BÁO CÁO THỰC HÀNH

Môn học: Pháp chứng kỹ thuật số

Lab 6: Final Test

GVHD: Đoàn Minh Trung

1. THÔNG TIN CHUNG:

(Liệt kê tất cả các thành viên trong nhóm)

Lớp: NT334.N21.ATCL.1

STT	Họ và tên	MSSV	Email
1	Lê Viết Tài Mẫn	20521593	20521593@gm.uit.edu.vn
2	Vũ Hoàng Thạch Thiết	20521957	20521957@gm.uit.edu.vn
3	Hoàng Thanh Lâm	20521513	20521513@gm.uit.edu.vn

2. NỘI DUNG THỰC HIỆN:[1]

STT	Công việc	Kết quả tự đánh giá
1	Dump	100%

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

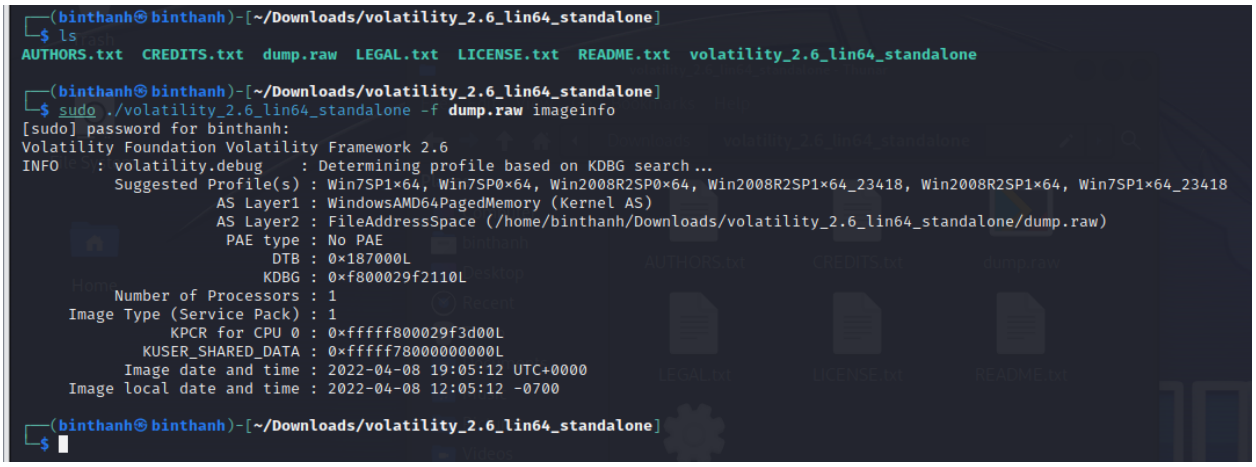
[1] Ghi nội dung công việc, các kịch bản trong bài Thực hành

BÁO CÁO CHI TIẾT

1. Dump

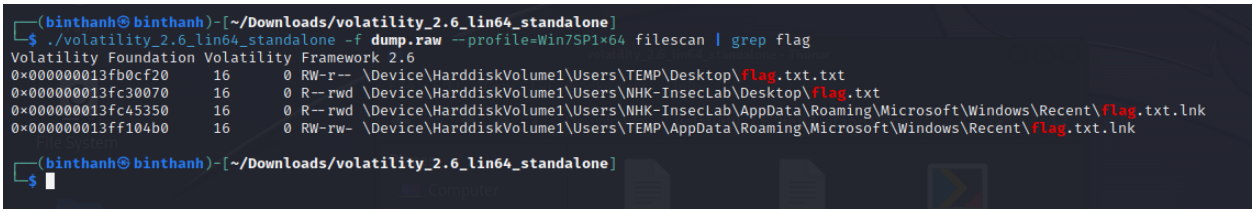
Sau khi có dữ liệu là file dump.zip em tiến hành giải nén và thu được file dump.raw

Lấy thông tin cơ bản bằng imageinfo

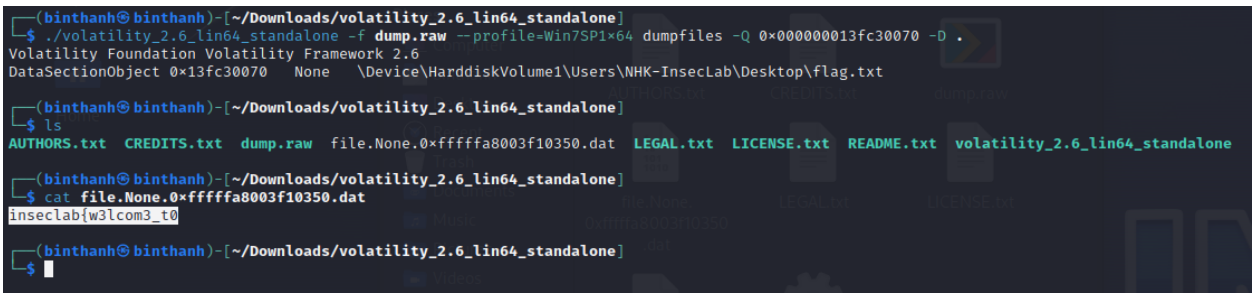


+ Thu thập các file bất thường để ghép mảnh flag.

Thực hiện scan file để tìm tìm thông tin liên quan tới “flag”



Ở địa chỉ là 0x000000013fc30070 có file **flag.txt** nên ta sẽ dump file này và khai thác



Ta đã có flag tuy nhiên chỉ mới được 1 nửa: **inseclab{w3lcom3_t0**

Tiếp theo ta xài pstree để tìm hiểu tất cả các tiến trình đang chạy thì thấy web đang chạy bằng lệnh dưới :

./volatility_2.6_lin64_standalone -f dump.raw --profile=Win7SP1x64 pstree

```
┌──(binthanh㉿binthanh)-[~/Downloads/volatility_2.6_lin64_standalone]
└─$ ./volatility_2.6_lin64_standalone -f dump.raw --profile=Win7SP1x64 pstree
Volatility Foundation Volatility Framework 2.6
Name                                                  Pid   PPid   Thds   Hnds Time
-------------------------------------------------- ------ ------ ------ ------ ----
 0xfffffa800cdfc570:wininit.exe                       392    332      3     76 2022-04-08 17:44:22 UTC+0000
. 0xfffffa8005a1cb10:services.exe                     456    392      7    223 2022-04-08 17:44:22 UTC+0000
.. 0xfffffa8005c04870:svchost.exe                     384    456     15    482 2022-04-08 17:44:23 UTC+0000
... 0xfffffa800bdfa880:csrss.exe                      404    384     16    279 2022-04-08 17:44:22 UTC+0000
.... 0xfffffa80062eab10:conhost.exe                  4352    404      2     52 2022-04-08 19:05:10 UTC+0000
... 0xfffffa8005a248f0:winlogon.exe                   496    384      3    110 2022-04-08 17:44:22 UTC+0000
. 0xfffffa8005a1f750:lsm.exe                          472    392      9    157 2022-04-08 17:44:22 UTC+0000
 0xfffffa800584d060:csrss.exe                         340    332      9    502 2022-04-08 17:44:22 UTC+0000
. 0xfffffa8005eee8c0:conhost.exe                     1680    340      2     33 2022-04-08 17:44:24 UTC+0000
 0xfffffa8003c71b10:System                              4      0     91    546 2022-04-08 17:44:21 UTC+0000
. 0xfffffa8005334620:smss.exe                         264      4      2     29 2022-04-08 17:44:21 UTC+0000
 0xfffffa8006156b10:explorer.exe                     2528   2504     25    937 2022-04-08 17:44:39 UTC+0000
. 0xfffffa80063ff600:vmtoolsd.exe                    1732   2528      8    278 2022-04-08 17:44:47 UTC+0000
. 0xfffffa8004220060:chrome.exe                      2332   2528      0 ------ 2022-04-08 19:02:52 UTC+0000
.. 0xfffffa8005461700:DumpIt.exe                     4512   2332      5     46 2022-04-08 19:05:10 UTC+0000
 0xfffffa8006265060:GoogleCrashHan                   2916   2884      5     90 2022-04-08 17:44:40 UTC+0000
 0xfffffa80062689c0:GoogleCrashHan                   2924   2884      5     83 2022-04-08 17:44:41 UTC+0000
```

Dựa vào gợi ý của bạn bè thì nhóm em thực hiện dump lịch sử trình duyệt web với -plugin chromehistory. Và khai thác

Trước đó thì ta cần tải [volatility-plugins] sau đó bỏ vào file plugins của volatility.

python2 vol.py --plugins=volatility-plugins/ -f dump.raw --profile=Win7SP1x64 chromehistory

```
  21 https://inseclab.uit.edu.vn/bai-bao-ngh ... eu-hoinghi-khoa-hoc-quoc-te-nics-2021/ The UIT Information Security Laboratory
   N/A
  20 https://inseclab.uit.edu.vn/                                                      The UIT Information Security Laboratory
   N/A
  17 https://mh-nexus.de/en/hxd/                                                       HxD - Freeware Hex Editor and Disk Editor | mh-nexus
   N/A
  15 https://github.com/goliate/hidden-tear/ ... -tear/bin/Debug/hidden-tear.vshost.exe hidden-tear/hidden-tear.vshost.exe at master · goliate/hidden-tear · GitHub
N/A
  14 https://github.com/goliate/hidden-tear/ ... ster/hidden-tear/hidden-tear/bin/Debug hidden-tear/hidden-tear/hidden-tear/bin ... aster · goliate/hidden-tear · GitHu
N/A
  13 https://github.com/goliate/hidden-tear/ ... ter/hidden-tear/hidden-tear/Properties hidden-tear/hidden-tear/hidden-tear/Pro ... aster · goliate/hidden-tear · GitHu
N/A
  12 https://github.com/goliate/hidden-tear/tree/master/hidden-tear/hidden-tear       hidden-tear/hidden-tear/hidden-tear at master · goliate/hidden-tear · GitHub
N/A
  11 https://github.com/goliate/hidden-tear/tree/master/hidden-tear                    hidden-tear/hidden-tear/hidden-tear at master · goliate/hidden-tear · GitHub
N/A
  10 https://github.com/goliate/hidden-tear                                            GitHub - goliate/hidden-tear: ransomware open-sources
   N/A
   8 https://pastebin.com/k2HuWZmp                                                     https://drive.google.com/file/d/1TxvMNb ... RWjD7wZc/view?usp=shari - Pastebin.
   N/A
   3 https://www.win-rar.com/download.html?&L=0                                        WinRAR download free and support: WinRAR Download Latest Version
   N/A
   2 https://www.win-rar.com/download.html                                             WinRAR download free and support: WinRAR Download Latest Version
   N/A
```

Trong lịch sử ta thấy có phần mềm WinRAR được tải về, có thể là để giải nén một file nào đó (có thể là flag) nên ta sẽ thử tìm các file .rar xem có file nào liên quan tới flag không

Kết quả là có file h4lf-fl4g.rar (half-flag) có thể là nửa flag còn lại

```
┌──(binthanh㉿binthanh)-[~/Downloads/volatility_2.6_lin64_standalone]
└─$ ./volatility_2.6_lin64_standalone -f dump.raw --profile=Win7SP1x64 filescan | grep -E "\.rar"
Volatility Foundation Volatility Framework 2.6
0x00000000071f3a10     16      0 RW---- \Device\HarddiskVolume1\Users\TEMP\Desktop\h4lf-fl4g.rar
0x000000013feb7f20     16      0 R--rwd \Device\HarddiskVolume1\Users\NHK-InsecLab\AppData\Roaming\Microsoft\Windows\Recent\fl4g.rar.lnk

┌──(binthanh㉿binthanh)-[~/Downloads/volatility_2.6_lin64_standalone]
└─$
```

Tiến hành dump và đổi tên file thành halfflag để tiện sử dụng:

```
┌──(binthanh㉿binthanh)-[~/Downloads/volatility_2.6_lin64_standalone]
└─$ ./volatility_2.6_lin64_standalone -f dump.raw --profile=Win7SP1x64 dumpfiles -Q 0x00000000071f3a10 -D .
Volatility Foundation Volatility Framework 2.6
DataSectionObject 0x071f3a10   None   \Device\HarddiskVolume1\Users\TEMP\Desktop\h4lf-fl4g.rar

┌──(binthanh㉿binthanh)-[~/Downloads/volatility_2.6_lin64_standalone]
└─$ ls
AUTHORS.txt  CREDITS.txt  dump.raw  file.None.0xfffffa8003d61f10.dat  file.None.0xfffffa8003f10350.dat  LEGAL.txt  LICENSE.txt  README.txt  volatility_2.6_lin64_standalone

┌──(binthanh㉿binthanh)-[~/Downloads/volatility_2.6_lin64_standalone]
└─$ sudo mv file.None.0xfffffa8003d61f10.dat halfflag.rar
[sudo] password for binthanh:

┌──(binthanh㉿binthanh)-[~/Downloads/volatility_2.6_lin64_standalone]
└─$ ls
AUTHORS.txt  CREDITS.txt  dump.raw  file.None.0xfffffa8003f10350.dat  halfflag.rar  LEGAL.txt  LICENSE.txt  README.txt  volatility_2.6_lin64_standalone
```

Sau đó để thuận tiện em đổi tên file thành hidden.rar rồi sau đó tiến hành giải nén nhưng nó yêu cầu mật khẩu

Sau khi tham khảo và các gợi ý thì ta sẽ sử dụng rar2john để có mã hash của file hidden.rar

```
┌──(binthanh㉿binthanh)-[~/Downloads/volatility_2.6_lin64_standalone]
└─$ rar2john halfflag.rar > halfflag.txt
Created directory: /home/binthanh/.john

┌──(binthanh㉿binthanh)-[~/Downloads/volatility_2.6_lin64_standalone]
└─$ ls
AUTHORS.txt  CREDITS.txt  dump.raw  file.None.0xfffffa8003f10350.dat  h4lf-fl4g.txt  halfflag.rar  halfflag.txt  LEGAL.txt  LICENSE.txt  README.txt  volatility_2.6_lin64_standalone

┌──(binthanh㉿binthanh)-[~/Downloads/volatility_2.6_lin64_standalone]
└─$ cat halfflag.txt
halfflag.rar:$rar5$16$7a3f367e550900d03550fdaaa0937470$15$6cff83d489ca5fef8c6ae8fc7abd4168$8$2948156db3e079b9

┌──(binthanh㉿binthanh)-[~/Downloads/volatility_2.6_lin64_standalone]
└─$
```

Tại đây ta đã nắm được hash password rar có dạng như trên.
Sau đó dùng john để tìm password có mã hash tương ứng với wordlist rockyou sử dụng công cụ john
john --wordlist=/usr/share/wordlists/rockyou.txt hidden.txt

```
└─$ john --wordlist=/usr/share/wordlists/rockyou.txt hidden.txt
Using default input encoding: UTF-8
Loaded 1 password hash (RAR5 [PBKDF2-SHA256 256/256 AVX2 8x])
Cost 1 (iteration count) is 32768 for all loaded hashes
Will run 4 OpenMP threads
Press 'q' or Ctrl-C to abort, almost any other key for status
r0cky0u          (hidden.rar)
1g 0:00:02:23 DONE (2023-06-21 10:27) 0.006986g/s 105.5p/s 105.5c/s 105.5C/s iluvyou1..lovemike
Use the "--show" option to display all of the cracked passwords reliably
Session completed.
```

Tìm thấy password r0cky0u. Tiến hành giải nén file với mật khẩu trên

Kết quả ta tìm được 1 nửa còn lại của flag : **_th3_w0rld_NHK}**

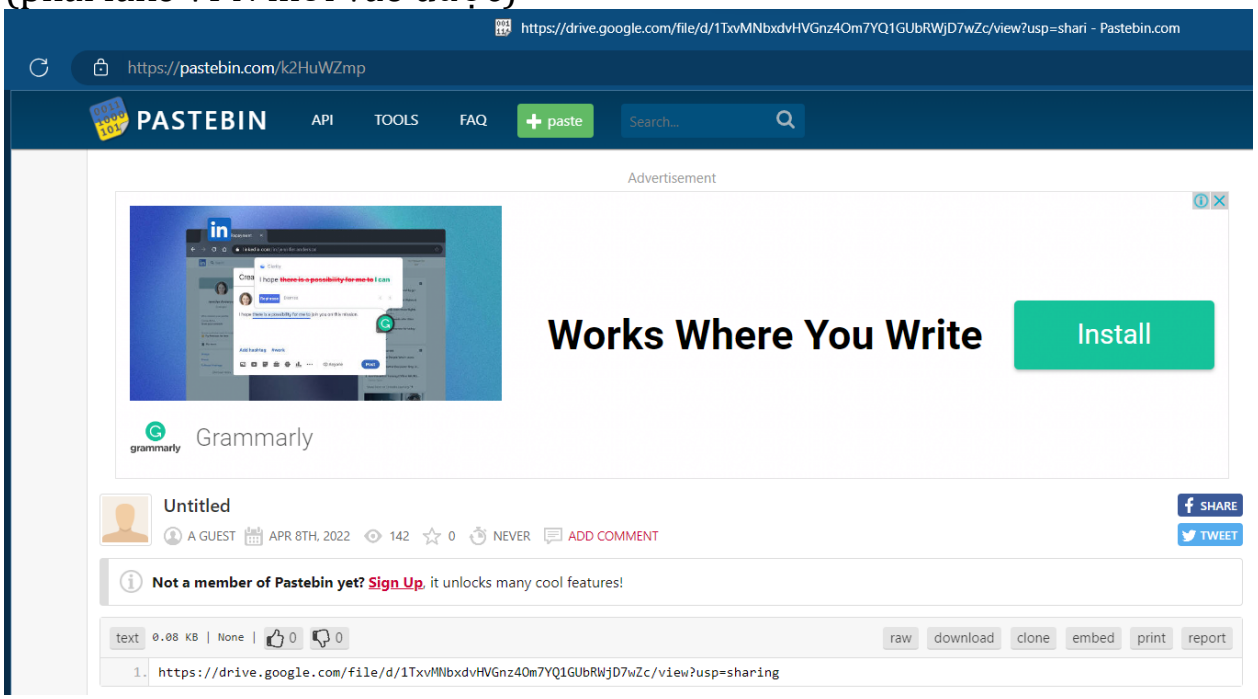
Kết hợp với một nửa tìm được ở trên ta có flag hoàn hình:
inseclab{w3lcom3_t0 _th3_w0rld_NHK}

Liệu họ có để lại những dấu vết trên trình duyệt web?.

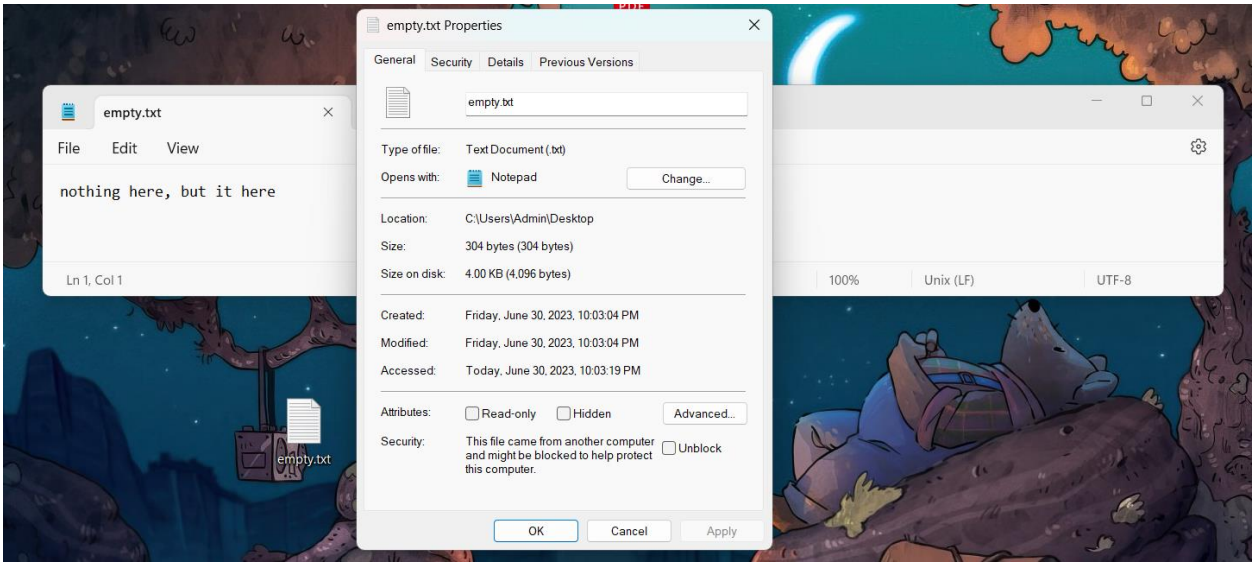
Ta tiến hành dump lịch sử duyệt web với plugins chrome history.
python2 vol.py --plugins=volatility-plugins/ -f dump.raw --profile=Win7SP1x64 chromehistory
Ngoài việc tải WinRAR ta thấy còn link:

```
21 https://inseclab.uit.edu.vn/bai-bao-ngh ... eu-hoinghi-khoa-hoc-quoc-te-nics-2021/ The UIT Information Security Laboratory
 N/A
20 https://inseclab.uit.edu.vn/                                                      The UIT Information Security Laboratory
 N/A
17 https://mh-nexus.de/en/hxd/                                                       HxD - Freeware Hex Editor and Disk Editor | mh-nexus
 N/A
15 https://github.com/goliate/hidden-tear/ ... -tear/bin/Debug/hidden-tear.vshost.exe hidden-tear/hidden-tear.vshost.exe at master · goliate/hidden-tear · GitHub
N/A
14 https://github.com/goliate/hidden-tear/ ... ster/hidden-tear/hidden-tear/bin/Debug hidden-tear/hidden-tear/hidden-tear/bin ... aster · goliate/hidden-tear · GitHu
N/A
13 https://github.com/goliate/hidden-tear/ ... ter/hidden-tear/hidden-tear/Properties hidden-tear/hidden-tear/hidden-tear/Pro ... aster · goliate/hidden-tear · GitHu
N/A
12 https://github.com/goliate/hidden-tear/tree/master/hidden-tear/hidden-tear       hidden-tear/hidden-tear/hidden-tear at master · goliate/hidden-tear · GitHub
N/A
11 https://github.com/goliate/hidden-tear/tree/master/hidden-tear                   hidden-tear/hidden-tear/hidden-tear at master · goliate/hidden-tear · GitHub
N/A
10 https://github.com/goliate/hidden-tear                                           GitHub - goliate/hidden-tear: ransomware open-sources
 N/A
 8 https://pastebin.com/k2HuWZmp                                                    https://drive.google.com/file/d/1TxvMNb ... RWjD7wZc/view?usp=shari - Pastebin.
 N/A
 3 https://www.win-rar.com/download.html?&L=0                                       WinRAR download free and support: WinRAR Download Latest Version
 N/A
 2 https://www.win-rar.com/download.html                                            WinRAR download free and support: WinRAR Download Latest Version
 N/A
```

Sau đó Truy cập vào đường dẫn **https://pastebin.com/k2HuWZmp**
(phải fake VPN mới vào được)



Tại đây PASTEBIN lưu một link khác. Truy cập và tải file empty.txt



Dù nội dung file này rất ngắn nhưng dung lượng lại không khớp, tận 304 bytes

Ta bỏ vào tool HxD để xem file raw có flag ẩn gì hay không.

empty.txt

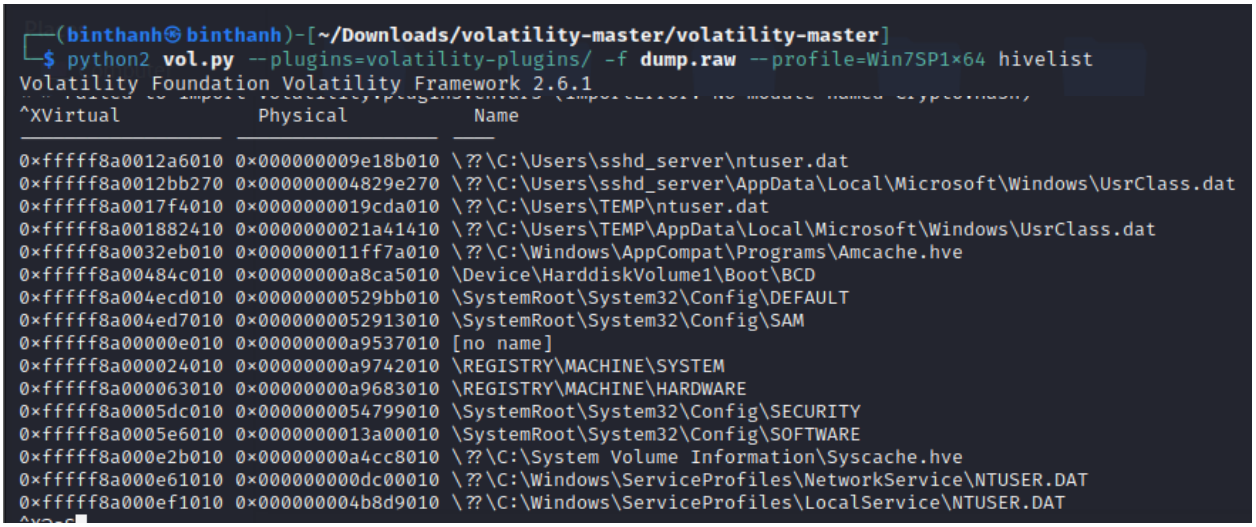
Offset (h)	00	01	02	03	04	05	06	07	08	09	0A	0B	0C	0D	0E	0F	Decoded text
00000000	6E	6F	74	68	69	6E	67	20	68	65	72	65	2C	20	62	75	nothing here, bu
00000010	74	20	69	74	20	68	65	72	65	09	20	20	20	20	09	20	t it here. .
00000020	09	20	20	09	09	20	20	20	09	20	20	20	20	20	20	0A	. .. . .
00000030	20	20	20	20	20	20	09	20	20	20	20	09	20	20	20	20	. .
00000040	20	20	20	09	20	20	09	20	09	20	09	20	20	20	09	20	. . . . .
00000050	09	20	20	20	20	20	20	20	09	20	0A	20	20	20	20	09	. . . .
00000060	09	09	20	20	09	09	20	20	20	09	20	20	20	20	20	20	.. .. .
00000070	20	09	20	20	20	20	20	09	20	20	20	20	20	20	20	09	. . .
00000080	20	20	20	20	20	20	20	0A	20	20	20	20	09	20	20	20	. .
00000090	20	20	09	20	09	20	20	09	20	09	20	20	20	09	20	20	. . . . .
000000A0	20	20	09	20	20	20	20	20	09	20	20	20	20	20	20	20	. .
000000B0	09	20	20	20	20	20	20	20	0A	09	09	20	20	20	20	09	. ... .
000000C0	20	20	09	20	20	20	20	20	09	20	20	20	20	09	20	20	. . .
000000D0	09	20	20	20	20	20	09	20	20	20	20	20	09	20	20	20	. . .
000000E0	20	20	20	20	0A	20	20	20	20	20	20	20	09	20	20	20	. .
000000F0	20	09	20	20	09	20	09	20	20	20	20	20	20	20	09	20	. . . .
00000100	09	20	20	20	20	20	09	20	20	20	20	09	20	20	20	20	. . .
00000110	20	09	20	20	20	0A	20	20	20	20	20	09	20	20	20	20	. . .
00000120	09	20	20	20	09	20	20	20	20	20	20	20	09	20	20	0A	. . . .

Các ký tự "không đọc được" (dấu chấm) được phân cách khá lạ, để ý kỹ thì đoạn sau chỉ có các byte như 09(tab) → parse thành ký tự ".", 20(space) → khoảng trắng, 0A(new line – xuống dòng) → ký tự "."
Dựa vào gợi ý và tìm kieemss thì ta kiếm được một tool stegsnow

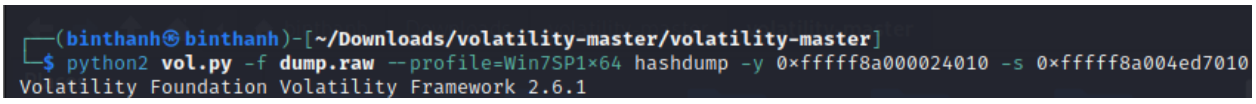
Sau đó em chạy lệnh stegsnow và thu được flag là **inseclab{y0u_c4n_s33_fl4g}**

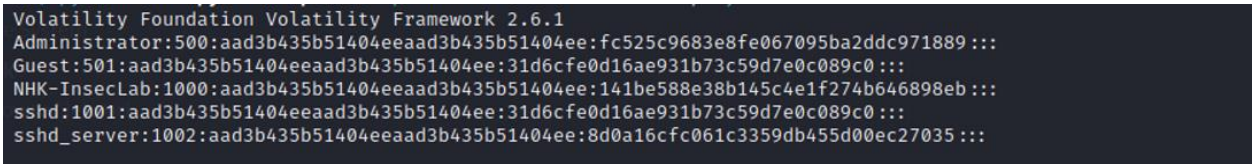
Và hình như kẻ xâm nhập bằng một cách nào đó đã lấy được password laptop của NHK. Hãy tìm password đó.

Lấy mật khẩu của laptop thì chúng ta có thể mình crack NTML hash của user thôi. Xem thông tin registry bằng hivelist:
python2 vol.py --plugins=volatility-plugins/ -f dump.raw --profile=Win7SP1x64 hivelist



Trích xuất hash bằng hashdump tại địa chỉ ảo từ 0xfffff8a000024010 (\REGISTRY\MACHINE\SYSTEM) đến 0xfffff8a004ed7010 (\SystemRoot\System32\Config\SAM):
python2 vol.py -f dump.raw --profile=Win7SP1x64 hashdump -y 0xfffff8a000024010 -s 0xfffff8a004ed7010





Kết quả ta có được tài khoản NHK-InsecLab:1000:aad3b435b51404eeaad3b435b51404ee:141be588e38b145c4e1f274b646898eb
Thử giải mã bằng các công cụ phổ biến đều không cho ra kết quả khả quan

Sau khi tham khảo các gợi ý thì ta thử dùng plugin là lsadump để dump ra password hoặc LSA secret key, ...

```
└─$ python2 vol.py -f dump.raw --profile=Win7SP1x64 lsadump
Volatility Foundation Volatility Framework 2.6.1
NL$KM
0x00000000  40 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00   @...............
0x00000010  ef 8e 01 77 ad a5 85 29 da 7c 46 c4 d1 5b a7 d4   ...w...).|F..[..
0x00000020  10 38 2d d7 b5 84 7d 93 45 5d 7b e7 28 5f e9 c1   .8-...}.E]{.(_..
0x00000030  fe be 9e 6a 42 d8 a5 6b 47 99 30 67 fc a7 5c 6c   ...jB..kG.0g..\l
0x00000040  49 ea 4c 1e 2b 89 21 56 a2 33 01 bd e6 71 fa 4d   I.L.+.!V.3...q.M
0x00000050  90 36 4c e1 5f a5 29 5a 13 12 08 90 4d 7c 15 67   .6L._.)Z....M|.g

DefaultPassword
0x00000000  12 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00   ................
0x00000010  50 00 61 00 73 00 73 00 77 00 30 00 72 00 64 00   P.a.s.s.w.0.r.d.
0x00000020  21 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00   !...............

_SC_OpenSSHd
0x00000000  14 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00   ................
0x00000010  44 00 40 00 72 00 6a 00 33 00 33 00 6c 00 31 00   D.@.r.j.3.3.l.1.
0x00000020  6e 00 67 00 00 00 00 00 00 00 00 00 00 00 00 00   n.g.............

DPAPI_SYSTEM
0x00000000  2c 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00   ,...............
0x00000010  01 00 00 00 4a b5 78 3e 9b 1a 62 d6 52 08 75 86   ....J.x>..b.R.u.
0x00000020  13 a2 3b 36 3c 96 ad 6e 74 1e 31 1d bf e1 89 85   ..;6<..nt.1.....
0x00000030  49 ac 51 cf ca 28 97 2d 8d c6 a4 b6 00 00 00 00   I.Q..(.-........
```

Tìm được password nhưng chưa xác định nhưng chưa biết của user nào nên ta tiếp tục sử dụng tool Mimikatz giúp lấy được password, một trong những cách để nó retrieve là tiến trình lsass.exe phải tồn tại trong file dump. Kiểm tra bằng pslist thì thấy có tiến trình này:

```
Volatility Foundation Volatility Framework 2.6.1
Offset(V)          Name                    PID   PPID   Thds     Hnds   Sess  Wow64 Start                          Exit
------------------ -------------------- ------ ------ ------ -------- ------ ------ ------------------------------ ------------------------------
0xfffffa8003c71b10 System                    4      0     91      546 ------      0 2022-04-08 17:44:21 UTC+0000
0xfffffa8005334620 smss.exe                264      4      2       29 ------      0 2022-04-08 17:44:21 UTC+0000
0xfffffa800584d060 csrss.exe               340    332      9      502      0      0 2022-04-08 17:44:22 UTC+0000
0xfffffa800cdfc570 wininit.exe             392    332      3       76      0      0 2022-04-08 17:44:22 UTC+0000
0xfffffa800bdfa880 csrss.exe               404    384     16      279      1      0 2022-04-08 17:44:22 UTC+0000
0xfffffa8005a1cb10 services.exe            456    392      7      223      0      0 2022-04-08 17:44:22 UTC+0000
0xfffffa8005a276f0 lsass.exe               464    392      7      598      0      0 2022-04-08 17:44:22 UTC+0000
0xfffffa8005a1f750 lsm.exe                 472    392      9      157      0      0 2022-04-08 17:44:22 UTC+0000
0xfffffa8005a248f0 winlogon.exe            496    384      3      110      1      0 2022-04-08 17:44:22 UTC+0000
```

Tiếp theo tiến hành tải plugins tại [community/FrancescoPicasso at master · volatilityfoundation/community · GitHub](#) và chúng ta cũng tải thêm python2-7 construct với lệnh **pip2 install construct==2.5.5-reupload** để chạy plugins.

```
└─$ python2 vol.py --plugins=/home/xuan/Documents/volati
Volatility Foundation Volatility Framework 2.6.1
Module   User             Domain           Password
wdigest  NHK-InsecLab     IEWIN7           AntiNHK
wdigest  sshd_server      IEWIN7           D@rj33ling
wdigest  IEWIN7$          WORKGROUP
```

Từ kết quả trên ta có flag **inseclab{AntiNHK}**

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

YÊU CẦU CHUNG

- Sinh viên tìm hiểu và thực hiện bài tập theo yêu cầu, 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]-ExeX_GroupY. (trong đó X là Thứ tự Bài tập, Y là mã số thứ tự nhóm trong danh sách mà GV phụ trách công bố).

  *Ví dụ: [*NT101.K11.ANTT*]-Exe01_Group03.*
- 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 nộp.
- Nộp file báo cáo trên theo thời gian đã thống nhất tại courses.uit.edu.vn.

Đánh giá:

- Hoàn thành tốt yêu cầu được giao.
- Có nội dung mở rộng, ứng dụng.

Bài sao chép, trễ, … sẽ được xử lý tùy mức độ vi phạm.

HẾT