# BÁO CÁO THỰC HÀNH

## Môn học: Pháp chứng kỹ thuật số

## Lab 1: Memory Forensic

*GVHD: Đoàn Minh Trung*

1. **THÔNG TIN CHUNG:**

*(Liệt kê tất cả các thành viên trong nhóm)*

Lớp: NT334.O21.ATCL.1

| STT | Họ và tên | MSSV | Email |
|---|---|---|---|
| 1 | Nguyễn Đình Bảo Long | 21522303 | 21522303@gm.uit.edu.vn |
| 2 | Nguyễn Tấn Phát | 21522447 | 21522447@gm.uit.edu.vn |
| 3 | Đào Vĩnh Thịnh | 21522632 | 21522632@gm.uit.edu.vn |
| 4 | Ngô Minh Thiên | 21522623 | 21522623@gm.uit.edu.vn |

2. **NỘI DUNG THỰC HIỆN:**[1]

| STT | Công việc | Kết quả tự đánh giá |
|---|---|---|
| 1 | Kịch bản 1 | 100% |
| 2 | Kịch bản 2 | 100% |
| 3 | Kịch bản 3 | 100% |
| 4 | Kịch bản 4 | 100% |
| 5 | Kịch bản 5 | 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

Vì kích thước file lớn nên nhóm phải tách thành 2 file mới có thể submit lên moodle.

**a. Kịch bản 01**

Yêu cầu 1. Phân tích, đánh giá.
Đánh giá các thông tin mà nhân viên điều tra có thể lấy được trọng file dump của bộ nhớ RAM.
Dưới đây là một số thông tin mà một nhân viên điều tra có thể tìm thấy trong file dump của bộ nhớ RAM:
Dữ liệu Quá Trình (Process Data):
- Thông tin về các quá trình đang chạy, bao gồm tên, ID quá trình, và các tham số liên quan.
- Các thư mục và đường dẫn mà quá trình đang làm việc.

Thông Tin Về Bộ Nhớ (Memory Information):
- Vùng nhớ đã được sử dụng và không sử dụng.
- Các địa chỉ bộ nhớ quan trọng.
- Thông tin về các vùng nhớ được cấp phát và giải phóng.

Dữ Liệu Giao Tiếp (Communication Data):
- Các kết nối mạng đang hoạt động và thông tin liên quan đến chúng.
- Dữ liệu truyền qua các kết nối mạng.

Thông Tin Người Dùng (User Information):
- Tài khoản người dùng đang đăng nhập và quyền hạn của họ.
- Hoạt động của người dùng, chẳng hạn như các tác vụ đang thực hiện.

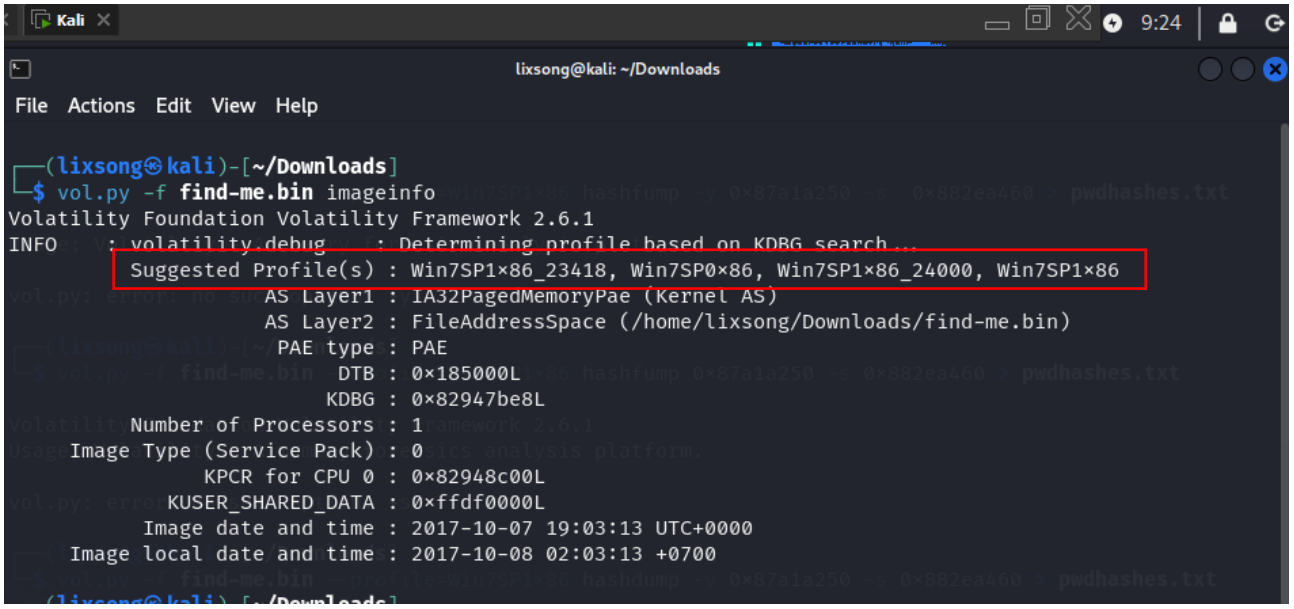
Thông Tin Hệ Thống (System Information):
- Phiên bản hệ điều hành và các bản cập nhật.
- Thông tin về phần cứng, chẳng hạn như CPU, RAM, và các thiết bị lưu trữ.

Dữ Liệu Mật Khẩu (Password Data):
- Mật khẩu hoặc các dữ liệu nhạy cảm khác nếu chúng được lưu trong bộ nhớ.

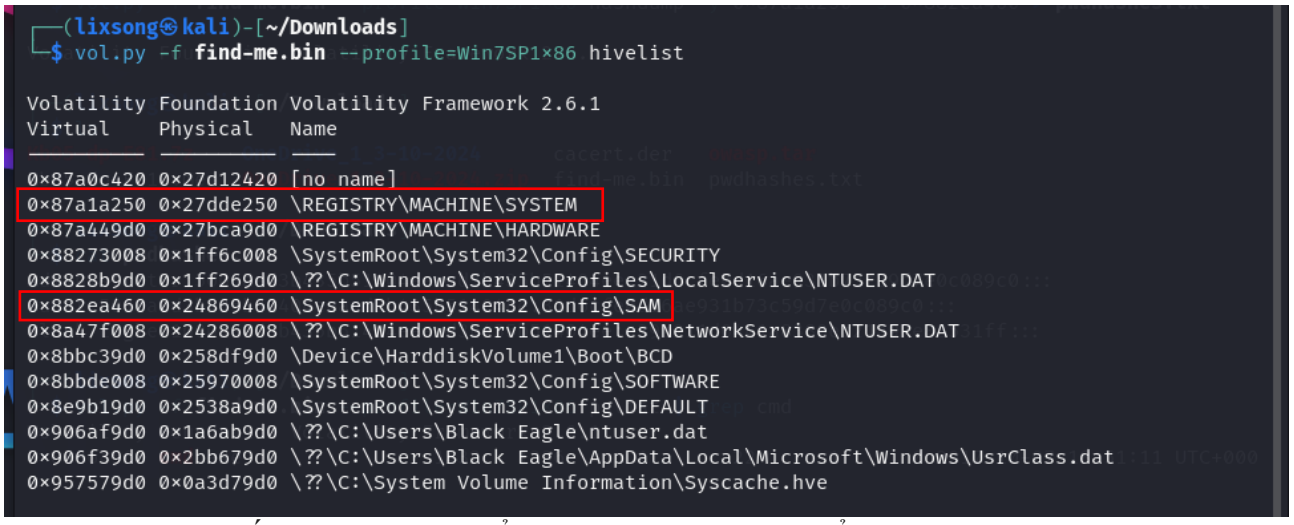
Việc này giống giám nghiệm và theo dõi hoạt động người dùng đang thực hiện thao tác trên máy tại thời điểm.

Kiểm tra profile của find-me.bin.

vol.py -f find-me.bin imageinfo




Thử nghiệm lấy thông tin mật khẩu.
Ở đây ta dùng hivelist để lấy ra trường địa chỉ bắt đầu trọng bộ nhớ của nơi lưu trữ thông tin đăng ký và quản lý về tài khoản người dùng Windows.
vol.py -f find-me.bin --profile=Win7SP1x86 hivelist




Sau đó ta trích xuất mã băm mật khẩu vào một tập tin text để tiện quan sát
vol.py -f find-me.bin --profile=Win7SP1x86 hashdump -y 0x87a1a250 -s 0x882ea460 > pwdhashes.txt

Mật khẩu đã được hash và thông tin chỉ được lưu lại ở dạng hash.
Có thể thu được thông tin gì từ việc xếm lịch sử của tiến trình cmd?
+ Việc xem được tiến trình cmd có thể cho biết được những thao tác đã thực hiện trên hệ thống.
+ Sự khác biệt giữa cmdscan và console
• Cmdscan: tìm kiếm bộ nhớ của csrss.exe và conhost.exe trên window để tìm các lệnh mà kẻ tấn công đã nhập thông qua giao diện điều khiển (cmd.exe). Đây là một trong những lệnh mạnh mẽ nhất mà bạn có thể sử dụng để có được khả năng hiển thị các hành động của kẻ tấn công trên hệ thống nạn nhân.
vol.py -f find-me.bin --profile=Win7SP1x86 cmdscan

```
┌──(lixsong㉿kali)-[~/Downloads]
└─$ vol.py -f find-me.bin --profile=Win7SP1x86 cmdscan
Volatility Foundation Volatility Framework 2.6.1
**************************************************
CommandProcess: conhost.exe Pid: 2284
CommandHistory: 0x200338 Application: cmd.exe Flags: Allocated, Reset
CommandCount: 2 LastAdded: 1 LastDisplayed: 1
FirstCommand: 0 CommandCountMax: 50
ProcessHandle: 0x5c
Cmd #0 @ 0x1fdb30: cd Desktop
Cmd #1 @ 0x204570: sdelete.exe -p 3 -s Th1s_is_Fl4g_f0r_100.pdf
Cmd #8 @ 0x390039: ???
Cmd #12 @ 0x2d0039: ??????????????????
Cmd #13 @ 0x390038: ???
Cmd #17 @ 0x2d0037: ??????????????????
Cmd #36 @ 0x1d00c4: ? ????
Cmd #37 @ 0x1fcee0: ?????
**************************************************
CommandProcess: conhost.exe Pid: 3444
CommandHistory: 0x2b0360 Application: DumpIt.exe Flags: Allocated
CommandCount: 0 LastAdded: -1 LastDisplayed: -1
FirstCommand: 0 CommandCountMax: 50
ProcessHandle: 0x5c
Cmd #36 @ 0x2800c4: *?+?(???(
Cmd #37 @ 0x2acf08: +?(????
```

• Console:Tương tự như cmdscan, plugin bảng điều khiển tìm các lệnh mà kẻ tấn công đã nhập vào cmd.exe hoặc thực thi thông qua cửa hậu. Tuy nhiên, thay vì quét COMMAND_HISTORY, plugin này sẽ quét CONSOLE_INFORMATION. Ưu điểm chính của plugin này là nó không chỉ in các lệnh mà kẻ tấn công đã nhập mà còn thu thập toàn bộ bộ đệm màn hình (đầu vào và đầu ra).

vol.py -f find-me.bin --profile=Win7SP1x86 consoles

```
┌──(lixsong㉿kali)-[~/Downloads]
└─$ vol.py -f find-me.bin --profile=Win7SP1x86 consoles
Volatility Foundation Volatility Framework 2.6.1
**************************************************
ConsoleProcess: conhost.exe Pid: 2284
Console: 0x1281c0 CommandHistorySize: 50
HistoryBufferCount: 2 HistoryBufferMax: 4
OriginalTitle: %SystemRoot%\system32\cmd.exe
Title: C:\Windows\system32\cmd.exe
AttachedProcess: cmd.exe Pid: 1432 Handle: 0x5c
----
CommandHistory: 0x200510 Application: sdelete.exe Flags:
CommandCount: 0 LastAdded: -1 LastDisplayed: -1
FirstCommand: 0 CommandCountMax: 50
ProcessHandle: 0x0
----
CommandHistory: 0x200338 Application: cmd.exe Flags: Allocated, Reset
CommandCount: 2 LastAdded: 1 LastDisplayed: 1
FirstCommand: 0 CommandCountMax: 50
ProcessHandle: 0x5c
Cmd #0 at 0x1fdb30: cd Desktop
Cmd #1 at 0x204570: sdelete.exe -p 3 -s Th1s_is_Fl4g_f0r_100.pdf
----
Screen 0x1e6198 X:80 Y:300
Dump:
Microsoft Windows [Version 6.1.7600]
Copyright (c) 2009 Microsoft Corporation.  All rights reserved.

C:\Users\Black Eagle>cd Desktop

C:\Users\Black Eagle\Desktop>sdelete.exe -p 3 -s Th1s_is_Fl4g_f0r_100.pdf

SDelete v2.0 - Secure file delete
Copyright (C) 1999-2016 Mark Russinovich
Sysinternals - www.sysinternals.com

SDelete is set for 3 passes.
Th1s_is_Fl4g_f0r_100.pdf ... deleted.

Files deleted: 1

C:\Users\Black Eagle\Desktop>sdelete.exe -p 3 -s Th1s_is_Fl4g_f0r_100.pdf

SDelete v2.0 - Secure file delete
Copyright (C) 1999-2016 Mark Russinovich
Sysinternals - www.sysinternals.com

SDelete is set for 3 passes.
Th1s_is_Fl4g_f0r_100.pdf ... deleted.

Files deleted: 1
```

```
C:\Users\Black Eagle\Desktop>
*********************************************
ConsoleProcess: conhost.exe Pid: 3444
Console: 0x1281c0 CommandHistorySize: 50
HistoryBufferCount: 1 HistoryBufferMax: 4
OriginalTitle: C:\Users\Black Eagle\Desktop\DumpIt.exe
Title: C:\Users\Black Eagle\Desktop\DumpIt.exe
AttachedProcess: DumpIt.exe Pid: 1720 Handle: 0x5c
---
CommandHistory: 0x2b0360 Application: DumpIt.exe Flags: Allocated
CommandCount: 0 LastAdded: -1 LastDisplayed: -1
FirstCommand: 0 CommandCountMax: 50
ProcessHandle: 0x5c
---
Screen 0x2961d0 X:80 Y:300
Dump:
  DumpIt - v1.3.2.20110401 - One click memory memory dumper
  Copyright (c) 2007 - 2011, Matthieu Suiche <http://www.msuiche.net>
  Copyright (c) 2010 - 2011, MoonSols <http://www.moonsols.com>

    Address space size:     1073741824 bytes (    1024 Mb)
    Free space size:        6739030016 bytes (    6426 Mb)

    * Destination = \??\C:\Users\Black Eagle\Desktop\WIN-Q64ES1E265Q-20171007-19
0311.raw

    --> Are you sure you want to continue? [y/n] y
    + Processing...
```

Xem thông tin của các tiến trình: iexplore.exe, gpg-agent.exe.

Đầu tiên ta liệt kê thông tin các process đang hoạt động để lấy PID của 2 tiến trình

vol.py -f find-me.bin --profile=Win7SP1x86 pstree | grep "iexplore.exe\|gpg.agent.exe"

```
┌──(lixsong㉿kali)-[~/Downloads]
└─$ vol.py -f find-me.bin --profile=Win7SP1x86 pstree | grep "iexplore.exe\|gpg.agent.exe"
Volatility Foundation Volatility Framework 2.6.1
. 0x849ad030:iexplore.exe                      2864   1336     17    638 2017-10-07 18:55:53 UTC+
0000
.. 0x84cb7558:iexplore.exe                     4064   2864     19    617 2017-10-07 18:56:02 UTC+
0000
.. 0x8496e7b0:iexplore.exe                     3704   2864     22    675 2017-10-07 18:55:53 UTC+
0000
 0x842d15d0:gpg-agent.exe                      3576   3556      3     79 2017-10-07 18:45:41 UTC+
0000
```

Xem thông tin tiến trình tại PID 2864

vol.py -f find-me.bin --profile=Win7SP1x86 cmdline -p 2864

```
┌──(lixsong㉿kali)-[~/Downloads]
└─$ vol.py -f find-me.bin --profile=Win7SP1x86 cmdline -p 2864
Volatility Foundation Volatility Framework 2.6.1
**************************************************************************
iexplore.exe pid:   2864
Command line : "C:\Program Files\Internet Explorer\iexplore.exe"
```

Dump tiến trình có PID 2864 ra

vol.py -f find-me.bin --profile=Win7SP1x86 memdump --dump-dir=./ -p 2864

```
┌──(lixsong㉿kali)-[~/Downloads]
└─$ vol.py -f find-me.bin --profile=Win7SP1x86 memdump --dump-dir=./ -p 2864
Volatility Foundation Volatility Framework 2.6.1
************************************************************************
Writing iexplore.exe [  2864] to 2864.dmp
```

Thử tìm kiếm thông tin trên file 2864.dmp

```
┌──(lixsong㉿kali)-[~/Downloads]
└─$ strings ./2864.dmp | grep "Flag"
GetTraceEnableFlags
WerSetFlags
EditFlags
GlobalFlags
EtwGetTraceEnableFlags
GetTraceEnableFlags
EtwGetTraceEnableFlags
EtwGetTraceEnableFlags
GetTraceEnableFlags
EtwGetTraceEnableFlags
DebugFlags
EtwGetTraceEnableFlags
GetTraceEnableFlags
WerpGetReportFlags
WerpSetReportFlags
EtwGetTraceEnableFlags
WerGetFlags
ProxyFlags
EtwGetTraceEnableFlags
$RxCscFlags$
EtwGetTraceEnableFlags
EtwGetTraceEnableFlags
EtwGetTraceEnableFlags
RasAddNotification called, hconn= %d, hevent= 0x%x, dwfFlags= 0x%x, ProcessId= %d
EtwGetTraceEnableFlags
EtwGetTraceEnableFlags
EtwGetTraceEnableFlags
EtwGetTraceEnableFlags
GetTraceEnableFlags
ImageList_GetFlags
ImageList_SetFlags
EtwGetTraceEnableFlags
GlobalFlags
EtwGetTraceEnableFlags
EtwGetTraceEnableFlags
EtwGetTraceEnableFlags
SeciAllocateAndSetCallFlags
SSPICLI.SeciAllocateAndSetCallFlags
EtwGetTraceEnableFlags
SeciAllocateAndSetCallFlags
SdbFreeFlagInfo
SdbGetEntryFlags
SdbQueryFlagInfo
SdbQueryFlagMask
SdbSetEntryFlags
ShimInfo(FlagName(%S))
EtwGetTraceEnableFlags
CryptSIPGetRegWorkingFlags
```

Xem thông tin tiến trình tại PID 3576

vol.py -f find-me.bin --profile=Win7SP1x86 cmdline -p 3576

```
┌──(lixsong㉿kali)-[~/Downloads]
└─$ vol.py -f find-me.bin --profile=Win7SP1x86 cmdline -p 3576
Volatility Foundation Volatility Framework 2.6.1
************************************************************************
gpg-agent.exe pid:   3576
Command line : "C:\Program Files\GnuPG\bin\gpg-agent.exe" --homedir "C:\Users\Black Eagle\AppData\Roami
ng\gnupg" --use-standard-socket --daemon
```

Dump tiến trình có PID 3576 ra

vol.py -f find-me.bin --profile=Win7SP1x86 memdump --dump-dir=./ -p 3576

```
┌──(lixsong㉿kali)-[~/Downloads]
└─$ vol.py -f find-me.bin --profile=Win7SP1x86 memdump --dump-dir=./ -p 3576
Volatility Foundation Volatility Framework 2.6.1
************************************************************************
Writing gpg-agent.exe [  3576] to 3576.dmp
```

Thử tìm kiếm thông tin trên file 3576.dmp

## b. Kịch bản 02

Đầu tiên ta dùng imageinfo để xem thông tin profile của file dump.

vol.py -f WIN-LEVQF1CLMR1-20181126-091622.raw imageinfo

```
lixsong@kali: ~/Downloads
File  Actions  Edit  View  Help

┌──(lixsong㉿kali)-[~/Downloads]
└─$ vol.py -f WIN-LEVQF1CLMR1-20181126-091622.raw imageinfo
Volatility Foundation Volatility Framework 2.6.1
INFO    : volatility.debug    : Determining profile based on KDBG search...
          Suggested Profile(s) : Win7SP1x64, Win7SP0x64, Win2008R2SP0x64, Win2008R2SP1x64_24000, Win200
8R2SP1x64_23418, Win2008R2SP1x64, Win7SP1x64_24000, Win7SP1x64_23418
                     AS Layer1 : WindowsAMD64PagedMemory (Kernel AS)
                     AS Layer2 : FileAddressSpace (/home/lixsong/Downloads/WIN-LEVQF1CLMR1-20181126-091
622.raw)
                      PAE type : No PAE
                           DTB : 0x187000L
                          KDBG : 0xf80002bfe0a0L
          Number of Processors : 2
     Image Type (Service Pack) : 1
                KPCR for CPU 0 : 0xfffff80002bffd00L
                KPCR for CPU 1 : 0xfffff880009ef000L
             KUSER_SHARED_DATA : 0xfffff78000000000L
           Image date and time : 2018-11-26 09:16:31 UTC+0000
     Image local date and time : 2018-11-26 16:16:31 +0700
```

Tiếp theo dùng pslist để xem các tiến trình đang chạy

vol.py -f WIN-LEVQF1CLMR1-20181126-091622.raw --profile=Win7SP1x64 pslist


Dùng hivelist để tìm thông tin tài khoản người dùng trên máy đối tượng

vol.py -f WIN-LEVQF1CLMR1-20181126-091622.raw --profile=Win7SP1x64 hivelist

```
┌──(lixsong㉿kali)-[~/Downloads]
└─$ vol.py -f WIN-LEVQF1CLMR1-20181126-091622.raw --profile=Win7SP1x64 hivelist
Volatility Foundation Volatility Framework 2.6.1
Virtual            Physical           Name
------------------ ------------------ ----
0xfffff8a00000f010 0x000000002d202010 [no name]
0xfffff8a000024010 0x000000002d38d010 \REGISTRY\MACHINE\SYSTEM
0xfffff8a0000571b0 0x000000002d6401b0 \REGISTRY\MACHINE\HARDWARE
0xfffff8a0004c8410 0x000000001ed2c410 \Device\HarddiskVolume1\Boot\BCD
0xfffff8a0014e1010 0x000000001df37010 \SystemRoot\System32\Config\SOFTWARE
0xfffff8a001722010 0x000000001a6c8010 \??\C:\Windows\ServiceProfiles\LocalService\NTUSER.DAT
0xfffff8a00172e010 0x000000002086f010 \SystemRoot\System32\Config\SAM
0xfffff8a001858410 0x0000000076314410 \??\C:\Windows\ServiceProfiles\NetworkService\NTUSER.DAT
0xfffff8a001c1d010 0x0000000011b60010 \??\C:\Users\FL\ntuser.dat
0xfffff8a001c46010 0x0000000011760010 \??\C:\Users\FL\AppData\Local\Microsoft\Windows\UsrClass.dat
0xfffff8a002215010 0x000000008e58010 \??\C:\System Volume Information\Syscache.hve
0xfffff8a005f30240 0x000000001cd2240 \SystemRoot\System32\Config\DEFAULT
0xfffff8a005fc7010 0x000000000353c010 \SystemRoot\System32\Config\SECURITY
```

vol.py -f WIN-LEVQF1CLMR1-20181126-091622.raw --profile=Win7SP1x64 hashdump -y 0xfffff8a000024010 -s 0xfffff8a00172e010 > BL.txt

```
┌──(lixsong㉿kali)-[~/Downloads]
└─$ vol.py -f WIN-LEVQF1CLMR1-20181126-091622.raw --profile=Win7SP1x64 hashdump -y 0xfffff8a000024010 -s 0xfffff8a00
172e010 > BL.txt
Volatility Foundation Volatility Framework 2.6.1
```

Ta trích xuất thông tin tài khoản người dùng ra file text để tiện theo dõi

```
┌──(lixsong㉿kali)-[~/Downloads]
└─$ cat BL.txt
Administrator:500:aad3b435b51404eeaad3b435b51404ee:31d6cfe0d16ae931b73c59d7e0c089c0:::
Guest:501:aad3b435b51404eeaad3b435b51404ee:31d6cfe0d16ae931b73c59d7e0c089c0:::
FL:1000:aad3b435b51404eeaad3b435b51404ee:31d6cfe0d16ae931b73c59d7e0c089c0:::
```

Xem lịch sử tiến trình cmd bằng consoles
vol.py -f WIN-LEVQF1CLMR1-20181126-091622.raw --profile=Win7SP1x64 consoles

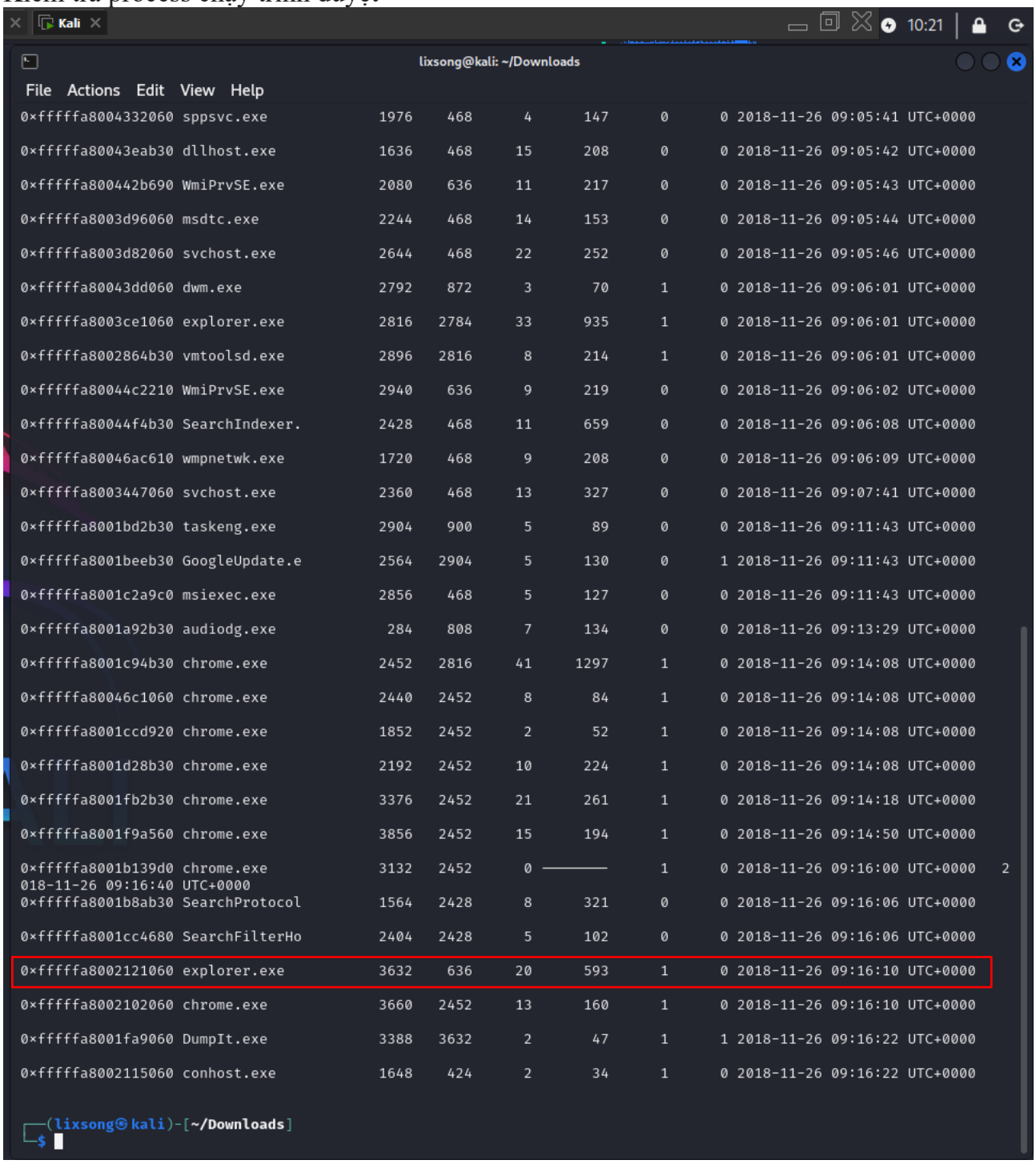
```
┌──(lixsong㉿kali)-[~/Downloads]
└─$ vol.py -f WIN-LEVQF1CLMR1-20181126-091622.raw --profile=Win7SP1x64 consoles
Volatility Foundation Volatility Framework 2.6.1
**************************************************
ConsoleProcess: conhost.exe Pid: 1648
Console: 0xffd56200 CommandHistorySize: 50
HistoryBufferCount: 1 HistoryBufferMax: 4
OriginalTitle: C:\Users\FL\Downloads\DumpIt\DumpIt.exe
Title: C:\Users\FL\Downloads\DumpIt\DumpIt.exe
AttachedProcess: DumpIt.exe Pid: 3388 Handle: 0x60
----
CommandHistory: 0x109430 Application: DumpIt.exe Flags: Allocated
CommandCount: 0 LastAdded: -1 LastDisplayed: -1
FirstCommand: 0 CommandCountMax: 50
ProcessHandle: 0x60
----
Screen 0xee400 X:80 Y:300
Dump:
  DumpIt - v1.3.2.20110401 - One click memory memory dumper
  Copyright (c) 2007 - 2011, Matthieu Suiche <http://www.msuiche.net>
  Copyright (c) 2010 - 2011, MoonSols <http://www.moonsols.com>


   Address space size:        2147483648 bytes (   2048 Mb)
   Free space size:          19385778176 bytes (  18487 Mb)

   * Destination = \??\C:\Users\FL\Downloads\DumpIt\WIN-LEVQF1CLMR1-20181126-09
1622.raw

   --> Are you sure you want to continue? [y/n] y
   + Processing...
```

Xem nội dung một tập tin text do người dùng soạn thảo sử dụng notepad.
Ở đây ta không tìm thấy file notepad
vol.py -f WIN-LEVQF1CLMR1-20181126-091622.raw --profile=Win7SP1x64 pslist | grep "notepad"

```
┌──(lixsong㉿kali)-[~/Downloads]
└─$ vol.py -f WIN-LEVQF1CLMR1-20181126-091622.raw --profile=Win7SP1x64 pslist | grep "notepad"
Volatility Foundation Volatility Framework 2.6.1
```

Xem 2 URL mà người dùng truy cập gần nhất.

Kiểm tra process chạy trình duyệt




Dump memory tại tiến trình explorer có PID 3632

vol.py -f WIN-LEVQF1CLMR1-20181126-091622.raw --profile=Win7SP1x64 memdump --dump-dir=./ -p 3632

```
(lixsong㉿kali)-[~/Downloads]
$ vol.py -f WIN-LEVQF1CLMR1-20181126-091622.raw --profile=Win7SP1x64 memdump --dump-dir=./ -p 3632
Volatility Foundation Volatility Framework 2.6.1
************************************************************************
Writing explorer.exe [  3632] to 3632.dmp
```

Kiểm tra  file 3632.dmp http
strings ./3632.dmp | grep "http"

```
┌──(lixsong㉿kali)-[~/Downloads]
└─$ strings ./3632.dmp | grep "http"
<libraryDescription xmlns="http://schemas.microsoft.com/windows/2009/library">
        <dpiAware  xmlns="http://schemas.microsoft.com/SMI/2005/WindowsSettings">true</dpiAware>
        <dpiAware  xmlns="http://schemas.microsoft.com/SMI/2005/WindowsSettings">true</dpiAware>
        <dpiAware  xmlns="http://schemas.microsoft.com/SMI/2005/WindowsSettings">true</dpiAware>
        <dpiAware  xmlns="http://schemas.microsoft.com/SMI/2005/WindowsSettings">true</dpiAware>
        <dpiAware  xmlns="http://schemas.microsoft.com/SMI/2005/WindowsSettings">true</dpiAware>
        <dpiAware  xmlns="http://schemas.microsoft.com/SMI/2005/WindowsSettings">true</dpiAware>
http://ns.adobe.com/xap/1.0/
http://ns.adobe.com/xap/1.0/
        <dpiAware  xmlns="http://schemas.microsoft.com/SMI/2005/WindowsSettings">true</dpiAware>
        <dpiAware  xmlns="http://schemas.microsoft.com/SMI/2005/WindowsSettings">true</dpiAware>
rpchttp.dll
        <dpiAware  xmlns="http://schemas.microsoft.com/SMI/2005/WindowsSettings">true</dpiAware>
        <dpiAware  xmlns="http://schemas.microsoft.com/SMI/2005/WindowsSettings">true</dpiAware>
http
https
http://www.w3.org/1999/02/22-rdf-syntax-ns#
http://purl.org/rss/1.0/
<ie8tldlistdescription xmlns="http://www.microsoft.com/schemas/ie8tldlistdescription/1.0">
The HTTP kernel driver (http.sys) reached a corrupted state and can not recover.  This means
https://chrome.google.com/webstore?hl=bnChrome
 <code>http://</code>
 <code>http://</code>
 <a href="http://example.com" target="_blank">http://example.com</a>
able-mark-http-as@0
able-mark-http-as@1
able-mark-http-as@2
able-mark-http-as@3
able-mark-http-as@4
able-mark-http-as@5
able-mark-http-as@6
mplify-https-indicator@0
mplify-https-indicator@1
mplify-https-indicator@2
mplify-https-indicator@3
mplify-https-indicator@4
mplify-https-indicator@5
mplify-https-indicator@6
d:\w7rtm\minio\http\sys\apool.c
d:\w7rtm\minio\http\sys\cache.c
d:\w7rtm\minio\http\sys\cgroup.c
d:\w7rtm\minio\http\sys\errlog.c
d:\w7rtm\minio\http\sys\fastio.c
d:\w7rtm\minio\http\sys\logutil.h
d:\w7rtm\minio\http\sys\httpconn.c
d:\w7rtm\minio\http\sys\httprcv.c
d:\w7rtm\minio\http\sys\ioctl.c
d:\w7rtm\minio\http\sys\logutil.c
d:\w7rtm\minio\http\sys\rangesupport.c
d:\w7rtm\minio\http\sys\sendresponse.c
d:\w7rtm\minio\http\sys\filecache.h
d:\w7rtm\minio\http\sys\thrdpool.c
d:\w7rtm\minio\http\sys\timeouts.c
d:\w7rtm\minio\http\sys\tl.c
d:\w7rtm\minio\http\sys\tokencache.c
```

Kéo xuống dưới để thấy 2 URL mà người dùng truy cập gần nhất

```
pcc-m1sbtx1sdnlogvboxdunknownunknownnetbus-prounknownmailsweeperipdtp-portchupacabraunknown1pulse-1cstrackathand-mmp
gauntlet-adminunknownunknownunknownunknownunknowngnuservgirlfriendunknownvofr-gatewayunknowntvpmwebphonenetspeak-isn
etspeak-csnetspeak-acdnetspeak-cpssnapenetiooptocontrolunknownunknownprosiakwnn6wnn4_Cnwnn4_Krwnn4_Twhpnpdvocaltec-w
confaws-brfbrf-gwwhackjobunknownmed-ltpmed-fsp-rxmed-fsp-txmed-suppmed-ovwmed-cimed-net-svcfilespherevista-4glpower-
brokerpower-brokerpower-brokerintel_rcibinkpflashfilerproactivatesnipicl-twobase1icl-twobase2icl-twobase3icl-twobase
4icl-twobase5icl-twobase6icl-twobase7icl-twobase8icl-twobase9icl-twobase10telalertaol-im-alternate-(safe)vocaltec-ho
swebcam32niobserverniprobequakewnn6-dsezproxyezmeetingk3software-svrk3software-cligserverflexlm0flexlm1flexlm2flexlm
3flexlm4flexlm5flexlm6flexlm7flexlm8flexlm9flexlm10mongodbimagepumpaspkopek-httpheadTrinoo_Masterunknowntw-auth-keyt
ribesmongodbbackdoor.latinustheunexplainedpago-services1pago-services2netspherenetspherenetspheresocket23kuangEliten
etspydkxqosdtetrinetschwindlerbackdoor-zdemon2lm-mongamesmith-porthack-a-tackhack-a-tackhack-a-tackunknownunknownsym
antec-fax-smtp-serverinterceptor-firewall-adminfilenet-tmsfilenet-rpcfilenet-nchfilenet-rmifilenet-pasometimes-rpc9s
ometimes-rpc11sometimes-rpc13sometimes-rpc15sometimes-rpc17sometimes-rpc19sometimes-rpc21sometimes-rpc23sometimes-rp
c25sometimes-rpc27idmgratmtrinityv3diamondporttracerouteunknownunknownspirit2001unknownturbonote-2biggluckunknownmst
ratbizunknownunknownkastenxpipeneckaryetanotherlandesk-cbagalaxy7-datalandesk-cbaintelpdsturbonote-1unknownthe-spycs
cpcsccredircsccfirewallunknownunknownfs-qosunknowninoculancrestron-cipcrestron-ctpcandpcandrpcaerpcunknownreachoutre
achoutndm-agent-portip-provisionpmcdpmcdproxywinrouteadmintiny-personal-firewall-(remote-administration)unknowncoldf
usion-authcoldfusion-authrockwell-encapnetrangerinvision-agebassr-servermgrmbusdbbrowsedirectplaysrvrapbacnetbackdoo
r.antilamnimcontrollernimspoolernimhubnimgtwcom-bardac-dwcompaqdiagpop3proxypop3proxypop3proxypop3proxypop3proxyunkn
ownunknownsockets-de-trojeforeunknowndialpadwinshutbo2kschoolbusunknownnetraidersap-r3-instguiunknowntfidofidonetpro
wler-managernetprowler-manager2netprowler-sensortelecommandounknowndevilpcanywherebackdoor-port
http://www.usertrust.com1
1http://crl.usertrust.com/UTN-USERFirst-Object.crl05
http://ocsp.usertrust.com0
#http://crl.thawte.com/ThawtePCA.crl0
http://ocsp.thawte.com0
http://th.symcb.com/th.crl0
https://www.thawte.com/cps0/
!https://www.thawte.com/repository0W
http://th.symcd.com0&
http://th.symcb.com/th.crt0
http://www.usertrust.com1
https://d.symcb.com/cps0%
https://d.symcb.com/rpa0
http://sv.symcb.com/sv.crl0W
http://sv.symcd.com0&
http://sv.symcb.com/sv.crt0
http://s2.symcb.com0
http://www.symauth.com/cps0(
http://www.symauth.com/rpa00
http://s1.symcb.com/pca3-g5.crl0
http://www.usertrust.com1
1http://crl.usertrust.com/UTN-USERFirst-Object.crl05
http://ocsp.usertrust.com0
http://www.usertrust.com1
    <asmv3:windowsSettings xmlns="http://schemas.microsoft.com/SMI/2005/WindowsSettings">

┌──(lixsong㉿kali)-[~/Downloads]
└─$
```

### c. Kịch bản 03

Cung cấp bằng chứng xác định file được cho là file dump từ bộ nhớ máy ảo.
Xác định hệ điều hành của máy này.
vol.py -f Kb03-dp-e81.raw imageinfo

```
┌──(lixsong㉿kali)-[~/Downloads/OneDrive_1_3-10-2024]
└─$ vol.py -f Kb03-dp-e81.raw imageinfo
Volatility Foundation Volatility Framework 2.6.1
INFO    : volatility.debug    : Determining profile based on KDBG search...
          Suggested Profile(s) : Win10x64_10240_17770, Win10x64
                     AS Layer1 : SkipDuplicatesAMD64PagedMemory (Kernel AS)
                     AS Layer2 : VirtualBoxCoreDumpElf64 (Unnamed AS)
                     AS Layer3 : FileAddressSpace (/home/lixsong/Downloads/OneDrive_1_3-10-2024/Kb03-dp-e81.raw)
                      PAE type : No PAE
                           DTB : 0x1aa000L
                          KDBG : 0xf80185d1db20L
          Number of Processors : 1
     Image Type (Service Pack) : 0
                KPCR for CPU 0 : 0xfffff80185d77000L
             KUSER_SHARED_DATA : 0xffffff78000000000L
           Image date and time : 2016-04-04 16:17:53 UTC+0000
     Image local date and time : 2016-04-04 18:17:53 +0200
```

Qua hình trên ta thấy rằng file được dump từ máy ảo VirtualBox đang chạy máy ảo window10.

Kiểm tra các tiến trình đang chạy
vol.py -f Kb03-dp-e81.raw --profile=Win10x64 pslist

```
┌──(lixsong㉿kali)-[~/Downloads/OneDrive_1_3-10-2024]
└─$ vol.py -f Kb03-dp-e81.raw --profile=Win10x64 pslist
Volatility Foundation Volatility Framework 2.6.1
Offset(V)          Name                    PID   PPID   Thds     Hnds   Sess  Wow64 Start                          Exit
------------------ -------------------- ------ ------ ------ -------- ------ ------ ------------------------------ ------------------------------
0xffffe00032553780 System                    4      0    126        0 ------      0 2016-04-04 16:12:33 UTC+0000
0xffffe0003389c040 smss.exe                268      4      2        0 ------      0 2016-04-04 16:12:33 UTC+0000
0xffffe0003381b080 csrss.exe               344    336      8        0      0      0 2016-04-04 16:12:33 UTC+0000
0xffffe000325ba080 wininit.exe             404    336      1        0      0      0 2016-04-04 16:12:34 UTC+0000
0xffffe000325c7080 csrss.exe               412    396      9        0      1      0 2016-04-04 16:12:34 UTC+0000
0xffffe00033ec6080 winlogon.exe            460    396      2        0      1      0 2016-04-04 16:12:34 UTC+0000
0xffffe00033efb440 services.exe            484    404      3        0      0      0 2016-04-04 16:12:34 UTC+0000
0xffffe00033f08080 lsass.exe               492    404      6        0      0      0 2016-04-04 16:12:34 UTC+0000
0xffffe00033ec5780 svchost.exe             580    484     16        0      0      0 2016-04-04 16:12:34 UTC+0000
0xffffe00034202280 svchost.exe             612    484      9        0      0      0 2016-04-04 16:12:34 UTC+0000
0xffffe000341cb640 dwm.exe                 712    460      8        0      1      0 2016-04-04 16:12:34 UTC+0000
0xffffe00034222780 svchost.exe             796    484     45        0      0      0 2016-04-04 16:12:34 UTC+0000
0xffffe000342a7780 VBoxService.ex          828    484     10        0      0      0 2016-04-04 16:12:34 UTC+0000
0xffffe000342ad780 svchost.exe             844    484      8        0      0      0 2016-04-04 16:12:34 UTC+0000
0xffffe000342c0080 svchost.exe             852    484      6        0      0      0 2016-04-04 16:12:34 UTC+0000
0xffffe000342dd780 svchost.exe             892    484     18        0      0      0 2016-04-04 16:12:34 UTC+0000
0xffffe000342bc780 svchost.exe             980    484     17        0      0      0 2016-04-04 16:12:34 UTC+0000
0xffffe00034377780 svchost.exe             608    484     17        0      0      0 2016-04-04 16:12:34 UTC+0000
0xffffe000343e7780 spoolsv.exe            1072    484      8        0      0      0 2016-04-04 16:12:34 UTC+0000
0xffffe000343e9780 svchost.exe            1092    484     23        0      0      0 2016-04-04 16:12:35 UTC+0000
0xffffe0003442a780 rundll32.exe           1148    796      1        0      0      0 2016-04-04 16:12:35 UTC+0000
0xffffe00034494780 CompatTelRunne         1224   1148      9        0      0      0 2016-04-04 16:12:35 UTC+0000
0xffffe00034495780 svchost.exe            1276    484     10        0      0      0 2016-04-04 16:12:35 UTC+0000
0xffffe0003461d780 svchost.exe            1564    484      5        0      0      0 2016-04-04 16:12:35 UTC+0000
0xffffe000345da780 wlms.exe               1616    484      2        0      0      0 2016-04-04 16:12:35 UTC+0000
0xffffe00034623780 MsMpEng.exe            1628    484     24        0      0      0 2016-04-04 16:12:35 UTC+0000
0xffffe000343b2340 cygrunsrv.exe          1832    484      4        0      0      0 2016-04-04 16:12:35 UTC+0000
0xffffe0003479b780 cygrunsrv.exe          1976   1832      0 ------      0      0 2016-04-04 16:12:36 UTC+0000   2016-04-04 16:12:36 UTC+0000
0xffffe000347aa780 conhost.exe            2004   1976      2        0      0      0 2016-04-04 16:12:36 UTC+0000
0xffffe000347c1080 sshd.exe               2028   1976      3        0      0      0 2016-04-04 16:12:36 UTC+0000
0xffffe00033e00780 svchost.exe            1772    484      3        0      0      0 2016-04-04 16:12:37 UTC+0000
0xffffe00033f1f780 sihost.exe               92    796     10        0      1      0 2016-04-04 16:12:37 UTC+0000
0xffffe0003259b3c0 taskhostw.exe          1532    796      9        0      1      0 2016-04-04 16:12:37 UTC+0000
0xffffe000339d4340 NisSrv.exe             2272    484      6        0      0      0 2016-04-04 16:12:38 UTC+0000
0xffffe00036e8780 userinit.exe            2312    460      0 ------      1      0 2016-04-04 16:12:38 UTC+0000   2016-04-04 16:13:04 UTC+0000
0xffffe000336e3780 explorer.exe           2336   2312     31        0      1      0 2016-04-04 16:12:38 UTC+0000
0xffffe0003374f780 RuntimeBroker.         2456    580      6        0      1      0 2016-04-04 16:12:38 UTC+0000
0xffffe00033a39080 SearchIndexer.         2664    484     13        0      0      0 2016-04-04 16:12:39 UTC+0000
0xffffe00033a79780 ShellExperienc         2952    580     41        0      1      0 2016-04-04 16:12:39 UTC+0000
0xffffe00033b57780 SearchUI.exe           3144    580     38        0      1      0 2016-04-04 16:12:40 UTC+0000
0xffffe00033e1d780 DismHost.exe           3636   1224      2        0      0      0 2016-04-04 16:12:47 UTC+0000
0xffffe00034 8e9780 svchost.exe           3992    484      6        0      0      0 2016-04-04 16:12:52 UTC+0000
0xffffe000348c6780 VBoxTray.exe           3324   2336     10        0      1      0 2016-04-04 16:12:55 UTC+0000
0xffffe00034b08780 OneDrive.exe           1692   2336     10        0      1      1 2016-04-04 16:12:55 UTC+0000
0xffffe00034b0f780 mspaint.exe            4092   2336      3        0      1      0 2016-04-04 16:13:21 UTC+0000
0xffffe00034ade080 svchost.exe             628    484      1        0      1      0 2016-04-04 16:14:43 UTC+0000
0xffffe0003472b080 notepad.exe            2012   2336      1        0      1      0 2016-04-04 16:14:49 UTC+0000
0xffffe000349e4780 WmiPrvSE.exe           3032    580      6        0      0      0 2016-04-04 16:16:37 UTC+0000
0xffffe000349285c0 taskhostw.exe           332    796     10        0      1      0 2016-04-04 16:17:40 UTC+0000

┌──(lixsong㉿kali)-[~/Downloads/OneDrive_1_3-10-2024]
└─$
```

Ta thấy được tiến trình 4092 đang chạy mspaint.exe

Thực hiện dump tiến trình 4092
vol.py -f Kb03-dp-e81.raw --profile=Win10x64 memdump --dump-dir=./ -p 4092

```
┌──(lixsong㉿kali)-[~/Downloads/OneDrive_1_3-10-2024]
└─$ vol.py -f Kb03-dp-e81.raw --profile=Win10x64 memdump --dump-dir=./ -p 4092
Volatility Foundation Volatility Framework 2.6.1
************************************************************************
Writing mspaint.exe [  4092] to 4092.dmp
```

Thử tìm kiếm flag CTF trong file 4092.dmp

```
┌──(lixsong㉿kali)-[~/Downloads/OneDrive_1_3-10-2024]
└─$ strings ./4092.dmp | grep "CTF"
        MSCTFIME UI
MSCTFIME Composition
        MSCTFIME UI
MSCTFIME Composition
MSCTFIME Composition
        MSCTFIME UI
        MSCTFIME UI
        MSCTFIME UI
MSCTFIME Composition
        MSCTFIME UI
MSCTFIME Composition
        MSCTFIME UI
MSCTFIME Composition
MSCTFIME Composition
        MSCTFIME UI
MSCTFIME UI
'MSCTFIME Composition
        MSCTFIME UI
MSCTF.dll
MSCTF.dll
CMNbCTF
        MSCTFIME UI
        MSCTFIME UI
MSCTFIME Composition
        MSCTFIME UI
MSCTFIME Composition
MSCTFIME Composition
        MSCTFIME UI
        MSCTFIME UI
        MSCTFIME UI
MSCTFIME Composition
        MSCTFIME UI
MSCTFIME Composition
        MSCTFIME UI
MSCTFIME Composition
MSCTFIME Composition
        MSCTFIME UI
MSCTFIME UI
'MSCTFIME Composition
        MSCTFIME UI
MSCTFIME Composition
MSCTFIME Composition
```

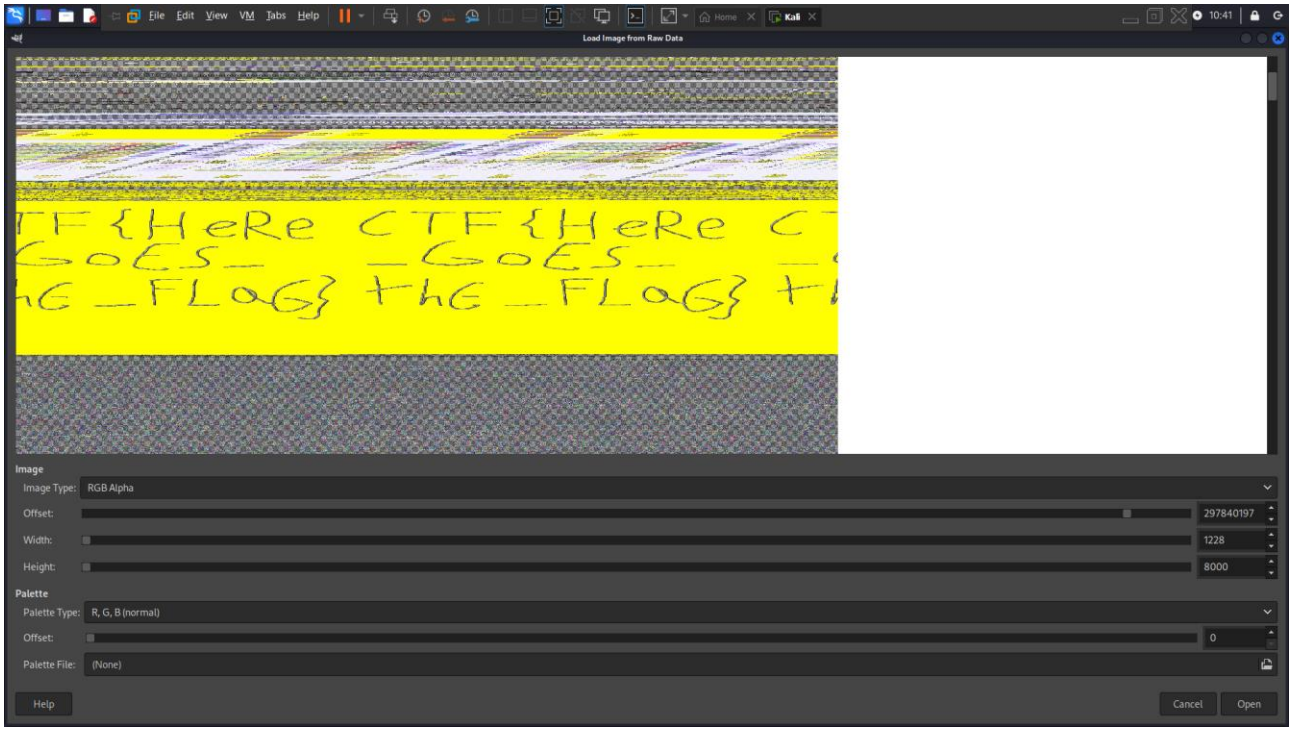
```
┌──(lixsong㉿kali)-[~/Downloads/OneDrive_1_3-10-2024]
└─$ strings ./4092.dmp | grep "Flag"
.?AV?$RuntimeClass@U?$RuntimeClassFlags@$01@WRL@Microsoft@@UIUnknown@@VNil@Details@23@V5623@V5623@V5623@V5623@V5623@V5623@@WRL@Microsoft@@
.?AV?$RuntimeClass@U?$InterfaceList@UIUnknown@@VNil@Details@WRL@Microsoft@@@Details@WRL@Microsoft@@U?$RuntimeClassFlags@$01@34@$00$0A@$0A@@Details@WRL@Microsoft@@
.?AU?$ImplementsHelper@U?$RuntimeClassFlags@$01@WRL@Microsoft@@U?$InterfaceList@UIUnknown@@VNil@Details@WRL@Microsoft@@@Details@23@$0A@$0A@@Details@WRL@Microsoft@@
.?AU?$RuntimeClassFlags@$03@WRL@Microsoft@@
dwFlags: 0x%08X, guidEvent: %ws, bstrDeviceID: %ws, callback: 0x%p
DropFlags
GetTraceEnableFlags
GlobalFlags
SetMapperFlags
EtwGetTraceEnableFlags
EtwGetTraceEnableFlags
EtwGetTraceEnableFlags
GetTraceEnableFlags
GlobalFlags
GetGadgetFlags
SetWindowResizeFlag
SetGadgetFlags
ImageList_GetFlags
ImageList_SetFlags
GlobalFlags
GdipGetImageFlags
GdipSetStringFormatFlags
SetMapperFlags
CM_Get_HW_Prof_FlagsA_ExW
CM_Set_HW_Prof_FlagsA_ExW
EtwGetTraceEnableFlags
EtwGetTraceEnableFlags
EtwGetTraceEnableFlags
EtwGetTraceEnableFlags
EtwGetTraceEnableFlags
CMP_GetServerSideDeviceInstallFlags
CM_Get_HW_Prof_FlagsA
CM_Get_HW_Prof_FlagsW
CM_Get_HW_Prof_FlagsA_ExA
CM_Get_HW_Prof_FlagsA_ExW
CM_Set_HW_Prof_FlagsA
CM_Set_HW_Prof_FlagsW
CM_Set_HW_Prof_FlagsA_ExA
CM_Set_HW_Prof_FlagsA_ExW
Global_WindowsStorage_lrFlags
Global_WindowsStorage_tlsThreadFlags
SHFileOperationWithAdditionalFlags
STORAGE_CreateStorageItemFromShellItem_FullTrustCaller_UseImplicitFlagsAndPackage
EtwGetTraceEnableFlags
WerGetFlagsWorker
WerSetFlagsWorker
GetRegistryExtensionFlags
GetThreadIOPendingFlag
GetTraceEnableFlags
NTDLL.EtwGetTraceEnableFlags
RegKrnGetTermsrvRegistryExtensionFlags
RegKrnSetTermsrvRegistryExtensionFlags
WerGetFlags
WerSetFlags
CtfImmGetTMAEFlags
CtfImmSetAppCompatFlags
ImmGetAppCompatFlags
```

Ta không tìm thấy flag nào cả.

Đổi đuôi .dmp thành .data để mở bằng gimp

```
lixsong@kali: ~/Downloads/OneDrive_1_3-10-2024
File  Actions  Edit  View  Help

┌──(lixsong㉿kali)-[~/Downloads/OneDrive_1_3-10-2024]
└─$ gimp 4092.data
gimp_device_info_set_device: trying to set GdkDevice 'VirtualPS/2 VMware VMMouse' on GimpDeviceInfo which already has a device
```

Thực hiện điều chỉnh các thông số để có thể đọc được flag




Ta có được flag là: **CTF{HeRe_GoES_thE_FLaG}**