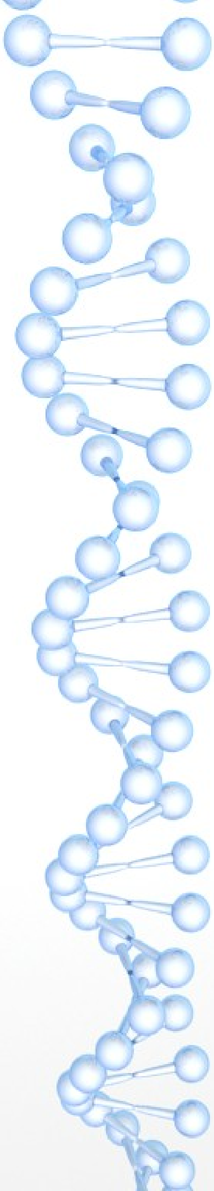


Step 1 - imageinfo

```
$ volatility -f WIN-TTUMF6EI3O3-20140203-123134.raw imageinfo
Volatility Foundation Volatility Framework 2.6
INFO    : volatility.debug    : Determining profile based on KDBG search...
          Suggested Profile(s) : Win7SP1x86_23418, Win7SP0x86, Win7SP1x86_24000, 
Win7SP1x86
                     AS Layer1 : IA32PagedMemoryPae (Kernel AS)
                     AS Layer2 : FileAddressSpace (...)
                      PAE type : PAE
                           DTB : 0x185000L
                          KDBG : 0x82968c28L
          Number of Processors : 1
     Image Type (Service Pack) : 1
                KPCR for CPU 0 : 0x82969c00L
...
```

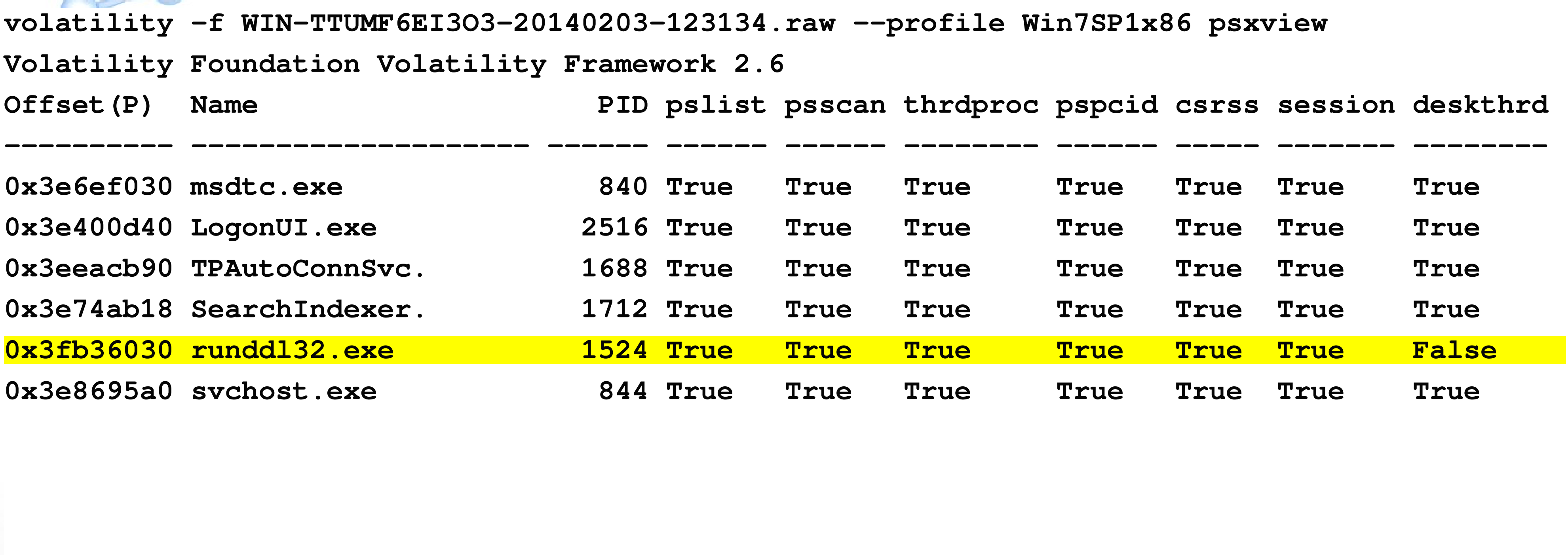
Step 2 - psxview

```
volatility -f WIN-TTUMF6EI3O3-20140203-123134.raw --profile Win7SP1x86 psxview
Volatility Foundation Volatility Framework 2.6
Offset(P)  Name                    PID pslist psscan thrdproc pspcid csrss session deskthrd
---------- -------------------- ------ ------ ------ -------- ------ ----- ------- --------
0x3e6ef030 msdtc.exe               840 True   True   True     True   True  True    True
0x3e400d40 LogonUI.exe            2516 True   True   True     True   True  True    True
0x3eeacb90 TPAutoConnSvc.         1688 True   True   True     True   True  True    True
0x3e74ab18 SearchIndexer.         1712 True   True   True     True   True  True    True
0x3fb36030 rundd132.exe           1524 True   True   True     True   True  True    False
0x3e8695a0 svchost.exe             844 True   True   True     True   True  True    True
```

What is ps*

pslist	– Traverses PsActiveProcessHead
Psscan	– EPROCESS pool scanning
Thrdproc	– ETHREAD pool scanning, then reference parent
Pspcid	– handle table for process and thread client IDs
Csrss	– participates in thread/process creation Has open handle to every thread/process
Session	– Processes → sessions → processes
Deskthrd	– Pools[tagDESKTOP] → threads → processes

Step 3 – Find Weird Process



```
volatility -f WIN-TTUMF6EI3O3-20140203-123134.raw --profile Win7SP1x86 psxview
Volatility Foundation Volatility Framework 2.6
Offset(P)  Name                    PID pslist psscan thrdproc pspcid csrss session deskthrd
---------- -------------------- ------ ------ ------ -------- ------ ----- ------- --------
0x3e6ef030 msdtc.exe               840 True   True   True     True   True  True    True
0x3e400d40 LogonUI.exe            2516 True   True   True     True   True  True    True
0x3eeacb90 TPAutoConnSvc.         1688 True   True   True     True   True  True    True
0x3e74ab18 SearchIndexer.         1712 True   True   True     True   True  True    True
0x3fb36030 rundd132.exe           1524 True   True   True     True   True  True    False
0x3e8695a0 svchost.exe             844 True   True   True     True   True  True    True
```

Step 4 – List DLLs

```
$ volatility -f WIN-TTUMF6EI3O3-20140203-123134.raw --profile Win7SP1x86 dlllist -p 1524
Volatility Foundation Volatility Framework 2.6
************************************************************************
rundd132.exe pid:   1524
Command line : "C:\Users\TEKDEF~1\AppData\Local\Temp\MSDCSC\rundd132.exe"  - Weird path
Service Pack 1

Base                  Size  LoadCount LoadTime                       Path
---------- ---------- ---------- ------------------------------ ----
0x00400000    0xb2000     0xffff 1970-01-01 00:00:00 UTC+0000   C:\Users\TEKDEF~1\AppData\Local\
Temp\MSDCSC\rundd132.exe
0x76dc0000   0x13c000     0xffff 1970-01-01 00:00:00 UTC+0000   C:\Windows\SYSTEM32\ntdll.dll
0x75c20000    0xd4000     0xffff 2014-02-03 12:27:18 UTC+0000   C:\Windows\system32\kernel32.dll
0x74f60000    0x4b000     0xffff 2014-02-03 12:27:18 UTC+0000   C:\Windows\system32\KERNELBASE.dll
```

Step 5 – Is File in Memory

```
Filescan – scans for FILE_OBJECTs


volatility -f WIN-TTUMF6EI3O3-20140203-123134.raw --profile Win7SP1x86 filescan
| grep runddl32.exe

Volatility Foundation Volatility Framework 2.6


0x000000003eee8690      4      0 R--r-d
\Device\HarddiskVolume1\Users\TEKDEF~1\AppData\Local\Temp\MSDCSC\runddl32.exe


0x000000003fa2cc00      8      0 RWD---
\Device\HarddiskVolume1\Users\TEKDEF~1\AppData\Local\Temp\MSDCSC\runddl32.exe
```

Step 5 – Dump .exe

```
$ volatility -f WIN-TTUMF6EI3O3-20140203-123134.raw --profile Win7SP1x86
procdump -D . -p 1524

Volatility Foundation Volatility Framework 2.6

Process(V) ImageBase  Name                 Result

---------- ---------- -------------------- ------

0x84536030 0x00400000 runddl32.exe         OK: executable.1524.exe


$ ls -l

total 1049664

-rw-r--r-- 1 michael michael     674304 Feb 23 11:56 executable.1524.exe
```

You can do “strings executable.1524.exe”

Step 6 – Process Tree

```
$ volatility -f WIN-TTUMF6EI3O3-20140203-123134.raw --profile Win7SP1x86 pstree
Volatility Foundation Volatility Framework 2.6
Name                                                  Pid   PPid   Thds   Hnds Time
-------------------------------------------------- ------ ------ ------ ------ ----
 0x84536030:runddl32.exe                             1524   3220     10    161
. 0x84506480:notepad.exe                             1896   1524      2     57
```

Step 7 – MalFind

Find weird VADs - having executable permissions and not backed by a file

VAD tags “VadS”/”VadF” - not backed by file

```
$ volatility -f WIN-TTUMF6EI3O3-20140203-123134.raw --profile Win7SP1x86 malfind -p 1896
```

Many string VADs

The code is in the last VAD

```
Process: notepad.exe Pid: 1896 Address: 0x160000
Vad Tag: VadS Protection: PAGE_EXECUTE_READWRITE
Flags: CommitCharge: 1, MemCommit: 1, PrivateMemory: 1, Protection: 6

0x00160000  54 65 72 6d 69 6e 61 74 65 50 72 6f 63 65 73 73   TerminateProcess
0x00160010  00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00   ................


Process: notepad.exe Pid: 1896 Address: 0x190000
Vad Tag: VadS Protection: PAGE_EXECUTE_READWRITE
Flags: CommitCharge: 1, MemCommit: 1, PrivateMemory: 1, Protection: 6

0x00190000  57 61 69 74 46 6f 72 53 69 6e 67 6c 65 4f 62 6a   WaitForSingleObj
0x00190010  65 63 74 00 00 00 00 00 00 00 00 00 00 00 00 00   ect.............


Process: notepad.exe Pid: 1896 Address: 0x180000
Vad Tag: VadS Protection: PAGE_EXECUTE_READWRITE
Flags: CommitCharge: 1, MemCommit: 1, PrivateMemory: 1, Protection: 6

0x00180000  44 43 5f 4d 55 54 45 58 2d 4b 48 4e 45 57 30 36   DC_MUTEX-KHNEW06
0x00180010  00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00   ................

Process: notepad.exe Pid: 1896 Address: 0x1a0000
Vad Tag: VadS Protection: PAGE_EXECUTE_READWRITE
Flags: CommitCharge: 1, MemCommit: 1, PrivateMemory: 1, Protection: 6
```

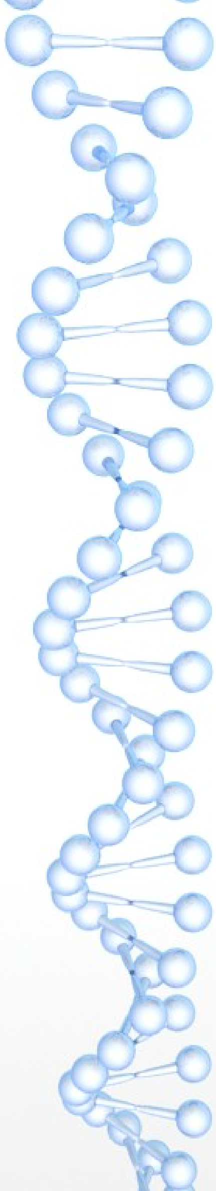
```
Process: notepad.exe Pid: 1896 Address: 0x1a0000
Vad Tag: VadS Protection: PAGE_EXECUTE_READWRITE
Flags: CommitCharge: 1, MemCommit: 1, PrivateMemory: 1, Protection: 6

0x001a0000  43 3a 5c 55 73 65 72 73 5c 54 45 4b 44 45 46 7e   C:\Users\TEKDEF~
0x001a0010  31 5c 41 70 70 44 61 74 61 5c 4c 6f 63 61 6c 5c   1\AppData\Local\
0x001a0020  54 65 6d 70 5c 4d 53 44 43 53 43 5c 72 75 6e 64   Temp\MSDCSC\rund
0x001a0030  64 6c 33 32 2e 65 78 65 00 00 00 00 00 00 00 00   dl32.exe........
=
Process: notepad.exe Pid: 1896 Address: 0x1c0000
Vad Tag: VadS Protection: PAGE_EXECUTE_READWRITE
Flags: CommitCharge: 1, MemCommit: 1, PrivateMemory: 1, Protection: 6

0x001c0000 55                PUSH EBP
0x001c0001 8bec              MOV EBP, ESP
0x001c0003 83c4ac            ADD ESP, -0x54
0x001c0006 53                PUSH EBX
0x001c0007 56                PUSH ESI
0x001c0008 57                PUSH EDI
0x001c0009 8b5d08            MOV EBX, [EBP+0x8]
0x001c000c 8b4340            MOV EAX, [EBX+0x40]
0x001c000f 50                PUSH EAX
0x001c0010 8b4338            MOV EAX, [EBX+0x38]
0x001c0013 50                PUSH EAX
0x001c0014 ff13              CALL DWORD [EBX]
...
```

Step 8 – Handles

```
$ volatility -f WIN-TTUMF6EI3O3-20140203-123134.raw --profile Win7SP1x86 handles -p 1524
-t Mutant
Volatility Foundation Volatility Framework 2.6
Offset(V)     Pid     Handle     Access Type             Details
---------- ------ ---------- ---------- ---------------- -------
0x84a71de0   1524       0x58   0x1f0001 Mutant
0x84a9c670   1524      0x150   0x1f0001 Mutant           DC_MUTEX-KHNEW06
0x85333c40   1524      0x1dc   0x1f0001 Mutant
0x8459e298   1524      0x1e4   0x1f0001 Mutant
```

Step 9 – Strings

```
$ volatility -f WIN-TTUMF6EI3O3-20140203-123134.raw --profile Win7SP1x86 memdump -D . -p
1524

$ strings -a 1524.dmp | less

#BEGIN DARKCOMET DATA --

MUTEX={DC_MUTEX-KHNEW06}     SID={Guest16}     FWB={0}    NETDATA={test213.no-ip.info:1604}

GENCODE={F6FE8i2BxCpu}       INSTALL={1}      COMBOPATH={10}  EDTPATH={MSDCSC\runddl32.exe}

KEYNAME={MicroUpdate}          EDTDATE={16/04/2007} PERSINST={1}     MELT={0}

CHANGEDATE={1}                 DIRATTRIB={6}          FILEATTRIB={6}  SH1={1}

CHIDEF={1}                     CHIDED={1}             PERS={1}        OFFLINEK={1}

#EOF DARKCOMET DATA --
```



DarkComet (from Wikipedia)

- DarkComet is a remote access trojan (RAT)
- DarkComet allows a user to control the system with a graphical user interface. It has many features which allows a user to use it as administrative remote help tool; however, DarkComet has many features which can be used maliciously. DarkComet is commonly used to spy on the victims by taking screen captures, key-logging, or password stealing.

Step 10 – Reading Strings Carefully

```
$ strings –a 1524.dmp | grep dclogs
dclogs\
dclogs\
dclogs\
dclogs\
C:\Users\Tek Defense\AppData\Roaming\dclogs\2014-02-03-2.dc
```

Step 11 – Reading Files

Is open? If not, we need the HD image

```
$ volatility -f WIN-TTUMF6EI3O3-20140203-123134.raw --profile Win7SP1x86 filescan | grep
dclogs
```

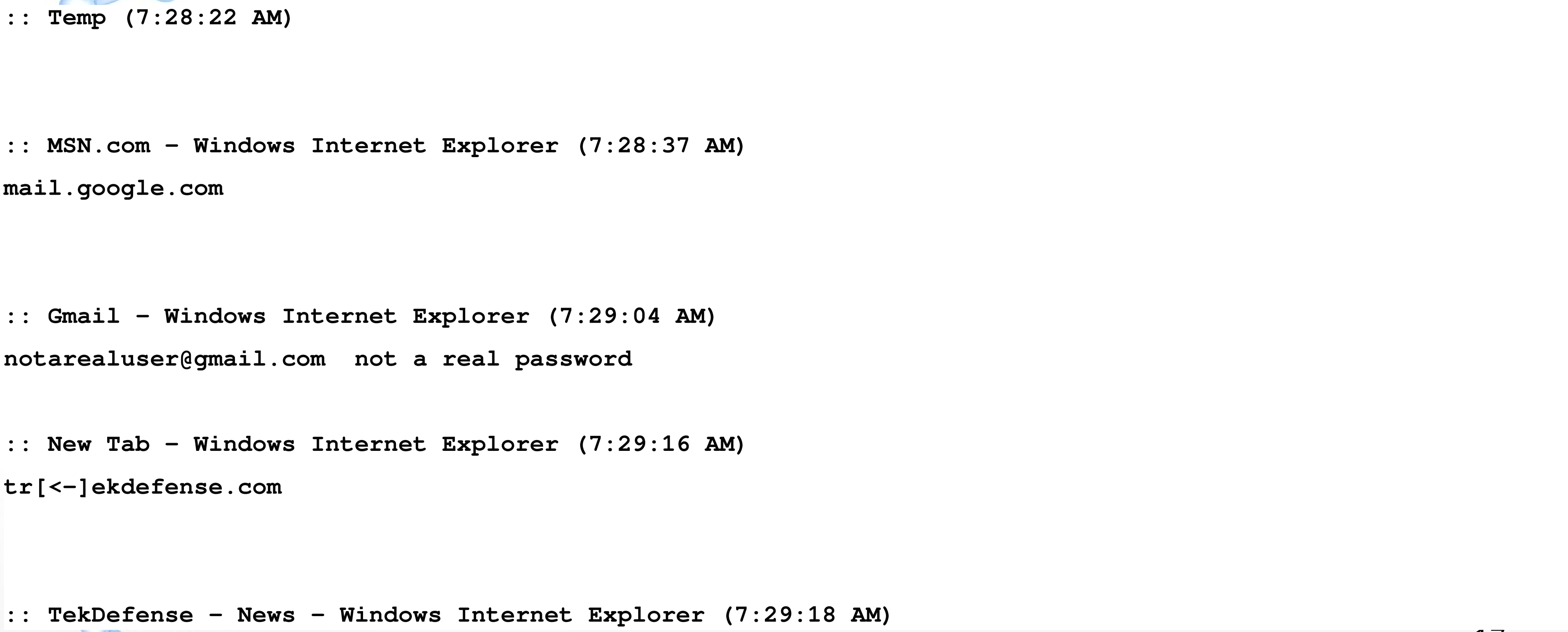
```
0x000000003eee9330      8      0 -W-r-- \Device\HarddiskVolume1\Users\Tek Defense\AppData\
Roaming\dclogs\2014-02-03-2.dc
```

```
$ volatility -f WIN-TTUMF6EI3O3-20140203-123134.raw --profile Win7SP1x86 dumpfiles -D . -Q
0x000000003eee9330
```

Not every file will be currently active or in the VAD

    such files will not be dumped unless -Q is used

What’s in the file?



```
:: Temp (7:28:22 AM)



:: MSN.com - Windows Internet Explorer (7:28:37 AM)
mail.google.com



:: Gmail - Windows Internet Explorer (7:29:04 AM)
notarealuser@gmail.com  not a real password

:: New Tab - Windows Internet Explorer (7:29:16 AM)
tr[<-]ekdefense.com



:: TekDefense - News - Windows Internet Explorer (7:29:18 AM)
```

Step 12 – Persistence

```
$ volatility -f WIN-TTUMF6EI3O3-20140203-123134.raw --profile Win7SP1x86 printkey -K "Software\
Microsoft\Windows\CurrentVersion\Run"


Registry: \??\C:\Windows\ServiceProfiles\LocalService\NTUSER.DAT

Values:

REG_EXPAND_SZ Sidebar         : (S) %ProgramFiles%\Windows Sidebar\Sidebar.exe /autoRun


Registry: \??\C:\Windows\ServiceProfiles\NetworkService\NTUSER.DAT

Values:

REG_EXPAND_SZ Sidebar         : (S) %ProgramFiles%\Windows Sidebar\Sidebar.exe /autoRun


Registry: \??\C:\Users\Tek Defense\ntuser.dat

Values:

REG_SZ        MicroUpdate     : (S) C:\Users\TEKDEF~1\AppData\Local\Temp\MSDCSC\runddl32.exe
```