Forensic Study - 3 Windows Dump (1) - Example

2017.10.17

KUICS

2014210009 주어진

목차

Memory Dump?

컴퓨팅에서, 코어 덤프(core dump), 메모리 덤프(memory dump), 또는 시스템 덤프(system dump)는 컴퓨터 프로그램이 특정 시점에 작업 중이던 메모리 상태를 기록한 것으로, 보통 프로그램이 비정상적으로 종료했을 때 만들어진다.

실제로는, 그 외에 중요한 프로그램 상태도 같이 기록되곤 하는데, 프로그램 카운터, 스택 포인터 등 CPU 레지스터나, 메모리 관리 정보, 그 외 프로세서 및 운영 체제 플래그 및 정보 등이 포함된다.

출처 : https://ko.wikipedia.org/wiki/%EC%BD%94%EC%96%B4_%EB%8D%A4%ED%94%84

Memory Dump?

덤프를 뜨는 툴

Linux - gdb

Windows - DumpIt

Intro of the Memory Dump Analysis

1. Strings로 Alphanumeric 문자열을 뽑아낸다.

2. 근거가 될 수 있는 문자열을 발견하지 못했다면 메모리 덤프 툴을 이용해 분석을 시작한다.

   - 운영체제의 종류를 알아낸다. (Memory Map이 Windows 버전마다 다르기 때문에 최우선)

   - 이를 바탕으로 어떤 프로세스가 로드되어 있는지 또는 프로세스들간의 부모-자식 관계를 확인한다.
     - 의심가는 프로세스를 발견했다면 이를 추출하거나 PID를 근거로 Network Connection, Dll list등을 확인한다.
     - 만약 발견하지 못했다면 Driver나 Dll Injection등이 있는지를 확인한다.

   - 레지스트리 항목을 확인한다. (특히 Software항목이나 Run/RunOnce 또는 BHO)

Intro of the Memory Dump Analysis

1. Strings로 Alphanumeric 문자열을 뽑아낸다.

-> 대부분의 덤프파일은 1번 단계에서 많은 단서를 찾을 수 있다.

Intro of the Memory Dump Analysis

2. 근거가 될 수 있는 문자열을 발견하지 못했다면 메모리 덤프 툴을 이용해 분석을 시작한다.

- 운영체제의 종류를 알아낸다. (Memory Map이 Windows 버전마다 다르기 때문에 최우선)
  -> Linux의 경우 커널 버전 업마다 모듈/라이브러리등이 자주 바뀌므로 덤프 분석이 힘들다.

Intro of the Memory Dump Analysis

2. 근거가 될 수 있는 문자열을 발견하지 못했다면 메모리 덤프 툴을 이용해 분석을 시작한다.

- 이를 바탕으로 어떤 프로세스가 로드되어 있는지 또는 프로세스들간의 부모-자식 관계를 확인한다.
  - 의심가는 프로세스를 발견했다면 이를 추출하거나 PID를 근거로 Network Connection, Dll list등을 확인한다.
  - 만약 발견하지 못했다면 Driver나 Dll Injection등이 있는지를 확인한다.

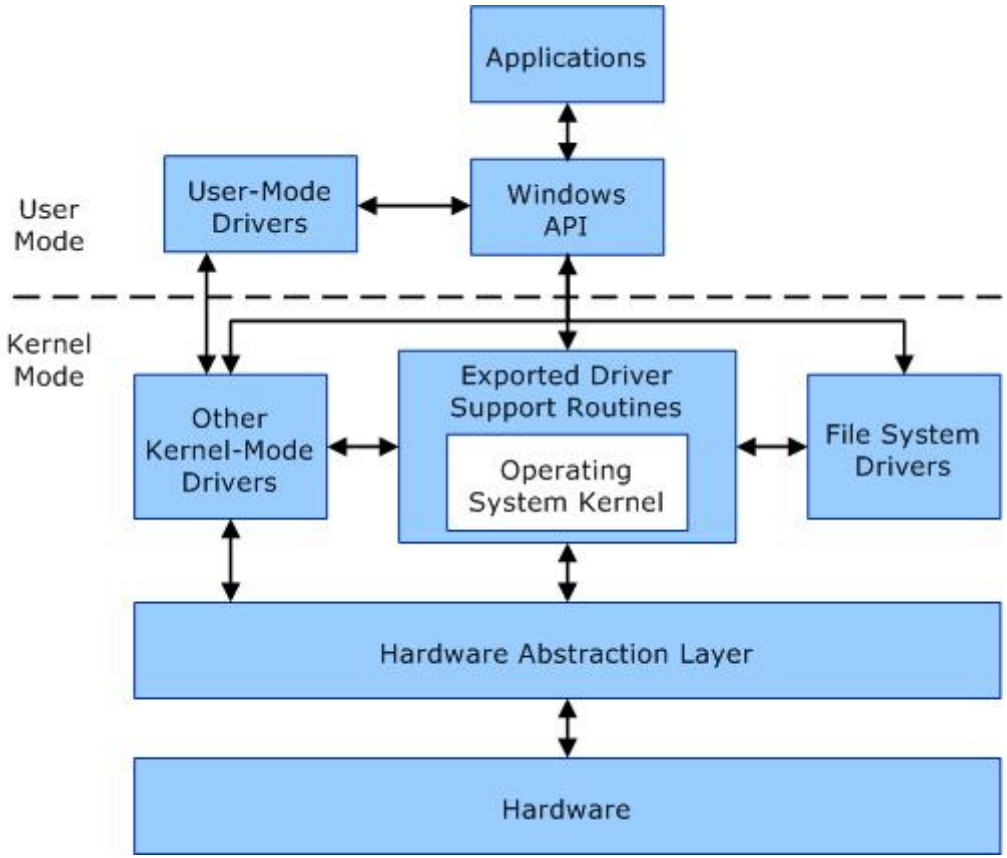
-> 엉뚱한 부모밑에 시스템 프로세스와 같은 이름을 가진 이상한 프로세스가 존재하는지 확인.
-> 그 프로세스이 가지고 있는 권한도 확인해주는 것이 좋다.

Intro of the Memory Dump Analysis

2. 근거가 될 수 있는 문자열을 발견하지 못했다면 메모리 덤프 툴을 이용해 분석을 시작한다.

- 레지스트리 항목을 확인한다. (특히 Software항목이나 Run/RunOnce 또는 BHO)
  -> 5~6번째 시간부터 자세히 배웁니다. Dump 분석에 Registry까지 자연스럽게 분석하니,
  Dump 분석에 익숙해지셔야 합니다.

Intro of the Memory Dump Analysis



Example - KUICS Wargame (Big Truck)

다운로드 : https://drive.google.com/open?id=0B7Llj1y13Ueab2xpa014LTdGTlE

Volatility

다운로드 : http://www.volatilityfoundation.org/26

Github : https://github.com/volatilityfoundation/volatility

커맨드 사용법 :
https://github.com/volatilityfoundation/volatility/wiki/Command-Reference

Example - Big Truck 풀이

목표

1. Flag 찾기 (개론대로만 하면 Flag는 쉽게 찾을 수 있습니다.)

2. Flag를 생성한 프로세스가 무엇이며, 이 프로세스는 어떤 특징을 가지고 있는가 / 어떠한 동작을 하는가 알아내기. (리버싱 필요)

시간 : 30분

- Wiki에 필요한 명령어들의 사용법이 있습니다.
- 정말 모르겠다 싶으면 뒤의 풀이를 따라해보셔도 좋습니다.

Example - Big Truck 풀이

```
C:₩Users₩akwke₩Desktop₩Study>volatility_2.6_win64_standalone.exe imageinfo -f d8c2fba72206f18493fb393b87606f98
Volatility Foundation Volatility Framework 2.6
INFO    : volatility.debug    : Determining profile based on KDBG search...
          Suggested Profile(s) : Win7SP1x64, Win7SP0x64, Win2008R2SP0x64, Win2008R2SP1x64_23418, Win2008R2SP1x64, Win7SP
1x64_23418
                     AS Layer1 : WindowsAMD64PagedMemory (Kernel AS)
                     AS Layer2 : FileAddressSpace (C:₩Users₩akwke₩Desktop₩Study₩d8c2fba72206f18493fb393b87606f98)
                      PAE type : No PAE
                           DTB : 0x187000L
                          KDBG : 0xf80002df90f0L
          Number of Processors : 2
     Image Type (Service Pack) : 1
                KPCR for CPU 0 : 0xfffff80002dfad00L
                KPCR for CPU 1 : 0xfffff88003700000L
             KUSER_SHARED_DATA : 0xfffff78000000000L
           Image date and time : 2017-08-13 16:11:08 UTC+0000
     Image local date and time : 2017-08-14 01:11:08 +0900

C:₩Users₩akwke₩Desktop₩Study>_
```

1. 운영체제의 종류 찾기.

Example - Big Truck 풀이

2. 1번을 기반으로
프로세스 리스트 확인

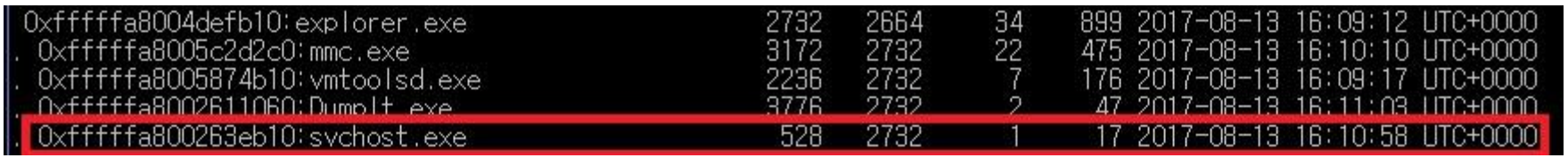
```
C:\Users\Wakwke\Desktop\Study>volatility_2.6_win64_standalone.exe pslist --profile=Win7SP1x64 -f d8c2fba72206f18493fb393b87606f98
Volatility Foundation Volatility Framework 2.6
Offset(V)          Name                    PID   PPID   Thds     Hnds   Sess  Wow64 Start                          Exit
------------------ -------------------- ------ ------ ------ -------- ------ ------ ------------------------------ ------------------------------
0xfffffa80024c4870 System                    4      0     87      575 ------      0 2017-08-13 16:08:39 UTC+0000
0xfffffa800414c040 smss.exe                240      4      2       30 ------      0 2017-08-13 16:08:39 UTC+0000
0xfffffa8003d338e0 csrss.exe               328    304      9      678      0      0 2017-08-13 16:08:44 UTC+0000
0xfffffa8004cb7060 wininit.exe             412    304      3       79      0      0 2017-08-13 16:08:49 UTC+0000
0xfffffa8004cb6670 csrss.exe               424    404     10      277      1      0 2017-08-13 16:08:49 UTC+0000
0xfffffa800569f5d0 services.exe            468    412     11      247      0      0 2017-08-13 16:08:49 UTC+0000
0xfffffa800569d7e0 winlogon.exe            500    404      6      130      1      0 2017-08-13 16:08:50 UTC+0000
0xfffffa80056ae8b0 lsass.exe               512    412      8      615      0      0 2017-08-13 16:08:51 UTC+0000
0xfffffa80056b8b10 lsm.exe                 520    412     10      143      0      0 2017-08-13 16:08:51 UTC+0000
0xfffffa8005728b10 svchost.exe             636    468     13      376      0      0 2017-08-13 16:08:52 UTC+0000
0xfffffa80057723d0 vmacthlp.exe            696    468      4       56      0      0 2017-08-13 16:08:52 UTC+0000
0xfffffa8005787b10 svchost.exe             732    468      8      321      0      0 2017-08-13 16:08:52 UTC+0000
0xfffffa80057e0720 svchost.exe             812    468     23      520      0      0 2017-08-13 16:08:52 UTC+0000
0xfffffa800586fb10 svchost.exe             884    468     22      452      0      0 2017-08-13 16:08:52 UTC+0000
0xfffffa8005880870 svchost.exe             912    468     51     1122      0      0 2017-08-13 16:08:53 UTC+0000
0xfffffa80058bf7e0 audiodg.exe             996    812      7      135      0      0 2017-08-13 16:08:53 UTC+0000
0xfffffa8005907060 TrustedInstall          352    468      5      217      0      0 2017-08-13 16:08:53 UTC+0000
0xfffffa8005909b10 svchost.exe             264    468     27      773      0      0 2017-08-13 16:08:53 UTC+0000
0xfffffa80044ef510 svchost.exe             980    468     21      419      0      0 2017-08-13 16:08:55 UTC+0000
0xfffffa8005956210 spoolsv.exe            1108    468     14      343      0      0 2017-08-13 16:08:55 UTC+0000
0xfffffa800595bb10 svchost.exe            1140    468     22      324      0      0 2017-08-13 16:08:55 UTC+0000
0xfffffa8005b90b10 svchost.exe            1248    468     23      285      0      0 2017-08-13 16:08:56 UTC+0000
0xfffffa8005bc4060 sppsvc.exe             1300    468      4      150      0      0 2017-08-13 16:08:56 UTC+0000
0xfffffa8005c07b10 VGAuthService.         1388    468      4       89      0      0 2017-08-13 16:08:56 UTC+0000
0xfffffa8005b5b520 vmtoolsd.exe           1436    468     10      299      0      0 2017-08-13 16:08:56 UTC+0000
0xfffffa8005c75710 ManagementAgen         1480    468     11      100      0      0 2017-08-13 16:08:56 UTC+0000
0xfffffa8005cf42a0 svchost.exe            1720    468      7       98      0      0 2017-08-13 16:08:57 UTC+0000
0xfffffa8005d77b10 dllhost.exe            1820    468     22      211      0      0 2017-08-13 16:08:58 UTC+0000
0xfffffa8003e8e060 WmiPrvSE.exe           1892    636     10      201      0      0 2017-08-13 16:08:58 UTC+0000
0xfffffa8003f9c060 dllhost.exe            1960    468     19      213      0      0 2017-08-13 16:08:58 UTC+0000
0xfffffa80044ab060 msdtc.exe              1076    468     15      158      0      0 2017-08-13 16:08:59 UTC+0000
0xfffffa800451f060 VSSVC.exe              2080    468      7      123      0      0 2017-08-13 16:09:00 UTC+0000
0xfffffa8004cfd060 mscorsvw.exe           2496    468      9      156      0      1 2017-08-13 16:09:09 UTC+0000
0xfffffa8004d93b10 mscorsvw.exe           2520    468      6      101      0      0 2017-08-13 16:09:09 UTC+0000
0xfffffa8004dad620 taskhost.exe           2624    468     10      184      1      0 2017-08-13 16:09:12 UTC+0000
0xfffffa8004de5b10 dwm.exe                2704    884      4       77      1      0 2017-08-13 16:09:12 UTC+0000
0xfffffa8004defb10 explorer.exe           2732   2664     34      899      1      0 2017-08-13 16:09:12 UTC+0000
0xfffffa80056b4500 SearchIndexer.         2988    468     15      750      0      0 2017-08-13 16:09:15 UTC+0000
0xfffffa80057c9720 SearchProtocol         1788   2988      7      285      0      0 2017-08-13 16:09:15 UTC+0000
0xfffffa8005850b10 SearchFilterHo         2148   2988      5      107      0      0 2017-08-13 16:09:15 UTC+0000
0xfffffa8005874b10 vmtoolsd.exe           2236   2732      7      176      1      0 2017-08-13 16:09:17 UTC+0000
0xfffffa80044d4730 WmiPrvSE.exe           2348    636     13      305      0      0 2017-08-13 16:09:19 UTC+0000
0xfffffa80049bb060 WmiApSrv.exe           2408    468      7      122      0      0 2017-08-13 16:09:21 UTC+0000
0xfffffa8004ebc580 wmpnetwk.exe           2900    468     12      219      0      0 2017-08-13 16:09:24 UTC+0000
0xfffffa8005c2d2c0 mmc.exe                3172   2732     22      475      1      0 2017-08-13 16:10:10 UTC+0000
0xfffffa8002667060 svchost.exe            3712    468     15      383      0      0 2017-08-13 16:10:57 UTC+0000
0xfffffa800263eb10 svchost.exe             528   2732      1       17      1      1 2017-08-13 16:10:58 UTC+0000
0xfffffa8002641060 conhost.exe            3580    424      3       92      1      0 2017-08-13 16:10:58 UTC+0000
0xfffffa8002611060 DumpIt.exe             3776   2732      2       47      1      1 2017-08-13 16:11:09 UTC+0000
0xfffffa8002625b10 conhost.exe            3788    424      3       92      1      0 2017-08-13 16:11:09 UTC+0000
0xfffffa8002626b10 mscorsvw.exe           3236   2496      7       18 ------      1 2017-08-13 16:11:25 UTC+0000
```

Example - Big Truck 풀이

2. 1번을 기반으로
프로세스 부모-자식 확인

```
C:\Users\Wakwke\Desktop\Study>volatility_2.6_win64_standalone.exe pstree --profile=Win7SP1x64 -f d8c2fba72206f18493fb393b87606f98
Volatility Foundation Volatility Framework 2.6
Name                                                  Pid   PPid   Thds   Hnds Time
-------------------------------------------------- ------ ------ ------ ------ ----
 0xfffffa8004cb7060:wininit.exe                       412    304      3     79 2017-08-13 16:08:49 UTC+0000
. 0xfffffa80056ae8b0:lsass.exe                        512    412      8    615 2017-08-13 16:08:51 UTC+0000
. 0xfffffa80056b8b10:lsm.exe                          520    412     10    143 2017-08-13 16:08:51 UTC+0000
. 0xfffffa800569f5d0:services.exe                     468    412     11    247 2017-08-13 16:08:49 UTC+0000
.. 0xfffffa8004dad620:taskhost.exe                   2624    468     10    184 2017-08-13 16:09:12 UTC+0000
.. 0xfffffa8005d77b10:dllhost.exe                    1820    468     22    211 2017-08-13 16:08:58 UTC+0000
.. 0xfffffa8005c07b10:VGAuthService.                 1388    468      4     89 2017-08-13 16:08:56 UTC+0000
.. 0xfffffa80056b4500:SearchIndexer.                 2988    468     15    750 2017-08-13 16:09:15 UTC+0000
... 0xfffffa8005850b10:SearchFilterHo                2148   2988      5    107 2017-08-13 16:09:15 UTC+0000
... 0xfffffa80057c9720:SearchProtocol                1788   2988      7    285 2017-08-13 16:09:15 UTC+0000
.. 0xfffffa8005880870:svchost.exe                     912    468     51   1122 2017-08-13 16:08:53 UTC+0000
.. 0xfffffa8005bc4060:sppsvc.exe                     1300    468      4    150 2017-08-13 16:08:56 UTC+0000
.. 0xfffffa8004ebc580:wmpnetwk.exe                   2900    468     12    219 2017-08-13 16:09:24 UTC+0000
.. 0xfffffa800586fb10:svchost.exe                     884    468     22    452 2017-08-13 16:08:52 UTC+0000
... 0xfffffa8004de5b10:dwm.exe                       2704    884      4     77 2017-08-13 16:09:12 UTC+0000
.. 0xfffffa800451f060:VSSVC.exe                      2080    468      7    123 2017-08-13 16:09:00 UTC+0000
.. 0xfffffa8005c75710:ManagementAgen                 1480    468     11    100 2017-08-13 16:08:56 UTC+0000
.. 0xfffffa8005b5b520:vmtoolsd.exe                   1436    468     10    299 2017-08-13 16:08:56 UTC+0000
.. 0xfffffa80057e0720:svchost.exe                     812    468     23    520 2017-08-13 16:08:52 UTC+0000
... 0xfffffa80058bf7e0:audiodg.exe                    996    812      7    135 2017-08-13 16:08:53 UTC+0000
.. 0xfffffa8005909b10:svchost.exe                     264    468     27    773 2017-08-13 16:08:53 UTC+0000
.. 0xfffffa80044ab060:msdtc.exe                      1076    468     15    158 2017-08-13 16:08:59 UTC+0000
.. 0xfffffa80057723d0:vmacthlp.exe                    696    468      4     56 2017-08-13 16:08:52 UTC+0000
.. 0xfffffa8004cfd060:mscorsvw.exe                   2496    468      9    156 2017-08-13 16:09:09 UTC+0000
... 0xfffffa8002626b10:mscorsvw.exe                  3236   2496      7     18 2017-08-13 16:11:25 UTC+0000
.. 0xfffffa8005907060:TrustedInstall                  352    468      5    217 2017-08-13 16:08:53 UTC+0000
.. 0xfffffa8005cf42a0:svchost.exe                    1720    468      7     98 2017-08-13 16:08:57 UTC+0000
.. 0xfffffa8005956210:spoolsv.exe                    1108    468     14    343 2017-08-13 16:08:55 UTC+0000
.. 0xfffffa8004d93b10:mscorsvw.exe                   2520    468      6    101 2017-08-13 16:09:09 UTC+0000
.. 0xfffffa8005787b10:svchost.exe                     732    468      8    321 2017-08-13 16:08:52 UTC+0000
.. 0xfffffa8005b90b10:svchost.exe                    1248    468     23    285 2017-08-13 16:08:56 UTC+0000
.. 0xfffffa80049bb060:WmiApSrv.exe                   2408    468      7    122 2017-08-13 16:09:21 UTC+0000
.. 0xfffffa8003f9c060:dllhost.exe                    1960    468     19    213 2017-08-13 16:08:58 UTC+0000
.. 0xfffffa800595bb10:svchost.exe                    1140    468     22    324 2017-08-13 16:08:55 UTC+0000
.. 0xfffffa80044ef510:svchost.exe                     980    468     21    419 2017-08-13 16:08:55 UTC+0000
.. 0xfffffa8002667060:svchost.exe                    3712    468     15    383 2017-08-13 16:10:57 UTC+0000
.. 0xfffffa8005728b10:svchost.exe                     636    468     13    376 2017-08-13 16:08:52 UTC+0000
... 0xfffffa8003e8e060:WmiPrvSE.exe                  1892    636     10    201 2017-08-13 16:08:58 UTC+0000
... 0xfffffa80044d4730:WmiPrvSE.exe                  2348    636     13    305 2017-08-13 16:09:19 UTC+0000
 0xfffffa8003d338e0:csrss.exe                         328    304      9    678 2017-08-13 16:08:44 UTC+0000
 0xfffffa8004defb10:explorer.exe                     2732   2664     34    899 2017-08-13 16:09:12 UTC+0000
. 0xfffffa8005c2d2c0:mmc.exe                         3172   2732     22    475 2017-08-13 16:10:10 UTC+0000
. 0xfffffa8005874b10:vmtoolsd.exe                    2236   2732      7    176 2017-08-13 16:09:17 UTC+0000
. 0xfffffa8002611060:DumpIt.exe                      3776   2732      2     47 2017-08-13 16:11:03 UTC+0000
. 0xfffffa800263eb10:svchost.exe                      528   2732      1     17 2017-08-13 16:10:58 UTC+0000
 0xfffffa80024c4870:System                              4      0     87    575 2017-08-13 16:08:39 UTC+0000
. 0xfffffa800414c040:smss.exe                        240      4      2     30 2017-08-13 16:08:39 UTC+0000
 0xfffffa8004cb6670:csrss.exe                        424    404     10    277 2017-08-13 16:08:49 UTC+0000
. 0xfffffa8002625b10:conhost.exe                     3788    424      3     92 2017-08-13 16:11:03 UTC+0000
. 0xfffffa8002641060:conhost.exe                     3580    424      3     92 2017-08-13 16:10:58 UTC+0000
 0xfffffa800569d7e0:winlogon.exe                     500    404      6    130 2017-08-13 16:08:50 UTC+0000
```

Example - Big Truck 풀이



2. 1번을 기반으로 프로세스 부모-자식 확인 (의심가는 프로세스 확인)

Example - Big Truck 풀이

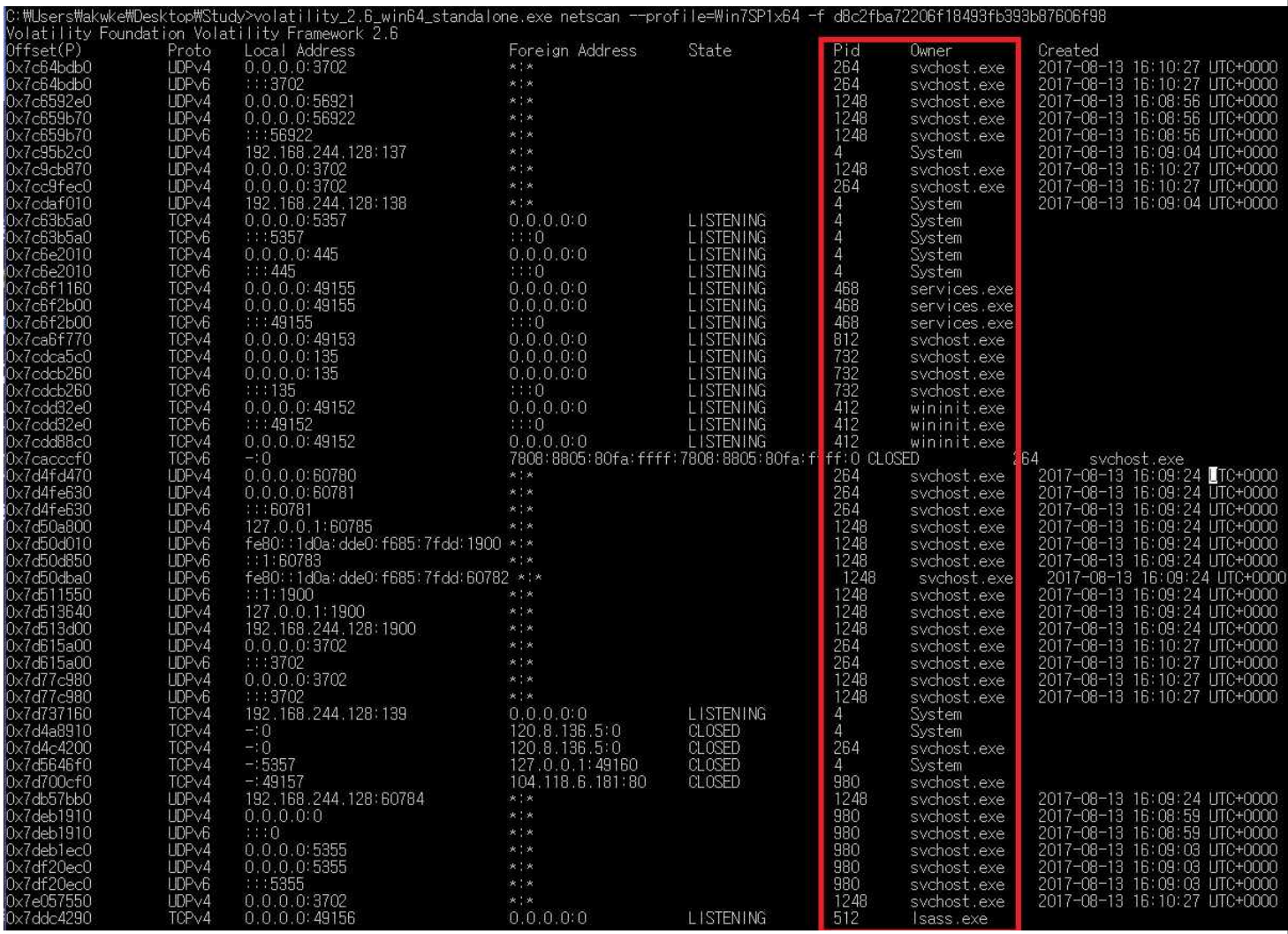
```
svchost.exe (528): S-1-5-21-285125983-2218342051-2926112896-1000 (Chobo)
svchost.exe (528): S-1-5-21-285125983-2218342051-2926112896-513 (Domain Users)
svchost.exe (528): S-1-1-0 (Everyone)
svchost.exe (528): S-1-5-114 (Local Account (Member of Administrators))
svchost.exe (528): S-1-5-32-544 (Administrators)
svchost.exe (528): S-1-5-32-545 (Users)
svchost.exe (528): S-1-5-4 (Interactive)
svchost.exe (528): S-1-2-1 (Console Logon (Users who are logged onto the physical console))
svchost.exe (528): S-1-5-11 (Authenticated Users)
svchost.exe (528): S-1-5-15 (This Organization)
svchost.exe (528): S-1-5-113 (Local Account)
svchost.exe (528): S-1-5-5-0-429020 (Logon Session)
svchost.exe (528): S-1-2-0 (Local (Users with the ability to log in locally))
svchost.exe (528): S-1-5-64-10 (NTLM Authentication)
svchost.exe (528): S-1-16-12288 (High Mandatory Level)
```

3. 권한 확인 (getsids) - Chobo라는 유저에서 실행된 것이므로 짝퉁 Svchost 100%

Example - Big Truck 풀이

4. 네트워크 연결 확인

(의심되는
프로세스의 PID = 528)



```
C:₩Users₩akwke₩Desktop₩Study>volatility_2.6_win64_standalone.exe netscan --profile=Win7SP1x64 -f d8c2fba72206f18493fb393b87606f98
Volatility Foundation Volatility Framework 2.6
Offset(P)          Proto    Local Address                  Foreign Address      State            Pid      Owner          Created
0x7c64bdb0         UDPv4    0.0.0.0:3702                   *:*                                   264      svchost.exe    2017-08-13 16:10:27 UTC+0000
0x7c64bdb0         UDPv6    :::3702                        *:*                                   264      svchost.exe    2017-08-13 16:10:27 UTC+0000
0x7c6592e0         UDPv4    0.0.0.0:56921                  *:*                                   1248     svchost.exe    2017-08-13 16:08:56 UTC+0000
0x7c659b70         UDPv4    0.0.0.0:56922                  *:*                                   1248     svchost.exe    2017-08-13 16:08:56 UTC+0000
0x7c659b70         UDPv6    :::56922                       *:*                                   1248     svchost.exe    2017-08-13 16:08:56 UTC+0000
0x7c95b2c0         UDPv4    192.168.244.128:137            *:*                                   4        System         2017-08-13 16:09:04 UTC+0000
0x7c9cb870         UDPv4    0.0.0.0:3702                   *:*                                   1248     svchost.exe    2017-08-13 16:10:27 UTC+0000
0x7cc9fec0         UDPv4    0.0.0.0:3702                   *:*                                   264      svchost.exe    2017-08-13 16:10:27 UTC+0000
0x7cdaf010         UDPv4    192.168.244.128:138            *:*                                   4        System         2017-08-13 16:09:04 UTC+0000
0x7c63b5a0         TCPv4    0.0.0.0:5357                   0.0.0.0:0            LISTENING        4        System
0x7c63b5a0         TCPv6    :::5357                        :::0                 LISTENING        4        System
0x7c6e2010         TCPv4    0.0.0.0:445                    0.0.0.0:0            LISTENING        4        System
0x7c6e2010         TCPv6    :::445                         :::0                 LISTENING        4        System
0x7c6f1160         TCPv4    0.0.0.0:49155                  0.0.0.0:0            LISTENING        468      services.exe
0x7c6f2b00         TCPv4    0.0.0.0:49155                  0.0.0.0:0            LISTENING        468      services.exe
0x7c6f2b00         TCPv6    :::49155                       :::0                 LISTENING        468      services.exe
0x7ca6f770         TCPv4    0.0.0.0:49153                  0.0.0.0:0            LISTENING        812      svchost.exe
0x7cdca5c0         TCPv4    0.0.0.0:135                    0.0.0.0:0            LISTENING        732      svchost.exe
0x7cdcb260         TCPv4    0.0.0.0:135                    0.0.0.0:0            LISTENING        732      svchost.exe
0x7cdcb260         TCPv6    :::135                         :::0                 LISTENING        732      svchost.exe
0x7cdd32e0         TCPv4    0.0.0.0:49152                  0.0.0.0:0            LISTENING        412      wininit.exe
0x7cdd32e0         TCPv6    :::49152                       :::0                 LISTENING        412      wininit.exe
0x7cdd88c0         TCPv4    0.0.0.0:49152                  0.0.0.0:0            LISTENING        412      wininit.exe
0x7cacccf0         TCPv6    -:0                            7808:8805:80fa:ffff:7808:8805:80fa:ffff:0 CLOSED          264      svchost.exe
0x7d4fd470         UDPv4    0.0.0.0:60780                  *:*                                   264      svchost.exe    2017-08-13 16:09:24 UTC+0000
0x7d4fe630         UDPv4    0.0.0.0:60781                  *:*                                   264      svchost.exe    2017-08-13 16:09:24 UTC+0000
0x7d4fe630         UDPv6    :::60781                       *:*                                   264      svchost.exe    2017-08-13 16:09:24 UTC+0000
0x7d50a800         UDPv4    127.0.0.1:60785                *:*                                   1248     svchost.exe    2017-08-13 16:09:24 UTC+0000
0x7d50d010         UDPv6    fe80::1d0a:dde0:f685:7fdd:1900 *:*                                   1248     svchost.exe    2017-08-13 16:09:24 UTC+0000
0x7d50d850         UDPv6    ::1:60783                      *:*                                   1248     svchost.exe    2017-08-13 16:09:24 UTC+0000
0x7d50dba0         UDPv6    fe80::1d0a:dde0:f685:7fdd:60782 *:*                                  1248     svchost.exe    2017-08-13 16:09:24 UTC+0000
0x7d511550         UDPv6    ::1:1900                       *:*                                   1248     svchost.exe    2017-08-13 16:09:24 UTC+0000
0x7d513640         UDPv4    127.0.0.1:1900                 *:*                                   1248     svchost.exe    2017-08-13 16:09:24 UTC+0000
0x7d513d00         UDPv4    192.168.244.128:1900           *:*                                   1248     svchost.exe    2017-08-13 16:09:24 UTC+0000
0x7d615a00         UDPv4    0.0.0.0:3702                   *:*                                   264      svchost.exe    2017-08-13 16:10:27 UTC+0000
0x7d615a00         UDPv6    :::3702                        *:*                                   264      svchost.exe    2017-08-13 16:10:27 UTC+0000
0x7d77c980         UDPv4    0.0.0.0:3702                   *:*                                   1248     svchost.exe    2017-08-13 16:10:27 UTC+0000
0x7d77c980         UDPv6    :::3702                        *:*                                   1248     svchost.exe    2017-08-13 16:10:27 UTC+0000
0x7d737160         TCPv4    192.168.244.128:139            0.0.0.0:0            LISTENING        4        System
0x7d4a8910         TCPv4    -:0                            120.8.136.5:0        CLOSED           4        System
0x7d4c4200         TCPv4    -:0                            120.8.136.5:0        CLOSED           264      svchost.exe
0x7d5646f0         TCPv4    -:5357                         127.0.0.1:49160      CLOSED           4        System
0x7d700cf0         TCPv4    -:49157                        104.118.6.181:80     CLOSED           980      svchost.exe
0x7db57bb0         UDPv4    192.168.244.128:60784          *:*                                   1248     svchost.exe    2017-08-13 16:09:24 UTC+0000
0x7deb1910         UDPv4    0.0.0.0:0                      *:*                                   980      svchost.exe    2017-08-13 16:08:59 UTC+0000
0x7deb1910         UDPv6    :::0                           *:*                                   980      svchost.exe    2017-08-13 16:08:59 UTC+0000
0x7deb1ec0         UDPv4    0.0.0.0:5355                   *:*                                   980      svchost.exe    2017-08-13 16:09:03 UTC+0000
0x7df20ec0         UDPv4    0.0.0.0:5355                   *:*                                   980      svchost.exe    2017-08-13 16:09:03 UTC+0000
0x7df20ec0         UDPv6    :::5355                        *:*                                   980      svchost.exe    2017-08-13 16:09:03 UTC+0000
0x7e057550         UDPv4    0.0.0.0:3702                   *:*                                   1248     svchost.exe    2017-08-13 16:10:27 UTC+0000
0x7ddc4290         TCPv4    0.0.0.0:49156                  0.0.0.0:0            LISTENING        512      lsass.exe
```

Example - Big Truck 풀이

```
C:₩Users₩akwke₩Desktop₩Study>volatility_2.6_win64_standalone.exe printkey -K "WOW6432Node₩Microsoft₩Windows₩CurrentVersion₩Run" --profile=Win7SP1x64 -f d8c2fba7220f18493fb393b87606f98
Volatility Foundation Volatility Framework 2.6
Legend: (S) = Stable   (V) = Volatile

----------------------------
Registry: ₩SystemRoot₩System32₩Config₩SOFTWARE
Key name: Run (S)
Last updated: 2017-08-13 15:17:36 UTC+0000

Subkeys:

Values:
REG_SZ        F14g            : (S) KUICS{EzDuMp4n41ys1s}

C:₩Users₩akwke₩Desktop₩Study>
```

5. Registry 확인 - pslist에서 WoW64로 돌아가는 것을 확인했으니,
WOW6432Node에 들어가서 확인해야 한다. (정답 찾음.)

Example - Big Truck 풀이

```
C:₩Users₩akwke₩Desktop₩Study>volatility_2.6_win64_standalone.exe procdump -D c:₩ --profile=Win7SP1x64 -f d8c2fba72206f18
493fb393b87606f98 -p 528
Volatility Foundation Volatility Framework 2.6
Process(V)         ImageBase          Name                 Result
------------------ ------------------ -------------------- ------
0xfffffa800263eb10 0x000000000011b0000 svchost.exe          OK: executable.528.exe
```

6. 정확히 뭘 하는 프로그램인지 체크하기 위해 덤프 파일에서 추출.

Example - Big Truck 풀이

```
011B102A    E8 D1 FF FF FF      call executable.528.11B1000
011B102F    FF 70 04            push dword ptr ds:[eax+4]
011B1032    FF 30               push dword ptr ds:[eax]
011B1034    FF 15 C8 20 1B 01   call dword ptr ds:[<&_stdio_common_vfprintf>]
011B103A    83 C4 18            add esp,18
011B103D    5E                  pop esi                                 esi:EntryPoint
011B103E    5D                  pop ebp
011B103F    C3                  ret
011B1040    55                  push ebp
011B1041    8B EC               mov ebp,esp
011B1043    83 EC 08            sub esp,8
011B1046    A1 04 30 1B 01      mov eax,dword ptr ds:[11B3004]
011B104B    33 C5               xor eax,ebp
011B104D    89 45 FC            mov dword ptr ss:[ebp-4],eax
011B1050    8D 45 F8            lea eax,dword ptr ss:[ebp-8]            [ebp-8]:BaseThreadInitThunk
011B1053    50                  push eax
011B1054    68 06 00 02 00      push 20006
011B1059    6A 00               push 0
011B105B    68 40 21 1B 01      push executable.528.11B2140             11B2140:"SOFTWARE\\Microsoft\\Windows\\CurrentVersion\\Run"
011B1060    68 02 00 00 80      push 80000002
011B1065    FF 15 08 20 1B 01   call dword ptr ds:[<&RegOpenKeyExA>]
011B106B    85 C0               test eax,eax
011B106D    75 34               jne executable.528.11B10A3
011B106F    56                  push esi                                esi:EntryPoint
011B1070    68 18 21 1B 01      push executable.528.11B2118             11B2118:"KUICS{EzDuMp4n41ys1s}"
011B1075    FF 15 14 20 1B 01   call dword ptr ds:[<&lstrlen>]
011B107B    50                  push eax
011B107C    68 18 21 1B 01      push executable.528.11B2118             11B2118:"KUICS{EzDuMp4n41ys1s}"
011B1081    6A 01               push 1
011B1083    6A 00               push 0
011B1085    68 30 21 1B 01      push executable.528.11B2130             11B2130:"F14g"
011B108A    FF 75 F8            push dword ptr ss:[ebp-8]               [ebp-8]:BaseThreadInitThunk
011B108D    FF 15 04 20 1B 01   call dword ptr ds:[<&RegSetValueExA>]
011B1093    FF 75 F8            push dword ptr ss:[ebp-8]               [ebp-8]:BaseThreadInitThunk
011B1096    8B F0               mov esi,eax                             esi:EntryPoint
011B1098    FF 15 00 20 1B 01   call dword ptr ds:[<&RegCloseKey>]
011B109E    85 F6               test esi,esi                            esi:EntryPoint
011B10A0    5E                  pop esi                                 esi:EntryPoint
011B10A1    74 0D               je executable.528.11B10B0
011B10A3    68 38 21 1B 01      push executable.528.11B2138             11B2138:"Error\n"
011B10A8    E8 63 FF FF FF      call executable.528.11B1010
011B10AD    83 C4 04            add esp,4
```

6. 정확히 뭘 하는 프로그램인지 체크하기 위해 덤프 파일에서 추출.

Example - Big Truck 풀이

```
int sub_11B1040()
{
  int v0; // eax@2
  LSTATUS v1; // esi@2
  HKEY phkResult; // [sp+0h] [bp-8h]@1

  if ( RegOpenKeyExA(HKEY_LOCAL_MACHINE, "SOFTWARE\\Microsoft\\Windows\\CurrentVersion\\Run", 0, 0x20006u, &phkResult)
    || (v0 = lstrlenA((LPCSTR)"KUICS{EzDuMp4n41ys1s}"),
        v1 = RegSetValueExA(phkResult, "F14g", 0, 1u, "KUICS{EzDuMp4n41ys1s}", v0),
        RegCloseKey(phkResult),
        v1) )
  {
    sub_11B1010();
  }
  Sleep(0x5F5E100u);
  return 0;
}
```

6. 정확히 뭘 하는 프로그램인지 체크하기 위해 덤프 파일에서 추출.

감사합니다

과제 : 10/23에 업로드 됩니다.

참조 :
https://github.com/volatilityfoundation/volatility
https://github.com/volatilityfoundation/volatility/wiki