....._Xo b
00000020: 0533 780c 067b 4b11 8a28 de64 c66d f103  .3x..{K..(.d.m..
00000030: b746 9f6b 4f8c aaa1 f346 2b81 f379 0636  .F.kO....F+..y.6
00000040: 9c9d f25b 459c ed31 c0d9 628b 9bf4 709f  ...[E..1..b...p.
00000050: 7649 8c5b 6880 464c ab1d 40cc c560 3d92  vI.[h.FL..@..`=.
00000060: 42fe 91e0 110f 8baa 294e 53ab 5192 c933  B.......)NS.Q..3
00000070: 3d0d 6f81 b55c a67a 0201 841b daea 8bec  =.o..\.z........

home ❯ Documents ❯ hashclash ❯ scripts (master)
❯_:
```

- Check xem hai file binary có khác nhau hay không:

```
❯_: diff collision1.bin collision2.bin
Binary files collision1.bin and collision2.bin differ
```

- Cuối cùng em check MD5 của hai file này:

```
❯_: md5sum collision1.bin collision2.bin
5bda832605787e249d22ba03d8540ea6  collision1.bin
5bda832605787e249d22ba03d8540ea6  collision2.bin
```

Như vậy em đã tìm được 2 file binary khác nhau có cùng mã băm MD5 từ 1 file prefix.

- **6-1b : Two different C++ programs but have the same MD5.**

Em viết 2 chương trình C++ như sau:

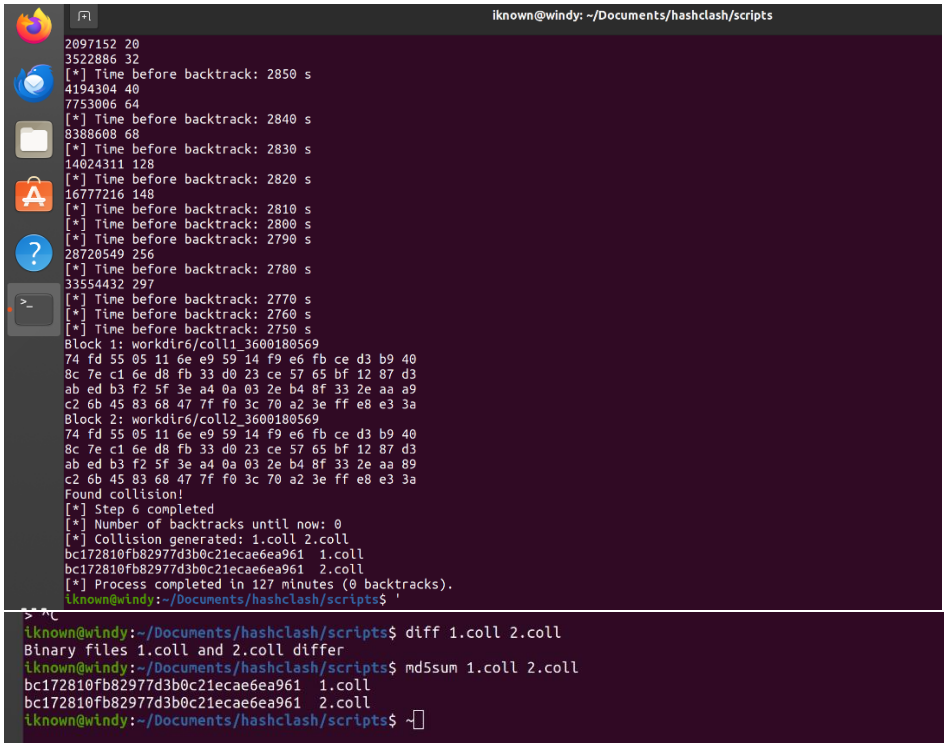
```
iknown@windy:~/Documents/hashclash/scripts$ cat 1.cpp
#include <iostream>

int main() {
        std::cout<<"Hello hhh";
}iknown@windy:~/Documents/hashclash/scripts$ cat 2.cpp
#include <iostream>

int main() {
        std::cout<< "22520064";
}iknown@windy:~/Documents/hashclash/scripts$
```

Sau đó compile hai chương trình này thành 2 file thực thi, dùng **hashclash** với script **cpc.sh** để tìm collision.

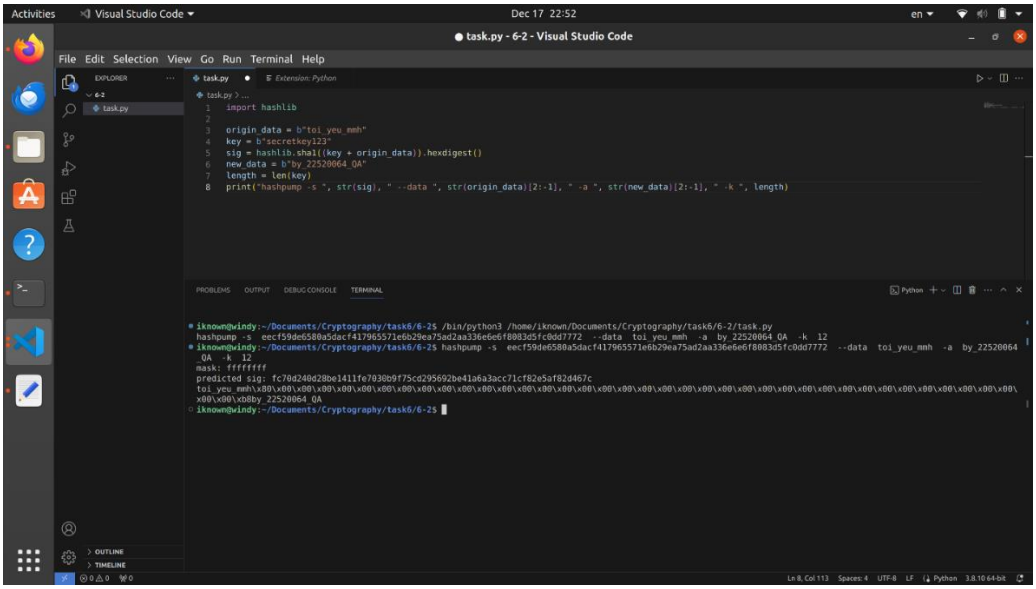
Sau 127 phút chạy thì em nhận được 2 file collision.



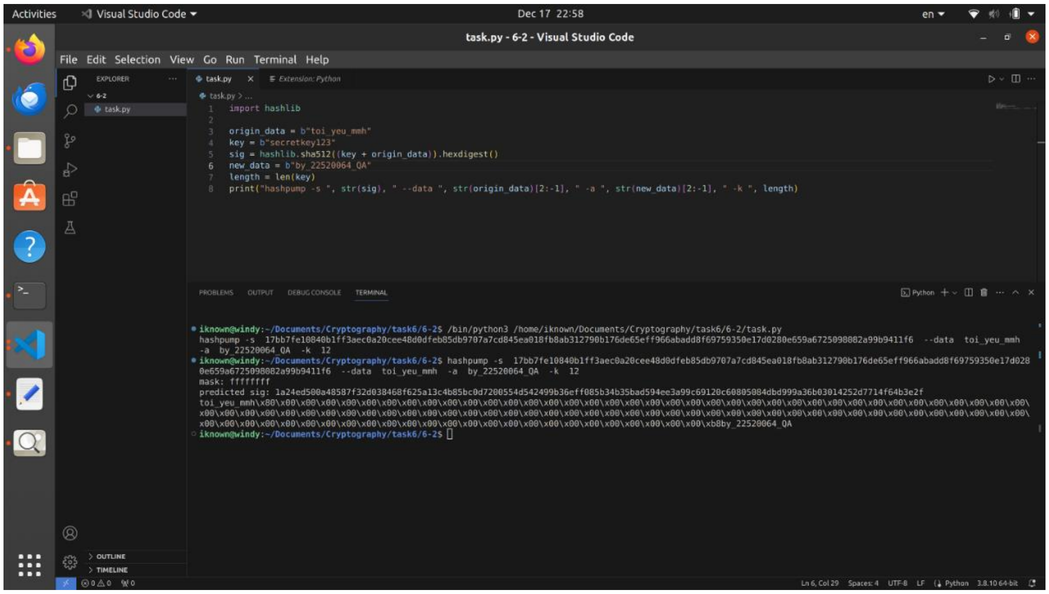
- **6-2a : Show length extension attacks on MAC using SHA1, SHA256, SHA512 using hashpump tool.**

Sử dụng tool **hashpump** để attack, đầu tiên em dùng python tạo origin data, key, sau đó tính hash(key + origin data) và chiều dài của key. Để attack, cần thêm một chuỗi dữ liệu thêm vào phía sau. Em dùng tool với câu lệnh `**hashpump -s <origin_sig> --data <origin_data> -a <additional data> -k <key_length>** ` để attack được origin data mà không cần biết key là gì. Sau đây là ảnh demo của em.

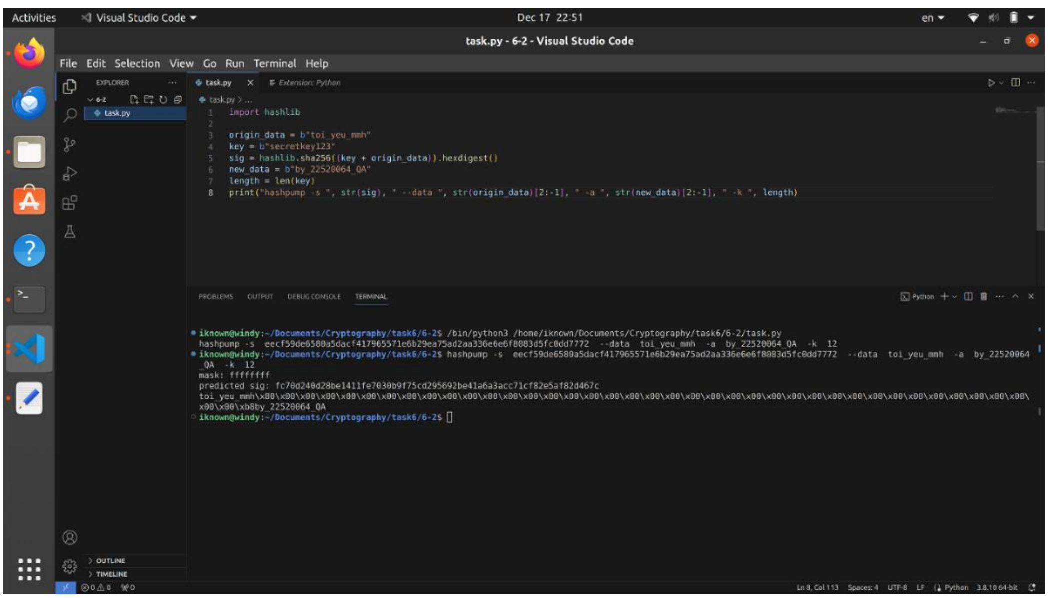
SHA1:



SHA256:



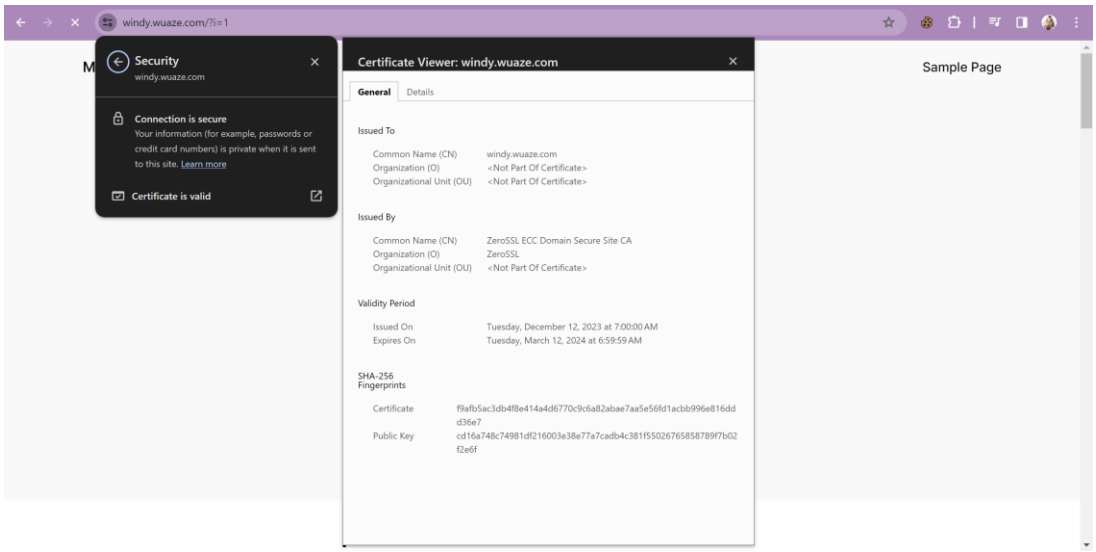
SHA512:



3. Bonus point

- Sử dụng InfinityFree để đăng kí một domain
- Sau đó dùng ZeroSSL để đăng kí certificate cho domain này
- Cuối cùng dùng Apache để thêm certificate cho domain này được công nhận là security.

Đây là web của em sau khi hoàn thành các bước trên.


windy.wuaze.com/?i=1
Security
windy.wuaze.com
Connection is secure
Your information (for example, passwords or credit card numbers) is private when it is sent to this site. Learn more
Certificate is valid
Certificate Viewer: windy.wuaze.com
General
Details
Issued To
Common Name (CN) windy.wuaze.com
Organization (O) <Not Part Of Certificate>
Organizational Unit (OU) <Not Part Of Certificate>
Issued By
Common Name (CN) ZeroSSL ECC Domain Secure Site CA
Organization (O) ZeroSSL
Organizational Unit (OU) <Not Part Of Certificate>
Validity Period
Issued On Tuesday, December 12, 2023 at 7:00:00 AM
Expires On Tuesday, March 12, 2024 at 6:59:59 AM
SHA-256 Fingerprints
Certificate f9afb5ac3db4f8e414a4d6770c9c6a82abae7aa5e56fd1acbb996e816ddd36e7
Public Key cd16a748c74981df216003e38e77a7cadb4c381f55026765858789f7b02f2e6f
Sample Page