LAB 12

Thầy Mai Hoàng Đỉnh
Trường đại học FPT

Người thực hiện
Đặng Hoàng Nguyên

Lab-Proj 12: The Sleuth Kit and Autopsy

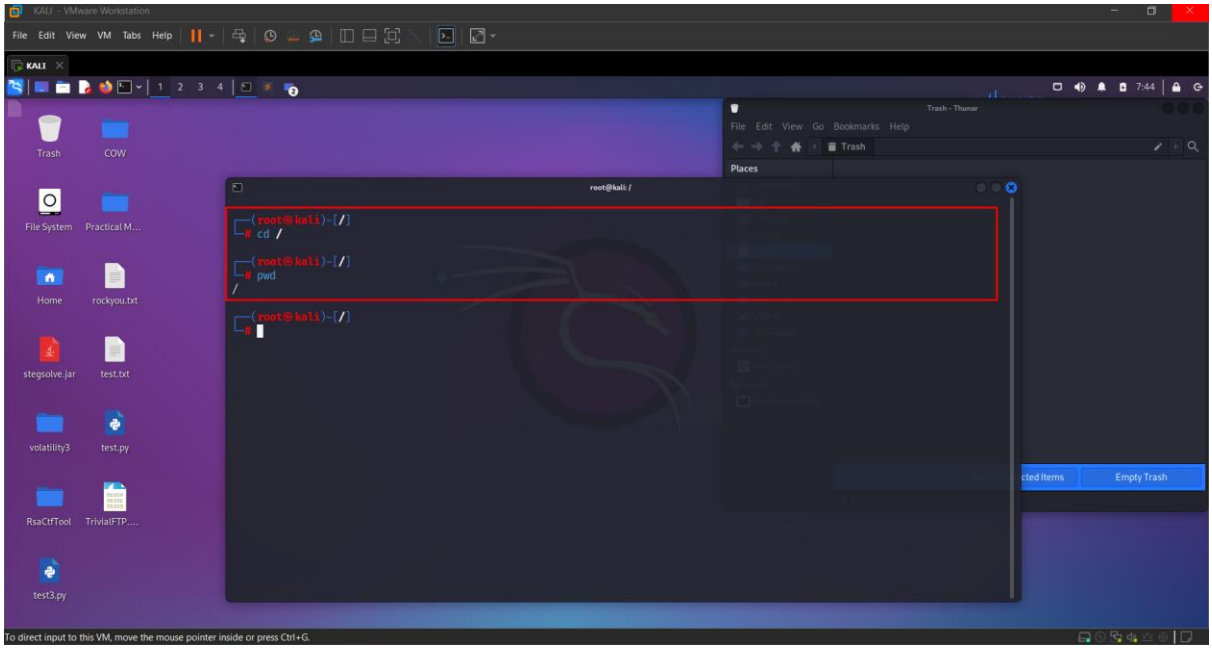
Những thứ cần cho bài lab

- Tại đây em sử dụng máy ảo Kali Linux phiên bản mới nhất (Kali purple). Chúng ta có thể thay vì sử dụng Kali thì có thể sử dụng máy ảo Deft để có thể sử dụng d
- Link https://www.sleuthkit.org/autopsy/

Putting the Evidence in the Backtrack VM

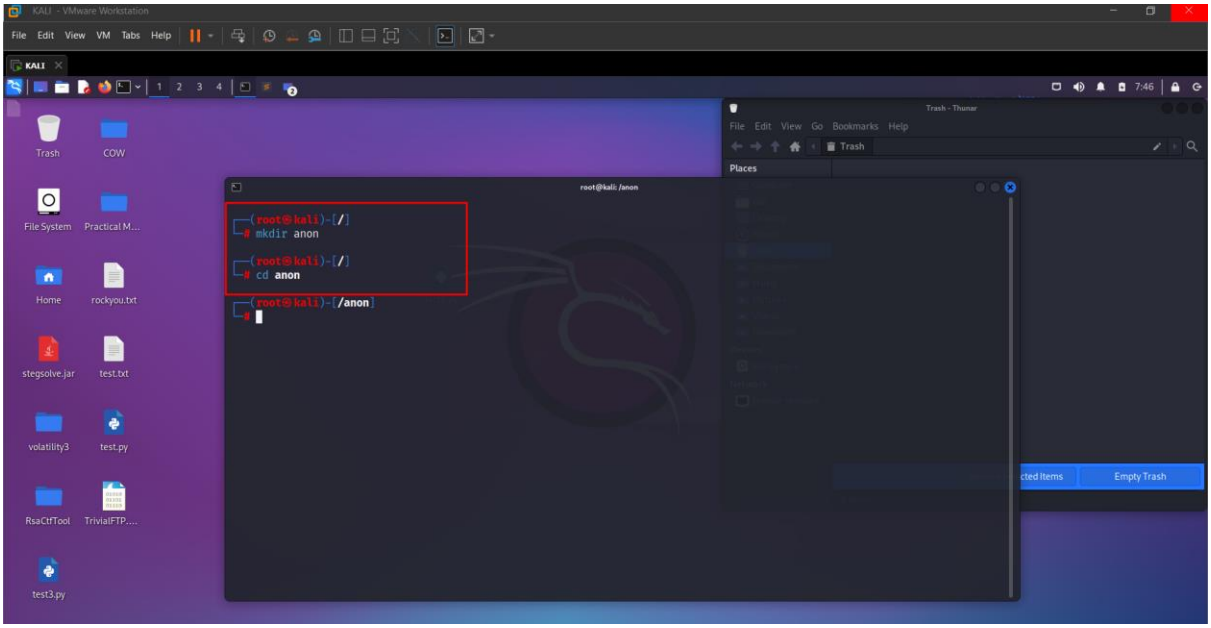
Trong máy ảo Kali, chúng ta sẽ thực hiện những câu lệnh sau để có thể lấy bằng chứng về để phuc vụ phân tích một cách dễ dàng hơn. Đầu tiên chúng ta sẽ vào bên trong thư mục root và bằng câu lệnh sau. Và kiểm tra bằng câu lệnh pwd

```
cd /
```



Sau đó tiến hành tạo một thư mục có tên là anon và truy cập vào trong thư mục anon đó với các câu lệnh sau:

```
mkdir anon
cd anon
```



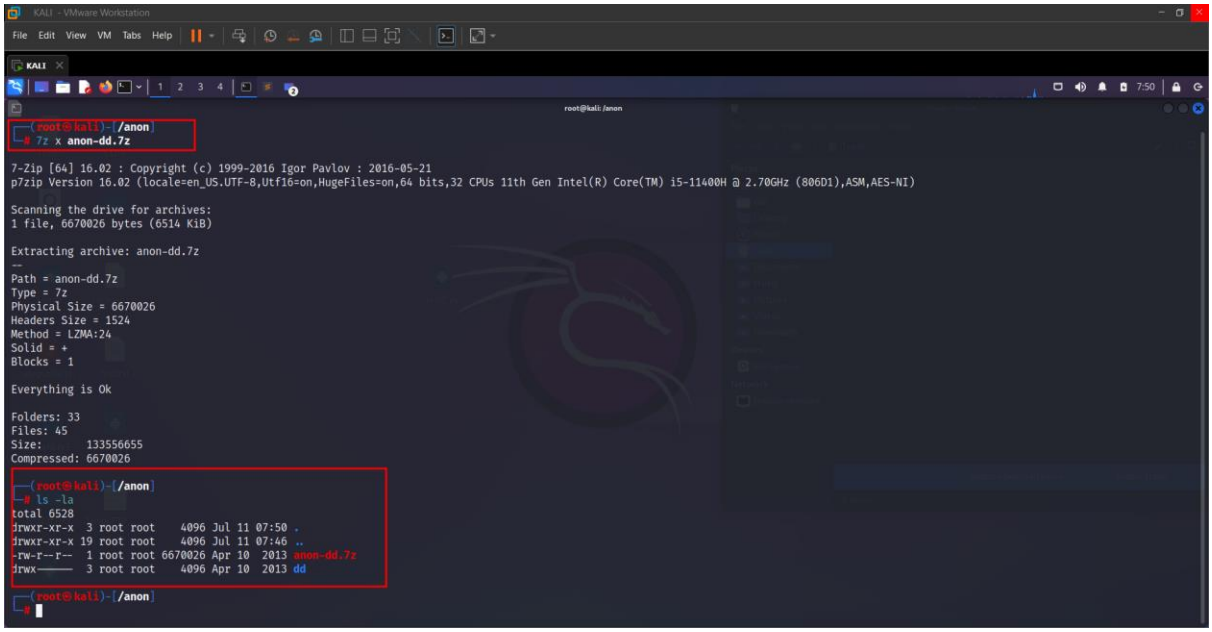
Sau khi đã vào được bên trong, ta sẽ tiến hành download bằng câu lệnh wget - Câu lệnh "wget" là một câu lệnh được sử dụng trong hệ điều hành Linux và các hệ điều hành tương tự như Unix để tải xuống (download) file từ Internet. Từ viết tắt "wget" có nghĩa là "Web Get". Và sau đó sử dụng câu lệnh ls -la để hiển thị tất cả các file, folder có trong thư mục anon để kiểm tra xem đã Download thành công hay chưa.

```
wget http://samsclass.info/121/proj/anon-dd.7z
```

Nhận thấy rằng file này có đuôi file là 7z nên chúng ta sẽ sử dụng câu lệnh **7z** để có thể giải nén file ra. Sử dụng câu lệnh như sau:

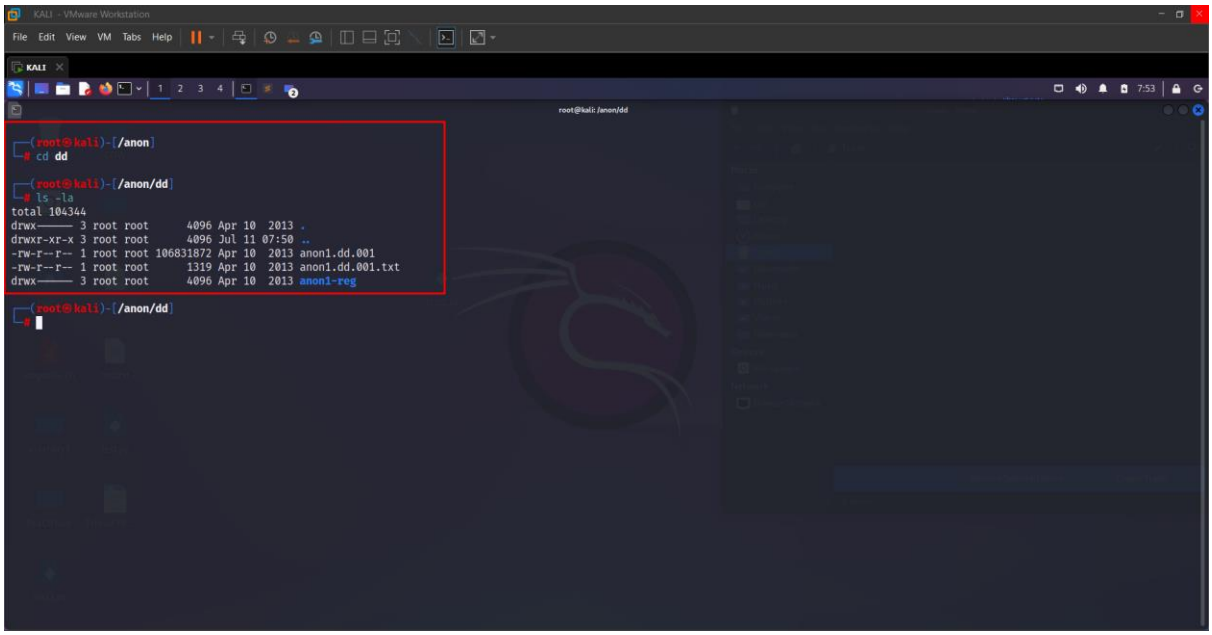
```
7z x anon-dd.7z
```

Như ta thấy trong hình thì đã extract thành công. Sử dụng tiếp câu lệnh **ls -la** để có thể xem những file nào đã có bên trong folder. Thì ta dễ dàng thấy được sau khi unzip bằng chứng download từ trên mạng xuống thì ta thấy được rằng có một folder dd đã được tạo ra



Sử dụng câu lệnh cd vào bên trong folder dd vừa mới được giải nén xong và kiểm tra file trong đó thông qua câu lệnh **ls -la**

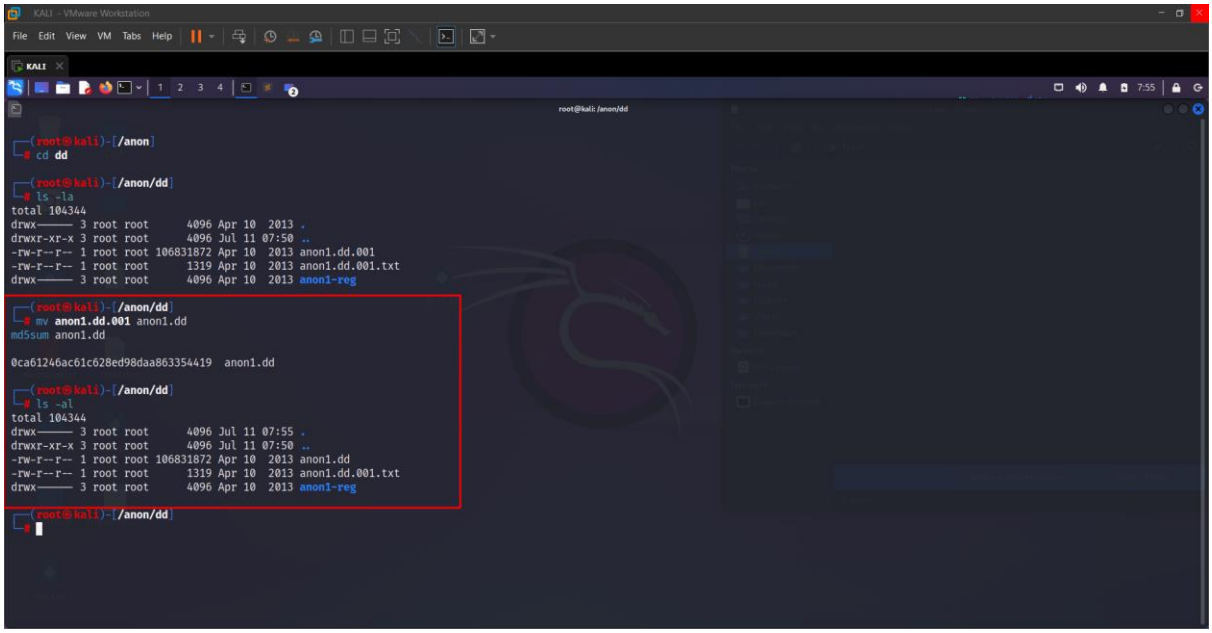
```
cd dd
```



Sau đó ta sẽ sử dụng câu lệnh **mv** để có thể đổi tên của file anon1.dd.001 thành anon1.dd và check md5sum của chúng qua câu lệnh md5sum:

```
mv anon1.dd.001 anon1.dd
md5sum anon1.dd
```

Như ta thấy rằng bây giờ file đã được chuyển từ anon1.dd.001 giờ đã chuyển đổi thành anon1.dd



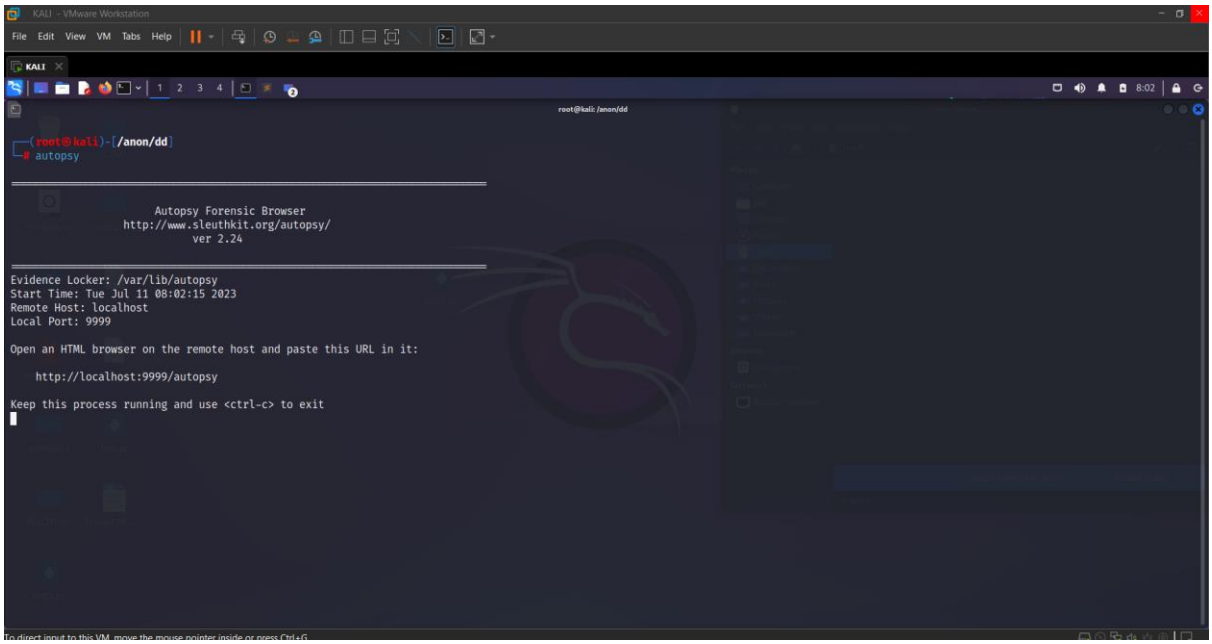
Sau khi kiểm tra md5sum của file với md5sum của bài lab thì có vẻ như là md5sum của chúng hoàn toàn là giống nhau với số đuôi là 4410

```
root@bt:/anon/dd# md5sum anon1.dd
0ca61246ac61c628ed98daa863354419  anon1.dd
root@bt:/anon/dd#
```

Starting Autopsy

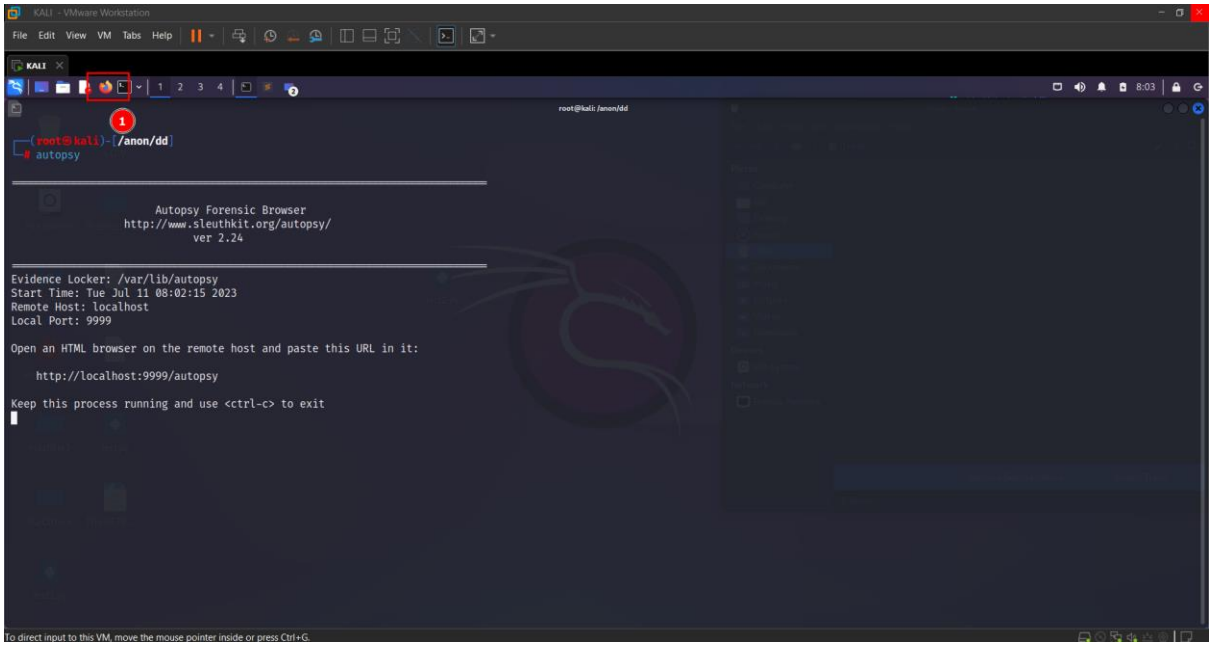
Trong kali linux, vì autopsy là một trình cài sẵn có bên trong kali, nên chúng ta chỉ việc vào bên trogn terminal và thực hiện các câu lệnh sau:

```
autopsy
```



Theo như hình ta có thể thấy rằng autopsy đã được khởi động thành công. Chạy local với port 9999. Việc của chúng ta bây giờ chỉ cần mở trình duyệt web trên Kali lên. Trong trường hợp này là firefox và truy cập vào đường dẫn url đó là được

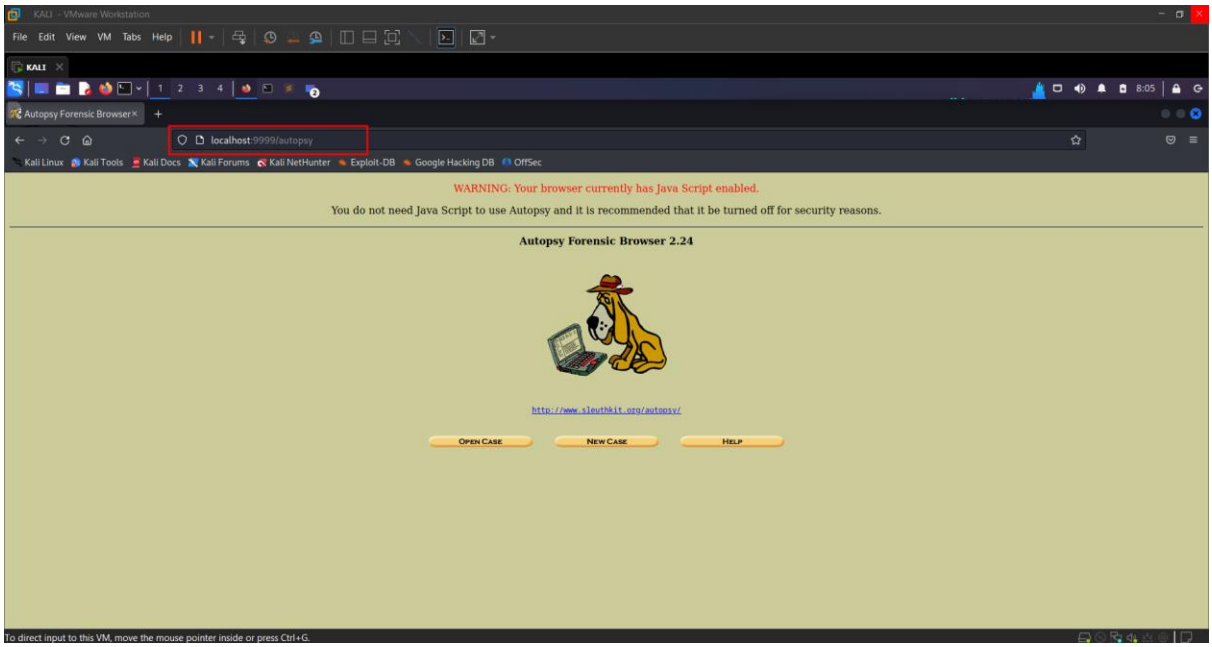
Trên thanh menu của Kali, có biểu tượng như hình dưới đây và chúng ta chỉ cần click vòa nó là được.



Khi trình duyệt Firefox đã được mở lên, chúng ta sẽ truy cập vòa đường dẫn mà autopsy đã cho chúng ta từ trước. Trong trường hợp này là:

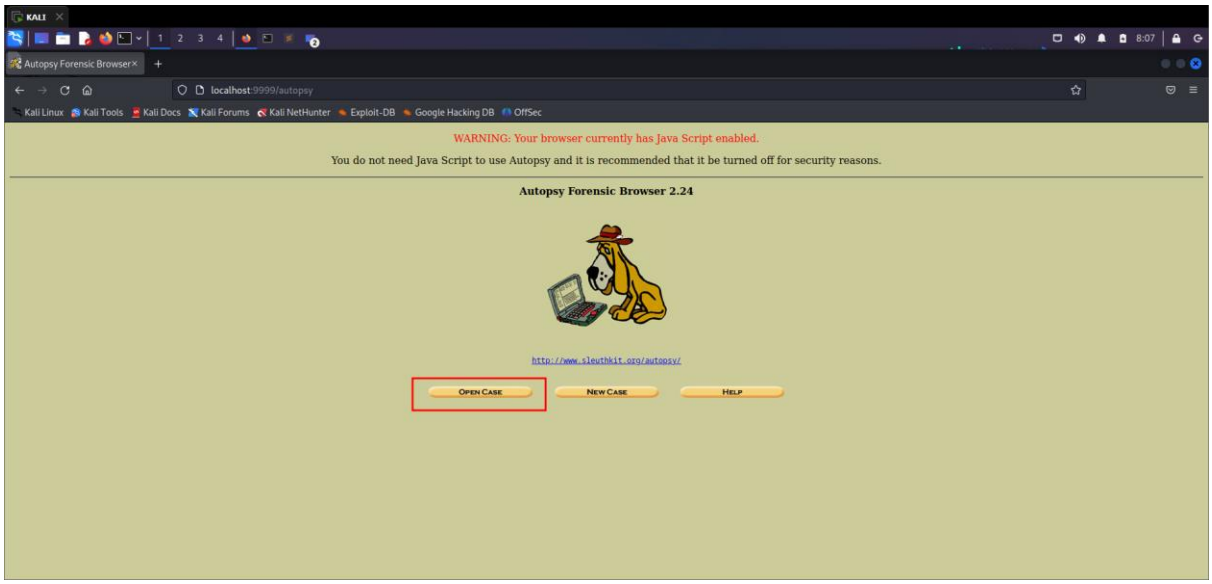
```
http://localhost:9999/autopsy
```

Như ta thấy hình bên dưới thì autopsy đã được kích hoạt thành công



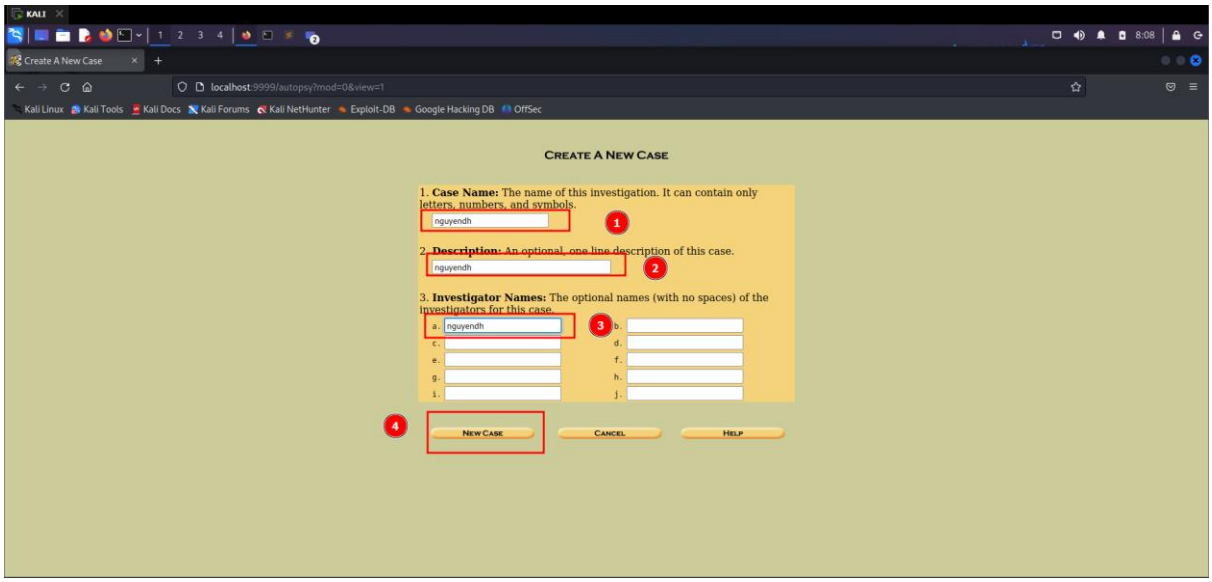
Opening a New Case in Autopsy

Trong phần mềm, chúng ta click chọn vào bên trogn phần “Open case” như hình bên dưới đây:

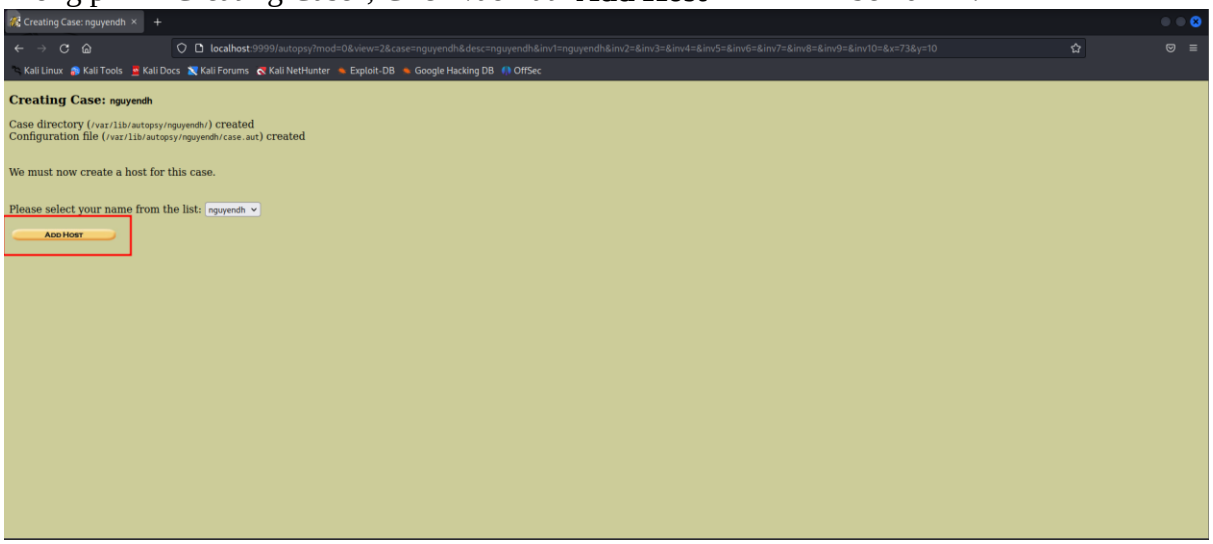


Chúng ta sẽ điền các thông tin cơ bản vào bên trong phần “Create a new case” như là case name, description và investigator name. Trong trường hợp này sẽ đển tên là nguyendh tại trường case name, description và investigator name như hình bên dưới đây

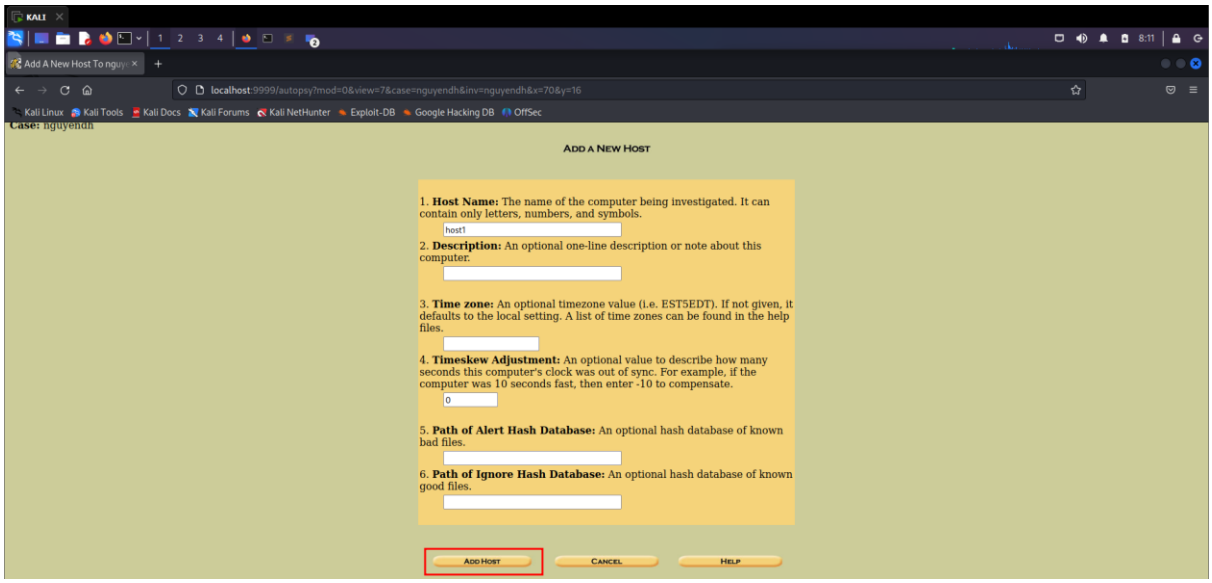
Sau đó click vào “New Case”



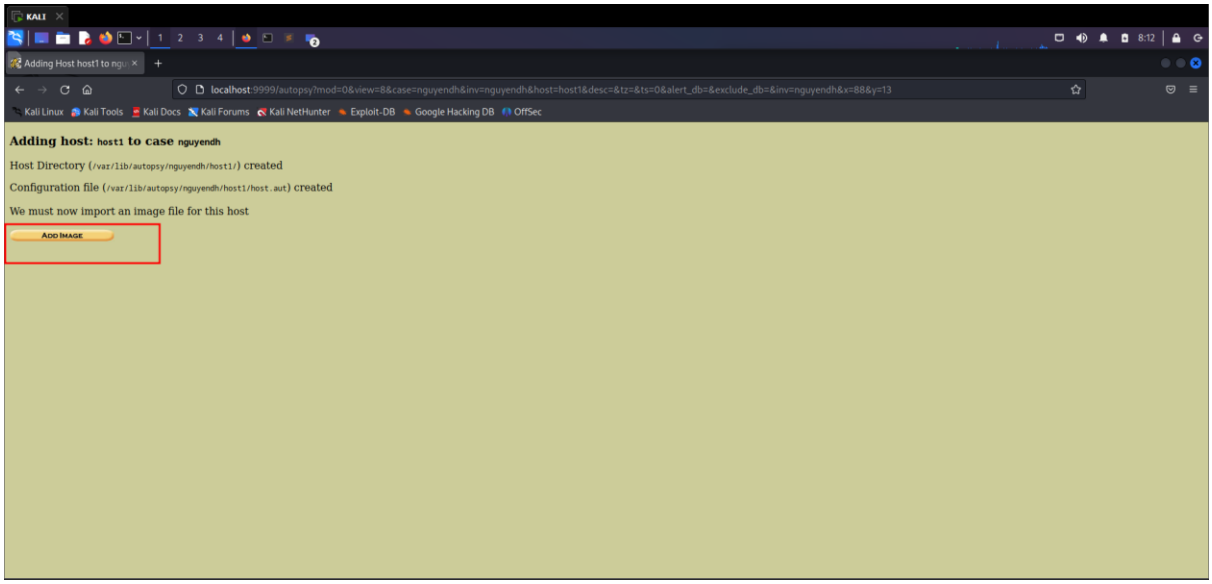
Trong phần "Creating Case", Click vào nút "**Add Host**" như hình bên dưới .



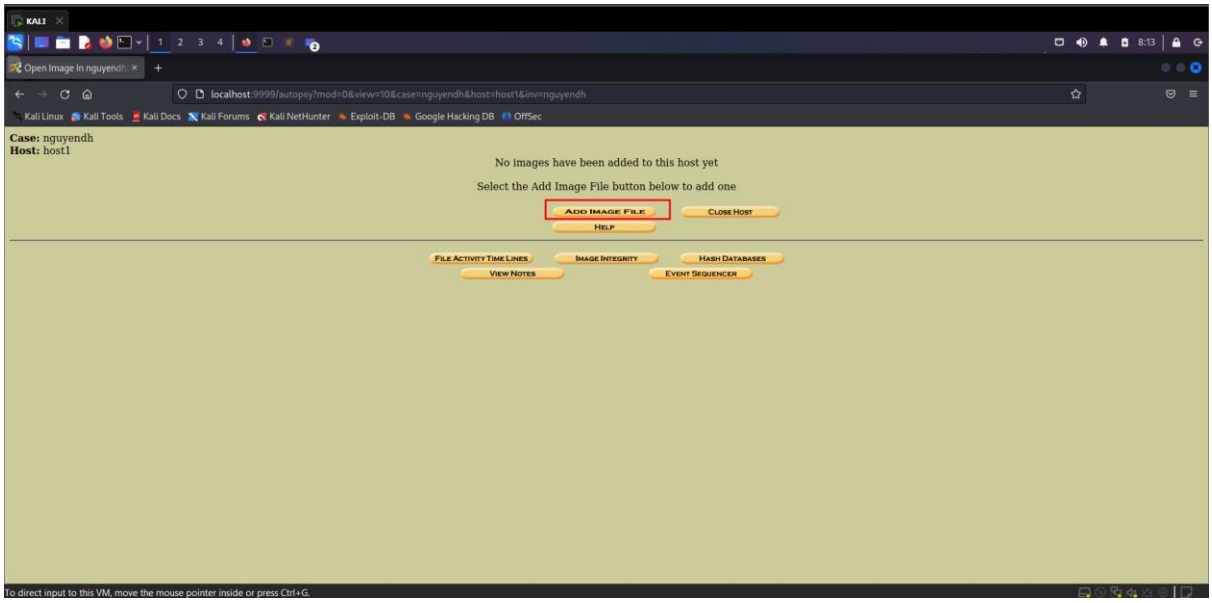
Trong phần "Add a New Host", thiết lập những tùy chọn mặc định và sau đso nhấn vào nút "**Add Host'.**



Trong phần "Adding host", nhấn vào phần "**Add Image**".



Trong cửa sổ tiếp theo, nhấn vào “Add Imgae File” để có thể cho thêm vào file chứng cứ,



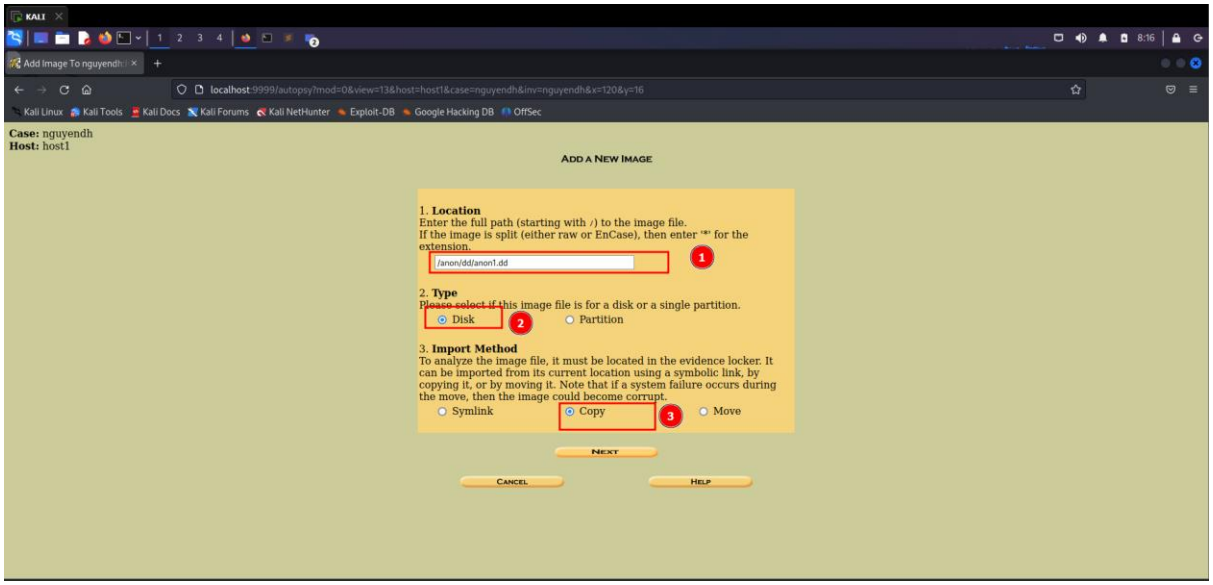
Trong phần “Add a New Image” Chúng ta sẽ lựa chọn theo những lựa chọn dưới đây đối với bài lab này.

- Location: **/anon/dd/anon1.dd**
- Type: **Disk**
- Import Method: **Copy**

Location là nơi mà ổ đĩa đang có, trong trường hợp này sẽ là /anon/dd/anon1.dd

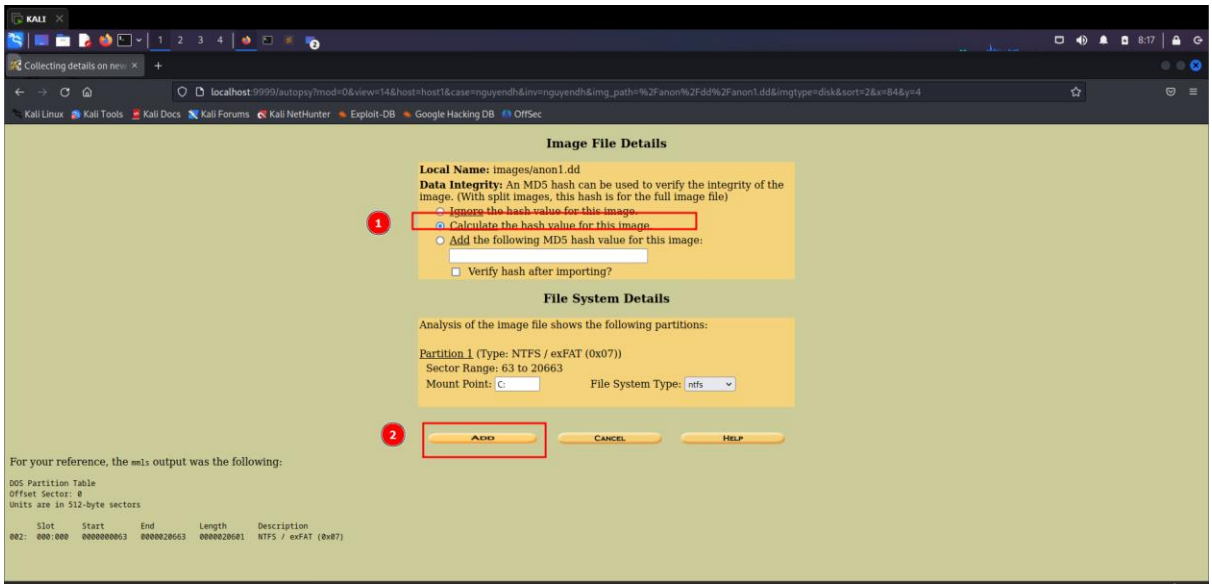
Type: là loại ổ đĩa mà chúng ta đang cần mà phân tích. Trong trường hợp này là Disk

Import Method: Phương thức ở đây chúng ta sẽ chọn là Copy

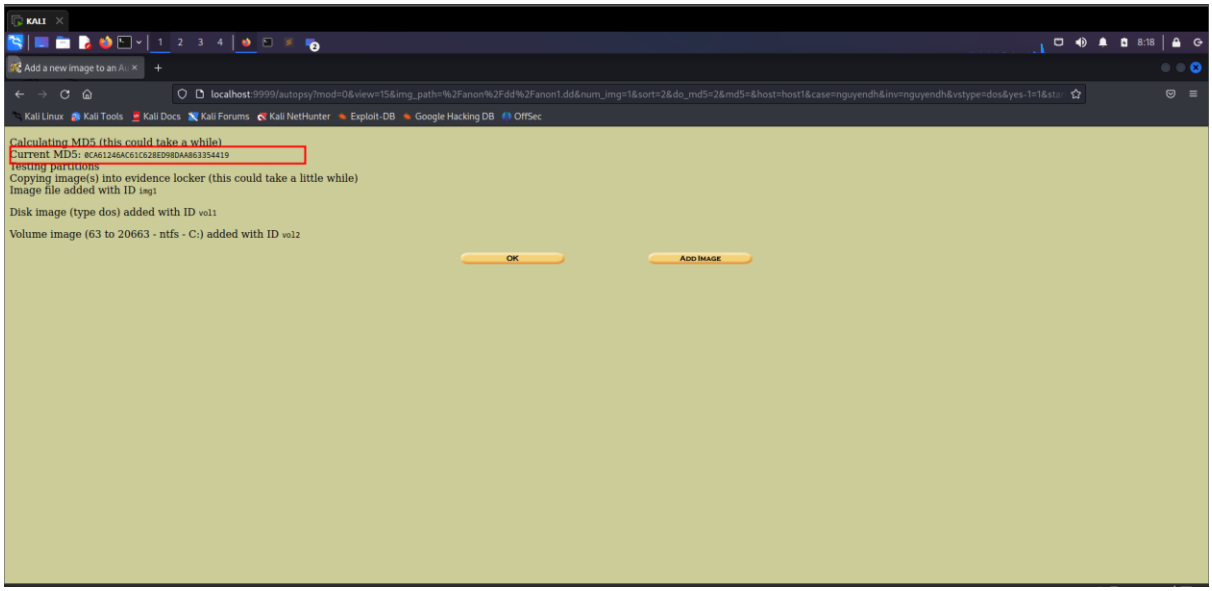


Sau đó nhấn vào next **Next**.

Trong phần "Image File Details", nhấn vào "**Calculate the hash value for this image**" như hình bên dưới và sau đó nhấn vào**Add**.



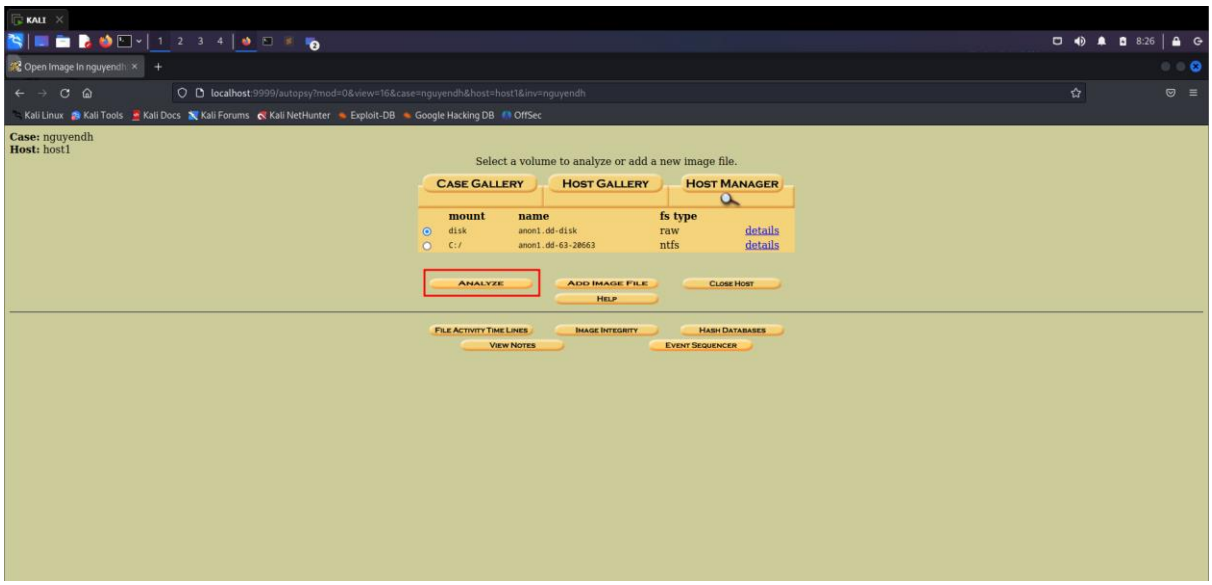
Sau đó, trên mà hình của chúng ta sẽ hiện ra mã hash của file anon1.dd thì ta có thể dễ dàng thấy được mã hash mà autopsy tính ra trùng với mã hash mà chúng ta đã tính từ trước đó



Sau đó nhấn vào **OK**.

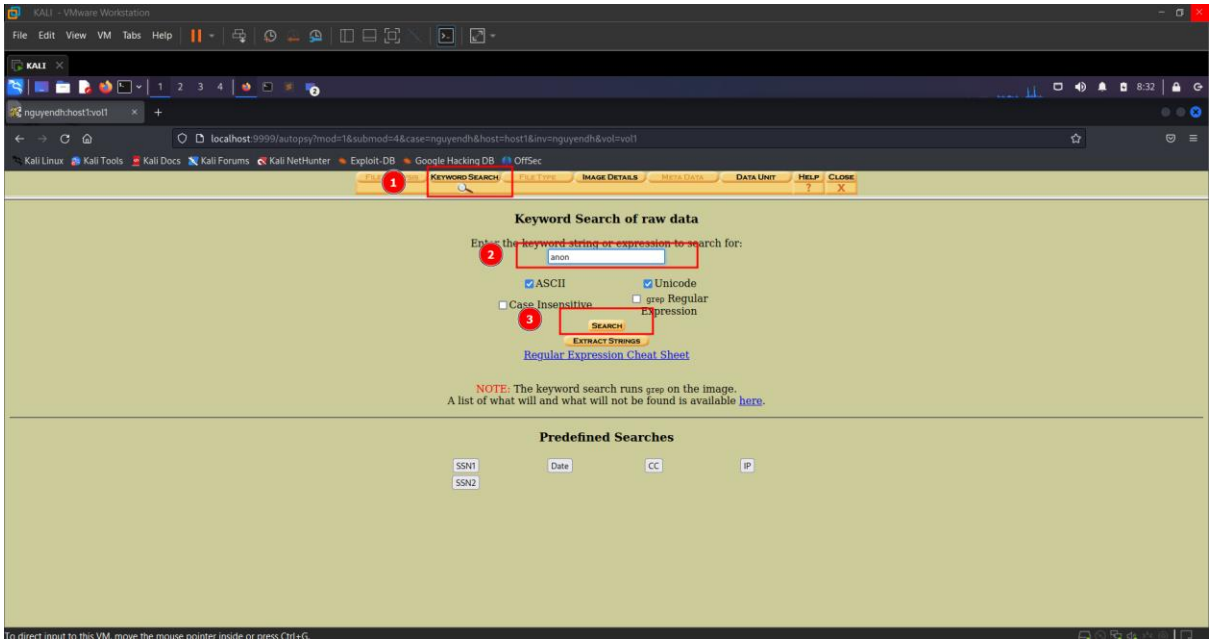
Searching in Autopsy

Sau đó, sẽ có phần "Select a volume to analyze or add a new image file" xuất hiện, như hình bên dưới, nhấn vào bên trong phần **Analyze**



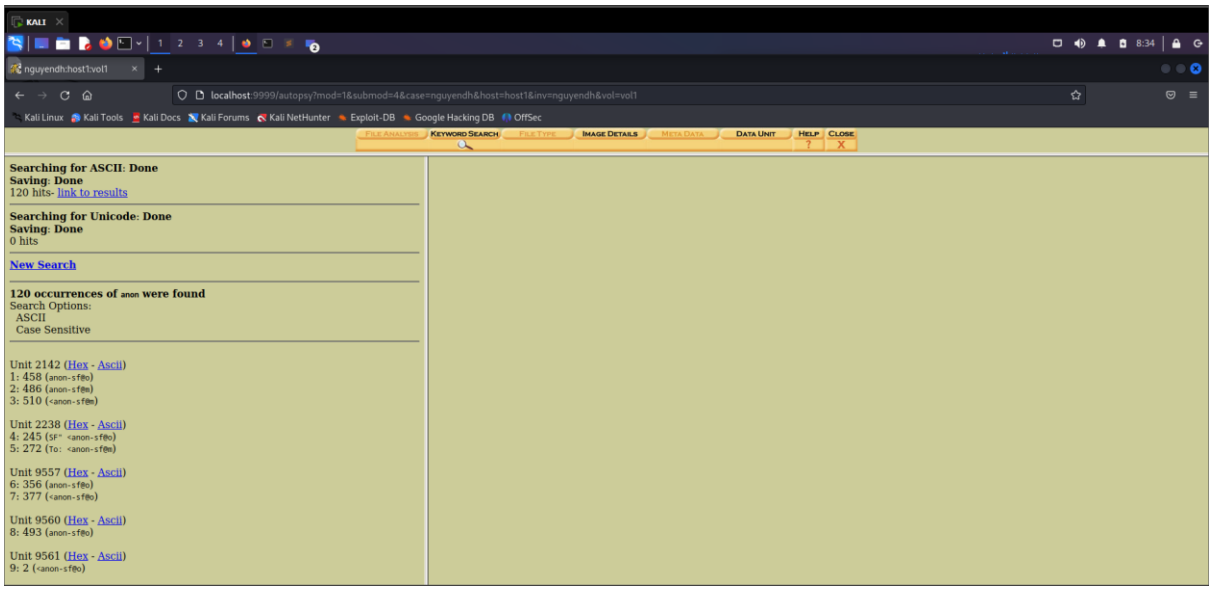
Trong cửa sổ tiếp theo nhấn vào phần Search.

Trong phần search, chúng ta sẽ nhấn kiểm tra chuỗi anon, và sau đó nahasn search



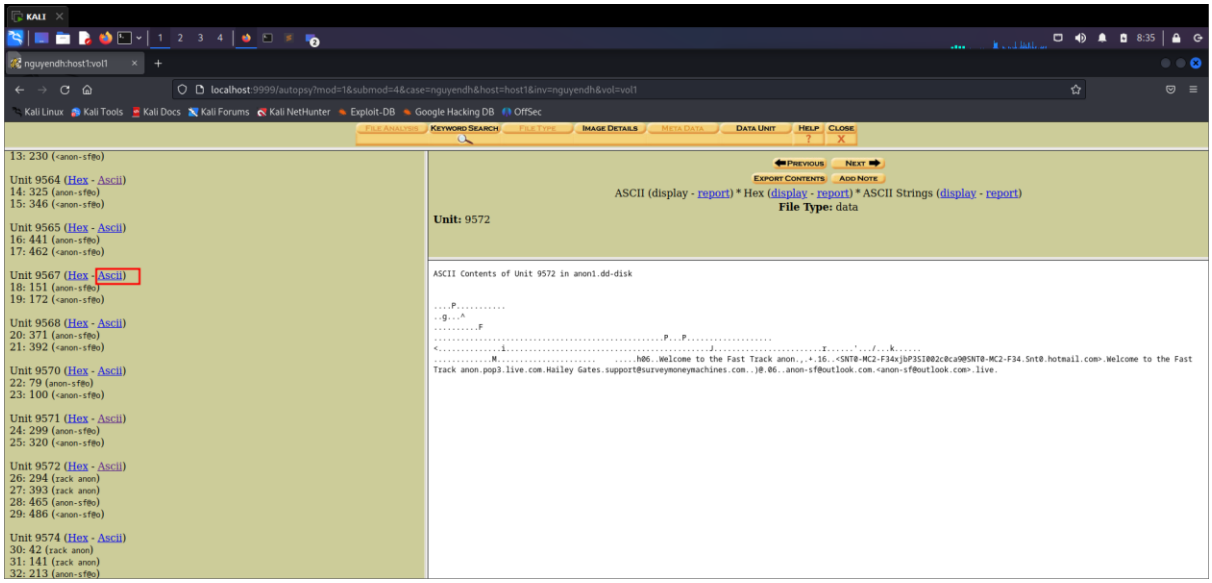
Results of the Search

Như ta thấy hình bên dưới thì có vẻ như là từ anon này được tìm thấy rất nhiều, tận 120 lần tìm thấy



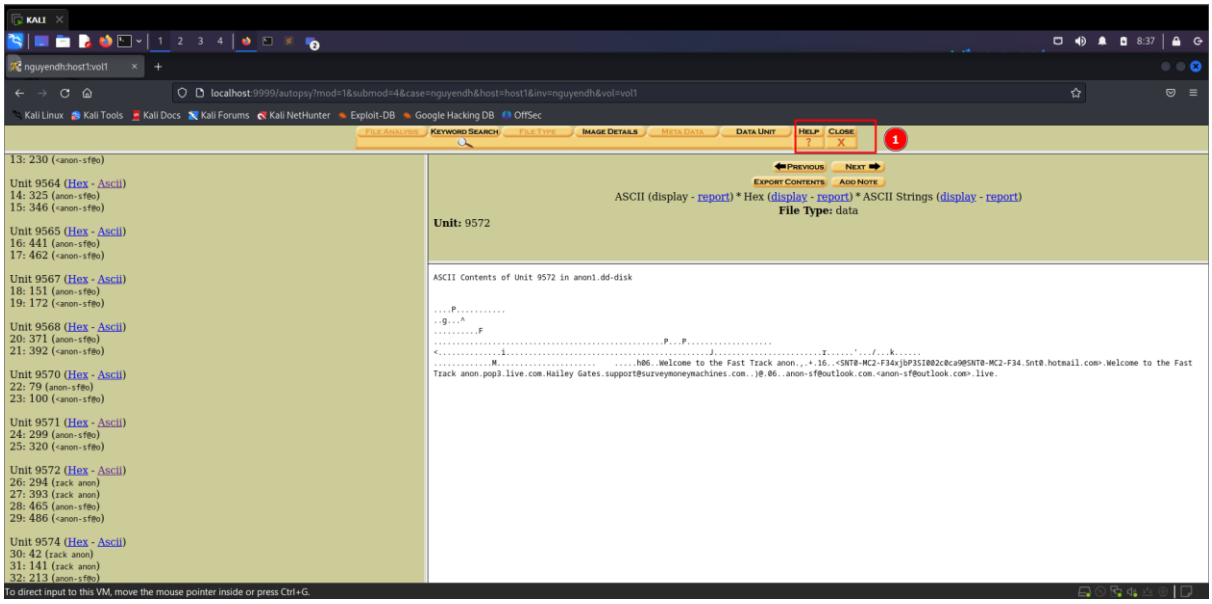
Examining the Hits

Trên phía bên trái, nhấp vào các liên kết Ascii màu xanh đầu tiên để xem chi tiết về kết quả trong khung bên phải, như được hiển thị dưới đây.

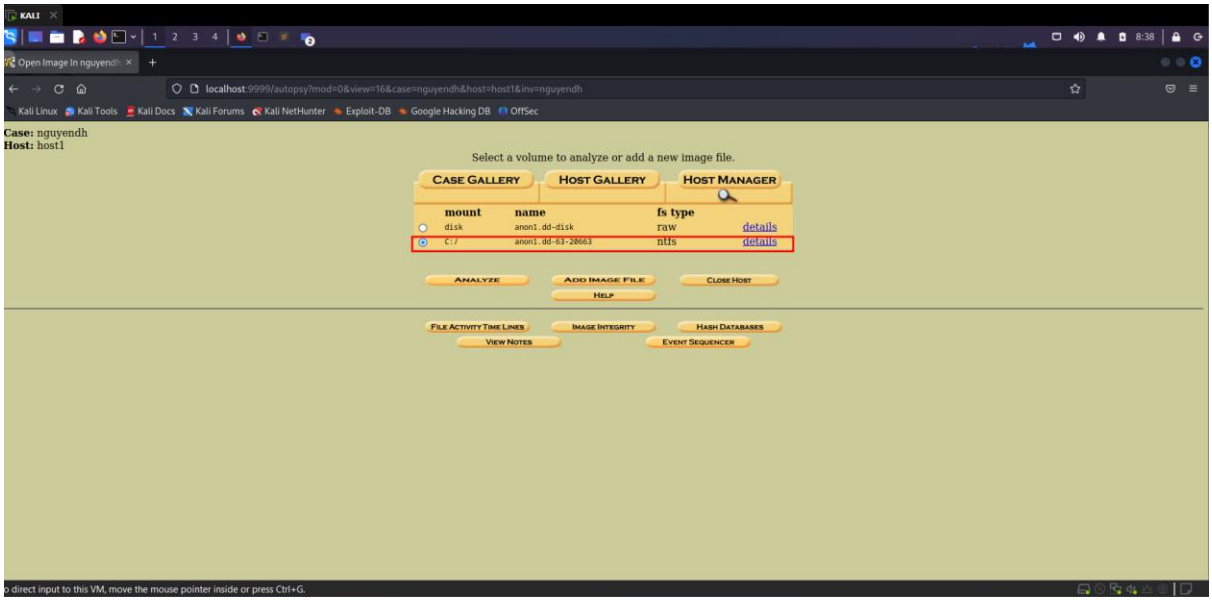


File Analysis

Sau khi tìm chuỗi xong, trên góc màn hình, nhấn vào close để có thể kết thúc case



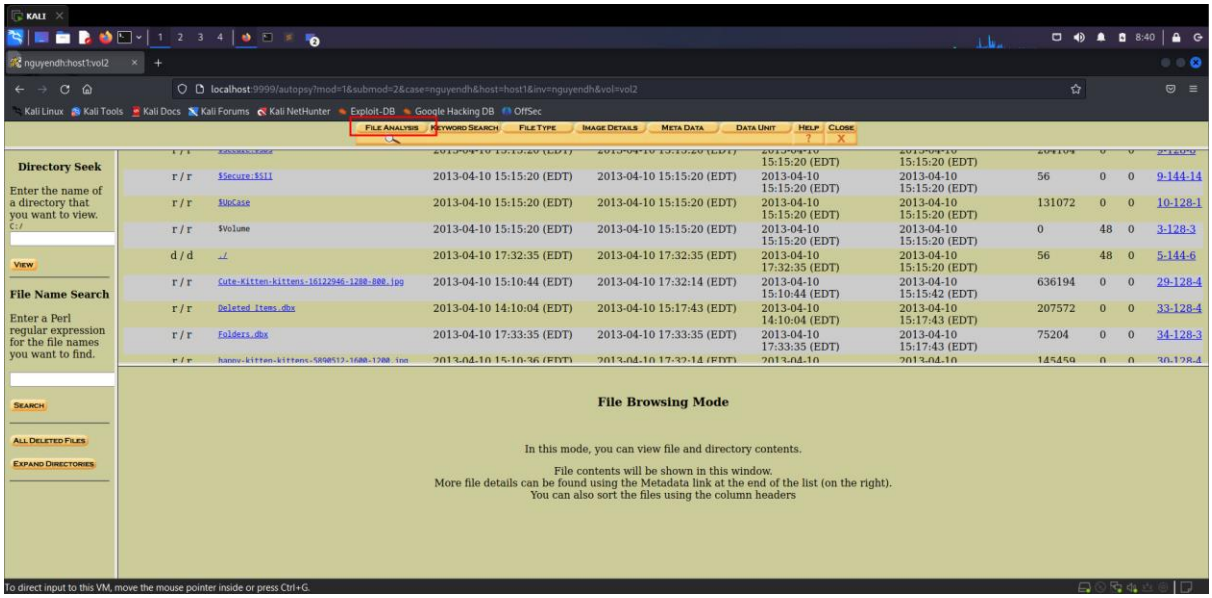
Trong phần các case, nhấn vào phần ổ C:/ như hình bên dưới



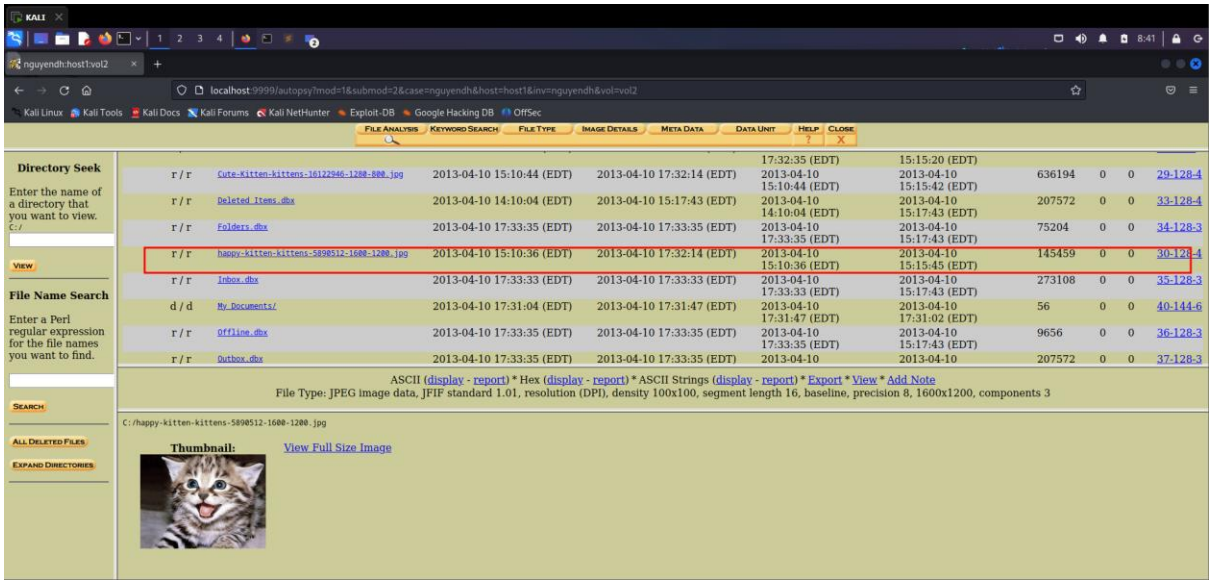
Sau đó chúng ta sex nhấn chọn tiếp vào bên trong phần Analyze

Ở trên bên trái, nhấn vào bên trong phần "**File Analysis**".

Một list thư mục được hiện như hình bên dưới



Ta sẽ tìm tới file những chú mèo con như hình dứi đây


KALI
nguyendh:host1:vol2
localhost:9999/autopsy?mod=1&submod=2&case=nguyendh&host=host1&inv=nguyendh&vol=vol2
Kali Linux
Kali Tools
Kali Docs
Kali Forums
Kali NetHunter
Exploit-DB
Google Hacking DB
OffSec
File Analysis
Keyword Search
File Type
Image Details
Meta Data
Data Unit
Help
Close
Directory Seek
Enter the name of a directory that you want to view.
C:/
View
File Name Search
Enter a Perl regular expression for the file names you want to find.
Search
All Deleted Files
Expand Directories
r / r Cute-Kitten-kittens-16122946-1280-800.jpg 2013-04-10 15:10:44 (EDT) 2013-04-10 17:32:14 (EDT) 2013-04-10 15:10:44 (EDT) 2013-04-10 15:15:42 (EDT) 636194 0 0 29-128-4
r / r Deleted Items.dbx 2013-04-10 14:10:04 (EDT) 2013-04-10 15:17:43 (EDT) 2013-04-10 14:10:04 (EDT) 2013-04-10 15:17:43 (EDT) 207572 0 0 33-128-4
r / r Folders.dbx 2013-04-10 17:33:35 (EDT) 2013-04-10 17:33:35 (EDT) 2013-04-10 17:33:35 (EDT) 2013-04-10 15:17:43 (EDT) 75204 0 0 34-128-3
r / r happy-kitten-kittens-5890512-1600-1200.jpg 2013-04-10 15:10:36 (EDT) 2013-04-10 17:32:14 (EDT) 2013-04-10 15:10:36 (EDT) 2013-04-10 15:15:45 (EDT) 145459 0 0 30-128-4
r / r Inbox.dbx 2013-04-10 17:33:33 (EDT) 2013-04-10 17:33:33 (EDT) 2013-04-10 17:33:33 (EDT) 2013-04-10 15:17:43 (EDT) 273108 0 0 35-128-3
d / d My Documents/ 2013-04-10 17:31:04 (EDT) 2013-04-10 17:31:47 (EDT) 2013-04-10 17:31:47 (EDT) 2013-04-10 17:31:02 (EDT) 56 0 0 40-144-6
r / r Offline.dbx 2013-04-10 17:33:35 (EDT) 2013-04-10 17:33:35 (EDT) 2013-04-10 17:33:35 (EDT) 2013-04-10 15:17:43 (EDT) 9656 0 0 36-128-3
r / r Outbox.dbx 2013-04-10 17:33:35 (EDT) 2013-04-10 17:33:35 (EDT) 2013-04-10 2013-04-10 207572 0 0 37-128-3
ASCII (display - report) * Hex (display - report) * ASCII Strings (display - report) * Export * View * Add Note
File Type: JPEG image data, JFIF standard 1.01, resolution (DPI), density 100x100, segment length 16, baseline, precision 8, 1600x1200, components 3
C:/happy-kitten-kittens-5890512-1600-1200.jpg
Thumbnail:
View Full Size Image