WinObj plugin

Shachaf Atun

Introduction

WinObj is a volatility plugin that helps us map the *Object Manager* (similarly to Sysinterals' WinObj tool). Moreover, it can help us parse all kind of *Object Directories* content.
For every object inside a directory, *WinObj* plugin will supply some useful information about the object.

The main problem with converting Sysinternals' *WinObj* tool or any other available tools for enumeration of *Object Directories* into a volatility plugin is the fact that each of the tools uses APIs such as **NtQueryDirectoryObject**, and while performing offline memory analysis, without the ability to execute such APIs, I had to understand how these objects are enumerated in memory.

Contents

Introduction 1

Object Manager 2

Object Directory in General 2

In Depth Look Inside the Object Manager 2

Object Manager for Security Researchers 2

About the Research 3

Optional Flags 5

Usage Examples 6

KnownDlls Case Study 10

More Useful Examples 11

Summary 13

Object Manager

Object Directory in General

The *Object Manager*'s main role is to manage NT objects.

There are some useful native NT API which allows programs from user mode to browse the namespace and query the status of objects located there, but the interfaces are undocumented. These objects are called *Object Directories*.

An *Object Directory* is a named object that is mostly used to contain other named objects (You can find some examples here).

In Depth Look Inside the Object Manager

The *Object Manager* was designed to provide the following (taken from Windows Internals Part 1):

- A common, uniform mechanism for using system resources.
- Isolate object protection to one location in the operating system to ensure uniform and consistent object access policy.
- Provide a mechanism to charge processes for their use of objects so that limits can be placed on the usage of system resources.
- Establish an object-naming scheme that can readily incorporate existing objects, such as the devices, files, and directories of a file system, or other independent collections of objects.
- Support the requirements of various operating system environments, such as the ability of a process to inherit resources from a parent process (needed by Windows and Subsystem for UNIX Applications) and the ability to create case-sensitive file names (needed by Subsystem for UNIX Applications).
- Establish uniform rules for object retention (that is, for keeping an object available until all processes have finished using it).
- Provide the ability to isolate objects for a specific session to allow for both local and global objects in the namespace.

As mentioned earlier, we can query these objects with several native APIs but in order to parse them in memory we must understand the method used to save and enumerate these objects.

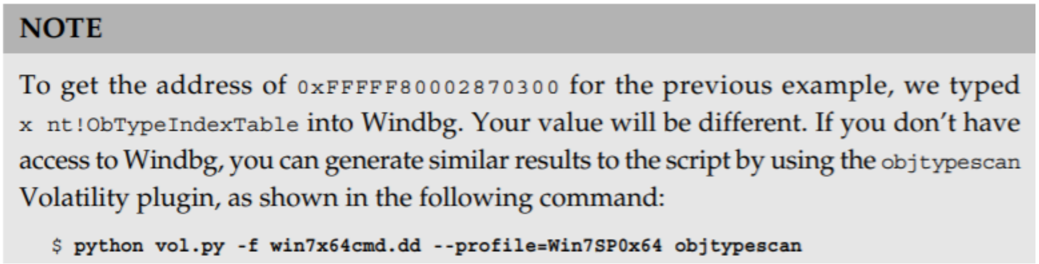
Object Manager for Security Researchers

Every researcher can find use in parsing object directories. Other than general research purposes and helping us with understanding causes for errors, as Digital Forensics investigators we can find attacks under *KnownDlls*, find suspicious objects under specific session's namespace and map the *Object Manager* completely as seen later in this document.

About the Research

The main motivation was the lack of independency when it comes to the enumeration of kernel objects in memory without scanning the entire memory dump for these objects.

A great example of that can be found in Art of Memory Forensics:



NOTE

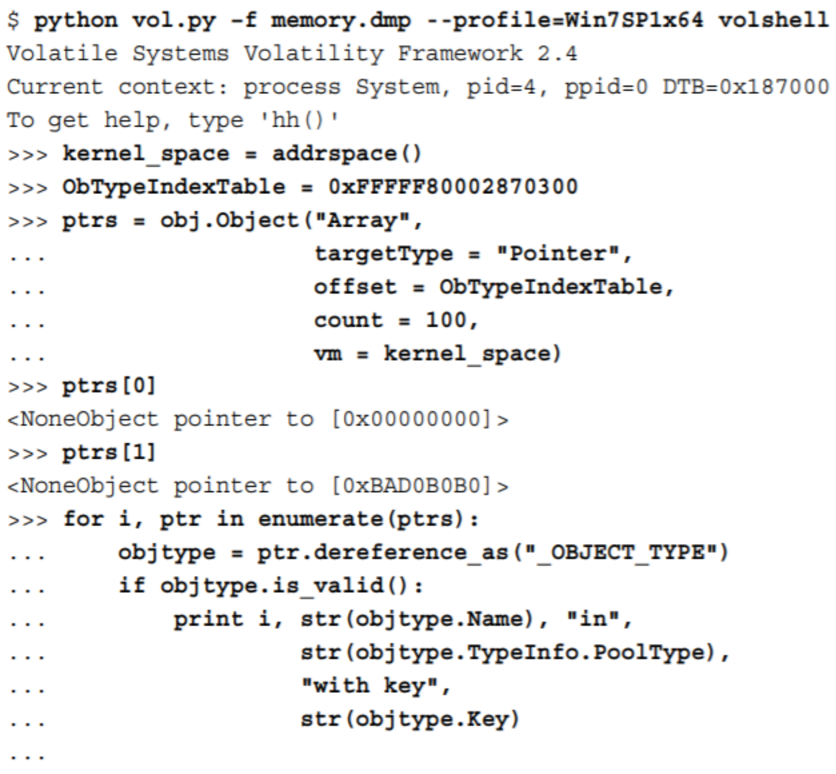
To get the address of `0xFFFFF80002870300` for the previous example, we typed `x nt!ObTypeIndexTable` into Windbg. Your value will be different. If you don't have access to Windbg, you can generate similar results to the script by using the `objtypescan` Volatility plugin, as shown in the following command:

```
$ python vol.py -f win7x64cmd.dd --profile=Win7SP0x64 objtypescan
```

Figure 1 - objtypescan example from Art of Memory Forensics

In the above figure, we can see that it was difficult to find kernel objects without using *Windbg*, and *WinObj* plugin can help us find many of these objects.

A bit earlier in the book, I saw a *volshell* script:



```
$ python vol.py -f memory.dmp --profile=Win7SP1x64 volshell
Volatile Systems Volatility Framework 2.4
Current context: process System, pid=4, ppid=0 DTB=0x187000
To get help, type 'hh()'
>>> kernel_space = addrspace()
>>> ObTypeIndexTable = 0xFFFFF80002870300
>>> ptrs = obj.Object("Array",
...                      targetType = "Pointer",
...                      offset = ObTypeIndexTable,
...                      count = 100,
...                      vm = kernel_space)
>>> ptrs[0]
<NoneObject pointer to [0x00000000]>
>>> ptrs[1]
<NoneObject pointer to [0xBAD0B0B0]>
>>> for i, ptr in enumerate(ptrs):
...     objtype = ptr.dereference_as("_OBJECT_TYPE")
...     if objtype.is_valid():
...         print i, str(objtype.Name), "in",
...                  str(objtype.TypeInfo.PoolType),
...                  "with key",
...                  str(objtype.Key)
...
```

Figure 2 - Art of Memory Forensics enumeration snippet

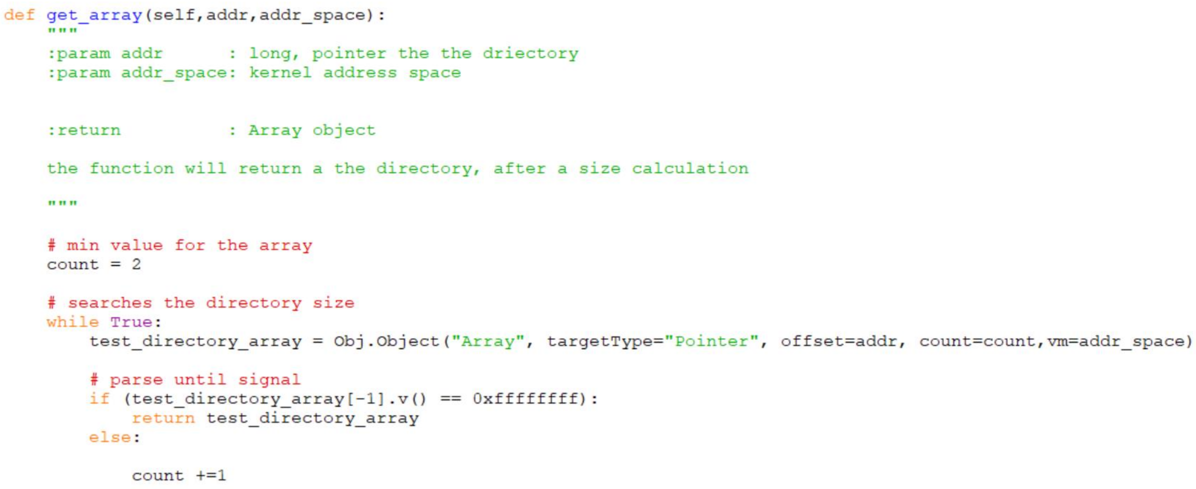
Unfortunately, when I tried it on my memory images it did not work ☹

Moreover, the size of the array will have to be different between Windows platforms because the number of objects will be different, so other than understanding how to enumerate we need to understand when to stop as well.

My first objective was understanding where to begin enumerating objects until I've found what I'm looking for - the root directory. The root directory addresses can be retrieved from the *KDBG* structure. After I retrieved the address, I tried some list entries enumeration and failed, so I needed to find something else.

After some reversing and debugging the mystery was solved.

Let's start from the easy part – when to stop:

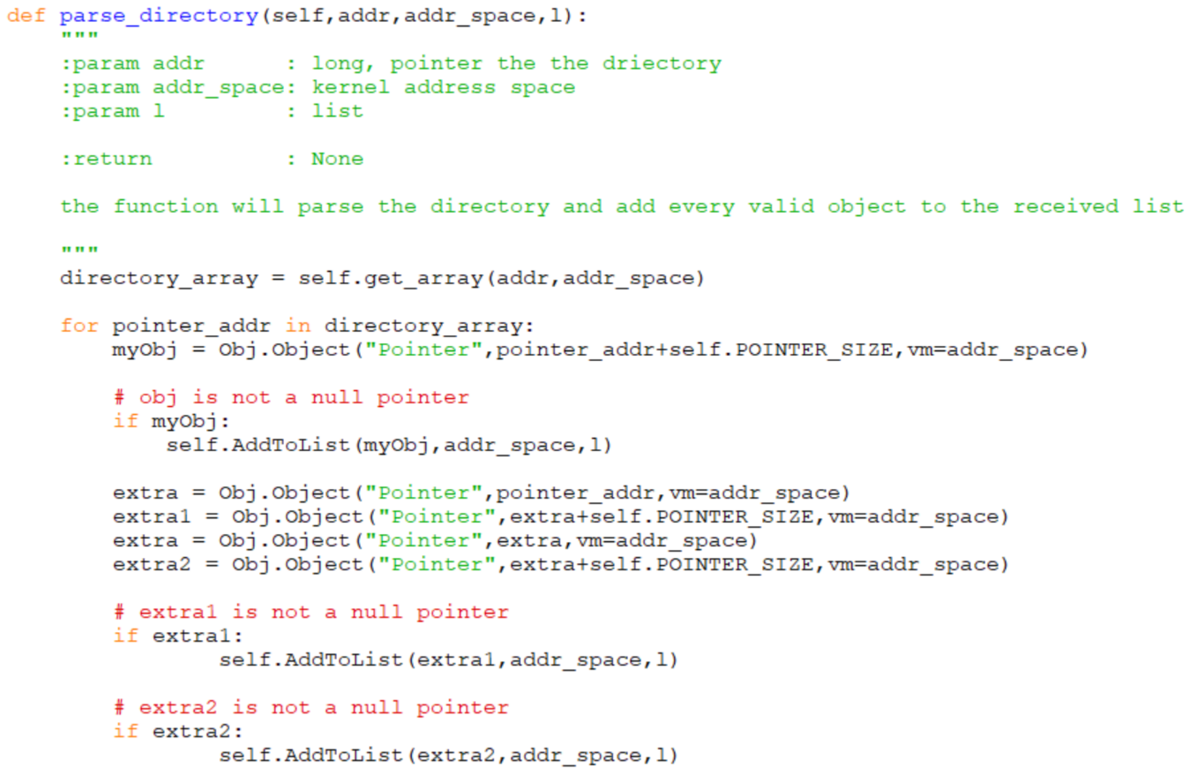


```
def get_array(self,addr,addr_space):
    """
    :param addr      : long, pointer the the driectory
    :param addr_space: kernel address space


    :return          : Array object

    the function will return a the directory, after a size calculation

    """

    # min value for the array
    count = 2

    # searches the directory size
    while True:
        test_directory_array = Obj.Object("Array", targetType="Pointer", offset=addr, count=count,vm=addr_space)

        # parse until signal
        if (test_directory_array[-1].v() == 0xffffffff):
            return test_directory_array
        else:

            count +=1
```

Figure 3 - WinObj get_array function

As you can see in the *get_array* function, the search will be executed until it will find the stop signal that is the same in both platforms x86 and x64.

Now let’s view the enumeration itself.



```
def parse_directory(self,addr,addr_space,l):
    """
    :param addr      : long, pointer the the driectory
    :param addr_space: kernel address space
    :param l         : list

    :return          : None

    the function will parse the directory and add every valid object to the received list

    """
    directory_array = self.get_array(addr,addr_space)

    for pointer_addr in directory_array:
        myObj = Obj.Object("Pointer",pointer_addr+self.POINTER_SIZE,vm=addr_space)

        # obj is not a null pointer
        if myObj:
            self.AddToList(myObj,addr_space,l)

        extra = Obj.Object("Pointer",pointer_addr,vm=addr_space)
        extra1 = Obj.Object("Pointer",extra+self.POINTER_SIZE,vm=addr_space)
        extra = Obj.Object("Pointer",extra,vm=addr_space)
        extra2 = Obj.Object("Pointer",extra+self.POINTER_SIZE,vm=addr_space)

        # extra1 is not a null pointer
        if extra1:
                self.AddToList(extra1,addr_space,l)

        # extra2 is not a null pointer
        if extra2:
                self.AddToList(extra2,addr_space,l)
```

Figure 4 - WinObj Parse-Directory

In this function there are a lot of pointers to pointers, but after jumping through a road of pointers we can finally get an object, parse it by its header and receive useful information about it.

As mentioned earlier, I wanted the plugin to be as generic as possible and due to that it supports all Windows platforms and was tested on Windows XP to Window 10.

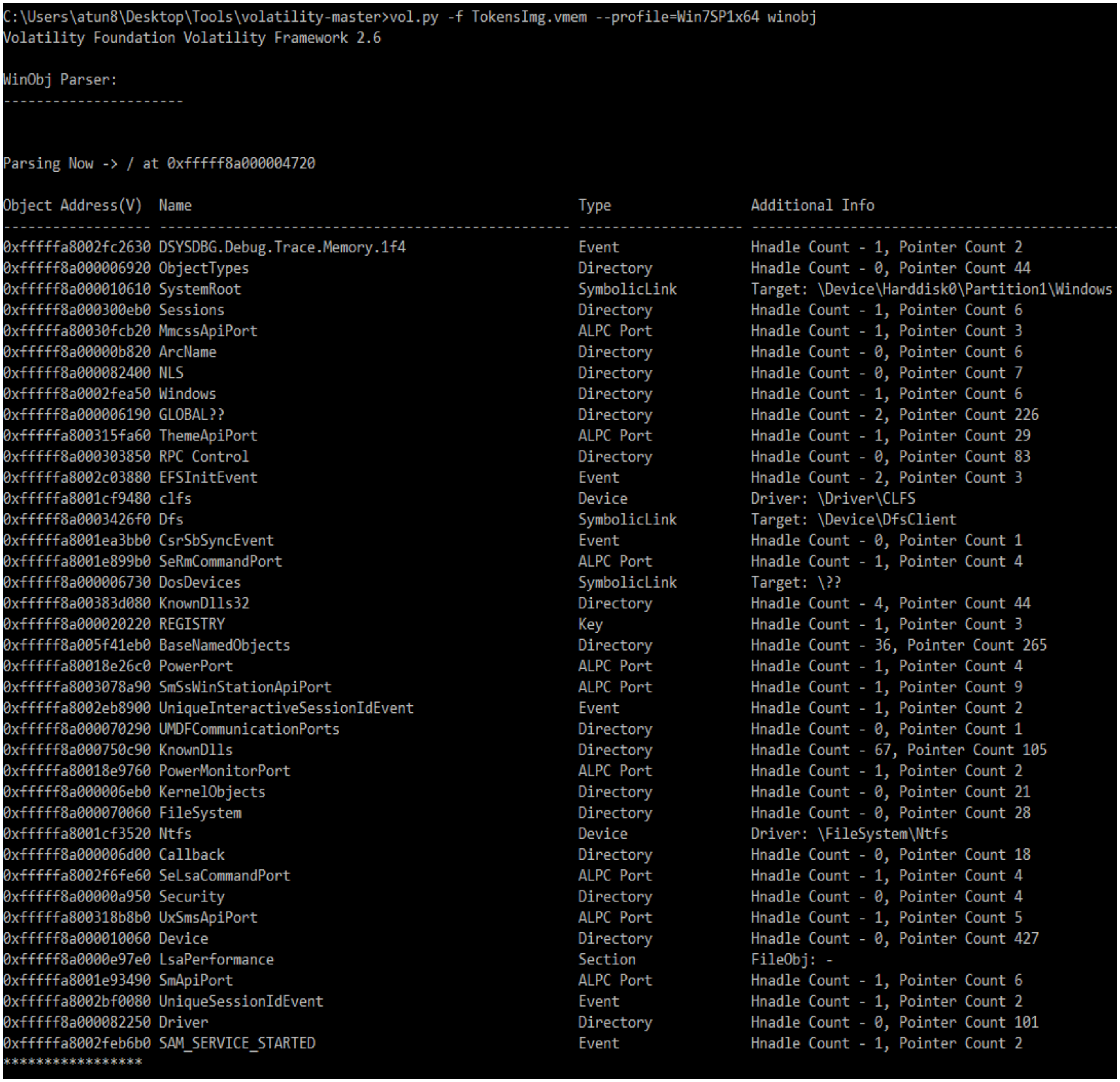
Optional Flags

-P (--FULL-PATH)	Parse a directory found by full path location.
-a (--SUPPLY-ADDR)	Parse directories under specific addresses.
-A (--PARSE-ALL)	Parse every directory under the root directory.

Usage Examples

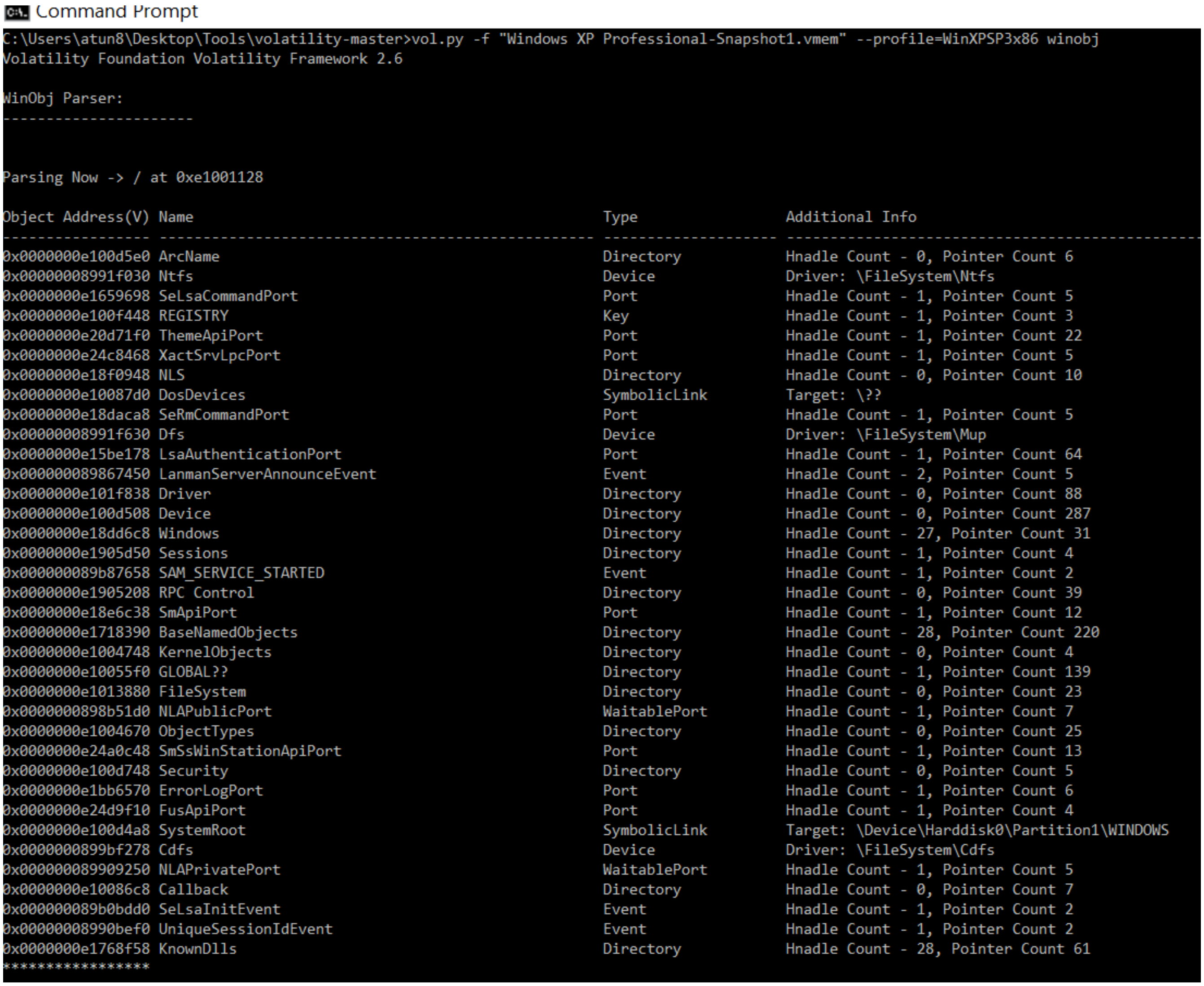
In some examples, we will find the same results as other plugins (i.e. *objtypescan*), and the main difference will be that *WinObj* plugin parses the results without scanning for the requested objects and therefore the output will be significantly faster in large images.

Example 1- Regular output:



```
C:\Users\atun8\Desktop\Tools\volatility-master>vol.py -f TokensImg.vmem --profile=Win7SP1x64 winobj
Volatility Foundation Volatility Framework 2.6

WinObj Parser:
----------------------


Parsing Now -> / at 0xfffff8a000004720

Object Address(V)  Name                                               Type                 Additional Info
------------------ -------------------------------------------------- -------------------- ---------------------------------------------
0xfffffa8002fc2630 DSYSDBG.Debug.Trace.Memory.1f4                     Event                Hnadle Count - 1, Pointer Count 2
0xfffff8a000006920 ObjectTypes                                        Directory            Hnadle Count - 0, Pointer Count 44
0xfffff8a000010610 SystemRoot                                         SymbolicLink         Target: \Device\Harddisk0\Partition1\Windows
0xfffff8a000300eb0 Sessions                                           Directory            Hnadle Count - 1, Pointer Count 6
0xfffffa80030fcb20 MmcssApiPort                                       ALPC Port            Hnadle Count - 1, Pointer Count 3
0xfffff8a00000b820 ArcName                                            Directory            Hnadle Count - 0, Pointer Count 6
0xfffff8a000082400 NLS                                                Directory            Hnadle Count - 0, Pointer Count 7
0xfffff8a0002fea50 Windows                                            Directory            Hnadle Count - 1, Pointer Count 6
0xfffff8a000006190 GLOBAL??                                           Directory            Hnadle Count - 2, Pointer Count 226
0xfffffa800315fa60 ThemeApiPort                                       ALPC Port            Hnadle Count - 1, Pointer Count 29
0xfffff8a000303850 RPC Control                                        Directory            Hnadle Count - 0, Pointer Count 83
0xfffffa8002c03880 EFSInitEvent                                       Event                Hnadle Count - 2, Pointer Count 3
0xfffffa8001cf9480 clfs                                               Device               Driver: \Driver\CLFS
0xfffff8a0003426f0 Dfs                                                SymbolicLink         Target: \Device\DfsClient
0xfffffa8001ea3bb0 CsrSbSyncEvent                                     Event                Hnadle Count - 0, Pointer Count 1
0xfffffa8001e899b0 SeRmCommandPort                                    ALPC Port            Hnadle Count - 1, Pointer Count 4
0xfffff8a000006730 DosDevices                                         SymbolicLink         Target: \??
0xfffff8a00383d080 KnownDlls32                                        Directory            Hnadle Count - 4, Pointer Count 44
0xfffff8a000020220 REGISTRY                                           Key                  Hnadle Count - 1, Pointer Count 3
0xfffff8a005f41eb0 BaseNamedObjects                                   Directory            Hnadle Count - 36, Pointer Count 265
0xfffffa80018e26c0 PowerPort                                          ALPC Port            Hnadle Count - 1, Pointer Count 4
0xfffffa8003078a90 SmSsWinStationApiPort                              ALPC Port            Hnadle Count - 1, Pointer Count 9
0xfffffa8002eb8900 UniqueInteractiveSessionIdEvent                    Event                Hnadle Count - 1, Pointer Count 2
0xfffff8a000070290 UMDFCommunicationPorts                             Directory            Hnadle Count - 0, Pointer Count 1
0xfffff8a000750c90 KnownDlls                                          Directory            Hnadle Count - 67, Pointer Count 105
0xfffffa80018e9760 PowerMonitorPort                                   ALPC Port            Hnadle Count - 1, Pointer Count 2
0xfffff8a000006eb0 KernelObjects                                      Directory            Hnadle Count - 0, Pointer Count 21
0xfffff8a000070060 FileSystem                                         Directory            Hnadle Count - 0, Pointer Count 28
0xfffffa8001cf3520 Ntfs                                               Device               Driver: \FileSystem\Ntfs
0xfffff8a000006d00 Callback                                           Directory            Hnadle Count - 0, Pointer Count 18
0xfffffa8002f6fe60 SeLsaCommandPort                                   ALPC Port            Hnadle Count - 1, Pointer Count 4
0xfffff8a00000a950 Security                                           Directory            Hnadle Count - 0, Pointer Count 4
0xfffffa800318b8b0 UxSmsApiPort                                       ALPC Port            Hnadle Count - 1, Pointer Count 5
0xfffff8a000010060 Device                                             Directory            Hnadle Count - 0, Pointer Count 427
0xfffff8a0000e97e0 LsaPerformance                                     Section              FileObj: -
0xfffffa8001e93490 SmApiPort                                          ALPC Port            Hnadle Count - 1, Pointer Count 6
0xfffffa8002bf0080 UniqueSessionIdEvent                               Event                Hnadle Count - 1, Pointer Count 2
0xfffff8a000082250 Driver                                             Directory            Hnadle Count - 0, Pointer Count 101
0xfffffa8002feb6b0 SAM_SERVICE_STARTED                                Event                Hnadle Count - 1, Pointer Count 2
*****************
```

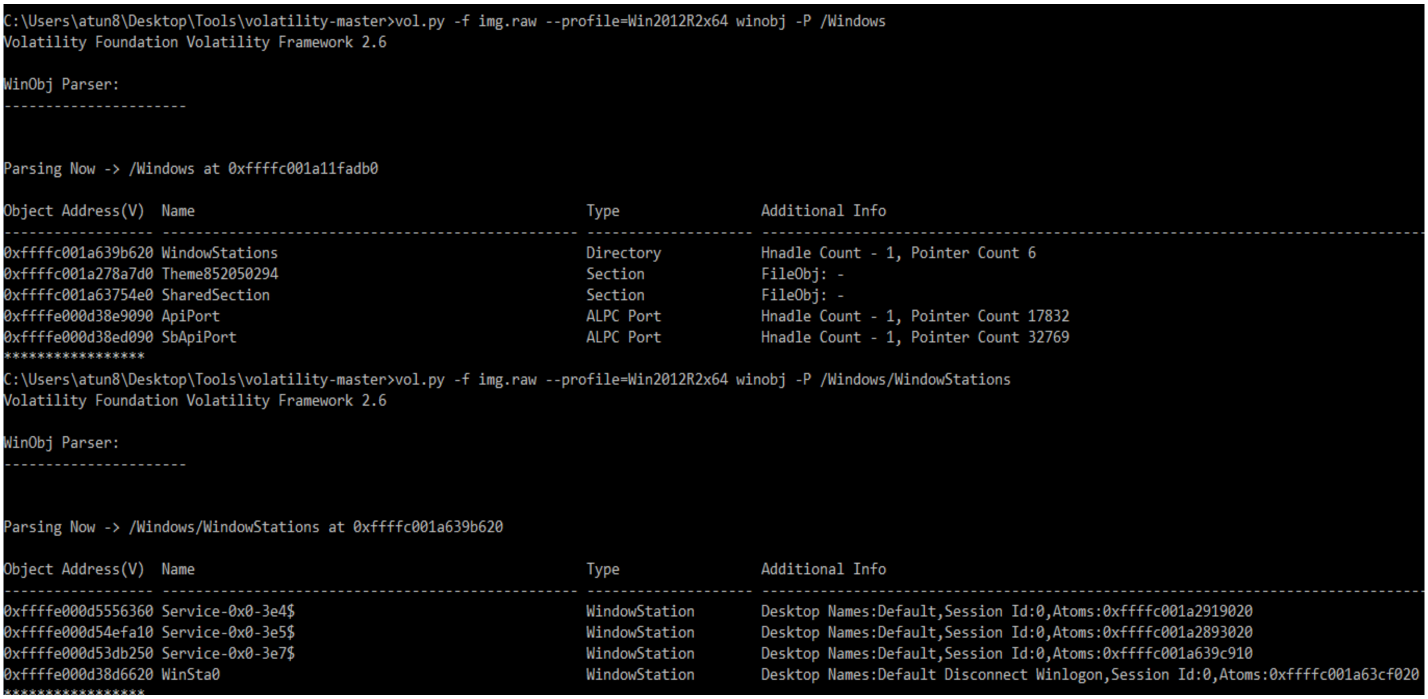
Figure 5 - WinObj output, Windows 7



```
C:\Users\atun8\Desktop\Tools\volatility-master>vol.py -f "Windows XP Professional-Snapshot1.vmem" --profile=WinXPSP3x86 winobj
Volatility Foundation Volatility Framework 2.6

WinObj Parser:
----------------------


Parsing Now -> / at 0xe1001128

Object Address(V) Name                                               Type                 Additional Info
----------------- -------------------------------------------------- -------------------- ------------------------------------------------
0x0000000e100d5e0 ArcName                                            Directory            Hnadle Count - 0, Pointer Count 6
0x00000008991f030 Ntfs                                               Device               Driver: \FileSystem\Ntfs
0x0000000e1659698 SeLsaCommandPort                                   Port                 Hnadle Count - 1, Pointer Count 5
0x0000000e100f448 REGISTRY                                           Key                  Hnadle Count - 1, Pointer Count 3
0x0000000e20d71f0 ThemeApiPort                                       Port                 Hnadle Count - 1, Pointer Count 22
0x0000000e24c8468 XactSrvLpcPort                                     Port                 Hnadle Count - 1, Pointer Count 5
0x0000000e18f0948 NLS                                                Directory            Hnadle Count - 0, Pointer Count 10
0x0000000e10087d0 DosDevices                                         SymbolicLink         Target: \??
0x0000000e18daca8 SeRmCommandPort                                    Port                 Hnadle Count - 1, Pointer Count 5
0x00000008991f630 Dfs                                                Device               Driver: \FileSystem\Mup
0x0000000e15be178 LsaAuthenticationPort                              Port                 Hnadle Count - 1, Pointer Count 64
0x000000089867450 LanmanServerAnnounceEvent                          Event                Hnadle Count - 2, Pointer Count 5
0x0000000e101f838 Driver                                             Directory            Hnadle Count - 0, Pointer Count 88
0x0000000e100d508 Device                                             Directory            Hnadle Count - 0, Pointer Count 287
0x0000000e18dd6c8 Windows                                            Directory            Hnadle Count - 27, Pointer Count 31
0x0000000e1905d50 Sessions                                           Directory            Hnadle Count - 1, Pointer Count 4
0x000000089b87658 SAM_SERVICE_STARTED                                Event                Hnadle Count - 1, Pointer Count 2
0x0000000e1905208 RPC Control                                        Directory            Hnadle Count - 0, Pointer Count 39
0x0000000e18e6c38 SmApiPort                                          Port                 Hnadle Count - 1, Pointer Count 12
0x0000000e1718390 BaseNamedObjects                                   Directory            Hnadle Count - 28, Pointer Count 220
0x0000000e1004748 KernelObjects                                      Directory            Hnadle Count - 0, Pointer Count 4
0x0000000e10055f0 GLOBAL??                                           Directory            Hnadle Count - 1, Pointer Count 139
0x0000000e1013880 FileSystem                                         Directory            Hnadle Count - 0, Pointer Count 23
0x0000000898b51d0 NLAPublicPort                                      WaitablePort         Hnadle Count - 1, Pointer Count 7
0x0000000e1004670 ObjectTypes                                        Directory            Hnadle Count - 0, Pointer Count 25
0x0000000e24a0c48 SmSsWinStationApiPort                              Port                 Hnadle Count - 1, Pointer Count 13
0x0000000e100d748 Security                                           Directory            Hnadle Count - 0, Pointer Count 5
0x0000000e1bb6570 ErrorLogPort                                       Port                 Hnadle Count - 1, Pointer Count 6
0x0000000e24d9f10 FusApiPort                                         Port                 Hnadle Count - 1, Pointer Count 4
0x0000000e100d4a8 SystemRoot                                         SymbolicLink         Target: \Device\Harddisk0\Partition1\WINDOWS
0x00000000899bf278 Cdfs                                              Device               Driver: \FileSystem\Cdfs
0x000000089909250 NLAPrivatePort                                     WaitablePort         Hnadle Count - 1, Pointer Count 5
0x0000000e10086c8 Callback                                           Directory            Hnadle Count - 0, Pointer Count 7
0x000000089b0bdd0 SeLsaInitEvent                                     Event                Hnadle Count - 1, Pointer Count 2
0x00000008990bef0 UniqueSessionIdEvent                               Event                Hnadle Count - 1, Pointer Count 2
0x0000000e1768f58 KnownDlls                                          Directory            Hnadle Count - 28, Pointer Count 61
*****************
```

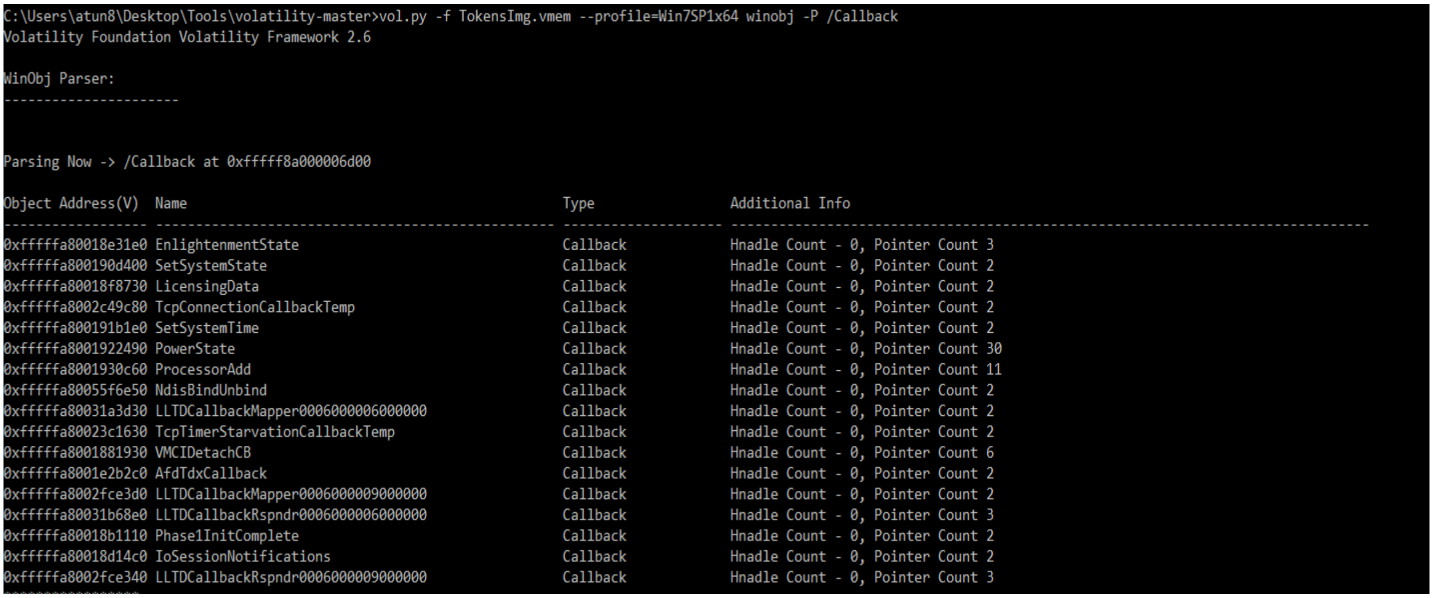
Figure 6 - WinObj output snippet Windows XP

Example 2: Using Path flag.



```
C:\Users\atun8\Desktop\Tools\volatility-master>vol.py -f img.raw --profile=Win2012R2x64 winobj -P /Windows
Volatility Foundation Volatility Framework 2.6

WinObj Parser:
----------------------



Parsing Now -> /Windows at 0xffffc001a11fadb0

Object Address(V)  Name                                               Type                Additional Info
------------------ -------------------------------------------------- ------------------- --------------------------------------------------------------------------------
0xffffc001a639b620 WindowStations                                     Directory           Hnadle Count - 1, Pointer Count 6
0xffffc001a278a7d0 Theme852050294                                     Section             FileObj: -
0xffffc001a63754e0 SharedSection                                      Section             FileObj: -
0xffffe000d38e9090 ApiPort                                            ALPC Port           Hnadle Count - 1, Pointer Count 17832
0xffffe000d38ed090 SbApiPort                                          ALPC Port           Hnadle Count - 1, Pointer Count 32769
*****************
C:\Users\atun8\Desktop\Tools\volatility-master>vol.py -f img.raw --profile=Win2012R2x64 winobj -P /Windows/WindowStations
Volatility Foundation Volatility Framework 2.6

WinObj Parser:
----------------------



Parsing Now -> /Windows/WindowStations at 0xffffc001a639b620

Object Address(V)  Name                                               Type                Additional Info
------------------ -------------------------------------------------- ------------------- --------------------------------------------------------------------------------
0xffffe000d5556360 Service-0x0-3e4$                                   WindowStation       Desktop Names:Default,Session Id:0,Atoms:0xffffc001a2919020
0xffffe000d54efa10 Service-0x0-3e5$                                   WindowStation       Desktop Names:Default,Session Id:0,Atoms:0xffffc001a2893020
0xffffe000d53db250 Service-0x0-3e7$                                   WindowStation       Desktop Names:Default,Session Id:0,Atoms:0xffffc001a639c910
0xffffe000d38d6620 WinSta0                                            WindowStation       Desktop Names:Default Disconnect Winlogon,Session Id:0,Atoms:0xffffc001a63cf020
*****************
```

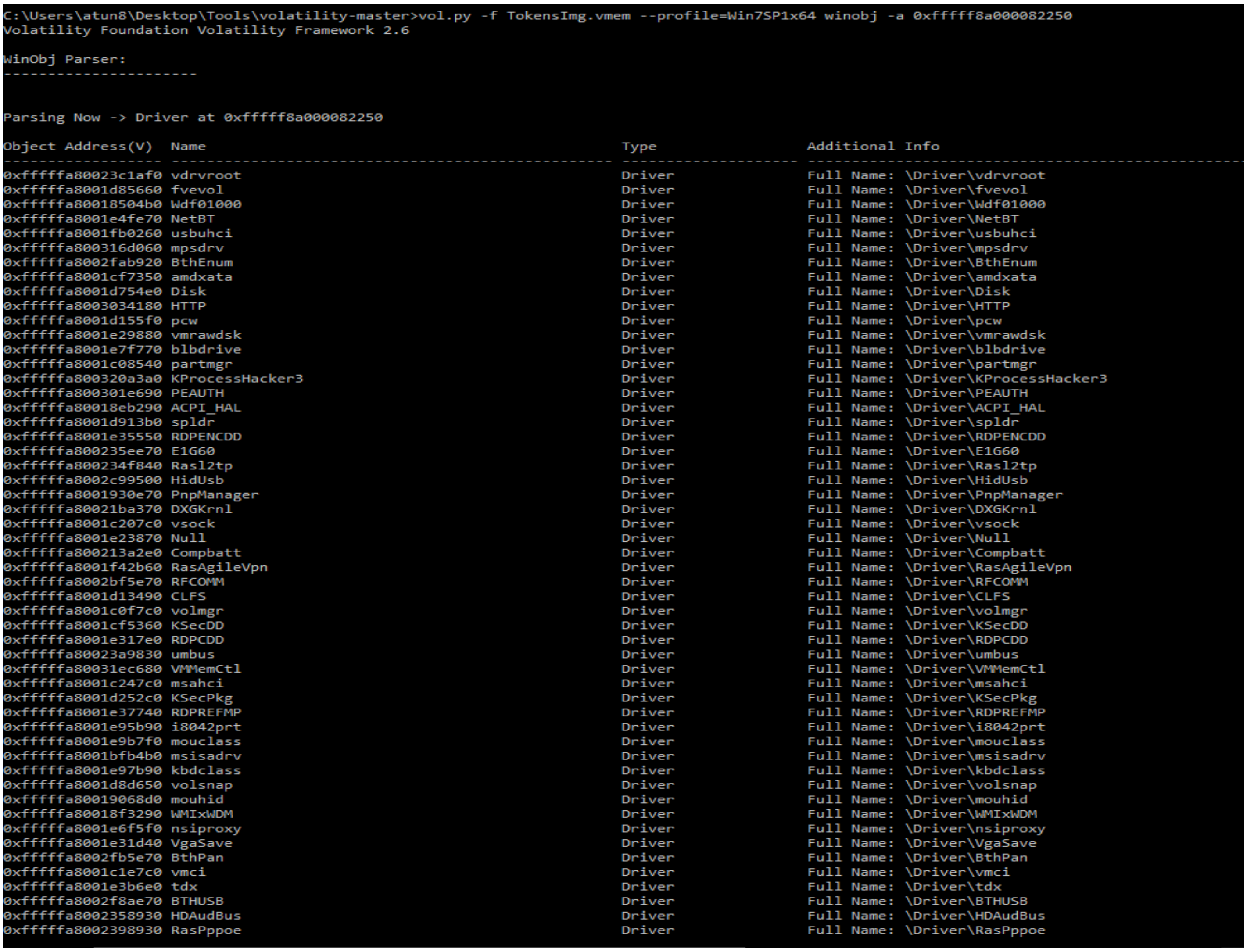
Figure 7 - Example for "traveling" inside the object manager's namespace



```
C:\Users\atun8\Desktop\Tools\volatility-master>vol.py -f TokensImg.vmem --profile=Win7SP1x64 winobj -P /Callback
Volatility Foundation Volatility Framework 2.6

WinObj Parser:
----------------------



Parsing Now -> /Callback at 0xfffff8a000006d00

Object Address(V)  Name                                               Type                Additional Info
------------------ -------------------------------------------------- ------------------- --------------------------------------------------------------------------------
0xfffffa80018e31e0 EnlightenmentState                                 Callback            Hnadle Count - 0, Pointer Count 3
0xfffffa800190d400 SetSystemState                                     Callback            Hnadle Count - 0, Pointer Count 2
0xfffffa80018f8730 LicensingData                                      Callback            Hnadle Count - 0, Pointer Count 2
0xfffffa8002c49c80 TcpConnectionCallbackTemp                          Callback            Hnadle Count - 0, Pointer Count 2
0xfffffa800191b1e0 SetSystemTime                                      Callback            Hnadle Count - 0, Pointer Count 2
0xfffffa8001922490 PowerState                                         Callback            Hnadle Count - 0, Pointer Count 30
0xfffffa8001930c60 ProcessorAdd                                       Callback            Hnadle Count - 0, Pointer Count 11
0xfffffa80055f6e50 NdisBindUnbind                                     Callback            Hnadle Count - 0, Pointer Count 2
0xfffffa80031a3d30 LLTDCallbackMapper0006000006000000                 Callback            Hnadle Count - 0, Pointer Count 2
0xfffffa80023c1630 TcpTimerStarvationCallbackTemp                     Callback            Hnadle Count - 0, Pointer Count 2
0xfffffa8001881930 VMCIDetachCB                                       Callback            Hnadle Count - 0, Pointer Count 6
0xfffffa8001e2b2c0 AfdTdxCallback                                     Callback            Hnadle Count - 0, Pointer Count 2
0xfffffa8002fce3d0 LLTDCallbackMapper0006000009000000                 Callback            Hnadle Count - 0, Pointer Count 2
0xfffffa80031b68e0 LLTDCallbackRspndr0006000006000000                 Callback            Hnadle Count - 0, Pointer Count 3
0xfffffa80018b1110 Phase1InitComplete                                 Callback            Hnadle Count - 0, Pointer Count 2
0xfffffa80018d14c0 IoSessionNotifications                             Callback            Hnadle Count - 0, Pointer Count 2
0xfffffa8002fce340 LLTDCallbackRspndr0006000009000000                 Callback            Hnadle Count - 0, Pointer Count 3
```

Figure 8 - /Callback enumeration using path flag

Example 3: Address flag.



```
C:\Users\atun8\Desktop\Tools\volatility-master>vol.py -f TokensImg.vmem --profile=Win7SP1x64 winobj -a 0xfffff8a000082250
Volatility Foundation Volatility Framework 2.6

WinObj Parser:
----------------------


Parsing Now -> Driver at 0xfffff8a000082250

Object Address(V)  Name                                               Type                 Additional Info
------------------ -------------------------------------------------- -------------------- -------------------------------------------------
0xfffffa80023c1af0 vdrvroot                                           Driver               Full Name: \Driver\vdrvroot
0xfffffa8001d85660 fvevol                                             Driver               Full Name: \Driver\fvevol
0xfffffa80018504b0 Wdf01000                                           Driver               Full Name: \Driver\Wdf01000
0xfffffa8001e4fe70 NetBT                                              Driver               Full Name: \Driver\NetBT
0xfffffa8001fb0260 usbuhci                                            Driver               Full Name: \Driver\usbuhci
0xfffffa800316d060 mpsdrv                                             Driver               Full Name: \Driver\mpsdrv
0xfffffa8002fab920 BthEnum                                            Driver               Full Name: \Driver\BthEnum
0xfffffa8001cf7350 amdxata                                            Driver               Full Name: \Driver\amdxata
0xfffffa8001d754e0 Disk                                               Driver               Full Name: \Driver\Disk
0xfffffa8003034180 HTTP                                               Driver               Full Name: \Driver\HTTP
0xfffffa8001d155f0 pcw                                                Driver               Full Name: \Driver\pcw
0xfffffa8001e29880 vmrawdsk                                           Driver               Full Name: \Driver\vmrawdsk
0xfffffa8001e7f770 blbdrive                                           Driver               Full Name: \Driver\blbdrive
0xfffffa8001c08540 partmgr                                            Driver               Full Name: \Driver\partmgr
0xfffffa800320a3a0 KProcessHacker3                                    Driver               Full Name: \Driver\KProcessHacker3
0xfffffa800301e690 PEAUTH                                             Driver               Full Name: \Driver\PEAUTH
0xfffffa80018eb290 ACPI_HAL                                           Driver               Full Name: \Driver\ACPI_HAL
0xfffffa8001d913b0 spldr                                              Driver               Full Name: \Driver\spldr
0xfffffa8001e35550 RDPENCDD                                           Driver               Full Name: \Driver\RDPENCDD
0xfffffa800235ee70 E1G60                                              Driver               Full Name: \Driver\E1G60
0xfffffa800234f840 Rasl2tp                                            Driver               Full Name: \Driver\Rasl2tp
0xfffffa8002c99500 HidUsb                                             Driver               Full Name: \Driver\HidUsb
0xfffffa8001930e70 PnpManager                                         Driver               Full Name: \Driver\PnpManager
0xfffffa80021ba370 DXGKrnl                                            Driver               Full Name: \Driver\DXGKrnl
0xfffffa8001c207c0 vsock                                              Driver               Full Name: \Driver\vsock
0xfffffa8001e23870 Null                                               Driver               Full Name: \Driver\Null
0xfffffa800213a2e0 Compbatt                                           Driver               Full Name: \Driver\Compbatt
0xfffffa8001f42b60 RasAgileVpn                                        Driver               Full Name: \Driver\RasAgileVpn
0xfffffa8002bf5e70 RFCOMM                                             Driver               Full Name: \Driver\RFCOMM
0xfffffa8001d13490 CLFS                                               Driver               Full Name: \Driver\CLFS
0xfffffa8001c0f7c0 volmgr                                             Driver               Full Name: \Driver\volmgr
0xfffffa8001cf5360 KSecDD                                             Driver               Full Name: \Driver\KSecDD
0xfffffa8001e317e0 RDPCDD                                             Driver               Full Name: \Driver\RDPCDD
0xfffffa80023a9830 umbus                                              Driver               Full Name: \Driver\umbus
0xfffffa80031ec680 VMMemCtl                                           Driver               Full Name: \Driver\VMMemCtl
0xfffffa8001c247c0 msahci                                             Driver               Full Name: \Driver\msahci
0xfffffa8001d252c0 KSecPkg                                            Driver               Full Name: \Driver\KSecPkg
0xfffffa8001e37740 RDPREFMP                                           Driver               Full Name: \Driver\RDPREFMP
0xfffffa8001e95b90 i8042prt                                           Driver               Full Name: \Driver\i8042prt
0xfffffa8001e9b7f0 mouclass                                           Driver               Full Name: \Driver\mouclass
0xfffffa8001bfb4b0 msisadrv                                           Driver               Full Name: \Driver\msisadrv
0xfffffa8001e97b90 kbdclass                                           Driver               Full Name: \Driver\kbdclass
0xfffffa8001d8d650 volsnap                                            Driver               Full Name: \Driver\volsnap
0xfffffa80019068d0 mouhid                                             Driver               Full Name: \Driver\mouhid
0xfffffa80018f3290 WMIxWDM                                            Driver               Full Name: \Driver\WMIxWDM
0xfffffa8001e6f5f0 nsiproxy                                           Driver               Full Name: \Driver\nsiproxy
0xfffffa8001e31d40 VgaSave                                            Driver               Full Name: \Driver\VgaSave
0xfffffa8002fb5e70 BthPan                                             Driver               Full Name: \Driver\BthPan
0xfffffa8001c1e7c0 vmci                                               Driver               Full Name: \Driver\vmci
0xfffffa8001e3b6e0 tdx                                                Driver               Full Name: \Driver\tdx
0xfffffa8002f8ae70 BTHUSB                                             Driver               Full Name: \Driver\BTHUSB
0xfffffa8002358930 HDAudBus                                           Driver               Full Name: \Driver\HDAudBus
0xfffffa8002398930 RasPppoe                                           Driver               Full Name: \Driver\RasPppoe
```

/Driver enumeration using the address flag

KnownDlls Case Study

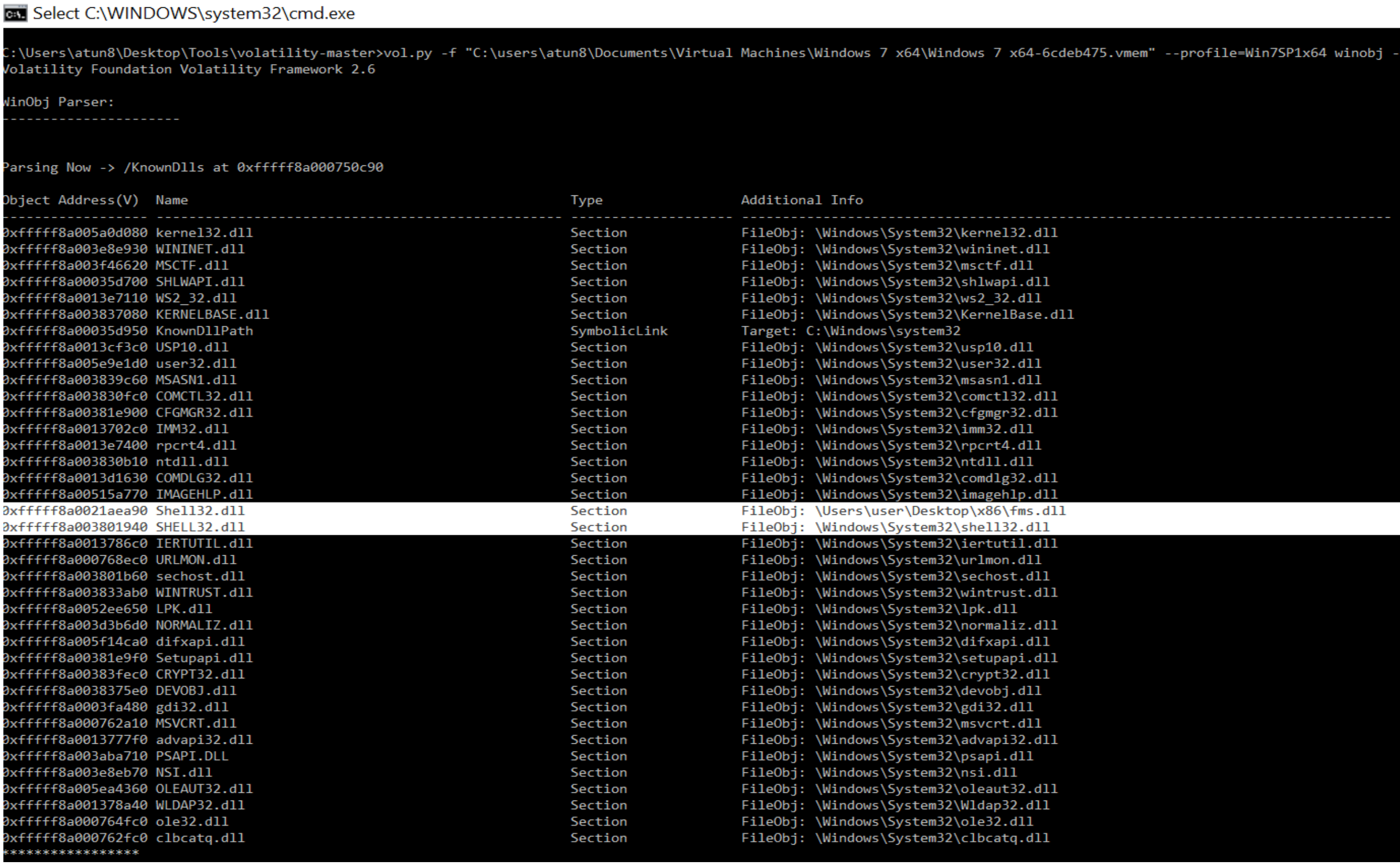
An interesting directory to enumerate is the *KnownDlls/KnownDlls32* directory and parsing it can be extremely useful (KnownDlls).

There are some known attacks in that surface. You can find great examples in the below links:

- https://www.codeproject.com/Articles/325603/Injection-into-a-Process-Using-KnownDlls
- https://modexp.wordpress.com/2019/08/12/windows-process-injection-knowndlls/

With the ability of parsing the *KnownDlls* directory from memory, we can identify the attacks above in two major methods:

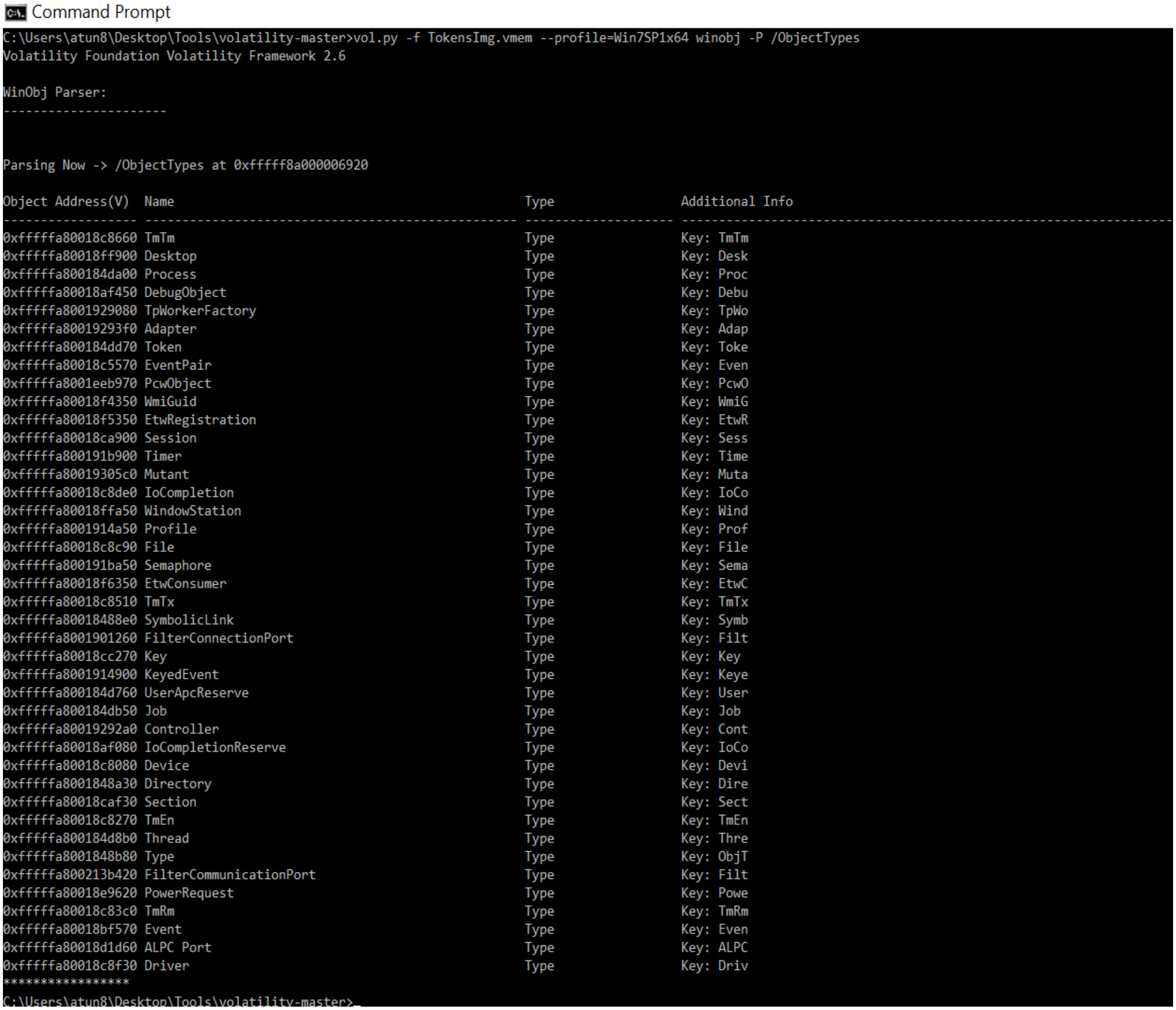
- The first, parsing the *KnownDlls* and look for hooks
- The second, if we suspect that there was an injection using *KnownDlls* pointer replacing, we can follow these steps:
    1. Take the address of the directory using the *handles* plugin.
    2. Validate the address via comparing with the address shown in *Winobj* plugin.
    3. If there is indeed an injection, we can detect the infected Dlls using *Winobj* plugin with the –A flag to the address we already found in step 1.



```
C:\Users\atun8\Desktop\Tools\volatility-master>vol.py -f "C:\users\atun8\Documents\Virtual Machines\Windows 7 x64\Windows 7 x64-6cdeb475.vmem" --profile=Win7SP1x64 winobj -
Volatility Foundation Volatility Framework 2.6

WinObj Parser:
----------------------


Parsing Now -> /KnownDlls at 0xfffff8a000750c90

Object Address(V)  Name                                               Type                 Additional Info
------------------ -------------------------------------------------- -------------------- --------------------------------------------------------------------------------
0xfffff8a005a0d080 kernel32.dll                                       Section              FileObj: \Windows\System32\kernel32.dll
0xfffff8a003e8e930 WININET.dll                                        Section              FileObj: \Windows\System32\wininet.dll
0xfffff8a003f46620 MSCTF.dll                                          Section              FileObj: \Windows\System32\msctf.dll
0xfffff8a00035d700 SHLWAPI.dll                                        Section              FileObj: \Windows\System32\shlwapi.dll
0xfffff8a0013e7110 WS2_32.dll                                         Section              FileObj: \Windows\System32\ws2_32.dll
0xfffff8a003837080 KERNELBASE.dll                                     Section              FileObj: \Windows\System32\KernelBase.dll
0xfffff8a00035d950 KnownDllPath                                       SymbolicLink         Target: C:\Windows\system32
0xfffff8a0013cf3c0 USP10.dll                                          Section              FileObj: \Windows\System32\usp10.dll
0xfffff8a005e9e1d0 user32.dll                                         Section              FileObj: \Windows\System32\user32.dll
0xfffff8a003839c60 MSASN1.dll                                         Section              FileObj: \Windows\System32\msasn1.dll
0xfffff8a003830fc0 COMCTL32.dll                                       Section              FileObj: \Windows\System32\comctl32.dll
0xfffff8a00381e900 CFGMGR32.dll                                       Section              FileObj: \Windows\System32\cfgmgr32.dll
0xfffff8a0013702c0 IMM32.dll                                          Section              FileObj: \Windows\System32\imm32.dll
0xfffff8a0013e7400 rpcrt4.dll                                         Section              FileObj: \Windows\System32\rpcrt4.dll
0xfffff8a003830b10 ntdll.dll                                          Section              FileObj: \Windows\System32\ntdll.dll
0xfffff8a0013d1630 COMDLG32.dll                                       Section              FileObj: \Windows\System32\comdlg32.dll
0xfffff8a00515a770 IMAGEHLP.dll                                       Section              FileObj: \Windows\System32\imagehlp.dll
0xfffff8a0021aea90 Shell32.dll                                        Section              FileObj: \Users\user\Desktop\x86\fms.dll
0xfffff8a003801940 SHELL32.dll                                        Section              FileObj: \Windows\System32\shell32.dll
0xfffff8a0013786c0 IERTUTIL.dll                                       Section              FileObj: \Windows\System32\iertutil.dll
0xfffff8a000768ec0 URLMON.dll                                         Section              FileObj: \Windows\System32\urlmon.dll
0xfffff8a003801b60 sechost.dll                                        Section              FileObj: \Windows\System32\sechost.dll
0xfffff8a003833ab0 WINTRUST.dll                                       Section              FileObj: \Windows\System32\wintrust.dll
0xfffff8a0052ee650 LPK.dll                                            Section              FileObj: \Windows\System32\lpk.dll
0xfffff8a003d3b6d0 NORMALIZ.dll                                       Section              FileObj: \Windows\System32\normaliz.dll
0xfffff8a005f14ca0 difxapi.dll                                        Section              FileObj: \Windows\System32\difxapi.dll
0xfffff8a00381e9f0 Setupapi.dll                                       Section              FileObj: \Windows\System32\setupapi.dll
0xfffff8a00383fec0 CRYPT32.dll                                        Section              FileObj: \Windows\System32\crypt32.dll
0xfffff8a0038375e0 DEVOBJ.dll                                         Section              FileObj: \Windows\System32\devobj.dll
0xfffff8a0003fa480 gdi32.dll                                          Section              FileObj: \Windows\System32\gdi32.dll
0xfffff8a000762a10 MSVCRT.dll                                         Section              FileObj: \Windows\System32\msvcrt.dll
0xfffff8a0013777f0 advapi32.dll                                       Section              FileObj: \Windows\System32\advapi32.dll
0xfffff8a003aba710 PSAPI.DLL                                          Section              FileObj: \Windows\System32\psapi.dll
0xfffff8a003e8eb70 NSI.dll                                            Section              FileObj: \Windows\System32\nsi.dll
0xfffff8a005ea4360 OLEAUT32.dll                                       Section              FileObj: \Windows\System32\oleaut32.dll
0xfffff8a001378a40 WLDAP32.dll                                        Section              FileObj: \Windows\System32\Wldap32.dll
0xfffff8a000764fc0 ole32.dll                                          Section              FileObj: \Windows\System32\ole32.dll
0xfffff8a000762fc0 clbcatq.dll                                        Section              FileObj: \Windows\System32\clbcatq.dll
*****************
```

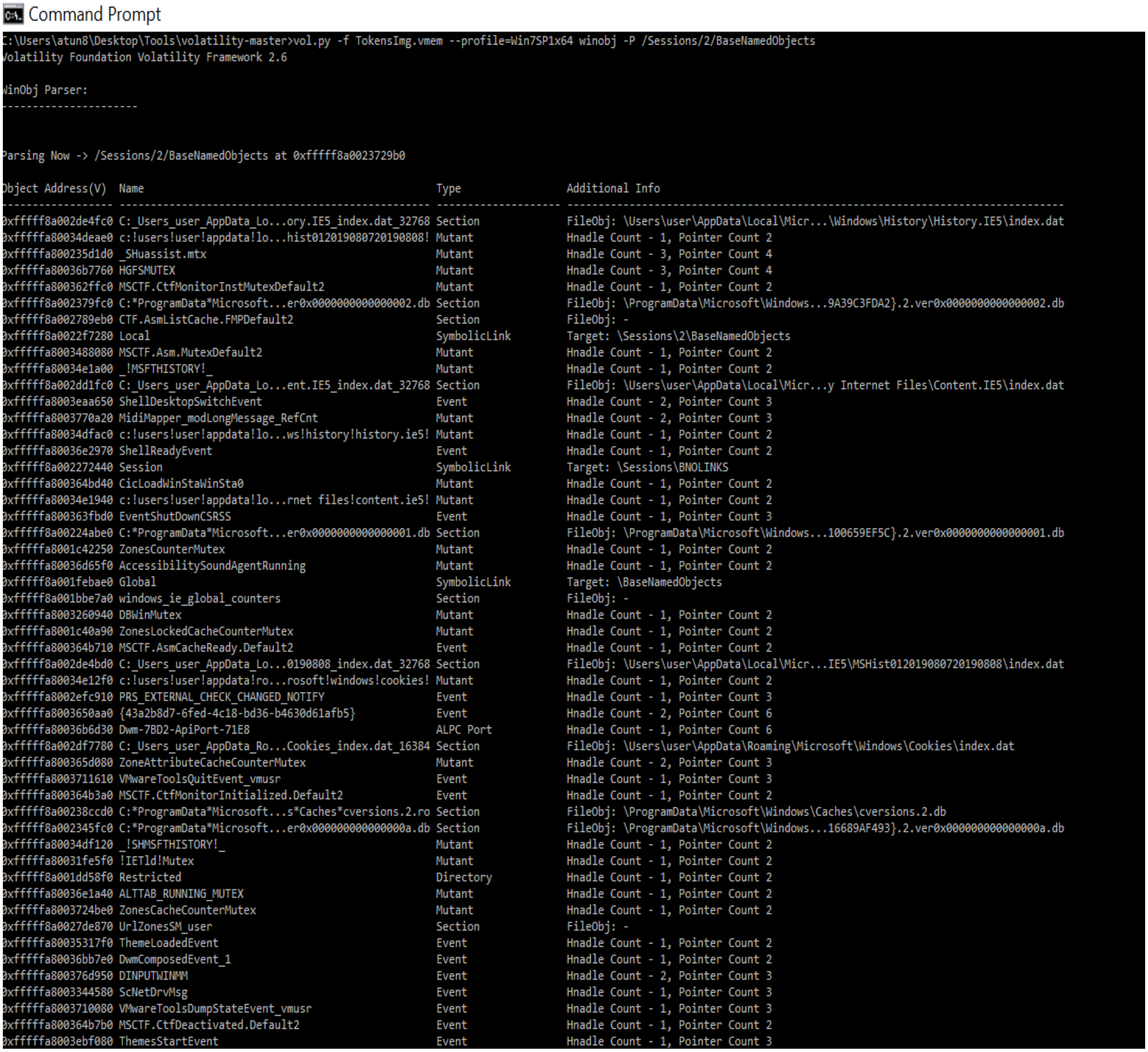
KnownDlls hook example

More Useful Examples



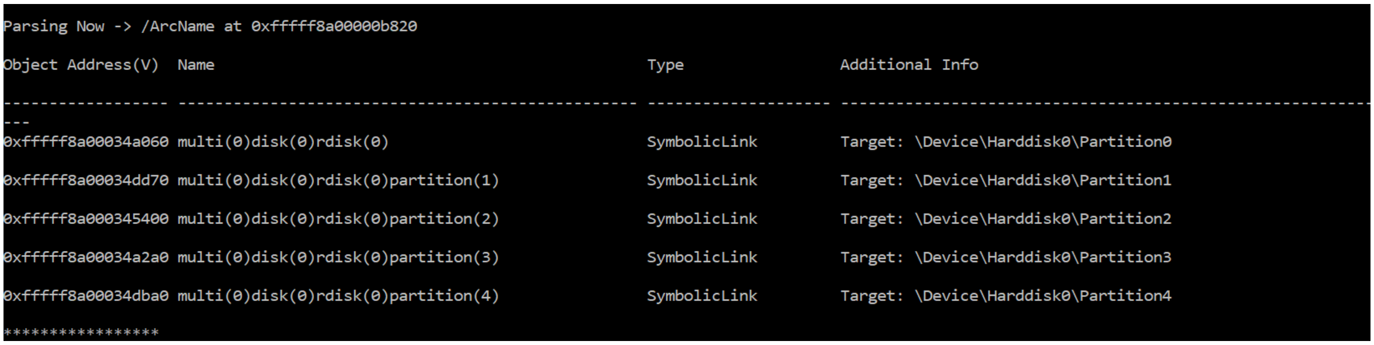
```
C:\Users\atun8\Desktop\Tools\volatility-master>vol.py -f TokensImg.vmem --profile=Win7SP1x64 winobj -P /ObjectTypes
Volatility Foundation Volatility Framework 2.6

WinObj Parser:
----------------------


Parsing Now -> /ObjectTypes at 0xfffff8a000006920

Object Address(V)  Name                                               Type                 Additional Info
------------------ -------------------------------------------------- -------------------- ------------------------------------------------------------------
0xfffffa80018c8660 TmTm                                               Type                 Key: TmTm
0xfffffa80018ff900 Desktop                                            Type                 Key: Desk
0xfffffa800184da00 Process                                            Type                 Key: Proc
0xfffffa80018af450 DebugObject                                        Type                 Key: Debu
0xfffffa8001929080 TpWorkerFactory                                    Type                 Key: TpWo
0xfffffa80019293f0 Adapter                                            Type                 Key: Adap
0xfffffa800184dd70 Token                                              Type                 Key: Toke
0xfffffa80018c5570 EventPair                                          Type                 Key: Even
0xfffffa8001eeb970 PcwObject                                          Type                 Key: PcwO
0xfffffa80018f4350 WmiGuid                                            Type                 Key: WmiG
0xfffffa80018f5350 EtwRegistration                                    Type                 Key: EtwR
0xfffffa80018ca900 Session                                            Type                 Key: Sess
0xfffffa800191b900 Timer                                              Type                 Key: Time
0xfffffa80019305c0 Mutant                                             Type                 Key: Muta
0xfffffa80018c8de0 IoCompletion                                       Type                 Key: IoCo
0xfffffa80018ffa50 WindowStation                                      Type                 Key: Wind
0xfffffa8001914a50 Profile                                            Type                 Key: Prof
0xfffffa80018c8c90 File                                               Type                 Key: File
0xfffffa800191ba50 Semaphore                                          Type                 Key: Sema
0xfffffa80018f6350 EtwConsumer                                        Type                 Key: EtwC
0xfffffa80018c8510 TmTx                                               Type                 Key: TmTx
0xfffffa80018488e0 SymbolicLink                                       Type                 Key: Symb
0xfffffa8001901260 FilterConnectionPort                               Type                 Key: Filt
0xfffffa80018cc270 Key                                                Type                 Key: Key
0xfffffa8001914900 KeyedEvent                                         Type                 Key: Keye
0xfffffa800184d760 UserApcReserve                                     Type                 Key: User
0xfffffa800184db50 Job                                                Type                 Key: Job
0xfffffa80019292a0 Controller                                         Type                 Key: Cont
0xfffffa80018af080 IoCompletionReserve                                Type                 Key: IoCo
0xfffffa80018c8080 Device                                             Type                 Key: Devi
0xfffffa8001848a30 Directory                                          Type                 Key: Dire
0xfffffa80018caf30 Section                                            Type                 Key: Sect
0xfffffa80018c8270 TmEn                                               Type                 Key: TmEn
0xfffffa800184d8b0 Thread                                             Type                 Key: Thre
0xfffffa8001848b80 Type                                               Type                 Key: ObjT
0xfffffa800213b420 FilterCommunicationPort                            Type                 Key: Filt
0xfffffa80018e9620 PowerRequest                                       Type                 Key: Powe
0xfffffa80018c83c0 TmRm                                               Type                 Key: TmRm
0xfffffa80018bf570 Event                                              Type                 Key: Even
0xfffffa80018d1d60 ALPC Port                                          Type                 Key: ALPC
0xfffffa80018c8f30 Driver                                             Type                 Key: Driv
*****************
C:\Users\atun8\Desktop\Tools\volatility-master>_
```

Get object type list



```
C:\Users\atun8\Desktop\Tools\volatility-master>vol.py -f TokensImg.vmem --profile=Win7SP1x64 winobj -P /Sessions/2/BaseNamedObjects
Volatility Foundation Volatility Framework 2.6

WinObj Parser:
---------------------


Parsing Now -> /Sessions/2/BaseNamedObjects at 0xfffff8a0023729b0

Object Address(V)  Name                                               Type               Additional Info
------------------ -------------------------------------------------- ------------------ --------------------------------------------------------------------------------
0xfffff8a002de4fc0 C:_Users_user_AppData_Lo...ory.IE5_index.dat_32768 Section            FileObj: \Users\user\AppData\Local\Micr...\Windows\History\History.IE5\index.dat
0xfffffa80034deae0 c:!users!user!appdata!lo...hist012019080720190808! Mutant             Hnadle Count - 1, Pointer Count 2
0xfffffa800235d1d0 _SHuassist.mtx                                     Mutant             Hnadle Count - 3, Pointer Count 4
0xfffffa80036b7760 HGFSMUTEX                                          Mutant             Hnadle Count - 3, Pointer Count 4
0xfffffa800362ffc0 MSCTF.CtfMonitorInstMutexDefault2                  Mutant             Hnadle Count - 1, Pointer Count 2
0xfffff8a002379fc0 C:*ProgramData*Microsoft...er0x0000000000000002.db Section            FileObj: \ProgramData\Microsoft\Windows...9A39C3FDA2}.2.ver0x0000000000000002.db
0xfffff8a002789eb0 CTF.AsmListCache.FMPDefault2                       Section            FileObj: -
0xfffff8a0022f7280 Local                                              SymbolicLink       Target: \Sessions\2\BaseNamedObjects
0xfffffa8003488080 MSCTF.Asm.MutexDefault2                            Mutant             Hnadle Count - 1, Pointer Count 2
0xfffffa80034e1a00 _!MSFTHISTORY!_                                    Mutant             Hnadle Count - 1, Pointer Count 2
0xfffff8a002dd1fc0 C:_Users_user_AppData_Lo...ent.IE5_index.dat_32768 Section            FileObj: \Users\user\AppData\Local\Micr...y Internet Files\Content.IE5\index.dat
0xfffffa8003eaa650 ShellDesktopSwitchEvent                            Event              Hnadle Count - 2, Pointer Count 3
0xfffffa8003770a20 MidiMapper_modLongMessage_RefCnt                   Mutant             Hnadle Count - 2, Pointer Count 3
0xfffffa80034dfac0 c:!users!user!appdata!lo...ws!history!history.ie5! Mutant             Hnadle Count - 1, Pointer Count 2
0xfffffa80036e2970 ShellReadyEvent                                    Event              Hnadle Count - 1, Pointer Count 2
0xfffff8a002272440 Session                                            SymbolicLink       Target: \Sessions\BNOLINKS
0xfffffa800364bd40 CicLoadWinStaWinSta0                               Mutant             Hnadle Count - 1, Pointer Count 2
0xfffffa80034e1940 c:!users!user!appdata!lo...rnet files!content.ie5! Mutant             Hnadle Count - 1, Pointer Count 2
0xfffffa800363fbd0 EventShutDownCSRSS                                 Event              Hnadle Count - 1, Pointer Count 3
0xfffff8a00224abe0 C:*ProgramData*Microsoft...er0x0000000000000001.db Section            FileObj: \ProgramData\Microsoft\Windows...100659EF5C}.2.ver0x0000000000000001.db
0xfffffa8001c42250 ZonesCounterMutex                                  Mutant             Hnadle Count - 1, Pointer Count 2
0xfffffa80036d65f0 AccessibilitySoundAgentRunning                     Mutant             Hnadle Count - 1, Pointer Count 2
0xfffff8a001febae0 Global                                             SymbolicLink       Target: \BaseNamedObjects
0xfffff8a001bbe7a0 windows_ie_global_counters                         Section            FileObj: -
0xfffffa8003260940 DBWinMutex                                         Mutant             Hnadle Count - 1, Pointer Count 2
0xfffffa8001c40a90 ZonesLockedCacheCounterMutex                       Mutant             Hnadle Count - 1, Pointer Count 2
0xfffffa800364b710 MSCTF.AsmCacheReady.Default2                       Event              Hnadle Count - 1, Pointer Count 2
0xfffff8a002de4bd0 C:_Users_user_AppData_Lo...0190808_index.dat_32768 Section            FileObj: \Users\user\AppData\Local\Micr...IE5\MSHist012019080720190808\index.dat
0xfffffa80034e12f0 c:!users!user!appdata!ro...rosoft!windows!cookies! Mutant             Hnadle Count - 1, Pointer Count 2
0xfffffa8002efc910 PRS_EXTERNAL_CHECK_CHANGED_NOTIFY                  Event              Hnadle Count - 1, Pointer Count 3
0xfffffa8003650aa0 {43a2b8d7-6fed-4c18-bd36-b4630d61afb5}             Event              Hnadle Count - 2, Pointer Count 6
0xfffffa80036b6d30 Dwm-7BD2-ApiPort-71E8                              ALPC Port          Hnadle Count - 1, Pointer Count 6
0xfffff8a002df7780 C:_Users_user_AppData_Ro...Cookies_index.dat_16384 Section            FileObj: \Users\user\AppData\Roaming\Microsoft\Windows\Cookies\index.dat
0xfffffa800365d080 ZoneAttributeCacheCounterMutex                     Mutant             Hnadle Count - 2, Pointer Count 3
0xfffffa8003711610 VMwareToolsQuitEvent_vmusr                         Event              Hnadle Count - 1, Pointer Count 3
0xfffffa800364b3a0 MSCTF.CtfMonitorInitialized.Default2               Event              Hnadle Count - 1, Pointer Count 2
0xfffff8a00238ccd0 C:*ProgramData*Microsoft...s*Caches*cversions.2.ro Section            FileObj: \ProgramData\Microsoft\Windows\Caches\cversions.2.db
0xfffff8a002345fc0 C:*ProgramData*Microsoft...er0x000000000000000a.db Section            FileObj: \ProgramData\Microsoft\Windows...16689AF493}.2.ver0x000000000000000a.db
0xfffffa80034df120 _!SHMSFTHISTORY!_                                  Mutant             Hnadle Count - 1, Pointer Count 2
0xfffffa80031fe5f0 !IETld!Mutex                                       Mutant             Hnadle Count - 1, Pointer Count 2
0xfffff8a001dd58f0 Restricted                                         Directory          Hnadle Count - 1, Pointer Count 2
0xfffffa80036e1a40 ALTTAB_RUNNING_MUTEX                               Mutant             Hnadle Count - 1, Pointer Count 2
0xfffffa8003724be0 ZonesCacheCounterMutex                             Mutant             Hnadle Count - 1, Pointer Count 2
0xfffff8a0027de870 UrlZonesSM_user                                    Section            FileObj: -
0xfffffa80035317f0 ThemeLoadedEvent                                   Event              Hnadle Count - 1, Pointer Count 2
0xfffffa80036bb7e0 DwmComposedEvent_1                                 Event              Hnadle Count - 1, Pointer Count 2
0xfffffa800376d950 DINPUTWINMM                                        Event              Hnadle Count - 2, Pointer Count 3
0xfffffa8003344580 ScNetDrvMsg                                        Event              Hnadle Count - 1, Pointer Count 3
0xfffffa8003710080 VMwareToolsDumpStateEvent_vmusr                    Event              Hnadle Count - 1, Pointer Count 3
0xfffffa800364b7b0 MSCTF.CtfDeactivated.Default2                      Event              Hnadle Count - 1, Pointer Count 2
0xfffffa8003ebf080 ThemesStartEvent                                   Event              Hnadle Count - 1, Pointer Count 3
```

Get specific session’s namespace



```
Parsing Now -> /ArcName at 0xfffff8a00000b820

Object Address(V)  Name                                               Type                 Additional Info

------------------ -------------------------------------------------- -------------------- ----------------------------------------------------------
---
0xfffff8a00034a060 multi(0)disk(0)rdisk(0)                            SymbolicLink         Target: \Device\Harddisk0\Partition0

0xfffff8a00034dd70 multi(0)disk(0)rdisk(0)partition(1)                SymbolicLink         Target: \Device\Harddisk0\Partition1

0xfffff8a000345400 multi(0)disk(0)rdisk(0)partition(2)                SymbolicLink         Target: \Device\Harddisk0\Partition2

0xfffff8a00034a2a0 multi(0)disk(0)rdisk(0)partition(3)                SymbolicLink         Target: \Device\Harddisk0\Partition3

0xfffff8a00034dba0 multi(0)disk(0)rdisk(0)partition(4)                SymbolicLink         Target: \Device\Harddisk0\Partition4

*****************
```

Partition information

Summary

The *Object Manager* can help us figure out many things whether in live or offline memory analysis. *WinObj* plugin helps us map the *Object Manager* and parse arbitrary directory objects in memory as well. It can help us in forensics investigations or for research purpose.

Until now it was difficult to parse objects like *KnownDlls* in memory although attackers often take advantage of them. Some of the directories can also save us a significant amount of time when investigating large memory images with using enumeration to find objects as discussed earlier, instead of scanning the entire image.