

# BÁO CÁO THỰC HÀNH

Môn học: Pháp chứng kỹ thuật số

Kỳ báo cáo: Buổi 6

Tên chủ đề: root-me

GVHD: Lê Đức Thịnh

Ngày báo cáo: 12/6/2023

**Nhóm: 7**

## 1. THÔNG TIN CHUNG:

(Liệt kê tất cả các thành viên trong nhóm)

Lớp: NT334.N21.ANTN

STT	Họ và tên	MSSV	Email
1	Nguyễn Bùi Kim Ngân	20520648	20520648@gm.uit.edu.vn
2	Nguyễn Bình Thục Trâm	20520815	20520815@gm.uit.edu.vn
3	Võ Anh Kiệt	20520605	20520605@gm.uit.edu.vn

## 2. NỘI DUNG THỰC HIỆN:<sup>1</sup>

STT	Công việc	Thực hiện	Thành viên thực hiện	Kết quả tự đánh giá
1	Root-me	5 challenge Command & Control	Kiệt Trâm Ngân	100%
2	Root-me	11 challenge Steganography	Kiệt Trâm Ngân	100%
3				

**Lưu ý:** Chỉ ghi Kịch bản thực hành được GVTH chỉ định phải làm báo cáo

Phần bên dưới của báo cáo này là tài liệu báo cáo chi tiết của nhóm thực hiện.

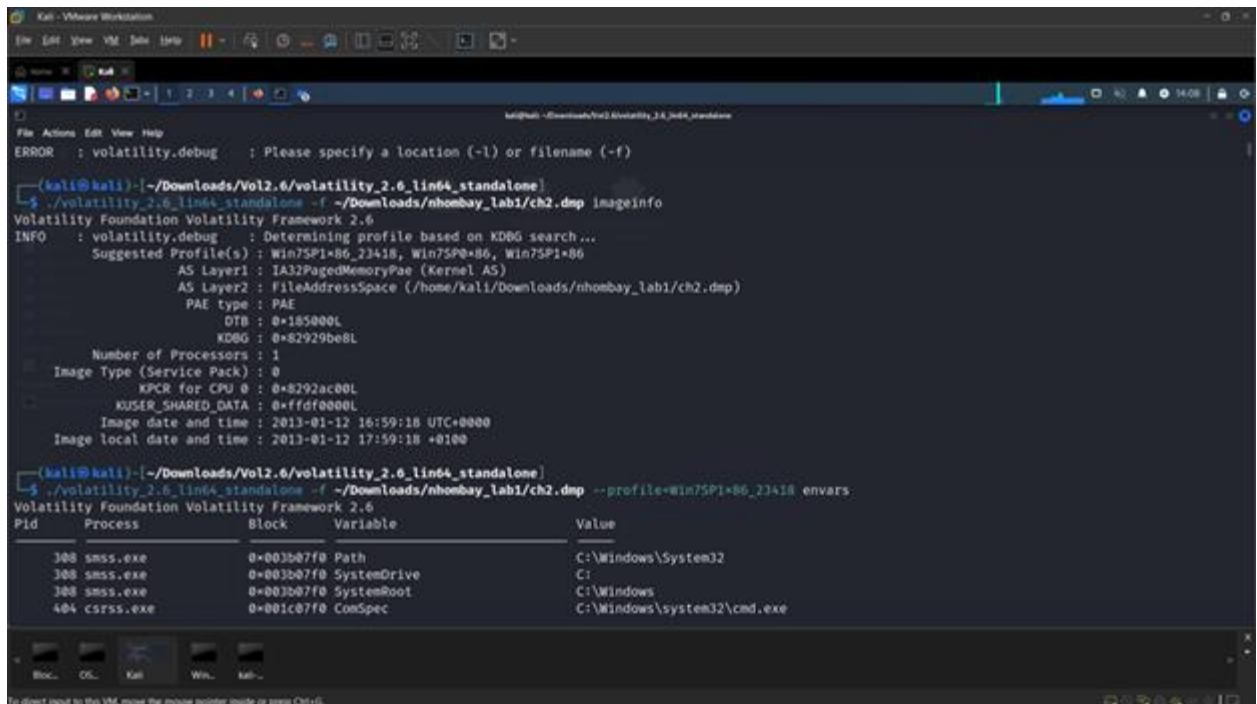
(Xem trang kế tiếp)

<sup>1</sup> Ghi nội dung công việc, các kịch bản trong bài Thực hành,

# BÁO CÁO CHI TIẾT

## Challenge 1: Command & Control 2

Đầu tiên, ta sẽ dùng lệnh imageinfo để kiểm tra thông tin file dump. Ta có thể thấy được profile của file để sử dụng trong các lệnh tiếp theo.



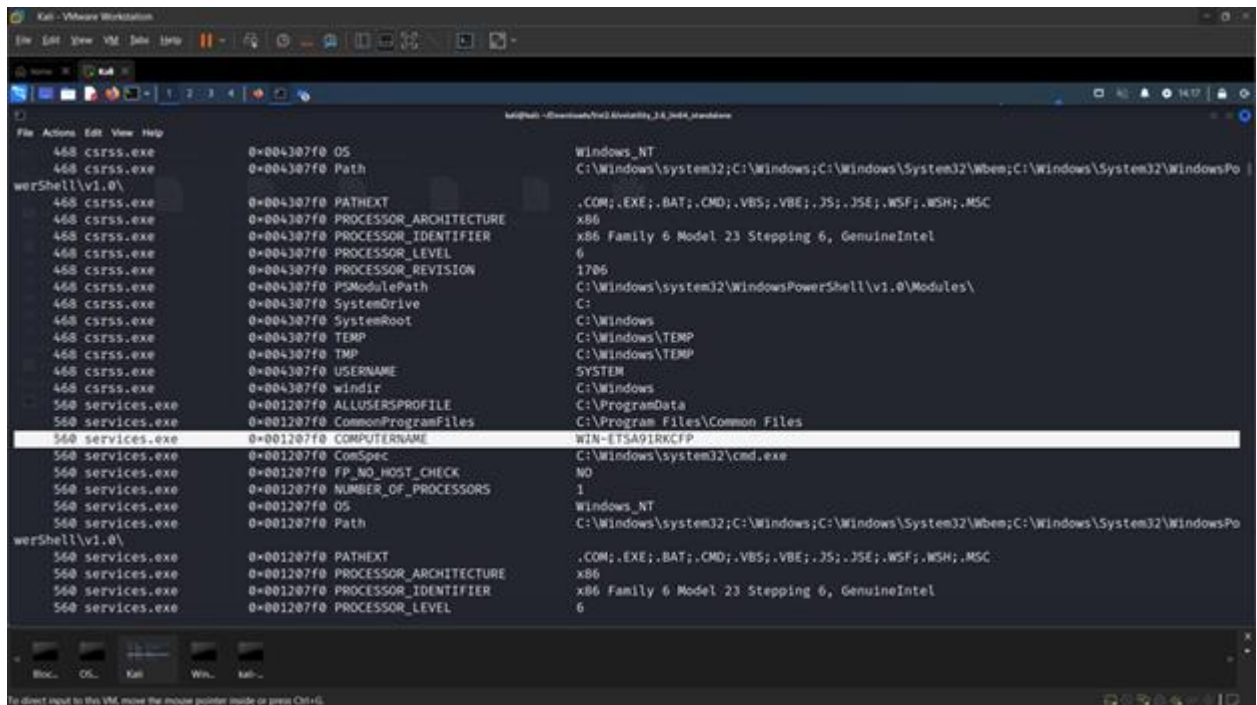
```
(kali@kali)~/.Downloads/Vol2.6/volatility_2.6_lin64_standalone
ERROR : volatility.debug : Please specify a location (-l) or filename (-f)

(kali@kali)~/.Downloads/Vol2.6/volatility_2.6_lin64_standalone
$ ./volatility_2.6_lin64_standalone -f ~/Downloads/nhombay_lab1/ch2.dmp imageinfo
Volatility Foundation Volatility Framework 2.6
INFO : volatility.debug : Determining profile based on KDBG search...
Suggested Profile(s) : Win7SP1x86_23418, Win7SP0x86, Win7SP1x86
AS Layer1 : IA32PagedMemoryPae (Kernel AS)
AS Layer2 : FileAddressSpace (/home/kali/Downloads/nhombay_lab1/ch2.dmp)
PAE type : PAE
DTB : 0x185000L
KDBG : 0x82929be8L
Number of Processors : 1
Image Type (Service Pack) : 0
XPCR for CPU 0 : 0x8292ac00L
KUSER_SHARED_DATA : 0xffdf0000L
Image date and time : 2013-01-12 16:59:18 UTC+0000
Image local date and time : 2013-01-12 17:59:18 +0100

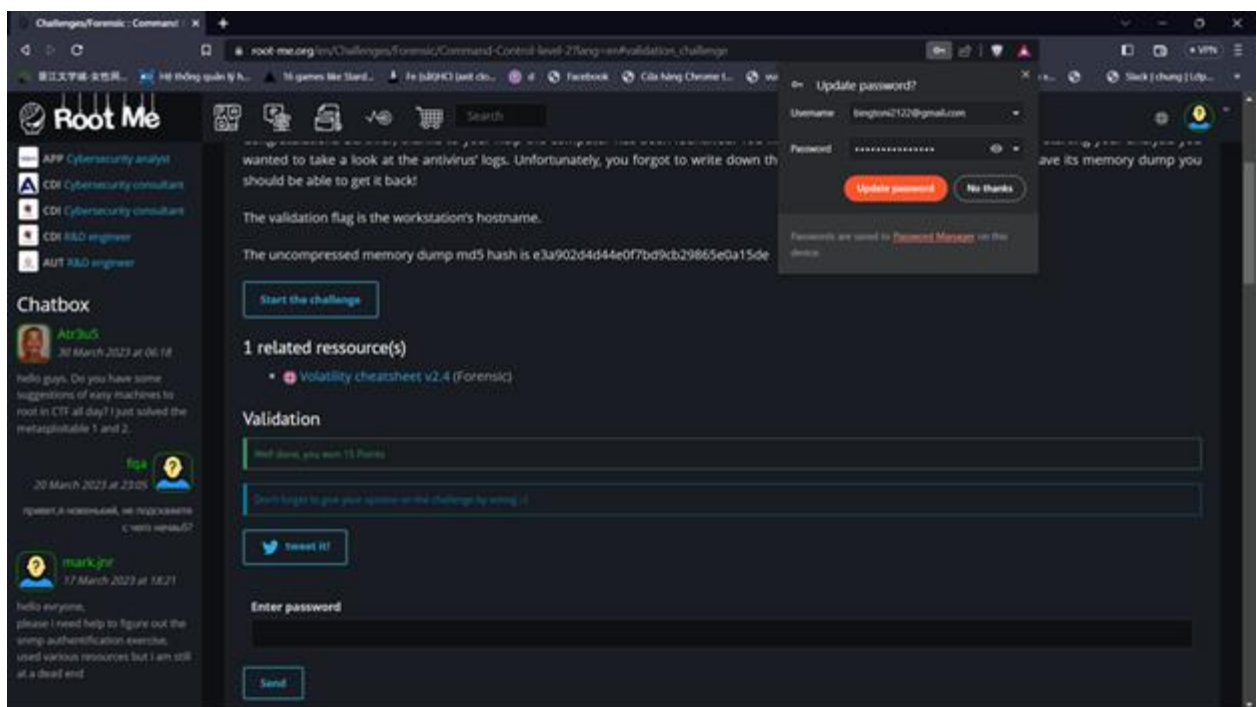
(kali@kali)~/.Downloads/Vol2.6/volatility_2.6_lin64_standalone
$ ./volatility_2.6_lin64_standalone -f ~/Downloads/nhombay_lab1/ch2.dmp --profile=Win7SP1x86_23418 envvars
Volatility Foundation Volatility Framework 2.6
```

Pid	Process	Block	Variable	Value
308	smss.exe	0x003b07f0	Path	C:\Windows\System32
308	smss.exe	0x003b07f0	SystemDrive	C:
308	smss.exe	0x003b07f0	SystemRoot	C:\Windows
404	csrss.exe	0x001c07f0	ComSpec	C:\Windows\system32\cmd.exe

Yêu cầu của bài này là sẽ tìm được COMPUTERNAME của file dump này. Theo như docs cmd thì plugin envvars sẽ trả về giá trị các biến môi trường của quy trình, thường thì nó sẽ là số lượng CPU được cài đặt và kiến trúc phần cứng, thư mục hiện tại của quy trình, thư mục tạm thời, tên phiên, tên máy tính, tên người dùng và nhiều tạo phẩm thú vị khác. Hiện tại, ta đang cần tìm computername, vì vậy ta sẽ dùng envvar để tìm được như hình bên dưới:



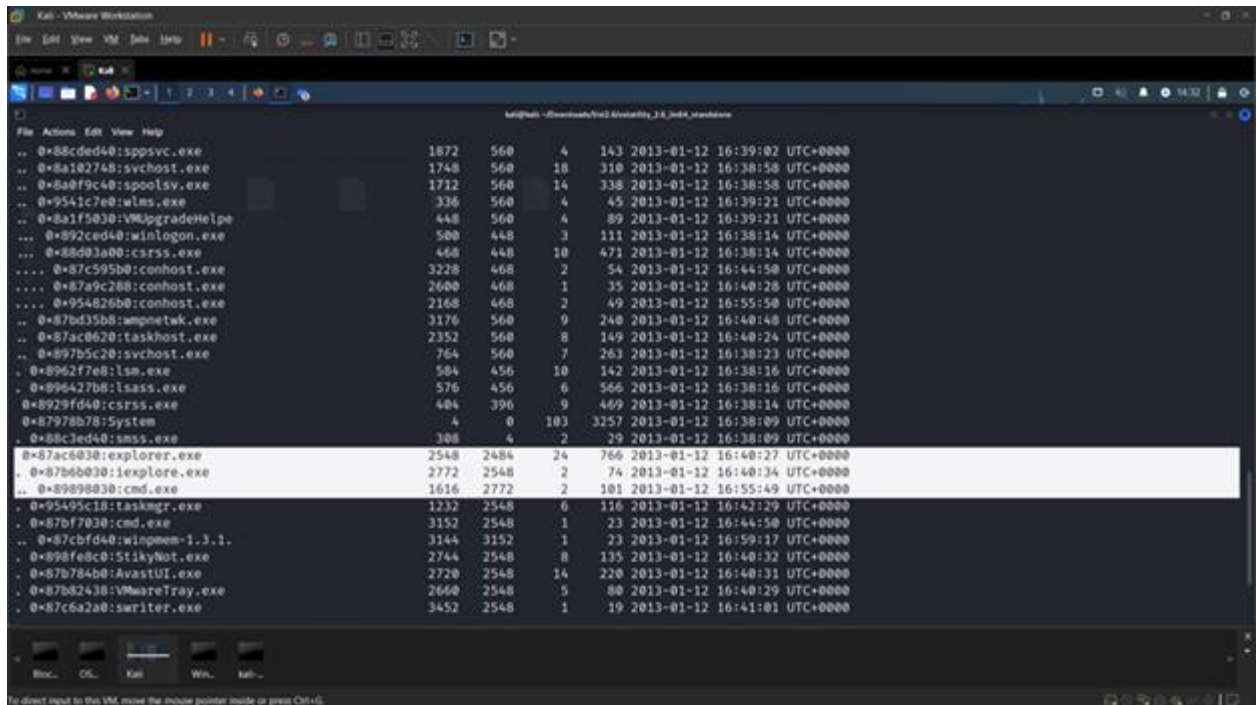
Sau đó, ta sẽ nhập flag: WIN-ETSA91RKCFP vào challenge và hoàn thành.



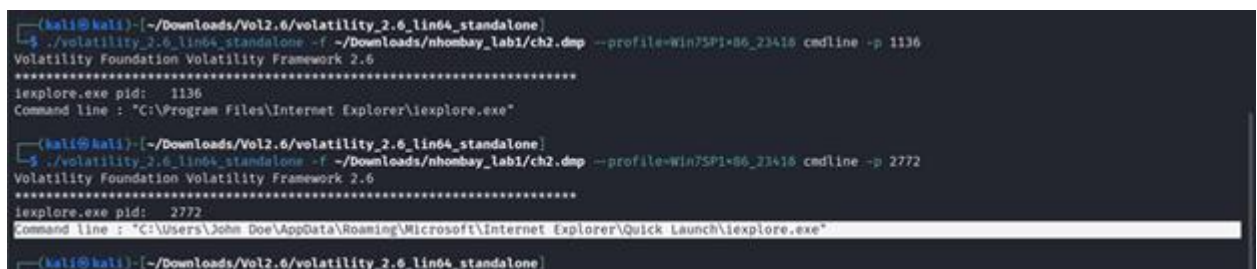
## Challenge 2: Command & Control 3

Trong câu này, đề bài yêu cầu tìm đường dẫn tuyệt đối của file thực thi nghi ngờ là malware. Trước tiên, chúng ta cần tìm file có các hành động bất thường trước. Em dùng plugin pstree để xem được các process đang chạy và quan hệ giữa chúng. Sau đó, chúng em tìm thấy có 1 process khá lạ ở explore.exe có process con là cmd.exe

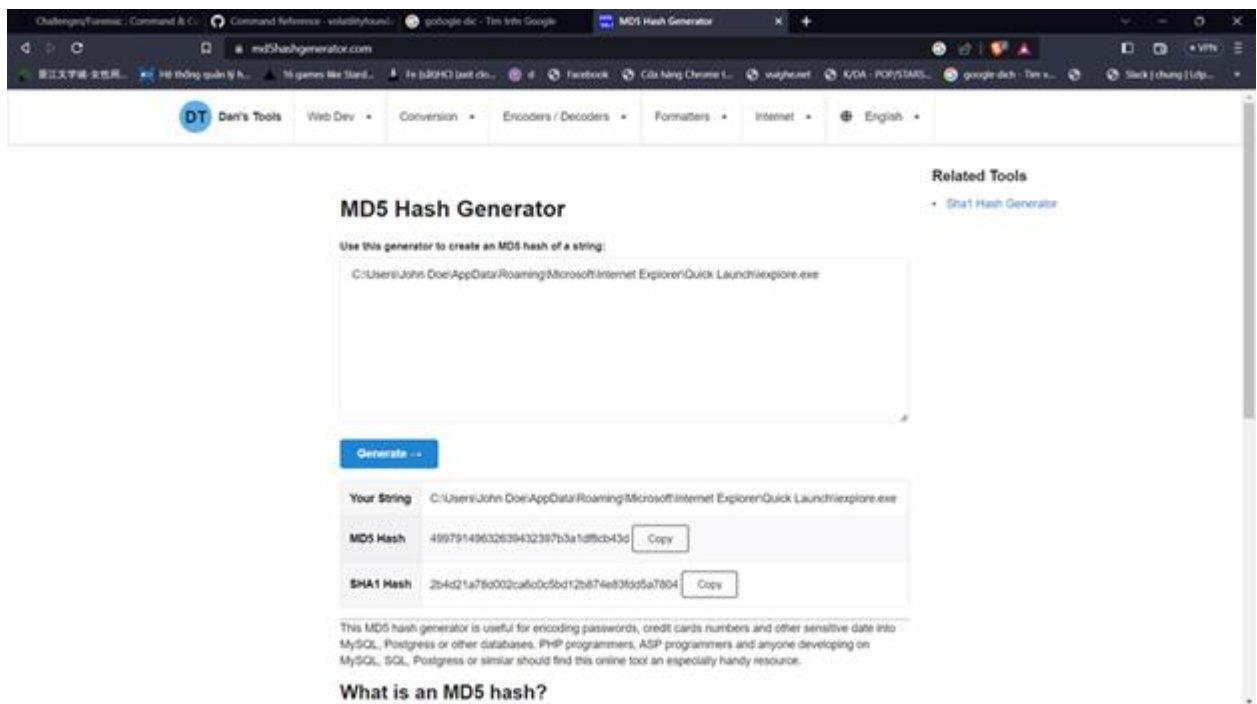
trong khi bên dưới cũng có 1 process explore.exe tương tự nhưng không hề chạy cmd.exe này.



=> File thực thi này có vẻ khá bất thường nên chúng em dự đoán nó có thể là malware, tụi em quyết định sẽ xem kĩ hơn khi thực thi file này nó đã chạy các lệnh nào bằng plugin cmdline. Bên dưới, chúng em đã kiểm tra cmdline của process explore.exe (1136) và thấy đường dẫn nó hoàn toàn khác so với đường dẫn của process đáng nghi trước đó (2772).

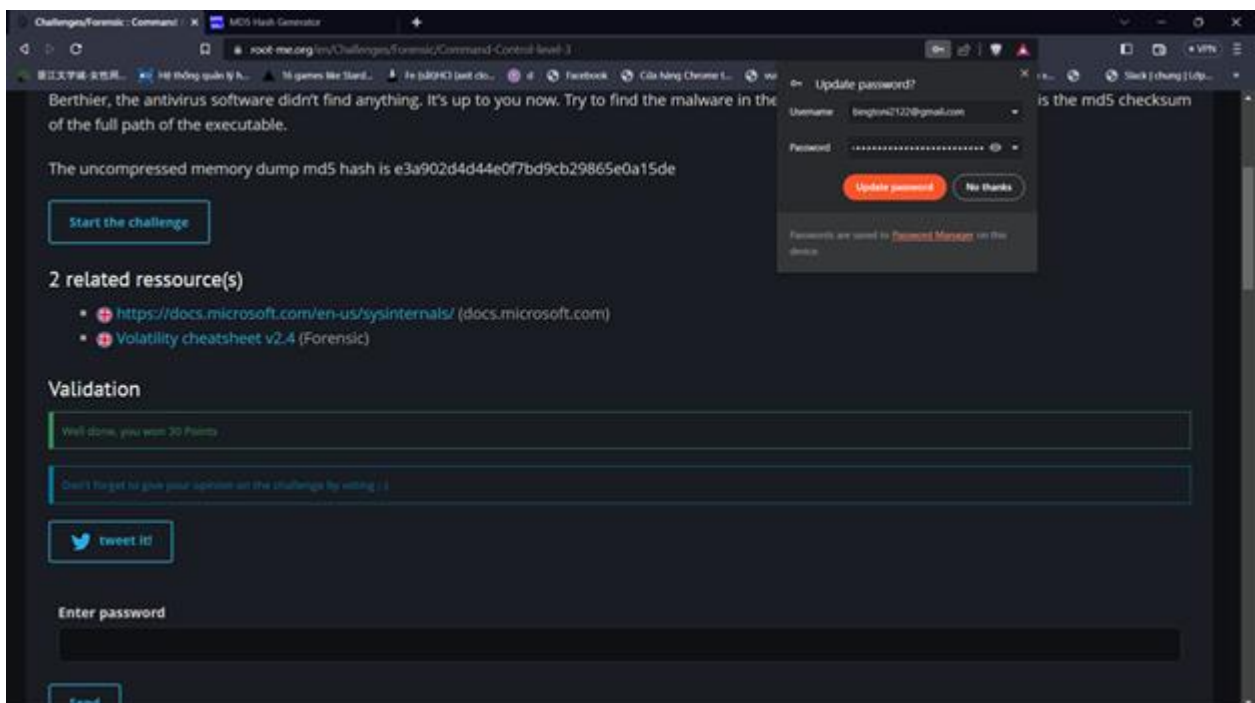


=> Vậy rất có thể đường dẫn này chính là flag mà đề bài yêu cầu. Vì vậy, chúng em dùng tool hash online để hash nó đúng định dạng flag.



Sau đó nộp bài thử với flag là: 49979149632639432397b3a1df8cb43d

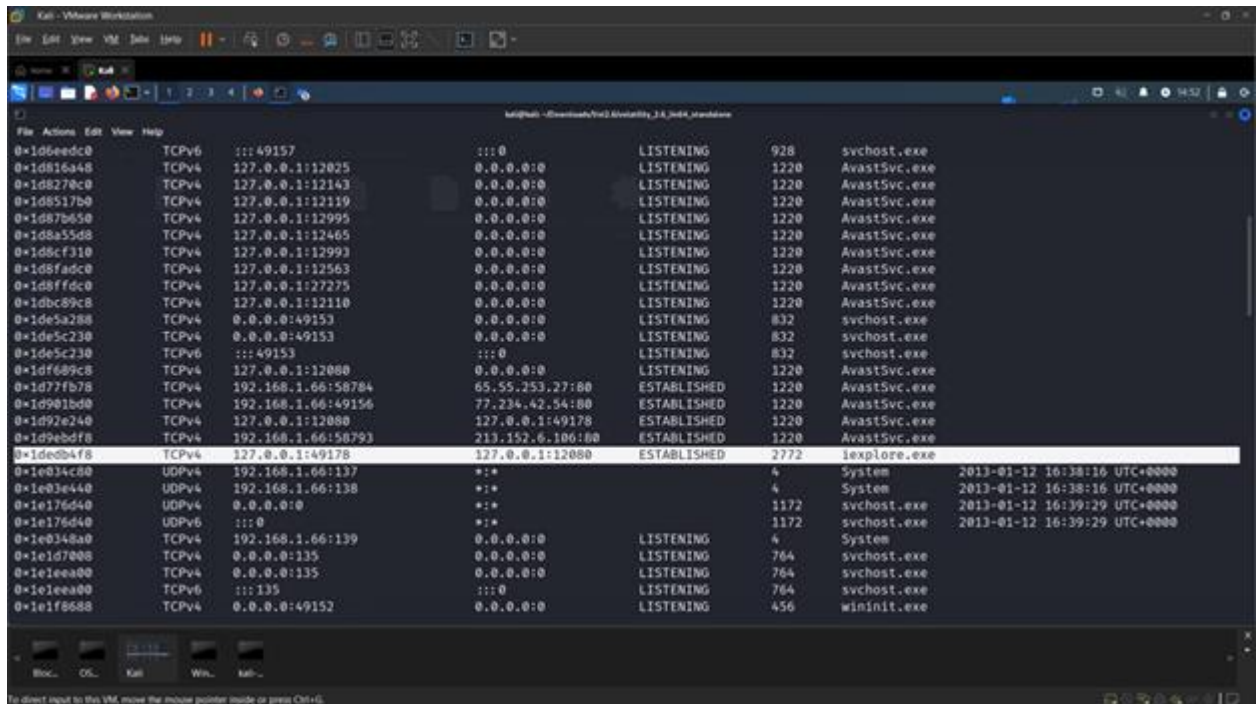
=> Hoàn thành challenge.



### Challenge 3: Command & Control 4

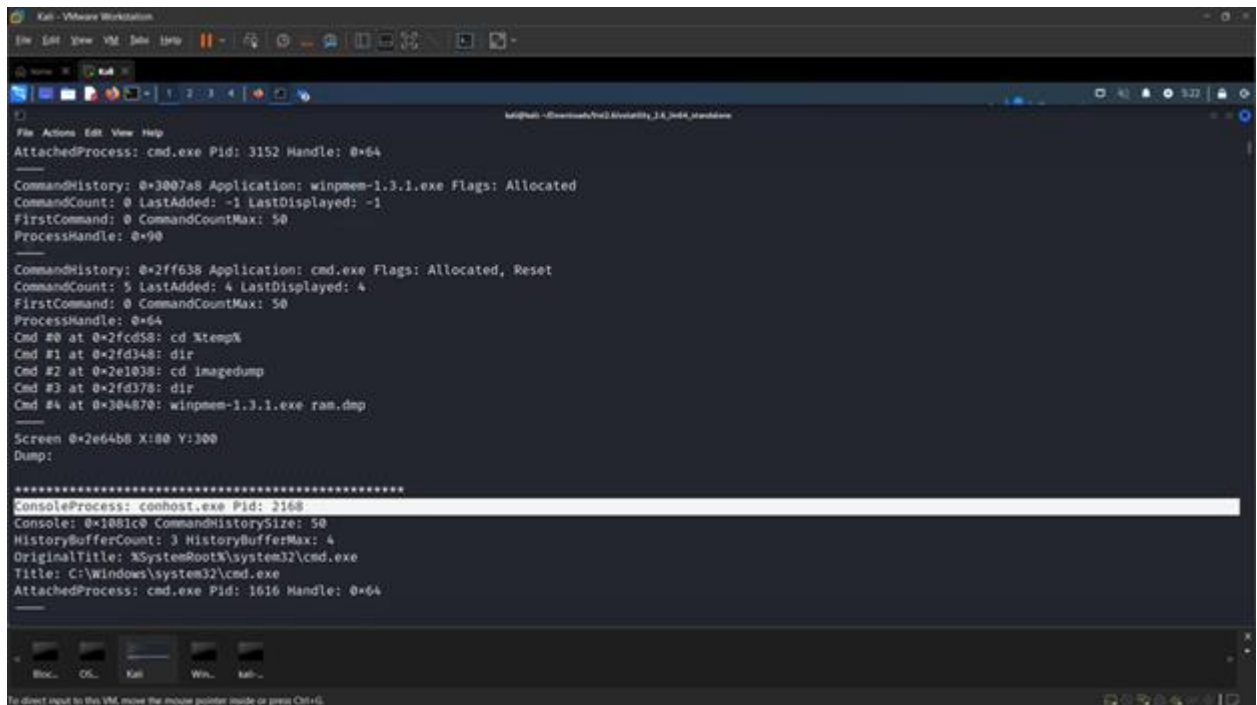


Trong challenge này yêu cầu tìm ip:port của máy target kế tiếp đang bị malware nhắm tới. Ban đầu em thấy yêu cầu ip:port nên nghĩ sẽ liên quan tới mạng, nhưng khi dùng plugin netscan và chú ý vào process malware vừa rồi thì không thấy được kết quả gì.



Vì vậy, em quyết định chuyển hướng làm, ban này chúng ta thấy file thực thi cmd.exe, vậy rất có thể là trong quá trình tấn công thì attacker này đã chạy ngầm một số lệnh gì đó, nên chúng em thử dùng plugin consoles để kiểm tra thử.

**\$ ./volatility\_2.6\_lin64\_standalone -f ~/Downloads/nhombay\_lab1/ch2.dmp --profile=Win7SP1x86\_23418 consoles**

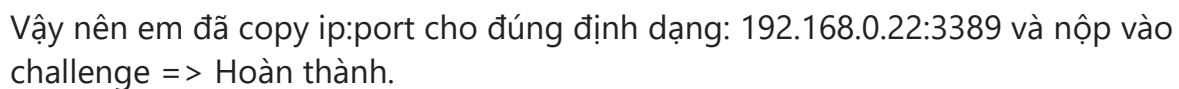


```
Kali - VMware Workstation
File Edit View VM Help
AttachedProcess: cmd.exe Pid: 3152 Handle: 0x64
-----
CommandHistory: 0x3007a8 Application: winpmem-1.3.1.exe Flags: Allocated
CommandCount: 0 LastAdded: -1 LastDisplayed: -1
FirstCommand: 0 CommandCountMax: 50
ProcessHandle: 0x90
-----
CommandHistory: 0x2ff638 Application: cmd.exe Flags: Allocated, Reset
CommandCount: 5 LastAdded: 4 LastDisplayed: 4
FirstCommand: 0 CommandCountMax: 50
ProcessHandle: 0x64
Cmd #0 at 0x2fcd58: cd %temp%
Cmd #1 at 0x2fd348: dir
Cmd #2 at 0x2e1038: cd imagedump
Cmd #3 at 0x2fd378: dir
Cmd #4 at 0x304870: winpmem-1.3.1.exe ram.dmp
-----
Screen 0x2e64b8 X:80 Y:300
Dump:
-----
*****
ConsoleProcess: conhost.exe Pid: 2168
Console: 0x1081c0 CommandHistorySize: 50
HistoryBufferCount: 3 HistoryBufferMax: 4
OriginalTitle: %SystemRoot%\system32\cmd.exe
Title: C:\Windows\system32\cmd.exe
AttachedProcess: cmd.exe Pid: 1616 Handle: 0x64
-----
-----
Bloc... OS... Kali Win... Kali...
```

Trong khi kiểm tra, chúng em thấy các lệnh trong cmd có vẻ không có gì đặc biệt, nhưng ngoài ra thì cũng tìm thấy console process với PID 2168 trông có vẻ khá đáng nghi, có lẽ bên trong gọi lệnh gì đó. Vậy nên tụi em quyết định dump riêng process này để kiểm tra.

Dump xong, tụi em dùng strings để đọc được nội dung bên trong. Ban đầu em nghĩ ip:port thì chắc sẽ liên quan đến các protocol nên đã tìm thử với keyword TCP thì không thấy gì, nhưng tcp thì có một đoạn tcpreplay.exe tới một ip:port như bên dưới. Đã vậy kể bên còn có chữ yoursecret => Em nghĩ đây là flag.

└─\$ strings 2168.dmp | grep tcp

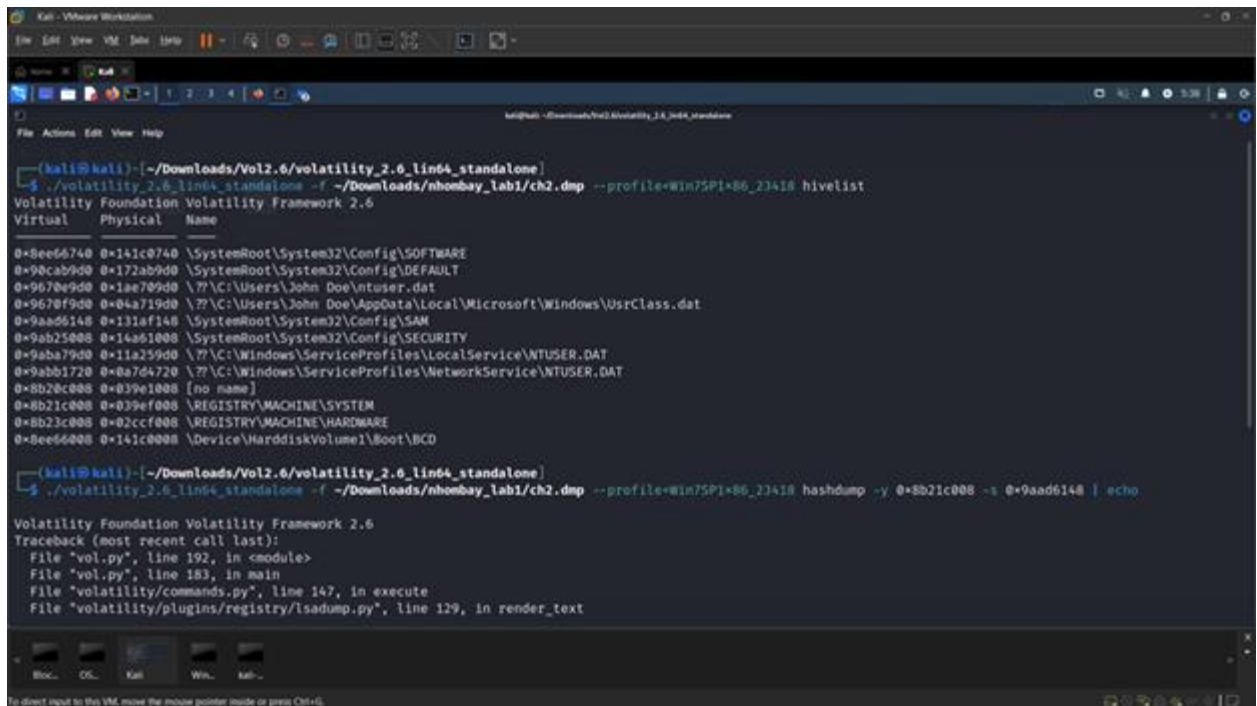




[http://systemmanager.ru/win2k\\_registry.en/46661.htm](http://systemmanager.ru/win2k_registry.en/46661.htm)

[http://systemmanager.ru/win2k\\_registry.en/46658.htm](http://systemmanager.ru/win2k_registry.en/46658.htm)

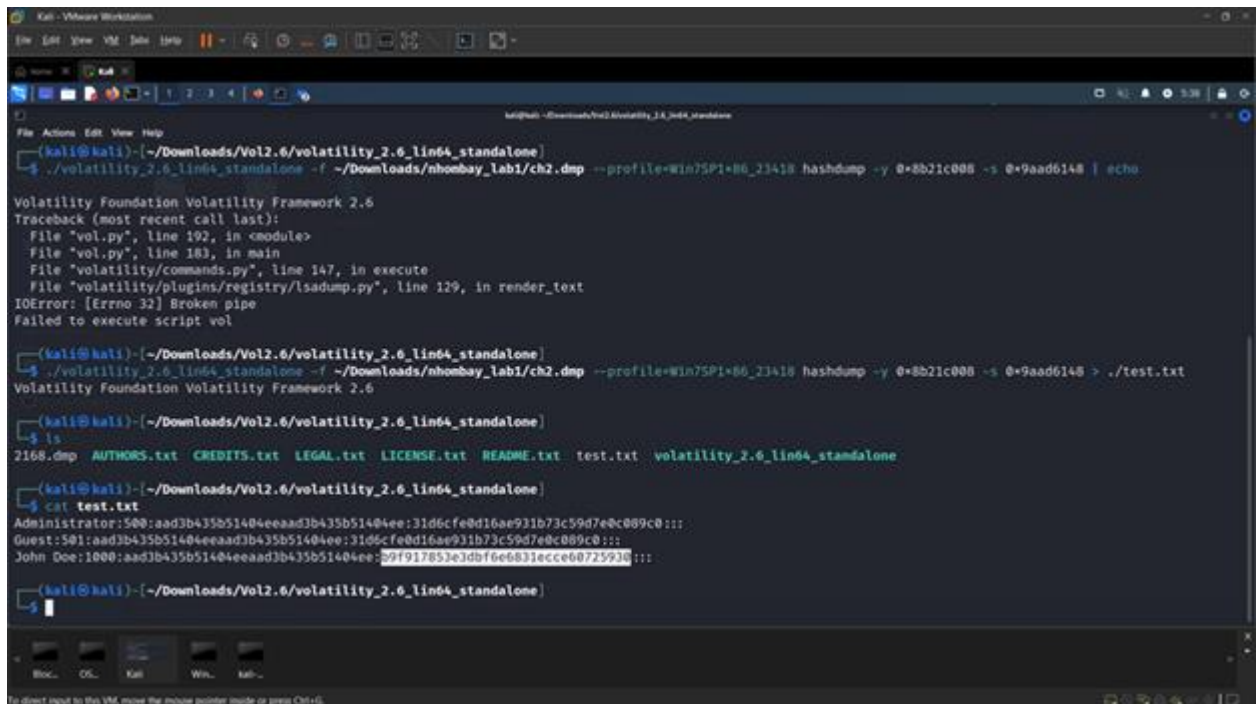
Đầu tiên, theo như hướng dẫn thì sẽ cần định vị địa chỉ ảo và đường dẫn đầy đủ trên ổ đĩa trước, chúng em sẽ dùng hivelist để thực hiện việc này.



```
(kali@kali) ~/Downloads/Vol2.6/volatility_2.6_lin64_standalone
$ ./volatility_2.6_lin64_standalone -f ~/Downloads/nhombay_lab1/ch2.dmp --profile=Win7SP1x86_23418 hivelist
Volatility Foundation Volatility Framework 2.6
Virtual    Physical  Name
-----
0x8ee66740 0x141c0740 \SystemRoot\System32\Config\SOFTWARE
0x90cab9d0 0x172ab9d0 \SystemRoot\System32\Config\DEFAULT
0x9670e9d0 0x1ae709d0 \??\C:\Users\John Doe\ntuser.dat
0x9670f9d0 0x04a719d0 \??\C:\Users\John Doe\AppData\Local\Microsoft\Windows\UsrClass.dat
0x9aad6148 0x131af148 \SystemRoot\System32\Config\SAM
0x9ab25008 0x14a61008 \SystemRoot\System32\Config\SECURITY
0x9aba79d0 0x11a259d0 \??\C:\Windows\ServiceProfiles\LocalService\NTUSER.DAT
0x9abb1720 0x8a7d4720 \??\C:\Windows\ServiceProfiles\NetworkService\NTUSER.DAT
0x8b20c008 0x039e1008 [no name]
0x8b21c008 0x039ef008 \REGISTRY\MACHINE\SYSTEM
0x8b23c008 0x02ccf008 \REGISTRY\MACHINE\HARDWARE
0x8ee66008 0x141c0008 \Device\HarddiskVolume1\Boot\BCD

(kali@kali) ~/Downloads/Vol2.6/volatility_2.6_lin64_standalone
$ ./volatility_2.6_lin64_standalone -f ~/Downloads/nhombay_lab1/ch2.dmp --profile=Win7SP1x86_23418 hashdump -y 0x8b21c008 -s 0x9aad6148 | echo
Volatility Foundation Volatility Framework 2.6
Traceback (most recent call last):
  File "vol.py", line 192, in <module>
  File "vol.py", line 183, in main
  File "volatility/commands.py", line 147, in execute
  File "volatility/plugins/registry/isadump.py", line 129, in render_text
```

Sau đó, có 2 đường dẫn và địa chỉ ảo cần chú ý là của SAM và SYSTEM trên hình. Theo như tài liệu thì đây là nơi lưu HKEY\_LOCAL\_MACHINE\SYSTEM key và HKEY\_LOCAL\_MACHINE\SAM key cần để trích xuất và giải mã thông tin xác thực miền đã lưu trong bộ nhớ cache được lưu trữ trong sổ đăng ký bằng hashdump.



```
(kali@kali)~[~/Downloads/Vol2.6/volatility_2.6_lin64_standalone]
$ ./volatility_2.6_lin64_standalone -f ~/Downloads/nhombay_lab1/ch2.dmp --profile=Win7SP1x86_23418 hashdump -y 0x8b21c008 -s 0x9aad6148 | echo
Volatility Foundation Volatility Framework 2.6
Traceback (most recent call last):
  File "vol.py", line 192, in <module>
  File "vol.py", line 183, in main
  File "volatility/commands.py", line 147, in execute
  File "volatility/plugins/registry/lsadump.py", line 129, in render_text
IOError: [Errno 32] Broken pipe
Failed to execute script vol

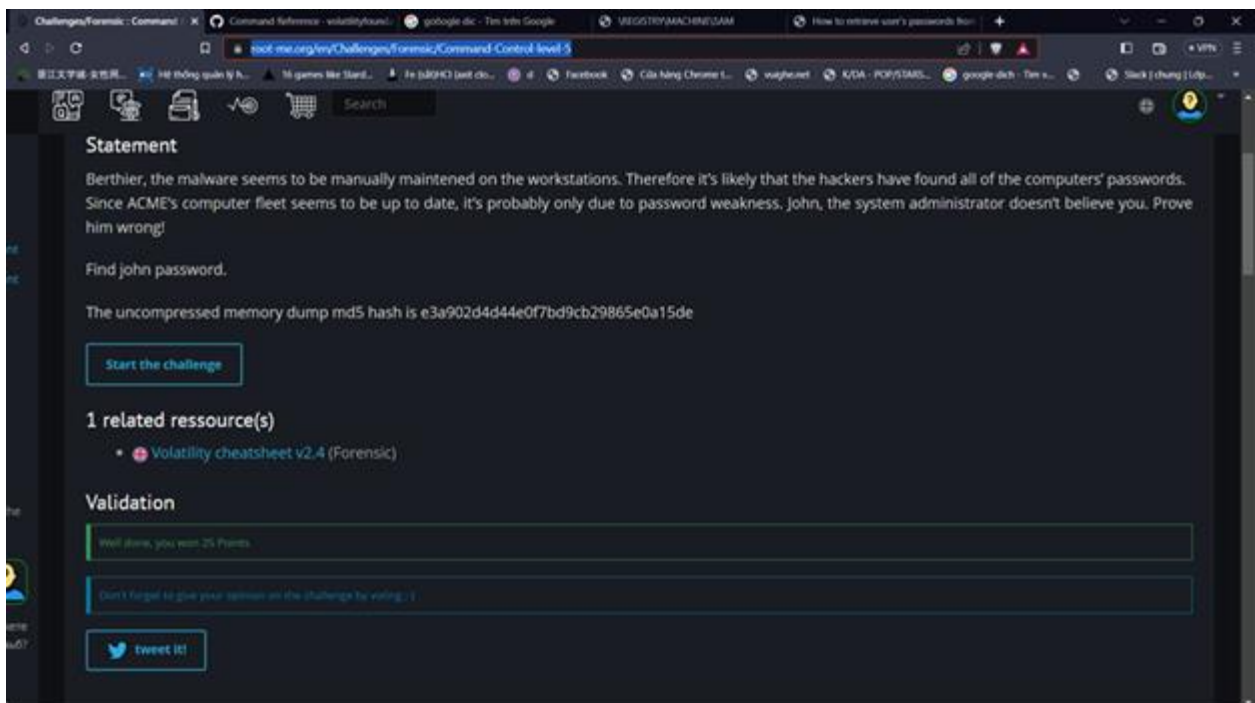
(kali@kali)~[~/Downloads/Vol2.6/volatility_2.6_lin64_standalone]
$ ./volatility_2.6_lin64_standalone -f ~/Downloads/nhombay_lab1/ch2.dmp --profile=Win7SP1x86_23418 hashdump -y 0x8b21c008 -s 0x9aad6148 > ./test.txt
Volatility Foundation Volatility Framework 2.6

(kali@kali)~[~/Downloads/Vol2.6/volatility_2.6_lin64_standalone]
$ ls
2168.dmp  AUTHORS.txt  CREDITS.txt  LEGAL.txt  LICENSE.txt  README.txt  test.txt  volatility_2.6_lin64_standalone

(kali@kali)~[~/Downloads/Vol2.6/volatility_2.6_lin64_standalone]
$ cat test.txt
Administrator:500:aad3b435b51404eeaad3b435b51404ee:31d6cfe0d16ae931b73c59d7e0c089c0:::
Guest:501:aad3b435b51404eeaad3b435b51404ee:31d6cfe0d16ae931b73c59d7e0c089c0:::
John Doe:1000:aad3b435b51404eeaad3b435b51404ee:39f917853e3dbf6e6831ecce60725930:::
```

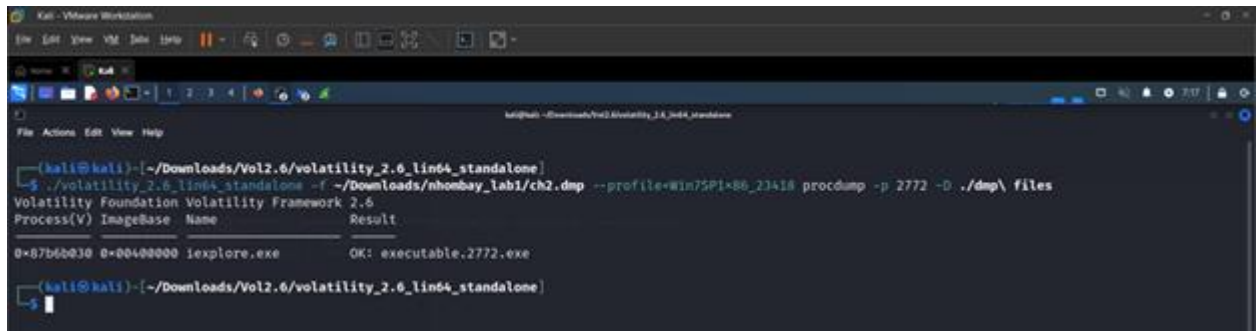
Sau đó, ta chạy hashdump với các địa chỉ ảo đã tìm được, thấy được file lưu password của các account trong hệ thống.

Cuối cùng, ta dùng tool crack hash để xem được password và nhập vào challenge flag: passw0rd.



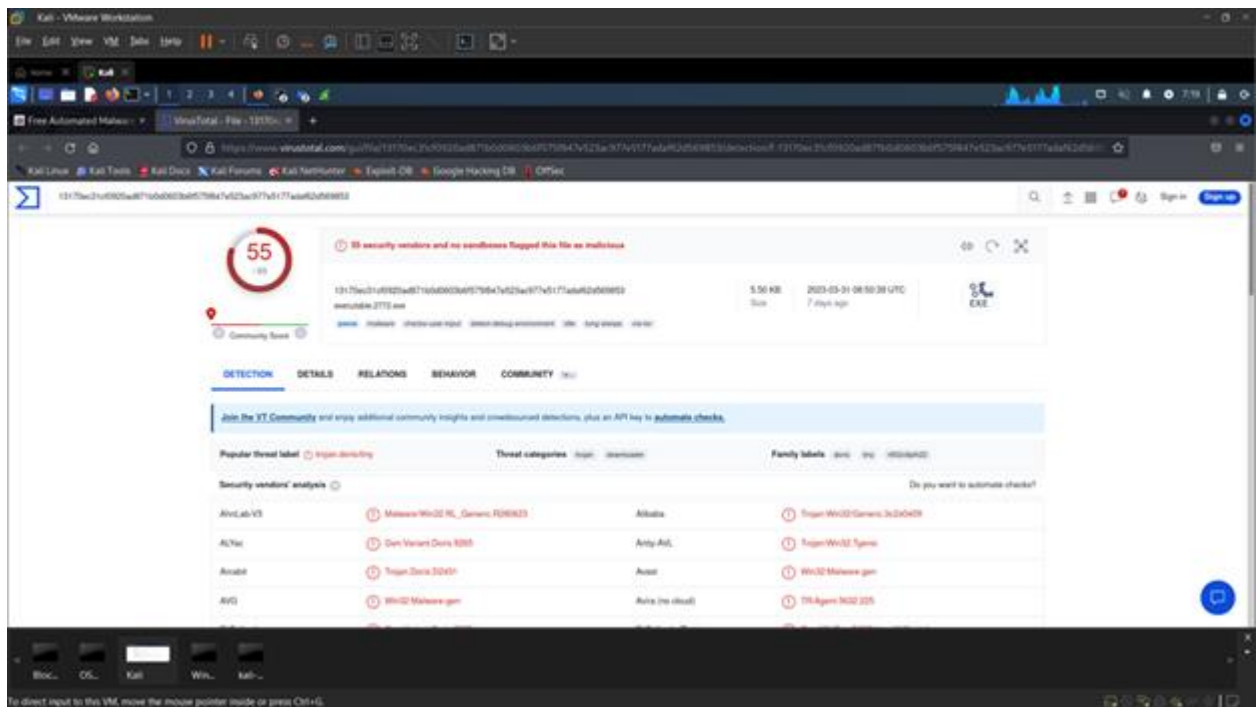
## Challenge 5: Command & Control 6

Trong challenge này, đề bài yêu cầu tìm được domain liên quan đến malware. Để làm được điều này, chúng em sẽ dump process 2772 ra trước và thử sử dụng tool malware analysis để phân tích.



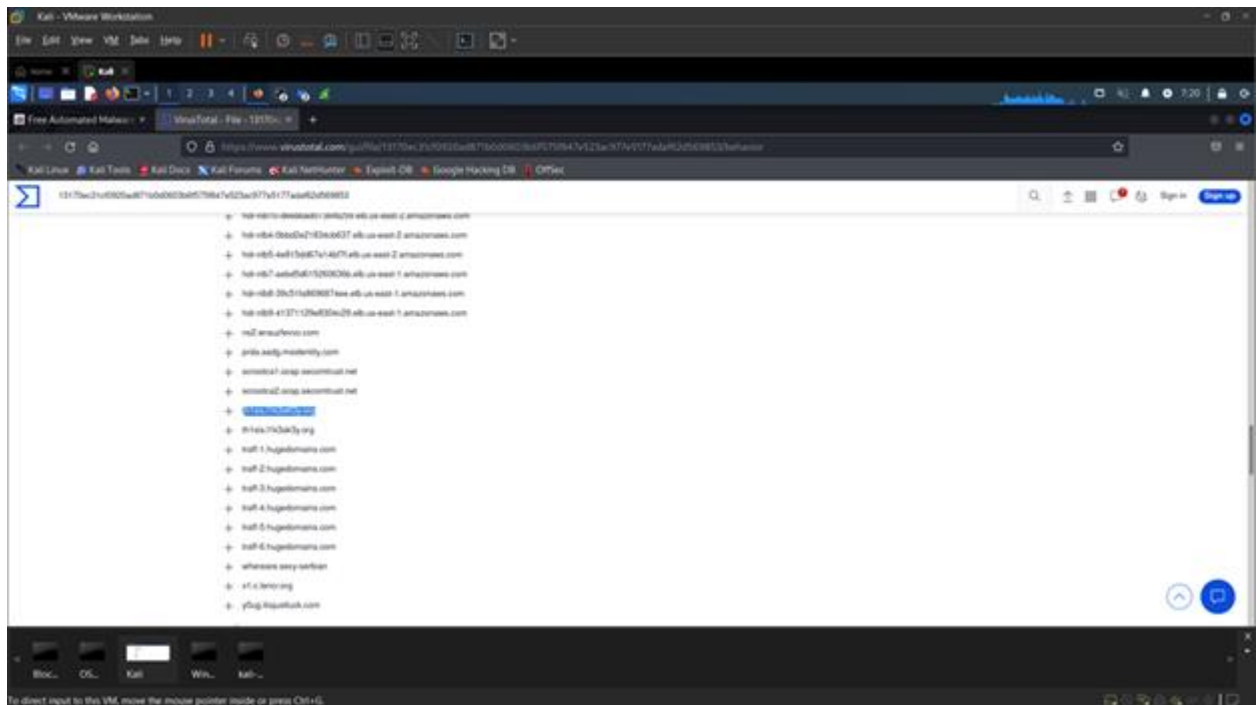
```
(kali@kali)-[~/Downloads/Vol2.6/volatility_2.6_lin64_standalone]
$ ./volatility 2.6 lin64_standalone -f ~/Downloads/nhombay_lab1/ch2.dmp --profile=Win7SP1x86_23418 procdump -p 2772 -D ./dmp\ files
Volatility Foundation Volatility Framework 2.6
Process(V) ImageBase Name Result
0x87b6b030 0x00400000 iexplore.exe OK: executable.2772.exe
(kali@kali)-[~/Downloads/Vol2.6/volatility_2.6_lin64_standalone]
$
```

Dump xong, tụi em dùng Hybrid Analysis và upload file đã dump ra để phân tích. Phần phân tích cho thấy file thực thi này đúng là mã độc.



Và khi kiểm tra thêm phần behavior ta có thể thấy được rất nhiều domain liên quan bị tấn công. Trong đó em thấy có 1 domain có vẻ đúng với format đề, vì vậy chúng em đoán đây là flag.

Paste flag vào trang rootme và hoàn thành bài challenge.



## Steganography

### EXIF - Metadata

Đầu tiên thực hiện tải file về

```
(kali@kali) ~/Downloads/stegno
$ wget http://challenge01.root-me.org/steganographie/ch1/ch1.png
--2023-05-31 12:47:08-- http://challenge01.root-me.org/steganographie/ch1/ch1.png
Resolving challenge01.root-me.org (challenge01.root-me.org) ... 212.129.38.224, 2001:bc8:35b0:c166::151
Connecting to challenge01.root-me.org (challenge01.root-me.org)|212.129.38.224|:80... connected.
HTTP request sent, awaiting response... 200 OK
Length: 13210 (13K) [image/png]
Saving to: 'ch1.png'

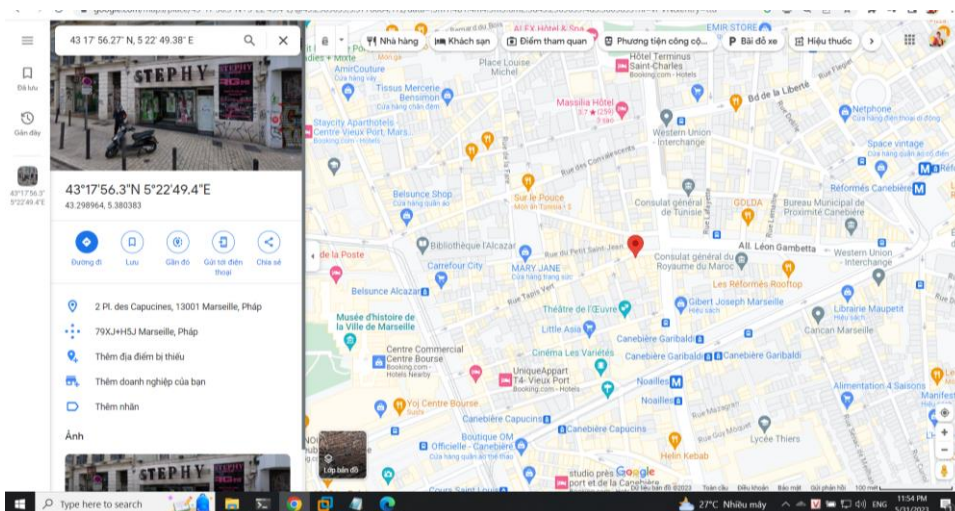
ch1.png
100%[=====>] 12.90K --KB/s in 0s

2023-05-31 12:47:11 (45.3 MB/s) - 'ch1.png' saved [13210/13210]
```

Tiếp tục sử dụng exiftool để check hình ảnh

```
kali-linux-2023.1-vmware-amd64 - VMware Workstation
File Edit View VM Tabs Help
Home kali@kali: ~/Downloads/stegno
File Actions Edit View Help
--(kali@kali)~/Downloads/stegno
exiftool ch1.png
ExifTool Version Number : 12.57
File Name : ch1.png
Directory :
File Size : 13 kb
File Modification Date/Time : 2023:05:31 12:47:11+00:00
File Access Date/Time : 2023:05:31 12:47:11+00:00
File Inode Change Date/Time : 2023:05:31 12:47:11+00:00
File Permissions : -rw-r--r--
File Type : PNG
File Type Extension : png
MIME Type : image/png
Image Width : 96
Image Height : 96
Bit Depth : 8
Color Type : RGB with Alpha
Compression : Deflate/Inflate
Filter : Adaptive
Interlace : Noninterlaced
Subsampling : 1:1:1
Pixels Per Unit X : 3780
Pixels Per Unit Y : 3780
Pixel Units : meters
Exif Byte Order : Big-endian (Motorola, MM)
Image Description : 0892_M_Schneire_Oilwell
Resolution Unit : inches
Y Co-Ord. Resampling : Centroidal
Exif Version : 0022
Components Configuration : Y, Cb, Cr, -
Flashpix Version : 1000
Owner Name :
GPS Latitude Ref : North
GPS Longitude Ref : East
Image Size : 96x96
Megapixels : 0.9216
GPS Latitude : 43 deg 17' 56.27" N
GPS Longitude : 5 deg 22' 49.38" E
GPS Position : 43 deg 17' 56.27" N, 5 deg 22' 49.38" E
--(kali@kali)~/Downloads/stegno
```

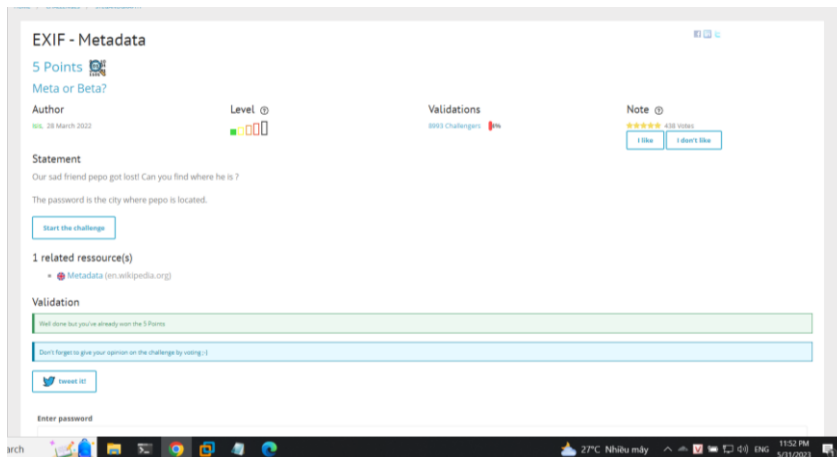
Tìm kiếm địa chỉ trên google map 43 17' 56.27" N, 5 22' 49.38" E



Ta có thông tin thành phố, cũng là flag: Marseille

Kiểm tra kết quả





Flag: Marseille

## Dot and next line

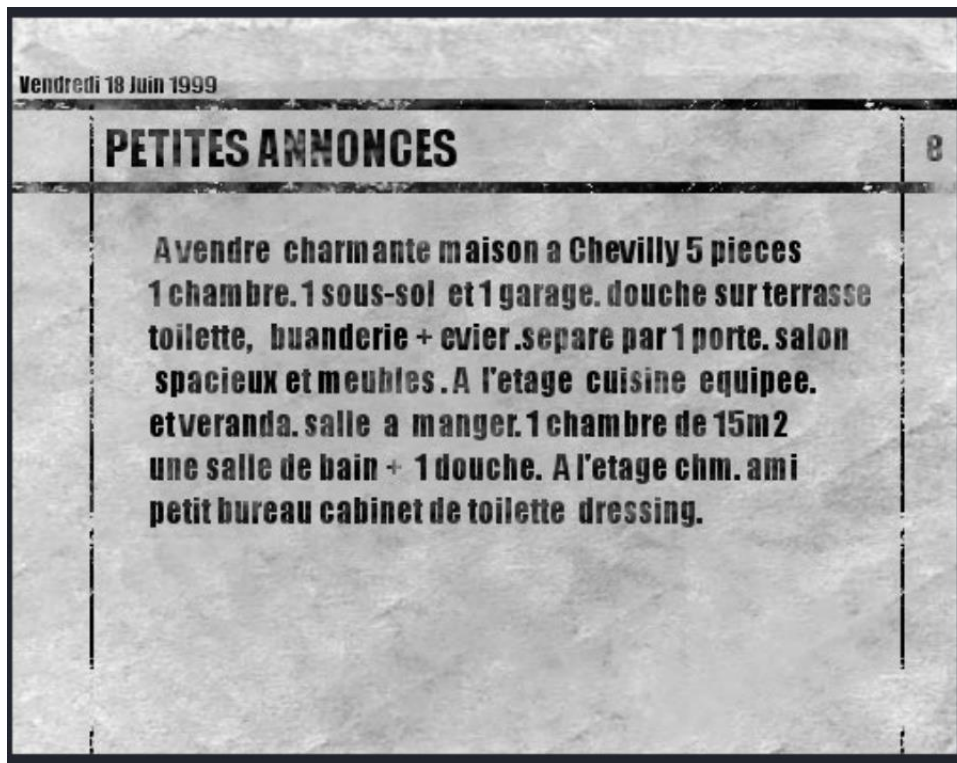
Đầu tiên ta thực hiện tải file

```
(kali@kali)~[~/Downloads/stegno]
$ wget http://challenge01.root-me.org/steganographie/ch5/ch5.zip
--2023-05-31 12:55:47-- http://challenge01.root-me.org/steganographie/ch5/ch5.zip
Resolving challenge01.root-me.org (challenge01.root-me.org)... 212.129.38.224, 2001:bc8:35b0:c166::1
Connecting to challenge01.root-me.org (challenge01.root-me.org)|212.129.38.224|:80 ... connected.
HTTP request sent, awaiting response... 200 OK
Length: 52241 (51K) [application/zip]
Saving to: 'ch5.zip'

ch5.zip                               100%[=====]
2023-05-31 12:55:50 (78.6 KB/s) - 'ch5.zip' saved [52241/52241]

(kali@kali)~[~/Downloads/stegno]
$
```

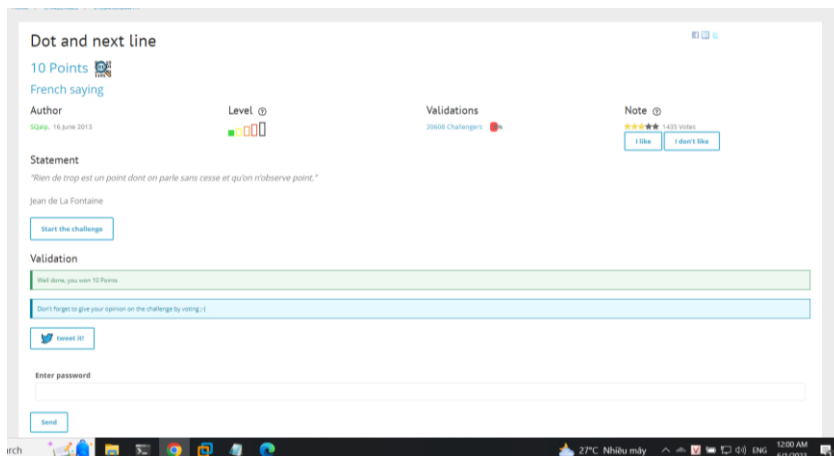
Tiếp tục thực hiện giải nén và ta có hình ảnh



Thực hiện giải mã bằng cách:

Ghép các ký tự bên dưới dấu chấm lại với nhau và ngược lại, ta có được flag là chatelet15h

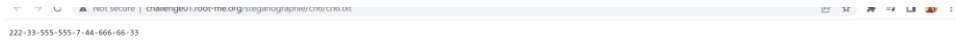
Kiểm tra kết quả



Flag: chatelet15h

## Steganomobile

Đầu tiên ta sẽ mở file để xem thông tin

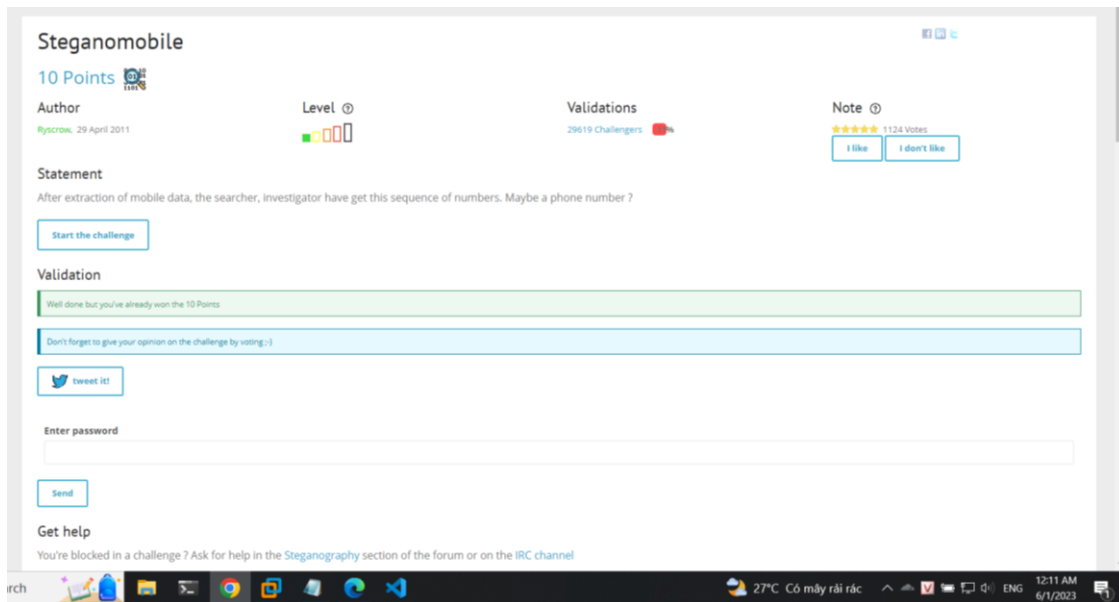


Với những con số này thì ta có bảng map tương ứng

```
1 table = {
2   2 : "a",
3   22 : "b",
4   222 : "c",
5   3 : "d",
6   33 : "e",
7   333 : "f",
8   4 : "g",
9   44 : "h",
10  444 : "i",
11  5 : "j",
12  55 : "k",
13  555 : "l",
14  6 : "m",
15  66 : "n",
16  666 : "o",
17  7 : "p",
18  77 : "q",
19  777 : "r",
20  7777 : "s",
21  8 : "t",
22  88 : "u",
23  888 : "v",
24  9 : "w",
25  99 : "x",
26  999 : "y",
27  9999 : "z",
28 }
29
30
```

Thực hiện giải mã số điện thoại theo map này thì ta có kết quả là cellphone

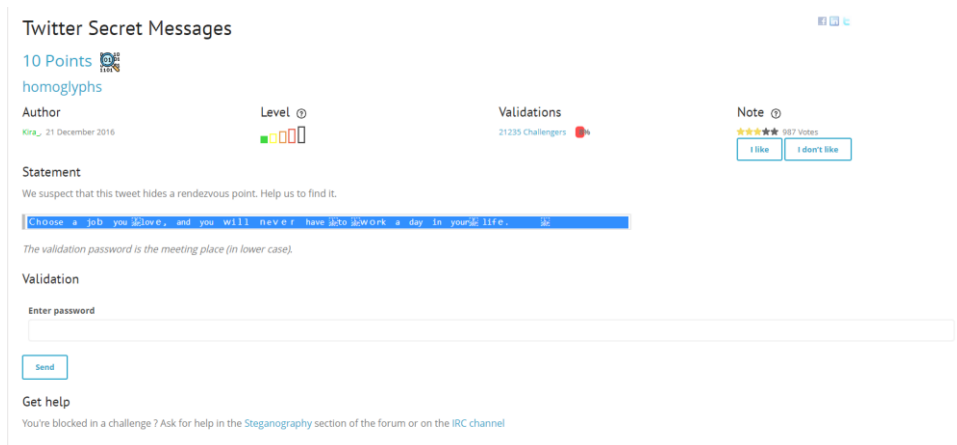
Thực hiện kiểm tra kết quả



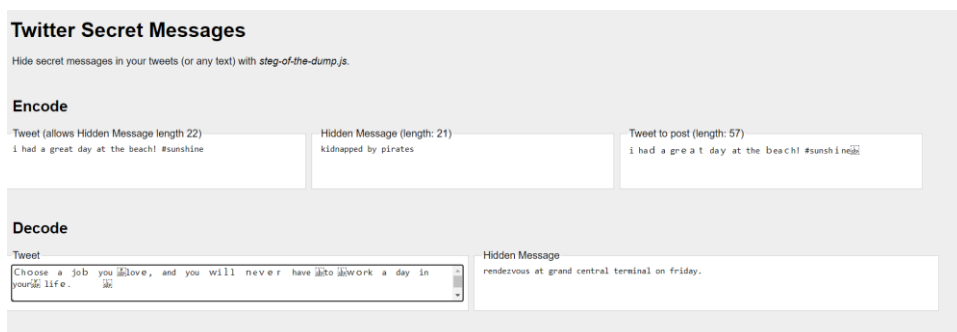
Flag: cellphone

## Twitter Secret Messages

Đầu tiên ta có một thông điệp



Thực hiện giải mã bằng công cụ <https://holloway.nz/steg>



Ta có thông điệp rendezvous at grand central terminal on friday.

Vậy flag là grand central terminal

Thực hiện kiểm tra kết quả

**Twitter Secret Messages**

10 Points

Author: Kira\_ 21 December 2016

Level:

Validations: 21235 Challengers

Note: 967 Votes

**Statement**

We suspect that this tweet hides a rendezvous point. Help us to find it.

Choose a job you love, and you will never have to work a day in your life.

The validation password is the meeting place (in lower case).

**Validation**

Well done, you won 10 Points

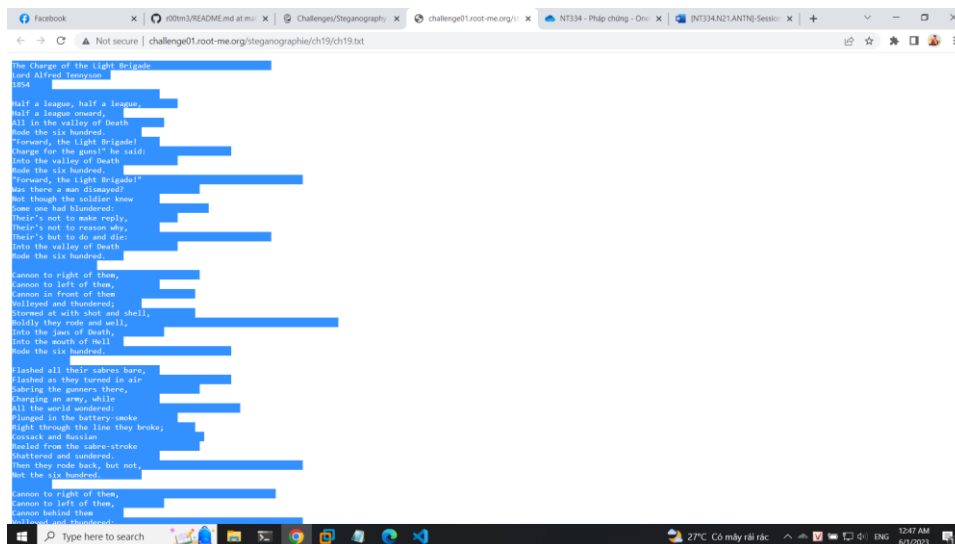
Don't forget to give your opinion on the challenge by voting :)

tweet it

**Enter password**

## Poem from Space

Đầu tiên ta có được đoạn thông điệp



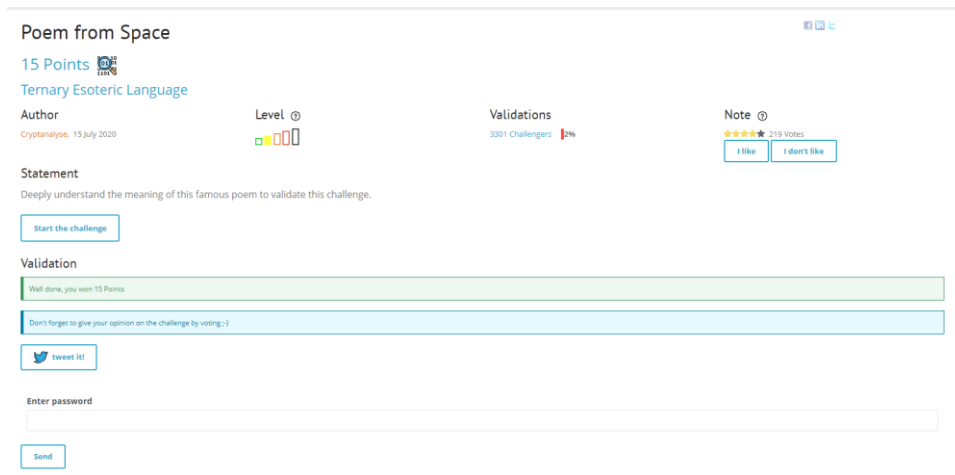
Ta thấy có một số khoảng trắng lạ ta sẽ thực hiện decode



Ta có flag là RootMe{Wh1t3\_Sp4c3}

Kiểm tra kết quả

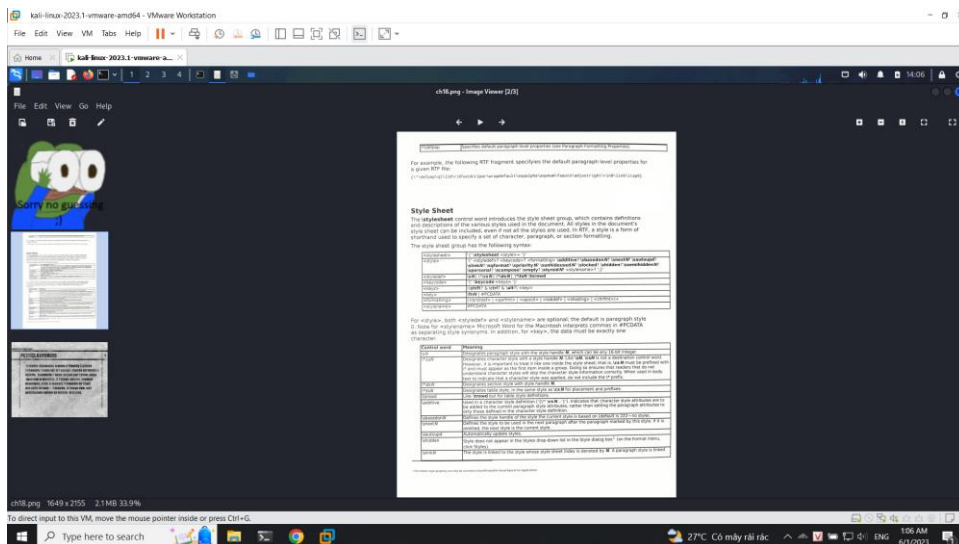




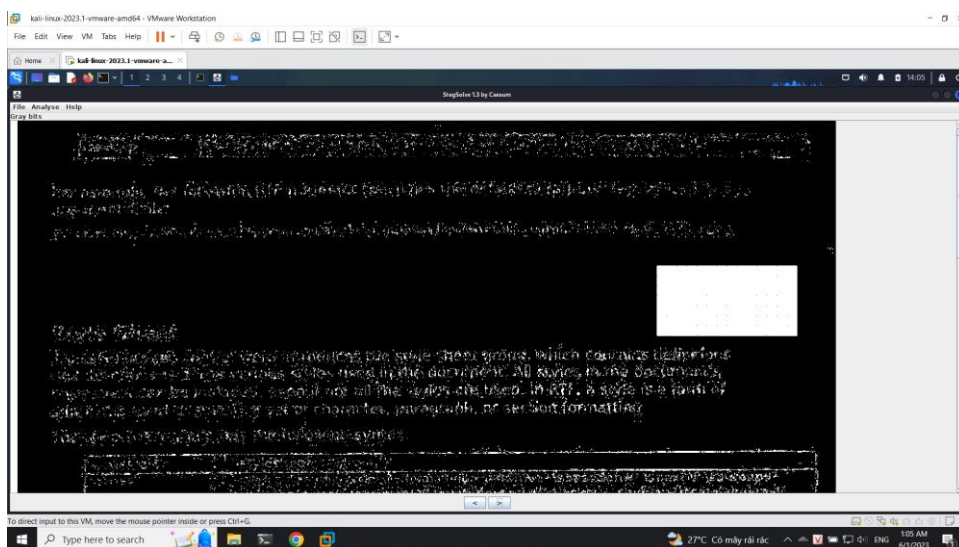
Flag: RootMe{Wh1t3\_Sp4c3}

## Yellow dots

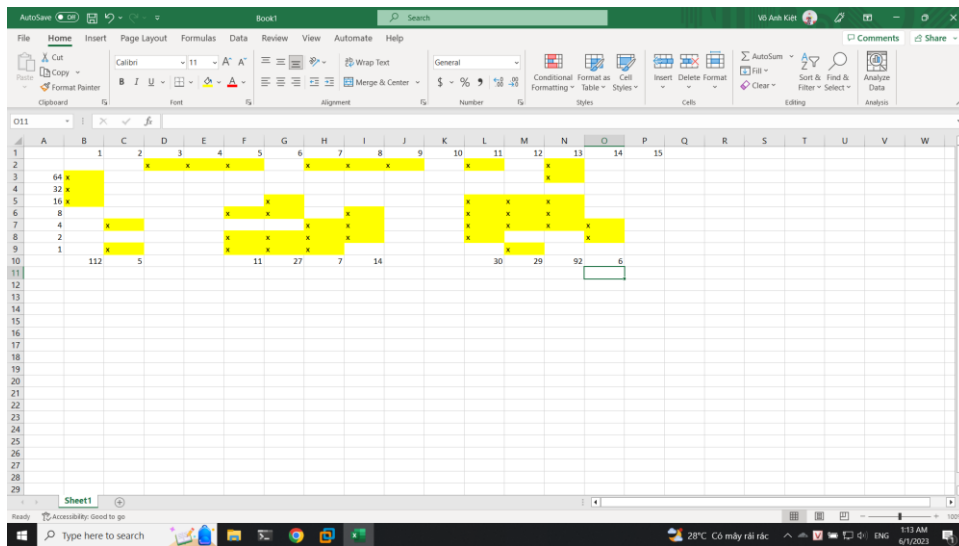
Đầu tiên ta tải file ảnh về



Tiếp tục sử dụng stegsolve để phân tích thì ta thấy chữ nổi cho người mù

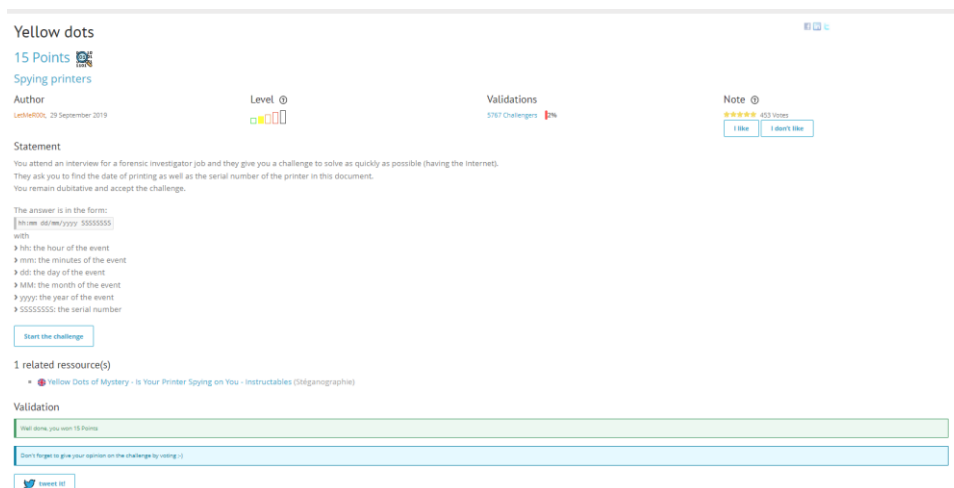


## Ta thực hiện giải mã



Ta có thông điệp là 11:05 27/07/2014 06922930

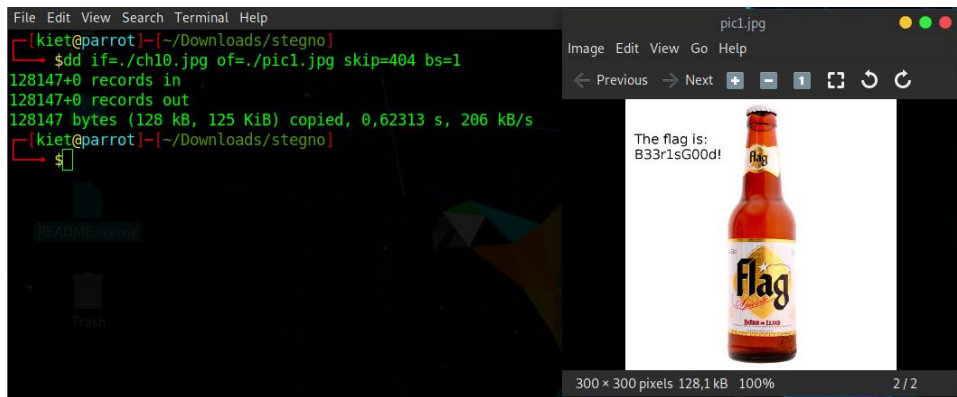
## Kiểm tra kết quả



## WAV - Noise analysis

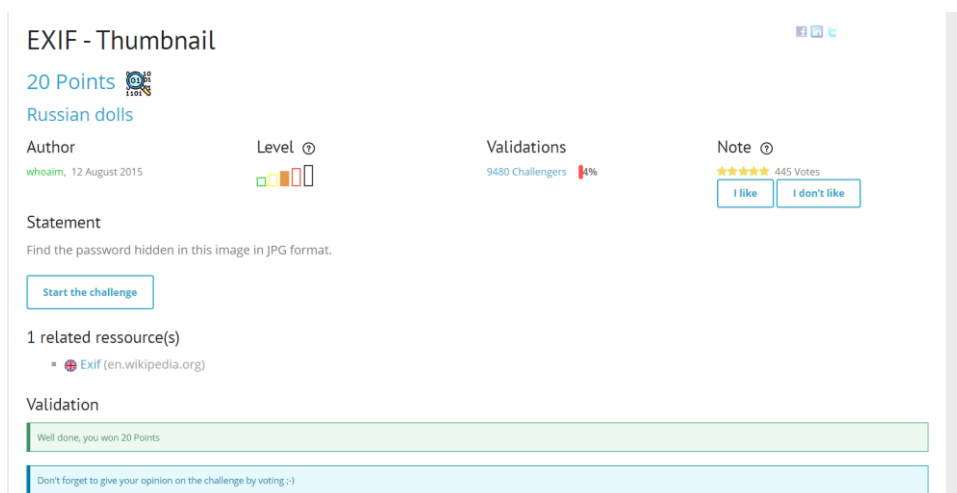
Đầu tiên ta tải file và mở bằng phần mềm audacity: Thực hiện cấu hình speed slow 30% và reverse đoạn âm thanh





Ta có flag là B33r1sG00d!

Kiểm tra kết quả



**TXT - George and Alfred**

Đầu tiên ta vào file để xem thông tin

Je suis très émue de vous dire que j'ai bien compris, l'autre jour, que vous avez toujours une envie folle de me faire danser. Je garde un souvenir de votre baiser et je voudrais que ce soit là une preuve que je puisse être aimée par vous. Je suis prête à vous montrer mon Affection toute désintéressée et sans calcul. Si vous voulez me voir ainsi dévoiler, sans aucun artifice mon âme toute nue, daignez donc me faire une visite Et nous causerons en amis et en chemin. Je vous prouverai que je suis la femme sincère capable de vous offrir l'affection la plus profonde et la plus étroite Amitié, en un mot, la meilleure amie que vous puissiez rêver. Puisque votre âme est libre, alors que l'abandon où je vis est bien long, bien dur et bien souvent pénible, ami très cher, j'ai le coeur gros, accourez vite et venez me le fait oublier. À l'amour, je veux me soumettre.

Alfred de Musset a répondu ceci :

Quand je vous jure, hélas, un éternel hommage  
Voulez-vous qu'un instant je change de langage  
Que ne puis-je, avec vous, goûter le vrai bonheur  
Je vous aime, ô ma belle, et ma plume en délire  
Couche sur le papier ce que je n'ose dire  
Avec soin, de mes vers, lisez le premier mot  
Vous saurez quel remède apporter à mes maux.

De la même manière George Sand a répondu ceci :

Cette grande faveur que votre ardeur réclame  
Nuit peut-être à l'honneur mais répond à ma flamme.

Utilisez la dernière "phrase cachée", pour valider cette épreuve.

## Câu thơ cuối có đóng mở ngoặc kép

Utilisez la dernière "phrase cachée", pour valider cette épreuve.

Ta thử dịch phần phrase cachée thì nó có nghĩa là Cette Nuit

Vậy flag là: Cette Nuit

Kiểm tra kết quả

TXT - George and Alfred

10 Points

Steganography in literature

Author

g0uZ, 20 December 2014

Level

Validations

21831 Challengers

Note

796 Votes

I like

I don't like

Statement

This challenge is only available in french language due to it specificity.

Start the challenge

Validation

Well done, you won 10 Points

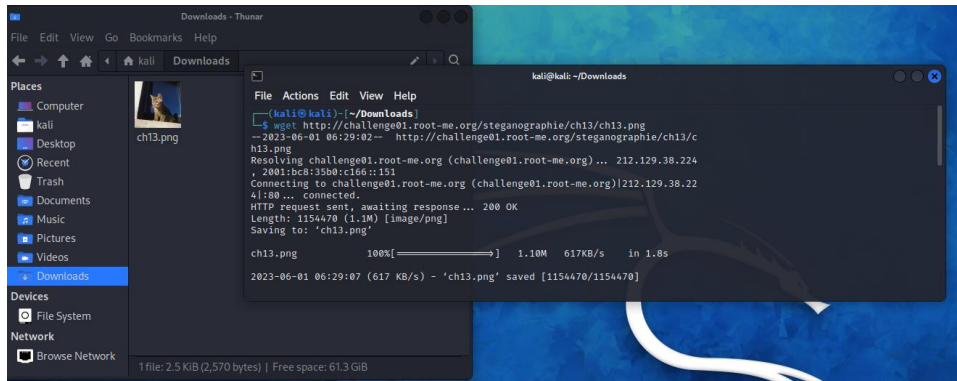
Don't forget to give your opinion on the challenge by voting :>)

tweet it!



## PNG - Pixel Indicator Technique

Đầu tiên tải ảnh về



Tiếp tục sử dụng tool stegopit để giải mã



Ta có flag là: PiTiSAls0aSteg4n0gr4ph1eM3thod

Kiểm tra kết quả

## PNG - Pixel Indicator Technique

30 Points

The Queen of the Savannah

Author

LetMeR00k, 7 August 2017

Level



Validations

1273 Challengers 1%

Note

★★★★★ 90 Votes

I like

I don't like

## Statement

Find the hidden message in this image.

SHA1 hash: 52062f33b7a58050c082a5f677a1ae626da32d88

Start the challenge

## 1 related resource(s)

- Pixel Indicator Technique for RGB Image Steganography - Adnan Abdul - Aziz Gutub (Stéganographie)

## Validation

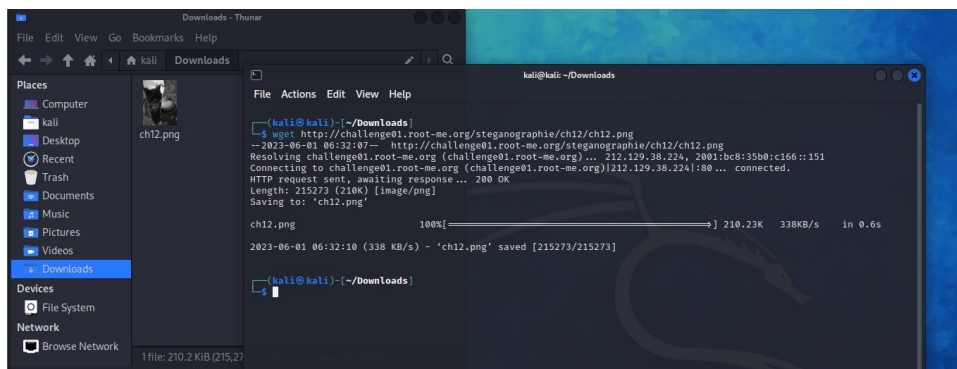
Well done, you won 30 Points

Don't forget to give your opinion on the challenge by voting :)

tweet it!

## PNG - Pixel Value Differencing

Đầu tiên thực hiện tải ảnh về



Sử dụng tool stegopvd để giải nén



Ta có flag là PvD:Pl4tiNuMvSDi4m0nd

Kiểm tra kết quả

## PNG - Pixel Value Differencing

30 Points

Wu and Tsai

Author

LetMeR00t, 7 November 2017

Level



Validations

1176 Challengers 1%

Note

★★★★★ 85 Votes

I like

I don't like

## Statement

Extract the hidden message from this image.

SHA1 : 06897894d602407321092489afeb84956ae2fd66

Start the challenge

## 2 related resource(s)

- A steganographic method based on pixel-value differencing and the perfect square number - Hsien-Wen Tseng and Hui-Shih Leng (Steganographie)
- Pixel-Value Differencing Steganography - El-Ailly - Al-Sadi (Steganographie)

## Validation

Well done, you won 30 Points

Don't forget to give your opinion on the challenge by voting :)

Tweet it!

---

*Sinh viên đọc kỹ yêu cầu trình bày bên dưới trang này*

## YÊU CẦU CHUNG

- Sinh viên tìm hiểu và thực hành theo hướng dẫn.
- Nộp báo cáo kết quả chi tiết những việc (**Report**) bạn đã thực hiện, quan sát thấy và kèm ảnh chụp màn hình kết quả (nếu có); giải thích cho quan sát (nếu có).
- Sinh viên báo cáo kết quả thực hiện và nộp bài.

### Báo cáo:

- File **.DOCX và .PDF**. Tập trung vào nội dung, không mô tả lý thuyết.
- Nội dung trình bày bằng **Font chữ Times New Romans/ hoặc font chữ của mẫu báo cáo này (UTM Neo Sans Intel/UTM Viet Sach)– cỡ chữ 13. Canh đều (Justify) cho văn bản. Canh giữa (Center) cho ảnh chụp.**
- Đặt tên theo định dạng: [Mã lớp]-SessionX\_GroupY. (trong đó X là Thứ tự buổi Thực hành, Y là số thứ tự Nhóm Thực hành đã đăng ký với GVHD-TH).

*Ví dụ: [NT101.H11.1]-Session1\_Group3.*

- Nếu báo cáo có nhiều file, nén tất cả file vào file .ZIP với cùng tên file báo cáo.
- **Không đặt tên đúng định dạng – yêu cầu, sẽ KHÔNG chấm điểm bài Lab.**
- Nộp file báo cáo trên theo thời gian đã thống nhất tại courses.uit.edu.vn.

**Đánh giá:** Sinh viên hiểu và tự thực hiện được bài thực hành. Khuyến khích:

- Chuẩn bị tốt và đóng góp tích cực tại lớp.
- Có nội dung mở rộng, ứng dụng trong kịch bản phức tạp hơn, có đóng góp xây dựng bài thực hành.

*Bài sao chép, trể, ... sẽ được xử lý tùy mức độ vi phạm.*

**HẾT**