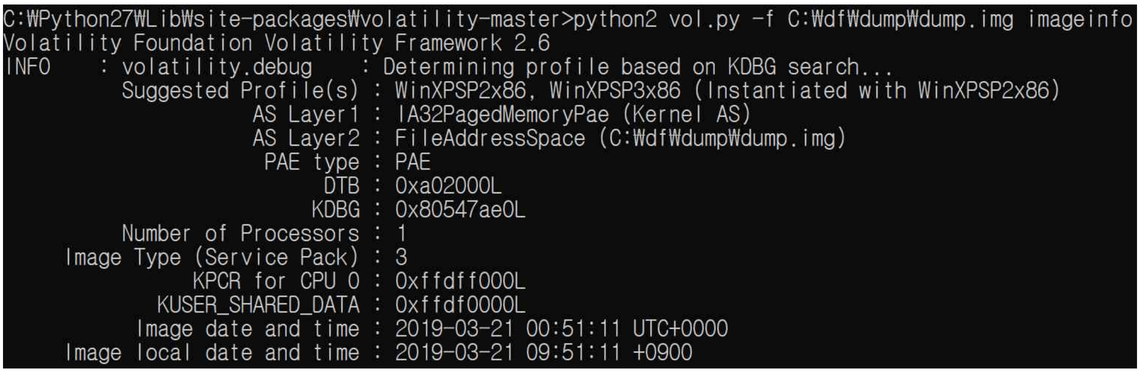
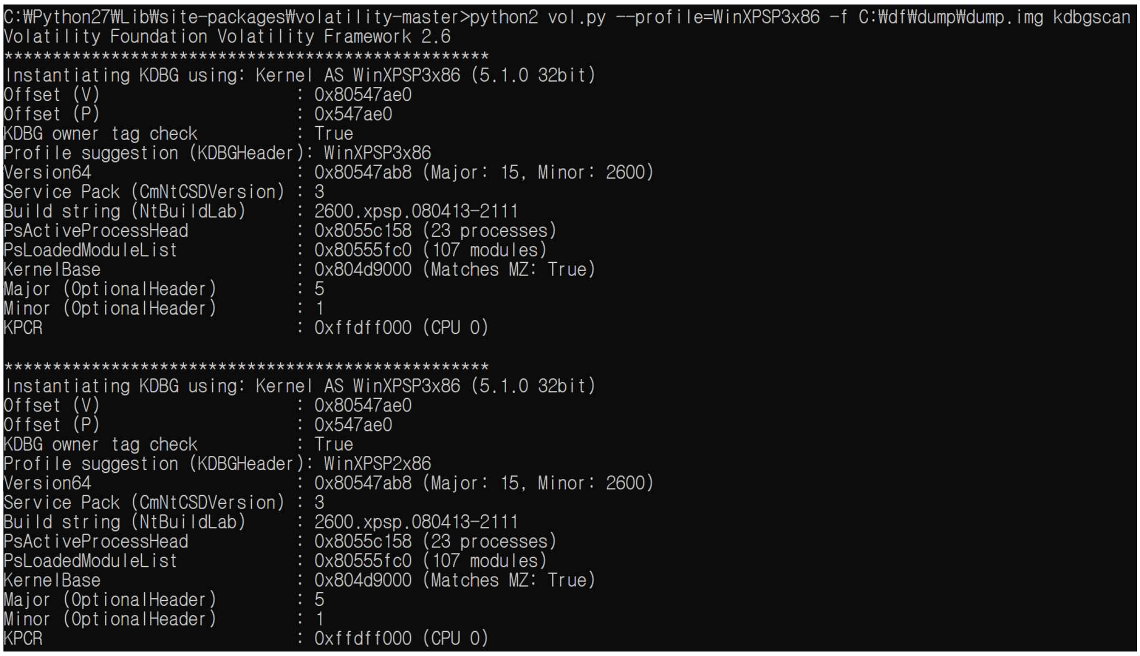
Image File의 System 정보



```
C:₩Python27₩Lib₩site-packages₩volatility-master>python2 vol.py -f C:₩df₩dump₩dump.img imageinfo
Volatility Foundation Volatility Framework 2.6
INFO    : volatility.debug    : Determining profile based on KDBG search...
          Suggested Profile(s) : WinXPSP2x86, WinXPSP3x86 (Instantiated with WinXPSP2x86)
                     AS Layer1 : IA32PagedMemoryPae (Kernel AS)
                     AS Layer2 : FileAddressSpace (C:₩df₩dump₩dump.img)
                      PAE type : PAE
                           DTB : 0xa02000L
                          KDBG : 0x80547ae0L
          Number of Processors : 1
     Image Type (Service Pack) : 3
                KPCR for CPU 0 : 0xffdff000L
             KUSER_SHARED_DATA : 0xffdf0000L
           Image date and time : 2019-03-21 00:51:11 UTC+0000
     Image local date and time : 2019-03-21 09:51:11 +0900
```

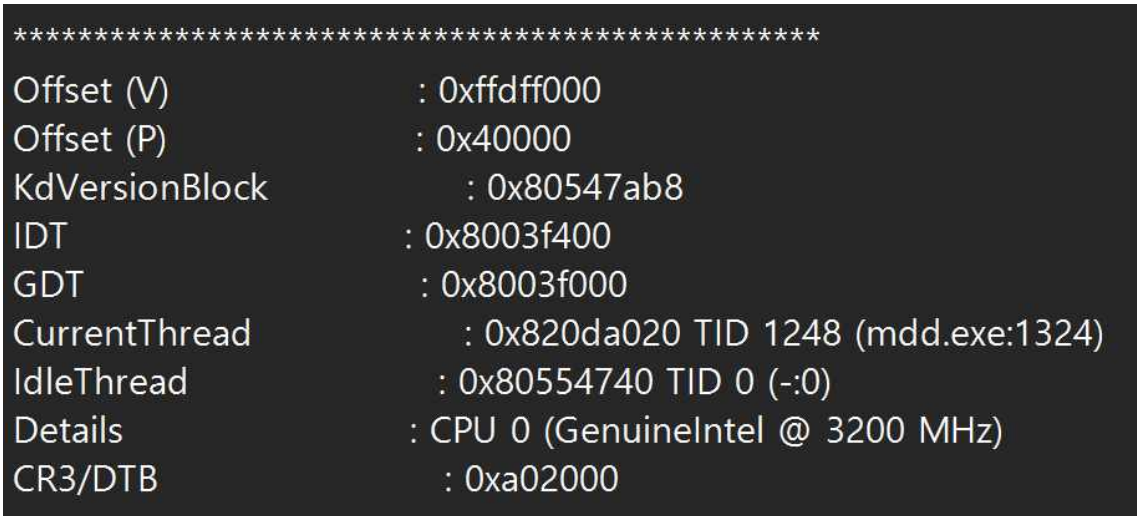
Image 정보

- kdbgscan



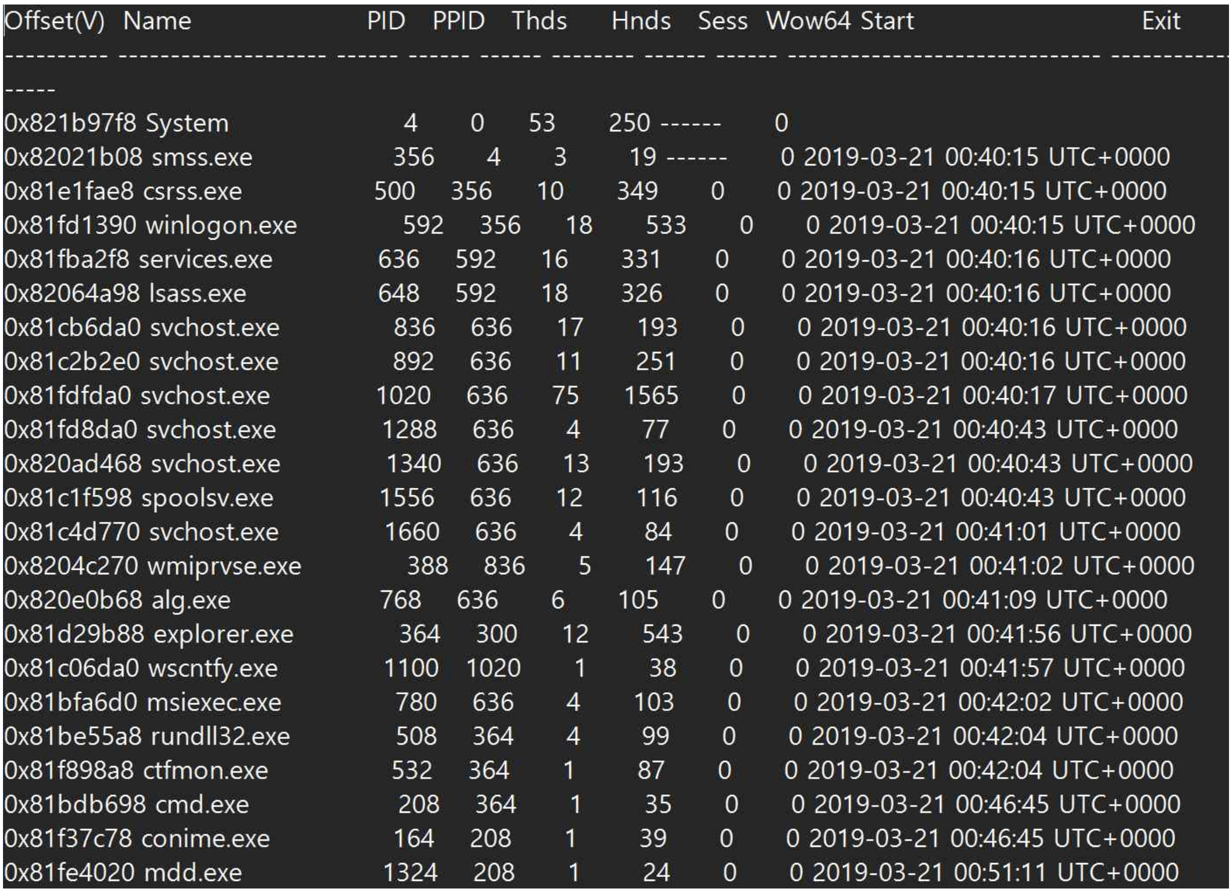
```
C:₩Python27₩Lib₩site-packages₩volatility-master>python2 vol.py --profile=WinXPSP3x86 -f C:₩df₩dump₩dump.img kdbgscan
Volatility Foundation Volatility Framework 2.6
**************************************************
Instantiating KDBG using: Kernel AS WinXPSP3x86 (5.1.0 32bit)
Offset (V)                    : 0x80547ae0
Offset (P)                    : 0x547ae0
KDBG owner tag check          : True
Profile suggestion (KDBGHeader): WinXPSP3x86
Version64                     : 0x80547ab8 (Major: 15, Minor: 2600)
Service Pack (CmNtCSDVersion) : 3
Build string (NtBuildLab)     : 2600.xpsp.080413-2111
PsActiveProcessHead           : 0x8055c158 (23 processes)
PsLoadedModuleList            : 0x80555fc0 (107 modules)
KernelBase                    : 0x804d9000 (Matches MZ: True)
Major (OptionalHeader)        : 5
Minor (OptionalHeader)        : 1
KPCR                          : 0xffdff000 (CPU 0)

**************************************************
Instantiating KDBG using: Kernel AS WinXPSP3x86 (5.1.0 32bit)
Offset (V)                    : 0x80547ae0
Offset (P)                    : 0x547ae0
KDBG owner tag check          : True
Profile suggestion (KDBGHeader): WinXPSP2x86
Version64                     : 0x80547ab8 (Major: 15, Minor: 2600)
Service Pack (CmNtCSDVersion) : 3
Build string (NtBuildLab)     : 2600.xpsp.080413-2111
PsActiveProcessHead           : 0x8055c158 (23 processes)
PsLoadedModuleList            : 0x80555fc0 (107 modules)
KernelBase                    : 0x804d9000 (Matches MZ: True)
Major (OptionalHeader)        : 5
Minor (OptionalHeader)        : 1
KPCR                          : 0xffdff000 (CPU 0)
```

- kprscan



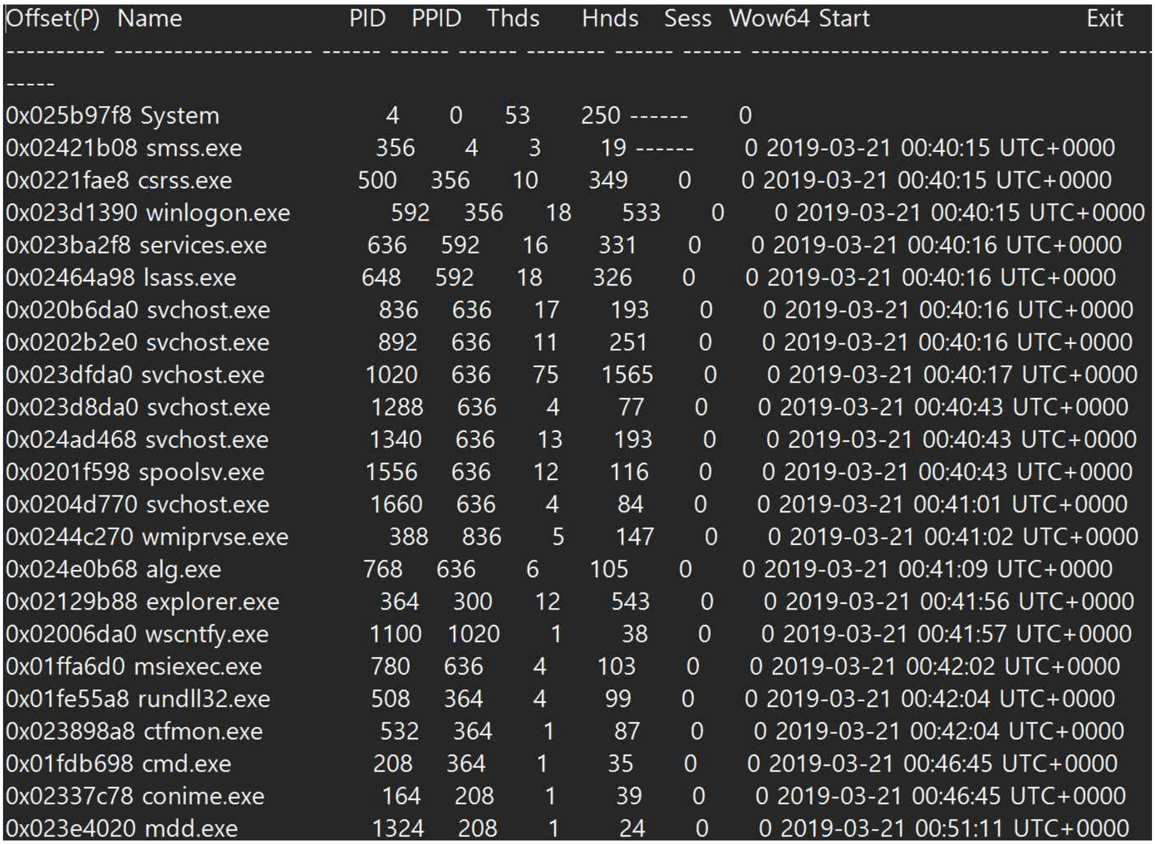
```
**************************************************
Offset (V)                    : 0xffdff000
Offset (P)                    : 0x40000
KdVersionBlock                : 0x80547ab8
IDT                           : 0x8003f400
GDT                           : 0x8003f000
CurrentThread                 : 0x820da020 TID 1248 (mdd.exe:1324)
IdleThread                    : 0x80554740 TID 0 (-:0)
Details                       : CPU 0 (GenuineIntel @ 3200 MHz)
CR3/DTB                       : 0xa02000
```

pslist



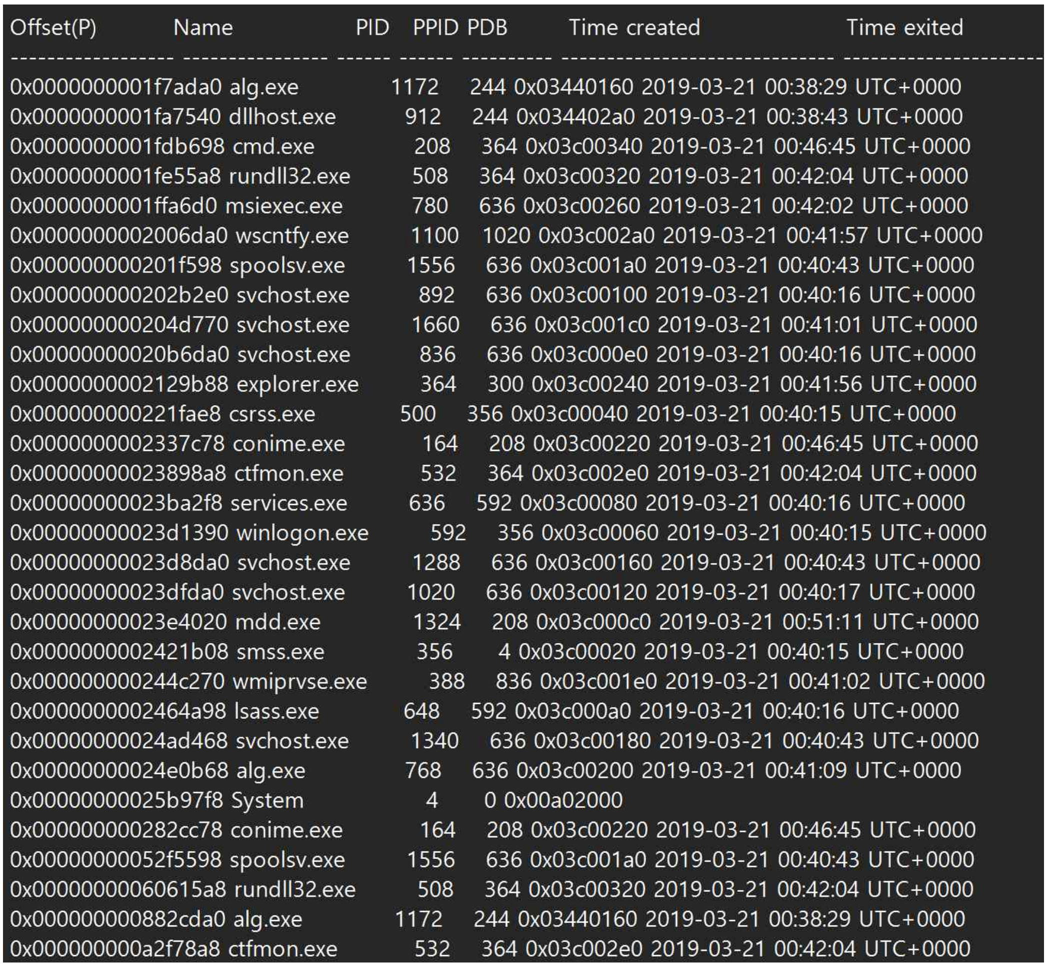
```
Offset(V)  Name                    PID   PPID   Thds     Hnds   Sess  Wow64 Start                          Exit
---------- -------------------- ------ ------ ------ -------- ------ ------ ------------------------------ -----------
-----
0x821b97f8 System                    4      0     53      250 ------      0
0x82021b08 smss.exe                356      4      3       19 ------      0 2019-03-21 00:40:15 UTC+0000
0x81e1fae8 csrss.exe               500    356     10      349      0      0 2019-03-21 00:40:15 UTC+0000
0x81fd1390 winlogon.exe            592    356     18      533      0      0 2019-03-21 00:40:15 UTC+0000
0x81fba2f8 services.exe            636    592     16      331      0      0 2019-03-21 00:40:16 UTC+0000
0x82064a98 lsass.exe               648    592     18      326      0      0 2019-03-21 00:40:16 UTC+0000
0x81cb6da0 svchost.exe             836    636     17      193      0      0 2019-03-21 00:40:16 UTC+0000
0x81c2b2e0 svchost.exe             892    636     11      251      0      0 2019-03-21 00:40:16 UTC+0000
0x81fdfda0 svchost.exe            1020    636     75     1565      0      0 2019-03-21 00:40:17 UTC+0000
0x81fd8da0 svchost.exe            1288    636      4       77      0      0 2019-03-21 00:40:43 UTC+0000
0x820ad468 svchost.exe            1340    636     13      193      0      0 2019-03-21 00:40:43 UTC+0000
0x81c1f598 spoolsv.exe            1556    636     12      116      0      0 2019-03-21 00:40:43 UTC+0000
0x81c4d770 svchost.exe            1660    636      4       84      0      0 2019-03-21 00:41:01 UTC+0000
0x8204c270 wmiprvse.exe            388    836      5      147      0      0 2019-03-21 00:41:02 UTC+0000
0x820e0b68 alg.exe                 768    636      6      105      0      0 2019-03-21 00:41:09 UTC+0000
0x81d29b88 explorer.exe            364    300     12      543      0      0 2019-03-21 00:41:56 UTC+0000
0x81c06da0 wscntfy.exe            1100   1020      1       38      0      0 2019-03-21 00:41:57 UTC+0000
0x81bfa6d0 msiexec.exe             780    636      4      103      0      0 2019-03-21 00:42:02 UTC+0000
0x81be55a8 rundll32.exe            508    364      4       99      0      0 2019-03-21 00:42:04 UTC+0000
0x81f898a8 ctfmon.exe              532    364      1       87      0      0 2019-03-21 00:42:04 UTC+0000
0x81bdb698 cmd.exe                 208    364      1       35      0      0 2019-03-21 00:46:45 UTC+0000
0x81f37c78 conime.exe              164    208      1       39      0      0 2019-03-21 00:46:45 UTC+0000
0x81fe4020 mdd.exe                1324    208      1       24      0      0 2019-03-21 00:51:11 UTC+0000
```

pslist -p



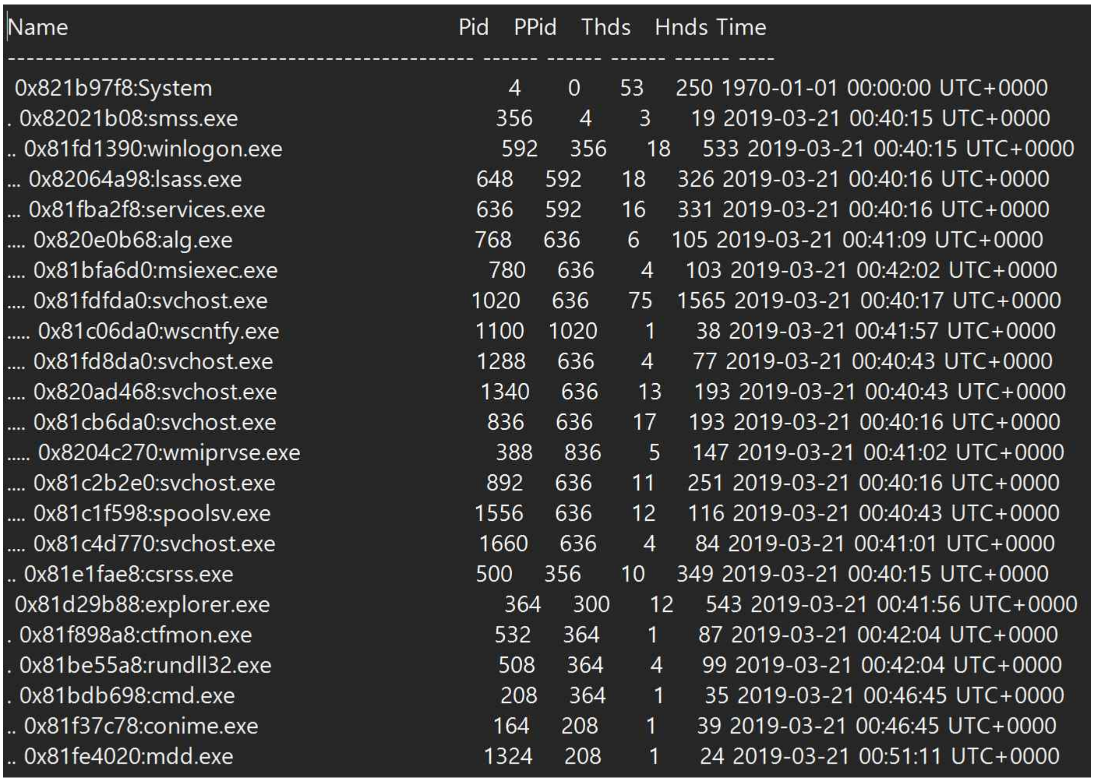
```
Offset(P)  Name                    PID   PPID   Thds     Hnds   Sess  Wow64 Start                          Exit
---------- -------------------- ------ ------ ------ -------- ------ ------ ------------------------------ ---------
-----
0x025b97f8 System                    4      0     53      250 ------      0
0x02421b08 smss.exe                356      4      3       19 ------      0 2019-03-21 00:40:15 UTC+0000
0x0221fae8 csrss.exe               500    356     10      349      0      0 2019-03-21 00:40:15 UTC+0000
0x023d1390 winlogon.exe            592    356     18      533      0      0 2019-03-21 00:40:15 UTC+0000
0x023ba2f8 services.exe            636    592     16      331      0      0 2019-03-21 00:40:16 UTC+0000
0x02464a98 lsass.exe               648    592     18      326      0      0 2019-03-21 00:40:16 UTC+0000
0x020b6da0 svchost.exe             836    636     17      193      0      0 2019-03-21 00:40:16 UTC+0000
0x0202b2e0 svchost.exe             892    636     11      251      0      0 2019-03-21 00:40:16 UTC+0000
0x023dfda0 svchost.exe            1020    636     75     1565      0      0 2019-03-21 00:40:17 UTC+0000
0x023d8da0 svchost.exe            1288    636      4       77      0      0 2019-03-21 00:40:43 UTC+0000
0x024ad468 svchost.exe            1340    636     13      193      0      0 2019-03-21 00:40:43 UTC+0000
0x0201f598 spoolsv.exe            1556    636     12      116      0      0 2019-03-21 00:40:43 UTC+0000
0x0204d770 svchost.exe            1660    636      4       84      0      0 2019-03-21 00:41:01 UTC+0000
0x0244c270 wmiprvse.exe            388    836      5      147      0      0 2019-03-21 00:41:02 UTC+0000
0x024e0b68 alg.exe                 768    636      6      105      0      0 2019-03-21 00:41:09 UTC+0000
0x02129b88 explorer.exe            364    300     12      543      0      0 2019-03-21 00:41:56 UTC+0000
0x02006da0 wscntfy.exe            1100   1020      1       38      0      0 2019-03-21 00:41:57 UTC+0000
0x01ffa6d0 msiexec.exe             780    636      4      103      0      0 2019-03-21 00:42:02 UTC+0000
0x01fe55a8 rundll32.exe            508    364      4       99      0      0 2019-03-21 00:42:04 UTC+0000
0x023898a8 ctfmon.exe              532    364      1       87      0      0 2019-03-21 00:42:04 UTC+0000
0x01fdb698 cmd.exe                 208    364      1       35      0      0 2019-03-21 00:46:45 UTC+0000
0x02337c78 conime.exe              164    208      1       39      0      0 2019-03-21 00:46:45 UTC+0000
0x023e4020 mdd.exe                1324    208      1       24      0      0 2019-03-21 00:51:11 UTC+0000
```

psscan



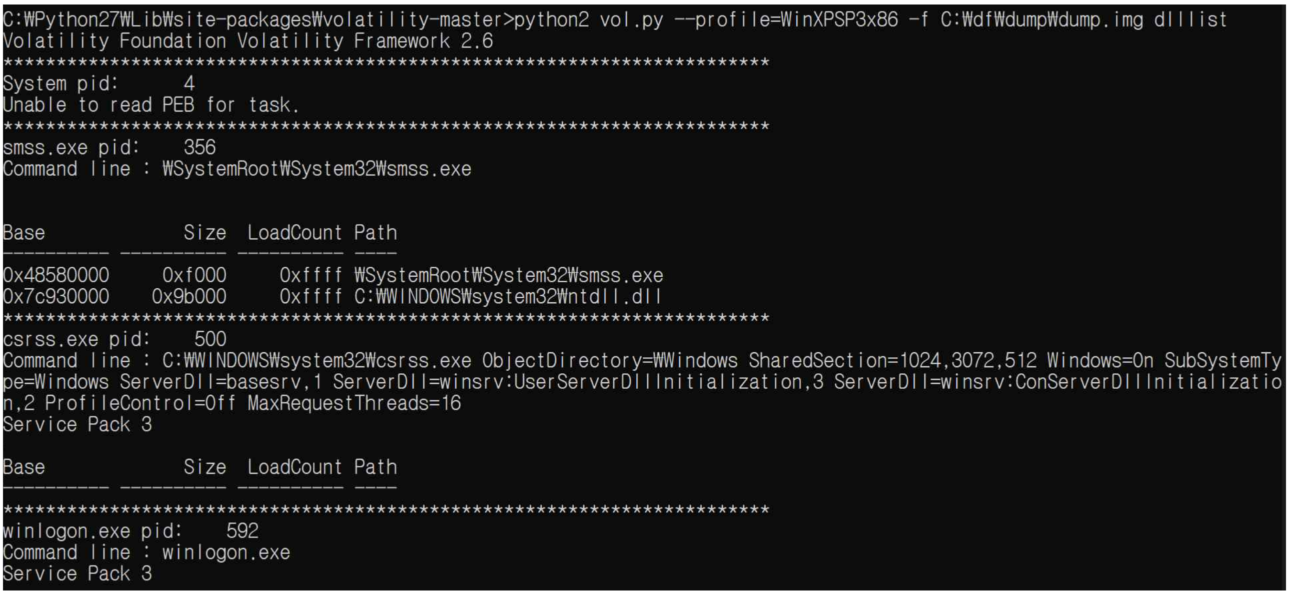
```
Offset(P)          Name                PID   PPID PDB        Time created                 Time exited
------------------ ---------------- ------ ------ ---------- ---------------------------- ----------------------
0x000000001f7ada0 alg.exe            1172    244 0x03440160 2019-03-21 00:38:29 UTC+0000
0x000000001fa7540 dllhost.exe         912    244 0x034402a0 2019-03-21 00:38:43 UTC+0000
0x000000001fdb698 cmd.exe             208    364 0x03c00340 2019-03-21 00:46:45 UTC+0000
0x000000001fe55a8 rundll32.exe        508    364 0x03c00320 2019-03-21 00:42:04 UTC+0000
0x000000001ffa6d0 msiexec.exe         780    636 0x03c00260 2019-03-21 00:42:02 UTC+0000
0x0000000002006da0 wscntfy.exe       1100   1020 0x03c002a0 2019-03-21 00:41:57 UTC+0000
0x000000000201f598 spoolsv.exe       1556    636 0x03c001a0 2019-03-21 00:40:43 UTC+0000
0x000000000202b2e0 svchost.exe        892    636 0x03c00100 2019-03-21 00:40:16 UTC+0000
0x000000000204d770 svchost.exe       1660    636 0x03c001c0 2019-03-21 00:41:01 UTC+0000
0x00000000020b6da0 svchost.exe        836    636 0x03c000e0 2019-03-21 00:40:16 UTC+0000
0x0000000002129b88 explorer.exe       364    300 0x03c00240 2019-03-21 00:41:56 UTC+0000
0x000000000221fae8 csrss.exe          500    356 0x03c00040 2019-03-21 00:40:15 UTC+0000
0x0000000002337c78 conime.exe         164    208 0x03c00220 2019-03-21 00:46:45 UTC+0000
0x00000000023898a8 ctfmon.exe         532    364 0x03c002e0 2019-03-21 00:42:04 UTC+0000
0x00000000023ba2f8 services.exe       636    592 0x03c00080 2019-03-21 00:40:16 UTC+0000
0x00000000023d1390 winlogon.exe       592    356 0x03c00060 2019-03-21 00:40:15 UTC+0000
0x00000000023d8da0 svchost.exe       1288    636 0x03c00160 2019-03-21 00:40:43 UTC+0000
0x00000000023dfda0 svchost.exe       1020    636 0x03c00120 2019-03-21 00:40:17 UTC+0000
0x00000000023e4020 mdd.exe           1324    208 0x03c000c0 2019-03-21 00:51:11 UTC+0000
0x0000000002421b08 smss.exe           356      4 0x03c00020 2019-03-21 00:40:15 UTC+0000
0x000000000244c270 wmiprvse.exe       388    836 0x03c001e0 2019-03-21 00:41:02 UTC+0000
0x0000000002464a98 lsass.exe          648    592 0x03c000a0 2019-03-21 00:40:16 UTC+0000
0x00000000024ad468 svchost.exe       1340    636 0x03c00180 2019-03-21 00:40:43 UTC+0000
0x00000000024e0b68 alg.exe            768    636 0x03c00200 2019-03-21 00:41:09 UTC+0000
0x00000000025b97f8 System               4      0 0x00a02000
0x000000000282cc78 conime.exe         164    208 0x03c00220 2019-03-21 00:46:45 UTC+0000
0x00000000052f5598 spoolsv.exe       1556    636 0x03c001a0 2019-03-21 00:40:43 UTC+0000
0x00000000060615a8 rundll32.exe       508    364 0x03c00320 2019-03-21 00:42:04 UTC+0000
0x000000000882cda0 alg.exe           1172    244 0x03440160 2019-03-21 00:38:29 UTC+0000
0x000000000a2f78a8 ctfmon.exe         532    364 0x03c002e0 2019-03-21 00:42:04 UTC+0000
```

pstree



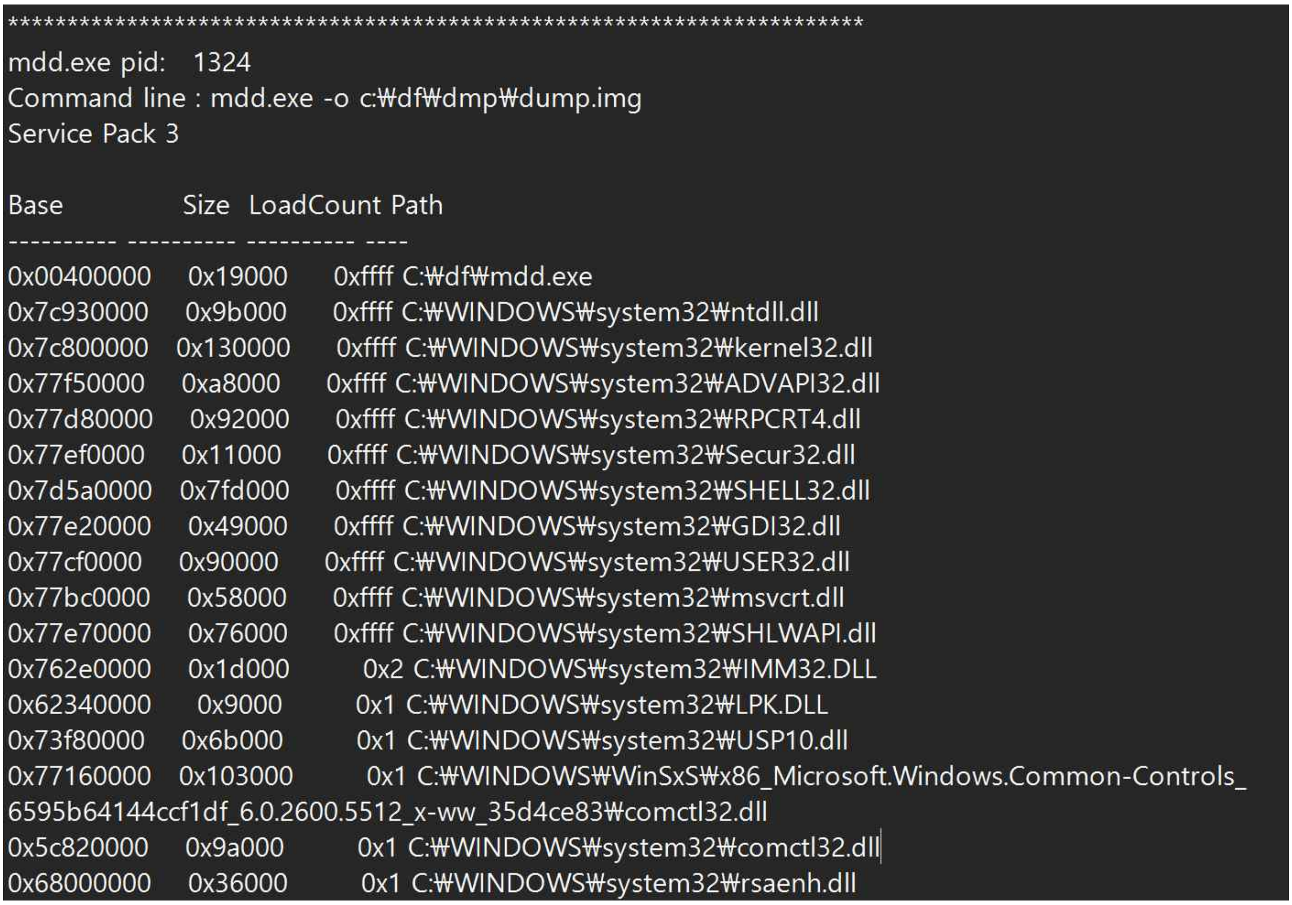
```
Name                                                  Pid   PPid   Thds   Hnds Time
-------------------------------------------------- ------ ------ ------ ------ ----
 0x821b97f8:System                                      4      0     53    250 1970-01-01 00:00:00 UTC+0000
. 0x82021b08:smss.exe                                 356      4      3     19 2019-03-21 00:40:15 UTC+0000
.. 0x81fd1390:winlogon.exe                            592    356     18    533 2019-03-21 00:40:15 UTC+0000
... 0x82064a98:lsass.exe                              648    592     18    326 2019-03-21 00:40:16 UTC+0000
... 0x81fba2f8:services.exe                           636    592     16    331 2019-03-21 00:40:16 UTC+0000
.... 0x820e0b68:alg.exe                               768    636      6    105 2019-03-21 00:41:09 UTC+0000
.... 0x81bfa6d0:msiexec.exe                           780    636      4    103 2019-03-21 00:42:02 UTC+0000
.... 0x81fdfda0:svchost.exe                          1020    636     75   1565 2019-03-21 00:40:17 UTC+0000
..... 0x81c06da0:wscntfy.exe                         1100   1020      1     38 2019-03-21 00:41:57 UTC+0000
.... 0x81fd8da0:svchost.exe                          1288    636      4     77 2019-03-21 00:40:43 UTC+0000
.... 0x820ad468:svchost.exe                          1340    636     13    193 2019-03-21 00:40:43 UTC+0000
.... 0x81cb6da0:svchost.exe                           836    636     17    193 2019-03-21 00:40:16 UTC+0000
..... 0x8204c270:wmiprvse.exe                         388    836      5    147 2019-03-21 00:41:02 UTC+0000
.... 0x81c2b2e0:svchost.exe                           892    636     11    251 2019-03-21 00:40:16 UTC+0000
.... 0x81c1f598:spoolsv.exe                          1556    636     12    116 2019-03-21 00:40:43 UTC+0000
.... 0x81c4d770:svchost.exe                          1660    636      4     84 2019-03-21 00:41:01 UTC+0000
.. 0x81e1fae8:csrss.exe                               500    356     10    349 2019-03-21 00:40:15 UTC+0000
 0x81d29b88:explorer.exe                              364    300     12    543 2019-03-21 00:41:56 UTC+0000
. 0x81f898a8:ctfmon.exe                               532    364      1     87 2019-03-21 00:42:04 UTC+0000
. 0x81be55a8:rundll32.exe                             508    364      4     99 2019-03-21 00:42:04 UTC+0000
. 0x81bdb698:cmd.exe                                  208    364      1     35 2019-03-21 00:46:45 UTC+0000
.. 0x81f37c78:conime.exe                              164    208      1     39 2019-03-21 00:46:45 UTC+0000
.. 0x81fe4020:mdd.exe                                1324    208      1     24 2019-03-21 00:51:11 UTC+0000
```

dlllist



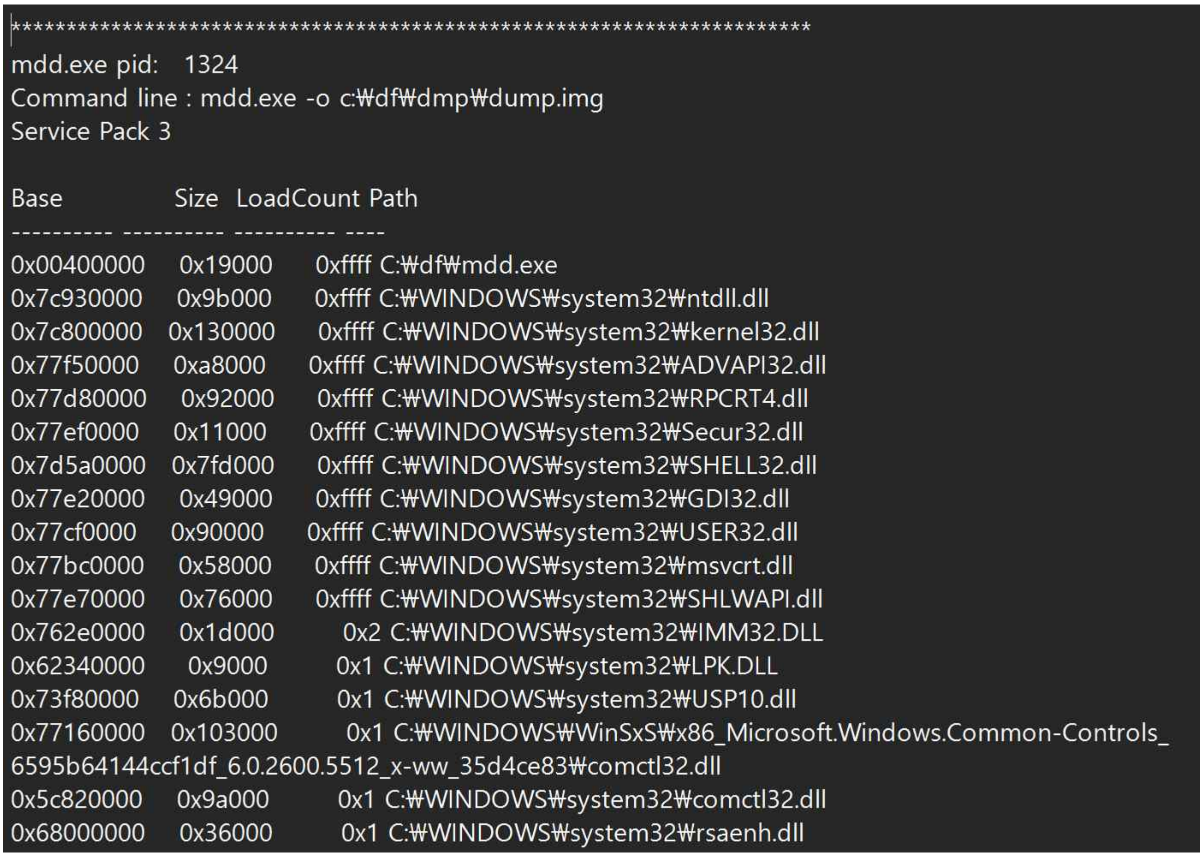
```
C:₩Python27₩Lib₩site-packages₩volatility-master>python2 vol.py --profile=WinXPSP3x86 -f C:₩df₩dump₩dump.img dlllist
Volatility Foundation Volatility Framework 2.6
************************************************************************
System pid:      4
Unable to read PEB for task.
************************************************************************
smss.exe pid:    356
Command line : ₩SystemRoot₩System32₩smss.exe


Base             Size  LoadCount Path
---------- ---------- ---------- ----
0x48580000     0xf000     0xffff ₩SystemRoot₩System32₩smss.exe
0x7c930000    0x9b000     0xffff C:₩WINDOWS₩system32₩ntdll.dll
************************************************************************
csrss.exe pid:    500
Command line : C:₩WINDOWS₩system32₩csrss.exe ObjectDirectory=₩Windows SharedSection=1024,3072,512 Windows=On SubSystemTy
pe=Windows ServerDll=basesrv,1 ServerDll=winsrv:UserServerDllInitialization,3 ServerDll=winsrv:ConServerDllInitializatio
n,2 ProfileControl=Off MaxRequestThreads=16
Service Pack 3

Base             Size  LoadCount Path
---------- ---------- ---------- ----

************************************************************************
winlogon.exe pid:    592
Command line : winlogon.exe
Service Pack 3
```

dlllist pid 1324



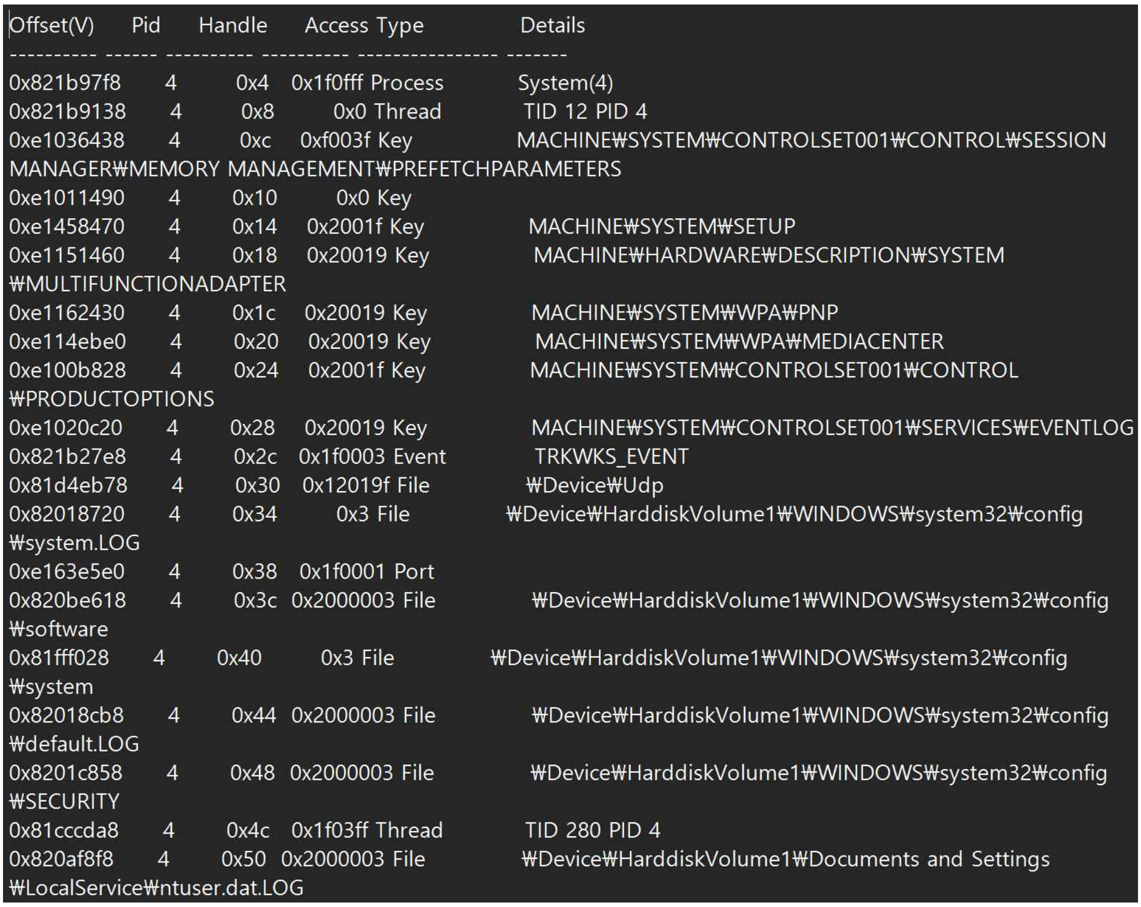
```
************************************************************************
mdd.exe pid:   1324
Command line : mdd.exe -o c:₩df₩dmp₩dump.img
Service Pack 3

Base             Size  LoadCount Path
---------- ---------- ---------- ----
0x00400000    0x19000     0xffff C:₩df₩mdd.exe
0x7c930000    0x9b000     0xffff C:₩WINDOWS₩system32₩ntdll.dll
0x7c800000   0x130000     0xffff C:₩WINDOWS₩system32₩kernel32.dll
0x77f50000    0xa8000     0xffff C:₩WINDOWS₩system32₩ADVAPI32.dll
0x77d80000    0x92000     0xffff C:₩WINDOWS₩system32₩RPCRT4.dll
0x77ef0000    0x11000     0xffff C:₩WINDOWS₩system32₩Secur32.dll
0x7d5a0000    0x7fd000    0xffff C:₩WINDOWS₩system32₩SHELL32.dll
0x77e20000    0x49000     0xffff C:₩WINDOWS₩system32₩GDI32.dll
0x77cf0000    0x90000     0xffff C:₩WINDOWS₩system32₩USER32.dll
0x77bc0000    0x58000     0xffff C:₩WINDOWS₩system32₩msvcrt.dll
0x77e70000    0x76000     0xffff C:₩WINDOWS₩system32₩SHLWAPI.dll
0x762e0000    0x1d000        0x2 C:₩WINDOWS₩system32₩IMM32.DLL
0x62340000     0x9000        0x1 C:₩WINDOWS₩system32₩LPK.DLL
0x73f80000    0x6b000        0x1 C:₩WINDOWS₩system32₩USP10.dll
0x77160000   0x103000        0x1 C:₩WINDOWS₩WinSxS₩x86_Microsoft.Windows.Common-Controls_
6595b64144ccf1df_6.0.2600.5512_x-ww_35d4ce83₩comctl32.dll
0x5c820000    0x9a000        0x1 C:₩WINDOWS₩system32₩comctl32.dll
0x68000000    0x36000        0x1 C:₩WINDOWS₩system32₩rsaenh.dll
```

dlllist offset



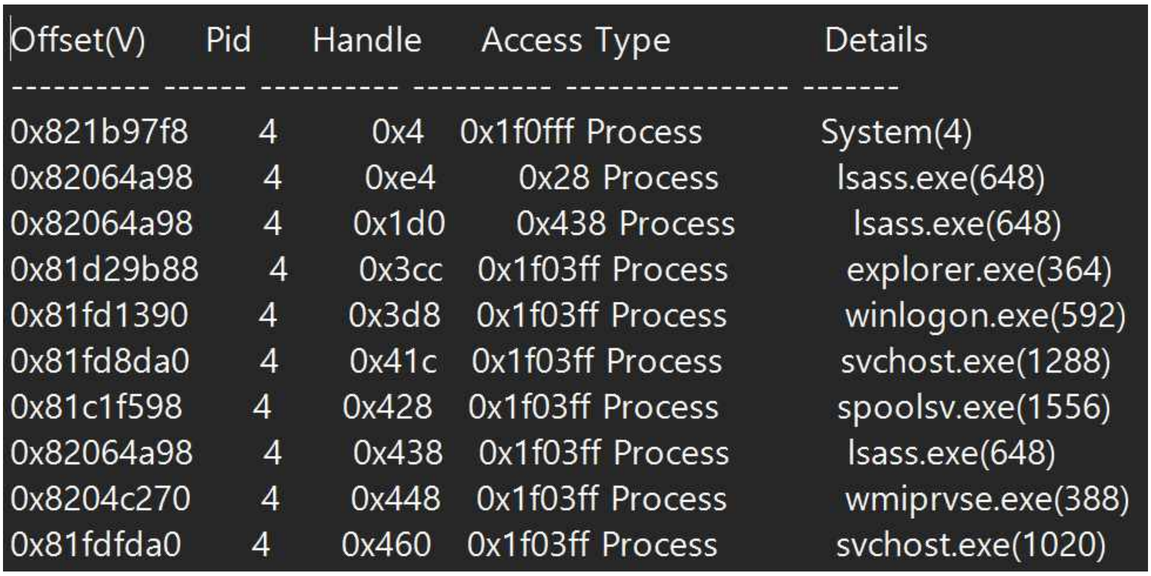
```
************************************************************************
mdd.exe pid:   1324
Command line : mdd.exe -o c:₩df₩dmp₩dump.img
Service Pack 3

Base             Size  LoadCount Path
---------- ---------- ---------- ----
0x00400000    0x19000     0xffff C:₩df₩mdd.exe
0x7c930000    0x9b000     0xffff C:₩WINDOWS₩system32₩ntdll.dll
0x7c800000   0x130000     0xffff C:₩WINDOWS₩system32₩kernel32.dll
0x77f50000    0xa8000     0xffff C:₩WINDOWS₩system32₩ADVAPI32.dll
0x77d80000    0x92000     0xffff C:₩WINDOWS₩system32₩RPCRT4.dll
0x77ef0000    0x11000     0xffff C:₩WINDOWS₩system32₩Secur32.dll
0x7d5a0000    0x7fd000    0xffff C:₩WINDOWS₩system32₩SHELL32.dll
0x77e20000    0x49000     0xffff C:₩WINDOWS₩system32₩GDI32.dll
0x77cf0000    0x90000     0xffff C:₩WINDOWS₩system32₩USER32.dll
0x77bc0000    0x58000     0xffff C:₩WINDOWS₩system32₩msvcrt.dll
0x77e70000    0x76000     0xffff C:₩WINDOWS₩system32₩SHLWAPI.dll
0x762e0000    0x1d000        0x2 C:₩WINDOWS₩system32₩IMM32.DLL
0x62340000     0x9000        0x1 C:₩WINDOWS₩system32₩LPK.DLL
0x73f80000    0x6b000        0x1 C:₩WINDOWS₩system32₩USP10.dll
0x77160000   0x103000        0x1 C:₩WINDOWS₩WinSxS₩x86_Microsoft.Windows.Common-Controls_
6595b64144ccf1df_6.0.2600.5512_x-ww_35d4ce83₩comctl32.dll
0x5c820000    0x9a000        0x1 C:₩WINDOWS₩system32₩comctl32.dll
0x68000000    0x36000        0x1 C:₩WINDOWS₩system32₩rsaenh.dll
```

handles



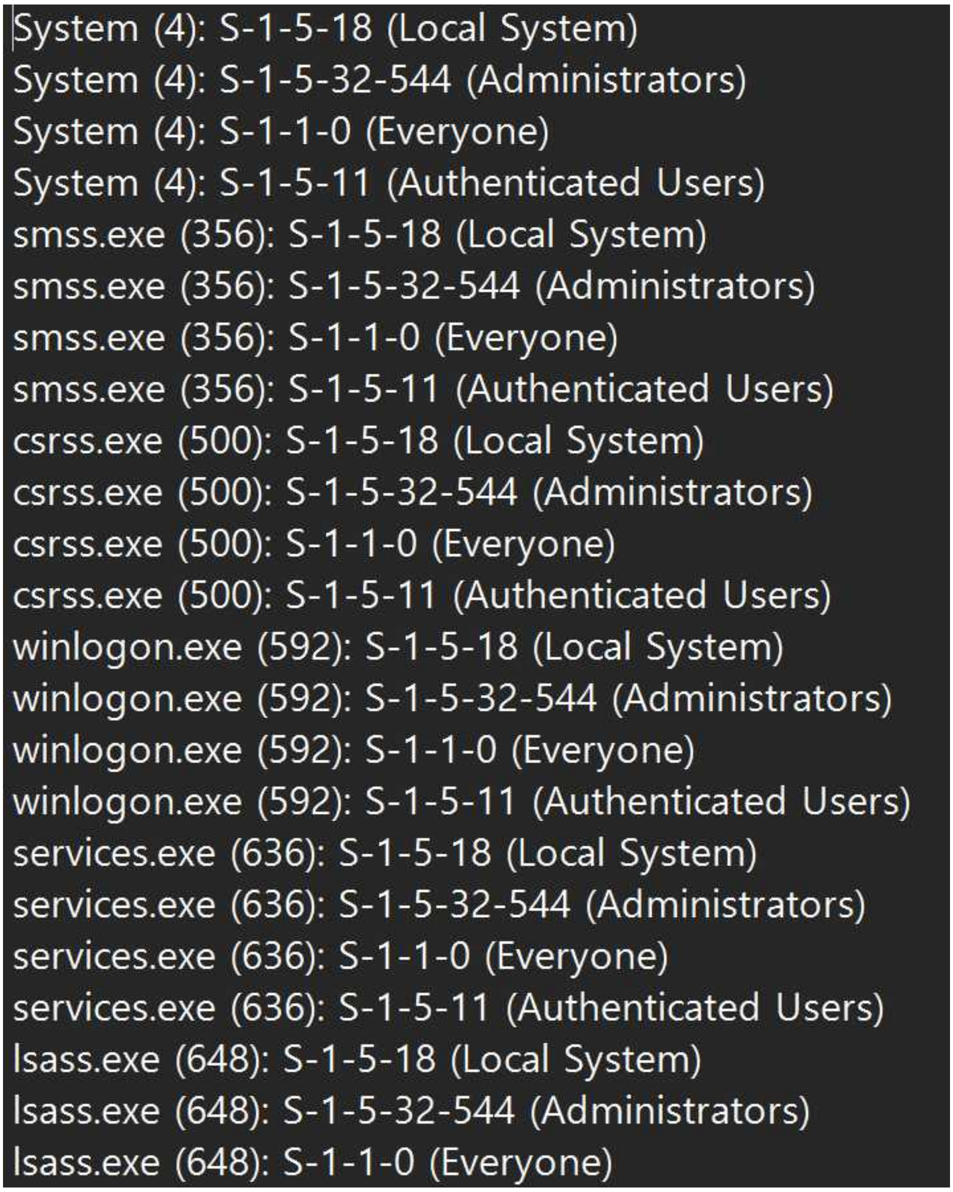
```
Offset(V)     Pid     Handle     Access Type             Details
---------- ------ ---------- ---------- ---------------- -------
0x821b97f8      4        0x4   0x1f0fff Process          System(4)
0x821b9138      4        0x8        0x0 Thread           TID 12 PID 4
0xe1036438      4        0xc   0xf003f Key               MACHINE₩SYSTEM₩CONTROLSET001₩CONTROL₩SESSION
MANAGER₩MEMORY MANAGEMENT₩PREFETCHPARAMETERS
0xe1011490      4       0x10        0x0 Key
0xe1458470      4       0x14    0x2001f Key              MACHINE₩SYSTEM₩SETUP
0xe1151460      4       0x18    0x20019 Key              MACHINE₩HARDWARE₩DESCRIPTION₩SYSTEM
₩MULTIFUNCTIONADAPTER
0xe1162430      4       0x1c    0x20019 Key              MACHINE₩SYSTEM₩WPA₩PNP
0xe114ebe0      4       0x20    0x20019 Key              MACHINE₩SYSTEM₩WPA₩MEDIACENTER
0xe100b828      4       0x24    0x2001f Key              MACHINE₩SYSTEM₩CONTROLSET001₩CONTROL
₩PRODUCTOPTIONS
0xe1020c20      4       0x28    0x20019 Key              MACHINE₩SYSTEM₩CONTROLSET001₩SERVICES₩EVENTLOG
0x821b27e8      4       0x2c   0x1f0003 Event            TRKWKS_EVENT
0x81d4eb78      4       0x30   0x12019f File             ₩Device₩Udp
0x82018720      4       0x34        0x3 File             ₩Device₩HarddiskVolume1₩WINDOWS₩system32₩config
₩system.LOG
0xe163e5e0      4       0x38   0x1f0001 Port
0x820be618      4       0x3c  0x2000003 File             ₩Device₩HarddiskVolume1₩WINDOWS₩system32₩config
₩software
0x81fff028      4       0x40        0x3 File             ₩Device₩HarddiskVolume1₩WINDOWS₩system32₩config
₩system
0x82018cb8      4       0x44  0x2000003 File             ₩Device₩HarddiskVolume1₩WINDOWS₩system32₩config
₩default.LOG
0x8201c858      4       0x48  0x2000003 File             ₩Device₩HarddiskVolume1₩WINDOWS₩system32₩config
₩SECURITY
0x81cccda8      4       0x4c   0x1f03ff Thread           TID 280 PID 4
0x820af8f8      4       0x50  0x2000003 File             ₩Device₩HarddiskVolume1₩Documents and Settings
₩LocalService₩ntuser.dat.LOG
```

handles -p



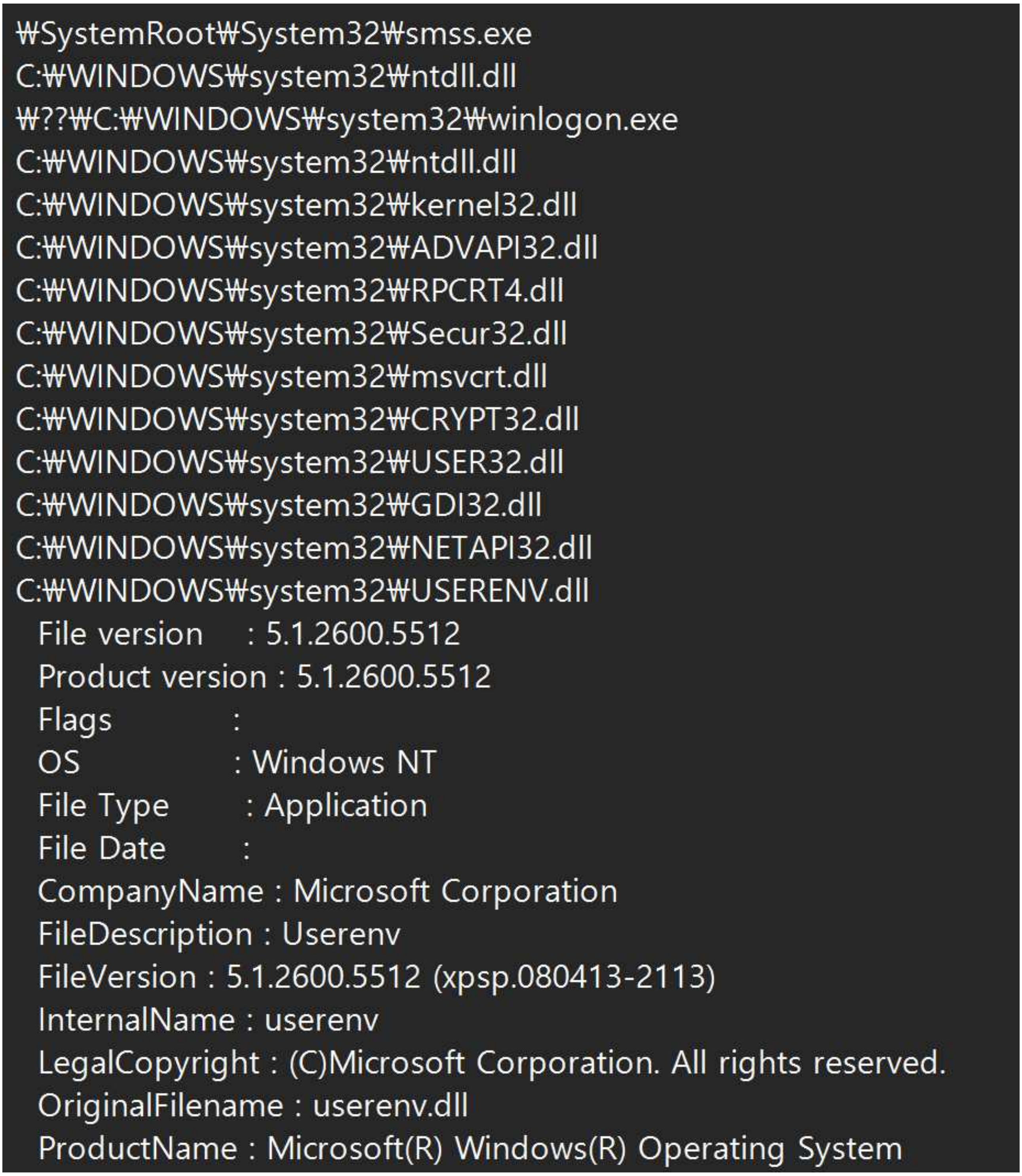
```
Offset(V)     Pid     Handle     Access Type             Details
---------- ------ ---------- ---------- ---------------- -------
0x821b97f8      4        0x4   0x1f0fff Process           System(4)
0x82064a98      4       0xe4       0x28 Process           lsass.exe(648)
0x82064a98      4      0x1d0      0x438 Process           lsass.exe(648)
0x81d29b88      4      0x3cc   0x1f03ff Process           explorer.exe(364)
0x81fd1390      4      0x3d8   0x1f03ff Process           winlogon.exe(592)
0x81fd8da0      4      0x41c   0x1f03ff Process           svchost.exe(1288)
0x81c1f598      4      0x428   0x1f03ff Process           spoolsv.exe(1556)
0x82064a98      4      0x438   0x1f03ff Process           lsass.exe(648)
0x8204c270      4      0x448   0x1f03ff Process           wmiprvse.exe(388)
0x81fdfda0      4      0x460   0x1f03ff Process           svchost.exe(1020)
```

getsids



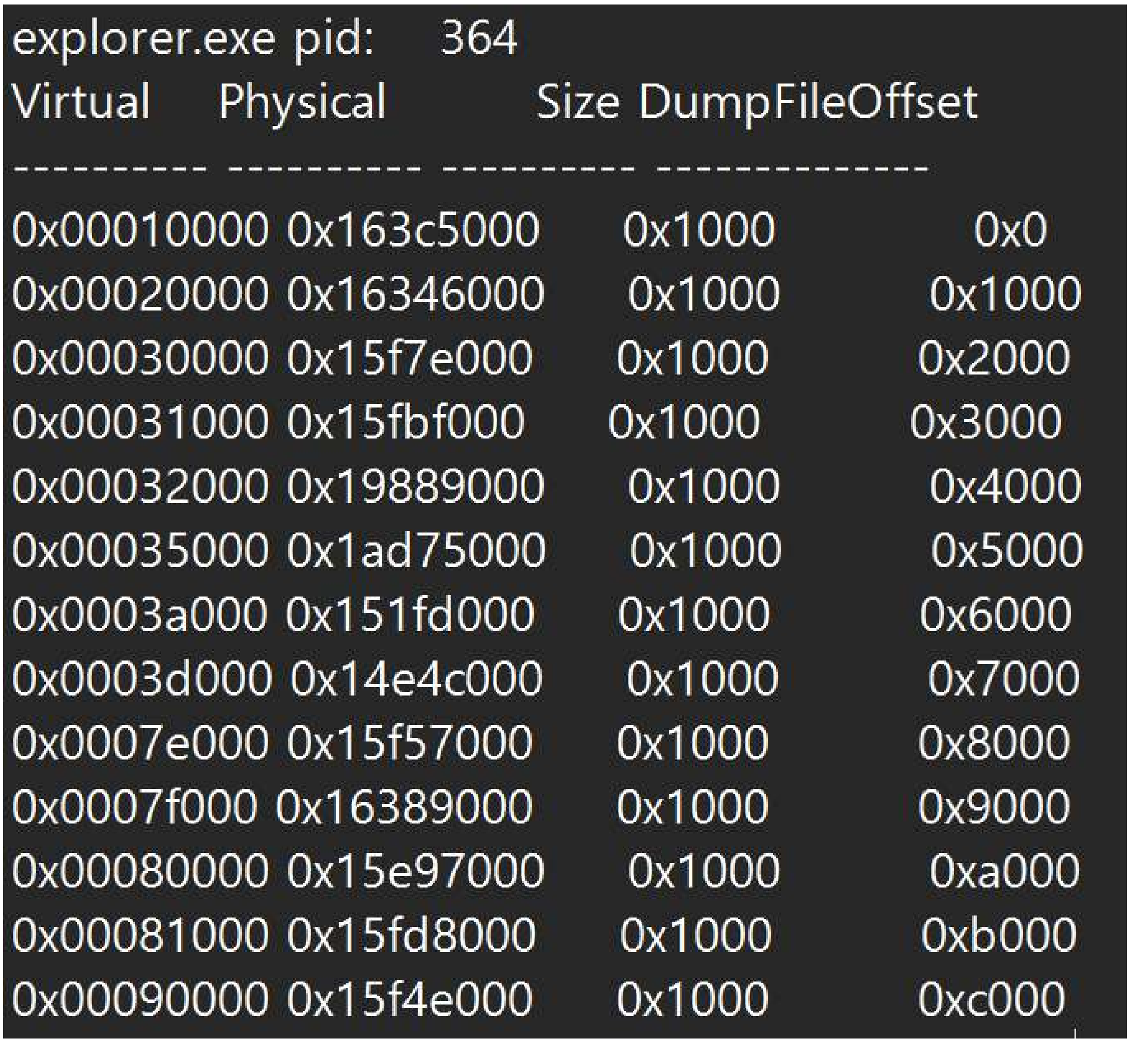
```
System (4): S-1-5-18 (Local System)
System (4): S-1-5-32-544 (Administrators)
System (4): S-1-1-0 (Everyone)
System (4): S-1-5-11 (Authenticated Users)
smss.exe (356): S-1-5-18 (Local System)
smss.exe (356): S-1-5-32-544 (Administrators)
smss.exe (356): S-1-1-0 (Everyone)
smss.exe (356): S-1-5-11 (Authenticated Users)
csrss.exe (500): S-1-5-18 (Local System)
csrss.exe (500): S-1-5-32-544 (Administrators)
csrss.exe (500): S-1-1-0 (Everyone)
csrss.exe (500): S-1-5-11 (Authenticated Users)
winlogon.exe (592): S-1-5-18 (Local System)
winlogon.exe (592): S-1-5-32-544 (Administrators)
winlogon.exe (592): S-1-1-0 (Everyone)
winlogon.exe (592): S-1-5-11 (Authenticated Users)
services.exe (636): S-1-5-18 (Local System)
services.exe (636): S-1-5-32-544 (Administrators)
services.exe (636): S-1-1-0 (Everyone)
services.exe (636): S-1-5-11 (Authenticated Users)
lsass.exe (648): S-1-5-18 (Local System)
lsass.exe (648): S-1-5-32-544 (Administrators)
lsass.exe (648): S-1-1-0 (Everyone)
```

verinfo



```
₩SystemRoot₩System32₩smss.exe
C:₩WINDOWS₩system32₩ntdll.dll
₩??₩C:₩WINDOWS₩system32₩winlogon.exe
C:₩WINDOWS₩system32₩ntdll.dll
C:₩WINDOWS₩system32₩kernel32.dll
C:₩WINDOWS₩system32₩ADVAPI32.dll
C:₩WINDOWS₩system32₩RPCRT4.dll
C:₩WINDOWS₩system32₩Secur32.dll
C:₩WINDOWS₩system32₩msvcrt.dll
C:₩WINDOWS₩system32₩CRYPT32.dll
C:₩WINDOWS₩system32₩USER32.dll
C:₩WINDOWS₩system32₩GDI32.dll
C:₩WINDOWS₩system32₩NETAPI32.dll
C:₩WINDOWS₩system32₩USERENV.dll
  File version    : 5.1.2600.5512
  Product version : 5.1.2600.5512
  Flags           :
  OS              : Windows NT
  File Type       : Application
  File Date       :
  CompanyName : Microsoft Corporation
  FileDescription : Userenv
  FileVersion : 5.1.2600.5512 (xpsp.080413-2113)
  InternalName : userenv
  LegalCopyright : (C)Microsoft Corporation. All rights reserved.
  OriginalFilename : userenv.dll
  ProductName : Microsoft(R) Windows(R) Operating System
```

memmap pid 364

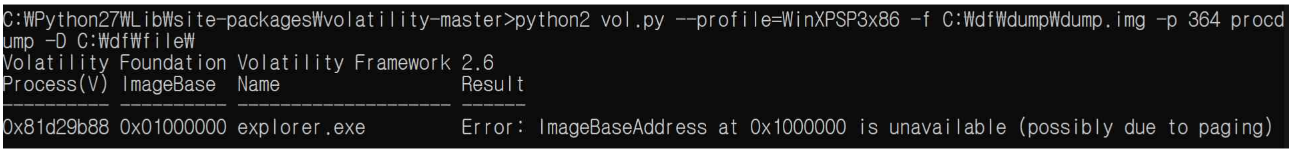


```
explorer.exe pid:     364
Virtual    Physical          Size DumpFileOffset
---------- ---------- ---------- --------------
0x00010000 0x163c5000     0x1000            0x0
0x00020000 0x16346000     0x1000         0x1000
0x00030000 0x15f7e000     0x1000         0x2000
0x00031000 0x15fbf000     0x1000         0x3000
0x00032000 0x19889000     0x1000         0x4000
0x00035000 0x1ad75000     0x1000         0x5000
0x0003a000 0x151fd000     0x1000         0x6000
0x0003d000 0x14e4c000     0x1000         0x7000
0x0007e000 0x15f57000     0x1000         0x8000
0x0007f000 0x16389000     0x1000         0x9000
0x00080000 0x15e97000     0x1000         0xa000
0x00081000 0x15fd8000     0x1000         0xb000
0x00090000 0x15f4e000     0x1000         0xc000
```

memdump 364 dump

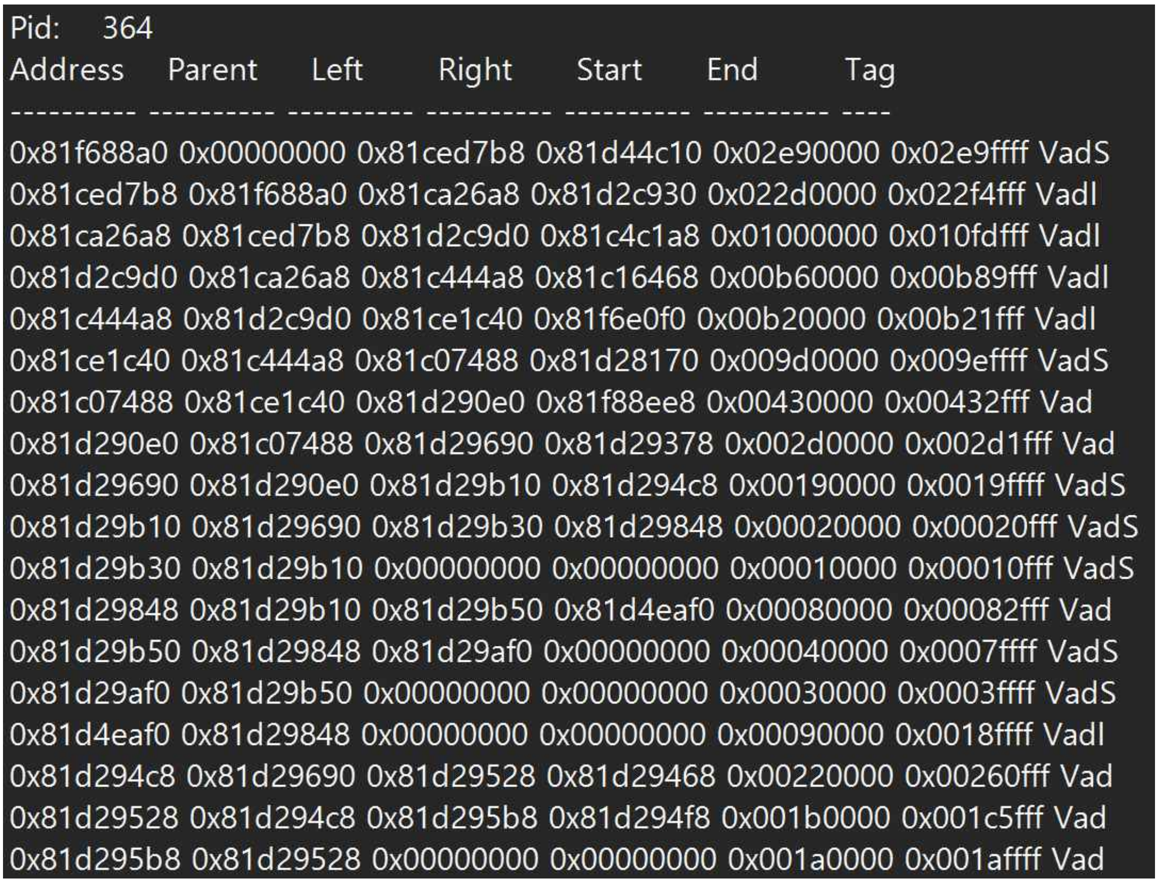
364.dmp

procdump



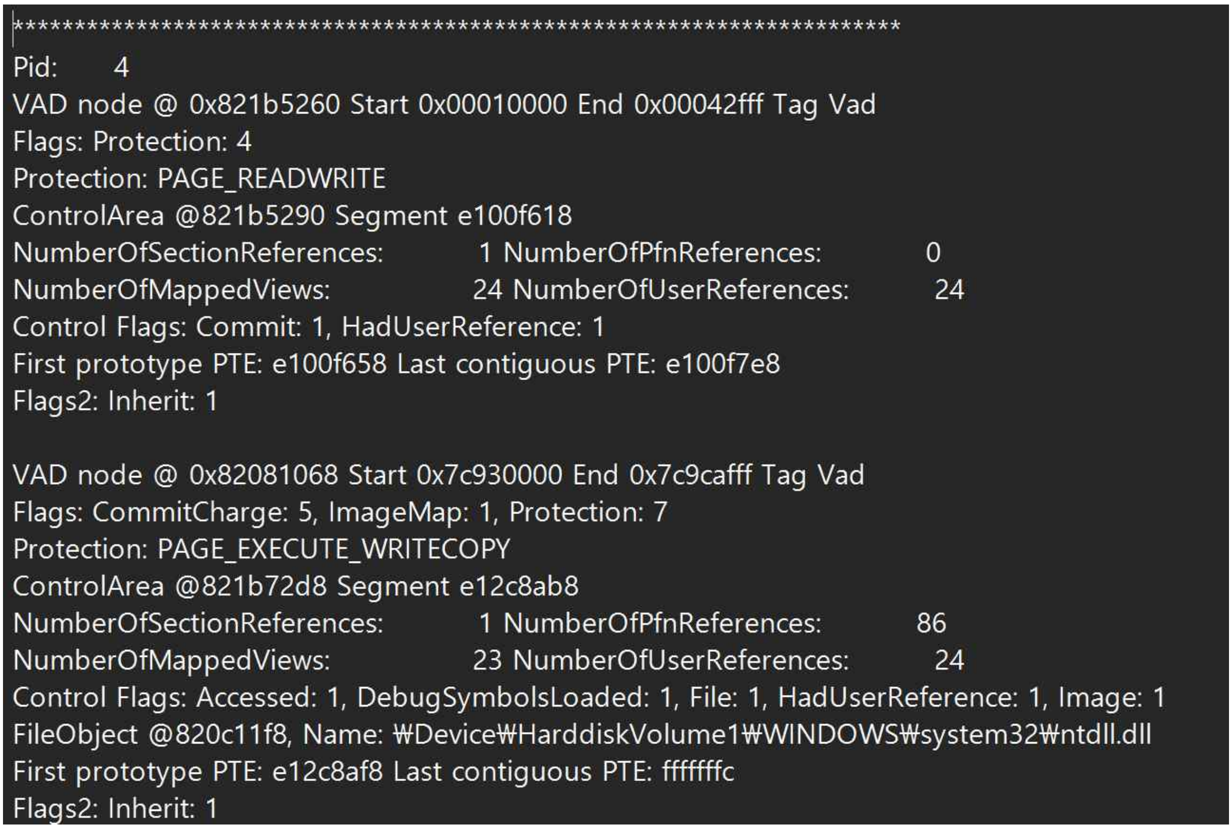
```
C:WPython27WLibWsite-packagesWvolatility-master>python2 vol.py --profile=WinXPSP3x86 -f C:WdfWdumpWdump.img -p 364 procd
ump -D C:WdfWfileW
Volatility Foundation Volatility Framework 2.6
Process(V) ImageBase  Name                 Result
---------- ---------- -------------------- ------
0x81d29b88 0x01000000 explorer.exe         Error: ImageBaseAddress at 0x1000000 is unavailable (possibly due to paging)
```

vadinfo



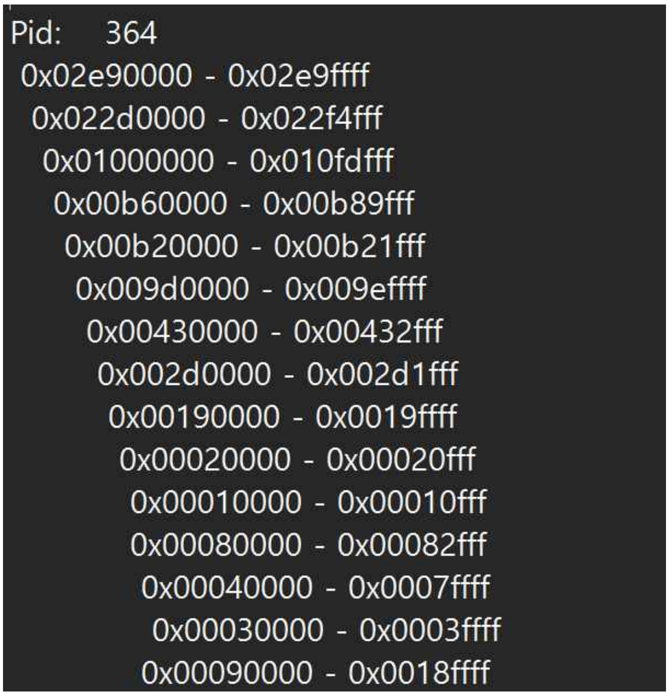
```
Pid:     364
Address     Parent     Left       Right      Start      End        Tag
---------- ---------- ---------- ---------- ---------- ---------- ----
0x81f688a0 0x00000000 0x81ced7b8 0x81d44c10 0x02e90000 0x02e9ffff VadS
0x81ced7b8 0x81f688a0 0x81ca26a8 0x81d2c930 0x022d0000 0x022f4fff Vadl
0x81ca26a8 0x81ced7b8 0x81d2c9d0 0x81c4c1a8 0x01000000 0x010fdfff Vadl
0x81d2c9d0 0x81ca26a8 0x81c444a8 0x81c16468 0x00b60000 0x00b89fff Vadl
0x81c444a8 0x81d2c9d0 0x81ce1c40 0x81f6e0f0 0x00b20000 0x00b21fff Vadl
0x81ce1c40 0x81c444a8 0x81c07488 0x81d28170 0x009d0000 0x009effff VadS
0x81c07488 0x81ce1c40 0x81d290e0 0x81f88ee8 0x00430000 0x00432fff Vad
0x81d290e0 0x81c07488 0x81d29690 0x81d29378 0x002d0000 0x002d1fff Vad
0x81d29690 0x81d290e0 0x81d29b10 0x81d294c8 0x00190000 0x0019ffff VadS
0x81d29b10 0x81d29690 0x81d29b30 0x81d29848 0x00020000 0x00020fff VadS
0x81d29b30 0x81d29b10 0x00000000 0x00000000 0x00010000 0x00010fff VadS
0x81d29848 0x81d29b10 0x81d29b50 0x81d4eaf0 0x00080000 0x00082fff Vad
0x81d29b50 0x81d29848 0x81d29af0 0x00000000 0x00040000 0x0007ffff VadS
0x81d29af0 0x81d29b50 0x00000000 0x00000000 0x00030000 0x0003ffff VadS
0x81d4eaf0 0x81d29848 0x00000000 0x00000000 0x00090000 0x0018ffff Vadl
0x81d294c8 0x81d29690 0x81d29528 0x81d29468 0x00220000 0x00260fff Vad
0x81d29528 0x81d294c8 0x81d295b8 0x81d294f8 0x001b0000 0x001c5fff Vad
0x81d295b8 0x81d29528 0x00000000 0x00000000 0x001a0000 0x001affff Vad
```

vadwalk



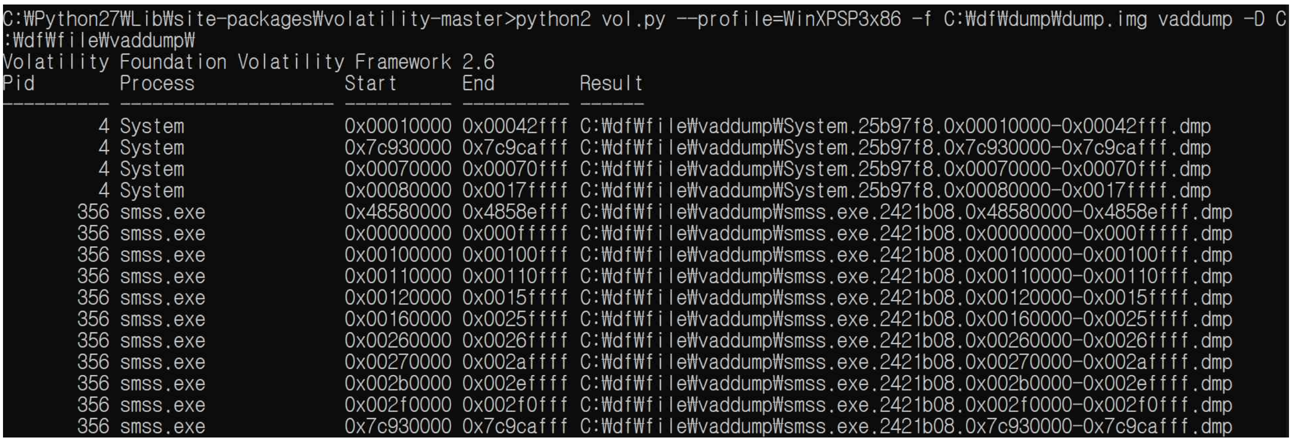
```
************************************************************************
Pid:       4
VAD node @ 0x821b5260 Start 0x00010000 End 0x00042fff Tag Vad
Flags: Protection: 4
Protection: PAGE_READWRITE
ControlArea @821b5290 Segment e100f618
NumberOfSectionReferences:          1 NumberOfPfnReferences:           0
NumberOfMappedViews:               24 NumberOfUserReferences:         24
Control Flags: Commit: 1, HadUserReference: 1
First prototype PTE: e100f658 Last contiguous PTE: e100f7e8
Flags2: Inherit: 1

VAD node @ 0x82081068 Start 0x7c930000 End 0x7c9cafff Tag Vad
Flags: CommitCharge: 5, ImageMap: 1, Protection: 7
Protection: PAGE_EXECUTE_WRITECOPY
ControlArea @821b72d8 Segment e12c8ab8
NumberOfSectionReferences:          1 NumberOfPfnReferences:          86
NumberOfMappedViews:               23 NumberOfUserReferences:         24
Control Flags: Accessed: 1, DebugSymbolsLoaded: 1, File: 1, HadUserReference: 1, Image: 1
FileObject @820c11f8, Name: ₩Device₩HarddiskVolume1₩WINDOWS₩system32₩ntdll.dll
First prototype PTE: e12c8af8 Last contiguous PTE: fffffffc
Flags2: Inherit: 1
```

vadtree



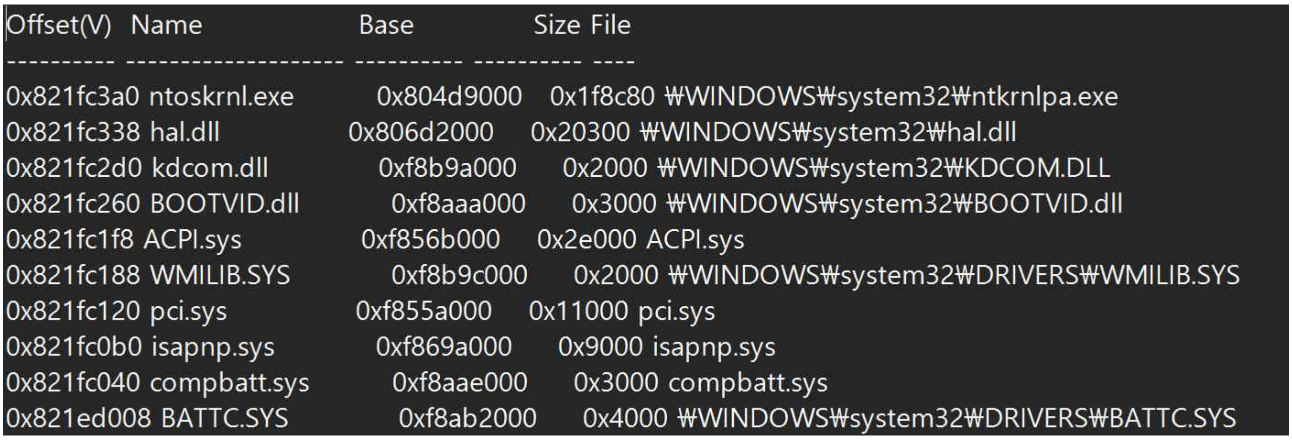
```
Pid:    364
 0x02e90000 - 0x02e9ffff
  0x022d0000 - 0x022f4fff
   0x01000000 - 0x010fdfff
    0x00b60000 - 0x00b89fff
     0x00b20000 - 0x00b21fff
      0x009d0000 - 0x009effff
       0x00430000 - 0x00432fff
        0x002d0000 - 0x002d1fff
         0x00190000 - 0x0019ffff
          0x00020000 - 0x00020fff
           0x00010000 - 0x00010fff
           0x00080000 - 0x00082fff
            0x00040000 - 0x0007ffff
             0x00030000 - 0x0003ffff
            0x00090000 - 0x0018ffff
```

vaddump



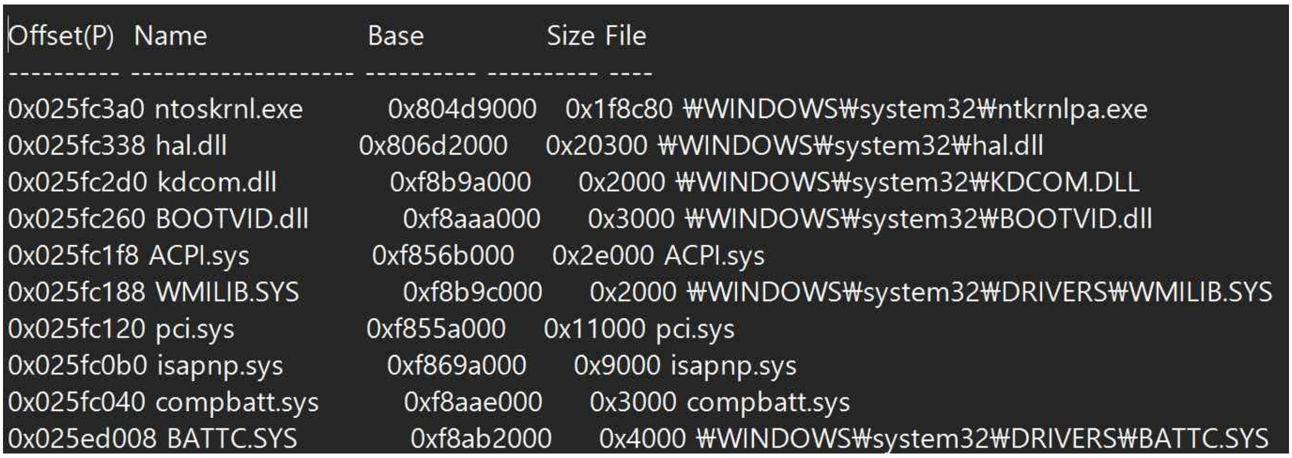
```
C:₩Python27₩Lib₩site-packages₩volatility-master>python2 vol.py --profile=WinXPSP3x86 -f C:₩df₩dump₩dump.img vaddump -D C
:₩df₩file₩vaddump₩
Volatility Foundation Volatility Framework 2.6
Pid        Process              Start      End        Result
---------- -------------------- ---------- ---------- ------
         4 System               0x00010000 0x00042fff C:₩df₩file₩vaddump₩System.25b97f8.0x00010000-0x00042fff.dmp
         4 System               0x7c930000 0x7c9cafff C:₩df₩file₩vaddump₩System.25b97f8.0x7c930000-0x7c9cafff.dmp
         4 System               0x00070000 0x00070fff C:₩df₩file₩vaddump₩System.25b97f8.0x00070000-0x00070fff.dmp
         4 System               0x00080000 0x0017ffff C:₩df₩file₩vaddump₩System.25b97f8.0x00080000-0x0017ffff.dmp
       356 smss.exe             0x48580000 0x4858efff C:₩df₩file₩vaddump₩smss.exe.2421b08.0x48580000-0x4858efff.dmp
       356 smss.exe             0x00000000 0x000fffff C:₩df₩file₩vaddump₩smss.exe.2421b08.0x00000000-0x000fffff.dmp
       356 smss.exe             0x00100000 0x00100fff C:₩df₩file₩vaddump₩smss.exe.2421b08.0x00100000-0x00100fff.dmp
       356 smss.exe             0x00110000 0x00110fff C:₩df₩file₩vaddump₩smss.exe.2421b08.0x00110000-0x00110fff.dmp
       356 smss.exe             0x00120000 0x0015ffff C:₩df₩file₩vaddump₩smss.exe.2421b08.0x00120000-0x0015ffff.dmp
       356 smss.exe             0x00160000 0x0025ffff C:₩df₩file₩vaddump₩smss.exe.2421b08.0x00160000-0x0025ffff.dmp
       356 smss.exe             0x00260000 0x0026ffff C:₩df₩file₩vaddump₩smss.exe.2421b08.0x00260000-0x0026ffff.dmp
       356 smss.exe             0x00270000 0x002affff C:₩df₩file₩vaddump₩smss.exe.2421b08.0x00270000-0x002affff.dmp
       356 smss.exe             0x002b0000 0x002effff C:₩df₩file₩vaddump₩smss.exe.2421b08.0x002b0000-0x002effff.dmp
       356 smss.exe             0x002f0000 0x002f0fff C:₩df₩file₩vaddump₩smss.exe.2421b08.0x002f0000-0x002f0fff.dmp
       356 smss.exe             0x7c930000 0x7c9cafff C:₩df₩file₩vaddump₩smss.exe.2421b08.0x7c930000-0x7c9cafff.dmp
```

modules(v)



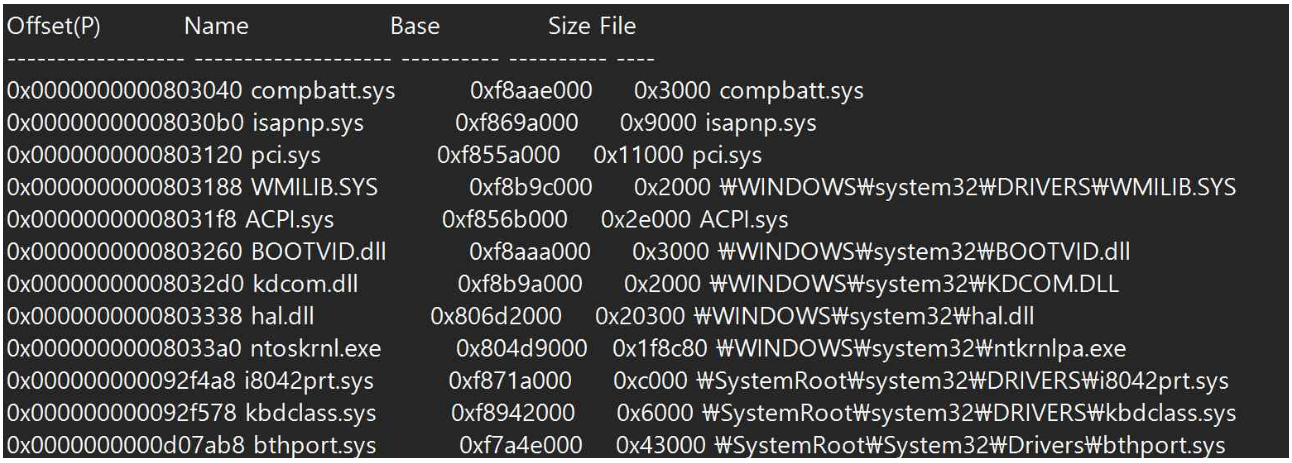
```
Offset(V)  Name                 Base       Size File
---------- -------------------- ---------- ---------- ----
0x821fc3a0 ntoskrnl.exe         0x804d9000   0x1f8c80 ₩WINDOWS₩system32₩ntkrnlpa.exe
0x821fc338 hal.dll              0x806d2000    0x20300 ₩WINDOWS₩system32₩hal.dll
0x821fc2d0 kdcom.dll            0xf8b9a000     0x2000 ₩WINDOWS₩system32₩KDCOM.DLL
0x821fc260 BOOTVID.dll          0xf8aaa000     0x3000 ₩WINDOWS₩system32₩BOOTVID.dll
0x821fc1f8 ACPI.sys             0xf856b000    0x2e000 ACPI.sys
0x821fc188 WMILIB.SYS           0xf8b9c000     0x2000 ₩WINDOWS₩system32₩DRIVERS₩WMILIB.SYS
0x821fc120 pci.sys              0xf855a000    0x11000 pci.sys
0x821fc0b0 isapnp.sys           0xf869a000     0x9000 isapnp.sys
0x821fc040 compbatt.sys         0xf8aae000     0x3000 compbatt.sys
0x821ed008 BATTC.SYS            0xf8ab2000     0x4000 ₩WINDOWS₩system32₩DRIVERS₩BATTC.SYS
```

modules(P)



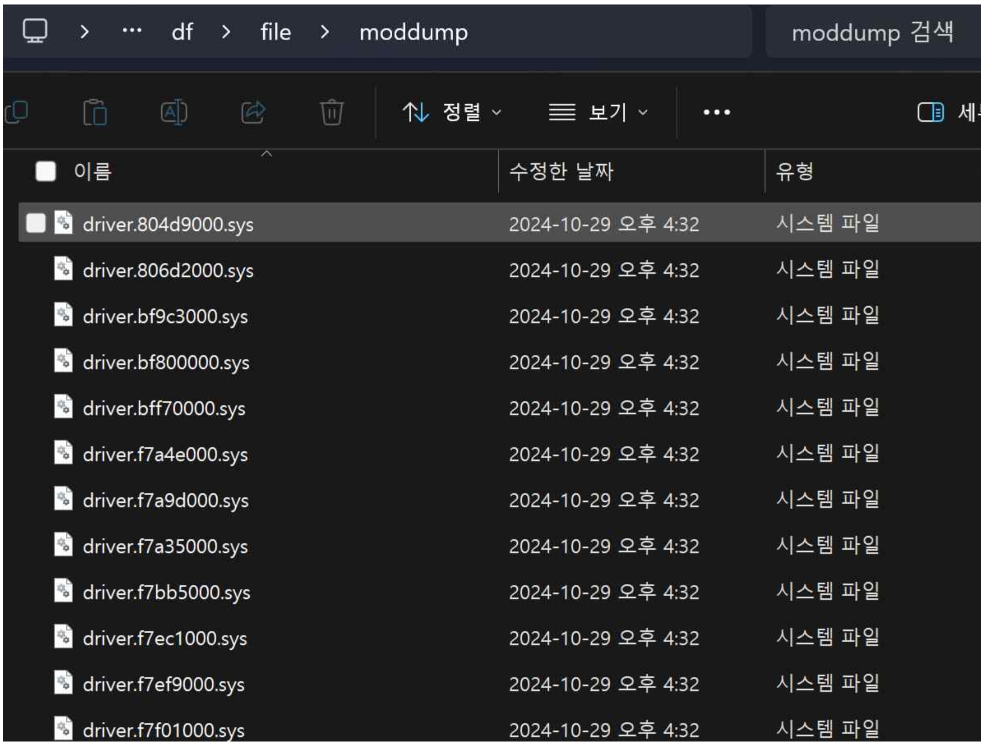
```
Offset(P)  Name                 Base       Size File
---------- -------------------- ---------- ---------- ----
0x025fc3a0 ntoskrnl.exe          0x804d9000   0x1f8c80 ₩WINDOWS₩system32₩ntkrnlpa.exe
0x025fc338 hal.dll               0x806d2000   0x20300 ₩WINDOWS₩system32₩hal.dll
0x025fc2d0 kdcom.dll             0xf8b9a000     0x2000 ₩WINDOWS₩system32₩KDCOM.DLL
0x025fc260 BOOTVID.dll           0xf8aaa000     0x3000 ₩WINDOWS₩system32₩BOOTVID.dll
0x025fc1f8 ACPI.sys              0xf856b000   0x2e000 ACPI.sys
0x025fc188 WMILIB.SYS            0xf8b9c000     0x2000 ₩WINDOWS₩system32₩DRIVERS₩WMILIB.SYS
0x025fc120 pci.sys               0xf855a000    0x11000 pci.sys
0x025fc0b0 isapnp.sys            0xf869a000     0x9000 isapnp.sys
0x025fc040 compbatt.sys          0xf8aae000     0x3000 compbatt.sys
0x025ed008 BATTC.SYS             0xf8ab2000     0x4000 ₩WINDOWS₩system32₩DRIVERS₩BATTC.SYS
```

modscan



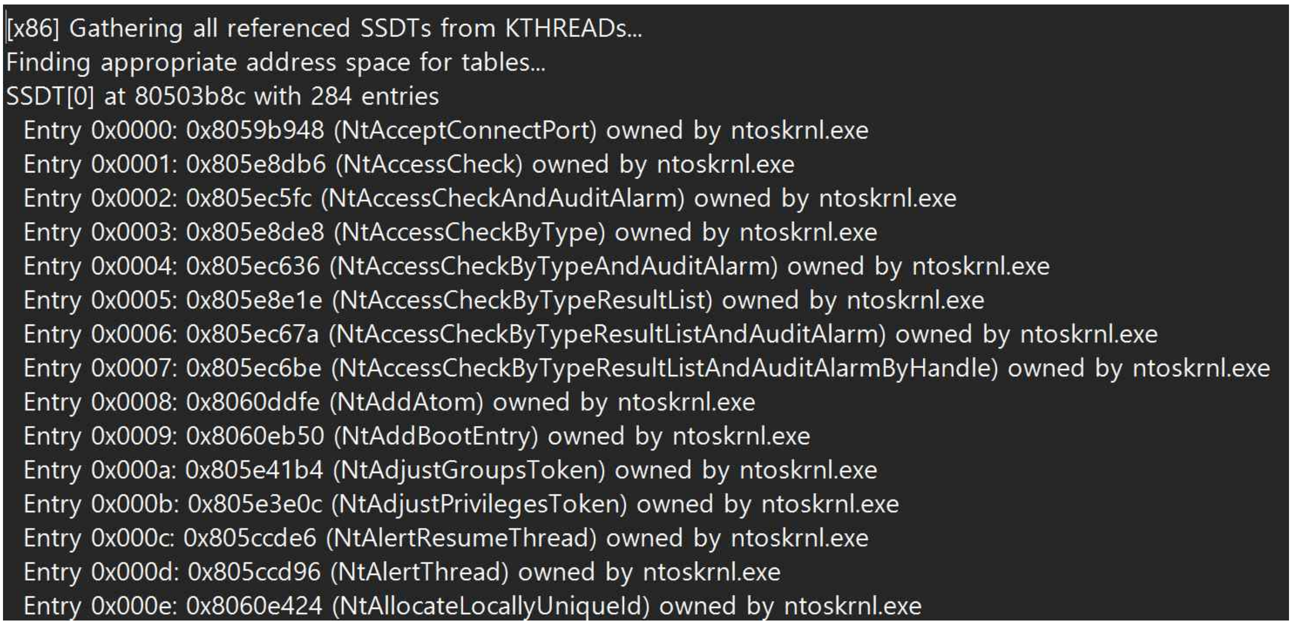
```
Offset(P)          Name                 Base       Size File
------------------ -------------------- ---------- ---------- ----
0x0000000000803040 compbatt.sys         0xf8aae000     0x3000 compbatt.sys
0x00000000008030b0 isapnp.sys           0xf869a000     0x9000 isapnp.sys
0x0000000000803120 pci.sys              0xf855a000    0x11000 pci.sys
0x0000000000803188 WMILIB.SYS           0xf8b9c000     0x2000 ₩WINDOWS₩system32₩DRIVERS₩WMILIB.SYS
0x00000000008031f8 ACPI.sys             0xf856b000    0x2e000 ACPI.sys
0x0000000000803260 BOOTVID.dll          0xf8aaa000     0x3000 ₩WINDOWS₩system32₩BOOTVID.dll
0x00000000008032d0 kdcom.dll            0xf8b9a000     0x2000 ₩WINDOWS₩system32₩KDCOM.DLL
0x0000000000803338 hal.dll              0x806d2000    0x20300 ₩WINDOWS₩system32₩hal.dll
0x00000000008033a0 ntoskrnl.exe         0x804d9000   0x1f8c80 ₩WINDOWS₩system32₩ntkrnlpa.exe
0x000000000092f4a8 i8042prt.sys         0xf871a000     0xc000 ₩SystemRoot₩system32₩DRIVERS₩i8042prt.sys
0x000000000092f578 kbdclass.sys         0xf8942000     0x6000 ₩SystemRoot₩system32₩DRIVERS₩kbdclass.sys
0x0000000000d07ab8 bthport.sys          0xf7a4e000    0x43000 ₩SystemRoot₩System32₩Drivers₩bthport.sys
```

moddump



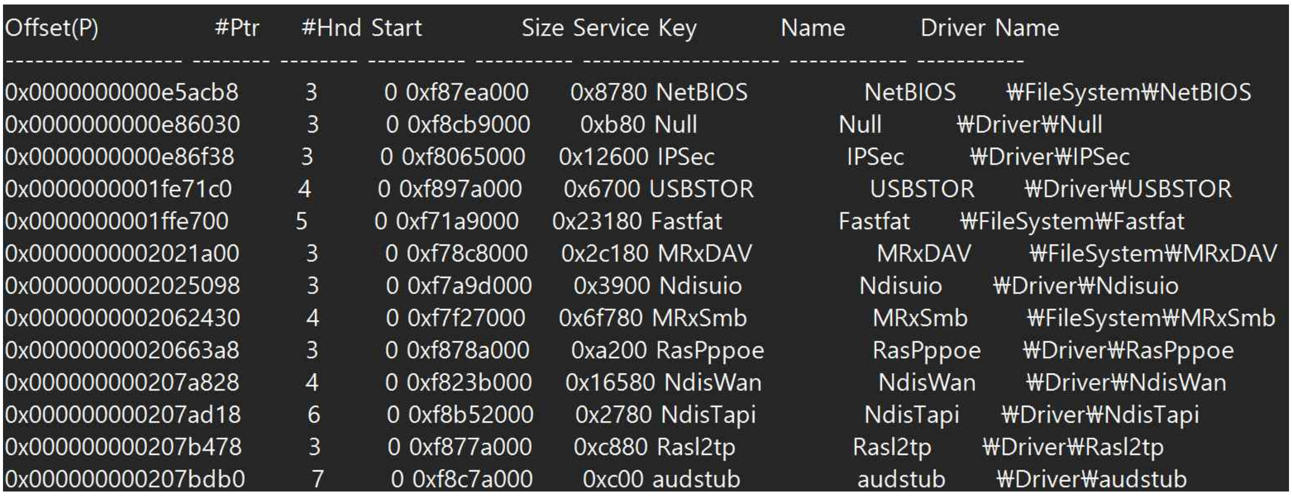
□ 이름	수정한 날짜	유형
□ driver.804d9000.sys	2024-10-29 오후 4:32	시스템 파일
driver.806d2000.sys	2024-10-29 오후 4:32	시스템 파일
driver.bf9c3000.sys	2024-10-29 오후 4:32	시스템 파일
driver.bf800000.sys	2024-10-29 오후 4:32	시스템 파일
driver.bff70000.sys	2024-10-29 오후 4:32	시스템 파일
driver.f7a4e000.sys	2024-10-29 오후 4:32	시스템 파일
driver.f7a9d000.sys	2024-10-29 오후 4:32	시스템 파일
driver.f7a35000.sys	2024-10-29 오후 4:32	시스템 파일
driver.f7bb5000.sys	2024-10-29 오후 4:32	시스템 파일
driver.f7ec1000.sys	2024-10-29 오후 4:32	시스템 파일
driver.f7ef9000.sys	2024-10-29 오후 4:32	시스템 파일
driver.f7f01000.sys	2024-10-29 오후 4:32	시스템 파일

ssdt



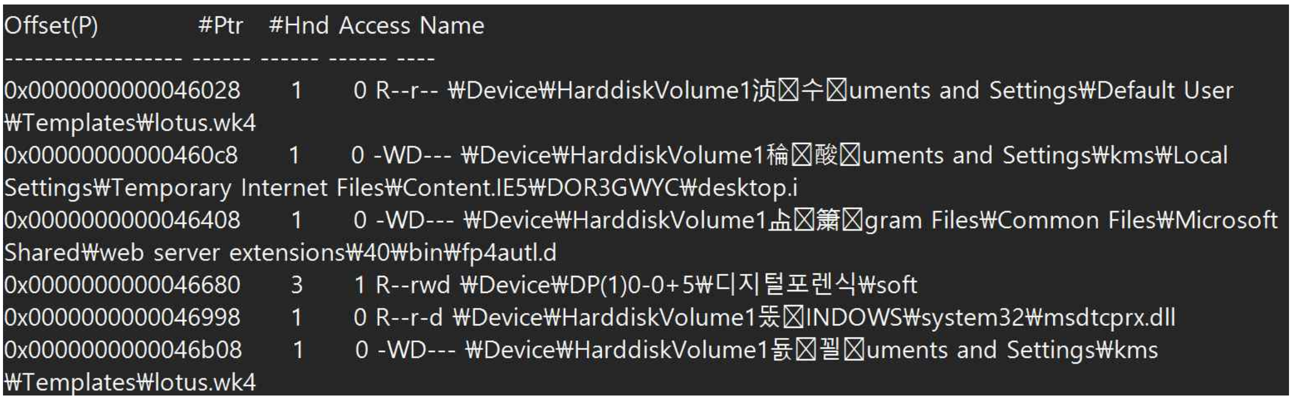
```
[x86] Gathering all referenced SSDTs from KTHREADs...
Finding appropriate address space for tables...
SSDT[0] at 80503b8c with 284 entries
  Entry 0x0000: 0x8059b948 (NtAcceptConnectPort) owned by ntoskrnl.exe
  Entry 0x0001: 0x805e8db6 (NtAccessCheck) owned by ntoskrnl.exe
  Entry 0x0002: 0x805ec5fc (NtAccessCheckAndAuditAlarm) owned by ntoskrnl.exe
  Entry 0x0003: 0x805e8de8 (NtAccessCheckByType) owned by ntoskrnl.exe
  Entry 0x0004: 0x805ec636 (NtAccessCheckByTypeAndAuditAlarm) owned by ntoskrnl.exe
  Entry 0x0005: 0x805e8e1e (NtAccessCheckByTypeResultList) owned by ntoskrnl.exe
  Entry 0x0006: 0x805ec67a (NtAccessCheckByTypeResultListAndAuditAlarm) owned by ntoskrnl.exe
  Entry 0x0007: 0x805ec6be (NtAccessCheckByTypeResultListAndAuditAlarmByHandle) owned by ntoskrnl.exe
  Entry 0x0008: 0x8060ddfe (NtAddAtom) owned by ntoskrnl.exe
  Entry 0x0009: 0x8060eb50 (NtAddBootEntry) owned by ntoskrnl.exe
  Entry 0x000a: 0x805e41b4 (NtAdjustGroupsToken) owned by ntoskrnl.exe
  Entry 0x000b: 0x805e3e0c (NtAdjustPrivilegesToken) owned by ntoskrnl.exe
  Entry 0x000c: 0x805ccde6 (NtAlertResumeThread) owned by ntoskrnl.exe
  Entry 0x000d: 0x805ccd96 (NtAlertThread) owned by ntoskrnl.exe
  Entry 0x000e: 0x8060e424 (NtAllocateLocallyUniqueId) owned by ntoskrnl.exe
```

driverscan



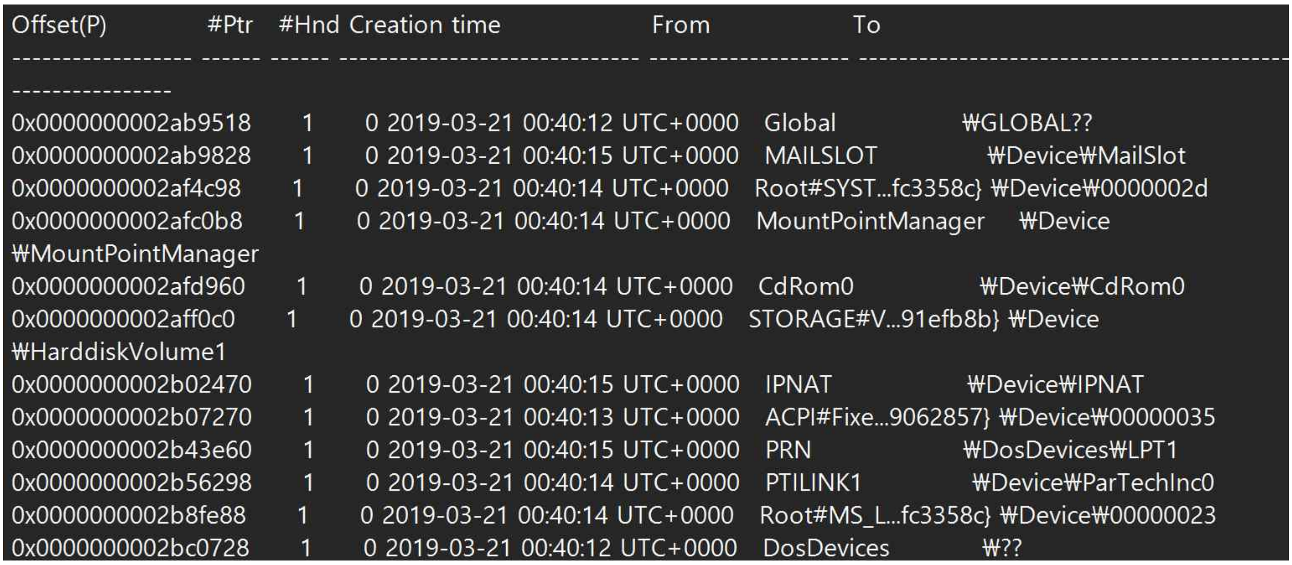
```
Offset(P)            #Ptr     #Hnd Start            Size Service Key          Name         Driver Name
------------------ -------- -------- ---------- ---------- -------------------- ------------ -----------
0x0000000000e5acb8        3        0 0xf87ea000     0x8780 NetBIOS              NetBIOS      ₩FileSystem₩NetBIOS
0x0000000000e86030        3        0 0xf8cb9000      0xb80 Null                 Null         ₩Driver₩Null
0x0000000000e86f38        3        0 0xf8065000    0x12600 IPSec                IPSec        ₩Driver₩IPSec
0x0000000001fe71c0        4        0 0xf897a000     0x6700 USBSTOR              USBSTOR      ₩Driver₩USBSTOR
0x0000000001ffe700        5        0 0xf71a9000    0x23180 Fastfat              Fastfat      ₩FileSystem₩Fastfat
0x0000000002021a00        3        0 0xf78c8000    0x2c180 MRxDAV               MRxDAV       ₩FileSystem₩MRxDAV
0x0000000002025098        3        0 0xf7a9d000     0x3900 Ndisuio              Ndisuio      ₩Driver₩Ndisuio
0x0000000002062430        4        0 0xf7f27000    0x6f780 MRxSmb               MRxSmb       ₩FileSystem₩MRxSmb
0x00000000020663a8        3        0 0xf878a000     0xa200 RasPppoe             RasPppoe     ₩Driver₩RasPppoe
0x000000000207a828        4        0 0xf823b000    0x16580 NdisWan              NdisWan      ₩Driver₩NdisWan
0x000000000207ad18        6        0 0xf8b52000     0x2780 NdisTapi             NdisTapi     ₩Driver₩NdisTapi
0x000000000207b478        3        0 0xf877a000     0xc880 Rasl2tp              Rasl2tp      ₩Driver₩Rasl2tp
0x000000000207bdb0        7        0 0xf8c7a000      0xc00 audstub              audstub      ₩Driver₩audstub
```

filescan



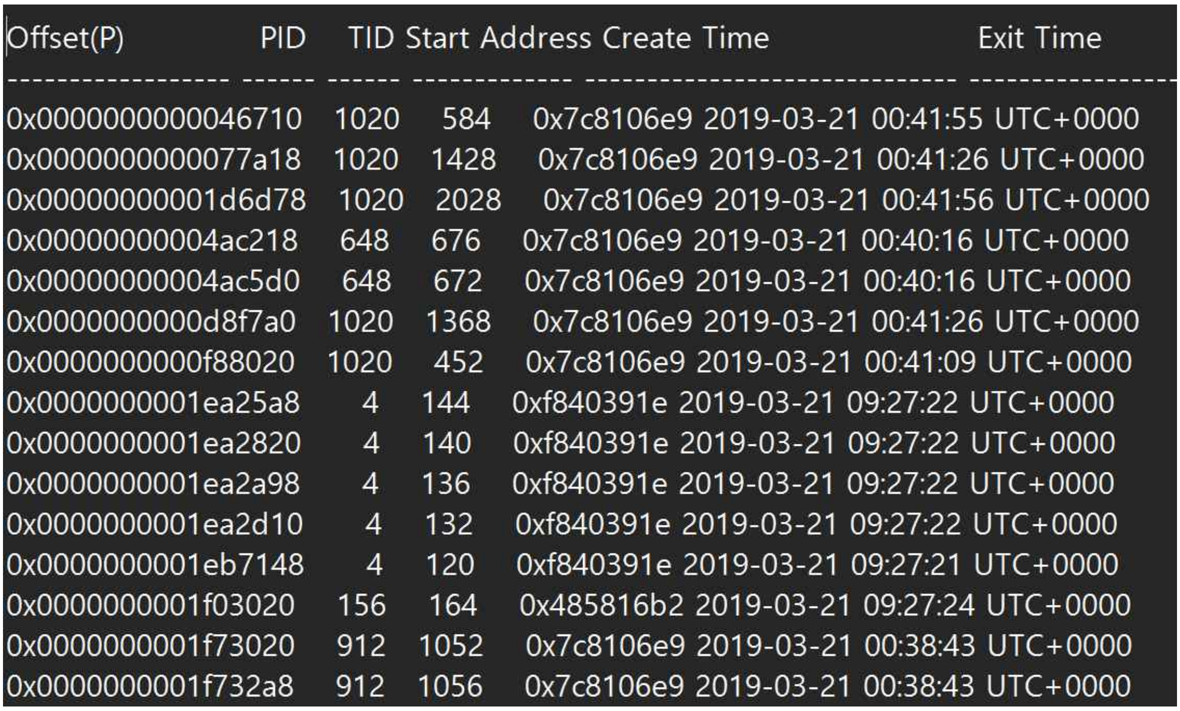
```
Offset(P)            #Ptr   #Hnd Access Name
------------------ ------ ------ ------ ----
0x0000000000046028      1      0 R--r-- ₩Device₩HarddiskVolume1浈⊠수⊠uments and Settings₩Default User
₩Templates₩lotus.wk4
0x00000000000460c8      1      0 -WD--- ₩Device₩HarddiskVolume1稐⊠酸⊠uments and Settings₩kms₩Local
Settings₩Temporary Internet Files₩Content.IE5₩DOR3GWYC₩desktop.i
0x0000000000046408      1      0 -WD--- ₩Device₩HarddiskVolume1쇼⊠簫⊠gram Files₩Common Files₩Microsoft
Shared₩web server extensions₩40₩bin₩fp4autl.d
0x0000000000046680      3      1 R--rwd ₩Device₩DP(1)0-0+5₩디지털프렌식₩soft
0x0000000000046998      1      0 R--r-d ₩Device₩HarddiskVolume1뜻⊠INDOWS₩system32₩msdtcprx.dll
0x0000000000046b08      1      0 -WD--- ₩Device₩HarddiskVolume1듥⊠뀔⊠uments and Settings₩kms
₩Templates₩lotus.wk4
```

symlinkscan



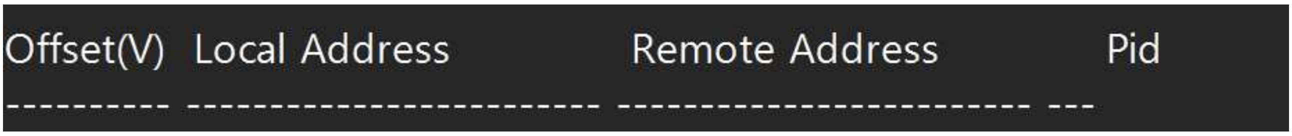
```
Offset(P)          #Ptr   #Hnd Creation time                  From                 To
------------------ ------ ------ ------------------------------ -------------------- ------------------------------------------
----------------
0x0000000002ab9518      1      0 2019-03-21 00:40:12 UTC+0000   Global               ₩GLOBAL??
0x0000000002ab9828      1      0 2019-03-21 00:40:15 UTC+0000   MAILSLOT             ₩Device₩MailSlot
0x0000000002af4c98      1      0 2019-03-21 00:40:14 UTC+0000   Root#SYST...fc3358c} ₩Device₩0000002d
0x0000000002afc0b8      1      0 2019-03-21 00:40:14 UTC+0000   MountPointManager    ₩Device
₩MountPointManager
0x0000000002afd960      1      0 2019-03-21 00:40:14 UTC+0000   CdRom0               ₩Device₩CdRom0
0x0000000002aff0c0      1      0 2019-03-21 00:40:14 UTC+0000   STORAGE#V...91efb8b} ₩Device
₩HarddiskVolume1
0x0000000002b02470      1      0 2019-03-21 00:40:15 UTC+0000   IPNAT                ₩Device₩IPNAT
0x0000000002b07270      1      0 2019-03-21 00:40:13 UTC+0000   ACPI#Fixe...9062857} ₩Device₩00000035
0x0000000002b43e60      1      0 2019-03-21 00:40:15 UTC+0000   PRN                  ₩DosDevices₩LPT1
0x0000000002b56298      1      0 2019-03-21 00:40:14 UTC+0000   PTILINK1             ₩Device₩ParTechInc0
0x0000000002b8fe88      1      0 2019-03-21 00:40:14 UTC+0000   Root#MS_L...fc3358c} ₩Device₩00000023
0x0000000002bc0728      1      0 2019-03-21 00:40:12 UTC+0000   DosDevices           ₩??
```

thrdscan



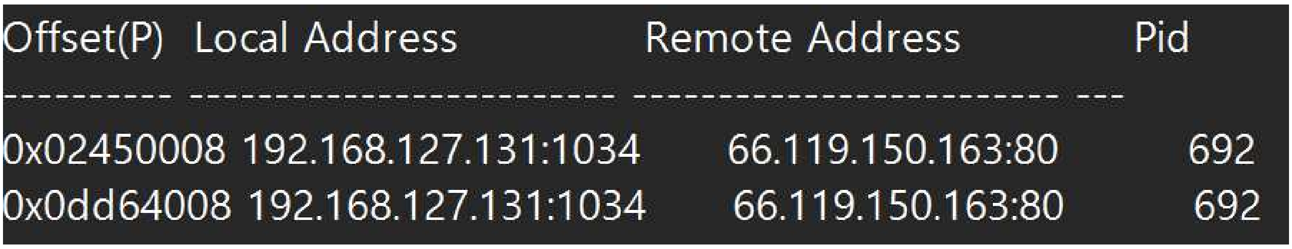
```
Offset(P)             PID    TID Start Address Create Time                    Exit Time
------------------ ------ ------ ------------- ------------------------------ ----------------
0x0000000000046710   1020    584    0x7c8106e9 2019-03-21 00:41:55 UTC+0000
0x0000000000077a18   1020   1428    0x7c8106e9 2019-03-21 00:41:26 UTC+0000
0x00000000001d6d78   1020   2028    0x7c8106e9 2019-03-21 00:41:56 UTC+0000
0x00000000004ac218    648    676    0x7c8106e9 2019-03-21 00:40:16 UTC+0000
0x00000000004ac5d0    648    672    0x7c8106e9 2019-03-21 00:40:16 UTC+0000
0x0000000000d8f7a0   1020   1368    0x7c8106e9 2019-03-21 00:41:26 UTC+0000
0x0000000000f88020   1020    452    0x7c8106e9 2019-03-21 00:41:09 UTC+0000
0x0000000001ea25a8      4    144    0xf840391e 2019-03-21 09:27:22 UTC+0000
0x0000000001ea2820      4    140    0xf840391e 2019-03-21 09:27:22 UTC+0000
0x0000000001ea2a98      4    136    0xf840391e 2019-03-21 09:27:22 UTC+0000
0x0000000001ea2d10      4    132    0xf840391e 2019-03-21 09:27:22 UTC+0000
0x0000000001eb7148      4    120    0xf840391e 2019-03-21 09:27:21 UTC+0000
0x0000000001f03020    156    164    0x485816b2 2019-03-21 09:27:24 UTC+0000
0x0000000001f73020    912   1052    0x7c8106e9 2019-03-21 00:38:43 UTC+0000
0x0000000001f732a8    912   1056    0x7c8106e9 2019-03-21 00:38:43 UTC+0000
```

connections



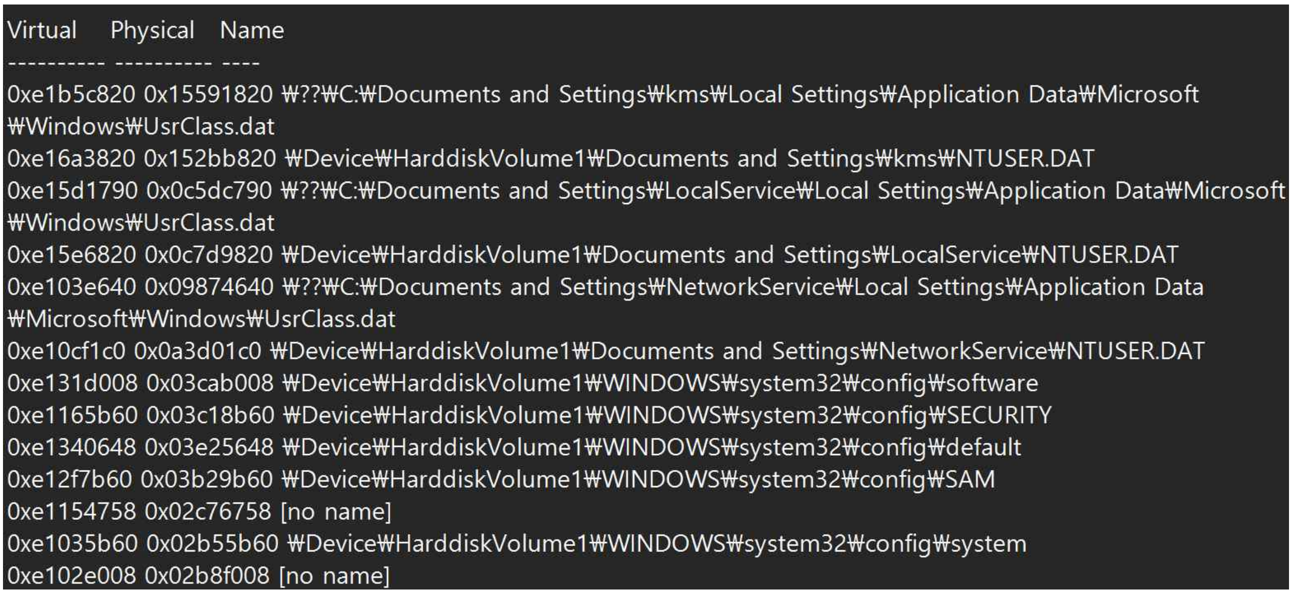
```
Offset(V)  Local Address             Remote Address            Pid
---------- ------------------------- ------------------------- ---
```

connscan



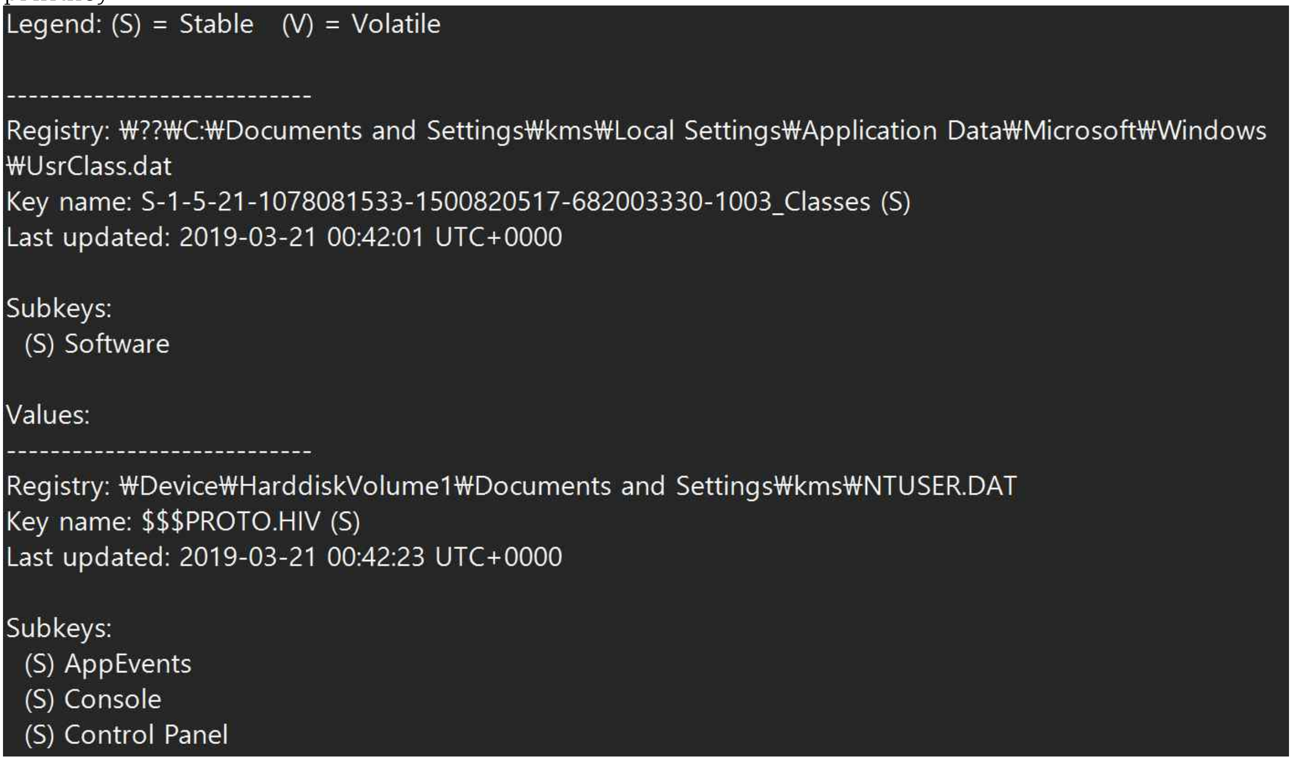
```
Offset(P)  Local Address             Remote Address            Pid
---------- ------------------------- ------------------------- ---
0x02450008 192.168.127.131:1034      66.119.150.163:80          692
0x0dd64008 192.168.127.131:1034      66.119.150.163:80          692
```

hivelist



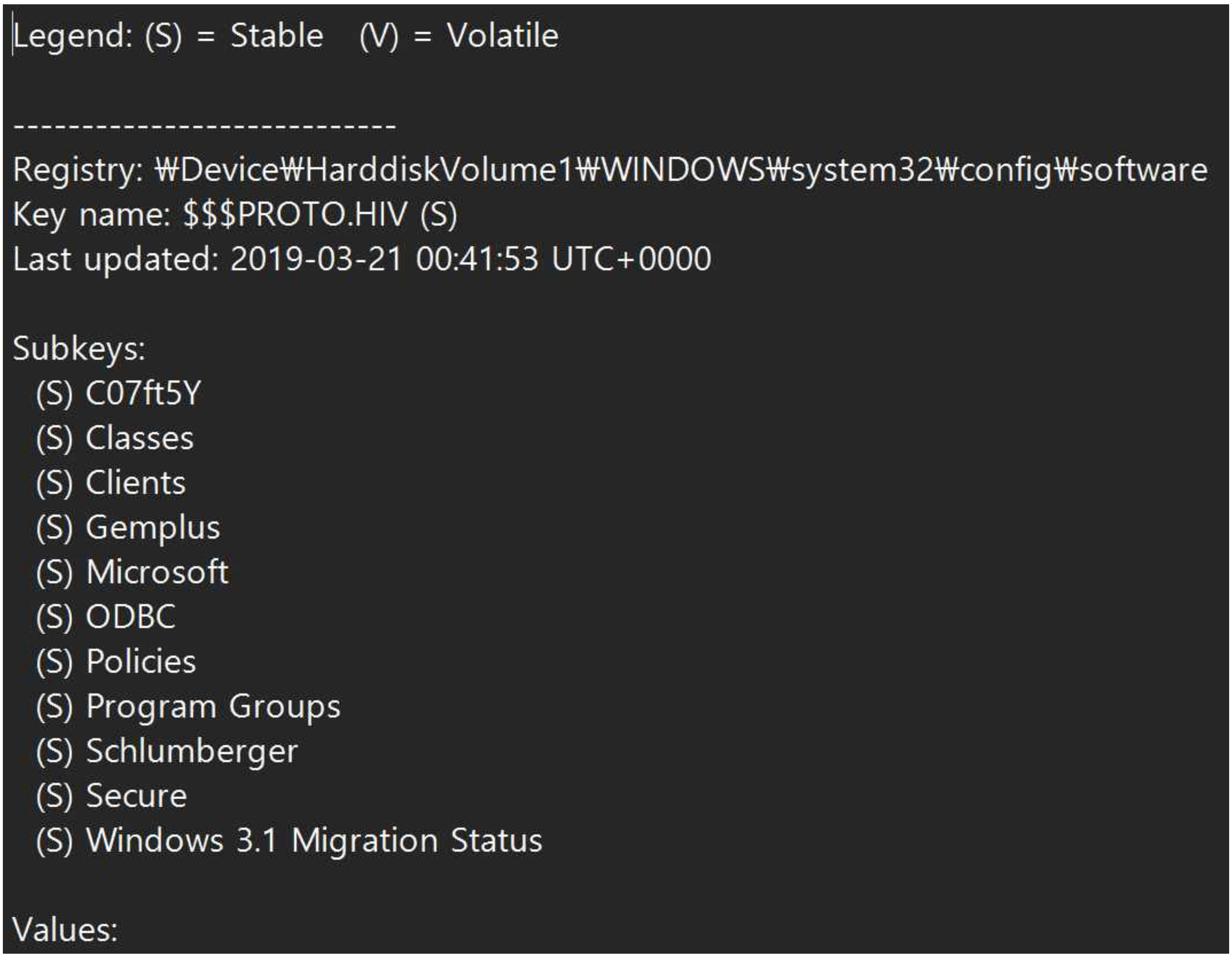
```
Virtual    Physical   Name
---------- ---------- ----
0xe1b5c820 0x15591820 ₩??₩C:₩Documents and Settings₩kms₩Local Settings₩Application Data₩Microsoft
₩Windows₩UsrClass.dat
0xe16a3820 0x152bb820 ₩Device₩HarddiskVolume1₩Documents and Settings₩kms₩NTUSER.DAT
0xe15d1790 0x0c5dc790 ₩??₩C:₩Documents and Settings₩LocalService₩Local Settings₩Application Data₩Microsoft
₩Windows₩UsrClass.dat
0xe15e6820 0x0c7d9820 ₩Device₩HarddiskVolume1₩Documents and Settings₩LocalService₩NTUSER.DAT
0xe103e640 0x09874640 ₩??₩C:₩Documents and Settings₩NetworkService₩Local Settings₩Application Data
₩Microsoft₩Windows₩UsrClass.dat
0xe10cf1c0 0x0a3d01c0 ₩Device₩HarddiskVolume1₩Documents and Settings₩NetworkService₩NTUSER.DAT
0xe131d008 0x03cab008 ₩Device₩HarddiskVolume1₩WINDOWS₩system32₩config₩software
0xe1165b60 0x03c18b60 ₩Device₩HarddiskVolume1₩WINDOWS₩system32₩config₩SECURITY
0xe1340648 0x03e25648 ₩Device₩HarddiskVolume1₩WINDOWS₩system32₩config₩default
0xe12f7b60 0x03b29b60 ₩Device₩HarddiskVolume1₩WINDOWS₩system32₩config₩SAM
0xe1154758 0x02c76758 [no name]
0xe1035b60 0x02b55b60 ₩Device₩HarddiskVolume1₩WINDOWS₩system32₩config₩system
0xe102e008 0x02b8f008 [no name]
```

printkey



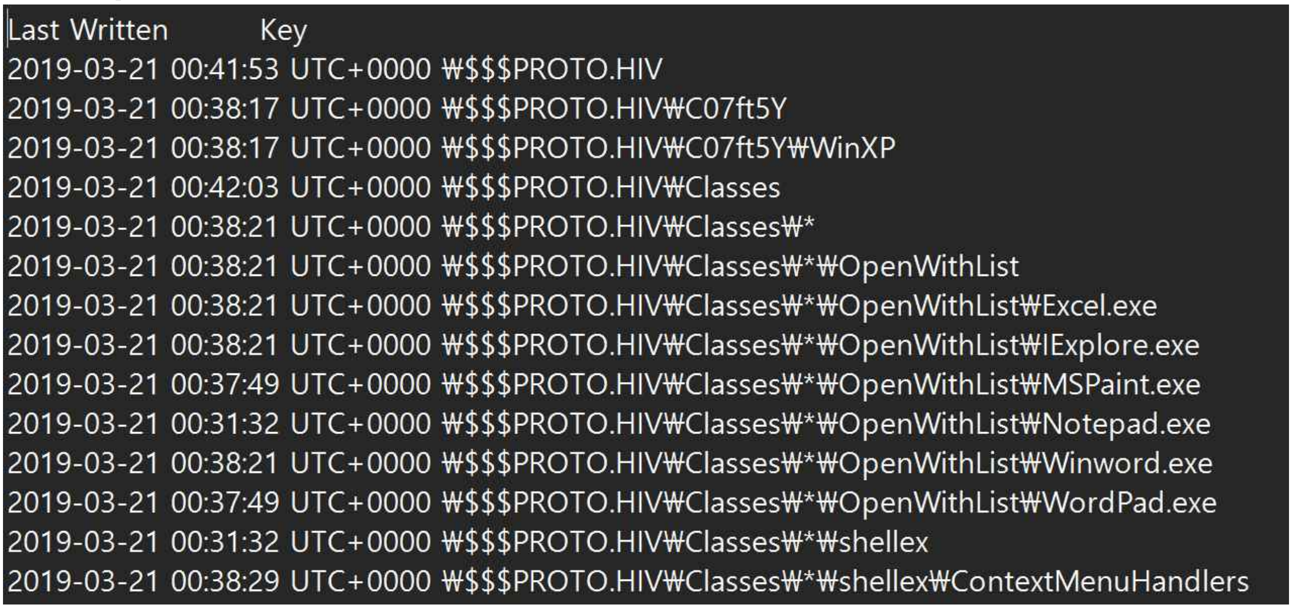
```
Legend: (S) = Stable   (V) = Volatile

----------------------------
Registry: ₩??₩C:₩Documents and Settings₩kms₩Local Settings₩Application Data₩Microsoft₩Windows
₩UsrClass.dat
Key name: S-1-5-21-1078081533-1500820517-682003330-1003_Classes (S)
Last updated: 2019-03-21 00:42:01 UTC+0000

Subkeys:
  (S) Software

Values:
----------------------------
Registry: ₩Device₩HarddiskVolume1₩Documents and Settings₩kms₩NTUSER.DAT
Key name: $$$PROTO.HIV (S)
Last updated: 2019-03-21 00:42:23 UTC+0000

Subkeys:
  (S) AppEvents
  (S) Console
  (S) Control Panel
```

printkey -o



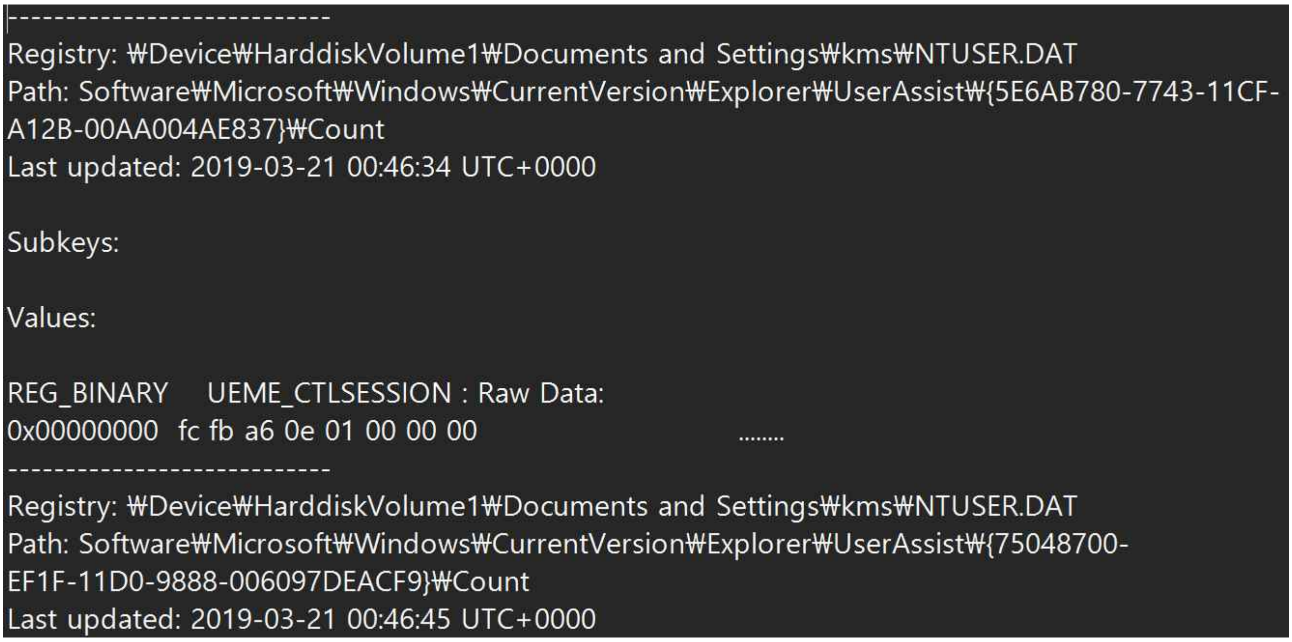
```
Legend: (S) = Stable   (V) = Volatile

----------------------------
Registry: ₩Device₩HarddiskVolume1₩WINDOWS₩system32₩config₩software
Key name: $$$PROTO.HIV (S)
Last updated: 2019-03-21 00:41:53 UTC+0000

Subkeys:
  (S) C07ft5Y
  (S) Classes
  (S) Clients
  (S) Gemplus
  (S) Microsoft
  (S) ODBC
  (S) Policies
  (S) Program Groups
  (S) Schlumberger
  (S) Secure
  (S) Windows 3.1 Migration Status

Values:
```

hivedump -o



```
Last Written          Key
2019-03-21 00:41:53 UTC+0000 ₩$$$PROTO.HIV
2019-03-21 00:38:17 UTC+0000 ₩$$$PROTO.HIV₩C07ft5Y
2019-03-21 00:38:17 UTC+0000 ₩$$$PROTO.HIV₩C07ft5Y₩WinXP
2019-03-21 00:42:03 UTC+0000 ₩$$$PROTO.HIV₩Classes
2019-03-21 00:38:21 UTC+0000 ₩$$$PROTO.HIV₩Classes₩*
2019-03-21 00:38:21 UTC+0000 ₩$$$PROTO.HIV₩Classes₩*₩OpenWithList
2019-03-21 00:38:21 UTC+0000 ₩$$$PROTO.HIV₩Classes₩*₩OpenWithList₩Excel.exe
2019-03-21 00:38:21 UTC+0000 ₩$$$PROTO.HIV₩Classes₩*₩OpenWithList₩IExplore.exe
2019-03-21 00:37:49 UTC+0000 ₩$$$PROTO.HIV₩Classes₩*₩OpenWithList₩MSPaint.exe
2019-03-21 00:31:32 UTC+0000 ₩$$$PROTO.HIV₩Classes₩*₩OpenWithList₩Notepad.exe
2019-03-21 00:38:21 UTC+0000 ₩$$$PROTO.HIV₩Classes₩*₩OpenWithList₩Winword.exe
2019-03-21 00:37:49 UTC+0000 ₩$$$PROTO.HIV₩Classes₩*₩OpenWithList₩WordPad.exe
2019-03-21 00:31:32 UTC+0000 ₩$$$PROTO.HIV₩Classes₩*₩shellex
2019-03-21 00:38:29 UTC+0000 ₩$$$PROTO.HIV₩Classes₩*₩shellex₩ContextMenuHandlers
```

userassist



```
----------------------------
Registry: ₩Device₩HarddiskVolume1₩Documents and Settings₩kms₩NTUSER.DAT
Path: Software₩Microsoft₩Windows₩CurrentVersion₩Explorer₩UserAssist₩{5E6AB780-7743-11CF-
A12B-00AA004AE837}₩Count
Last updated: 2019-03-21 00:46:34 UTC+0000

Subkeys:

Values:

REG_BINARY    UEME_CTLSESSION : Raw Data:
0x00000000  fc fb a6 0e 01 00 00 00                          ........
----------------------------
Registry: ₩Device₩HarddiskVolume1₩Documents and Settings₩kms₩NTUSER.DAT
Path: Software₩Microsoft₩Windows₩CurrentVersion₩Explorer₩UserAssist₩{75048700-
EF1F-11D0-9888-006097DEACF9}₩Count
Last updated: 2019-03-21 00:46:45 UTC+0000
```