

<휘발성 증거 수집 단계> - 증거 수집시 전원을 off하면 삭제되는 휘발성을 가진 증거들을 먼저 수집한다.

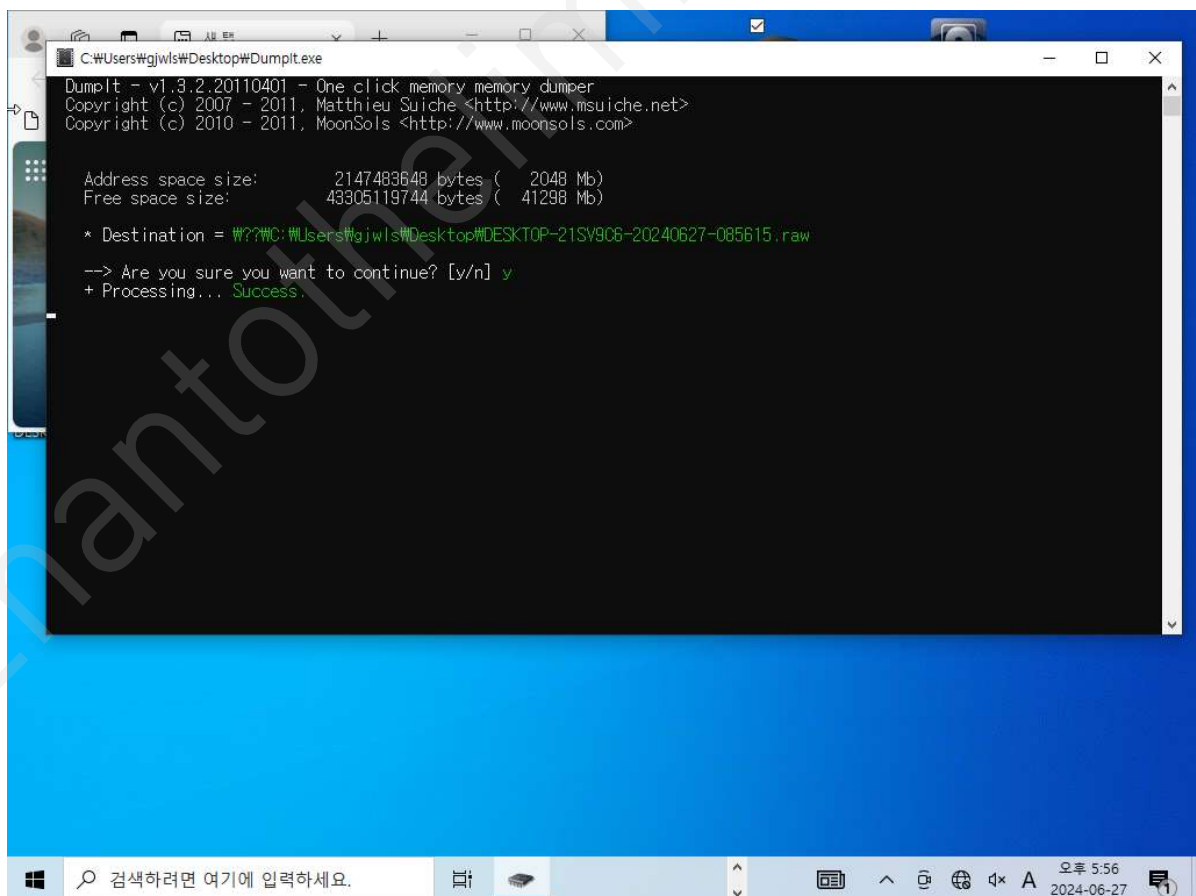
1. 조사대상물의 전원상태 확인
 - 전원이 켜져있을 경우 현재 화면 등을 촬영 등의 방법으로 기록.
2. 시간 정보를 수집
 - 한국 표준시인 UTC+9인지, Timezone Asia/Seoul인지 등 확인
3. 네트워크 정보 수집
 - 원격접속 등을 통한 증거인멸 우려가 있을 시 네트워크 정보 수집 후 즉시 네트워크 케이블 분리
4. 프로세스 정보 수집
5. 메모리 정보 수집
6. 시스템 정보 수집
7. 휘발성 정보가 저장된 파일에 대한 해시값을 생성하여 증거물 목록에 기재하고 입회인에게 확인 후 서명날인
8. 시스템 정보 파악 후 안전한 방법으로 전원 차단.

<메모리 정보 수집> - 메모리를 덤프(메모리의 해당 순간을 캡처하여 파일로 저장)하여 Volatility로 분석
(가상머신 환경 가정)

1. 수집 단계

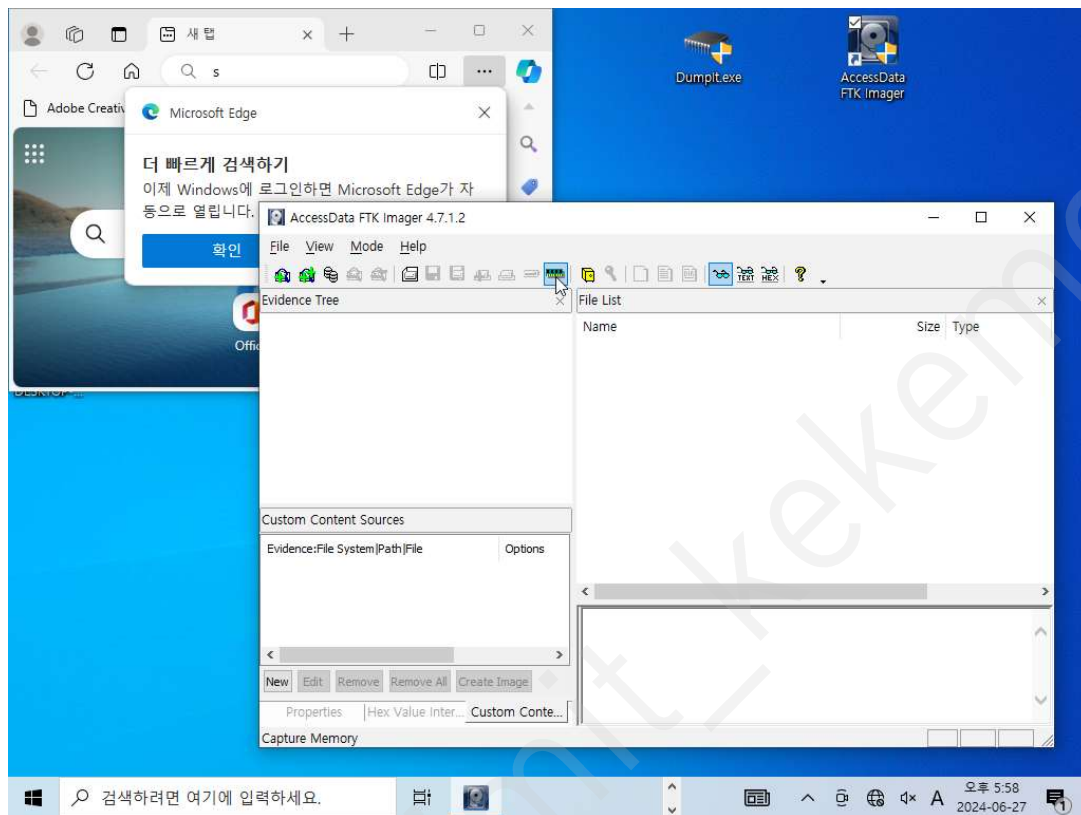
가. Dumpit을 활용한 수집

- Dumpit을 활용하여 .raw 파일로 덤프하여 다음과 같이 수집



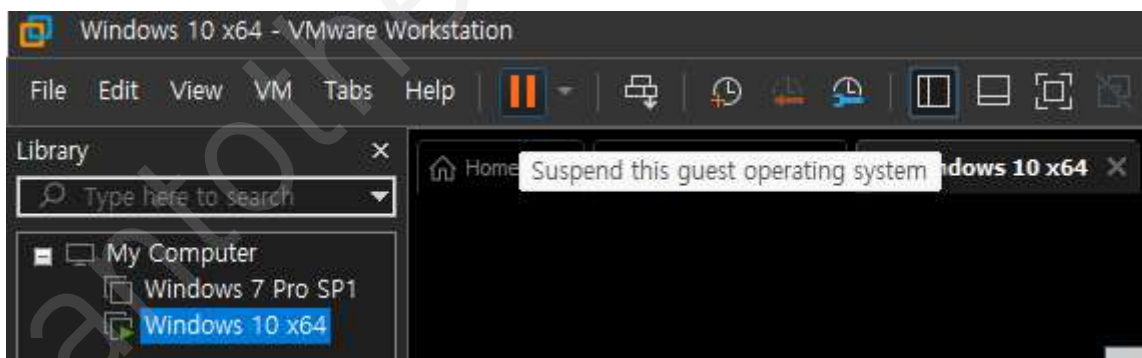
나. FTK Imager를 활용한 수집

- FTK Imager를 활용하여 .mem 파일로 덤프하여 다음과 같이 수집



다. (가상머신 환경 메모리 덤프의 경우) VMware 해당

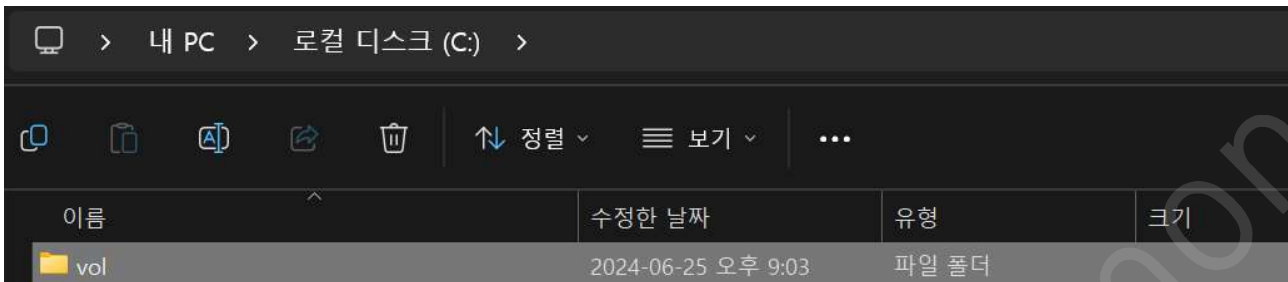
- 아래 일시정지 버튼 활용하여 .vmem 파일로 덤프하여 다음과 같이 수집



Virtual Machines > Windows 10 x64 >			
이름	수정된 날짜	유형	크기
564d2702-ff7b-8e29-713d-dd0bdce54a8c.vmem	2024-06-27 오후 5:52	VMEM 파일	2,097,152KB

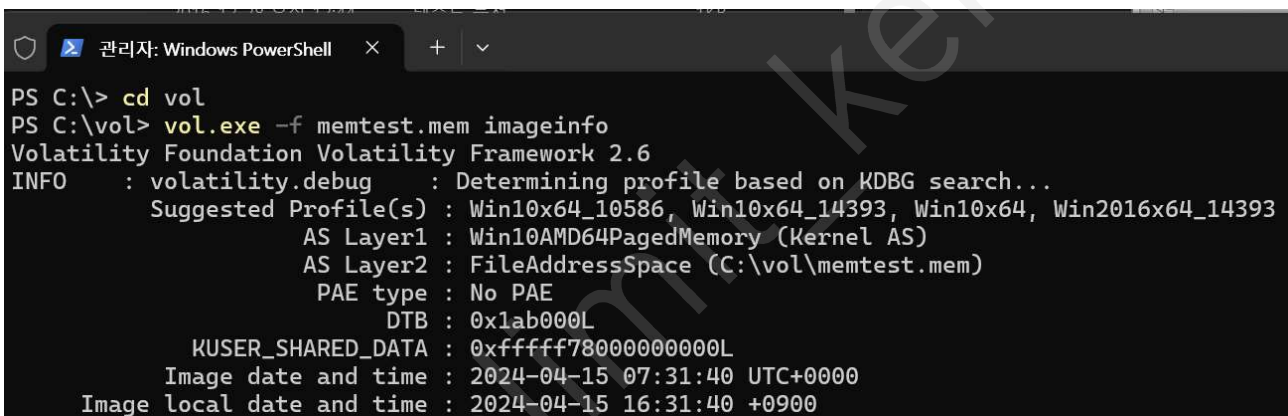
2. 분석 단계

가. 실행 편의를 위해 volatility.exe를 vol.exe로 폴더, 이름명 변환 및 C:\에 저장 및 환경 변수 설정



나. 프로파일정보 확인(imageinfo)

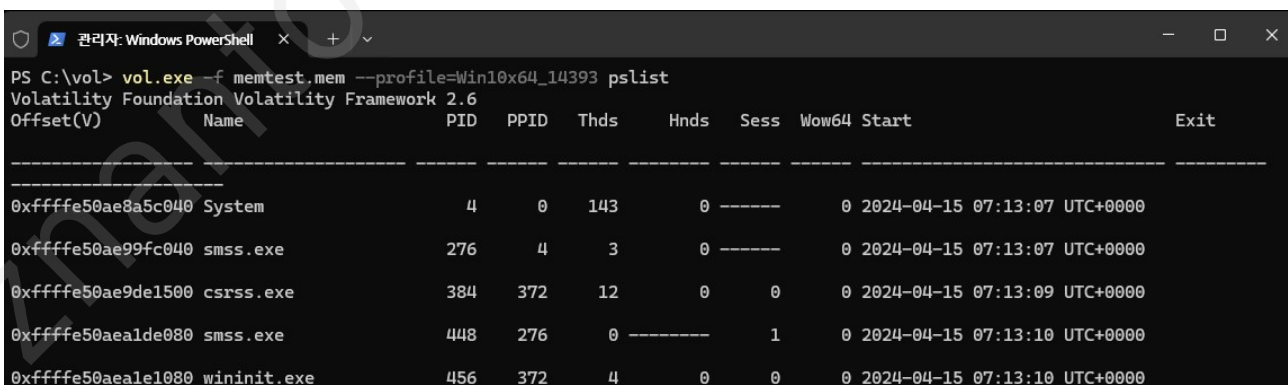
```
PS C:\> cd vol
PS C:\vol> vol.exe -f memory_dump.mem imageinfo
```



- Suggested Profile(s)로부터 프로파일 정보 획득

다. pslist

```
PS C:\vol> vol.exe -f memtest.mem --profile=Win10x64_14393 pslist
```

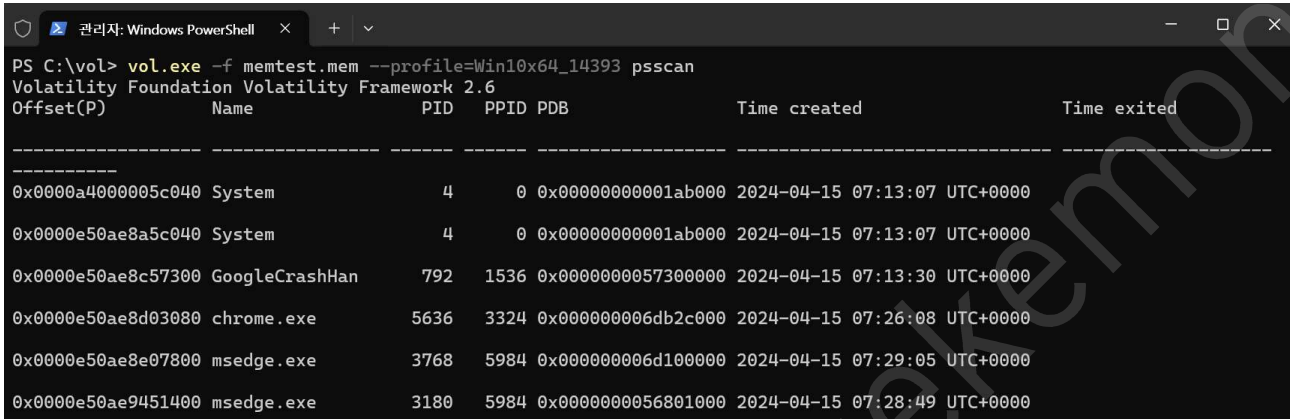


- pslist로 현재 작동 중인 모든 프로세스 리스트 시간순으로 출력

라. psscan

```
PS C:\vol> vol.exe -f memtest.mem --profile=Win10x64_14393 psscan
```

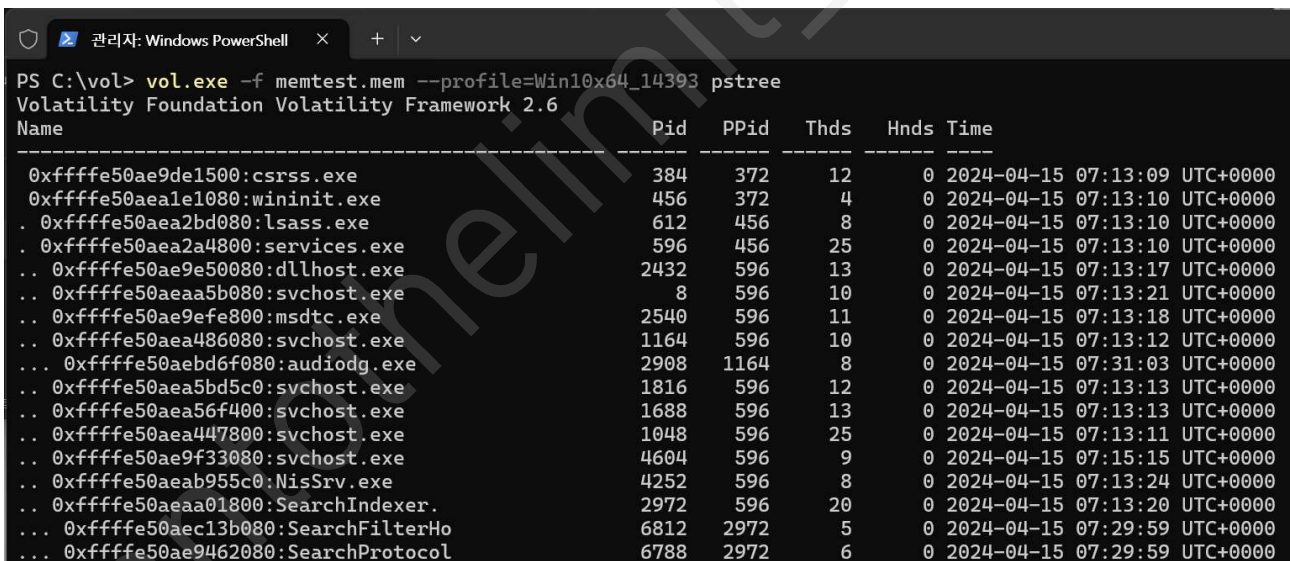
- pslist와 달리 현재 작동중인 프로세스를 포함하여 비활성화, 숨겨지거나 연결이 끊긴 모든 프로세스 확인 가능 (offset 순 출력)



Offset(P)	Name	PID	PPID	PDB	Time created	Time exited
0x0000a4000005c040	System	4	0	0x000000000001ab000	2024-04-15 07:13:07 UTC+0000	
0x0000e50ae8a5c040	System	4	0	0x000000000001ab000	2024-04-15 07:13:07 UTC+0000	
0x0000e50ae8c57300	GoogleCrashHan	792	1536	0x000000000057300000	2024-04-15 07:13:30 UTC+0000	
0x0000e50ae8d03080	chrome.exe	5636	3324	0x00000000006db2c000	2024-04-15 07:26:08 UTC+0000	
0x0000e50ae8e07800	msedge.exe	3768	5984	0x00000000006d100000	2024-04-15 07:29:05 UTC+0000	
0x0000e50ae9451400	msedge.exe	3180	5984	0x000000000056801000	2024-04-15 07:28:49 UTC+0000	

마. pstree

```
PS C:\vol> vol.exe -f memtest.mem --profile=Win10x64_14393 pstree
```

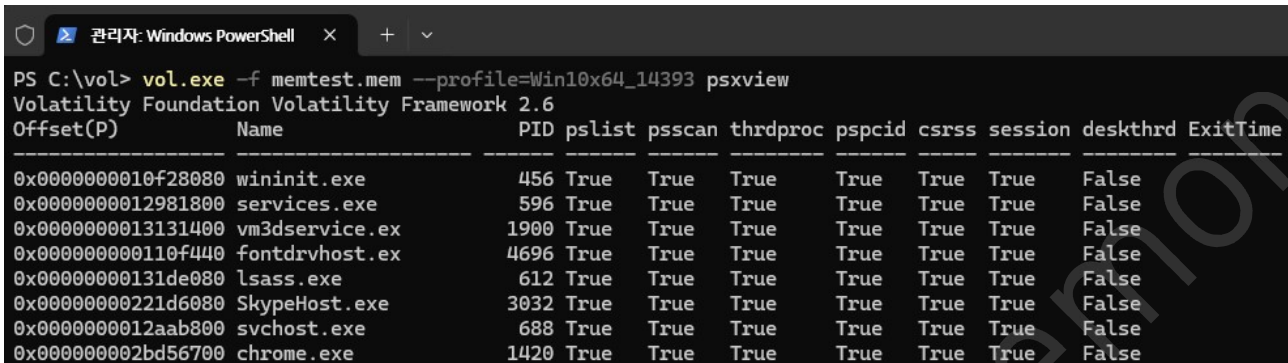


Name	Pid	PPid	Thds	Hnds	Time
0xfffffe50ae9de1500:csrss.exe	384	372	12	0	2024-04-15 07:13:09 UTC+0000
0xfffffe50aea1e1080:wininit.exe	456	372	4	0	2024-04-15 07:13:10 UTC+0000
.. 0xfffffe50aea2bd080:lsass.exe	612	456	8	0	2024-04-15 07:13:10 UTC+0000
.. 0xfffffe50aea2a4800:services.exe	596	456	25	0	2024-04-15 07:13:10 UTC+0000
.. 0xfffffe50ae9e50080:dllhost.exe	2432	596	13	0	2024-04-15 07:13:17 UTC+0000
.. 0xfffffe50aea5b080:svchost.exe	8	596	10	0	2024-04-15 07:13:21 UTC+0000
.. 0xfffffe50ae9efe800:msdtc.exe	2540	596	11	0	2024-04-15 07:13:18 UTC+0000
.. 0xfffffe50aea486080:svchost.exe	1164	596	10	0	2024-04-15 07:13:12 UTC+0000
... 0xfffffe50aebd6f080:audiodg.exe	2908	1164	8	0	2024-04-15 07:31:03 UTC+0000
.. 0xfffffe50aea5bd5c0:svchost.exe	1816	596	12	0	2024-04-15 07:13:13 UTC+0000
.. 0xfffffe50aea56f400:svchost.exe	1688	596	13	0	2024-04-15 07:13:13 UTC+0000
.. 0xfffffe50aea447800:svchost.exe	1048	596	25	0	2024-04-15 07:13:11 UTC+0000
.. 0xfffffe50ae9f33080:svchost.exe	4604	596	9	0	2024-04-15 07:15:15 UTC+0000
.. 0xfffffe50aeab955c0:NisSrv.exe	4252	596	8	0	2024-04-15 07:13:24 UTC+0000
.. 0xfffffe50aea01800:SearchIndexer.	2972	596	20	0	2024-04-15 07:13:20 UTC+0000
... 0xfffffe50aec13b080:SearchFilterHo	6812	2972	5	0	2024-04-15 07:29:59 UTC+0000
... 0xfffffe50ae9462080:SearchProtocol	6788	2972	6	0	2024-04-15 07:29:59 UTC+0000

- 프로세스 리스트를 부모(PPID)-자식(PID) 간 관계를 트리 형태로 . .. , 과 같은 형식으로 출력

바. psxview

```
PS C:\vol> vol.exe -f memtest.mem --profile=Win10x64_14393 psxview
```

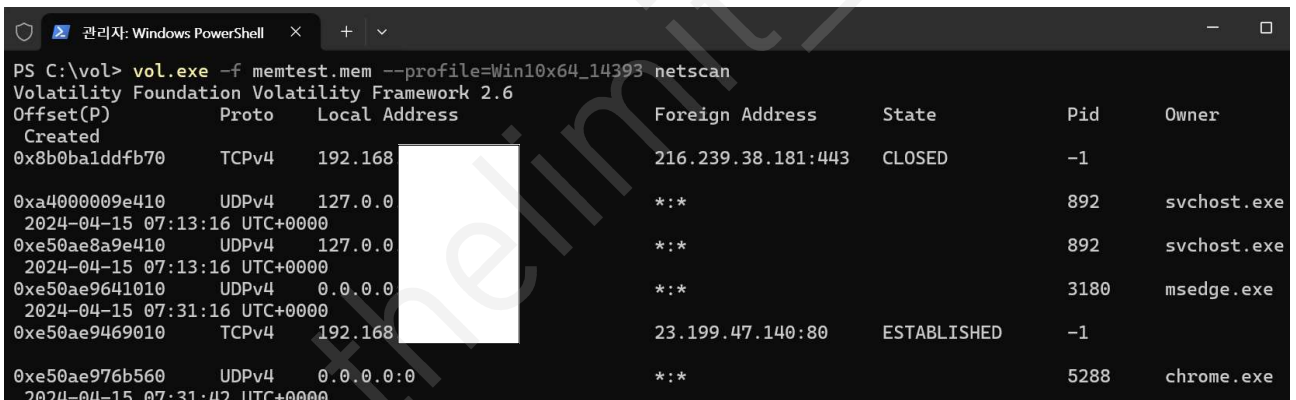


Offset(P)	Name	PID	pslist	psscan	thrdproc	pspcid	csrss	session	deskthrd	ExitTime
0x0000000010f28080	wininit.exe	456	True	True	True	True	True	True	False	
0x0000000012981800	services.exe	596	True	True	True	True	True	True	False	
0x0000000013131400	vm3dservice.ex	1900	True	True	True	True	True	True	False	
0x00000000110f440	fontdrvhost.ex	4696	True	True	True	True	True	True	False	
0x00000000131de080	lsass.exe	612	True	True	True	True	True	True	False	
0x00000000221d6080	SkypeHost.exe	3032	True	True	True	True	True	True	False	
0x0000000012aab800	svchost.exe	688	True	True	True	True	True	True	False	
0x000000002bd56700	chrome.exe	1420	True	True	True	True	True	True	False	

- pslist, psscan의 True/False 값을 통해 숨겨진 프로세스를 식별
- 예를 들어 pslist가 False이고, psscan이 True인 경우 숨겨진 프로세스(악성코드 등)일 가능성
- 숨겨진 프로세스 악성코드 침해사고분석 등에 응용

사. netscan

```
PS C:\vol> vol.exe -f memtest.mem --profile=Win10x64_14393 netscan
```



Offset(P)	Proto	Local Address	Foreign Address	State	Pid	Owner
Created						
0x8b0ba1ddfb70	TCPv4	192.168.0.1	216.239.38.181:443	CLOSED	-1	
0xa4000009e410	UDPv4	127.0.0.1	***		892	svchost.exe
2024-04-15 07:13:16 UTC+0000						
0xe50ae8a9e410	UDPv4	127.0.0.1	***		892	svchost.exe
2024-04-15 07:13:16 UTC+0000						
0xe50ae9641010	UDPv4	0.0.0.0	***		3180	msedge.exe
2024-04-15 07:31:16 UTC+0000						
0xe50ae9469010	TCPv4	192.168.0.1	23.199.47.140:80	ESTABLISHED	-1	
0xe50ae976b560	UDPv4	0.0.0.0:0	***		5288	chrome.exe
2024-04-15 07:31:42 UTC+0000						

- 프로세스 별 이용 프로토콜 및 IP주소, 포트 번호, 네트워크 연결 정보 등 확인

아. envvars

```
PS C:\vol> vol.exe -f memtest.mem --profile=Win10x64_14393 envvars
```

```
관리자: Windows PowerShell
PS C:\vol> vol.exe -f memtest.mem --profile=Win10x64_14393 envvars
Volatility Foundation Volatility Framework 2.6
Pid      Process      Block      Variable      Value
-----
384      csrss.exe    0x0000019ce1502600 ComSpec      C:\Windows\system32\cmd.exe
384      csrss.exe    0x0000019ce1502600 NUMBER_OF_PROCESSORS 2
384      csrss.exe    0x0000019ce1502600 OS           Windows_NT
384      csrss.exe    0x0000019ce1502600 Path         C:\Windows\system32;C:\Windows;C:\Windows\Sy
stem32\Wbem;C:\Windows\System32\WindowsPowerShell\v1.0\
384      csrss.exe    0x0000019ce1502600 PATHEXT      .COM;.EXE;.BAT;.CMD;.VBS;.VBE;.JS;.JSE;.WSF;
.WSH;.MSC
384      csrss.exe    0x0000019ce1502600 PROCESSOR_ARCHITECTURE AMD64
384      csrss.exe    0x0000019ce1502600 PROCESSOR_IDENTIFIER AMD64 Family 25 Model 80 Stepping 0, Authent
icAMD
384      csrss.exe    0x0000019ce1502600 PROCESSOR_LEVEL 25
384      csrss.exe    0x0000019ce1502600 PROCESSOR_REVISION 5000
384      csrss.exe    0x0000019ce1502600 PSModulePath %ProgramFiles%\WindowsPowerShell\Modules;C:\
```

- CPU 수, 하드웨어 아키텍처, 프로세스 현재/임시 디렉토리, 세션/컴퓨터/유저 이름 등의 프로세스 환경변수 확인

자. cmdline

```
PS C:\vol> vol.exe -f memtest.mem --profile=Win10x64_14393 cmdline
```

```
관리자: Windows PowerShell
PS C:\vol> vol.exe -f memtest.mem --profile=Win10x64_14393 cmdline
Volatility Foundation Volatility Framework 2.6
*****
System pid: 4
*****
smss.exe pid: 276
*****
csrss.exe pid: 384
Command line :
*****
smss.exe pid: 448
*****
wininit.exe pid: 456
*****
csrss.exe pid: 464
Command line : %SystemRoot%\system32\csrss.exe ObjectDirectory=\Windows SharedSection=1024,20480,768 Windows=On SubSystemType=Windows ServerDll=basesrv,1 ServerDll=winsrv:UserServerDllInitialization,3 ServerDll=sxssrv,4 ProfileControl=Off MaxRequestThreads=16
*****
winlogon.exe pid: 540
Command line : winlogon.exe
*****
services.exe pid: 596
Command line : C:\Windows\system32\services.exe
*****
lsass.exe pid: 612
Command line : C:\Windows\system32\lsass.exe
*****
svchost.exe pid: 688
Command line : C:\Windows\system32\svchost.exe -k DcomLaunch
```

- 프로세스가 실행되기 위한 인자값(커맨드 작동의 대상) 확인

차. dlllist

```
PS C:\vol> vol.exe -f memtest.mem --profile=Win10x64_14393 dlllist -p [PID]
```

```
관리자: Windows PowerShell
PS C:\vol> vol.exe -f memtest.mem --profile=Win10x64_14393 dlllist -p 5636
Volatility Foundation Volatility Framework 2.6
*****
chrome.exe pid: 5636
Command line : "C:\Program Files\Google\Chrome\Application\chrome.exe"

Base                               Size          LoadCount Path
-----
0x00007ff63e6f0000 0x2b6000      0x0 C:\Program Files\Google\Chrome\Application\chrome.exe
0x00007ff8b4680000 0x1d2000      0x0 C:\Windows\SYSTEM32\ntdll.dll
0x00007ff8b2590000 0xac000       0x0 C:\Windows\System32\KERNEL32.DLL
0x00007ff8b0fe0000 0x21d000      0x0 C:\Windows\System32\KERNELBASE.dll
0x00007ff8961b0000 0x147000      0x0 C:\Program Files\Google\Chrome\Application\123.0.6312.122\chrome_e
f.dll
0x00007ff8aafa0000 0xa000        0x0 C:\Windows\SYSTEM32\VERSION.dll
0x00007ff8b2b90000 0x9e000       0x0 C:\Windows\System32\msvcrt.dll
0x00007ff8b0b80000 0x6a000       0x0 C:\Windows\System32\bcryptprimitives.dll
0x00007ff8b2640000 0xa2000       0x0 C:\Windows\System32\ADVAPI32.dll
0x00007ff8b20f0000 0x59000       0x0 C:\Windows\System32\sechost.dll
0x00007ff8b4420000 0x121000      0x0 C:\Windows\System32\RPCRT4.dll
0x00007ff8af830000 0x32000       0x0 C:\Windows\system32\ntmarta.dll
0x00007ff8b1b10000 0xf5000       0x0 C:\Windows\System32\ucrtbase.dll
0x00007ff8b2f10000 0x1509000     0x0 C:\Windows\System32\SHELL32.dll
0x00007ff8b0ee0000 0x42000       0x0 C:\Windows\System32\cfgmgr32.dll
0x00007ff8b1200000 0x6d9000      0x0 C:\Windows\System32\windows.storage.dll
0x00007ff8b2c30000 0x2c8000      0x0 C:\Windows\System32\combase.dll
0x00007ff8b0af0000 0x4c000       0x0 C:\Windows\System32\powrprof.dll
0x00007ff8b4610000 0x52000       0x0 C:\Windows\System32\shlwapi.dll
0x00007ff8b1f70000 0x34000       0x0 C:\Windows\System32\GDI32.dll
```

- 특정 프로세스(위 예에선 chrome.exe, PID:5636)가 사용하는 동적 링크 라이브러리(dll) 확인
- 특정 프로세스 확인 위해 -p [PID] 옵션 추가로 주어야 함.

3. 추출 단계

가. 각 플러그인 별 .log파일로 추출

```
PS C:\vol> vol.exe -f memtest.mem --profile=Win10x64_14393 [플러그인명] > [파일명]
```

```
예) PS C:\vol> vol.exe -f memtest.mem --profile=Win10x64_14393 pslist > .\export\pslist.log
```

- 현재 디렉토리 하위 export 디렉토리에 pslist.log 저장

나. procdump

```
PS C:\vol> vol.exe -f memtest.mem --profile=Win10x64_14393 procdump -p [PID] -D [경로명]
```

```
예) PS C:\vol> vol.exe -f memtest.mem --profile=Win10x64_14393 procdump -p 5636 -D
.\export\
```

- 현재 디렉토리 하위 export 디렉토리에 특정 프로세스의 실행파일을 파일로 추출

다. memdump

```
PS C:\vol> vol.exe -f memtest.mem --profile=Win10x64_14393 memdump -p [PID] -D [경로명]
```

```
예) PS C:\vol> vol.exe -f memtest.mem --profile=Win10x64_14393 memdump -p 5636 -D
.\export\
```

- 현재 디렉토리 하위 export 디렉토리에 특정 프로세스의 메모리 영역을 파일로 추출