# Digital Forensics Tool Development

• • •

(with. Batch File Programming)

```
%_date% = 2019-10-15
%_Name% = COWB3LL
```

#### Contents

• • •

- 1. Batch File ?
- 2. Batch File Command
- 3. Command & Tool Explanation
- 4. Code review 1
- 5. Volatility ?
- b. Code review 2
- 7. 예제

#### batch file ?

여러 명령어를 한번에 실행시키기 위한 언어

DOS<sup>부분과</sup> Windows에서만 동작 반복적인 작업이나 선택적인 작업에 대한 <u>자동화 실행</u>을 만들 수 있다.

다만 UI를 지원하지 않으며 단순히 CMD창이나 DOS화면을 통해서만 동작하는 단점이 있음

#### Batch File Command

echo : 메시지를 보여주거나 명령어 반향을 켜거나 끔 (ex. echo off : 명령을 표시하지 않음)

pause : 실행중인 배치 파일 일시 정지

set : set 명령은 MS-DOS 환경 변수를 화면에 보여주거나 지정하고 제거하는데 이용되는 명령

### cmd Command & Tool Explanation

- 1. promqry.exe : MS 배포 툴, 네트워크가 프리미어스큐어스 모드인지 아닌지 여부를 확인
- 2. arp : IP<sup>주소에 대한</sup> MAC<sup>주소</sup> 확인
- 3. net user : 계정 정보 출력

• • •

- 4. pslist.exe : 프로세스 목록 및 정보 표시
- 5. handle.exe : 핸들 프로세스 확인
- b. Autorunsc.exe : 자동 실행되는 프로세스 확인
- 7. FDpro.exe : 메모리 덤프 툴
- 8. tcp dump.exe : 패킷 캡쳐 툴

• • •

```
9 :: intro
10 set ver=0.0.1
   title Incident Response Collect Script for Live Response %_ver%
12
13
14
   color 03
15
    @echo *****************************
                Incident Response Script % ver%
    @echo *****************************
21
   goto :main
22
23
    :main
   set date=%date%
   set HOSTNAME=%COMPUTERNAME%
   set _SYSDRIVE=%SYSTENDRIVE%\
   set _ToolPath=toolkit
   if "%PROCESSOR_ARCHITECTURE%" == "x86" set arch=32
   if "%PROCESSOR ARCHITECTURE%" == "AMD64" set arch=64
32
   :: Artifact Output Path
    set /p outputPath=[+] Output Path :
```

...... 관리자: Incident Response Collect Script for Live Response 0.0.1 \*\*\*\* Incident Response Script 0.0.1 +7 Output Path:

```
24 :main
26 set date=%date%
27 set _HOSTNAME=%COMPUTERNAME%
   set SYSDRIVE=%SYSTENDRIVE%\
29 set ToolPath=toolkit
   if "%PROCESSOR_ARCHITECTURE%" == "x86" set arch=32
31 if "%PROCESSOR ARCHITECTURE%" == "AMD64" set arch=64
    :: Artifact Output Path
    set /p outputPath=[+] Output Path :
   set /p isMemoryDump=[+] Memory Dump Execute→ (y/n) :
   if "%isMemoryDump%" == "y" (
       set isMemoryDump=yes
40 ) else (
       set isMemoryDump=no
42 )
   set /p isPacketDump=[+] Packet Dump Execute? \( \forall / n \) :
46 if "%isPacketDump%" == "y" (
       set isPacketDump=yes
48 ) else (
       set isPacketDump=no
53 set /p examiner=[+] Examiner:
54 set _path=%outputPath%\%_HOSTNAME%_%date%_%Examiner%
55 mkdir % path%
```

```
🚾 관리자: Incident Response Collect Script for Live Response 0.0.1
      Incident Response Script 0.0.1
 [+] Output Path : anavize
 [+] Memory Dump Execute? (y/n) :n
 +] Packet Dump Execute? (v/n) :n
 [+] Examiner:kimwoojong
₩ingan\OneDrive\b 하면\z렌식 도구개발 둘
보기
PC > 바탕 화면 > 포렌식 도구개발 툴
  이름
                                     수정한 날짜
                                     2019-10-05 오후 5:23
   anaylze
   test
                                     2019-10-05 오후 4:46
   toolkit
                   ₩ingan₩OneDrive₩바탕 화면₩포렌식 도구개발 툴
   tool-list
                    보기
   vol
                   PC → 바탕 화면 → 포렌식 도구개발 툴 → anay
   whay
  autoanalysis.bat
                     이름
  fcopy.exe
                      C0W8311_2019-10-05_kimwoojong
  test.bat
```

```
secho Computer information
secho Packet Dump Execute: %isPacketDump%
secho Memory Dump Execute: %isMemoryDump%
secho Path: %outputPath%
secho DATE: %_date%
secho Host Name: %_HOSTNAME%
secho Tool Path: %_Toolpath%
secho Arcitecture: %arch%
secho Pause
```

```
Memory Dump Execute : no
Path : anaylze
DATE : 2019-10-05
Host Name : COW8311
Tool Path : toolkit
Arcitecture : 64
계속하려면 아무 키나 누르십시오 . . . .
```

```
74   if not exist % path%\network (
        mkdir % path%\network
        set network_PATH=%_path%\network
 77 )
 80 echo 1_ Checking for Promiscuous Mode
 81 %_ToolPath%\SIS\promqry.exe > %network_PATH%\promiscuous_detect_promqry.txt
     echo 2_ Checking for ARP Cache
     arp -a > %network_PATH%\arp_a.txt
     echo 3 Checking for Net User
     net user > %network PATH%\net user.txt
 92 if not exist %_path%\process (
      mkdir %_path%\process
        set process_PATH=%_path%\process
 95 )
 98 echo 2 1 Checking for Process
99 %_ToolPath%\SIS\pslist.exe /accepteula > %process_PATH%\pslist.txt
100 %_ToolPath%\SIS\handle.exe /accepteula > %process_PATH%\handle.txt
101 %_ToolPath%\SIS\autorunsc.exe /accepteula > %process_PATH%\autorunsc.txt
```

이름	^	수정한 날짜	유형
network		2019-10-05 오후 5:51	파일 폴더
process		2019-10-05 오후 5:51	파일 폴더
이름	^	수정한 날짜	유형
arp_a.txt		2019-10-05 오후 5:51	텍스트 문/
net_user.	txt	2019-10-05 오후 5:51	텍스트 문/
promiscu	ous detect promgry.txt	2019-10-05 오후 5:51	텍스트 문/
arp_a.txt - Windows     व		-	
파일(F) 편집(E) 서식(O	보기(V) 도움말		
인터페이스: 192.168 인터넷 주소 192.168.25.1 192.168.25.7 192.168.25.22 192.168.25.54 192.168.25.63 224.0.0.22 224.0.0.251 224.0.0.252 239.255.255.255 인터페이스: 192.168	물리적 주소 유형 00-08-52-14-e5-c7 동적 70-2c-1f-0f-ef-cd 동적 00-16-6c-c7-dc-10 동적 f0-03-8c-7d-89-59 동적 ff-ff-ff-ff-ff 정적 01-00-5e-00-00-16 정적 01-00-5e-00-00-fc 정적 01-00-5e-7f-ff-fa 정적 ff-ff-ff-ff-ff-ff		
인터넷 주소 192.168.153.254 192.168.153.255 224.0.0.22 224.0.0.251 224.0.0.252 239.255.255.250 255.255.255.255	물리적 주소 유형 00-50-56-fc-9d-4d 동적 ff-ff-ff-ff-ff 정적 01-00-5e-00-00-16 정적 01-00-5e-00-00-fb 정적 01-00-5e-00-00-fc 정적 01-00-5e-7f-ff-fa 정적 ff-ff-ff-ff-ff-ff-ff		

• • •

```
104
    if not exist %_path%\memory (
105
        mkdir %_path%\memory
106
        set memory PATH=% path%\memory
107
108
109
     echo 3_1_Dumping Memory
110
     if "%isMemoryDump%" == "yes" (
111
112
        goto :acquire_memoryDump
113
     ) else (
114
        goto :packet dump
115
116
     echo %isMemoryDump%
117
118
     :acquire_memoryDump
119
     %_ToolPath%\memory\FDPro.exe %memory_PATH%\memdump.dd
```

```
:SELECT NIC
137
      set /p NIC=what's the NIC number you want to acquire (1.2.3...)? || goto :SELECT NIC
138
139
         mkdir % path%\Packet Dump
124
         set packetdump PATH=% path%\Packet Dump
125
    what's the NIC number you want to acquire (1.2.3...)? 8
2019-10-05 18:23:20.56 - created "Packet_Dump" directory in \times
2019-10-05 18:23:20.56 - Packet Dump Start
126
129
130
131
           Win98/ME/NT4/2000/XP/2003/Vista/2008/Win7/Win8/Win2012
132
133
134
          Microplap WinPCap to Packet Sniffer SDK migration module.
135
                           (c) Microolap Technologies,
136
                           Khalturin A.P. & Naumov D.A.
137
                            http://www.microolap.com
138
139
142
                 Topdump v4.5.1 (Nov 20, 2013) for Windows
           Win98/ME/NT4/2000/XP/2003/Vista/2008/Win7/Win8/Win2012
             built with Microolap Packet Sniffer SDK v6.1 and
          Microolap WinPCap to Packet Sniffer SDK migration module.
                           (c) Microolap Technologies.
```

## Volatility

• • •

#### 볼라틸리티란 ?

Python 기반 Windows Memory Forensic Tool
Windows, Linux, Mac 06에서 실행할 수 있음
Open source 이며, Plugin 형태로 다양한 기능들을 제공
플러그인을 자신이 직접 만들어 사용가능
메모리 덤프 파일(img, raw, dmp), 하이버네이션 파일(hiber), 가상 머신 메모리(vmem) 분석가능

### Volatility

#### 볼라틸리티로 획득할 수 있는 정보

트리 형태의 프로세스 리스트, 프로세스가 로드한 DLL과 핸들, 네트워크 정보, 시스템에서 로드했던 드라이 버 목록

실행 중이거나 종료 또는 루트킷으로 은닉된 프로세스의 오프셋, SID(보안 식별자), PID, 스레드 수, 핸들 수, 시작 및 종료시간

## Volatility

• • •

Volatility Command

psscan, pslist, pstree : 프로세스 정보 확인

memmap : 프로세스 메모리 분석

memdump : 메모리 더프

connscan : 네트워크 정보 확인

Handels : 핸들 정보 확인

```
10 title Autovol% ver%
12 set _ver=0.1
19 goto :main
21 :main
23 set date=%date%
24 set HOSTNAME=%COMPUTERNAME%
25 set _SYSDRIVE=%SYSTEMDRIVE%\
26 set Tool=vol.py
27 set SamplePath=sample
28 if "%PROCESSOR ARCHITECTURE%" == "x86" set arch=32
  if "%PROCESSOR ARCHITECTURE%" == "AMD64" set arch=64
   date : %date%
          Computer Name : %COMPUTERNAME%
          System Drive : %SYSTEMDRIVE%
          Process Architecture: %PROCESSOR ARCHITECTURE%
             Tool Name : % Tool%
          Path : %outputPath%
```

Tool name – vol.py

이 부분을 제외하면 Code review – 1 부분이랑 같습니다.!!

```
set /p outputPath=[+] Output Path:
     mkdir "%outputPath%"
48
    set /p file=Input analysis file :
51
     set /p imageinfo=Do you know the profile of this file? (Yes/No) :
52
     if "%imageinfo%" == "Yes" (
         set /p profile=Input profile :
53
                                                         1_ imageinfo
54
         goto :menu
                                                        Volatility Foundation Volatility Framework 2.6
55
     ) else (
                                                               : volatility.debug : Determining profile based on KDBG search...
         goto :imageinfo
56
                                                                  Suggested Profile(s): Win7SP1x86_23418, Win7SP0x86, Win7SP1x86
57
                                                                             AS Layer1: IA32PagedMemoryPae (Kernel AS)
                                                                             AS Layer2 : FileAddressSpace (C:\u00fcUsers\u00fcingan\u00fcOneDrive\u00fcU
                                                        olatility-masterWsampleWSCP.vmem)
                                                                              PAE type: PAE
                                                                                  DTB : 0×185000L
                                                                                  KDBG: 0x82b7ac28L
                                                                  Number of Processors : 2
                                                             Image Type (Service Pack) : 1
                                                                        KPCR for CPU 0 : 0x82b7bc00L
                                                                        KPCR for CPU 1 : 0x807ca000L
                                                                     KUSER SHARED DATA : 0xffdf0000L
                                                                   Image date and time: 2019-10-06 08:16:09 UTC+0000
                                                             Image local date and time: 2019-10-06 01:16:09 -0700
                                                         Input profile : Win7SP0x86
```

• • •

```
:menu
60 echo What do you want?
61 set /p num=0.profile 1.imageinfo 2.psscan 3.pslist 4.pstree 5.filescan 6.memmap 7.memdump 8.connscan 9.handles :
   if "%num%"== "0" (
        goto :profile
                                              What do you want?
O.profile 1.imageinfo 2.psscan 3.pslist 4.pstree 5.filescan 6.memmap 7.memdump 8.connscan 9.handles
    if "%num%"== "1" (
        goto :imageinfo
    if "%num%"== "2" (
        goto :psscan
    if "%num%"== "3" (
        goto :pslist
    if "%num%"== "4" (
        goto :pstree
    if "%num%"== "5" (
        goto :filescan
    if "%num%"== "6" (
        goto :memmap
    if "%num%"== "7" (
        goto :memdump
    if "%num%"== "8" (
        goto :connscan
    if "%num%"== "9" (
        goto :handles
    ) else (
        goto :quit
93 )
```

코드가 더러워 죄송합니다...;;

```
95
                                                              olatility-master
      :profile
      echo 0 profile
 97
      set /p profile =
                        Input profile :
                                                                        Number
 99
      goto :menu
100
101
      :imageinfo
102
      echo 1 imageinfo
103
      python % Tool% -f % SamplePath%\%file% imageinfo
104
                                                                   lmage loca
      set /p profile=Input profile :
                                                              Input profile
105
      goto :menu
106
107
108
      :psscan
109
      echo 2 psscan
110
      python % Tool% -f % SamplePath%\%file% --profile="%profile%" psscar0x8779d290 svchost.exe
111
112
      goto :menu
113
114
115
      :pslist
      echo 3 pslist
116
      python % Tool% -f % SamplePath%\%file% --profile="%profile%" pslist 0x8781c030 msdtc.exe
117
118
      goto :menu
110
```

```
1_ imageinfo
Volatility Foundation Volatility Framework 2.6
           : volatility.debug : Determining profile based on KDBG search...
Suggested Profile(s) : Win7SP1x86_23418, Win7SP0x86, Win7SP1x86
                                AS Laver1: IA32PagedMemoryPae (Kernel AS)
                         pslist.txt - Windows 메모장
                         파일(F) 편집(E) 서식(O) 보기(V) 도움말
                         Offset(V) Name
                                                               Thds
                                                                       Hnds Sess Wow64 Start
                        0x858d1020 System
                                                                                     0 2019-10-06 08:14:34 UTC+0000
                        0x864a08b8 smss.exe
                                                                                     0 2019-10-06 08:14:34 UTC+0000
                        0x86bc5600 csrss.exe
                                                           332
                                                                                    0 2019-10-06 08:14:35 UTC+0000
       Image Type 0x86dd8130 wininit.exe
                                                      428
                                                           332
                                                                                    0 2019-10-06 08:14:35 UTC+0000
                         0x86dd8c78 csrss.exe
                                                      436
                                                                         189
                                                                                     0 2019-10-06 08:14:35 UTC+0000
                        0x875fc5c0 services.exe
                                                                                     0 2019-10-06 08:14:35 UTC+0000
                        0x87610d40 winlogon.exe
                                                       516
                                                                                      0 2019-10-06 08:14:35 UTC+0000
                         0x876105a8 Isass.exe
                                                                                    0 2019-10-06 08:14:35 UTC+0000
                 mage 0x86dd7d40 Ism.exe
                                                           428
                                                      536
                                                                   10
                                                                         140
                                                                                0
                                                                                      0 2019-10-06 08:14:35 UTC+0000
                        0x87646b50 svchost.exe
                                                            484
                                                                          361
                                                                                      0 2019-10-06 08:14:36 UTC+0000
                         0x87685030 vmacthlp.exe
                                                                          54
                                                                                      0 2019-10-06 08:14:36 UTC+0000
                         0x876a9458 svchost.exe
                                                      772
                                                            484
                                                                         276
                                                                                0
                                                                                     0 2019-10-06 08:14:36 UTC+0000
                        0x876e2030 svchost.exe
                                                            484
                                                                         379
                                                                                0
                                                                                      0 2019-10-06 08:14:36 UTC+0000
                        0x876ee5c8 svchost.exe
                                                      896
                                                                   20
                                                                         386
                                                                                      0 2019-10-06 08:14:36 UTC+0000
                        0x876f55f8 svchost.exe
                                                     928
                                                           484
                                                                        776
                                                                                     0 2019-10-06 08:14:36 UTC+0000
                        0x877135d8 audiodg.exe
                                                      1016
                                                             864
                                                                    5
                                                                          124
                                                                                       0 2019-10-06 08:14:36 UTC+0000
                        0x87726438 svchost.exe
                                                      1084
                                                                   14
                                                                          552
                                                                                      0 2019-10-06 08:14:36 UTC+0000
                        0x87743598 svchost.exe
                                                      1168
                                                             484
                                                                   19
                                                                          357
                                                                                      0 2019-10-06 08:14:36 UTC+0000
                        0x87781670 spoolsv.exe
                                                      1288
                                                             484
                                                                          277
                                                                                      0 2019-10-06 08:14:36 UTC+0000
                                                                   14
                                                                          322
                                                      1332
                                                                   19
                                                                                      0 2019-10-06 08:14:36 UTC+0000
                         0x877e39a8 svchost.exe
                                                      1432
                                                            484
                                                                    9
                                                                         172
                                                                                      0 2019-10-06 08:14:37 UTC+0000
                        0x87808158 VGAuthService.
                                                       1480
                                                                                       0 2019-10-06 08:14:37 UTC+0000
                        0x8783c030 vmtoolsd.exe
                                                       1556
                                                             484
                                                                    10
                                                                          272
                                                                                       0 2019-10-06 08:14:37 UTC+0000
                        0x878e3600 taskhost.exe
                                                             484
                                                                          159
                                                      1920
                                                                   10
                                                                                      0 2019-10-06 08:14:37 UTC+0000
                        0x878ed3d0 svchost.exe
                                                                          94
                                                                                      0 2019-10-06 08:14:37 UTC+0000
                        0x87940338 sppsvc.exe
                                                      356
                                                            484
                                                                   5
                                                                         151
                                                                                      0 2019-10-06 08:14:38 UTC+0000
                        0x8782ca58 dllhost.exe
                                                     744
                                                           484
                                                                        203
                                                                                0
                                                                                     0 2019-10-06 08:14:38 UTC+0000
                        0x87833d40 dllhost.exe
                                                                   17
                                                                                      0 2019-10-06 08:14:39 UTC+0000
                                                       692
                                                            484
                                                                   16
                                                                          156
                                                                                0
                                                                                      0 2019-10-06 08:14:39 UTC+0000
                         0x879ad860 WmiPrvSE.exe
                                                                          192
                                                                                  0
                                                                                       0 2019-10-06 08:14:40 UTC+0000
```

<b>1</b>	Ŧ,	Edit As: Text												
	q	)10		30										
		System pid:		a: 5	B:1 055 .	//// handles	oct - Windows	메디자					_	□ ×
		Virtual	Physical	Size Du	umpFileOffset		도(E) 서식(O)		<b>도운막</b>					- A
$\sim$		0**00010000	0**6*406000	0x1000	0**0	0x864dd5		0x64		₩Device₩Hard	diskVolume2\Windows\System32\Log	gFiles₩WMI₩RtBackup₩EtwRTDiagLog.etl		
			0x6b406000	0x1000	0x0 0x1000	0x864b9e	10 4	0x68			Device\HarddiskVolume1\SExtend\\$Rr			
			0x6b407000 0x6b408000	0x1000	0x1000	0x864b74		0x6c		Device₩clfsTxf				
			0x6b408000	0x1000	0x3000	0x864bc3 0x864bdc		0x70 0x74		evice₩Harddis	skVolume1 Device₩HarddiskVolume1₩\$Extend₩\$Rr	Matadata WCTuff a a WCTuff a a		
			0x6b60a000	0x1000	0x4000	0x864bd6		0x74 0x78			Device₩HarddiskVolume1₩\$Extend₩\$Rr			
			0x6b60b000	0x1000	0x5000	0x864bc9				Device₩clfsKtr		·····cadatan + /x/20g ii + /x/20g		
120			0x6b60c000	0x1000	0x6000	0x9b2251		0x80		/ACHINE₩SYST	ΓΕΜ₩CONTROLSET001₩CONTROL₩CLA	.SS₩{4D36E96C-E325-11CE-BFC1-08002BE10318}₩0000	WMIXERSETTINGS	S
			0x6b60d000	0x1000	0x7000	0x864bd1		0x84			hilly it among the second	W4075 lefa		_
			0x6b60e000	0x1000	0x8000	0x863cb2 04046e6c		0x88	0x120089 File	#Device₩Hardo	diskVolume2₩System Volume Informati	on₩{1976d6f3-c673-11e9-9daf-000c2905a855}{380887	/6b-c1/6-4e48-b/	/ae-
			0x6b60f000	0x1000	0x9000	%profil 0x863cec	-18 4	0x8c	0x120089 File	¥Device₩Hardo	diskVolume2₩Svstem Volume Informatio	on₩{4626b196-e1df-11e9-bee9-0c96e6c9acc6}{38088	76b-c176-4e48-b7	7ae-
_			0x6b510000	0x1000	0xa000	04046e6c		550			Total			
			0x6b511000	0x1000	0xb000	0x85af362		0x90	0x120089 File #	†Device₩Hardd	liskVolume2\System Volume Informatic	on\{4eb7275b-c672-11e9-9489-000c2905a855}{38088	76b-c176-4e48-b	7ae-
131			0x6b512000	0x1000	0xc000	04046e6c		0.00	0.120000 51	WD - 1001 - 1	Ply Lawer William	W(4076   6/7   672 44 0 6   1 000 2005 055 (20002)	ICL 170 4 40 17	7
132			0x6b613000	0x1000	0xd000	0x863cc2l 04046e6c		0x94	0x120089 File	<del>v</del> ∪evice\Hardo	aiskvoiume2₩System Volume Informatio	on\{1976d6f7-c673-11e9-9daf-000c2905a855}{380887	юр-с1/6-4e48-b7	/ae-
122			0x6b614000	0x1000	0xe000	04040e00		ഹരദ	0x120089 File	₩Device₩Hard	diskVolume2#Svstem Volume Informati	ion\{1976d6d1-c673-11e9-9daf-000c2905a855}{38088	376b-c176-4e48-b	b7ae-
filescop but			0x6b615000	0x1000	0xf000				5X120005 1110		ansity statute 2 may stem. Variance mile main	(10100001 0010 1100 0000 00000000000		,, ac
파일(F) 편집(E)			0x6b616000	0x1000	0x10000					₩Device₩Hard	diskVolume2₩System Volume Informati	on₩{3808876b-c176-4e48-b7ae-04046e6cc752}		
Offset(P)			0x6b617000	0x1000	0x11000				0x12007f TmRm		PIVI DWG - VI I C	W(4   72757   672 11 0 0400 000 2005 055)(2000)	76 176 4 40 1	. 7
			0x6b618000	0x1000	0x12000				0x120089 File	#Device#Hard	diskVolume2\System Volume Informati	on\{4eb72757-c672-11e9-9489-000c2905a855}{38088	3/6b-c1/6-4e48-b	o/ae-
0x000000000		0x00023000	0x6b619000	0x1000	0x13000	Files₩BootCKCL.etl			0x12007f TmRm					
			0x6b6la000	0x1000	0x14000	ileswoodekez.eu			0xf003f TmTm					
0x0000000002		0x00025000	0x6b61b000	0x1000	0x15000				0x1f007f TmRm					
0x000000000		0x00026000	0x6c21c000	0x1000	0x16000	I				∀Device₩clfsKtı		- NA		
00000000000			0x6c21d000	0x1000	0x17000	01-6e01-11de-8bed-0	01e0bcd1	824}.TM			levice₩HarddiskVolume2₩\$Extend₩\$Rn Device₩HarddiskVolume2₩\$Extend₩\$Rn			
			0x6c21e000	0x1000	0x18000	pport.sys n32k.sys.mui						TxfLog\\$TxfLogContainer00000000000000000000		
0x000000000		0x00029000	0x6c11f000	0x1000	0x19000	.DAT			0x12019f File ₩	†Device₩clfs₩D	)evice₩HarddiskVolume2₩\$Extend₩\$Rn	nMetadata₩\$TxfLog₩\$TxfLog		
0x000000000		0x0002a000	0x6c220000	0x1000	0x1a000	b			0x12019f File ₩	Device₩Hardd	liskVolume2\\$Extend\\$RmMetadata\\$	TxfLog\\$TxfLogContainer000000000000000000000		
			0x6b621000	0x1000	0x1b000							Ln 1, Col 1 100% Win	dows (CRLF) UTF-8	ş
0x000000000		0x0002c000	0x6b622000	0x1000	0x1c000	niPerfClass.dll								
0x000000000		0x0002d000	0x6b623000	0x1000	0x1d000	000006.clb								
			0x6b624000	0x1000	0x1e000	r.DLL								
0x000000000			0x6b625000	0x1000	0x1f000									
0x0000000003		0x00030000	0x6b626000	0x1000	0x20000				conn2.txt -	메모장				
			0x6b627000	0x1000	0x21000			i	out	14 4 1 400	H7100 F.00100			
0x000000000		0x00032000	0x6b628000	0x1000	0x22000	-US₩pacer.sys.mui			파일(F) 편집(E)	서식(0)	보기(V) 도움말(H)	1117		
			0 <b>x</b> 58405000	0x1000	0x23000	icer.sys			Offset(P)	Local	Address	Remote Address	Pid	
0.00000000			0x6b646000	0x1000	0x24000	dSched.exe.mui								
0x00000000014		0x000e2000	0x6b647000	0x1000	0x25000	MDevAPI.dll.mui			050001400	9 179 1	6.176.143:1054	193.104.41.75:80	856	
0x000000001	)utpi	ut				:.windows.common-								
			01.1/514_none_ec83d						0x06015ab	0.0.0	.0:1056	193.104.41.75:80	856	
0x00000000bd					dows\System32\AUDIOKSE				outpu					
0x00000000bd					dows₩System32₩mfc140en dows₩System32₩QUTIL.DLI									
0x00000000bd					dows₩System32₩en-US₩Di									
0x0000000bd			W-rwd ₩Device₩Hard			. ,								
		-					L	Ln 1, Col 1						

```
11822 HCAMP {THIS IS NOT FLAG}
                                                                                        11823 OSp
                                                                                        11824 OSp
                                                                                         11825 OSpl
  Code review
                                                                                        11826 OSp
                                                                                        11827 OSp
                                                                                        11828 | 1Spn
                                                                                        11829 1Sp
                                                                                        11830 1Sp'
     139
                   :memdump
                                                                                         11831 1Sp
                  echo 7 memdump
     140
                                                                                        11832 Gal
                  set /p pid= Input Pid :
     141
                                                                                        11833 1SpS
     142
                   python % Tool% -f % SampleP 11834 oe Print
                  strings %outputPath%\%_pid%<sup>11835</sup> <sup>1Sp</sup>
     143
                                                                                         11836 Segoe Print Bold
     144
                  goto :menu
                                                                                        11837 | 1Sp
                                                                                         11838 | 1Sp
                                                                                        11839 Bold
O.profile 1.imageinfo 2.psscan 3.pslist
                                                                                        11840 dlic
                                                                                         11841 c2on con1
7_ memdump
                                                                                        11842 ,2,-1,
Input Pid: 2456
                                                                                        11843 1)"/>
  psscan.txt - Windows 메모장
                                                                                        Find Results
 파일(F) 편집(E) 서식(O) 보기(V) 도움말
                                                                                                         Address
                                                                                                                                                                                                          Value
 Offset(P)
                                                             PID PPID PDB
                             Name
                                                                                                 Found 13 occurrences of 'HCAMP'
                                                                                                                             HCAMP{THIS IS NOT FLAG}
                                                                                                  Line 11822
                                                                                                  Line 14827
                                                                                                                             HCAMP{
0x00000000052d1020 System
                                                                                   0
                                                                                                                             Line 24067
0x00000000bd4190b0 StikyNot.exe
                                                                      2456
                                                                                  23!
                                                                                                  Line 24069
                                                                                                                             HCAMP{THIS IS NOT FLAG}
0x0000000bd41fd40 vmtoolsd.exe
                                                                       2448
                                                                                  23
                                                                                                  Line 24076
                                                                                                                             x5040\tx5400\tx5760\tx6120\tx6480...11160\tx11520\highlight0\highlight0\highlight0\highlight0\highlight0\highlight0\highlight0\highlight0\highlight0\highlight0\highlight0\highlight0\highlight0\highlight0\highlight0\highlight0\highlight0\highlight0\highlight0\highlight0\highlight0\highlight0\highlight0\highlight0\highlight0\highlight0\highlight0\highlight0\highlight0\highlight0\highlight0\highlight0\highlight0\highlight0\highlight0\highlight0\highlight0\highlight0\highlight0\highlight0\highlight0\highlight0\highlight0\highlight0\highlight0\highlight0\highlight0\highlight0\highlight0\highlight0\highlight0\highlight0\highlight0\highlight0\highlight0\highlight0\highlight0\highlight0\highlight0\highlight0\highlight0\highlight0\highlight0\highlight0\highlight0\highlight0\highlight0\highlight0\highlight0\highlight0\highlight0\highlight0\highlight0\highlight0\highlight0\highlight0\highlight0\highlight0\highlight0\highlight0\highlight0\highlight0\highlight0\highlight0\highlight0\highlight0\highlight0\highlight0\highlight0\highlight0\highlight0\highlight0\highlight0\highlight0\highlight0\highlight0\highlight0\highlight0\highlight0\highlight0\highlight0\highlight0\highlight0\highlight0\highlight0\highlight0\highlight0\highlight0\highlight0\highlight0\highlight0\highlight0\highlight0\highlight0\highlight0\highlight0\highlight0\highlight0\highlight0\highlight0\highlight0\highlight0\highlight0\highlight0\highlight0\highlight0\highlight0\highlight0\highlight0\highlight0\highlight0\highlight0\highlight0\highlight0\highlight0\highlight0\highlight0\highlight0\highlight0\highlight0\highlight0\highlight0\highlight0\highlight0\highlight0\highlight0\highlight0\highlight0\highlight0\highlight0\highlight0\highlight0\highlight0\highlight0\highlight0\highlight0\highlight0\highlight0\highlight0\highlight0\highlight0\highlight0\highlight0\highlight0\highlight0\highlight0\highlight0\highlight0\highlight0\highlight0\highlight0\highlight0\highlight0\highlight0\highlight0\highlight0\highlight0\highlight0\highlight0\highlight0\highlight0\highl
                                                                                                  Line 24077
0x0000000bd472a48 SearchIndexer.
                                                                       2604
                                                                                   48
                                                                                                                             HCAMP{
                                                                                                 Line 24087
                                                                                                                              0x0000000bd4b2d40 SearchProtocol
                                                                        2708
                                                                                                 Line 24099
                                                                                                                             0x0000000bd4c0730 SearchFilterHo
                                                                       2728
                                                                                                 Line 26528
                                                                                                                             00\tx11160\tx11520\highlighto\fo\fs22 HCAMP\fTHIS IS NOT FLAG\highlightq\frac{1}{2}
                                                                                                                                                                                                                                                                                                 ,774KB
0x0000000bd507d40 notepad.exe
                                                                        2848
                                                                                                 Line 26579
                                                                                                                             HCAMP{
                                                                                                  Line 26584
                                                                                                                             HCAMP{THIS IS NOT FLAG}
0x0000000bd5285c0 WmiPrvSE.exe
                                                                        2928
                                                                                                 Line 759916
                                                                                                                             x5040\tx5400\tx5760\tx6120\tx6480...11160\tx11520\highlight0\fight0\fs22 HCAMP\f\lang9\f1\par
0x0000000bd549d40 WmiApSrv.exe
                                                                          2980
```

0x00000000bde08158 VGAuthService.

```
158
159
    :quit
160
    set /p stop=Do you want stop Volatility? (Yes/No) :
    if "%stop%" == "Yes" (
161
        162
163
                  date : %date%
164
                  Computer Name : %COMPUTERNAME%
165
                  System Drive : %SYSTEMDRIVE%
166
                  Process Architecture: %PROCESSOR ARCHITECTURE%
167
                         Tool Name : % Tool%
168
                  Path: %outputPath%
            169
                    What do you want?
170
                    O.profile 1.imageinfo 2.psscan 3.pslist 4.pstree 5.filescan 6.memmap 7.memdump 8.connscan 9.handles : exit
     ) else (
171
                    Do you want stop Volatility? (Yes/No) :Yes
172
        goto :menu
                     date: 2019-10-06
173
                                Computer Name : COW8311
                                System Drive : C:
                                Process Architecture: AMD64
                                Tool Name: vol.py
                                Path : SCP
                    계속하려면 아무 키나 누르십시오 . . .
                    C:\Users\ingan\OneDrive\Ub 항면\Tool2019-09-21\Vol\Volatility-2.6\Volatility-master>
```

 $\bullet \bullet \bullet$ 

#### 예제

누군가 메모장에 비밀 메시지를 기록해놓았다. 비밀 메시지에 내용을 찾아라

플<sup>래그 포</sup>맷 : COWB3LLCTF{CONTENT}

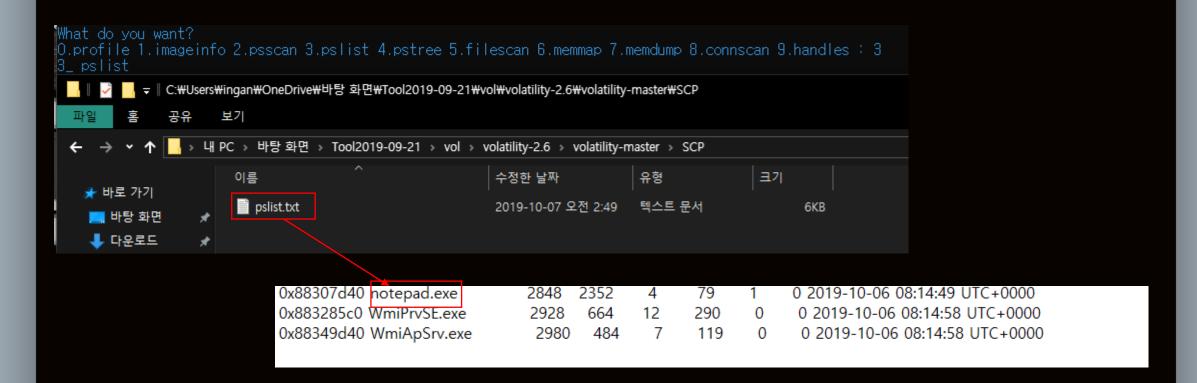
힌트 : 메모장은 프로세스에 올라갈 때 notepad.exe로 올라간다.

#### 예제

```
한 관리자: Autovol0.1
                                                                                                                     ×
date : 2019-10-06
                Computer Name : COW8311
                System Drive : C:
                Process Architecture: AMD64
               Tool Name : vol.py
Path : SCP
[+] Output Path:SCP
Input analysis file: SCP.vmem
Do you know the profile of this file? (Yes/No):No
Volatility Foundation Volatility Framework 2.6
          Suggested Profile(s): Win7SP1x86_23418, Win7SP0x86, Win7SP1x86
                    AS Layer1 : IA32PagedMemoryPae (Kernel AS)
                    AS Layer2 : FileAddressSpace (C:\Users\ingan\voneDrive\volumb\right) 화면\Tool2019-09-21\volumbool4volatility-2.6\vo
olatility-master\sample\SCP.vmem)
                      PAE type : PAE
                          DTB: 0x185000L
                         KDBG: 0x82b7ac28L
          Number of Processors : 2
     Image Type (Service Pack) : 1
                KPCR for CPU 0 : 0x82b7bc00L
                KPCR for CPU 1: 0x807ca000L
            KUSER SHARED DATA: 0xffdf0000L
           Image date and time: 2019-10-06 08:16:09 UTC+0000
     Image local date and time: 2019-10-06 01:16:09 -0700
Input profile: Win7SP1x86 23418_
```

#### 

#### 예제





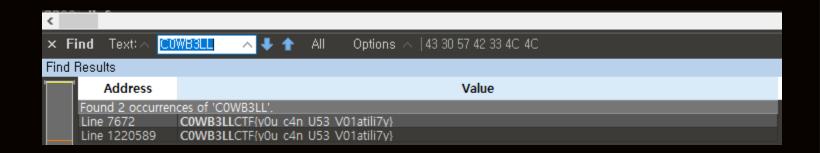


2848.dmp	2019-10-07 오전 2:52	DMP 파일	422,388KB
<b>1</b> 2848.txt	2019-10-07 오전 2:52	텍스트 문서	26,243KB



• • •

1	Ŧ	Edit And Taraka Bun Carinta a Contact a
1 4qQ 2 C:\Windows\system32\SHELL32.dll 3 C:\Windows\system32\SHELL32.dll.124.Config 4 C:\Windows\system32\ 5 en-US 3;0 7 0123456789 8 3;0 9 h:mm:ss tt 10 h:mm tt 11 M/d/yyyy 12 MMMM, yyyy 13 dddd, MMMM dd, yyyy 14 RESCDIR 15 I~2 16 C:\Windows\rescache 17 2fT3 18 ^K[ 19 vn 20 ^QJ 19 g: 22 ~^÷ 25 Eh` 24 't<5 25 q-k,I 26 ;%` 27 0V! 28 fEc 29 YZV 30 9\`t 31 f\ld{m} 33 Ye2 34 m&S 35 M4= 36 ows 37 z=\(\text{u}\) 38 9 40 E'~	*	To the syntax of the syntax o
C:\Windows\system32\SHELL32.dll C:\Windows\system32\SHELL32.dll.124.Config C:\Windows\system32\ En-US En-US 3;0 7 0123456789 8;0 9 h:mm:ss tt 10 h:mm tt 11 M/d/yyyy 12 MMMM, yyyy 13 dddd, MMMM dd, yyyy 14 RESCDIR 15 I-2 16 C:\Windows\rescache 17 2fT3 18 ^K[ 17 0 20 ^QJ 21 9g: 2-^÷ 25 q-k,I 26 ;%` 27 0V! 26 fEc 27 yzy 30 9\`t 31 f%□ 32 G 33 Ye2 34 m&S 35 M4= 36 oWs 3-1 2**Q 40 E'~*		
3 C:\Windows\system32\SHELL32.dll.124.Config 4 C:\Windows\system32\ 5 en-US 6 3;0 7 0123456789 8 3;0 9 h:mm:ss tt 10 h:mm tt 11 M/d/yyyy 12 MMMM, yyyy 13 dddd, MMMM dd, yyyy 14 RESCDIR 15 I-2 16 C:\Windows\rescache 17 2fT3 18 ^K[ 17 Vn 10 ^0J 19 9g: 20 ^0- 21 9g: 22 ~^÷ 25 Eh` 24 't<5 25 q-k,I 26 ;%` 27 0V! 26 fEc 27 YZV 28 9\`t 31 f%□ 32 G 33 Ye2 34 m&S 35 M4= 36 oWs 37 z=ü 38 39 2"Q 40 E'~		
4 C:\Windows\system32\ 5 en-US 3;0 7 0123456789 8 3;0 9 h:mm:ss tt 10 h:mm tt 11 M/d/yyyy 12 MMMM, yyyy 13 dddd, MMMM dd, yyyy 14 RESCDIR 15 I~2 16 C:\Windows\rescache 2fT3 18 ^K[ 19 vn 20 ^QJ 29 g: 22 ~^÷ 23 Eh` 24 't<5 25 q-k,I 26; %` 27 OV! 28 fEc 29 YZV 30 9\`t 31 f\ld{1} f\ld{1} 33 Ye2 34 mas 35 M4= 36 ows 37 2=\(\delta\) 38 39 2"Q 40 E'~		
5 en-US 3;0 7 0123456789 8 3;0 9 h:mm:ss tt 10 h:mm tt 11 M/d/yyyy MMMM, yyyy MMMM, yyyy 14 RESCDIR 15 I~2 16 C:\Windows\rescache 17 2fT3 18 ^K[ 19 vn 20 ^QJ 21 9g:		
6 3;0 7 0123456789 8 3;0 9 h:mm:ss tt 10 h:mm tt 11 M/d/yyyy 12 MMMM, yyyy 14 RESCDIR 15 I~2 16 C:\Windows\rescache 17 2fT3 18 7K[ 19 Vn 20 ^QJ 21 9g: 22 ~^÷ 24 't<5 25 q-k,I 26 ;%` 27 OV! 26 fEc 29 Y2V 30 9\`t 31 f%□ 32 G 33 Ye2 34 m&S 35 M4= 36 oWs 37 z=ü 38 39 2°Q 40 E'~		
7 0123456789 8 3;0 9 h:mm:ss tt 10 h:mm tt 11 M/d/yyyy 12 MMMM, yyyy 13 dddd, MMMM dd, yyyy 14 RESCDIR 15 I-2 16 C:\Windows\rescache 17 2fT3 18 ^K[ 17 v 10 v 20 ^QJ 21 9g: 2-^÷ 25 q-k,I 24 't<5 25 q-k,I 26;%` 27 OV! 26 fEc 29 YZV 30 9\`t 31 f%□ 32 G 33 Ye2 34 m&S 35 M4= 36 oWs 37 2=ü 38 39 2"Q 40 E'~		
8 3;0 9 h:mm:ss tt 10 h:mm tt 11 M/d/yyyy 12 MMMM, yyyy 13 dddd, MMMM dd, yyyy 14 RESCDIR 15 I~2 16 C:\Windows\rescache 17 2fT3 18 ^K[ 17 vn 10 ^QJ 19 9g: 22 ~^÷ 23 Eh 24 't<5 25 'q-k,I 26 '%' 27 OV! 26 fEc 27 YZV 30 9\'t 31 f%□ 32 G 33 Ye2 34 m&S 35 M4= 36 oWs 37 2=û 38 39 2"Q 40 E'~		
10 h:mm tt 11 M/d/yyyy 12 MMMM, yyyyy 13 dddd, MMMM dd, yyyy 14 RESCDIR 15 I~2 16 C:\Windows\rescache 17 2fT3 18 ^K[ 19 vn 20 ^QJ 21 9g: 22 ~^+ 24 't<5 24 't<5 25 q-k,I 26 ;%` 27 OV! 28 fEc 29 YZV 30 9\`t 31 f\ld{m} 31 f\ld{m} 33 Ye2 34 m&S 35 M4= 36 ows 37 z=\(\dat{u}\) 38 39 2"Q 40 E'~		
11 M/d/yyyy 12 MMMM, yyyy 13 dddd, MMMM dd, yyyy 14 RESCDIR 15 I~2 16 C:\Windows\rescache 17 2fT3 1		h:mm:ss tt
12 MMM, yyyy  dddd, MMMM dd, yyyy  RESCDIR  15 I-2  16 C:\Windows\rescache  17 2fT3  *K[  18 ^K[  19		h:mm tt
dddd, MMMM dd, yyyy RESCDIR  I 2 C:\Windows\rescache  7 2fT3  *K[  *Vn  20 ^OJ  9g:  22 ~^÷  28 Eh`  24 't<5  25 q-k,I  26 ;*`  27 OV!  fEcc  29 YZV  30 9\`t  31 f*□  32 G  33 Ye2  34 m&S  35 M4=  36 OWs  37 2=ü  38 9 2"Q  40 E'~		M/d/yyyy
dddd, MMMM dd, yyyy RESCDIR  I 2 C:\Windows\rescache  7 2fT3  *K[  *Vn  20 ^OJ  9g:  22 ~^÷  28 Eh`  24 't<5  25 q-k,I  26 ;*`  27 OV!  fEcc  29 YZV  30 9\`t  31 f*□  32 G  33 Ye2  34 m&S  35 M4=  36 OWs  37 2=ü  38 9 2"Q  40 E'~	12	МММ, уууу
15 I~2 16 C:\Windows\rescache 17 2fT3 1		dddd, MMMM dd, yyyy
16 C:\Windows\rescache 17 2fT3 18 ^K[ 19 Vn 20 ^QJ 21 9g: 22 ~^÷ 24 't<5 25 q-k,I 26 ;%` 27 OV! fEc 29 YZV 30 9\`t 31 f%□ 32 G 33 Ye2 34 m&S 35 M4= 36 oWs 37 2=ü 38 39 2"Q 40 E'~		RESCDIR
17 2fT3 18 ^K[ 19 vh 20 ^QJ 21 9g: 22 ~^÷ 23 Eh` 24 't<5 26 ;*` 27 0V! 28 fEc 29 YZV 30 9\`t fMD 31 fMD 32 G 33 Ye2 34 m&S 35 M4= 36 oWs 37 oWs 38  39 2"Q 40 E'~	15	
18 ^K[ 19 vn 20 ^QJ 20 ** 22 ~** 23 Eh 24 't<5 25 q-k,I 26 ;* 27 YZV 30 9\`t 31 f*\(\text{D}\) 31 f*\(\text{D}\) 32 G 33 Y=2 34 mas 35 M4= 36 ows 37 z=\(\text{U}\) 38 39 2"Q 40 E'~		
19 vn 20 ^QJ 21 9g: 22 ~^÷ 23 Eh' 24 't<5 25 q-k,I 26 ;%' 27 OV! 28 fEc 29 YZV 30 9\'t 31 f%□ 31 f%□ 32 G 33 Ye2 34 m&S 35 M4= 36 oWs 37 z=ü 38 39 2"Q 40 E'~		
20 ^QJ 21 9g:		
21 9g: 22 ~^÷ 22 ~^÷ 24 't<5 25 q-k,I 26 ;%` 27 OV! 26 gy 27 Sy 30 9\`t 31 f%□ 32 G 33 Ye2 34 m&S 35 M4= 36 oWs 37 z=ü 38 39 2"Q 40 E'~		
22 ~^÷ 23 Eh` 24 't<5 25 q-k,I 26 ;%` 27 OV! 28 fEc 29 YZV 30 9\`t 31 G 32 G 33 Ye2 34 m&S 35 M4= 36 oWs 37 z=ü 38 39 2"Q 40 E'~		
23 Eh` 24 't<5 25 q-k,I 25 q-k,I 27 0V! 28 fEc 29 YZV 30 9\`t 31 f% 31 g 32 Ye2 34 m&S 35 M4= 36 oWs 2=ü 38 39 2*Q 40 E'~		
24 't<5 25 q-k,I 26 ;%' 27 ov! 28 fEc 29 YZV 30 9\'t 31 f%  32		
25 q-k,I 26 ;%` 27 OV! 28 fEc 29 Y2V 30 9\`t 31 f%□ 33 Ye2 34 m&S 35 M4= 36 oWs 37 z=ü 38 39 2*Q 40 E'~		
26 ;%` 27 OV! 28 fEc 29 YZV 30 9\`t 31 f%□ 32 G 33 Ye2 34 m&S 35 M4= 36 oWs 37 z=ü 38 39 2"Q 40 E'~		
27 OV! 28 fEc 29 Y2V 31 fM□ 32 G 33 Ye2 34 m&S 35 M4= 36 oWs 37 z=ü 38 39 2"Q 40 E'~		
28 fEc 29 YZV 30 9\`t 31 f8□ 32 F8□ 33 Ye2 34 m&S 35 M4= 36 oWs 37 ows 38 ye2 39 ows 30 ows		
29 YZV 30 9\`t 31 f*\(\Pi\) 31 f*\(\Pi\) 33 Y=2 34 m&S 35 M4= 36 oWs 2=\(\pi\) 38 39 2"Q 40 E'~		
30 9\`t 31 f%□ 32 G 34 m&S 35 M4= 36 oWs 37 z=ü 38 39 2°Q 40 E'~		
31 f N □ 32 G 33 Ye2 34 maS 35 W4= 36 oWs 37 z=ü 38 39 2"Q 40 E'~		
32 G 33 Ye2 34 m&S 35 M4= 37 z=ü 38 39 2"Q 40 E'~		
33 Ye2 34 m&S 35 M4= 36 oWs 37 z=ü 38 39 2"Q 40 E'~	32	
34 m&S 35 M4= 36 oWs 37 z=ü 38 39 2"Q 40 E'~	33	
35 M4= 36 oWs 37 z=ü 38 39 z"Q 40 E'~		
36 oWs 37 z=ü 38 39 z"Q 40 E'~		
38 39 2"Q 40 E'~		
39 2"Q 40 E'~	37	z=ü
40 E'~		
		2"Q
<	40	E'~
	<	



```
7667 }H=
7668 @!9
7669 P*"
7670 }e0
7671 _D6
7672 COWB3LLCTF{yOu_c4n_U53_V0latili7y}
7673 |z5
7674 9p8
7675 +00
7676 /C:\
7677 9lidateFilenameChars
7678 }b(
7679 8Xp
```



## NEXT



Q&A

