Практическое задание. Операция «Спасти бухгалтера» (HW)

Задание 1.

Исследуйте файл «Win7-2515534d.vmem» с помощью Volatility 2. Введите имя родительского процесса для @WanaDecryptor (Pid 1060) в качестве ответа. Введите ответ в формате _.exe

Для дальнейшего анализа памяти в первую очередь определим профиль ОС с помощью плагина **imageinfo**. Это необходимо для правильной интерпретации данных памяти.

```
└─$ python2.7 vol.py -f ./Data/Win7-2515534d.vmem imageinfo
Volatility Foundation Volatility Framework 2.6.1
INFO    : volatility.debug    : Determining profile based on KDBG search...
          Suggested Profile(s) : Win7SP1x64, Win7SP0x64, Win2008R2SP0x64, Win2008R2SP1x6
4_24000, Win2008R2SP1x64_23418, Win2008R2SP1x64, Win7SP1x64_24000, Win7SP1x64_23418
                     AS Layer1 : WindowsAMD64PagedMemory (Kernel AS)
                     AS Layer2 : FileAddressSpace (/home/user/programs/volatility-master
/Data/Win7-2515534d.vmem)
                      PAE type : No PAE
                           DTB : 0x187000L
                          KDBG : 0xf80002be9120L
          Number of Processors : 1
     Image Type (Service Pack) : 1
                KPCR for CPU 0 : 0xfffff80002beb000L
             KUSER_SHARED_DATA : 0xfffff78000000000L
           Image date and time : 2023-06-22 12:34:03 UTC+0000
     Image local date and time : 2023-06-22 18:04:03 +0530
```

В результате работы выявили следующий профиль: Win7SP1*64.

Далее, для выполнения задания, используем плагин **pslist**, чтобы идентифицировать запущенные процессы.

```
└─$ python2.7 vol.py -f ./Data/Win7-2515534d.vmem --profile=Win7SP1x64 pslist | grep -v 'Failed'
Volatility Foundation Volatility Framework 2.6.1
Offset(V)          Name                    PID   PPID   Thds     Hnds   Sess  Wow64 Start                          Exit
0xfffffa8000ca8860 System                    4      0     97      446 ------      0 2023-06-22 12:04:39 UTC+0000
0xfffffa8001a64920 smss.exe                264      4      2       29 ------      0 2023-06-22 12:04:39 UTC+0000
0xfffffa80028a39a0 csrss.exe               352    344      8      626      0      0 2023-06-22 12:04:40 UTC+0000
0xfffffa8002a51730 wininit.exe             404    344      3       76      0      0 2023-06-22 12:04:41 UTC+0000
0xfffffa800291eb00 csrss.exe               416    396      9      307      1      0 2023-06-22 12:04:41 UTC+0000
0xfffffa8002a86340 winlogon.exe            464    396      3      113      1      0 2023-06-22 12:04:41 UTC+0000
0xfffffa8002ad8b00 services.exe            508    404      8      226      0      0 2023-06-22 12:04:41 UTC+0000
0xfffffa8002adbb00 lsass.exe               516    404      6      585      0      0 2023-06-22 12:04:41 UTC+0000
0xfffffa8002ae6b00 lsm.exe                 524    404      9      149      0      0 2023-06-22 12:04:41 UTC+0000
0xfffffa8002b4f720 svchost.exe             628    508     10      366      0      0 2023-06-22 12:04:42 UTC+0000
0xfffffa8002b7bb00 svchost.exe             696    508      7      288      0      0 2023-06-22 12:04:42 UTC+0000
0xfffffa8002ba0b00 svchost.exe             744    508     18      455      0      0 2023-06-22 12:04:42 UTC+0000
0xfffffa8002c00280 svchost.exe             868    508     19      443      0      0 2023-06-22 12:04:43 UTC+0000
0xfffffa8002c52710 svchost.exe             920    508     17      599      0      0 2023-06-22 12:04:43 UTC+0000
0xfffffa8002c5c680 svchost.exe             964    508     28      838      0      0 2023-06-22 12:04:43 UTC+0000
```

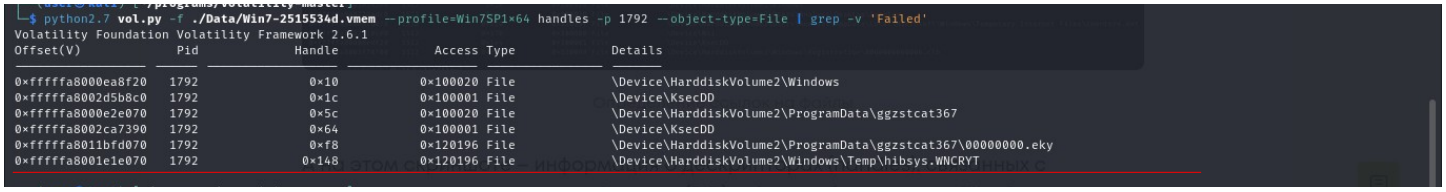
Найдём родительский процесс для @WanaDecryptor (Pid 1060)

```
0xfffffa8000e2e620 wmpnetwk.exe           2968    508     18      442      0      0 2023-06-22 12:06:48 UTC+0000
0xfffffa80022af430 ida64.exe              2248   2508      7      340      1      0 2023-06-22 12:16:18 UTC+0000
0xfffffa8001420300 x32dbg.exe             2820   2508     20      480      1      1 2023-06-22 12:23:34 UTC+0000
0xfffffa8000ee96d0 Ransomware.wan         1512   2820     11      167      1      1 2023-06-22 12:23:41 UTC+0000
0xfffffa8002ca4240 Ransomware.wan         2320    508    117      497      0      1 2023-06-22 12:30:19 UTC+0000
0xfffffa8002ad9560 dllhost.exe            1876    628      4       79      1      0 2023-06-22 12:30:20 UTC+0000
0xfffffa8001d0f8b0 tasksche.exe           2972   1512      0 ------      1      0 2023-06-22 12:31:13 UTC+0000   2023-06-22 12:31:43 UTC+0000
0xfffffa8001d22b00 tasksche.exe           1792   1044      8       82      0      1 2023-06-22 12:31:13 UTC+0000
0xfffffa8002fa3060 SearchProtocol          852   2756      8      289      0      0 2023-06-22 12:31:15 UTC+0000
0xfffffa8002572060 @WanaDecryptor         1060   1792      2       71      0      1 2023-06-22 12:31:27 UTC+0000
0xfffffa8001568060 taskhsvc.exe           3012   1060      4      101      0      1 2023-06-22 12:31:29 UTC+0000
0xfffffa8001ddb060 conhost.exe            2348    352      1       32      0      0 2023-06-22 12:31:29 UTC+0000
0xfffffa8000df81b0 VSSVC.exe               288    508      6      116      0      0 2023-06-22 12:31:43 UTC+0000
0xfffffa800141e9a0 @WanaDecryptor         3252   3212      1       75      1      1 2023-06-22 12:31:45 UTC+0000
0xfffffa80014e4a70 MpCmdRun.exe           3436   3412      5      116      0      0 2023-06-22 12:32:12 UTC+0000
0xfffffa80014c12c0 SearchFilterHo         3904   2756      6      109      0      0 2023-06-22 12:33:18 UTC+0000
0xfffffa8000f2f1c0 audiodg.exe            4048    744      6      128      0      0 2023-06-22 12:33:33 UTC+0000
0xfffffa8000dbc5a0 cmd.exe                2080   1468      0 ------      0      0 2023-06-22 12:34:03 UTC+0000   2023-06-22 12:34:03 UTC+0000
0xfffffa8000f90b00 conhost.exe            3292    352      0 ------      0      0 2023-06-22 12:34:03 UTC+0000   2023-06-22 12:34:03 UTC+0000
0xfffffa8000f7b790 ipconfig.exe           2360   2080      0 ------      0      0 2023-06-22 12:34:03 UTC+0000   2023-06-22 12:34:03 UTC+0000
```

Задание 2.

Исследуйте файл «Win7-2515534d.vmem» с помощью Volatility. В Taskche.exe (Pid 1792) открыто несколько дескрипторов файлов. В качестве ответа введите имя подозрительного файла, заканчивающееся на .WNCRYT. Введите ответ в формате _.WNCRYT

Для решения этого задания будем использовать плагин **handles** для поиска информации о дескрипторах, связанных с процессом Taskche.exe (Pid 1792), для объектов типа «файл».

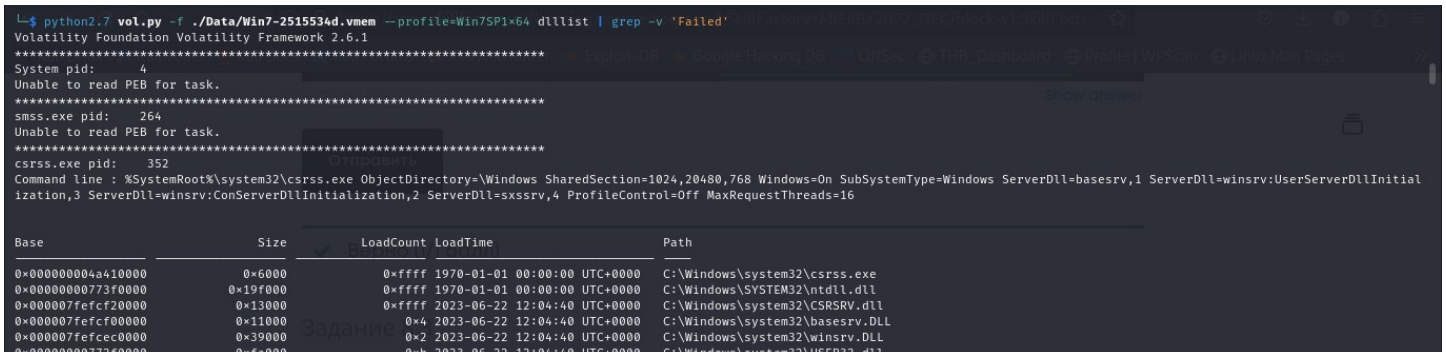


```
└─$ python2.7 vol.py -f ./Data/Win7-2515534d.vmem --profile=Win7SP1x64 handles -p 1792 --object-type=File | grep -v 'Failed'
Volatility Foundation Volatility Framework 2.6.1
Offset(V)          Pid      Handle              Access Type            Details
------------------ -------- ------------------ ------ --------------- -------
0xfffffa8000ea8f20   1792               0x10 0x100020 File            \Device\HarddiskVolume2\Windows
0xfffffa8002d5b8c0   1792               0x1c 0x100001 File            \Device\KsecDD
0xfffffa8000e2e070   1792               0x5c 0x100020 File            \Device\HarddiskVolume2\ProgramData\ggzstcat367
0xfffffa8002ca7390   1792               0x64 0x100001 File            \Device\KsecDD
0xfffffa8011bfd070   1792               0xf8 0x120196 File            \Device\HarddiskVolume2\ProgramData\ggzstcat367\00000000.eky
0xfffffa8001e1e070   1792              0x148 0x120196 File            \Device\HarddiskVolume2\Windows\Temp\hibsys.WNCRYT
```

Задание 3.

Исследуйте файл «Win7-2515534d.vmem» с помощью Volatility. Найдите Pid (process id) процесса, который загрузил zlib1.dll.

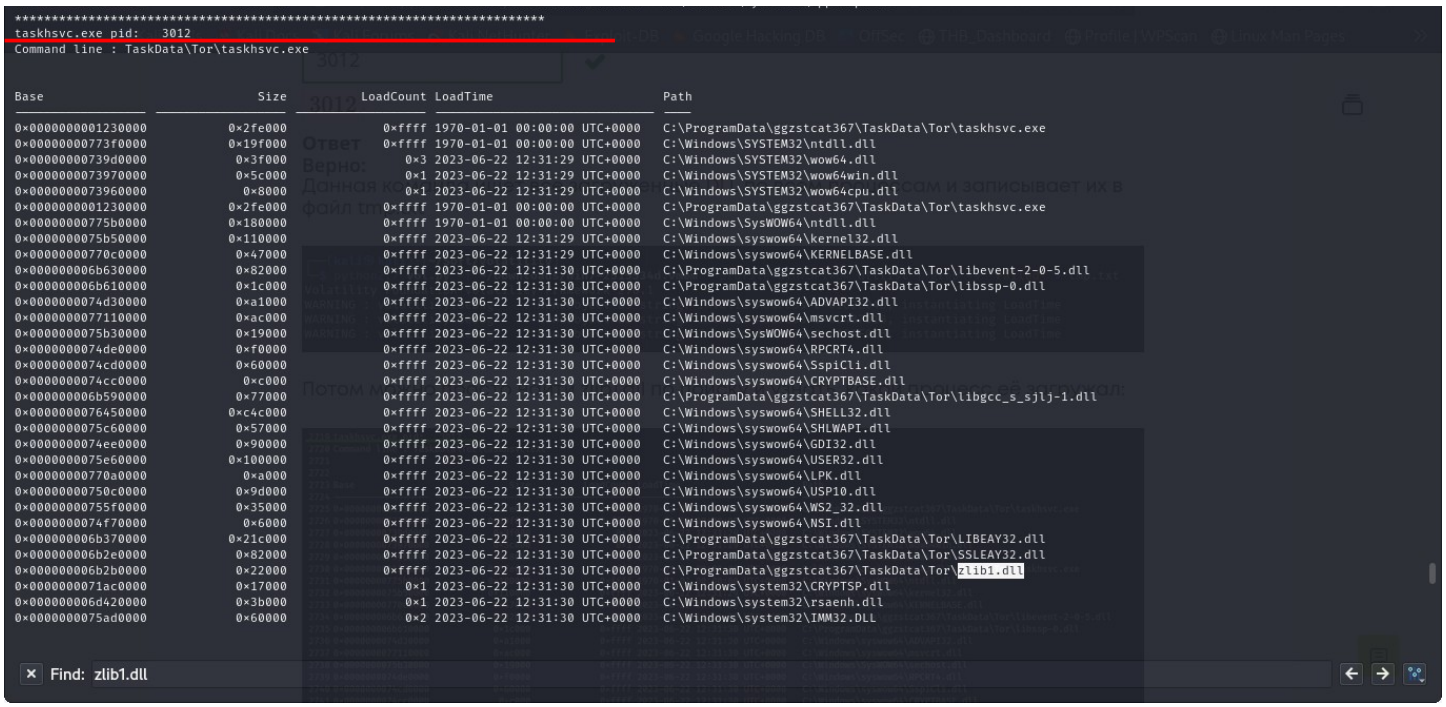
Используем плагин **dlllist** для вывода списка динамически подключаемых библиотек.



```
└─$ python2.7 vol.py -f ./Data/Win7-2515534d.vmem --profile=Win7SP1x64 dlllist | grep -v 'Failed'
Volatility Foundation Volatility Framework 2.6.1
************************************************************************
System pid:      4
Unable to read PEB for task.
************************************************************************
smss.exe pid:    264
Unable to read PEB for task.
************************************************************************
csrss.exe pid:    352
Command line : %SystemRoot%\system32\csrss.exe ObjectDirectory=\Windows SharedSection=1024,20480,768 Windows=On SubSystemType=Windows ServerDll=basesrv,1 ServerDll=winsrv:UserServerDllInitial
ization,3 ServerDll=winsrv:ConServerDllInitialization,2 ServerDll=sxssrv,4 ProfileControl=Off MaxRequestThreads=16

Base                             Size     LoadCount LoadTime                       Path
-------------------- ---------- -------- ---------- ------------------------------ ----
0x000000004a410000         0x6000           0xffff 1970-01-01 00:00:00 UTC+0000   C:\Windows\system32\csrss.exe
0x00000000773f0000        0x19f000          0xffff 1970-01-01 00:00:00 UTC+0000   C:\Windows\SYSTEM32\ntdll.dll
0x000007fefcf20000        0x13000           0xffff 2023-06-22 12:04:40 UTC+0000   C:\Windows\system32\CSRSRV.dll
0x000007fefcf00000        0x11000              0x4 2023-06-22 12:04:40 UTC+0000   C:\Windows\system32\basesrv.DLL
0x000007fefcec0000        0x39000              0x2 2023-06-22 12:04:40 UTC+0000   C:\Windows\system32\winsrv.DLL
```

С помощью поисковой строки найдем библиотеку zlib1.dll и идентифицируем процесс



```
************************************************************************
taskhsvc.exe pid:   3012
Command line : TaskData\Tor\taskhsvc.exe

Base                             Size     LoadCount LoadTime                       Path
-------------------- ---------- -------- ---------- ------------------------------ ----
0x0000000001230000         0x2fe000          0xffff 1970-01-01 00:00:00 UTC+0000   C:\ProgramData\ggzstcat367\TaskData\Tor\taskhsvc.exe
0x00000000773f0000        0x19f000          0xffff 1970-01-01 00:00:00 UTC+0000   C:\Windows\SYSTEM32\ntdll.dll
0x00000000739d0000         0x3f000              0x3 2023-06-22 12:31:29 UTC+0000   C:\Windows\SYSTEM32\wow64.dll
0x0000000073970000         0x5c000              0x1 2023-06-22 12:31:29 UTC+0000   C:\Windows\SYSTEM32\wow64win.dll
0x0000000073960000         0x8000               0x1 2023-06-22 12:31:29 UTC+0000   C:\Windows\SYSTEM32\wow64cpu.dll
0x0000000001230000         0x2fe000          0xffff 1970-01-01 00:00:00 UTC+0000   C:\ProgramData\ggzstcat367\TaskData\Tor\taskhsvc.exe
0x00000000775b0000        0x180000          0xffff 1970-01-01 00:00:00 UTC+0000   C:\Windows\SysWOW64\ntdll.dll
0x0000000075b50000        0x110000          0xffff 2023-06-22 12:31:29 UTC+0000   C:\Windows\syswow64\kernel32.dll
0x0000000770c0000         0x47000           0xffff 2023-06-22 12:31:29 UTC+0000   C:\Windows\syswow64\KERNELBASE.dll
0x000000006b630000         0x82000           0xffff 2023-06-22 12:31:30 UTC+0000   C:\ProgramData\ggzstcat367\TaskData\Tor\libevent-2-0-5.dll
0x000000006b610000         0x1c000           0xffff 2023-06-22 12:31:30 UTC+0000   C:\ProgramData\ggzstcat367\TaskData\Tor\libssp-0.dll
0x0000000074d30000         0xa1000           0xffff 2023-06-22 12:31:30 UTC+0000   C:\Windows\syswow64\ADVAPI32.dll
0x0000000077110000         0xac000           0xffff 2023-06-22 12:31:30 UTC+0000   C:\Windows\syswow64\msvcrt.dll
0x0000000075b30000         0x19000           0xffff 2023-06-22 12:31:30 UTC+0000   C:\Windows\SysWOW64\sechost.dll
0x0000000074de0000         0xf0000           0xffff 2023-06-22 12:31:30 UTC+0000   C:\Windows\syswow64\RPCRT4.dll
0x0000000074cd0000         0x60000           0xffff 2023-06-22 12:31:30 UTC+0000   C:\Windows\syswow64\SspiCli.dll
0x0000000074cc0000          0xc000           0xffff 2023-06-22 12:31:30 UTC+0000   C:\Windows\syswow64\CRYPTBASE.dll
0x000000006b590000         0x77000           0xffff 2023-06-22 12:31:30 UTC+0000   C:\ProgramData\ggzstcat367\TaskData\Tor\libgcc_s_sjlj-1.dll
0x0000000076450000         0xc4c000          0xffff 2023-06-22 12:31:30 UTC+0000   C:\Windows\syswow64\SHELL32.dll
0x0000000075c60000         0x57000           0xffff 2023-06-22 12:31:30 UTC+0000   C:\Windows\syswow64\SHLWAPI.dll
0x0000000074ee0000         0x90000           0xffff 2023-06-22 12:31:30 UTC+0000   C:\Windows\syswow64\GDI32.dll
0x0000000075e60000        0x100000          0xffff 2023-06-22 12:31:30 UTC+0000   C:\Windows\syswow64\USER32.dll
0x0000000770a0000          0xa000           0xffff 2023-06-22 12:31:30 UTC+0000   C:\Windows\syswow64\LPK.dll
0x0000000750c0000         0x9d000           0xffff 2023-06-22 12:31:30 UTC+0000   C:\Windows\syswow64\USP10.dll
0x0000000755f0000         0x35000           0xffff 2023-06-22 12:31:30 UTC+0000   C:\Windows\syswow64\WS2_32.dll
0x0000000074f70000          0x6000           0xffff 2023-06-22 12:31:30 UTC+0000   C:\Windows\syswow64\NSI.dll
0x000000006b370000         0x21c000          0xffff 2023-06-22 12:31:30 UTC+0000   C:\ProgramData\ggzstcat367\TaskData\Tor\LIBEAY32.dll
0x000000006b2e0000         0x82000           0xffff 2023-06-22 12:31:30 UTC+0000   C:\ProgramData\ggzstcat367\TaskData\Tor\SSLEAY32.dll
0x000000006b2b0000         0x22000           0xffff 2023-06-22 12:31:30 UTC+0000   C:\ProgramData\ggzstcat367\TaskData\Tor\zlib1.dll
0x0000000071ac0000         0x17000              0x1 2023-06-22 12:31:30 UTC+0000   C:\Windows\system32\CRYPTSP.dll
0x000000006d420000         0x3b000              0x1 2023-06-22 12:31:30 UTC+0000   C:\Windows\system32\rsaenh.dll
0x0000000075ad0000         0x60000              0x2 2023-06-22 12:31:30 UTC+0000   C:\Windows\system32\IMM32.DLL
```

Find: zlib1.dll