**LAB 3**

**Fuzzing - Reverse Engineering - Cryptography**

|  |
| --- |
| Họ tên và MSSV: 1050080267  Lớp: 10\_ĐH\_CNPM3 |
| Link youtube:  Link github |

* *Các sinh viên bị phát hiện sao chép bài của nhau sẽ nhận 0đ cho tất cả bài thực hành của môn này.*
* *Bài nộp phải ở dạng docx, hình minh họa phải rõ ràng chi tiết.* Hình minh hoạ chỉ cần chụp ở nội dung thực hiện, không chụp toàn màn hình.
* *Quay quá trình làm có face để gv biết anh chị đang làm*
* *Anh chị nào không có video trên kênh sẽ không chấm bài*

**Câu 1: Thực hiện kỹ thuật Reverse Engineering với công cụ IDA Pro**

Tham khảo và thực hiện hướng dẫn thực hiện kỹ thuật Reverse Engineering với công cụ IDA Pro. Chụp hình minh hoạ các bước thực hiện như trong hướng dẫn.

<https://samsclass.info/126/proj/p2x-126-IDA.html>

## Tải xuống IDA Pro miễn phí

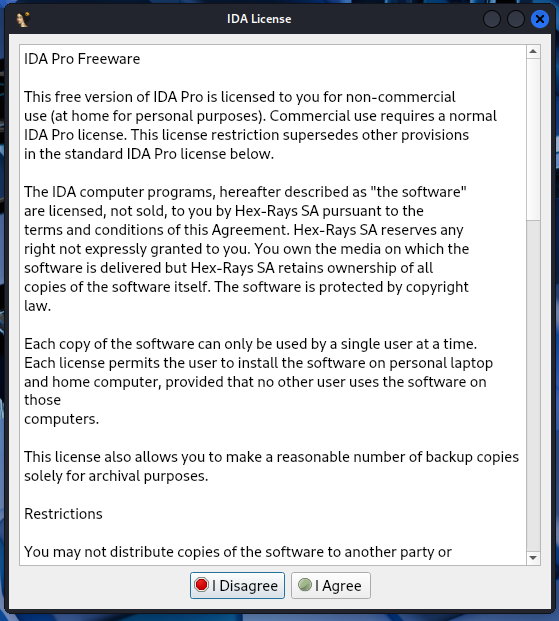
Mở trình duyệt web và truy cập <http://www.hex-rays.com/products/ida/support/download_freeware.shtml>

Ở cuối trang, nhấp vào liên kết "IDA Freeware (16mb)".

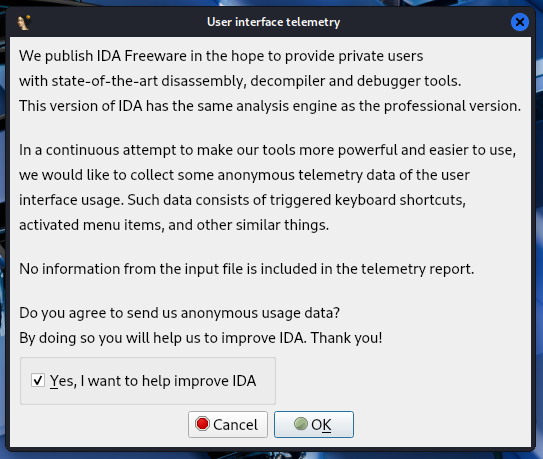
Cài đặt phần mềm với các tùy chọn mặc định. Tôi thấy một thông báo lỗi nói rằng không tìm thấy thư mục có dấu nháy đơn, nhưng chỉ cần đóng nó lại và có vẻ như không có vấn đề gì.

Khi bạn thấy cửa sổ IDA hiển thị bên dưới, hãy nhấp vào nút **OK** .

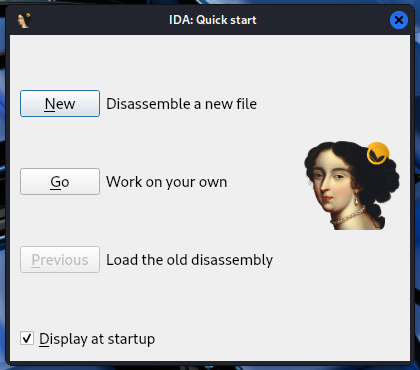




Nhấp vào " **Tôi đồng ý** ".

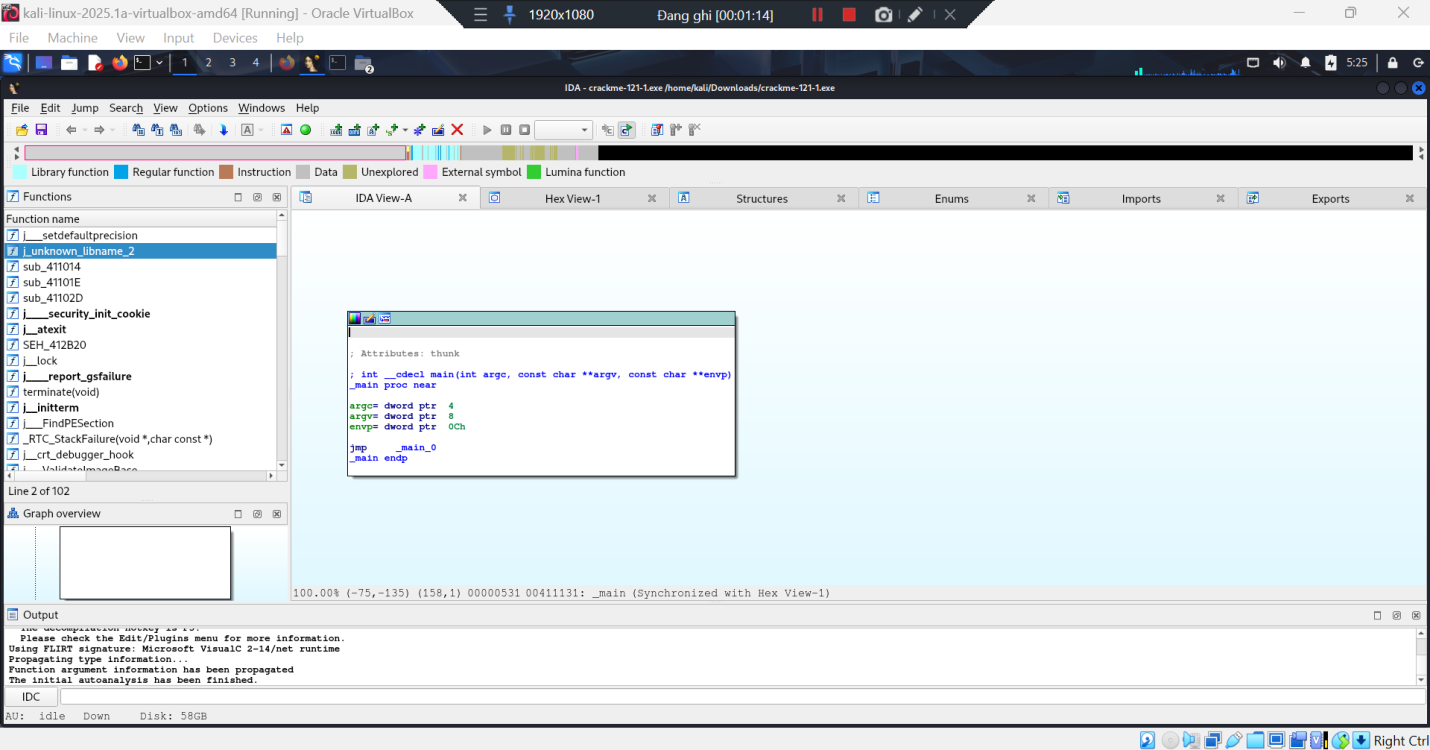


Trong hộp "Chào mừng đến với IDA!" như hiển thị bên dưới, hãy nhấp vào nút **Mới** .



## Xem Mã đã tháo rời

Trong IDA Pro, hãy tìm ngăn "View-A", ngăn này hiển thị các hộp chứa mã được liên kết với các hộp khác theo kiểu sơ đồ luồng. Phóng to ngăn này bằng cách nhấp vào nút được chỉ ra bởi mũi tên trong hình bên dưới:



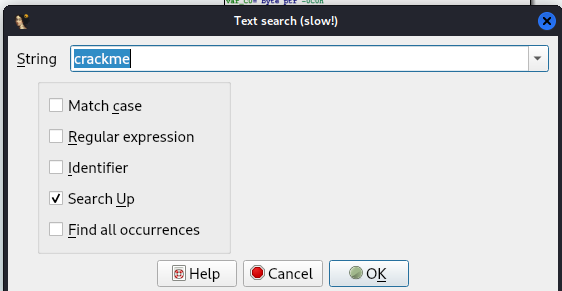
Đóng hộp "Tổng quan biểu đồ" ở góc dưới bên phải.

Kéo đường viền dưới của ngăn "View-A" xuống để tạo ra vùng xem rộng nhất có thể.

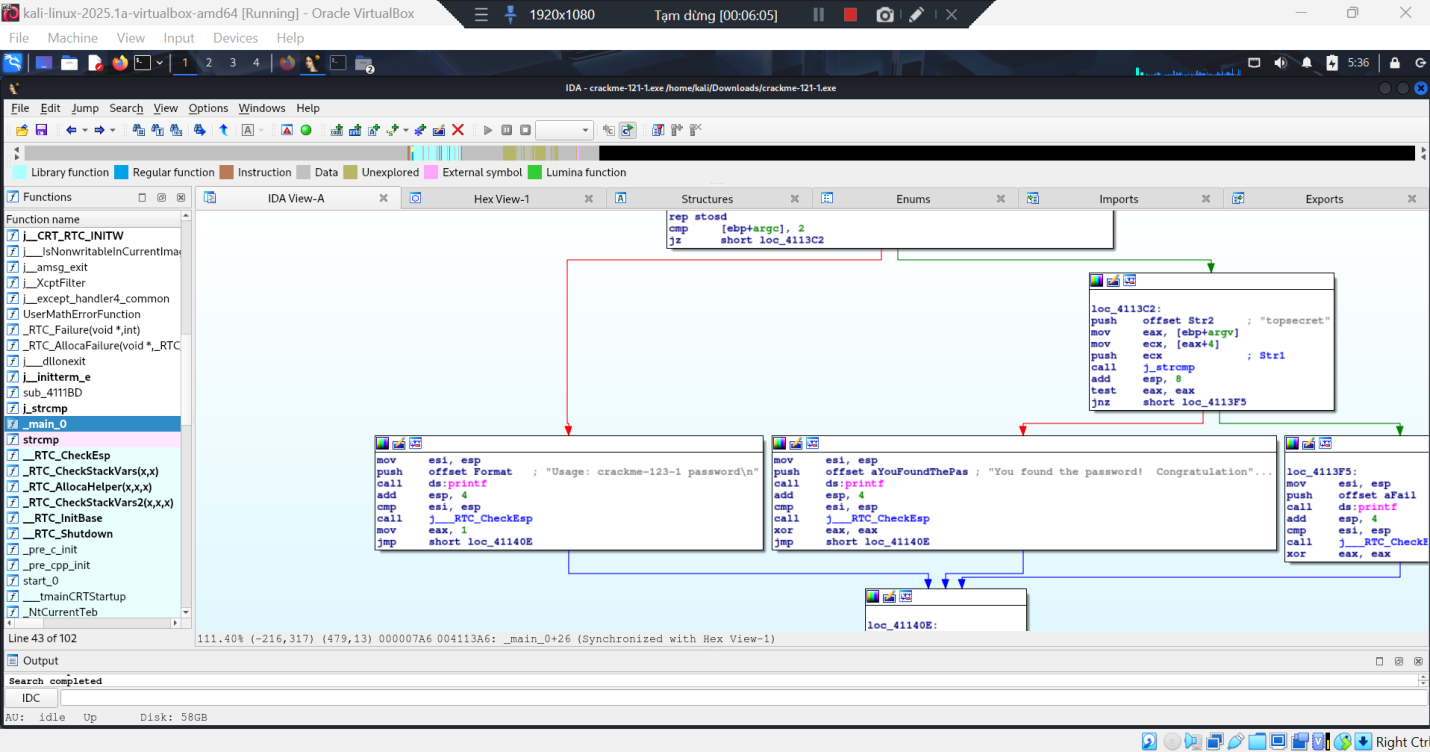
Từ thanh menu IDA, nhấp vào **Tìm kiếm** , **Văn bản** .

Tìm kiếm **crackme** như hình dưới đây.

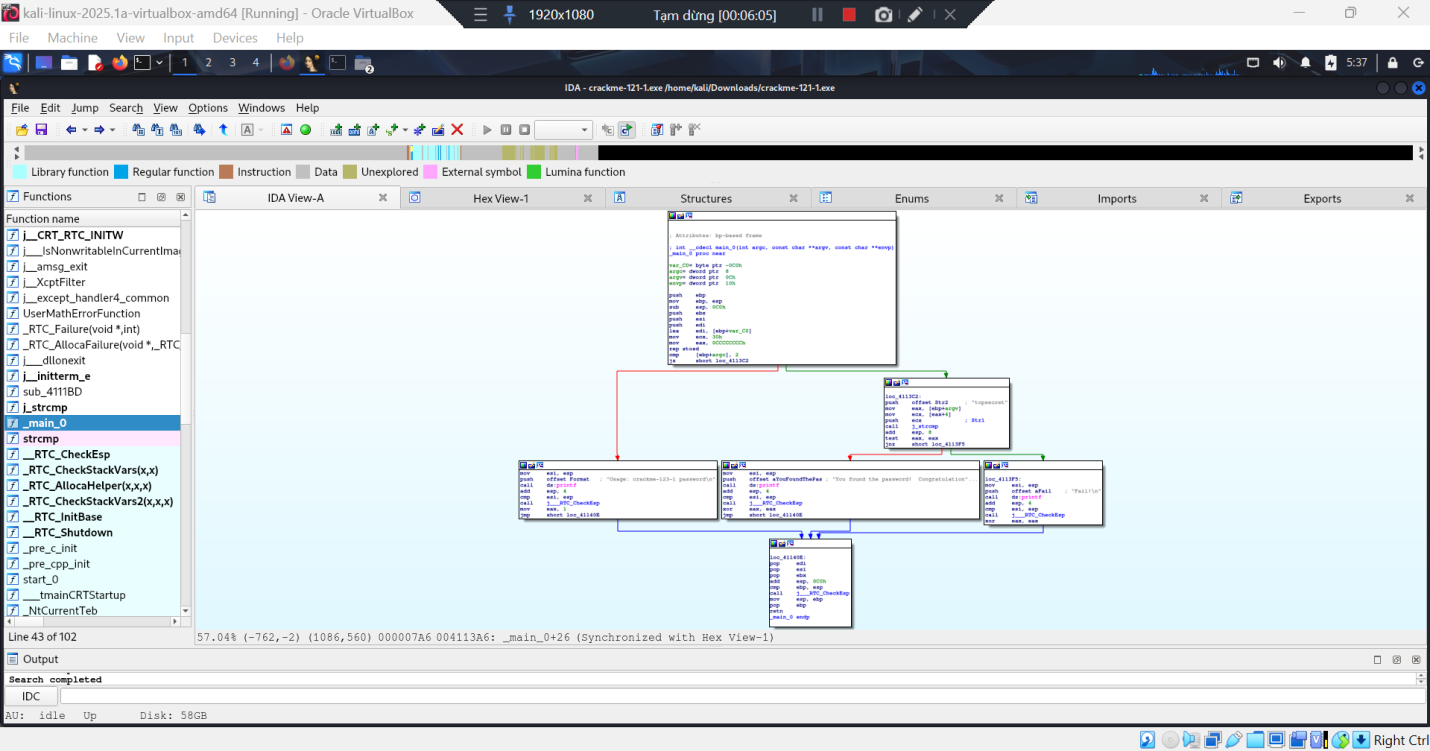
Nhấp vào **OK** .



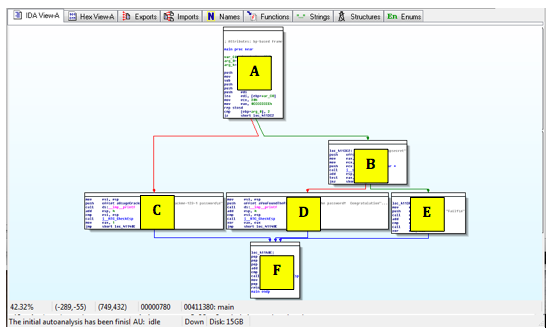
Nhấp chuột phải vào hộp "View-A" và nhấp vào " **Fit window** ", như hình dưới đây:



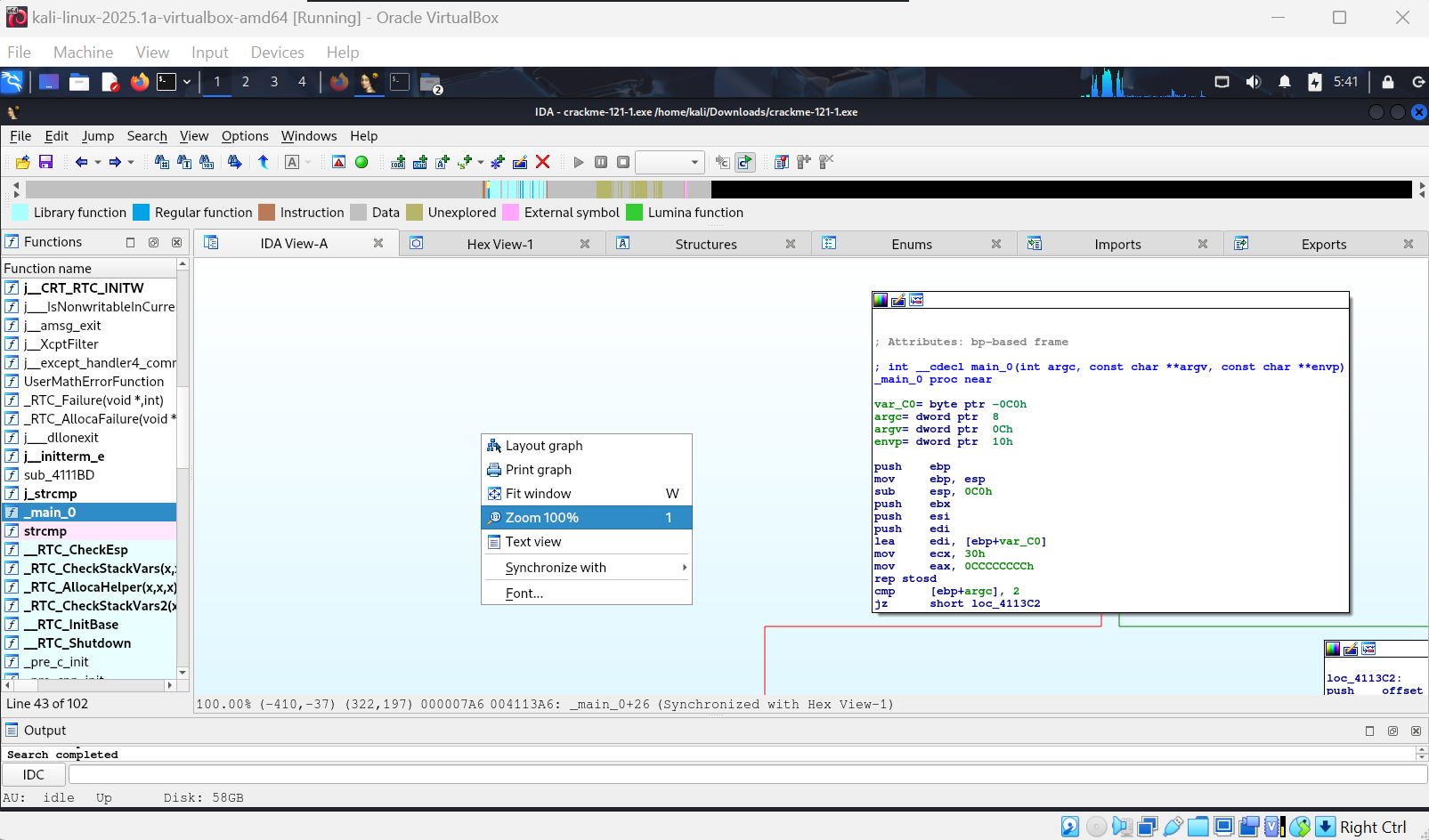
Bây giờ bạn sẽ thấy toàn bộ chương trình được hiển thị dưới dạng sáu hộp được kết nối bằng các đường thẳng, như hình dưới đây. (Bỏ qua hai hộp thừa ở góc trên bên trái):



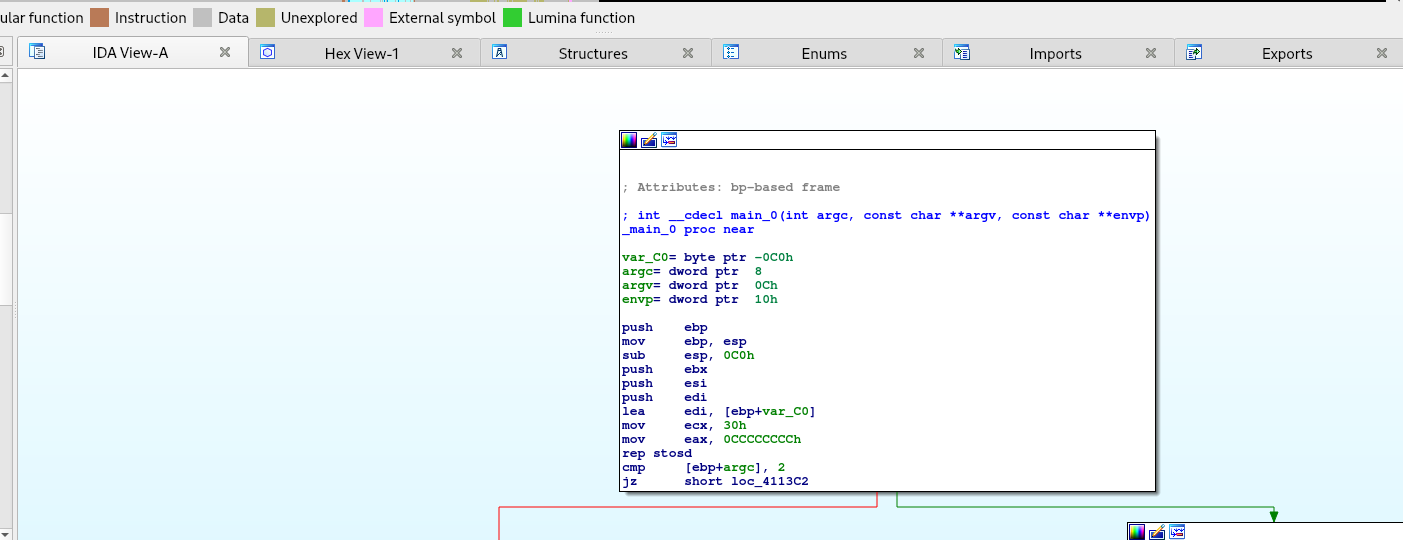
Đối với dự án này, tôi đã dán nhãn các mô-đun bằng các chữ cái như hiển thị bên dưới:



Nhấp chuột phải vào hộp "View-A" và nhấp vào " **Zoom 100%** ", như hình dưới đây:



Nhấp và kéo màn hình "View-A" khi cần để hiển thị mô-đun A, như hiển thị bên dưới:



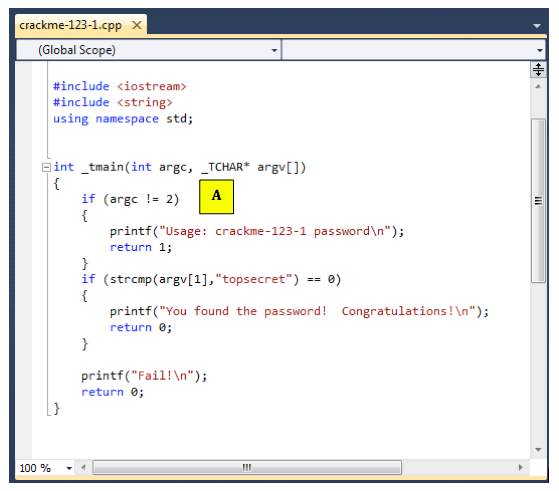
Mã lắp ráp khó đọc, nhưng bạn không cần phải hiểu tất cả. Tập trung vào hai hướng dẫn cuối cùng:

**Cmp [ebp+arg\_0],2  
jz short loc\_4113C2**

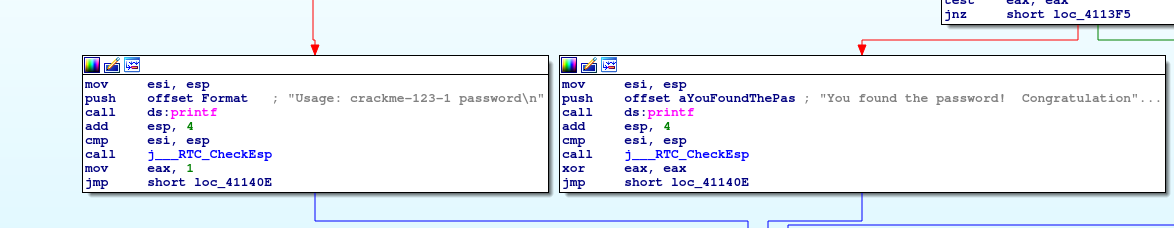
Thao tác này so sánh một số với 2 bằng thao tác **cmp** (So sánh) và nhảy đến một mô-đun khác nếu số đó bằng 2, bằng cách sử dụng thao tác **jz** (Nhảy nếu bằng 0).

## Mã nguồn C

Đây là mã nguồn C thực tế cho tệp bạn đang tháo rời. Mô-đun A là mã lắp ráp cho câu lệnh "if" đầu tiên, được gắn nhãn bằng hộp "A" màu vàng bên dưới:



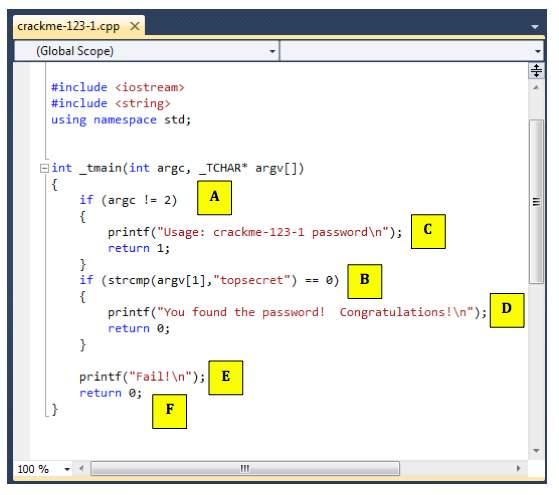
Kéo màn hình "View-A" để hiển thị Module C, như hiển thị bên dưới:



Lưu ý văn bản màu xám dễ đọc ở phía bên phải, ghi "Cách sử dụng: mật khẩu crackme-121-1".

Mô-đun này đẩy các ký tự đó vào ngăn xếp bằng lệnh **push** , sau đó gọi hàm printf bằng lệnh **call ds:\_imp\_printf** .

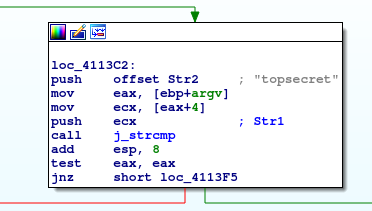
Hình bên dưới hiển thị các câu lệnh C tuân theo mô-đun "C":



Hãy làm theo IDA Pro và đảm bảo bạn thấy được chức năng của từng mô-đun trong sáu mô-đun và cách chúng tương ứng với mã nguồn C.

## Lưu hình ảnh

Kéo màn hình "View-A" để hiển thị mô-đun "B", như hình dưới đây:



Đảm bảo văn bản "tối mật" màu xám hiển thị rõ ràng.

Lưu hình ảnh này với tên tệp **Proj 2xa từ TÊN CỦA BẠN**

## Chạy tệp thực thi

Nhấp vào **Bắt đầu** , nhập **CMD** và nhấn Enter để mở cửa sổ Dấu nhắc Lệnh.

Trong cửa sổ Dấu nhắc lệnh, hãy thực hiện các lệnh sau:

**cd \IDA**

**crackme-121-1**

Bạn sẽ thấy thông báo "Sử dụng: mật khẩu crackme-121-1", như hiển thị bên dưới:

Nếu bạn thấy thông báo "Ứng dụng này không khởi động được vì không tìm thấy MSVCR100D.dll", hãy tải tệp đó xuống tại đây và đặt vào cùng thư mục với tệp .exe:

[msvcr100d.dll](https://samsclass.info/126/proj/msvcr100d.dll)

Thông báo này cho bạn biết rằng bạn cần thêm mật khẩu sau "crackme-121-1".

Trong cửa sổ Dấu nhắc lệnh, hãy thực hiện lệnh này:

**crackme-121-1 wrongpassword**

Bạn sẽ thấy thông báo "Không thành công!".

Trong cửa sổ Dấu nhắc lệnh, hãy thực hiện lệnh này:

**crackme-121-1 topsecret**

Bạn sẽ thấy thông báo "Bạn đã tìm thấy mật khẩu!" như hiển thị bên dưới:

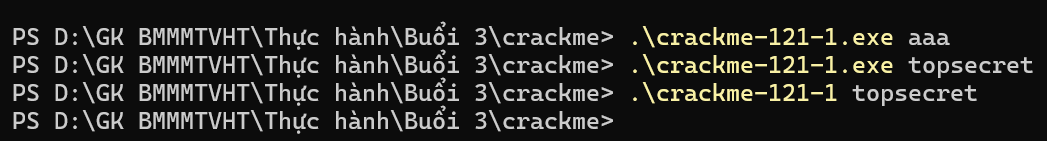
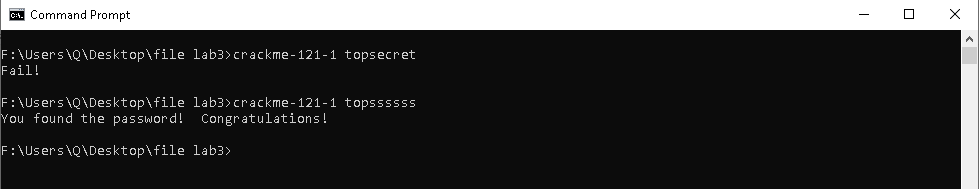
## Lưu hình ảnh

Đảm bảo dòng chữ "Bạn đã tìm thấy mật khẩu!" hiển thị rõ ràng.

Lưu hình ảnh này với tên tệp **Proj 2xb từ TÊN CỦA BẠN**

\* Kết quả thực hiện:

- Chạy lại chương trình crackme thì chương trình báo Fail!:



- Chúng ta nhập vào chuỗi mới sửa lại thì chương trình báo thành công:

**Câu 2: Thực hiện kỹ thuật Fuzzing với công cụ Spike**

Tham khảo và thực hiện hướng dẫn thực hiện kỹ thuật Fuzzing sử dụng công cụ Spike trên Kali Linux. Chụp hình minh hoạ các bước thực hiện như trong hướng dẫn.

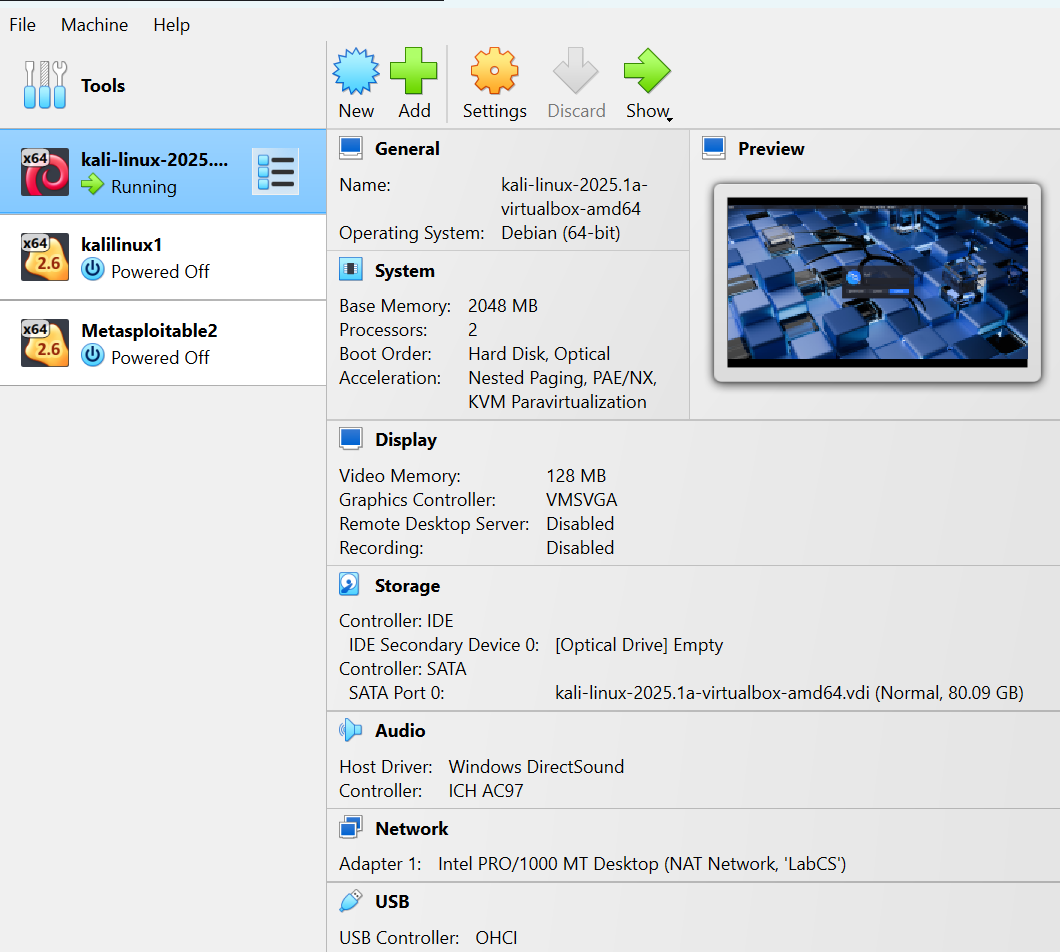
<https://samsclass.info/127/proj/p16-spike.htm>

## Những gì bạn cần

* Máy ảo Windows 2008 Server (hoặc bất kỳ máy Windows nào khác)



* Máy ảo Kali 2



## Mục đích

Để thực hành sử dụng Spike, một công cụ dò tìm mạng rất dễ sử dụng.

## Thiết lập mạng

## Để có kết quả tốt nhất, hãy sử dụng hai máy ảo trên cùng một máy chủ chạy ở chế độ NAT. Điều đó sẽ loại bỏ mọi lưu lượng mạng bên ngoài và giúp dự án dễ dàng hơn.

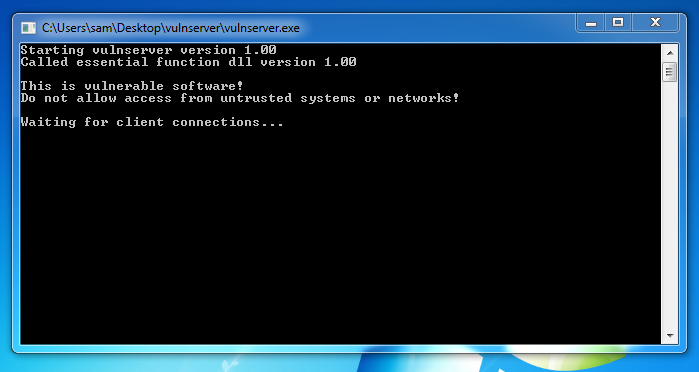
## Chuẩn bị máy chủ dễ bị tấn công

Trên máy Windows của bạn, bạn phải cài đặt Vulnerable Server từ các dự án trước đó. Nếu chưa, hãy tải xuống tại đây:

[http://sites.google.com/site/lupingreycorner/vulnserver.zip](https://sites.google.com/site/lupingreycorner/vulnserver.zip)

Nếu liên kết đó không hoạt động, hãy thử [*liên kết tải xuống thay thế*](https://samsclass.info/127/proj/vulnserver.zip) này .

Giải nén các tệp và nhấp đúp vào **vulnserver** . Ứng dụng Vulnserver mở ra như hình dưới đây.



## Cài đặt Nmap

Bạn cần Nmap trên máy Windows của mình. Nếu bạn không có, hãy tải xuống tại đây:

<https://nmap.org/>

## Cài đặt miễn dịch

Bạn phải cài đặt trình gỡ lỗi Immunity. Nếu chưa, hãy tải xuống tại đây:

<http://debugger.immunityinc.com/ID_register.py>

## Bắt đầu một Ncat Listener

Trên máy tính Windows của bạn, trong cửa sổ Dấu nhắc lệnh, hãy thực hiện các lệnh sau:

**ipconfig**

**cd "c:\program files\nmap"**

**ncat -vklp 9000**

Ghi lại địa chỉ IP của máy Windows.

Lệnh ncat khởi động một trình lắng nghe liên tục trên cổng 9000, trình này sẽ in ra tất cả dữ liệu được gửi đến.

Chúng tôi sẽ làm mờ nó để cho thấy Spike hoạt động như thế nào.

## Làm mờ Ncat Listener với văn bản liên tục

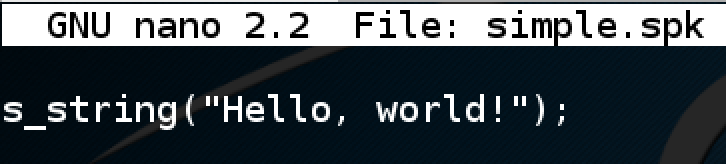
Đầu tiên, chúng ta cần tạo một tập lệnh Spike.

Trên máy Kali 2 của bạn, trong cửa sổ Terminal, hãy thực hiện các lệnh này:

**nano simple.spk**

Nhập dòng này vào tập lệnh như hiển thị bên dưới.

**s\_string("Hello, world!");**



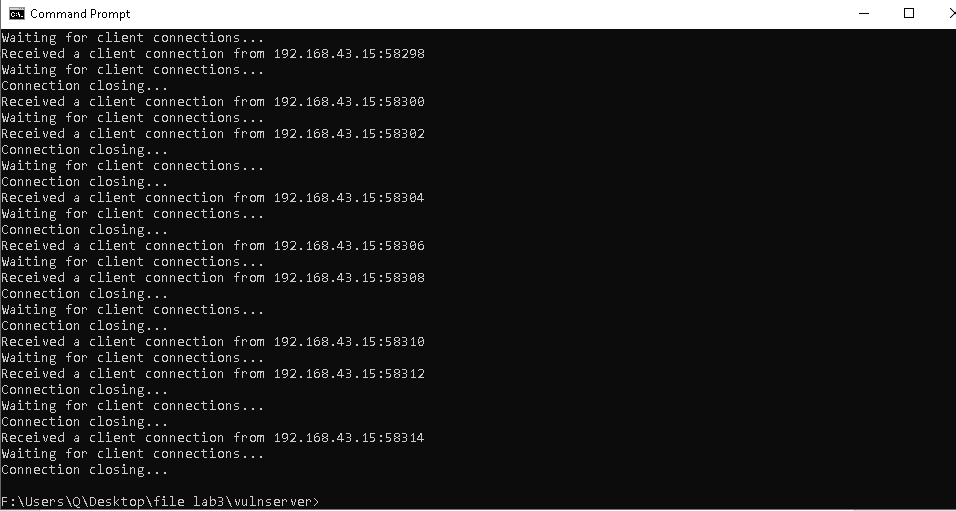
Lưu tệp bằng **Ctrl+X** , **Y** , **Enter** . Trên máy Kali 2 của bạn, trong cửa sổ Terminal, hãy thực hiện lệnh này, thay thế địa chỉ IP bằng địa chỉ IP của máy Windows.

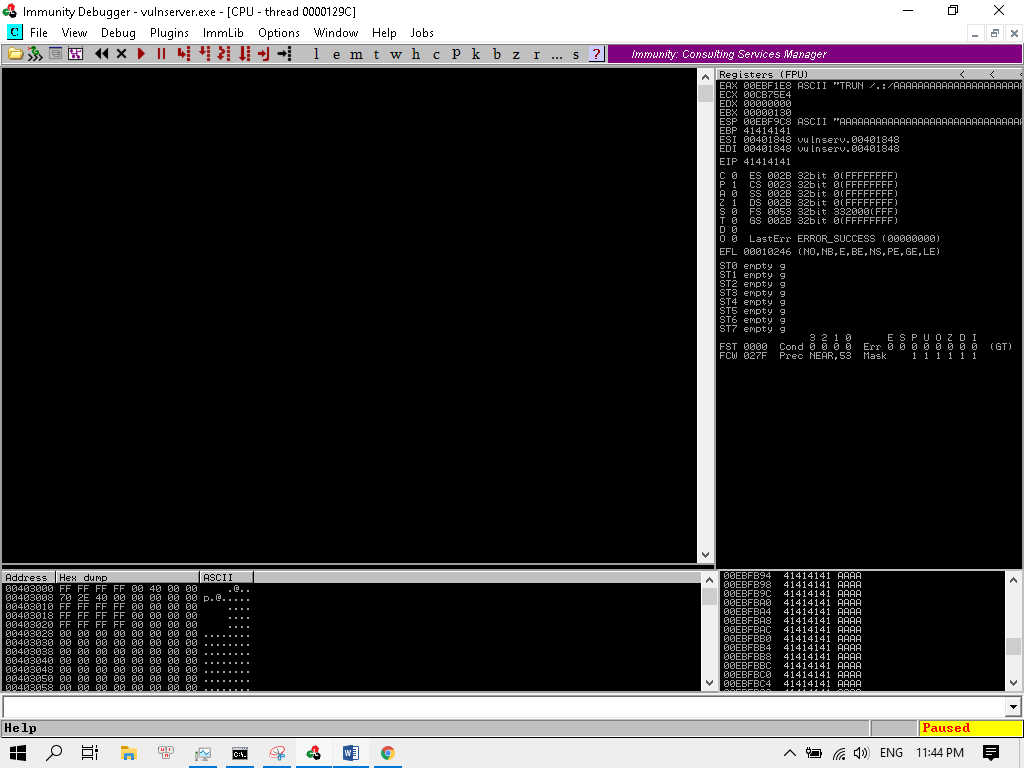
**generic\_send\_tcp 172.16.1.129 9000 simple.spk 0 0**

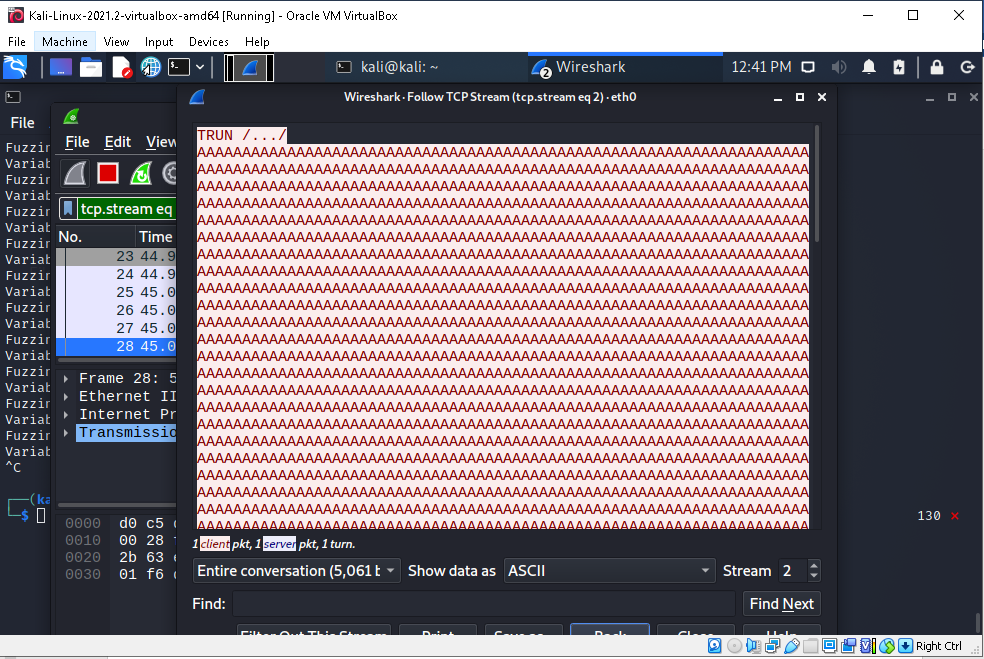
Dừng chế độ làm mờ bằng tổ hợp phím **Ctrl+C** .

Trên máy tính Windows, bạn sẽ thấy nhiều dòng có cùng thông báo như hiển thị bên dưới.

Hàm **s\_string** gửi một chuỗi cố định. Các tham số TCP đang được sửa đổi, không phải tải trọng lớp 7.







**Câu 3: Giải thuật băm**

Sử dụng một trang web online cho phép thực hiện giải thuật băm, ví dụ (<https://www.pelock.com/products/hash-calculator>) thực hiện các công việc sau:

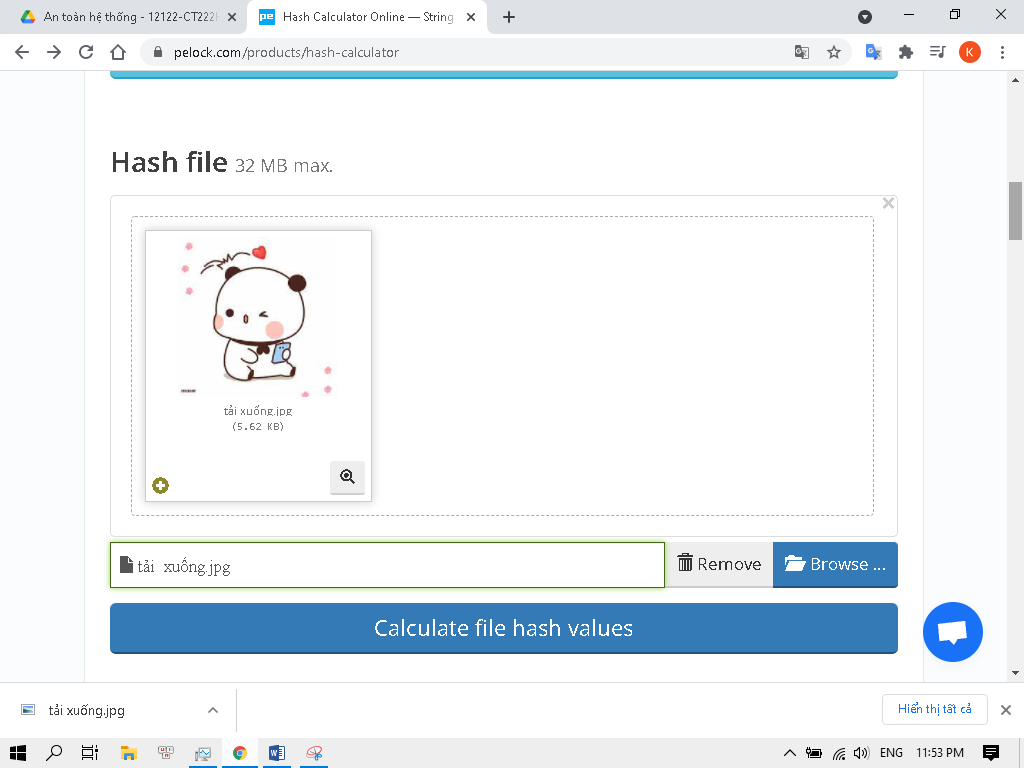
3.1. Tìm giá trị băm của chuỗi "@ntoanhethong\_ct222" sử dụng giải thuật MD5 và SHA512

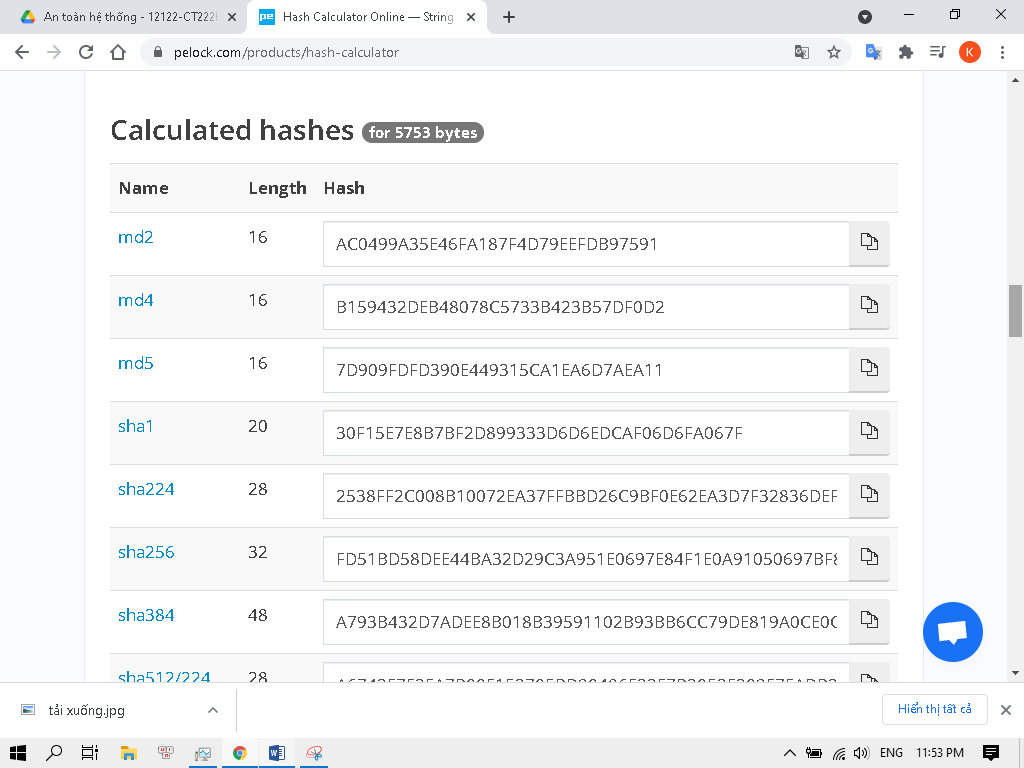
- Giá trị băm của giải thuật MD5 là: CDF279EC13F76CB3C87EE5D362463F88

- Giá trị băm của giải thuật SHA512 là: E6F3A3A5B5FBE1E4BEAF185ED958839EC2C51E

219AB0E69FA8ABA23F626B4B894D4E362F98F5505CB55D01A365F775630152F56BE6032CDCE5106C7F2D93D493

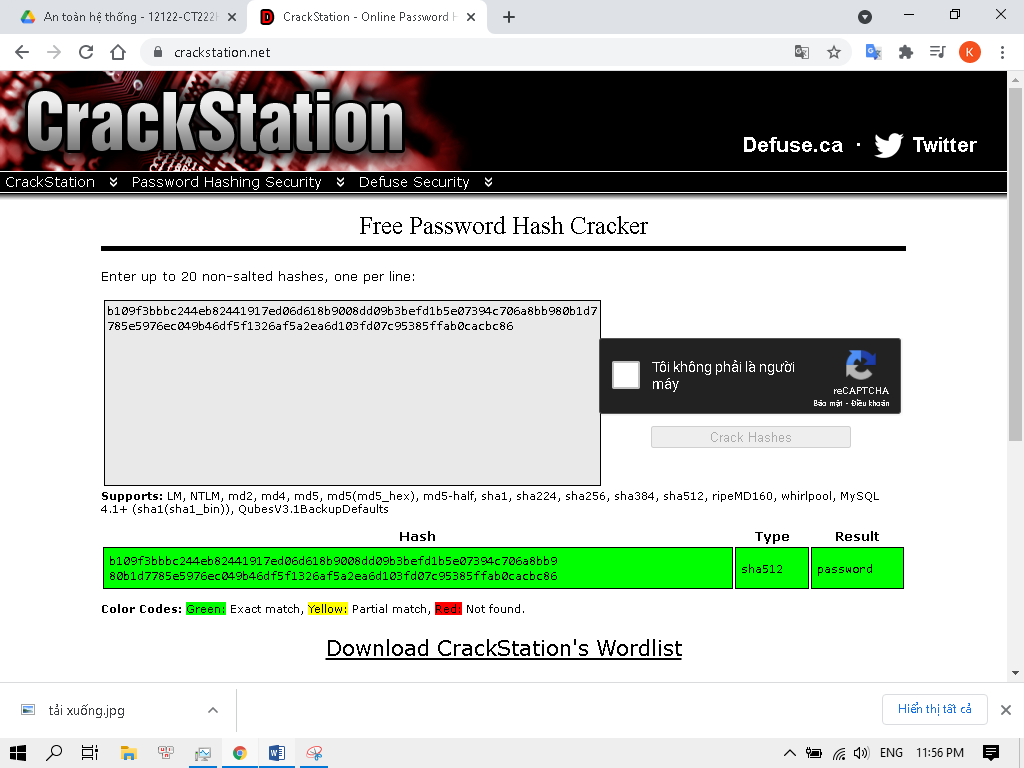
3.2. Upload 1 tập tin và tìm giá trị băm của tập tin đó sử dụng giải thuật MD5 và SHA512



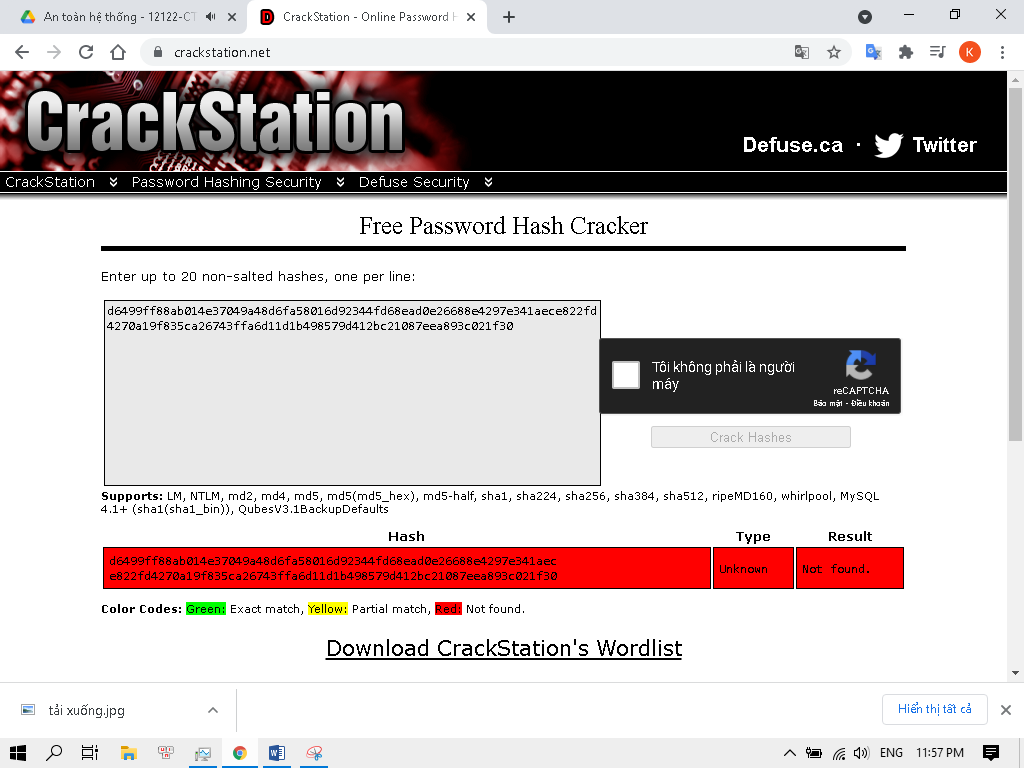


3.3. Sử dụng một trang web cho phép dịch ngược giá trị băm, ví dụ: <https://crackstation.net/>, để tim giá trị ban đầu của 2 giá trị băm sau:

* "b109f3bbbc244eb82441917ed06d618b9008dd09b3befd1b5e07394c706a8bb980b1d7785e5976ec049b46df5f1326af5a2ea6d103fd07c95385ffab0cacbc86"

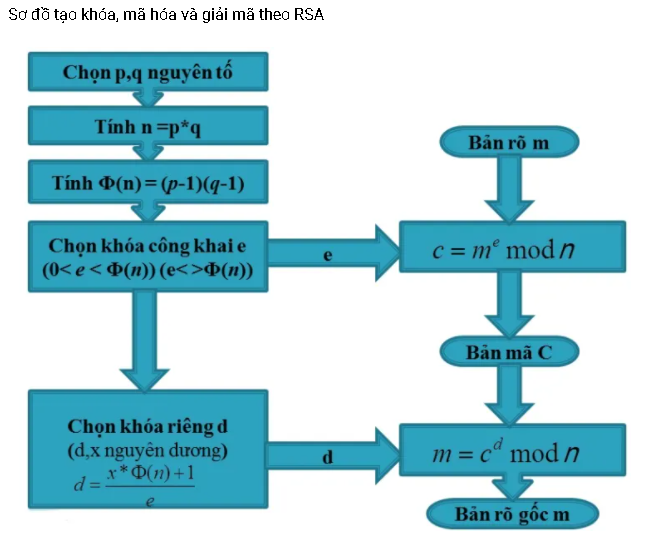


* ”d6499ff88ab014e37049a48d6fa58016d92344fd68ead0e26688e4297e341aece822fd4270a19f835ca26743ffa6d11d1b498579d412bc21087eea893c021f30”



**Câu 4: Tìm hiểu giải thuật RSA**

Truy cập đến địa chỉ <http://people.cs.pitt.edu/~kirk/cs1501/notes/rsademo/index.html> để tạo khóa, mã hóa, giải mã sử dụng giải thuật RSA. Sau đó mô tả ngắn gọn (sử dụng mã giả hoặc flow chart) cách RSA tạo khóa, mã hóa và giải mã.



**Câu 5: Chứng chỉ số**

Sử dụng một trình duyệt web truy cập đến địa chỉ <https://www.ctu.edu.vn/>,, sau đó tìm chứng chỉ số (SSL Server Certificate) của địa chỉ nói trên và trả lời các thông tin sau:

- Đơn vị phát hành chứng chỉ: AlphaSSL CA –SHA256 –G2

- Ngày hết hạn chứng chỉ: 29/05/2022

- Khóa công khai (public key) của chứng chỉ: RSA (2048 Bits)

30 82 01 0a 02 82 01 01 00 c5 43 0d 01 e0 ae d1 c9 26 f0 bc d7 6e bb ac e0 21 58 45 20 e2 34 2d ae 59 dd 93 73 25 3f ef 94 04 97 a5 e8 a3 91 b9 05 4a ce c1 0e 6d 2b 6f 8e e6 c4 63 af 14 ca a8 dc 8c 0f cc bc 7d 07 4b 94 b3 3a f9 88 72 60 27 74 d9 14 e0 a3 01 28 6a 62 77 81 dc 0f 67 50 b3 c5 cb 0c b0 01 5d 9c 20 03 7c 50 28 8b 2a 94 0e 3a 92 73 bf 27 80 81 bc ee 2b 6e 38 f6 82 d1 a7 c1 a5 6a f7 8e a9 ae 0f 9f dc 23 fc 59 dd b0 4a ff c9 cf db e2 b8 2a 33 8f 9c 4b 00 db f6 0f 03 13 fa 87 e7 0d 55 ed 2c 2b 8d aa f4 33 ce 37 2d 02 c5 04 0b 08 a1 c3 aa 28 63 90 45 eb ce 2f 13 69 7c 94 24 c8 df fa dc ec 89 91 68 ad ac 2b 13 61 0f b1 f2 48 68 7b e2 64 f2 00 39 59 d2 d6 00 8e f0 8d ac b9 71 ea cc 44 f6 93 d2 b3 01 95 7d 81 f0 0e 2f 91 5a b7 de 18 22 50 f8 86 02 f0 7f 68 7f fa f6 1d b6 e5 db 8d 02 03 01 00 01

**Câu 6: Bẻ khoá giải thuật RSA sử dụng khoá ngắn (Không bắt buộc)**

Tham khảo và thực hiện hướng dẫn thực hiện bẻ khoá giải thuật RSA (sử dụng khoá ngắn). Chụp hình minh hoạ các bước thực hiện (chỉ cần thực hiện bước 5a trong hướng dẫn)

<https://samsclass.info/141/proj/p5RSA2.htm>

---HẾT---