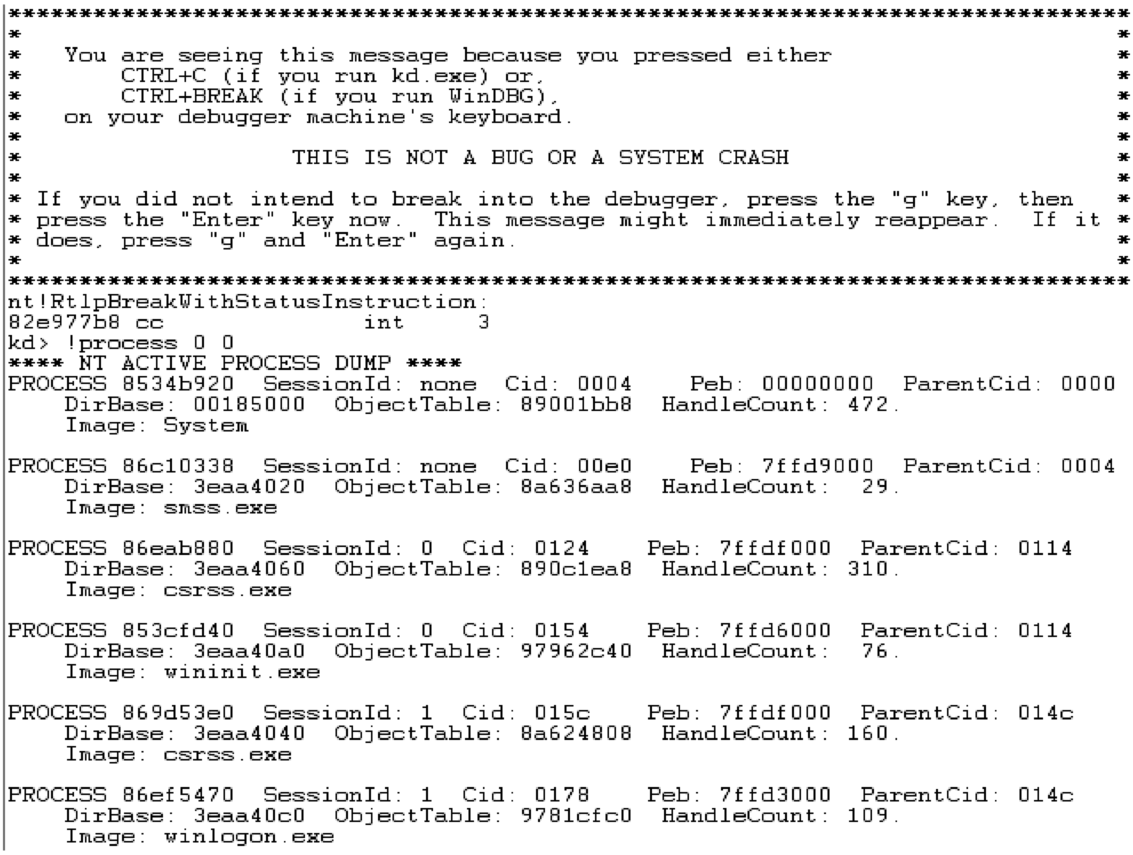
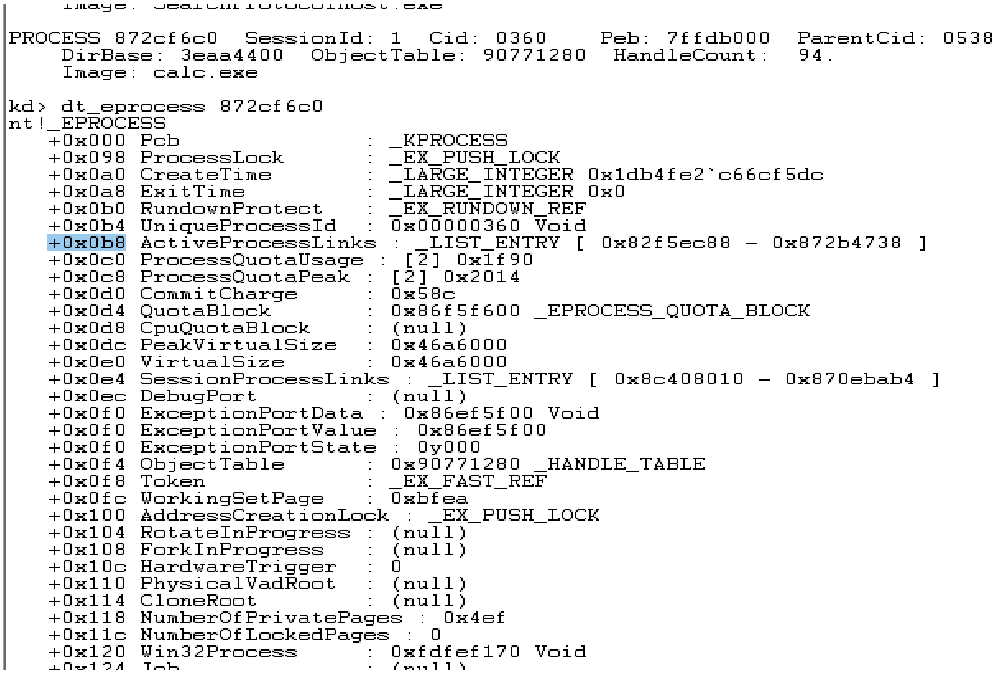
프로세스 정보 확인



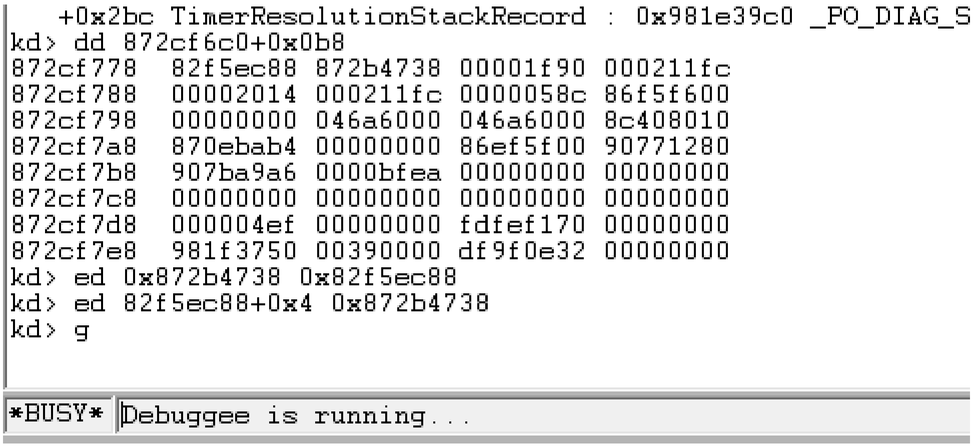
```
*******************************************************************************
*                                                                             *
*   You are seeing this message because you pressed either                    *
*       CTRL+C (if you run kd.exe) or,                                        *
*       CTRL+BREAK (if you run WinDBG),                                       *
*   on your debugger machine's keyboard.                                      *
*                                                                             *
*                   THIS IS NOT A BUG OR A SYSTEM CRASH                       *
*                                                                             *
* If you did not intend to break into the debugger, press the "g" key, then   *
* press the "Enter" key now.  This message might immediately reappear.  If it *
* does, press "g" and "Enter" again.                                          *
*                                                                             *
*******************************************************************************
nt!RtlpBreakWithStatusInstruction:
82e977b8 cc              int     3
kd> !process 0 0
**** NT ACTIVE PROCESS DUMP ****
PROCESS 8534b920  SessionId: none  Cid: 0004    Peb: 00000000  ParentCid: 0000
    DirBase: 00185000  ObjectTable: 89001bb8  HandleCount: 472.
    Image: System

PROCESS 86c10338  SessionId: none  Cid: 00e0    Peb: 7ffd9000  ParentCid: 0004
    DirBase: 3eaa4020  ObjectTable: 8a636aa8  HandleCount:  29.
    Image: smss.exe

PROCESS 86eab880  SessionId: 0  Cid: 0124    Peb: 7ffdf000  ParentCid: 0114
    DirBase: 3eaa4060  ObjectTable: 890c1ea8  HandleCount: 310.
    Image: csrss.exe

PROCESS 853cfd40  SessionId: 0  Cid: 0154    Peb: 7ffd6000  ParentCid: 0114
    DirBase: 3eaa40a0  ObjectTable: 97962c40  HandleCount:  76.
    Image: wininit.exe

PROCESS 869d53e0  SessionId: 1  Cid: 015c    Peb: 7ffdf000  ParentCid: 014c
    DirBase: 3eaa4040  ObjectTable: 8a624808  HandleCount: 160.
    Image: csrss.exe

PROCESS 86ef5470  SessionId: 1  Cid: 0178    Peb: 7ffd3000  ParentCid: 014c
    DirBase: 3eaa40c0  ObjectTable: 9781cfc0  HandleCount: 109.
    Image: winlogon.exe
```

해당 프로세스 상세정보 확인



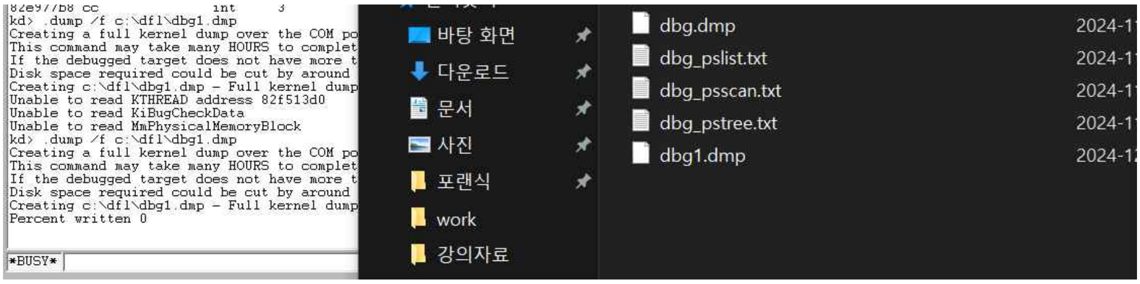
```
    Image: SearchProtocolHost.exe

PROCESS 872cf6c0  SessionId: 1  Cid: 0360    Peb: 7ffdb000  ParentCid: 0538
    DirBase: 3eaa4400  ObjectTable: 90771280  HandleCount:  94.
    Image: calc.exe

kd> dt_eprocess 872cf6c0
nt!_EPROCESS
   +0x000 Pcb              : _KPROCESS
   +0x098 ProcessLock      : _EX_PUSH_LOCK
   +0x0a0 CreateTime       : _LARGE_INTEGER 0x1db4fe2`c66cf5dc
   +0x0a8 ExitTime         : _LARGE_INTEGER 0x0
   +0x0b0 RundownProtect   : _EX_RUNDOWN_REF
   +0x0b4 UniqueProcessId  : 0x00000360 Void
   +0x0b8 ActiveProcessLinks : _LIST_ENTRY [ 0x82f5ec88 - 0x872b4738 ]
   +0x0c0 ProcessQuotaUsage : [2] 0x1f90
   +0x0c8 ProcessQuotaPeak : [2] 0x2014
   +0x0d0 CommitCharge     : 0x58c
   +0x0d4 QuotaBlock       : 0x86f5f600 _EPROCESS_QUOTA_BLOCK
   +0x0d8 CpuQuotaBlock    : (null)
   +0x0dc PeakVirtualSize  : 0x46a6000
   +0x0e0 VirtualSize      : 0x46a6000
   +0x0e4 SessionProcessLinks : _LIST_ENTRY [ 0x8c408010 - 0x870ebab4 ]
   +0x0ec DebugPort        : (null)
   +0x0f0 ExceptionPortData : 0x86ef5f00 Void
   +0x0f0 ExceptionPortValue : 0x86ef5f00
   +0x0f0 ExceptionPortState : 0y000
   +0x0f4 ObjectTable      : 0x90771280 _HANDLE_TABLE
   +0x0f8 Token            : _EX_FAST_REF
   +0x0fc WorkingSetPage   : 0xbfea
   +0x100 AddressCreationLock : _EX_PUSH_LOCK
   +0x104 RotateInProgress : (null)
   +0x108 ForkInProgress   : (null)
   +0x10c HardwareTrigger  : 0
   +0x110 PhysicalVadRoot  : (null)
   +0x114 CloneRoot        : (null)
   +0x118 NumberOfPrivatePages : 0x4ef
   +0x11c NumberOfLockedPages : 0
   +0x120 Win32Process     : 0xfdfef170 Void
   +0x124 Job              : (null)
```

process 은닉



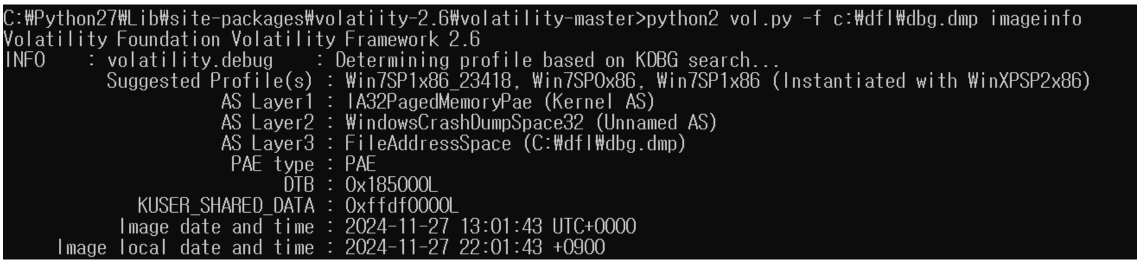
```
   +0x2bc TimerResolutionStackRecord : 0x981e39c0 _PO_DIAG_S
kd> dd 872cf6c0+0x0b8
872cf778  82f5ec88 872b4738 00001f90 000211fc
872cf788  00002014 000211fc 0000058c 86f5f600
872cf798  00000000 046a6000 046a6000 8c408010
872cf7a8  870ebab4 00000000 86ef5f00 90771280
872cf7b8  907ba9a6 0000bfea 00000000 00000000
872cf7c8  00000000 00000000 00000000 00000000
872cf7d8  000004ef 00000000 fdfef170 00000000
872cf7e8  981f3750 00390000 df9f0e32 00000000
kd> ed 0x872b4738 0x82f5ec88
kd> ed 82f5ec88+0x4 0x872b4738
kd> g
```

메모리 덤프



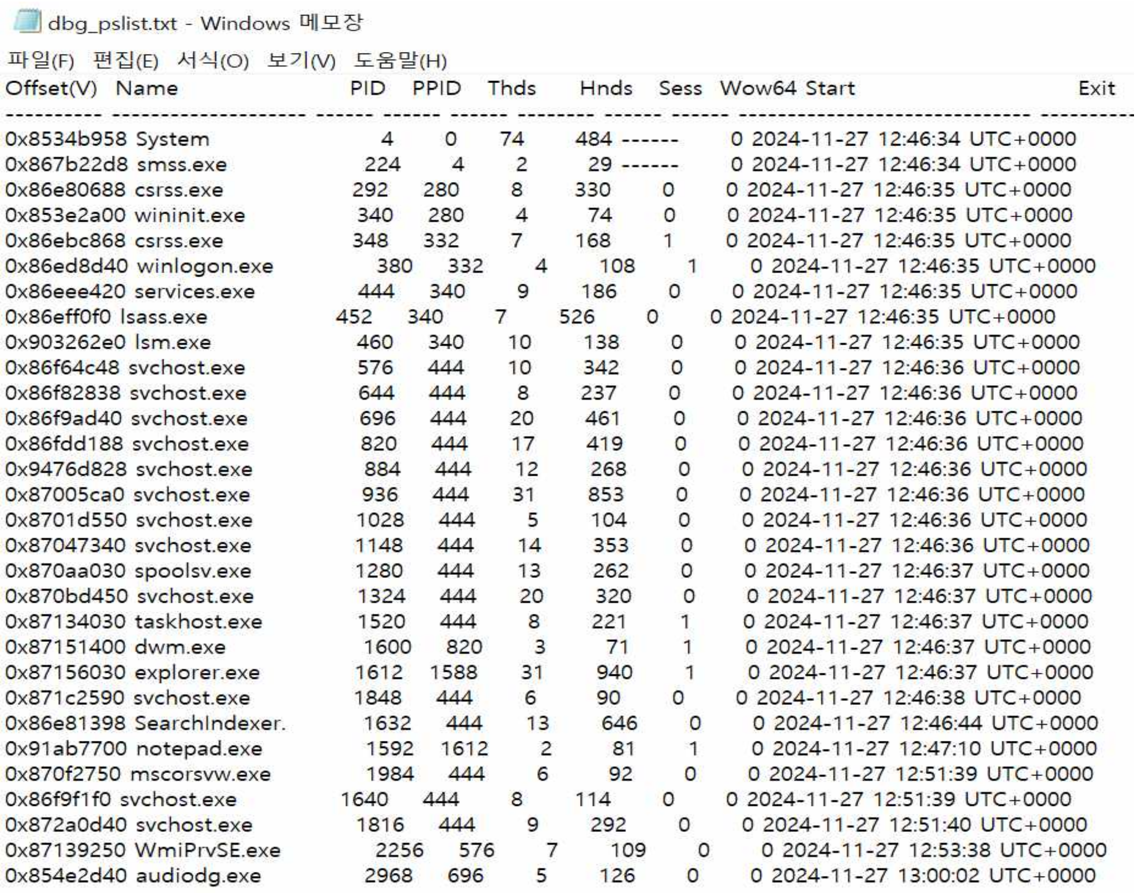
```
82e977b8 cc              int     3
kd> .dump /f c:\dfl\dbg1.dmp
Creating a full kernel dump over the COM po
This command may take many HOURS to complet
If the debugged target does not have more t
Disk space required could be cut by around
Creating c:\dfl\dbg1.dmp - Full kernel dump
Unable to read KTHREAD address 82f513d0
Unable to read KiBugCheckData
Unable to read MmPhysicalMemoryBlock
kd> .dump /f c:\dfl\dbg1.dmp
Creating a full kernel dump over the COM po
This command may take many HOURS to complet
If the debugged target does not have more t
Disk space required could be cut by around
Creating c:\dfl\dbg1.dmp - Full kernel dump
Percent written 0
```

덤프 파일 imageinfo



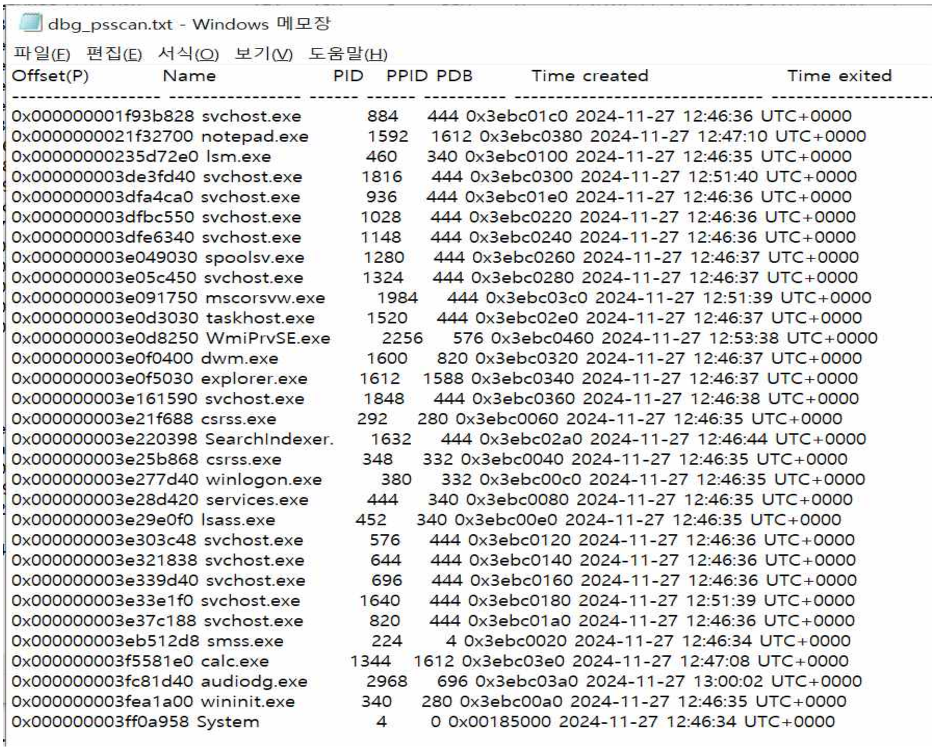
```
C:₩Python27₩Lib₩site-packages₩volatiity-2.6₩volatility-master>python2 vol.py -f c:₩dfl₩dbg.dmp imageinfo
Volatility Foundation Volatility Framework 2.6
INFO    : volatility.debug    : Determining profile based on KDBG search...
          Suggested Profile(s) : Win7SP1x86_23418, Win7SP0x86, Win7SP1x86 (Instantiated with WinXPSP2x86)
                     AS Layer1 : IA32PagedMemoryPae (Kernel AS)
                     AS Layer2 : WindowsCrashDumpSpace32 (Unnamed AS)
                     AS Layer3 : FileAddressSpace (C:₩dfl₩dbg.dmp)
                      PAE type : PAE
                           DTB : 0x185000L
             KUSER_SHARED_DATA : 0xffdf0000L
           Image date and time : 2024-11-27 13:01:43 UTC+0000
     Image local date and time : 2024-11-27 22:01:43 +0900
```

pslist


dbg_pslist.txt - Windows 메모장
파일(F) 편집(E) 서식(O) 보기(V) 도움말(H)

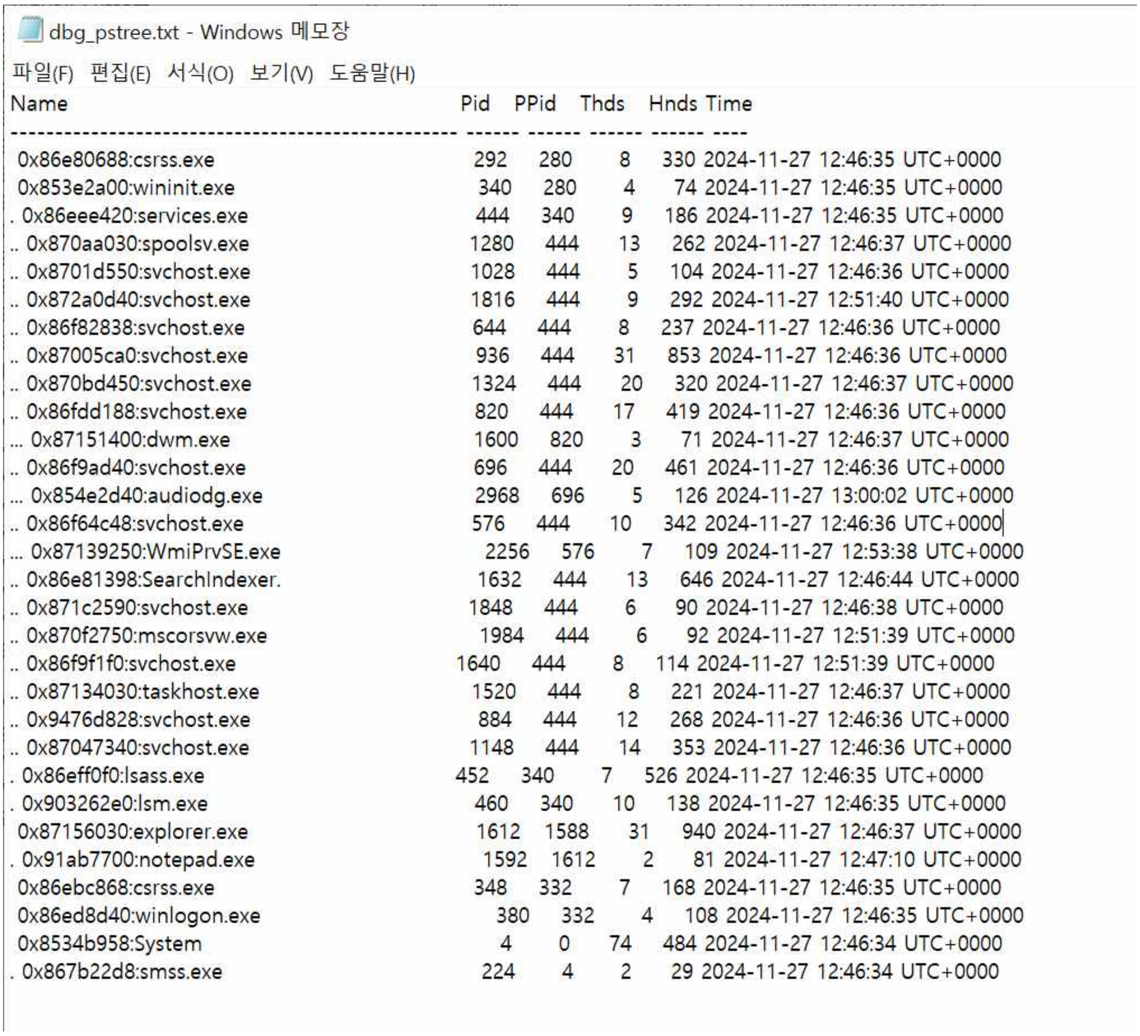
```
Offset(V)  Name                    PID   PPID   Thds     Hnds   Sess  Wow64 Start                          Exit
---------- -------------------- ------ ------ ------ -------- ------ ------ ------------------------------ ----------
0x8534b958 System                  4      0     74      484 ------      0 2024-11-27 12:46:34 UTC+0000
0x867b22d8 smss.exe              224      4      2       29 ------      0 2024-11-27 12:46:34 UTC+0000
0x86e80688 csrss.exe             292    280      8      330      0      0 2024-11-27 12:46:35 UTC+0000
0x853e2a00 wininit.exe           340    280      4       74      0      0 2024-11-27 12:46:35 UTC+0000
0x86ebc868 csrss.exe             348    332      7      168      1      0 2024-11-27 12:46:35 UTC+0000
0x86ed8d40 winlogon.exe          380    332      4      108      1      0 2024-11-27 12:46:35 UTC+0000
0x86eee420 services.exe          444    340      9      186      0      0 2024-11-27 12:46:35 UTC+0000
0x86eff0f0 lsass.exe             452    340      7      526      0      0 2024-11-27 12:46:35 UTC+0000
0x903262e0 lsm.exe               460    340     10      138      0      0 2024-11-27 12:46:35 UTC+0000
0x86f64c48 svchost.exe           576    444     10      342      0      0 2024-11-27 12:46:36 UTC+0000
0x86f82838 svchost.exe           644    444      8      237      0      0 2024-11-27 12:46:36 UTC+0000
0x86f9ad40 svchost.exe           696    444     20      461      0      0 2024-11-27 12:46:36 UTC+0000
0x86fdd188 svchost.exe           820    444     17      419      0      0 2024-11-27 12:46:36 UTC+0000
0x9476d828 svchost.exe           884    444     12      268      0      0 2024-11-27 12:46:36 UTC+0000
0x87005ca0 svchost.exe           936    444     31      853      0      0 2024-11-27 12:46:36 UTC+0000
0x8701d550 svchost.exe          1028    444      5      104      0      0 2024-11-27 12:46:36 UTC+0000
0x87047340 svchost.exe          1148    444     14      353      0      0 2024-11-27 12:46:36 UTC+0000
0x870aa030 spoolsv.exe          1280    444     13      262      0      0 2024-11-27 12:46:37 UTC+0000
0x870bd450 svchost.exe          1324    444     20      320      0      0 2024-11-27 12:46:37 UTC+0000
0x87134030 taskhost.exe         1520    444      8      221      1      0 2024-11-27 12:46:37 UTC+0000
0x87151400 dwm.exe              1600    820      3       71      1      0 2024-11-27 12:46:37 UTC+0000
0x87156030 explorer.exe         1612   1588     31      940      1      0 2024-11-27 12:46:37 UTC+0000
0x871c2590 svchost.exe          1848    444      6       90      0      0 2024-11-27 12:46:38 UTC+0000
0x86e81398 SearchIndexer.       1632    444     13      646      0      0 2024-11-27 12:46:44 UTC+0000
0x91ab7700 notepad.exe          1592   1612      2       81      1      0 2024-11-27 12:47:10 UTC+0000
0x870f2750 mscorsvw.exe         1984    444      6       92      0      0 2024-11-27 12:51:39 UTC+0000
0x86f9f1f0 svchost.exe          1640    444      8      114      0      0 2024-11-27 12:51:39 UTC+0000
0x872a0d40 svchost.exe          1816    444      9      292      0      0 2024-11-27 12:51:40 UTC+0000
0x87139250 WmiPrvSE.exe         2256    576      7      109      0      0 2024-11-27 12:53:38 UTC+0000
0x854e2d40 audiodg.exe          2968    696      5      126      0      0 2024-11-27 13:00:02 UTC+0000
```

psscan


dbg_psscan.txt - Windows 메모장
파일(F) 편집(E) 서식(O) 보기(V) 도움말(H)

```
Offset(P)          Name                PID   PPID PDB        Time created                   Time exited
------------------ ---------------- ------ ------ ---------- ------------------------------ ------------------------------
0x000000001f93b828 svchost.exe         884    444 0x3ebc01c0 2024-11-27 12:46:36 UTC+0000
0x0000000021f32700 notepad.exe        1592   1612 0x3ebc0380 2024-11-27 12:47:10 UTC+0000
0x00000000235d72e0 lsm.exe             460    340 0x3ebc0100 2024-11-27 12:46:35 UTC+0000
0x000000003de3fd40 svchost.exe        1816    444 0x3ebc0300 2024-11-27 12:51:40 UTC+0000
0x000000003dfa4ca0 svchost.exe         936    444 0x3ebc01e0 2024-11-27 12:46:36 UTC+0000
0x000000003dfbc550 svchost.exe        1028    444 0x3ebc0220 2024-11-27 12:46:36 UTC+0000
0x000000003dfe6340 svchost.exe        1148    444 0x3ebc0240 2024-11-27 12:46:36 UTC+0000
0x000000003e049030 spoolsv.exe        1280    444 0x3ebc0260 2024-11-27 12:46:37 UTC+0000
0x000000003e05c450 svchost.exe        1324    444 0x3ebc0280 2024-11-27 12:46:37 UTC+0000
0x000000003e091750 mscorsvw.exe       1984    444 0x3ebc03c0 2024-11-27 12:51:39 UTC+0000
0x000000003e0d3030 taskhost.exe       1520    444 0x3ebc02e0 2024-11-27 12:46:37 UTC+0000
0x000000003e0d8250 WmiPrvSE.exe       2256    576 0x3ebc0460 2024-11-27 12:53:38 UTC+0000
0x000000003e0f0400 dwm.exe            1600    820 0x3ebc0320 2024-11-27 12:46:37 UTC+0000
0x000000003e0f5030 explorer.exe       1612   1588 0x3ebc0340 2024-11-27 12:46:37 UTC+0000
0x000000003e161590 svchost.exe        1848    444 0x3ebc0360 2024-11-27 12:46:38 UTC+0000
0x000000003e21f688 csrss.exe           292    280 0x3ebc0060 2024-11-27 12:46:35 UTC+0000
0x000000003e220398 SearchIndexer.     1632    444 0x3ebc02a0 2024-11-27 12:46:44 UTC+0000
0x000000003e25b868 csrss.exe           348    332 0x3ebc0040 2024-11-27 12:46:35 UTC+0000
0x000000003e277d40 winlogon.exe        380    332 0x3ebc00c0 2024-11-27 12:46:35 UTC+0000
0x000000003e28d420 services.exe        444    340 0x3ebc0080 2024-11-27 12:46:35 UTC+0000
0x000000003e29e0f0 lsass.exe           452    340 0x3ebc00e0 2024-11-27 12:46:35 UTC+0000
0x000000003e303c48 svchost.exe         576    444 0x3ebc0120 2024-11-27 12:46:36 UTC+0000
0x000000003e321838 svchost.exe         644    444 0x3ebc0140 2024-11-27 12:46:36 UTC+0000
0x000000003e339d40 svchost.exe         696    444 0x3ebc0160 2024-11-27 12:46:36 UTC+0000
0x000000003e33e1f0 svchost.exe        1640    444 0x3ebc0180 2024-11-27 12:51:39 UTC+0000
0x000000003e37c188 svchost.exe         820    444 0x3ebc01a0 2024-11-27 12:46:36 UTC+0000
0x000000003eb512d8 smss.exe            224      4 0x3ebc0020 2024-11-27 12:46:34 UTC+0000
0x000000003f5581e0 calc.exe           1344   1612 0x3ebc03e0 2024-11-27 12:47:08 UTC+0000
0x000000003fc81d40 audiodg.exe        2968    696 0x3ebc03a0 2024-11-27 13:00:02 UTC+0000
0x000000003fea1a00 wininit.exe         340    280 0x3ebc00a0 2024-11-27 12:46:35 UTC+0000
0x000000003ff0a958 System                4      0 0x00185000 2024-11-27 12:46:34 UTC+0000
```

pstree


dbg_pstree.txt - Windows 메모장
파일(F) 편집(E) 서식(O) 보기(V) 도움말(H)

```
Name                                                  Pid   PPid   Thds   Hnds Time
-------------------------------------------------- ------ ------ ------ ------ ----
 0x86e80688:csrss.exe                                 292    280      8    330 2024-11-27 12:46:35 UTC+0000
 0x853e2a00:wininit.exe                               340    280      4     74 2024-11-27 12:46:35 UTC+0000
. 0x86eee420:services.exe                             444    340      9    186 2024-11-27 12:46:35 UTC+0000
.. 0x870aa030:spoolsv.exe                            1280    444     13    262 2024-11-27 12:46:37 UTC+0000
.. 0x8701d550:svchost.exe                            1028    444      5    104 2024-11-27 12:46:36 UTC+0000
.. 0x872a0d40:svchost.exe                            1816    444      9    292 2024-11-27 12:51:40 UTC+0000
.. 0x86f82838:svchost.exe                             644    444      8    237 2024-11-27 12:46:36 UTC+0000
.. 0x87005ca0:svchost.exe                             936    444     31    853 2024-11-27 12:46:36 UTC+0000
.. 0x870bd450:svchost.exe                            1324    444     20    320 2024-11-27 12:46:37 UTC+0000
.. 0x86fdd188:svchost.exe                             820    444     17    419 2024-11-27 12:46:36 UTC+0000
... 0x87151400:dwm.exe                               1600    820      3     71 2024-11-27 12:46:37 UTC+0000
.. 0x86f9ad40:svchost.exe                             696    444     20    461 2024-11-27 12:46:36 UTC+0000
... 0x854e2d40:audiodg.exe                           2968    696      5    126 2024-11-27 13:00:02 UTC+0000
.. 0x86f64c48:svchost.exe                             576    444     10    342 2024-11-27 12:46:36 UTC+0000
... 0x87139250:WmiPrvSE.exe                          2256    576      7    109 2024-11-27 12:53:38 UTC+0000
.. 0x86e81398:SearchIndexer.                         1632    444     13    646 2024-11-27 12:46:44 UTC+0000
.. 0x871c2590:svchost.exe                            1848    444      6     90 2024-11-27 12:46:38 UTC+0000
.. 0x870f2750:mscorsvw.exe                           1984    444      6     92 2024-11-27 12:51:39 UTC+0000
.. 0x86f9f1f0:svchost.exe                            1640    444      8    114 2024-11-27 12:51:39 UTC+0000
.. 0x87134030:taskhost.exe                           1520    444      8    221 2024-11-27 12:46:37 UTC+0000
.. 0x9476d828:svchost.exe                             884    444     12    268 2024-11-27 12:46:36 UTC+0000
.. 0x87047340:svchost.exe                            1148    444     14    353 2024-11-27 12:46:36 UTC+0000
. 0x86eff0f0:lsass.exe                                452    340      7    526 2024-11-27 12:46:35 UTC+0000
. 0x903262e0:lsm.exe                                  460    340     10    138 2024-11-27 12:46:35 UTC+0000
 0x87156030:explorer.exe                             1612   1588     31    940 2024-11-27 12:46:37 UTC+0000
. 0x91ab7700:notepad.exe                             1592   1612      2     81 2024-11-27 12:47:10 UTC+0000
 0x86ebc868:csrss.exe                                 348    332      7    168 2024-11-27 12:46:35 UTC+0000
 0x86ed8d40:winlogon.exe                              380    332      4    108 2024-11-27 12:46:35 UTC+0000
 0x8534b958:System                                      4      0     74    484 2024-11-27 12:46:34 UTC+0000
. 0x867b22d8:smss.exe                                 224      4      2     29 2024-11-27 12:46:34 UTC+0000
```

결론

pslist, pstree에서는 계산기가 보이지 않고 psscan에서는 계산기가 보이므로 프로세스 은닉에 성공했다.