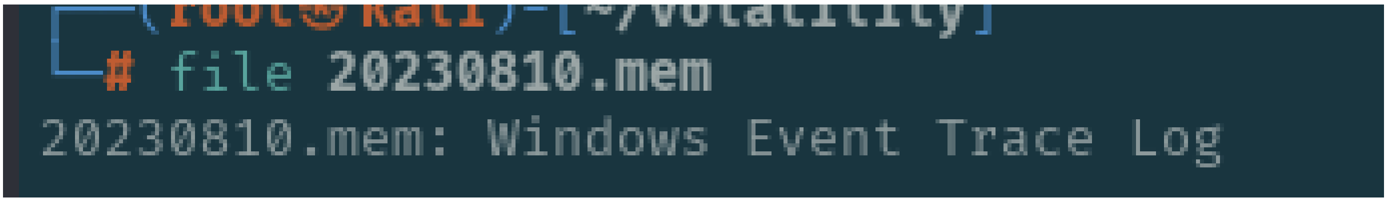
RogueOne,mem(volatility2，後面用3)

```
Sherlock Scenario
Your SIEM system generated multiple alerts in less than a minute, indicating potential C2 communication from Simon Stark's workstation. Despite Simon not noticing anything unusual, the IT team had him share screenshots of his task manager to check for any unusual processes. No suspicious processes were found, yet alerts about C2 communications persisted. The SOC manager then directed the immediate containment of the workstation and a memory dump for analysis. As a memory forensics expert, you are tasked with assisting the SOC team at Forela to investigate and resolve this urgent incident.
```

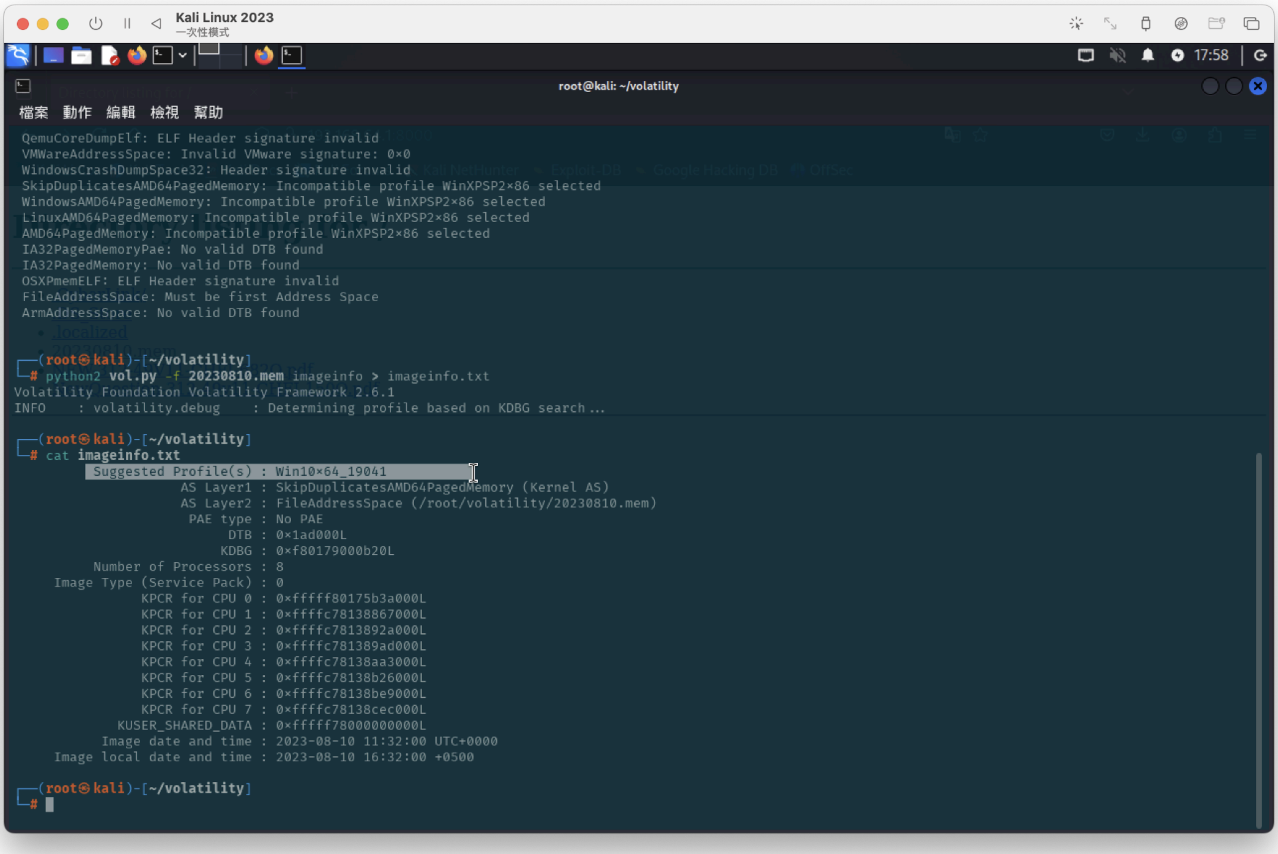
tool：使用volatility2 進行內存取證



```
  (root㉿kali)-[~/volatility]
└─# file 20230810.mem
20230810.mem: Windows Event Trace Log
```

先查看訊息

```
python2 vol.py -f 20230810.mem imageinfo
```



```
QemuCoreDumpElf: ELF Header signature invalid
VMWareAddressSpace: Invalid VMware signature: 0×0
WindowsCrashDumpSpace32: Header signature invalid
SkipDuplicatesAMD64PagedMemory: Incompatible profile WinXPSP2×86 selected
WindowsAMD64PagedMemory: Incompatible profile WinXPSP2×86 selected
LinuxAMD64PagedMemory: Incompatible profile WinXPSP2×86 selected
AMD64PagedMemory: Incompatible profile WinXPSP2×86 selected
IA32PagedMemoryPae: No valid DTB found
IA32PagedMemory: No valid DTB found
OSXPmemELF: ELF Header signature invalid
FileAddressSpace: Must be first Address Space
ArmAddressSpace: No valid DTB found

┌──(root㉿kali)-[~/volatility]
└─# python2 vol.py -f 20230810.mem imageinfo > imageinfo.txt
Volatility Foundation Volatility Framework 2.6.1
INFO    : volatility.debug    : Determining profile based on KDBG search ...

┌──(root㉿kali)-[~/volatility]
└─# cat imageinfo.txt
          Suggested Profile(s) : Win10×64_19041
                     AS Layer1 : SkipDuplicatesAMD64PagedMemory (Kernel AS)
                     AS Layer2 : FileAddressSpace (/root/volatility/20230810.mem)
                      PAE type : No PAE
                           DTB : 0×1ad000L
                          KDBG : 0×f80179000b20L
          Number of Processors : 8
     Image Type (Service Pack) : 0
                KPCR for CPU 0 : 0×fffff80175b3a000L
                KPCR for CPU 1 : 0×ffffc78138867000L
                KPCR for CPU 2 : 0×ffffc7813892a000L
                KPCR for CPU 3 : 0×ffffc781389ad000L
                KPCR for CPU 4 : 0×ffffc78138aa3000L
                KPCR for CPU 5 : 0×ffffc78138b26000L
                KPCR for CPU 6 : 0×ffffc78138be9000L
                KPCR for CPU 7 : 0×ffffc78138cec000L
             KUSER_SHARED_DATA : 0×fffff78000000000L
           Image date and time : 2023-08-10 11:32:00 UTC+0000
     Image local date and time : 2023-08-10 16:32:00 +0500

┌──(root㉿kali)-[~/volatility]
└─# 
```

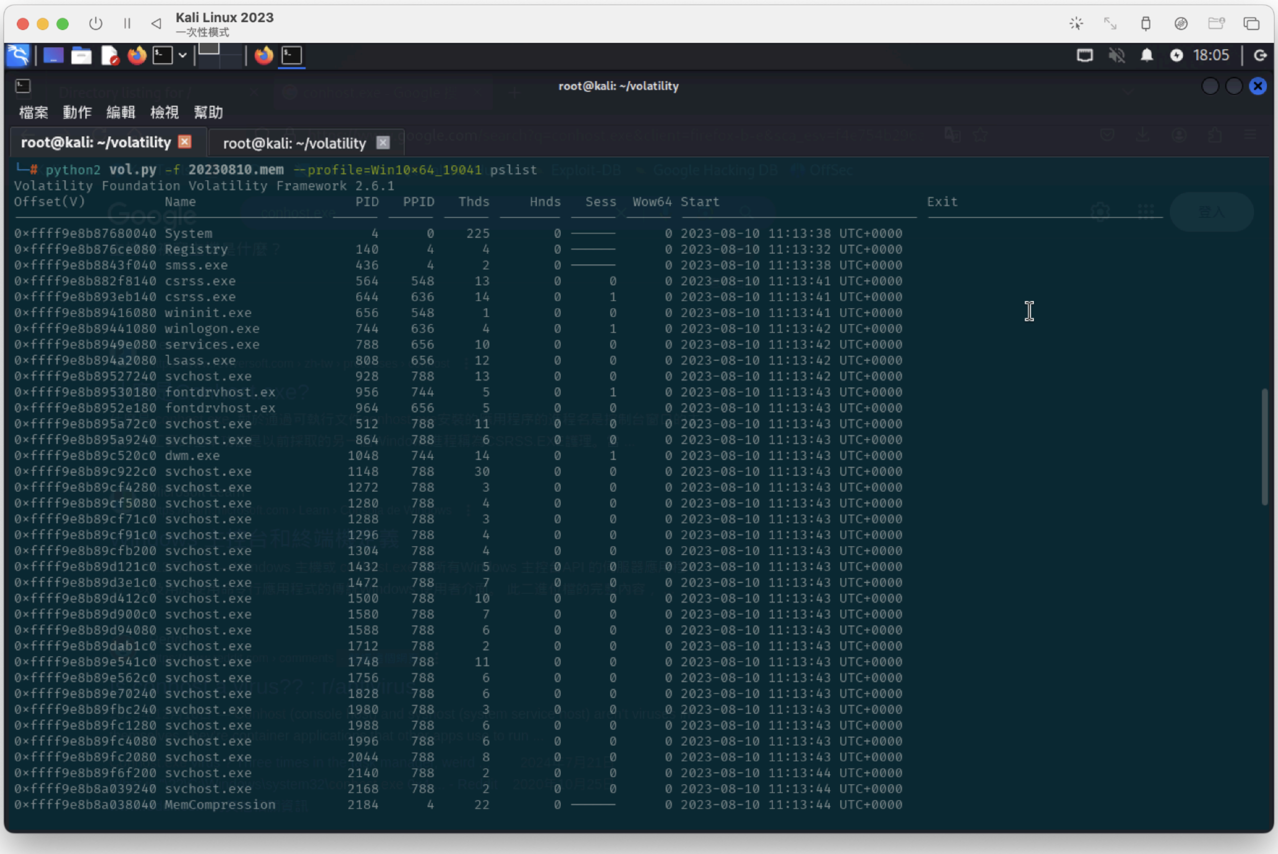
Task 1

Please identify the malicious process and confirm process id of malicious process.

檢查進程是否有惡意

```
python2 vol.py -f 20230810.mem --profile=Win10x64_19041 pslist
```

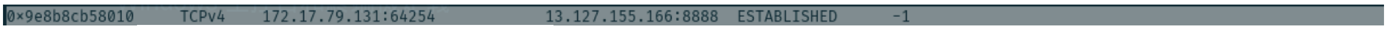
看起來都是win預設，無中毒現象



```
└─# python2 vol.py -f 20230810.mem --profile=Win10x64_19041 pslist
Volatility Foundation Volatility Framework 2.6.1
Offset(V)          Name                    PID   PPID   Thds     Hnds   Sess  Wow64 Start                          Exit
------------------ -------------------- ------ ------ ------ -------- ------ ------ ------------------------------ ------------------------------
0xffff9e8b87680040 System                    4      0    225        0 ------      0 2023-08-10 11:13:38 UTC+0000
0xffff9e8b876ce080 Registry                140      4      4        0 ------      0 2023-08-10 11:13:32 UTC+0000
0xffff9e8b8843f040 smss.exe                436      4      2        0 ------      0 2023-08-10 11:13:38 UTC+0000
0xffff9e8b882f8140 csrss.exe               564    548     13        0      0      0 2023-08-10 11:13:41 UTC+0000
0xffff9e8b893eb140 csrss.exe               644    636     14        0      1      0 2023-08-10 11:13:41 UTC+0000
0xffff9e8b89416080 wininit.exe             656    548      1        0      0      0 2023-08-10 11:13:41 UTC+0000
0xffff9e8b89441080 winlogon.exe            744    636      4        0      1      0 2023-08-10 11:13:42 UTC+0000
0xffff9e8b8949e080 services.exe            788    656     10        0      0      0 2023-08-10 11:13:42 UTC+0000
0xffff9e8b894a2080 lsass.exe               808    656     12        0      0      0 2023-08-10 11:13:42 UTC+0000
0xffff9e8b89527240 svchost.exe             928    788     13        0      0      0 2023-08-10 11:13:42 UTC+0000
0xffff9e8b89530180 fontdrvhost.ex          956    744      5        0      1      0 2023-08-10 11:13:43 UTC+0000
0xffff9e8b8952e180 fontdrvhost.ex          964    656      5        0      0      0 2023-08-10 11:13:43 UTC+0000
0xffff9e8b895a72c0 svchost.exe             512    788     11        0      0      0 2023-08-10 11:13:43 UTC+0000
0xffff9e8b895a9240 svchost.exe             864    788      6        0      0      0 2023-08-10 11:13:43 UTC+0000
0xffff9e8b89c520c0 dwm.exe                1048    744     14        0      1      0 2023-08-10 11:13:43 UTC+0000
0xffff9e8b89c922c0 svchost.exe            1148    788     30        0      0      0 2023-08-10 11:13:43 UTC+0000
0xffff9e8b89cf4280 svchost.exe            1272    788      3        0      0      0 2023-08-10 11:13:43 UTC+0000
0xffff9e8b89cf5080 svchost.exe            1280    788      4        0      0      0 2023-08-10 11:13:43 UTC+0000
0xffff9e8b89cf71c0 svchost.exe            1288    788      3        0      0      0 2023-08-10 11:13:43 UTC+0000
0xffff9e8b89cf91c0 svchost.exe            1296    788      4        0      0      0 2023-08-10 11:13:43 UTC+0000
0xffff9e8b89cfb200 svchost.exe            1304    788      4        0      0      0 2023-08-10 11:13:43 UTC+0000
0xffff9e8b89d121c0 svchost.exe            1432    788      5        0      0      0 2023-08-10 11:13:43 UTC+0000
0xffff9e8b89d3e1c0 svchost.exe            1472    788      7        0      0      0 2023-08-10 11:13:43 UTC+0000
0xffff9e8b89d412c0 svchost.exe            1500    788     10        0      0      0 2023-08-10 11:13:43 UTC+0000
0xffff9e8b89d900c0 svchost.exe            1580    788      7        0      0      0 2023-08-10 11:13:43 UTC+0000
0xffff9e8b89d94080 svchost.exe            1588    788      6        0      0      0 2023-08-10 11:13:43 UTC+0000
0xffff9e8b89dab1c0 svchost.exe            1712    788      2        0      0      0 2023-08-10 11:13:43 UTC+0000
0xffff9e8b89e541c0 svchost.exe            1748    788     11        0      0      0 2023-08-10 11:13:43 UTC+0000
0xffff9e8b89e562c0 svchost.exe            1756    788      6        0      0      0 2023-08-10 11:13:43 UTC+0000
0xffff9e8b89e70240 svchost.exe            1828    788      6        0      0      0 2023-08-10 11:13:43 UTC+0000
0xffff9e8b89fbc240 svchost.exe            1980    788      3        0      0      0 2023-08-10 11:13:43 UTC+0000
0xffff9e8b89fc1280 svchost.exe            1988    788      6        0      0      0 2023-08-10 11:13:43 UTC+0000
0xffff9e8b89fc4080 svchost.exe            1996    788      6        0      0      0 2023-08-10 11:13:43 UTC+0000
0xffff9e8b89fc2080 svchost.exe            2044    788      8        0      0      0 2023-08-10 11:13:43 UTC+0000
0xffff9e8b89f6f200 svchost.exe            2140    788      2        0      0      0 2023-08-10 11:13:44 UTC+0000
0xffff9e8b8a039240 svchost.exe            2168    788      2        0      0      0 2023-08-10 11:13:44 UTC+0000
0xffff9e8b8a038040 MemCompression         2184      4     22        0 ------      0 2023-08-10 11:13:44 UTC+0000
```

查看有一筆連線

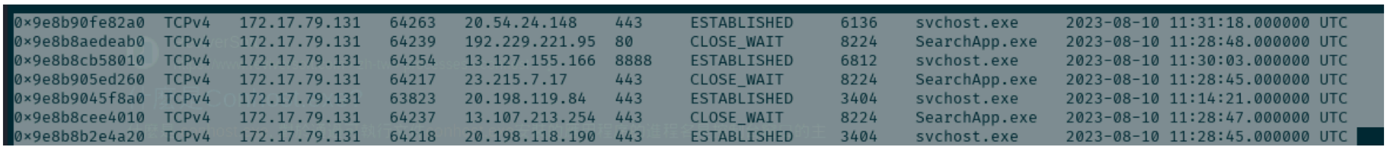
```
python2 vol.py -f 20230810.mem --profile=Win10x64_19041 netscan
```



```
0x9e8b8cb58010     TCPv4    172.17.79.131:64254           13.127.155.166:8888   ESTABLISHED      -1
```

但沒有pid
改用另一組工具volatility3執行

```
python3 vol.py -f 20230810.mem windows.netstat
```



```
0x9e8b90fe82a0  TCPv4   172.17.79.131   64263   20.54.24.148    443     ESTABLISHED     6136    svchost.exe     2023-08-10 11:31:18.000000 UTC
0x9e8b8aedeab0  TCPv4   172.17.79.131   64239   192.229.221.95  80      CLOSE_WAIT      8224    SearchApp.exe   2023-08-10 11:28:48.000000 UTC
0x9e8b8cb58010  TCPv4   172.17.79.131   64254   13.127.155.166  8888    ESTABLISHED     6812    svchost.exe     2023-08-10 11:30:03.000000 UTC
0x9e8b905ed260  TCPv4   172.17.79.131   64217   23.215.7.17     443     CLOSE_WAIT      8224    SearchApp.exe   2023-08-10 11:28:45.000000 UTC
0x9e8b9045f8a0  TCPv4   172.17.79.131   63823   20.198.119.84   443     ESTABLISHED     3404    svchost.exe     2023-08-10 11:14:21.000000 UTC
0x9e8b8cee4010  TCPv4   172.17.79.131   64237   13.107.213.254  443     CLOSE_WAIT      8224    SearchApp.exe   2023-08-10 11:28:47.000000 UTC
0x9e8b8b2e4a20  TCPv4   172.17.79.131   64218   20.198.118.190  443     ESTABLISHED     3404    svchost.exe     2023-08-10 11:28:45.000000 UTC
```

先猜是8888Port

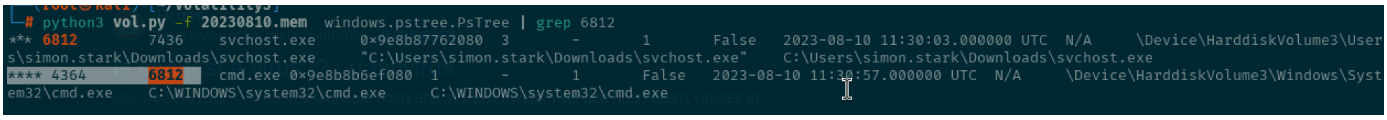
```
0x9e8b90fe82a0  TCPv4   172.17.79.131   64263   20.54.24.148    443
ESTABLISHED     6136    svchost.exe     2023-08-10 11:31:18.000000 UTC
0x9e8b8aedeab0  TCPv4   172.17.79.131   64239   192.229.221.95  80
CLOSE_WAIT      8224    SearchApp.exe   2023-08-10 11:28:48.000000 UTC
0x9e8b8cb58010  TCPv4   172.17.79.131   64254   13.127.155.166  8888
ESTABLISHED     6812    svchost.exe     2023-08-10 11:30:03.000000 UTC
0x9e8b905ed260  TCPv4   172.17.79.131   64217   23.215.7.17     443
CLOSE_WAIT      8224    SearchApp.exe   2023-08-10 11:28:45.000000 UTC
0x9e8b9045f8a0  TCPv4   172.17.79.131   63823   20.198.119.84   443
ESTABLISHED     3404    svchost.exe     2023-08-10 11:14:21.000000 UTC
0x9e8b8cee4010  TCPv4   172.17.79.131   64237   13.107.213.254  443
CLOSE_WAIT      8224    SearchApp.exe   2023-08-10 11:28:47.000000 UTC
0x9e8b8b2e4a20  TCPv4   172.17.79.131   64218   20.198.118.190  443
ESTABLISHED     3404    svchost.exe     2023-08-10 11:28:45.000000 UTC
```

`6812`

Task 2

The SOC team believe the malicious process may spawned another process which enabled threat actor to execute commands. What is the process ID of that child process?

```
python3 vol.py -f 20230810.mem  windows.pstree.PsTree | grep 6812
```



```
└─# python3 vol.py -f 20230810.mem  windows.pstree.PsTree | grep 6812
** 6812         7436    svchost.exe     0x9e8b87762080  3       -       1       False   2023-08-10 11:30:03.000000 UTC  N/A     \Device\HarddiskVolume3\Users\simon.stark\Downloads\svchost.exe     "C:\Users\simon.stark\Downloads\svchost.exe"    C:\Users\simon.stark\Downloads\svchost.exe
**** 4364       6812    cmd.exe 0x9e8b8b6ef080  1       -       1       False   2023-08-10 11:30:57.000000 UTC  N/A     \Device\HarddiskVolume3\Windows\System32\cmd.exe        C:\WINDOWS\system32\cmd.exe     C:\WINDOWS\system32\cmd.exe
```

`4364`

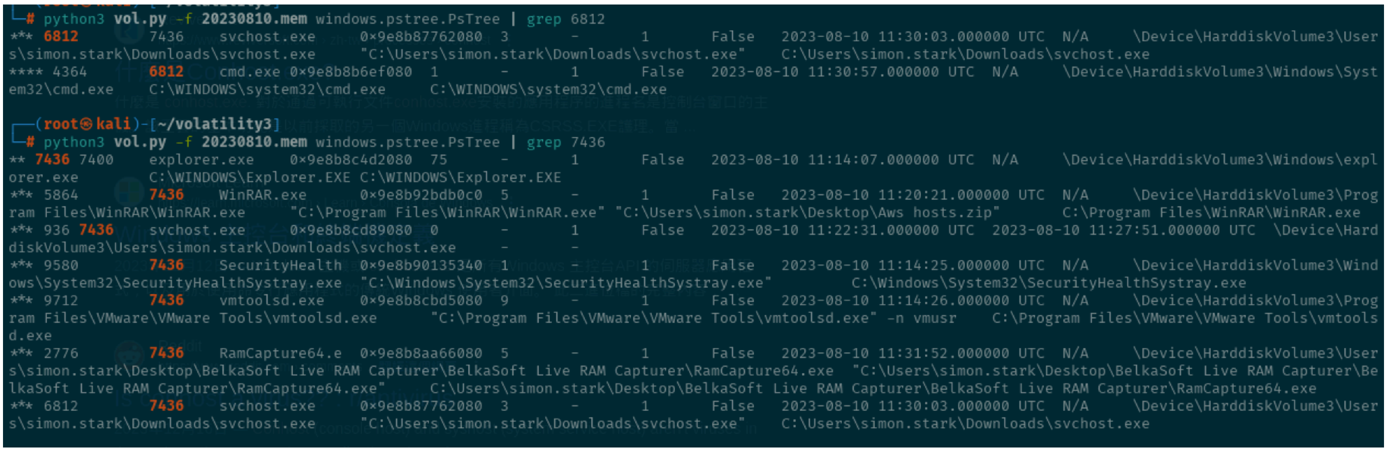
*PPID=7436 svchost.exe

Task 3

The reverse engineering team need the malicious file sample to analyze. Your SOC manager instructed you to find the hash of the file and then forward the sample to reverse engineering team. Whats the md5 hash of the malicious file?

查看父進程`7436`

`python3 vol.py -f 20230810.mem windows.pstree.PsTree | grep 7436`



```
└─# python3 vol.py -f 20230810.mem windows.pstree.PsTree | grep 6812
*** 6812        7436    svchost.exe     0x9e8b87762080  3       -       1       False   2023-08-10 11:30:03.000000 UTC  N/A     \Device\HarddiskVolume3\User
s\simon.stark\Downloads\svchost.exe     "C:\Users\simon.stark\Downloads\svchost.exe"    C:\Users\simon.stark\Downloads\svchost.exe
**** 4364       6812    cmd.exe 0x9e8b8b6ef080  1       -       1       False   2023-08-10 11:30:57.000000 UTC  N/A     \Device\HarddiskVolume3\Windows\Syst
em32\cmd.exe    C:\WINDOWS\system32\cmd.exe     C:\WINDOWS\system32\cmd.exe

┌──(root㉿kali)-[~/volatility3]
└─# python3 vol.py -f 20230810.mem windows.pstree.PsTree | grep 7436
** 7436 7400    explorer.exe    0x9e8b8c4d2080  75      -       1       False   2023-08-10 11:14:07.000000 UTC  N/A     \Device\HarddiskVolume3\Windows\expl
orer.exe        C:\WINDOWS\Explorer.EXE C:\WINDOWS\Explorer.EXE
*** 5864        7436    WinRAR.exe      0x9e8b92bdb0c0  5       -       1       False   2023-08-10 11:20:21.000000 UTC  N/A     \Device\HarddiskVolume3\Prog
ram Files\WinRAR\WinRAR.exe     "C:\Program Files\WinRAR\WinRAR.exe" "C:\Users\simon.stark\Desktop\Aws hosts.zip"       C:\Program Files\WinRAR\WinRAR.exe
*** 936 7436    svchost.exe     0x9e8b8cd89080  0       -       1       False   2023-08-10 11:22:31.000000 UTC  2023-08-10 11:27:51.000000 UTC  \Device\Hard
diskVolume3\Users\simon.stark\Downloads\svchost.exe     -       -
*** 9580        7436    SecurityHealth  0x9e8b90135340  1       -       1       False   2023-08-10 11:14:25.000000 UTC  N/A     \Device\HarddiskVolume3\Wind
ows\System32\SecurityHealthSystray.exe  "C:\Windows\System32\SecurityHealthSystray.exe"         C:\Windows\System32\SecurityHealthSystray.exe
*** 9712        7436    vmtoolsd.exe    0x9e8b8cbd5080  9       -       1       False   2023-08-10 11:14:26.000000 UTC  N/A     \Device\HarddiskVolume3\Prog
ram Files\VMware\VMware Tools\vmtoolsd.exe      "C:\Program Files\VMware\VMware Tools\vmtoolsd.exe" -n vmusr    C:\Program Files\VMware\VMware Tools\vmtools
d.exe
*** 2776        7436    RamCapture64.e  0x9e8b8aa66080  5       -       1       False   2023-08-10 11:31:52.000000 UTC  N/A     \Device\HarddiskVolume3\User
s\simon.stark\Desktop\BelkaSoft Live RAM Capturer\BelkaSoft Live RAM Capturer\RamCapture64.exe  "C:\Users\simon.stark\Desktop\BelkaSoft Live RAM Capturer\Be
lkaSoft Live RAM Capturer\RamCapture64.exe"     C:\Users\simon.stark\Desktop\BelkaSoft Live RAM Capturer\BelkaSoft Live RAM Capturer\RamCapture64.exe
*** 6812        7436    svchost.exe     0x9e8b87762080  3       -       1       False   2023-08-10 11:30:03.000000 UTC  N/A     \Device\HarddiskVolume3\User
s\simon.stark\Downloads\svchost.exe     "C:\Users\simon.stark\Downloads\svchost.exe"    C:\Users\simon.stark\Downloads\svchost.exe
```

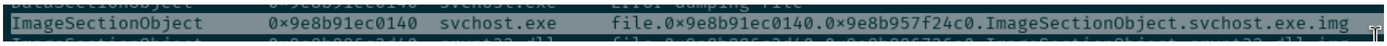
使用者執行了惡意程式碼，導致產生虛假或受損的

```
.svchost.exe、explorer.exe、explorer.exe、svchost.exe、svchost.exe
```

執行

```
python3 vol.py -f 20230810.mem windows.dumpfiles.DumpFiles --pid 6812
```

找PPID執行檔svchost.exe



```
ImageSectionObject      0x9e8b91ec0140  svchost.exe     file.0x9e8b91ec0140.0x9e8b957f24c0.ImageSectionObject.svchost.exe.img
```

```
└─# md5sum file.0x9e8b91ec0140.0x9e8b957f24c0.ImageSectionObject.svchost.exe.img
5bd547c6f5bfc4858fe62c8867acfbb5  file.0x9e8b91ec0140.0x9e8b957f24c0.ImageSectionObject.svchost.exe.img
```

`5bd547c6f5bfc4858fe62c8867acfbb5`

Task 4

In order to find the scope of the incident, the SOC manager has deployed a threat hunting team to sweep across the environment for any indicator of compromise. It would be a great help to the team if you are able to confirm the C2 IP address and ports so our team can utilise these in their sweep.

前面第一題
`13.127.155.166:8888`

Task 5

We need a timeline to help us scope out the incident and help the wider DFIR team to perform root cause analysis. Can you confirm time the process was executed and C2 channel was established?

前面第一題
`10/08/2023 11:30:03`

Task 6

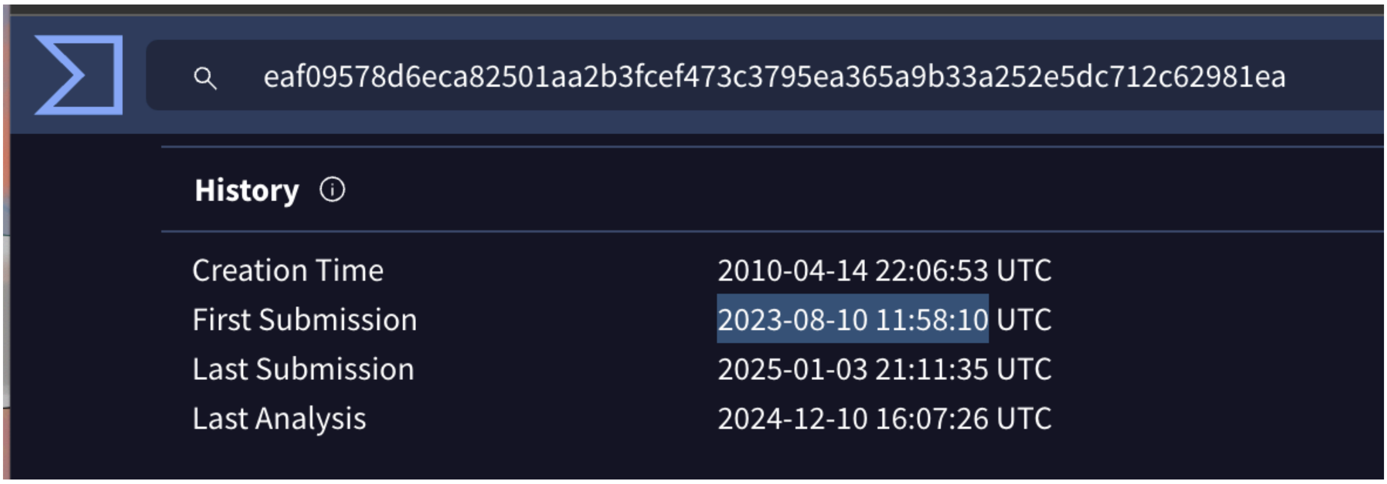
What is the memory offset of the malicious process?

前面第二題

`0x9e8b8b6ef080`

Task 7

You successfully analyzed a memory dump and received praise from your manager. The following day, your manager requests an update on the malicious file. You check VirusTotal and find that the file has already been uploaded, likely by the reverse engineering team. Your task is to determine when the sample was first submitted to VirusTotal.



eaf09578d6eca82501aa2b3fcef473c3795ea365a9b33a252e5dc712c62981ea

History

Creation Time	2010-04-14 22:06:53 UTC
First Submission	2023-08-10 11:58:10 UTC
Last Submission	2025-01-03 21:11:35 UTC
Last Analysis	2024-12-10 16:07:26 UTC

`10/08/2023 11:58:10`