

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 Thực Trâm | 20520815 | 20520815@gm.uit.edu.vn |
| 3 | Võ Anh Kiệt | 20520605 | 20520605@gm.uit.edu.vn |

2. NỘI DUNG THỰC HIỆN:¹

| STT | Công việc | Thực hiện | Thành viên thực hiện | Kết quả tự đánh giá |
|-----|-----------|--------------------------------|----------------------|---------------------|
| 1 | Root-me | 5 challenges Command & Control | Kiệt Trâm Ngân | 100% |
| 2 | Root-me | 11 challenges Steganography | Kiệt Trâm Ngân | 100% |
| 3 | Root-me | 4 challenges Forensics | Kiệt Trâm Ngân | 100% |
| 4 | Tổng kết | 20 Challenges root-me | Kiệt Trâm Ngân | 100% |

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

¹ Ghi nội dung công việc, các kịch bản trong bài Thực hành,

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

(Xem trang kế tiếp)

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]
$ ./volatility_2.6_lin64_standalone -f ~/Downloads/nhombay_lab1/ch2.dmp imageinfo
Volatility Foundation Volatility Framework 2.6
INFO : 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...
INFO : volatility.debug : 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
          KPCR for CPU 0 : 0x8292ac00L
          KUSER_SHARED_DATA : 0xfffff0000L
          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    0+003b07f0 Path        C:\Windows\System32
 308  smss.exe    0+003b07f0 SystemDrive C:
 308  smss.exe    0+003b07f0 SystemRoot  C:\Windows
 404  csrss.exe   0+001c07f0 ComSpec    C:\Windows\system32\cmd.exe

To direct input to this VM, move the mouse pointer inside or press Ctrl+I.
```

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 envar để tìm được như hình bên dưới:

```

File Actions Edit View Help
468 csrss.exe 0>004307f0 OS Windows_NT
468 csrss.exe 0>004307f0 Path C:\Windows\system32;C:\Windows;C:\Windows\System32\WBem;C:\Windows\System32\WindowsPo
werShell\v1.0;
468 csrss.exe 0>004307f0 PATHEXT .COM;.EXE;.BAT;.CMD;.VBS;.VBE;.JS;.JSE;.WSF;.WSH;.MSC
468 csrss.exe 0>004307f0 PROCESSOR_ARCHITECTURE x86
468 csrss.exe 0>004307f0 PROCESSOR_IDENTIFIER x86 Family 6 Model 23 Stepping 6, GenuineIntel
468 csrss.exe 0>004307f0 PROCESSOR_LEVEL 6
468 csrss.exe 0>004307f0 PROCESSOR_REVISION 1706
468 csrss.exe 0>004307f0 PSModulePath C:\Windows\system32\WindowsPowerShell\v1.0\Modules\
468 csrss.exe 0>004307f0 SystemDrive C:
468 csrss.exe 0>004307f0 SystemRoot C:\Windows
468 csrss.exe 0>004307f0 TEMP C:\Windows\TEMP
468 csrss.exe 0>004307f0 TMP C:\Windows\TEMP
468 csrss.exe 0>004307f0 USERNAME SYSTEM
468 csrss.exe 0>004307f0 windif C:\Windows
560 services.exe 0>001207f0 ALLUSERSPROFILE C:\ProgramData
560 services.exe 0>001207f0 CommonProgramFiles C:\Program Files\Common Files
560 services.exe 0>001207f0 COMPUTERNAME WIN-ETSA91RKCFF
560 services.exe 0>001207f0 ComSpec C:\Windows\system32\cmd.exe
560 services.exe 0>001207f0 FP_NO_HOST_CHECK NO
560 services.exe 0>001207f0 NUMBER_OF_PROCESSORS 1
560 services.exe 0>001207f0 OS Windows_NT
560 services.exe 0>001207f0 Path C:\Windows\system32;C:\Windows;C:\Windows\System32\WBem;C:\Windows\System32\WindowsPo
werShell\v1.0;
560 services.exe 0>001207f0 PATHEXT .COM;.EXE;.BAT;.CMD;.VBS;.VBE;.JS;.JSE;.WSF;.WSH;.MSC
560 services.exe 0>001207f0 PROCESSOR_ARCHITECTURE x86
560 services.exe 0>001207f0 PROCESSOR_IDENTIFIER x86 Family 6 Model 23 Stepping 6, GenuineIntel
560 services.exe 0>001207f0 PROCESSOR_LEVEL 6

```

Sau đó, ta sẽ nhập flag: WIN-ETSA91RKCFF vào challenge và hoàn thành.

The validation flag is the workstation's hostname.

The uncompressed memory dump md5 hash is e3a902d4d44e0f7bd9cb29865e0a15de

[Start the challenge](#)

1 related ressource(s)

- Volatility cheatsheet v2.4 (Forensic)

Validation

Send answer, you won 15 Points

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

[tweet it!](#)

Enter password

[Send](#)

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 | Actions | Edit | View | Help |
|-----------------------------------|---------|------|------|-----------------------------------|
| ... 0*88cedd40:sppsvc.exe | 1872 | 568 | 4 | 143 2013-01-12 16:39:02 UTC+0000 |
| ... 0*8a182748:svchost.exe | 1748 | 568 | 18 | 318 2013-01-12 16:38:58 UTC+0000 |
| ... 0*8a0f9c40:spoolsv.exe | 1712 | 568 | 14 | 338 2013-01-12 16:38:58 UTC+0000 |
| ... 0*9541c7e0:wlmss.exe | 336 | 568 | 4 | 45 2013-01-12 16:39:21 UTC+0000 |
| ... 0*8a1f5030:VM8upgradeHelp.exe | 648 | 568 | 4 | 89 2013-01-12 16:39:21 UTC+0000 |
| ... 0*892ced40:winlogon.exe | 500 | 448 | 3 | 111 2013-01-12 16:38:14 UTC+0000 |
| ... 0*88093a00:crssr.exe | 468 | 448 | 10 | 471 2013-01-12 16:38:14 UTC+0000 |
| ... 0*87c59500:conhost.exe | 3228 | 468 | 2 | 54 2013-01-12 16:44:58 UTC+0000 |
| ... 0*87a9c268:conhost.exe | 2600 | 468 | 1 | 35 2013-01-12 16:40:28 UTC+0000 |
| ... 0*954826b8:conhost.exe | 2168 | 468 | 2 | 49 2013-01-12 16:55:58 UTC+0000 |
| ... 0*87bd35b8:wpnetwk.exe | 3176 | 568 | 9 | 240 2013-01-12 16:40:48 UTC+0000 |
| ... 0*87ac0620:taskhost.exe | 2352 | 568 | 8 | 149 2013-01-12 16:40:24 UTC+0000 |
| ... 0*8975c20:svchost.exe | 764 | 568 | 7 | 263 2013-01-12 16:38:23 UTC+0000 |
| ... 0*8962f7e8:lsm.exe | 584 | 456 | 10 | 162 2013-01-12 16:38:16 UTC+0000 |
| ... 0*896427b8:lsass.exe | 576 | 456 | 6 | 566 2013-01-12 16:38:16 UTC+0000 |
| ... 0*8929fd40:csrss.exe | 404 | 396 | 9 | 469 2013-01-12 16:38:14 UTC+0000 |
| ... 0*87978078:System | 4 | 0 | 103 | 3257 2013-01-12 16:38:09 UTC+0000 |
| ... 0*8c3ed40:smss.exe | 308 | 4 | 2 | 29 2013-01-12 16:38:09 UTC+0000 |
| ... 0*87ac6030:explorer.exe | 2548 | 2484 | 24 | 766 2013-01-12 16:40:27 UTC+0000 |
| ... 0*87b6b030:explorer.exe | 2772 | 2548 | 2 | 74 2013-01-12 16:40:34 UTC+0000 |
| ... 0*8989030:cmd.exe | 1616 | 2772 | 2 | 101 2013-01-12 16:55:49 UTC+0000 |
| ... 0*85499c10:taskmgr.exe | 1232 | 2548 | 6 | 116 2013-01-12 16:42:29 UTC+0000 |
| ... 0*87bf7030:cmd.exe | 3152 | 2548 | 1 | 23 2013-01-12 16:44:58 UTC+0000 |
| ... 0*87cbfd40:winpmem-1.3.1. | 3144 | 3152 | 1 | 23 2013-01-12 16:59:17 UTC+0000 |
| ... 0*98fb08c0:stikyNot.exe | 2744 | 2548 | 8 | 135 2013-01-12 16:40:32 UTC+0000 |
| ... 0*87b784b0:AvastUI.exe | 2720 | 2548 | 14 | 220 2013-01-12 16:40:31 UTC+0000 |
| ... 0*87b82430:MinerTray.exe | 2660 | 2548 | 5 | 88 2013-01-12 16:40:29 UTC+0000 |
| ... 0*87c6a2a0:scrwriter.exe | 3452 | 2548 | 1 | 19 2013-01-12 16:41:01 UTC+0000 |

=> 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).

```
(kali㉿kali)-[~/Downloads/Vol2.6/volatility_2.6_lin64_standalone]
└─$ ./volatility_2.6_lin64_standalone -f ~/Downloads/nhombay_lab1/ch2.dmp --profile=Win7SP1x86_23416 cmdline -p 1136
Volatility Foundation Volatility Framework 2.6
*****
explore.exe pid: 1136
Command line : "C:\Program Files\Internet Explorer\iexplore.exe"

(kali㉿kali)-[~/Downloads/Vol2.6/volatility_2.6_lin64_standalone]
└─$ ./volatility_2.6_lin64_standalone -f ~/Downloads/nhombay_lab1/ch2.dmp --profile=Win7SP1x86_23416 cmdline -p 2772
Volatility Foundation Volatility Framework 2.6
*****
explore.exe pid: 2772
Command line : "%USER%\AppData\Roaming\Microsoft\Internet Explorer\Quick Launch\iexplore.exe"
└─$
```

=> 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.

The screenshot shows a web-based MD5 Hash Generator tool. In the input field, the string 'C:\Users\John Doe\AppData\Roaming\Microsoft\Internet Explorer\Quick Launch\explore.exe' is entered. Below the input field, there is a 'Generate' button. Under the generated hash, there are 'Copy' buttons for both the MD5 and SHA1 hashes.

Sau đó nộp bài thử với flag là: 49979149632639432397b3a1df8cb43d

=> Hoàn thành challenge.

The screenshot shows a challenge interface from root-me.org. It displays the flag '49979149632639432397b3a1df8cb43d' as the md5 checksum. A success message 'Well done, you won 20 Points' is shown. There is also a 'Start the challenge' button and a 'Validation' section with a note about using the password manager.

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.

| File | Actions | Edit | View | Help | Local Address | Foreign Address | State | Process |
|-------------|---------|--------------------|------------------|-------------|---------------|------------------------------|-------|---------|
| 0*1d6eedc0 | TCPv6 | 1:::49157 | :::0 | LISTENING | 928 | svchost.exe | | |
| 0*1d816a48 | TCPv4 | 127.0.0.1::12025 | 0.0.0.0::0 | LISTENING | 1220 | AvastSvc.exe | | |
| 0*1d8278c0 | TCPv4 | 127.0.0.1::12143 | 0.0.0.0::0 | LISTENING | 1220 | AvastSvc.exe | | |
| 0*1d8517b0 | TCPv4 | 127.0.0.1::12119 | 0.0.0.0::0 | LISTENING | 1220 | AvastSvc.exe | | |
| 0*1d870650 | TCPv4 | 127.0.0.1::12995 | 0.0.0.0::0 | LISTENING | 1220 | AvastSvc.exe | | |
| 0*1d8a55d8 | TCPv4 | 127.0.0.1::12465 | 0.0.0.0::0 | LISTENING | 1220 | AvastSvc.exe | | |
| 0*1d8cf310 | TCPv4 | 127.0.0.1::12993 | 0.0.0.0::0 | LISTENING | 1220 | AvastSvc.exe | | |
| 0*1d8fadcc0 | TCPv4 | 127.0.0.1::12563 | 0.0.0.0::0 | LISTENING | 1220 | AvastSvc.exe | | |
| 0*1d8ffdc0 | TCPv4 | 127.0.0.1::127275 | 0.0.0.0::0 | LISTENING | 1220 | AvastSvc.exe | | |
| 0*1dbc9c8 | TCPv4 | 127.0.0.1::12110 | 0.0.0.0::0 | LISTENING | 1220 | AvastSvc.exe | | |
| 0*1de5a288 | TCPv4 | 0.0.0.0::49153 | 0.0.0.0::0 | LISTENING | 832 | svchost.exe | | |
| 0*1de5c230 | TCPv4 | 0.0.0.0::49153 | 0.0.0.0::0 | LISTENING | 832 | svchost.exe | | |
| 0*1df689c8 | TCPv4 | 127.0.0.1::12080 | 0.0.0.0::0 | LISTENING | 1220 | AvastSvc.exe | | |
| 0*1d77fb78 | TCPv4 | 192.168.1.66:58784 | 65.55.253.27:80 | ESTABLISHED | 1220 | AvastSvc.exe | | |
| 0*1d901bd0 | TCPv4 | 192.168.1.66:49156 | 77.234.42.54:80 | ESTABLISHED | 1220 | AvastSvc.exe | | |
| 0*1d92e240 | TCPv4 | 127.0.0.1::12080 | 127.0.0.1:49178 | ESTABLISHED | 1220 | AvastSvc.exe | | |
| 0*1d9ebdf8 | TCPv4 | 192.168.1.66:58793 | 213.152.6.106:80 | ESTABLISHED | 1220 | AvastSvc.exe | | |
| 0*1de00478 | TCPv4 | 127.0.0.1::49178 | 127.0.0.1:12080 | ESTABLISHED | 2772 | lexplore.exe | | |
| 0*1e034c80 | UDPV4 | 192.168.1.66:1137 | *:* | 4 | System | 2013-01-12 16:38:16 UTC+0000 | | |
| 0*1e03e440 | UDPV4 | 192.168.1.66:1138 | *:* | 4 | System | 2013-01-12 16:38:16 UTC+0000 | | |
| 0*1e176d40 | UDPV4 | 0.0.0.0::0 | *:* | 1172 | svchost.exe | 2013-01-12 16:39:29 UTC+0000 | | |
| 0*1e176d40 | UDPV6 | :::0 | *:* | 1172 | svchost.exe | 2013-01-12 16:39:29 UTC+0000 | | |
| 0*1e0348a0 | TCPv4 | 192.168.1.66:1139 | 0.0.0.0::0 | LISTENING | 4 | System | | |
| 0*1e1d7088 | TCPv4 | 0.0.0.0::135 | 0.0.0.0::0 | LISTENING | 764 | svchost.exe | | |
| 0*1e1eeaa00 | TCPv4 | 0.0.0.0::135 | 0.0.0.0::0 | LISTENING | 764 | svchost.exe | | |
| 0*1e1eeaa00 | TCPv6 | ::135 | ::0 | LISTENING | 764 | svchost.exe | | |
| 0*1ef6868 | TCPv4 | 0.0.0.0::49152 | 0.0.0.0::0 | LISTENING | 456 | wminit.exe | | |

Vì vậy, em quyết định chuyển hướng làm, ban nãy 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 ||| 
File Actions Edit View 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 0x2fc58: cd %temp%
Cmd #1 at 0x2fd48: dir
Cmd #2 at 0x2e108: cd imagedump
Cmd #3 at 0x2fd38: 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: 0x1881c0 CommandHistorySize: 50
HistoryBufferCount: 3 HistoryBufferMax: 4
OriginalTitle: %SystemRoot%\system32\cmd.exe
Title: C:\Windows\system32\cmd.exe
AttachedProcess: cmd.exe Pid: 1616 Handle: 0x64
```

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 kế bên còn có chữ yoursecret => Em nghĩ đây là flag.

```
└─$ strings 2168.dmp | grep tcp
```

Vậy nên em đã copy ip:port cho đúng định dạng: 192.168.0.22:3389 và nộp vào challenge => Hoàn thành.

[Challenge/Forensic - Command](#) × [Command Reference - volatility4ounds](#) × [google dc - Tim Irm Google](#) +

root-me.org/Challenges/Forensic/Command-Control-level-4/flag-validation_challenge

Đại học Bách Khoa Hà Nội → Hỗ trợ kỹ thuật → Games Me Stand... → root-ME (root-me) → Facebook → Cửa Hàng Chơi Game → ...

Update password?

Username: [benjamins212@gmail.com](#)

Password:

Author: [ThienDuc](#), 16 February 2013

Level: Validated

77% Chu

Update password No thanks 252 Votes I don't like

Newest members: [Lamque](#), [patched1337](#), [ThienDuc](#), [Goldfire](#), [gamer](#), [Roung](#), [benjamins212](#)

Statement:

Berthier, thanks to this new information about the processes running on the workstation of the internal server targeted by the hackers!

The validation flag should have this format : IP:PORT

The uncompressed memory dump md5 hash is e3a902d4d44e0f7bd9cb29865e0a15de

Start the challenge

1 related resource(s)

- Volatility cheatsheets v2.4 (Forensic)

Validation

You done, you earn 25 Points

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

FAQ

20 March 2023 at 23:05

Power in knowledge, no奴隸主制

Check results?

[Twitter](#) Tweet it!

Challenge 4: Command & Control 5

Tài liệu tham khảo.

<https://andreafortuna.org/2017/11/15/how-to-retrieve-users-passwords-from-a-windows-memory-dump-using-volatility/>

http://systemmanager.ru/win2k_regestry.en/46661.htm

http://systemmanager.ru/win2k_regestry.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
0xBee66740 0x141c0740 \SystemRoot\System32\Config\SOFTWARE
0x90cab9d0 0x172ab9d0 \SystemRoot\System32\Config\DEFAULT
0x9670e9d0 0x1ae799d0 \?\C:\Users\John Doe\ntuser.dat
0x9670f9d0 0x04a719d0 \?\C:\Users\John Doe\AppData\Local\Microsoft\Windows\UsrClass.dat
0x9aaad6148 0x131af148 \SystemRoot\System32\Config\SAM
0x9ab25908 0x14a61088 \SystemRoot\System32\Config\SECURITY
0x9aba79d0 0x11a259d0 \?\C:\Windows\ServiceProfiles\LocalService\NTUSER.DAT
0x9abb1720 0x0a7d4720 \?\C:\Windows\ServiceProfiles\NetworkService\NTUSER.DAT
0xb2b2c088 0x039ef088 [no name]
0xb21c0088 0x039ef088 \REGISTRY\MACHINE\SYSTEM
0xb23c0088 0x02ccf088 \REGISTRY\MACHINE\HARDWARE
0xbee66008 0x141c0088 \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 0xb21c0088 -n 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
To direct input to this VM, move the mouse pointer inside or press Ctrl+G.
```

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 miễn lưu trong bộ nhớ cache được lưu trữ trong sổ đăng ký bằng hashdump.

```
Kali - VMware Workstation
File Edit View VM Help ||| 
File Actions Edit View Help
└─(kali㉿kali)-[~/Downloads/Vol2.6/volatility_2.6_lin64_standalone]
$ ./volatility_2.6_lin64_standalone -f ~/Downloads/nhombay_lab1/ch2.dmp --profile=Win7SP1x86_234x8 hashdump -y 0x8b21c000 -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_234x8 hashdump -y 0x8b21c000 -s 0x9aad6148 > ./test.txt
Volatility Foundation Volatility Framework 2.6

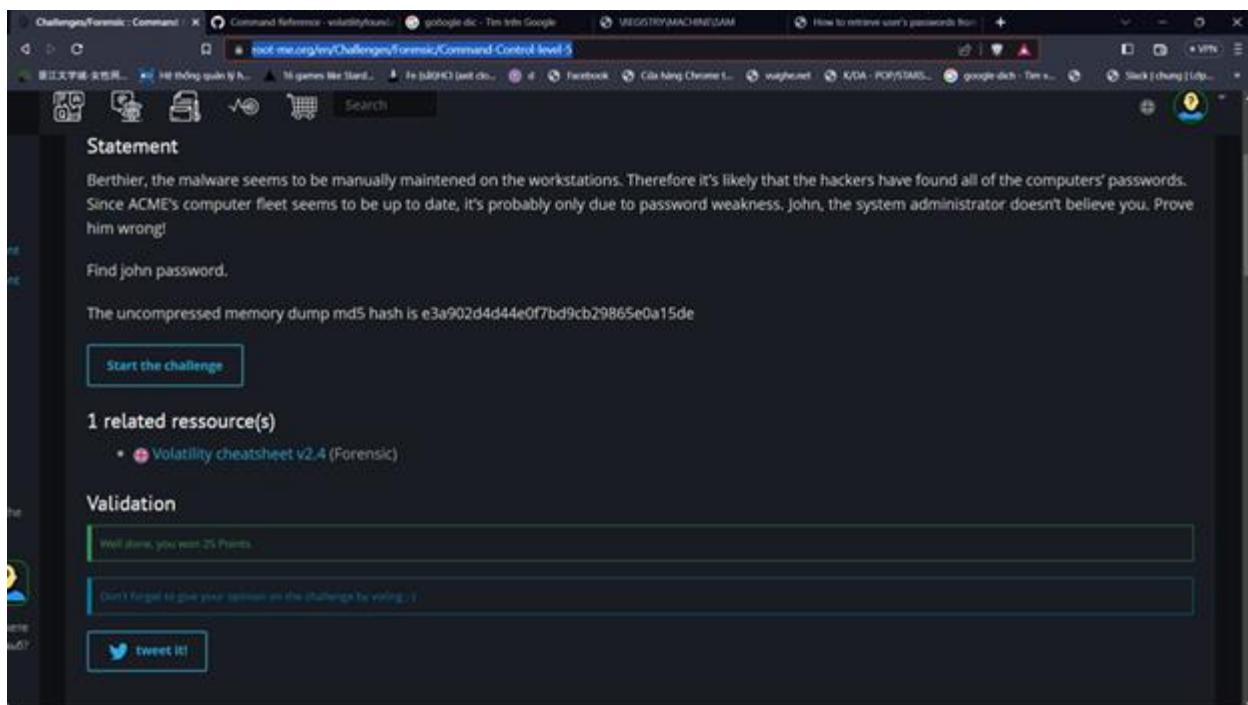
└─(kali㉿kali)-[~/Downloads/Vol2.6/volatility_2.6_lin64_standalone]
$ ls
2168.dmp AUTHORS.txt CREDITS.txt LEGAL.txt LICENSE.txt README.txt test.txt volatility_2.6_lin64_standalone

└─(kali㉿kali)-[~/Downloads/Vol2.6/volatility_2.6_lin64_standalone]
$ cat test.txt
Administrator:500:aad3b435b51404eeaad3b435b51404ee:31d6cfe0d1aae931b73c59d7e0c089c0:::
Guest:501:aad3b435b51404eeaad3b435b51404ee:31d6cfe0d1aae931b73c59d7e0c089c0:::
John Doe:1000:aad3b435b51404eeaad3b435b51404ee:3f917853e3db76e831cce60725930:::

└─(kali㉿kali)-[~/Downloads/Vol2.6/volatility_2.6_lin64_standalone]
```

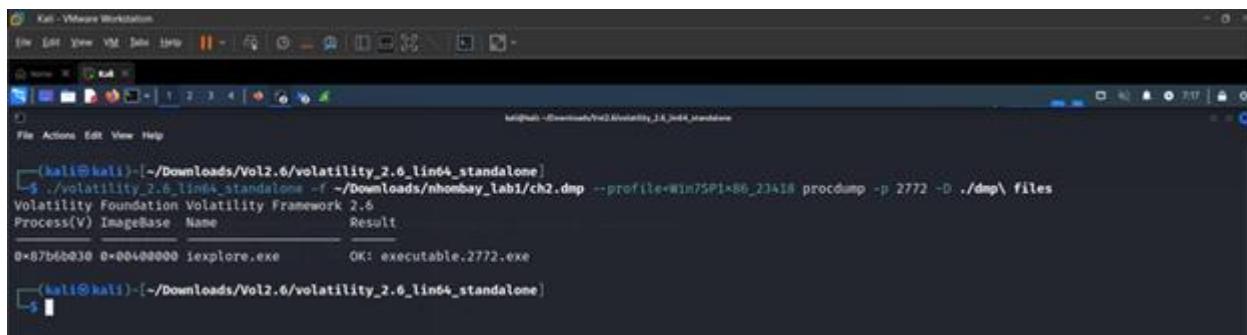
Sau đó, ta chạy hashdump với các địa chỉ ảo đã tìm được, thấy được file lưu password của các account trong hệ thống.

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.

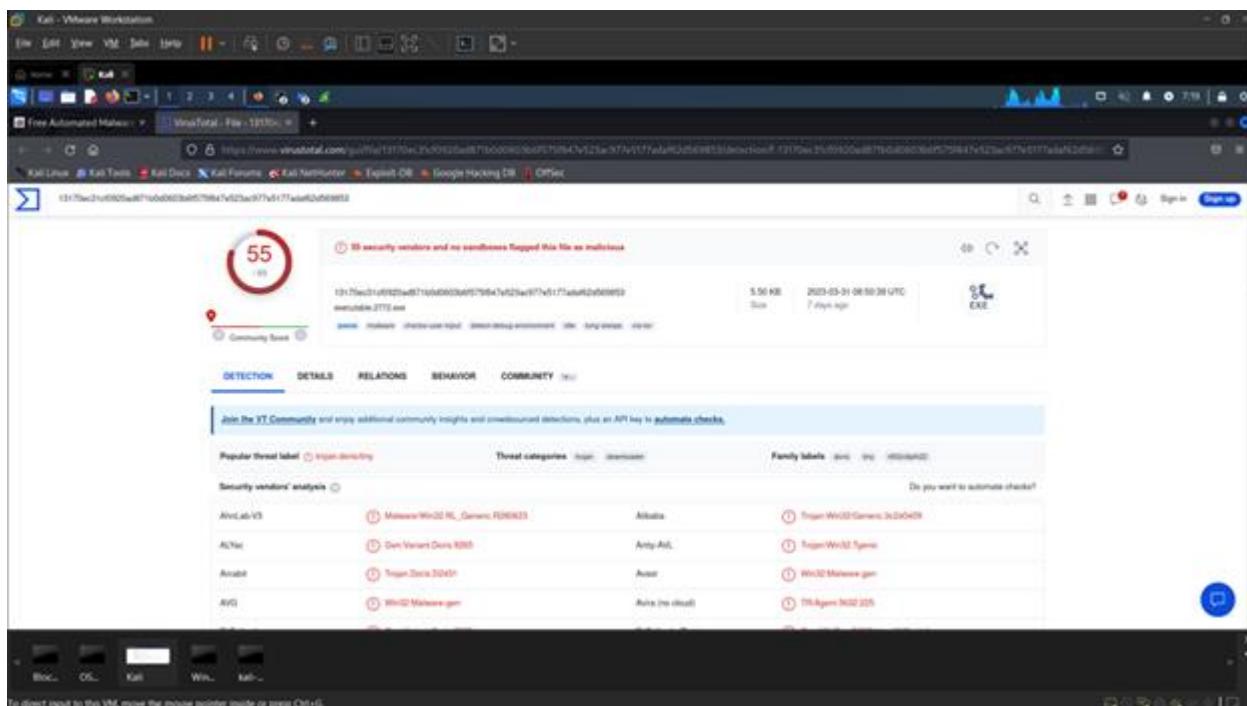


```

Kali - VMware Workstation
File Edit View VM Data Help
File Actions Edit View Help
[ kali@kali: ~/Downloads/Vol2.6 ]$ ./volatility_2.6_x86_64_standalone -f ~/Downloads/nhombay_lab1/ch2.dmp --profile=Win7SP1x86_23418 procdump -p 2772 -o ./dump\ files
Volatility Foundation Volatility Framework 2.6
Process(V) ImageBase Name Result
0x07b6b030 0x00400000 iexplore.exe OK: executable.2772.exe
[ kali@kali: ~/Downloads/Vol2.6 ]$ 

```

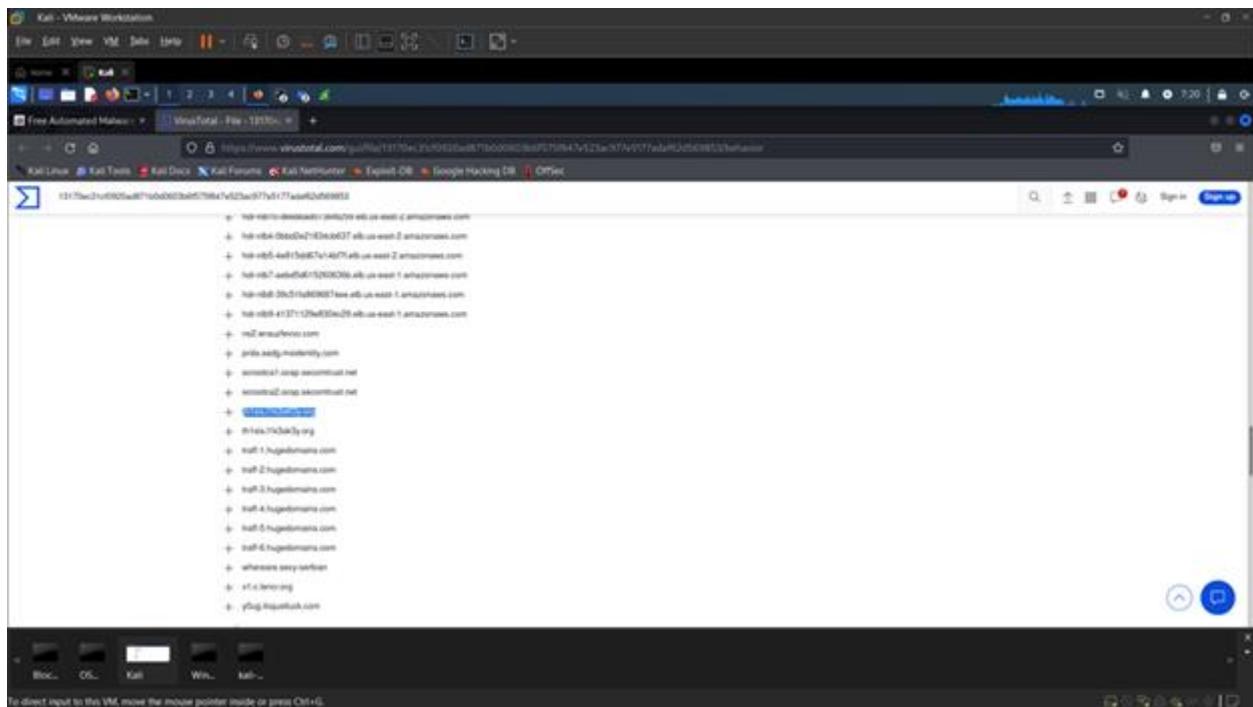
Dump xong, tụi em dùng Hybird Analysis và upload file đã dump ra để phân tích. Phần phân tích cho thấy file thực thi này đúng là mã độc.



The screenshot shows the VirusTotal analysis interface. A file named "executable.2772.exe" has been uploaded. The analysis results indicate 55 security vendors flagged it as malicious. Below the summary, there are tabs for DETECTION, DETAILS, RELATIONS, BEHAVIOR, and COMMUNITY. The BEHAVIOR tab is currently selected, showing various threat labels and their details. One prominent label is "Trojan/Win32.Generic.PJH0403". Other labels include "Malware/Win32.Generic.PJH0403", "Anti-Anti", "Anti-Avi", "Avast", "Avira (no result)", and "W32/Malware.gen". The COMMUNITY tab shows a list of users who have analyzed the file, including "Trojan/Win32.Generic.PJH0403" and "Trojan/Win32.Trojan".

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

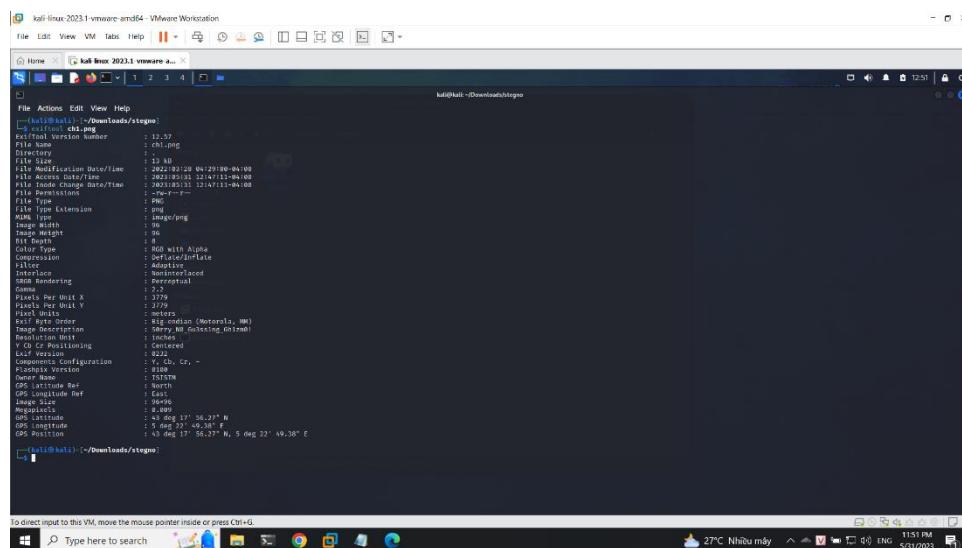
Đầu tiên thực hiện tải file về

```
(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'

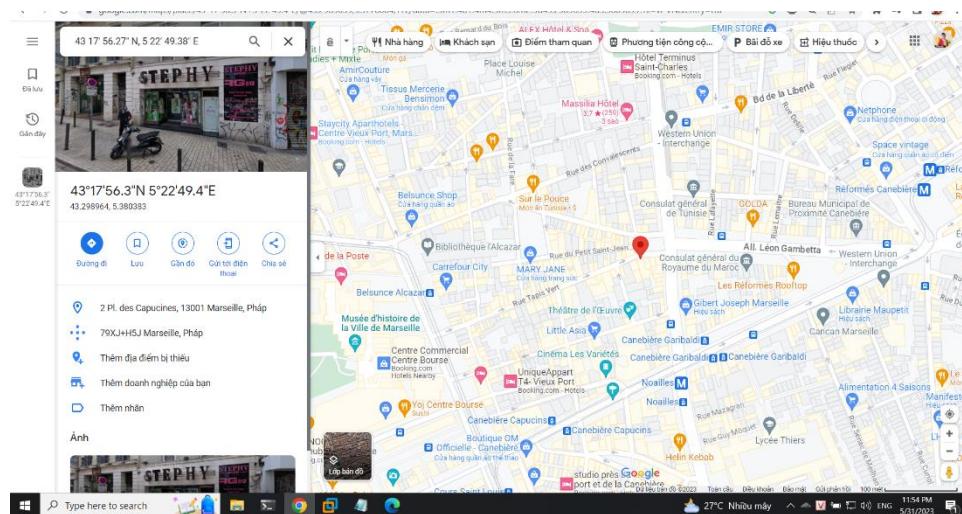
ch1.png          100%[=====] 12.90K -- .KB/s   in 0s

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

Tiếp tục sử dụng exiftool để check hình ảnh

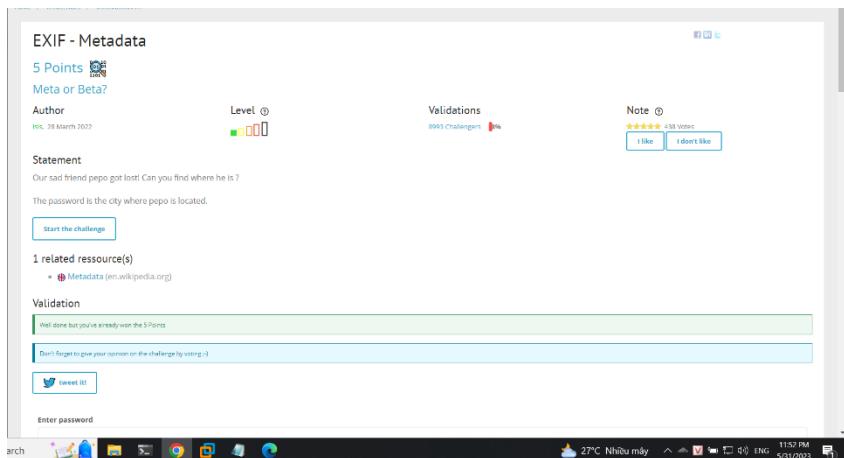


Tìm kiếm địa chỉ trên google map 43 17' 56.27" N, 5 22' 49.38" E



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

Kiểm tra kết quả



Flag: Marseille

Dot and next line

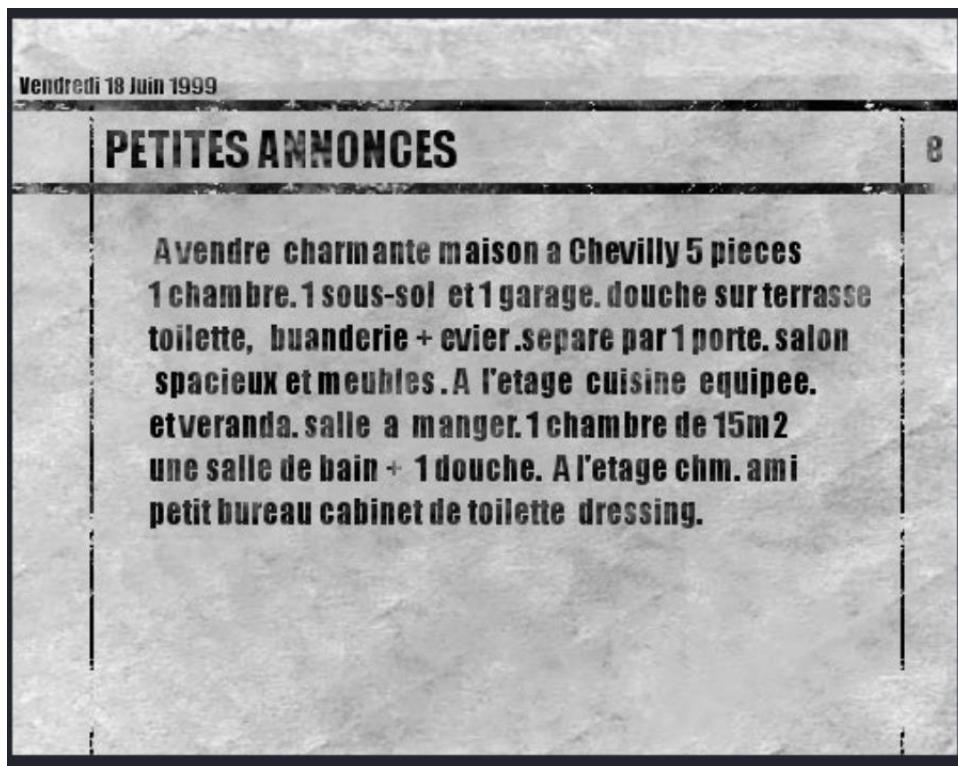
Đầu tiên ta thực hiện tải file

```
(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:

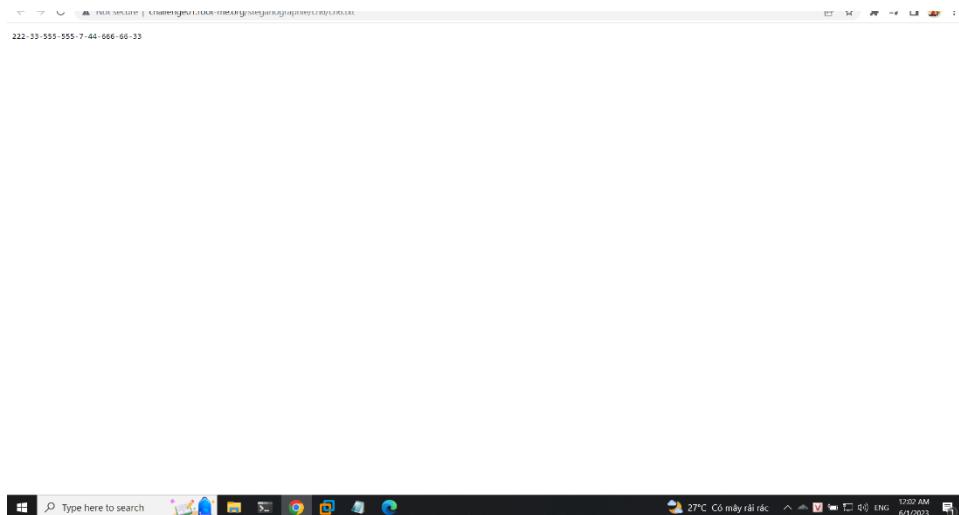
Ghép các ký tự bên dưới dấu chấm lại với nhau và ngược lại, ta có được flag là chatelet15h

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

```

mobile.py X
C:\Users\acer\Downloads>stegno>mobile.py>ans
1   kable = {
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  

homoglyphs

| | | | |
|---|---|---|--|
| Author Kira , 21 December 2016 | Level      | Validations 21235 Challengers  | Note       987 Votes   |
|---|---|---|--|

Statement

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

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

Validation

Well done, you won 10 Points

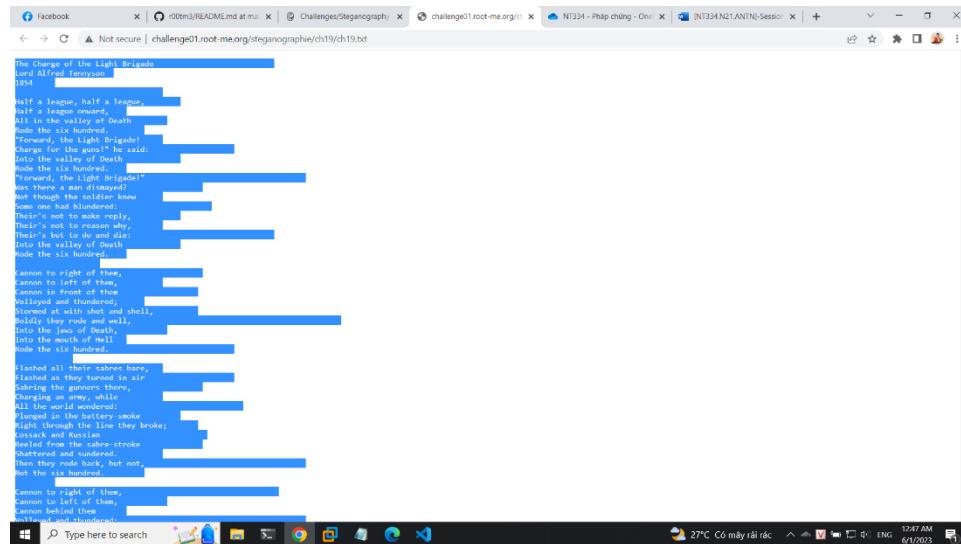
Don't forget to give your opinion on the challenge by voting:-)

 [tweet it!](#)

Enter password

Poem from Space

Đầu tiên ta có được đoạn thông điệp



Ta thấy có một số khoản trống lạ ta sẽ thực hiện decode

Search for a tool

- ★ SEARCH A TOOL ON DCODE BY KEYWORD:
e.g. type 'boolean'
- ★ BROWSE THE FULL DCODE TOOLS LIST [\[LIST\]](#)

Results

[RootMe\Wh1t3_Sp4c3{}](#)

WHITESPACE LANGUAGE

Informatics · Programming Language · Whitespace Language

INTERPRET/EXECUTE WHITESPACE CODE

IMPORT A .WNS FILE READ A WHITESPACE CODE BROWSE WHITESPACE CODE

WHITESPACE FILE .WS Choose File NO FILE CHOSEN

WHITESPACE CODED CIPHERTEXT

Summary

- ★ Interpret/Execute Whitespace code
- ★ Code some text with Whitespace
- ★ What is Whitespace
- lang| H C B (definition)
- ★ H C B in Whitespace?
- ★ How to use Whitespace?
- ★ How to recognize a Whitespace code?
- ★ When Whitespace was invented?

Similar pages

- ★ Brainfuck

Ta có flag là RootMe{Wh1t3_Sp4c3}

Kiểm tra kết quả

Poem from Space

15 Points

Ternary Esoteric Language

Author: Cryptanalyse, 15 july 2020

Level: ①

Validations: 3301 Challengers | 2%

Note: ② ★★★★ 219 Votes

I like I don't like

Statement

Deeply understand the meaning of this famous poem to validate this challenge.

Start the challenge

Validation

Well done, you won 15 Points

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

tweet it!

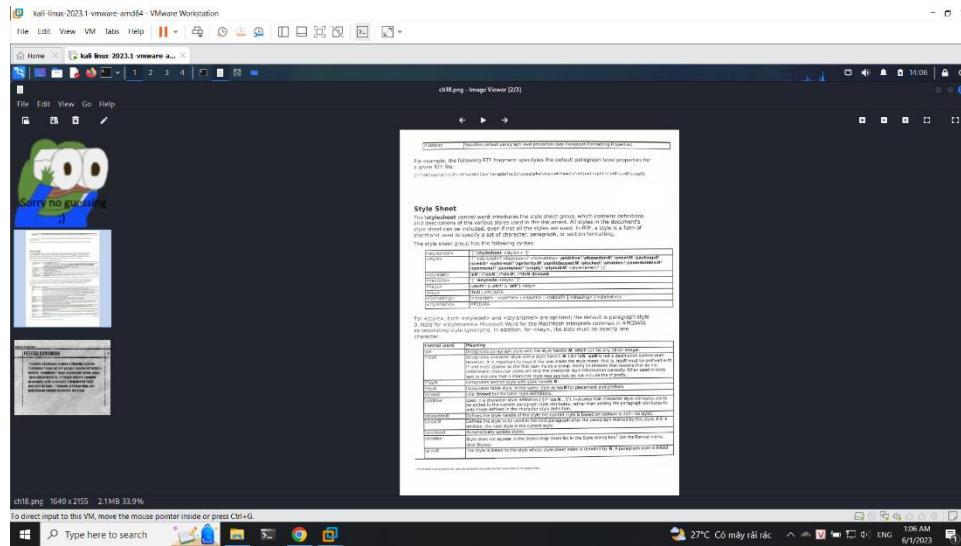
Enter password

send

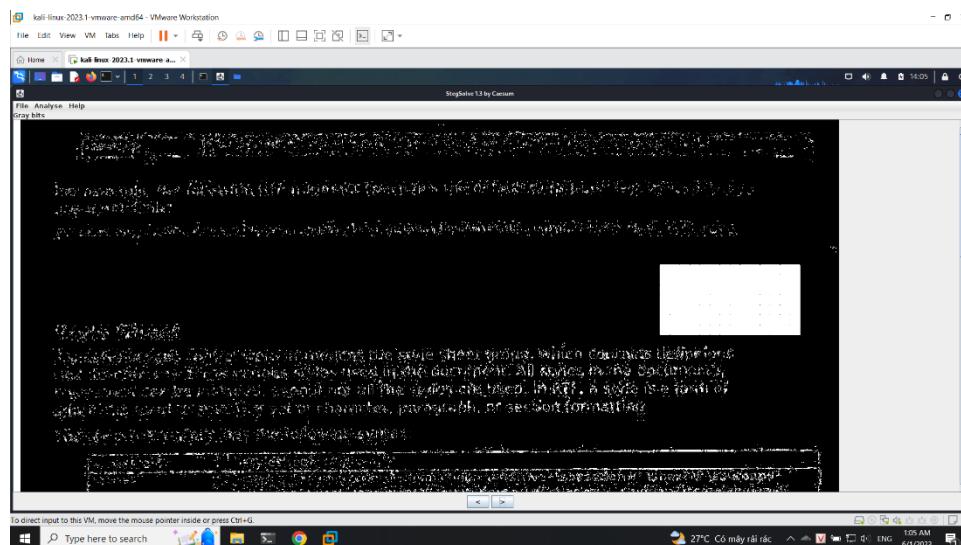
Flag: RootMe{Wh1t3_Sp4c3}

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



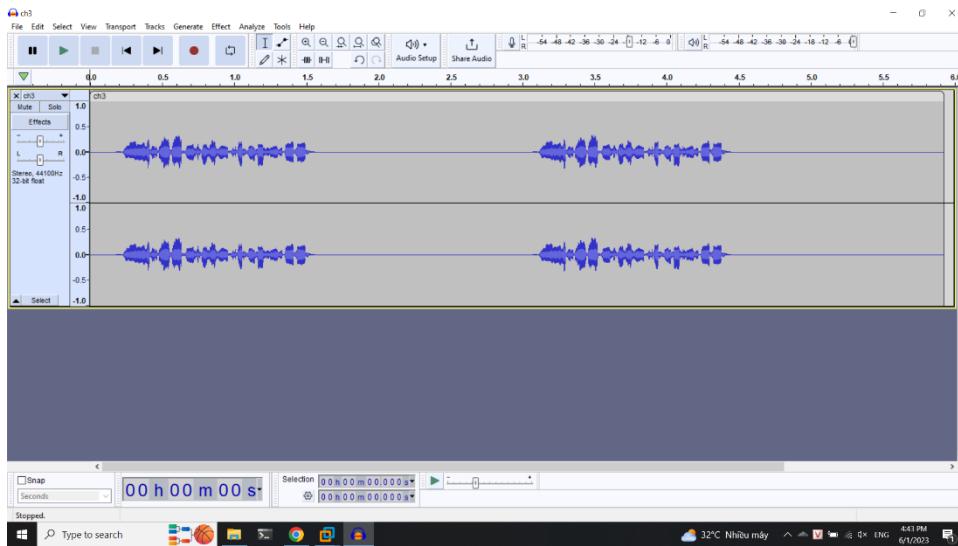
Ta thực hiện giải mã

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

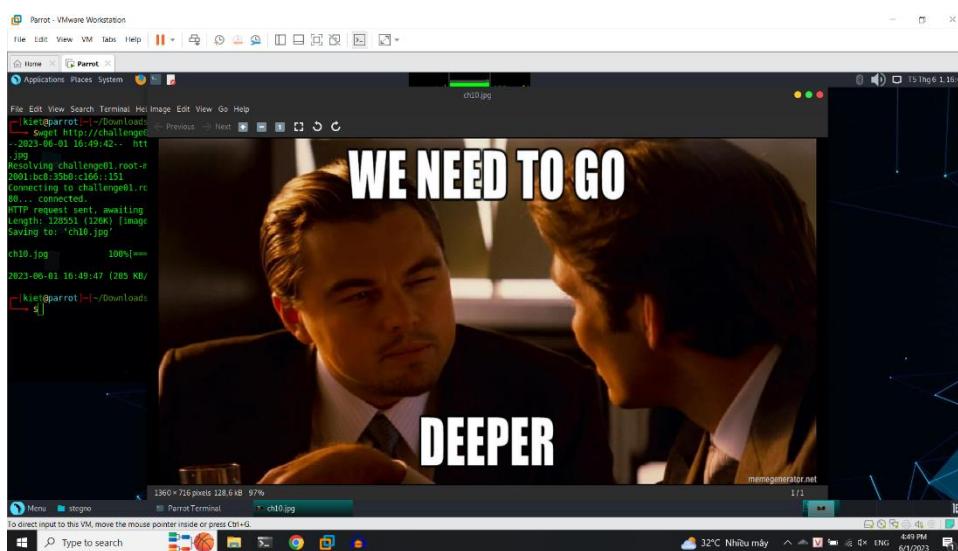


Ta có được flag 3b27641fc5h0

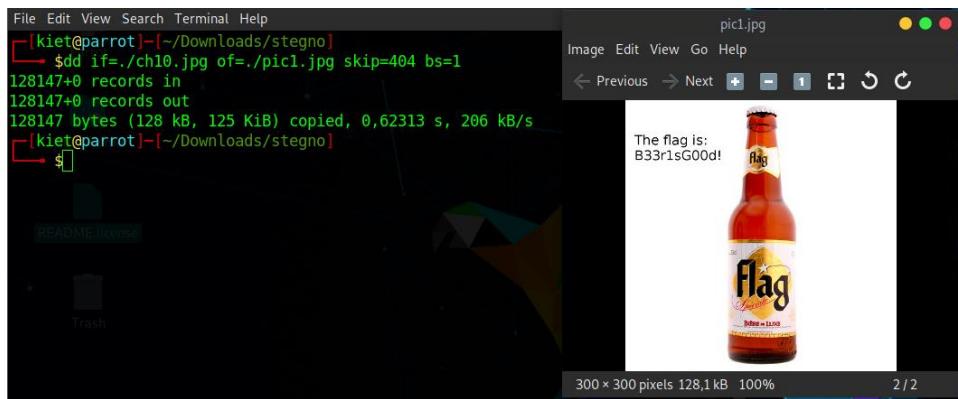
Kiểm tra kết quả

EXIF - Thumbnail

Đầu tiên ta thực hiện tải ảnh về



Thực hiện bóc tách thumbnail ta được thông tin



Ta có flag là B33r1sG00d!

Kiểm tra kết quả

EXIF - Thumbnail

20 Points

Russian dolls

| | | | |
|--|--------------|---|-------------|
| Author whoaim, 12 August 2015 | Level | Validations 9480 Challengers 4% | Note |
| Statement | | Find the password hidden in this image in JPG format. | |
| Start the challenge | | | |
| 1 related ressource(s) = Exif (en.wikipedia.org) | | | |
| Validation Well done, you won 20 Points | | | |
| Don't forget to give your opinion on the challenge by voting ;-) | | | |

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 cœur 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 délivre
Couché 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 mờ 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 | Level | Validations | Note |
|------------------------|---------|----------------------|--|
| g0uZ, 20 December 2014 | Level ① | 21831 Challengers 0% | ★★★★★ 796 Votes <input type="button" value="I like"/> <input type="button" value="I don't like"/> |

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

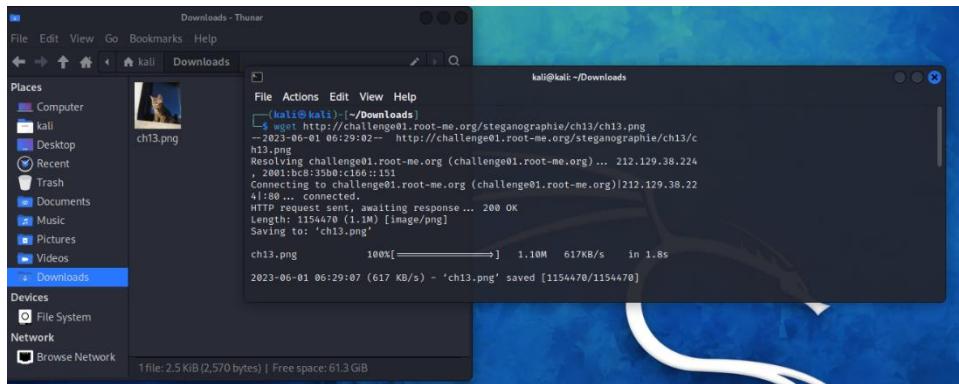
Validation

Well done, you won 10 Points

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

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

Lethle007, 7 August 2017

Level

①

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 ressource(s)

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

Validation

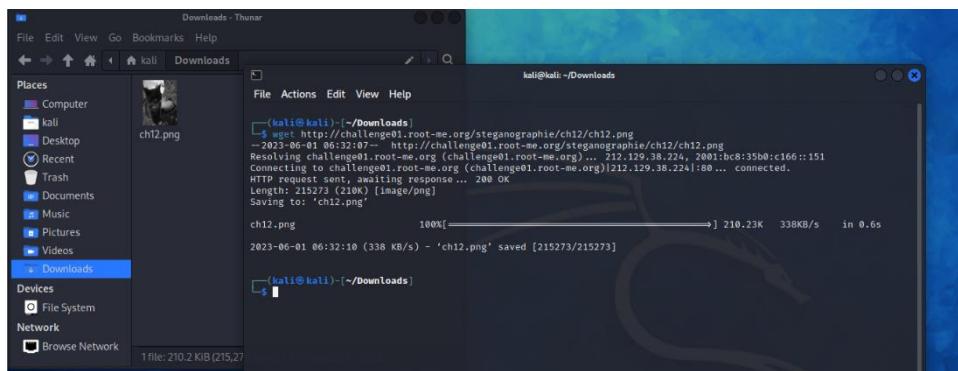
Well done, you won 30 Points

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: LesterROX, 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 (Stéganographie)
- Pixel-Value Differencing Steganography - El-Alfy - Al-Sadi (Stéganographie)

Validation

We did it, you won 30 Points

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

tweet it!

Logs Analysis:

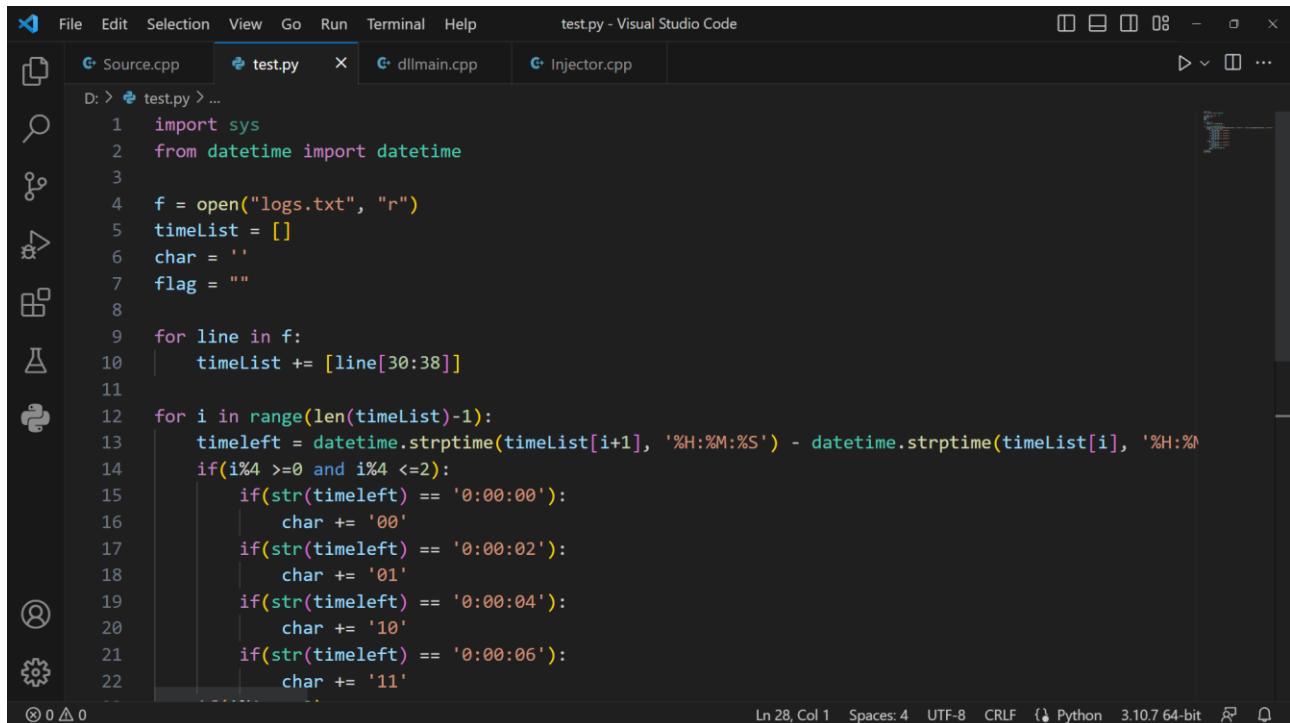
Khi kiểm tra có thể thấy được, đoạn logs được ghi lại ở dạng base64, tái hiện lại các lệnh SQL Blind mà attacker dùng để tấn công. Xem qua các đoạn query, ta có thể nhận thấy attacker đang cố tìm mỗi lần 2 bits của mật khẩu. Khoảng thời gian giữa 2 lần request tới trên log chính là khoảng thời gian giữa request và response của request đó.

The screenshot shows the CyberChef interface with a "From Base64" recipe selected. The input field contains a long base64 encoded string. The output field displays a complex multi-line SQL query. The query includes operations like `concat`, `substr`, and `char` to construct and compare strings, typical for a blind SQL injection exploit.

```

QVNDLChzZixLY3QgKGhlc2UgZm1lbGQoY29uY2F0KH#1Ynli0cmiuZyhiaW4oYXhjawaKoc3ViC3RyaW5nKIBc3N3b3jkLDEsMSkpKSwrLDpLH#1Ynli0cmiuZyhiaW4oYXhjawaKoc3ViC3RyaW5nKIBhch3N3b3jkLDEsMSkpKSwyLDEpkSxjb25jYXQoY2hhcig0CKplGhvbmlihdChjaGFyKDQ4KSksY29uY2F0KGhoyXIoDkplGhoyXIoDgpkKSxjb25jYXQoY2hhcig0OSksY2hhcig00skpxdoZw4gMSBaaGVuIFRSVUugd2h1biayIHRoZW4gc2x1ZXAoMikgd2h1biayIHRoZW4gc2x1ZXAoNCKgd2h1biayIHRoZW4gc2x1ZXAoNikgZw5kKSbcm#tG1lbwyZX#gd2h1cmJgaWQ9MSk%3d
    
```

Đoạn code thực hiện:



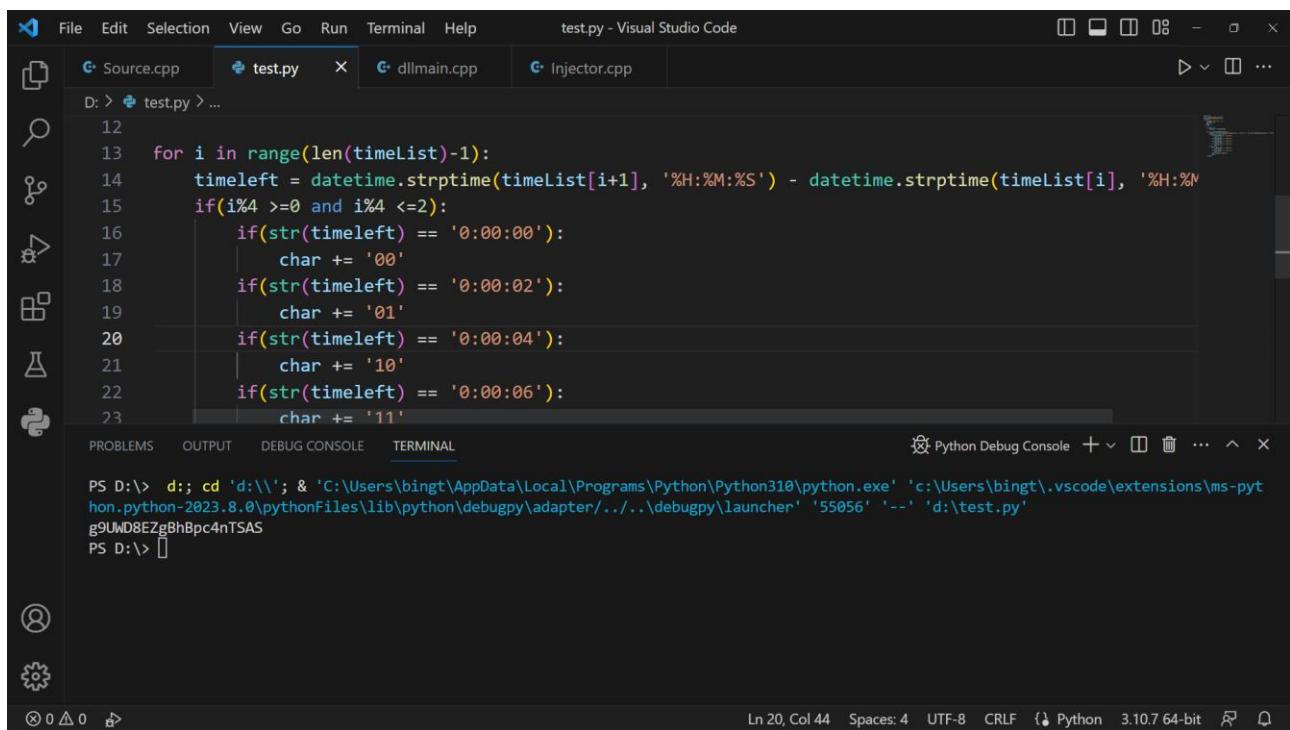
```

File Edit Selection View Go Run Terminal Help test.py - Visual Studio Code
Source.cpp test.py dllmain.cpp Injector.cpp
D: > test.py > ...
1 import sys
2 from datetime import datetime
3
4 f = open("logs.txt", "r")
5 timeList = []
6 char = ''
7 flag = ""
8
9 for line in f:
10     timeList += [line[30:38]]
11
12 for i in range(len(timeList)-1):
13     timeleft = datetime.strptime(timeList[i+1], '%H:%M:%S') - datetime.strptime(timeList[i], '%H:%M:%S')
14     if(i%4 >= 0 and i%4 <=2):
15         if(str(timeleft) == '0:00:00'):
16             char += '00'
17         if(str(timeleft) == '0:00:02'):
18             char += '01'
19         if(str(timeleft) == '0:00:04'):
20             char += '10'
21         if(str(timeleft) == '0:00:06'):
22             char += '11'

```

Ln 28, Col 1 Spaces: 4 UTF-8 CRLF { Python 3.10.7 64-bit

Lấy được flag:



```

File Edit Selection View Go Run Terminal Help test.py - Visual Studio Code
Source.cpp test.py dllmain.cpp Injector.cpp
D: > test.py > ...
12
13 for i in range(len(timeList)-1):
14     timeleft = datetime.strptime(timeList[i+1], '%H:%M:%S') - datetime.strptime(timeList[i], '%H:%M:%S')
15     if(i%4 >= 0 and i%4 <=2):
16         if(str(timeleft) == '0:00:00'):
17             char += '00'
18         if(str(timeleft) == '0:00:02'):
19             char += '01'
20         if(str(timeleft) == '0:00:04'):
21             char += '10'
22         if(str(timeleft) == '0:00:06'):
23             char += '11'

PROBLEMS OUTPUT DEBUG CONSOLE TERMINAL Python Debug Console + ×
PS D:\> d; cd 'd:\\'; & 'C:\Users\bingt\AppData\Local\Programs\Python\Python310\python.exe' 'c:\Users\bingt\.vscode\extensions\ms-pythonhon.python-2023.8.0\pythonFiles\lib\python\debugpy\adapter/../debugpy\launcher' '55056' '--' 'd:\test.py'
g9UD8EzBhBpc4nTSAS
PS D:\> []

Ln 20, Col 44 Spaces: 4 UTF-8 CRLF { Python 3.10.7 64-bit

```

Logs analysis - web attack

25 Points

Author: sambecks, 5 July 2015 | **Level**: ① | **Validations**: 7842 Challengers (3%) | **Note**: 739 Votes

Statement

Our website appears to have been attacked, but our system administrator does not understand web server logs. Can you find out if any data has been stolen ?

Validation

Well done but you've already won the 25 Points

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

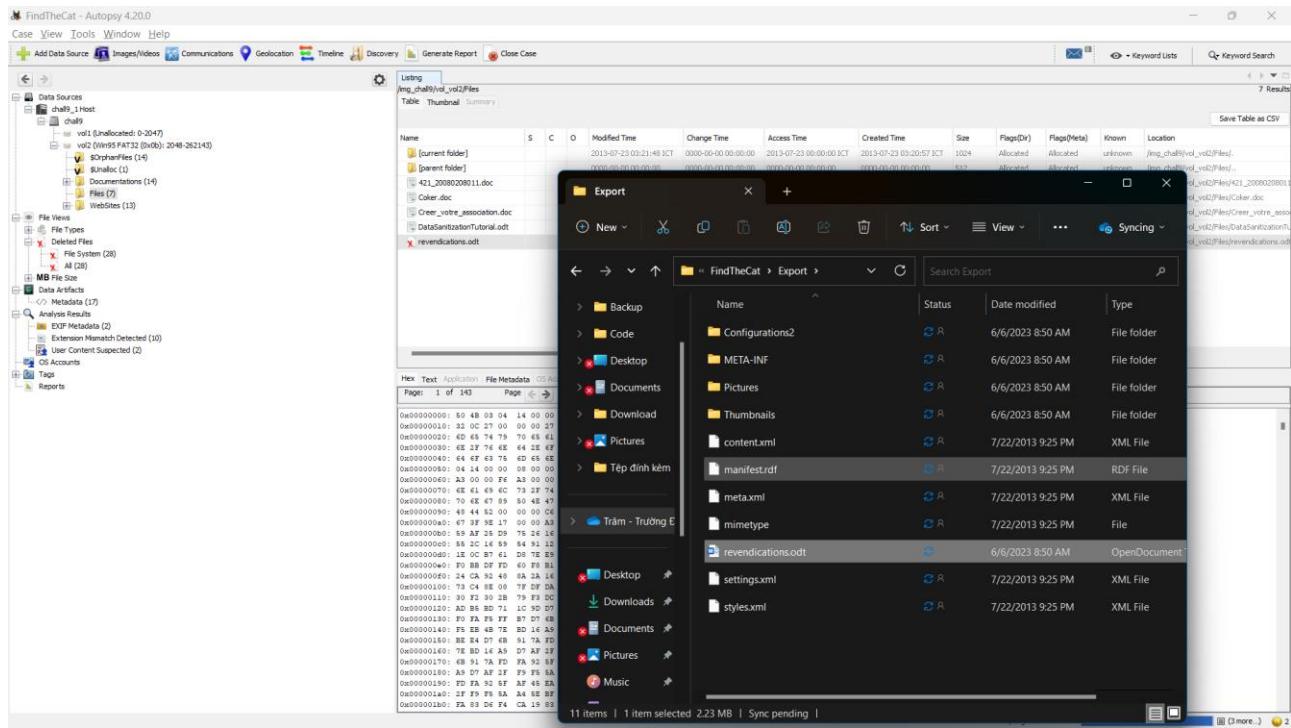
Enter password

Find the cat

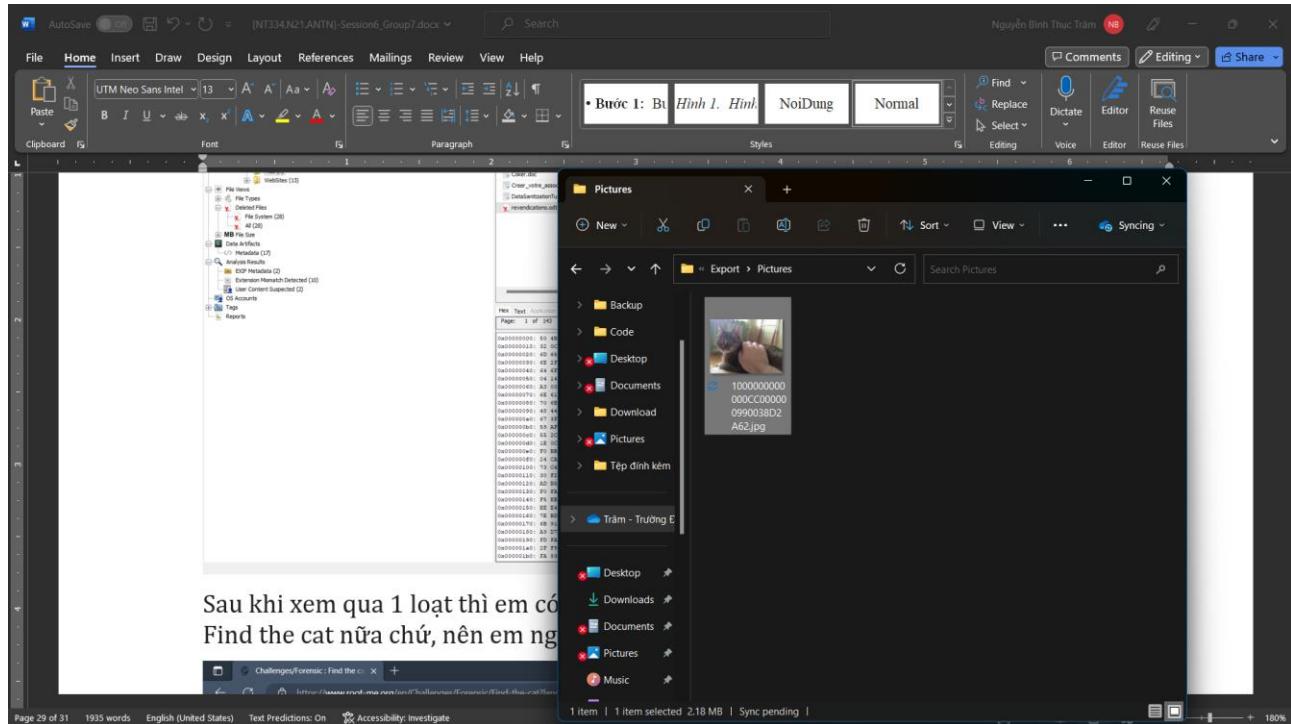
Bỏ file vào AutoSpy để điều tra thì em thấy được file này trông có vẻ khá lạ vì là file .odt mà lại có header là PK (File zip):

| Name | S | C | O | Modified Time | Change Time | Access Time | Created Time | Size | Flag(Dr) | Flag(Meta) | Known | Location |
|------------------------------|---|---|---|-------------------------|---------------------|-------------------------|-------------------------|---------|-------------|-------------|---------|---|
| [current folder] | | | | 2013-07-23 03:21:48 ICT | 2000-00-00 00:00:00 | 2013-07-23 00:00:00 ICT | 2013-07-23 03:20:57 ICT | 1024 | Allocated | Allocated | unknown | /img_chall9/vd_vo2/Files |
| [parent folder] | | | | 0000-00-00 00:00:00 | 0000-00-00 00:00:00 | 0000-00-00 00:00:00 | 0000-00-00 00:00:00 | 512 | Allocated | Allocated | unknown | /img_chall9/vd_vo2/Files |
| 421_200802080111-doc | | | | 2013-07-23 03:20:56 ICT | 2000-00-00 00:00:00 | 2013-07-23 00:00:00 ICT | 2013-07-23 03:20:57 ICT | 1197056 | Allocated | Allocated | unknown | /img_chall9/vd_vo2/Files/K1_200802080111 |
| Coker.doc | | | | 2013-07-23 03:20:56 ICT | 2000-00-00 00:00:00 | 2013-07-23 00:00:00 ICT | 2013-07-23 03:20:57 ICT | 142336 | Allocated | Allocated | unknown | /img_chall9/vd_vo2/Files/Coker.doc |
| Creer_votre_association.doc | | | | 2013-07-23 03:20:56 ICT | 0000-00-00 00:00:00 | 2013-07-23 00:00:00 ICT | 2013-07-23 03:20:57 ICT | 67944 | Allocated | Allocated | unknown | /img_chall9/vd_vo2/Files/Creer_votre_association.doc |
| DataSanitizationTutorial.odt | | | | 2013-07-23 03:20:56 ICT | 0000-00-00 00:00:00 | 2013-07-23 00:00:00 ICT | 2013-07-23 03:20:57 ICT | 62166 | Allocated | Allocated | unknown | /img_chall9/vd_vo2/Files/DataSanitizationTutorial.odt |
| revendications.odt | | | | 2013-07-23 03:20:56 ICT | 0000-00-00 00:00:00 | 2013-07-23 00:00:00 ICT | 2013-07-23 03:20:57 ICT | 2941273 | Unallocated | Unallocated | unknown | /img_chall9/vd_vo2/Files/revendications.odt |

Vì vậy em đã extract file này ra và giải nén thử, bên trong có khá nhiều folder.



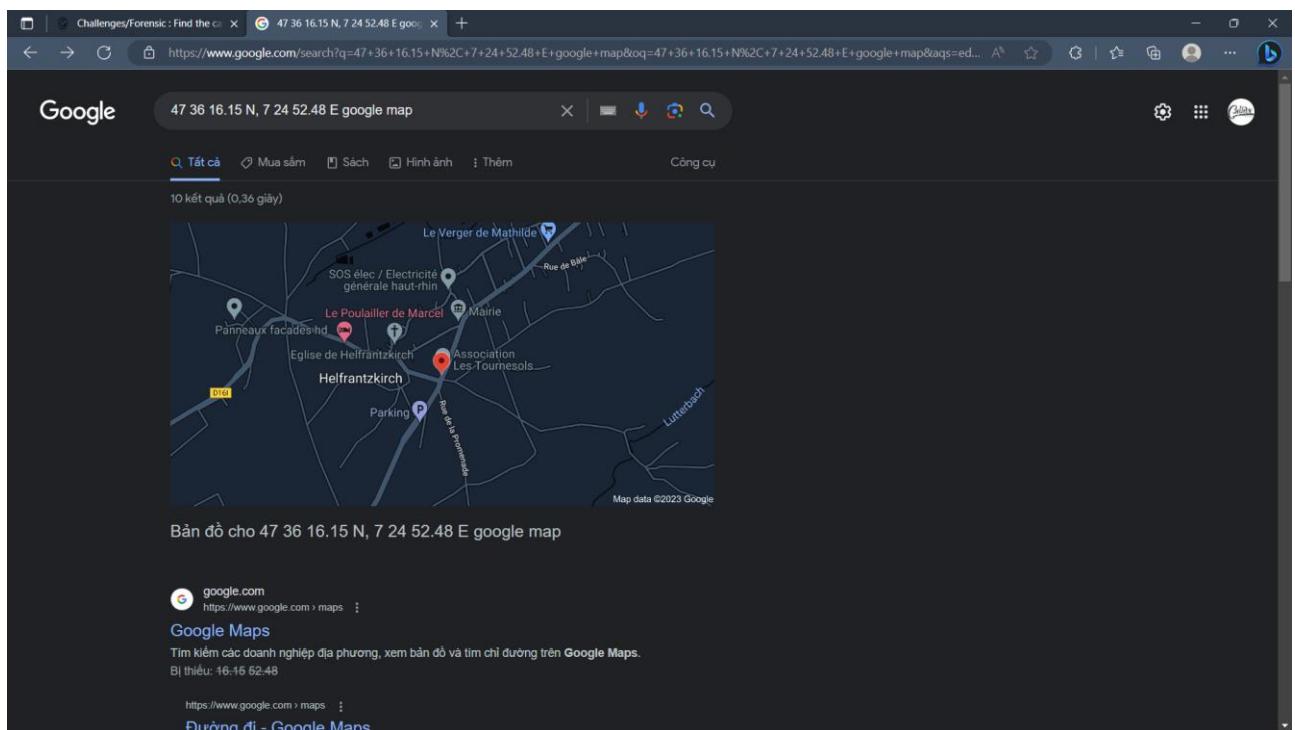
Sau khi xem qua 1 loạt thì em có thấy một số tấm hình là ảnh mèo, mà tên bài lại là Find the cat nữa chứ, nên em nghĩ đến việc check coordinate của mấy tấm ảnh mèo này:



Check thử tấm này thì thấy đúng là có tọa độ GPS.

```
(kali㉿kali)-[~/forensic]
$ mv /var/run/vmblock-fuse/blockdir/2Rvq9h/1000000000000CC000000990038D2A62.jpg cat
(kali㉿kali)-[~/forensic]
└─ exiftool cat | grep GPS
  GPS Latitude Ref : North
  GPS Longitude Ref : East
  GPS Altitude Ref : Above Sea Level
  GPS Time Stamp : 07:46:50.85
  GPS Img Direction Ref : True North
  GPS Img Direction : 247.3508772
  GPS Altitude : 16.7 m Above Sea Level
  GPS Latitude : 47 deg 36' 16.15" N
  GPS Longitude : 7 deg 24' 52.48" E
  GPS Position : 47 deg 36' 16.15" N, 7 deg 24' 52.48" E
(kali㉿kali)-[~/forensic]
$
```

Em search tọa độ vừa tìm được trên gg maps và thấy được tọa độ này ở Helfrantzkirch, vậy nên em thử submit flag này.



Done.

Job Interview:

Sau khi kiểm tra thì em biết được file này là dạng ewf:

```
(kali㉿kali)-[~/rootmeJobinterview]
$ file /var/run/vmblock-fuse/blockdir/sELgLU/jobinterview.e01
/var/run/vmblock-fuse/blockdir/sELgLU/jobinterview.e01: EWF/Expert Witness/EnCase image file format
```

Vì vậy, em sử dụng ewfmount để mount file vào, nhận được file ewf1 như hình dưới:

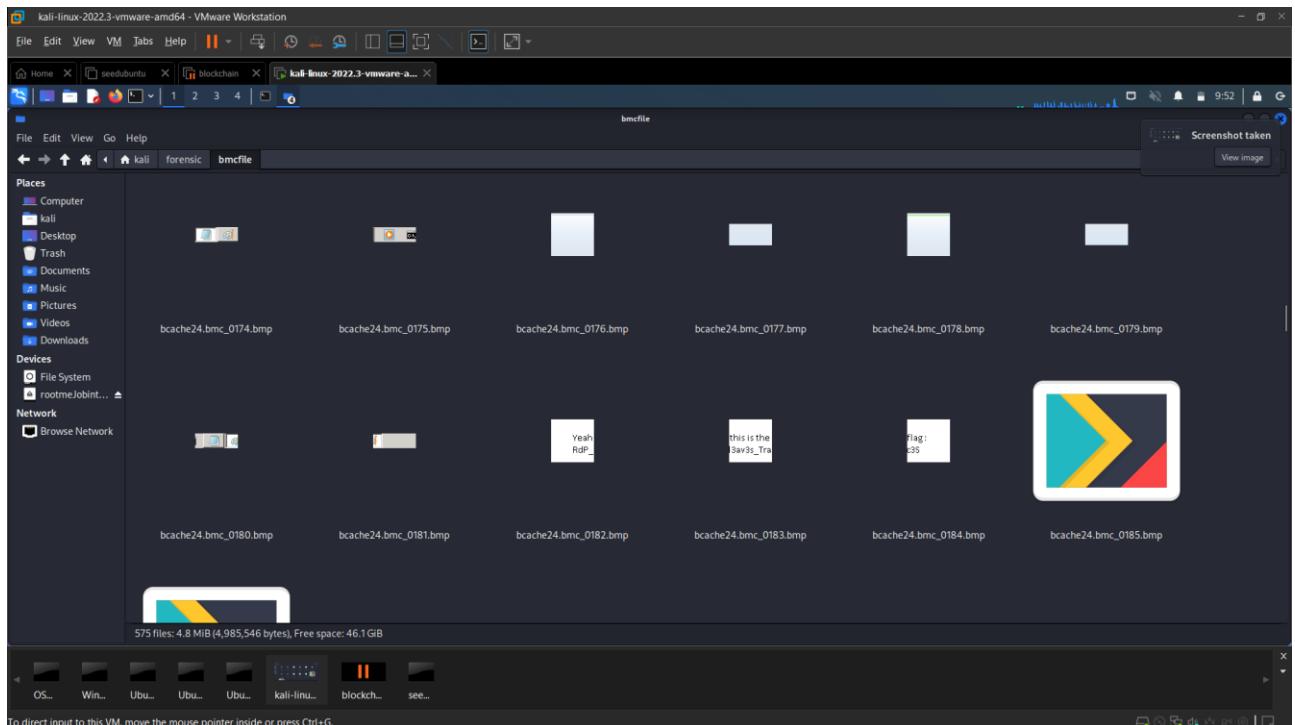
```
(kali㉿kali)-[~/rootmeJobinterview]
$ ls
ewf1
```

Sau khi extract file này ra, em nhận được file bcache24.bmc, file này là 1 file bmc nên em dùng bmc-tools để có thể giải nén nó ra:

```
(kali㉿kali)-[~/forensic/bmc-tools]
$ ./bmc-tools.py -s .. /bcache24.bmc -d .. /bmcfile/ -v
[+] Processing a single file: '../bcache24.bmc'.
[=] Successfully loaded '../bcache24.bmc' as a .BMC container.
[+] 100 tiles successfully extracted so far.
[+] 200 tiles successfully extracted so far.
[+] 300 tiles successfully extracted so far.
[+] 400 tiles successfully extracted so far.
[+] 500 tiles successfully extracted so far.
[=] 575 tiles successfully extracted in the end.
[=] Successfully exported 575 files.
```

Sau khi giải nén, ta nhận được 575 files bit ảnh, em tìm trong này và thấy được có 3 bits hiển thị flag.

RdP_l3av3s_Trac3S



Nhập flag và submit:

Deleted File:

Sau khi extract file đê cho ra, em nhận được file usb.image, khi kiểm tra thì thấy đây là 1 file DOS/MBR boot sector.

```
(kali㉿kali)-[~/forensic]
└─$ file usb.image
usb.image: DOS/MBR boot sector, code offset 0x3c+2, OEM-ID "mkfs.fat", sectors/cluster 4, reserved sectors 4, root entries 512, sectors 63488 (volumes < 32 MB), Media descriptor 0xf8, sectors/FAT 64, sectors/track 62, heads 124, hidden sectors 2048, reserved 0x1, serial number 0xc7ecde5b, label: "USB", FAT (16 bit)
```

Do tên bài là Deleted File nên em sẽ dùng sleuthkit để xem file nào đã bị xóa thì thấy được có 1 file ảnh, vậy nên tiếp tục dùng icat của sleuthkit để extract ảnh ra.

```
(kali㉿kali)-[~/forensic]
└─$ fls usb.image
r/r 3: USB          (Volume Label Entry)
r/r * 5:           anonyme.png
v/v 1013699:       $MBR
v/v 1013700:       $FAT1
v/v 1013701:       $FAT2
V/V 1013702:       $OrphanFiles

(kali㉿kali)-[~/forensic]
└─$ icat usb.image 5 > output
```

Lấy ảnh này ra bỏ lên trang đọc metadata thì thấy được tên người tạo ảnh. Em đoán đây là flag do đề nói flag là firstname_lastname của người sở hữu usb.

The data shown is all the metadata we could automatically extract from your file. It may be neither complete nor adequate. Metadata could have been changed or deleted in the past. Please be aware that the metadata is provided without liability.

Chỉnh flag lại đúng format: javier_turcot. Submit flag:

The screenshot shows a challenge titled "Deleted file" with 5 Points. The challenge details state: "You can look all you want, but this key is empty...". It includes information about the author (Manah), level (Easy), validations (632 Challengers, 1%), and a note section with 74 votes. A statement says: "Your cousin found a USB drive in the library this morning. He's not very good with computers, so he's hoping you can find the owner of this stick!". Below this, there is a form field: "The flag is the owner's identity in the form | Firstname_lastname |". The sha256sum of the file is listed as E3B0C44298FC1C149AFBF4C8996FB92427AE41E4649B934CA495991B7852B855. A "Start the challenge" button is present. The validation section shows: "Well done, you won 5 Points" and "Don't forget to give your opinion on the challenge by voting :-)". A "tweet it!" button is also visible.

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, trẽ, ... sẽ được xử lý tùy mức độ vi phạm.

HẾT