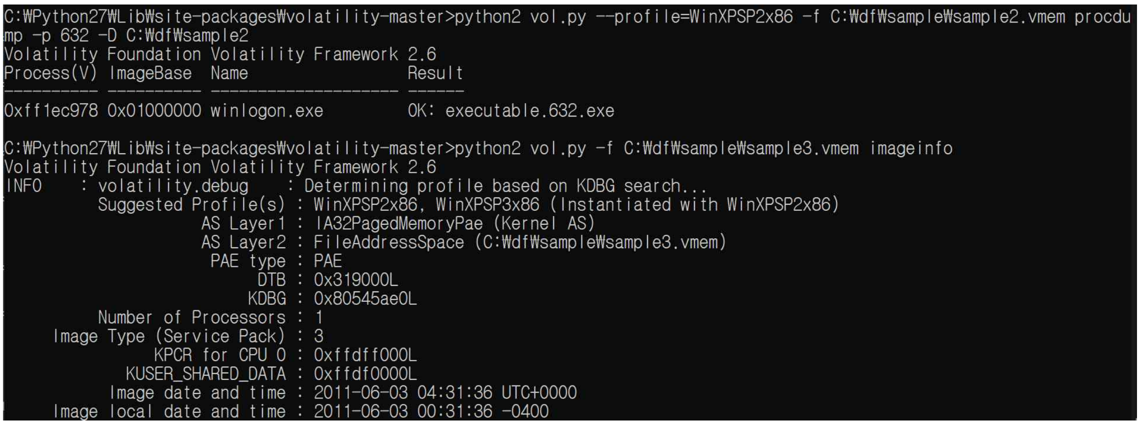
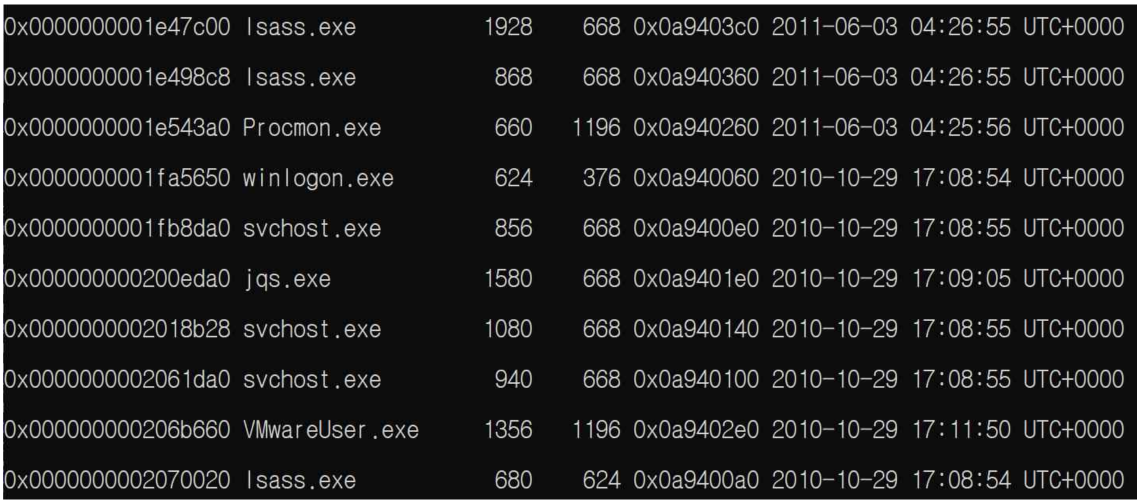
1. Image File의 System 정보



```
C:₩Python27₩Lib₩site-packages₩volatility-master>python2 vol.py --profile=WinXPSP2x86 -f C:₩df₩sample₩sample2.vmem procdu
mp -p 632 -D C:₩df₩sample2
Volatility Foundation Volatility Framework 2.6
Process(V) ImageBase  Name                 Result
---------- ---------- -------------------- ------
0xff1ec978 0x01000000 winlogon.exe         OK: executable.632.exe

C:₩Python27₩Lib₩site-packages₩volatility-master>python2 vol.py -f C:₩df₩sample₩sample3.vmem imageinfo
Volatility Foundation Volatility Framework 2.6
INFO    : volatility.debug    : Determining profile based on KDBG search...
          Suggested Profile(s) : WinXPSP2x86, WinXPSP3x86 (Instantiated with WinXPSP2x86)
                     AS Layer1 : IA32PagedMemoryPae (Kernel AS)
                     AS Layer2 : FileAddressSpace (C:₩df₩sample₩sample3.vmem)
                      PAE type : PAE
                           DTB : 0x319000L
                          KDBG : 0x80545ae0L
          Number of Processors : 1
     Image Type (Service Pack) : 3
                KPCR for CPU 0 : 0xffdff000L
             KUSER_SHARED_DATA : 0xffdf0000L
           Image date and time : 2011-06-03 04:31:36 UTC+0000
     Image local date and time : 2011-06-03 00:31:36 -0400
```

2. psscan



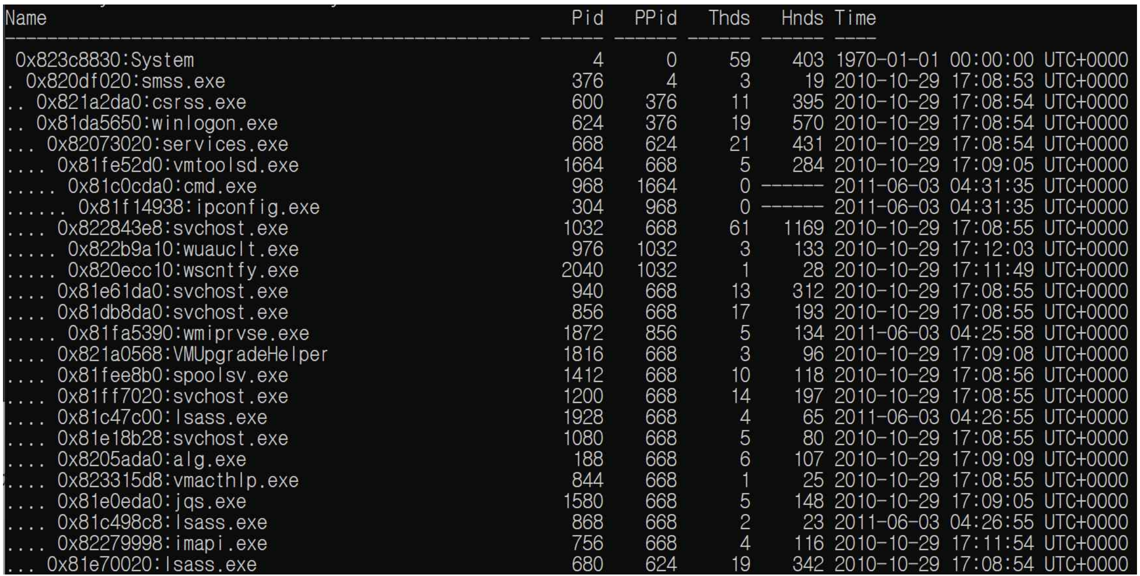
```
0x000000001e47c00 lsass.exe          1928    668 0x0a9403c0 2011-06-03 04:26:55 UTC+0000
0x000000001e498c8 lsass.exe           868    668 0x0a940360 2011-06-03 04:26:55 UTC+0000
0x000000001e543a0 Procmon.exe         660   1196 0x0a940260 2011-06-03 04:25:56 UTC+0000
0x000000001fa5650 winlogon.exe        624    376 0x0a940060 2010-10-29 17:08:54 UTC+0000
0x000000001fb8da0 svchost.exe         856    668 0x0a9400e0 2010-10-29 17:08:55 UTC+0000
0x00000000200eda0 jqs.exe            1580    668 0x0a9401e0 2010-10-29 17:09:05 UTC+0000
0x0000000002018b28 svchost.exe       1080    668 0x0a940140 2010-10-29 17:08:55 UTC+0000
0x0000000002061da0 svchost.exe        940    668 0x0a940100 2010-10-29 17:08:55 UTC+0000
0x000000000206b660 VMwareUser.exe    1356   1196 0x0a9402e0 2010-10-29 17:11:50 UTC+0000
0x0000000002070020 lsass.exe          680    624 0x0a9400a0 2010-10-29 17:08:54 UTC+0000
```

메모리에 3개의 lsass.exe 프로세스가 있음을 확인

보통 Windows XP 시스템에서 부모 프로세스가 항상 winlogon.exe인 lsass.exe는 1개만 존재해야 함.

lsass.exe는 사용자 인증 처리 포함한 보안 관련 기능 담당

3. pstree

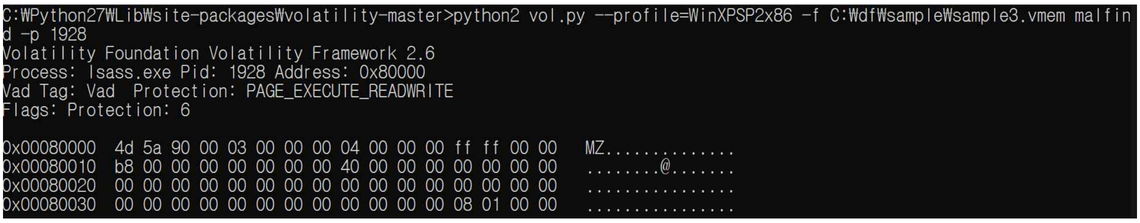


```
Name                                                  Pid   PPid   Thds   Hnds Time
-------------------------------------------------- ------ ------ ------ ------ ----
 0x823c8830:System                                      4      0     59    403 1970-01-01 00:00:00 UTC+0000
. 0x820df020:smss.exe                                 376      4      3     19 2010-10-29 17:08:53 UTC+0000
.. 0x821a2da0:csrss.exe                               600    376     11    395 2010-10-29 17:08:54 UTC+0000
.. 0x81da5650:winlogon.exe                            624    376     19    570 2010-10-29 17:08:54 UTC+0000
... 0x82073020:services.exe                           668    624     21    431 2010-10-29 17:08:54 UTC+0000
.... 0x81fe52d0:vmtoolsd.exe                         1664    668      5    284 2010-10-29 17:09:05 UTC+0000
..... 0x81c0cda0:cmd.exe                              968   1664      0 ------ 2011-06-03 04:31:35 UTC+0000
...... 0x81f14938:ipconfig.exe                        304    968      0 ------ 2011-06-03 04:31:35 UTC+0000
.... 0x822843e8:svchost.exe                          1032    668     61   1169 2010-10-29 17:08:55 UTC+0000
..... 0x822b9a10:wuauclt.exe                          976   1032      3    133 2010-10-29 17:12:03 UTC+0000
..... 0x820ecc10:wscntfy.exe                         2040   1032      1     28 2010-10-29 17:11:49 UTC+0000
.... 0x81e61da0:svchost.exe                           940    668     13    312 2010-10-29 17:08:55 UTC+0000
.... 0x81db8da0:svchost.exe                           856    668     17    193 2010-10-29 17:08:55 UTC+0000
..... 0x81fa5390:wmiprvse.exe                        1872    856      5    134 2011-06-03 04:25:58 UTC+0000
.... 0x821a0568:VMUpgradeHelper                      1816    668      3     96 2010-10-29 17:09:08 UTC+0000
.... 0x81fee8b0:spoolsv.exe                          1412    668     10    118 2010-10-29 17:08:56 UTC+0000
.... 0x81ff7020:svchost.exe                          1200    668     14    197 2010-10-29 17:08:55 UTC+0000
.... 0x81c47c00:lsass.exe                            1928    668      4     65 2011-06-03 04:26:55 UTC+0000
.... 0x81e18b28:svchost.exe                          1080    668      5     80 2010-10-29 17:08:55 UTC+0000
.... 0x8205ada0:alg.exe                               188    668      6    107 2010-10-29 17:09:09 UTC+0000
.... 0x823315d8:vmacthlp.exe                          844    668      1     25 2010-10-29 17:08:55 UTC+0000
.... 0x81e0eda0:jqs.exe                              1580    668      5    148 2010-10-29 17:09:05 UTC+0000
.... 0x81c498c8:lsass.exe                             868    668      2     23 2011-06-03 04:26:55 UTC+0000
.... 0x82279998:imapi.exe                             756    668      4    116 2010-10-29 17:11:54 UTC+0000
... 0x81e70020:lsass.exe                              680    624     19    342 2010-10-29 17:08:54 UTC+0000
```

PID가 1928과 868인 2개의 lsass.exe 프로세스는 services.exe의 부모를 가지고 있음. WinXP에서 부모 프로세스는 winlogon.exe여야 함.

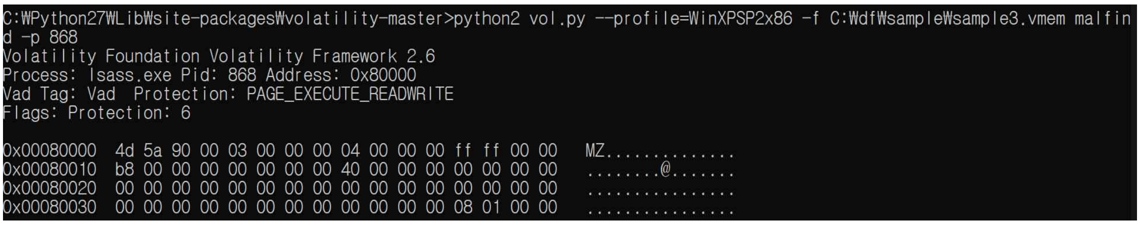
4. malfind

malfind -p 1928



```
C:₩Python27₩Lib₩site-packages₩volatility-master>python2 vol.py --profile=WinXPSP2x86 -f C:₩df₩sample₩sample3.vmem malfin
d -p 1928
Volatility Foundation Volatility Framework 2.6
Process: lsass.exe Pid: 1928 Address: 0x80000
Vad Tag: Vad  Protection: PAGE_EXECUTE_READWRITE
Flags: Protection: 6

0x00080000  4d 5a 90 00 03 00 00 00 04 00 00 00 ff ff 00 00   MZ..............
0x00080010  b8 00 00 00 00 00 00 00 40 00 00 00 00 00 00 00   ........@.......
0x00080020  00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00   ................
0x00080030  00 00 00 00 00 00 00 00 00 00 00 00 08 01 00 00   ................
```

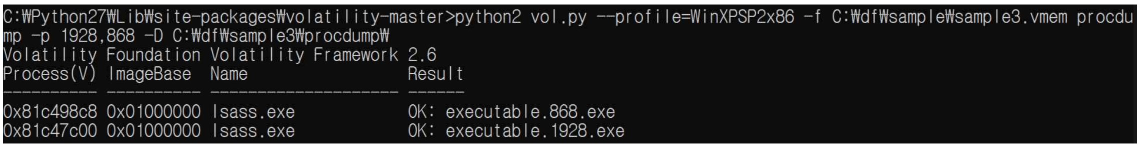
malfind -p 868



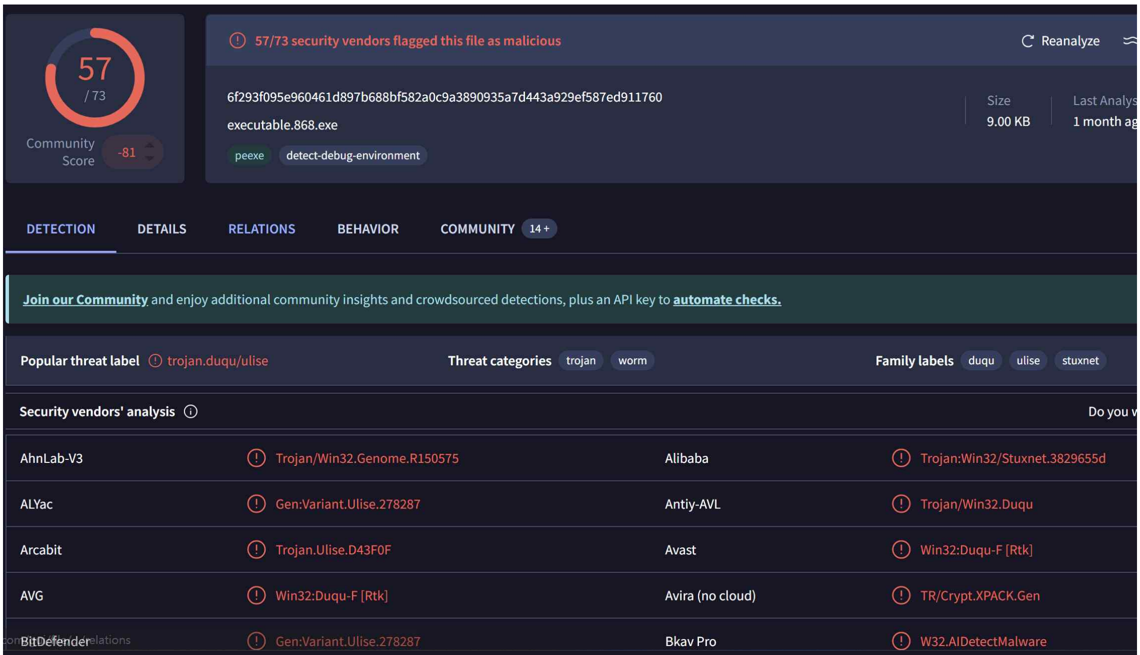
```
C:₩Python27₩Lib₩site-packages₩volatility-master>python2 vol.py --profile=WinXPSP2x86 -f C:₩df₩sample₩sample3.vmem malfin
d -p 868
Volatility Foundation Volatility Framework 2.6
Process: lsass.exe Pid: 868 Address: 0x80000
Vad Tag: Vad  Protection: PAGE_EXECUTE_READWRITE
Flags: Protection: 6

0x00080000  4d 5a 90 00 03 00 00 00 04 00 00 00 ff ff 00 00   MZ..............
0x00080010  b8 00 00 00 00 00 00 00 40 00 00 00 00 00 00 00   ........@.......
0x00080020  00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00   ................
0x00080030  00 00 00 00 00 00 00 00 00 00 00 00 08 01 00 00   ................
```

- 두 프로세스는 보호되는 메모리 영역 가지고 있음
- PAGE_EXECUTE_READWRITE. 일반적으로 메모리 섹션은 동시에 실행되고 쓰기가 가능해서는 안됨.
- 프로세스 이름과 경로는 정상이지만 메모리 영역이 잘못된 보호로 인해 실행되는 경우 있음

5. procdump 868, 1928



```
C:₩Python27₩Lib₩site-packages₩volatility-master>python2 vol.py --profile=WinXPSP2x86 -f C:₩df₩sample₩sample3.vmem procdu
mp -p 1928,868 -D C:₩df₩sample3₩procdump₩
Volatility Foundation Volatility Framework 2.6
Process(V) ImageBase  Name                 Result
---------- ---------- -------------------- ------
0x81c498c8 0x01000000 lsass.exe            OK: executable.868.exe
0x81c47c00 0x01000000 lsass.exe            OK: executable.1928.exe
```



57 / 73

Community Score -81

57/73 security vendors flagged this file as malicious

Reanalyze

6f293f095e960461d897b688bf582a0c9a3890935a7d443a929ef587ed911760

executable.868.exe

peexe detect-debug-environment

Size 9.00 KB

Last Analys
1 month ag

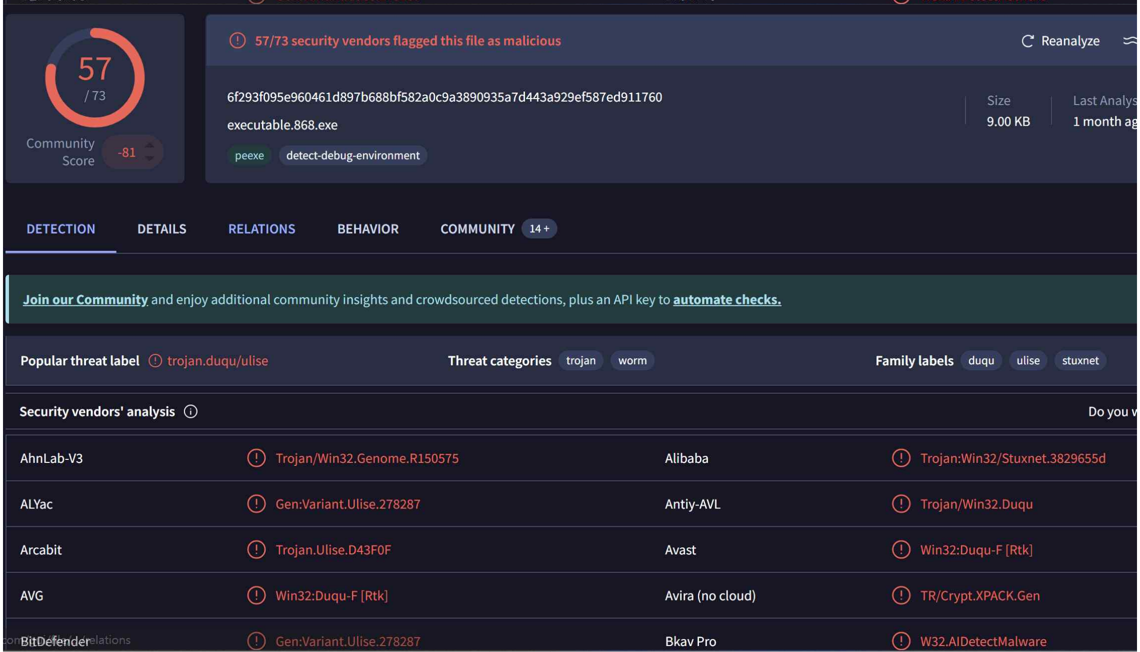
DETECTION DETAILS RELATIONS BEHAVIOR COMMUNITY 14 +

Join our Community and enjoy additional community insights and crowdsourced detections, plus an API key to **automate checks.**

Popular threat label trojan.duqu/ulise **Threat categories** trojan worm **Family labels** duqu ulise stuxnet

Security vendors' analysis Do you v

AhnLab-V3	Trojan/Win32.Genome.R150575	Alibaba	Trojan:Win32/Stuxnet.3829655d
ALYac	Gen:Variant.Ulise.278287	Antiy-AVL	Trojan/Win32.Duqu
Arcabit	Trojan.Ulise.D43F0F	Avast	Win32:Duqu-F [Rtk]
AVG	Win32:Duqu-F [Rtk]	Avira (no cloud)	TR/Crypt.XPACK.Gen
BitDefender	Gen:Variant.Ulise.278287	Bkav Pro	W32.AIDetectMalware



57 / 73

Community Score -81

57/73 security vendors flagged this file as malicious

Reanalyze

6f293f095e960461d897b688bf582a0c9a3890935a7d443a929ef587ed911760

executable.868.exe

peexe detect-debug-environment

Size 9.00 KB

Last Analys
1 month ag

DETECTION DETAILS RELATIONS BEHAVIOR COMMUNITY 14 +

Join our Community and enjoy additional community insights and crowdsourced detections, plus an API key to **automate checks.**

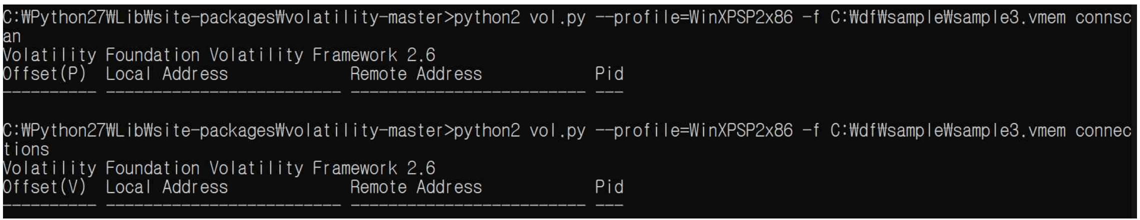
Popular threat label trojan.duqu/ulise **Threat categories** trojan worm **Family labels** duqu ulise stuxnet

Security vendors' analysis Do you v

AhnLab-V3	Trojan/Win32.Genome.R150575	Alibaba	Trojan:Win32/Stuxnet.3829655d
ALYac	Gen:Variant.Ulise.278287	Antiy-AVL	Trojan/Win32.Duqu
Arcabit	Trojan.Ulise.D43F0F	Avast	Win32:Duqu-F [Rtk]
AVG	Win32:Duqu-F [Rtk]	Avira (no cloud)	TR/Crypt.XPACK.Gen
BitDefender	Gen:Variant.Ulise.278287	Bkav Pro	W32.AIDetectMalware

바이러스 토탈 검사시 해당 프로세스가 '듀크' 악성이라는 것 확인 가능

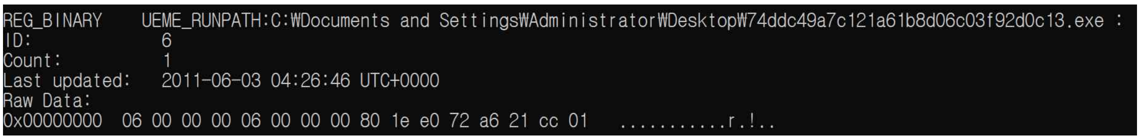
6. connscan, connections



```
C:₩Python27₩Lib₩site-packages₩volatility-master>python2 vol.py --profile=WinXPSP2x86 -f C:₩df₩sample₩sample3.vmem connsc
an
Volatility Foundation Volatility Framework 2.6
Offset(P)  Local Address             Remote Address            Pid
---------- ------------------------- ------------------------- ---

C:₩Python27₩Lib₩site-packages₩volatility-master>python2 vol.py --profile=WinXPSP2x86 -f C:₩df₩sample₩sample3.vmem connec
tions
Volatility Foundation Volatility Framework 2.6
Offset(V)  Local Address             Remote Address            Pid
---------- ------------------------- ------------------------- ---
```

메모리에서 열린 연결이 없다는 것을 알 수 있음

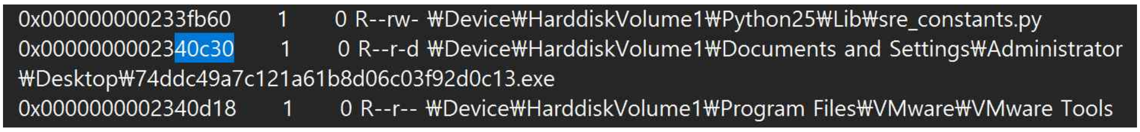
7. userassist – 레지스트리 관련 정보 확인



```
REG_BINARY    UEME_RUNPATH:C:₩Documents and Settings₩Administrator₩Desktop₩74ddc49a7c121a61b8d06c03f92d0c13.exe :
ID:             6
Count:          1
Last updated:   2011-06-03 04:26:46 UTC+0000
Raw Data:
0x00000000  06 00 00 00 06 00 00 00 80 1e e0 72 a6 21 cc 01   ...........r.!..
```

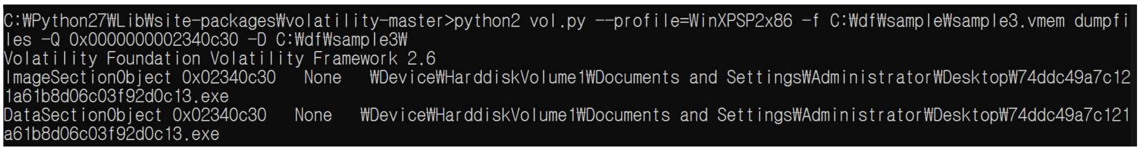
의심되는 파일 : 74ddc49a7c121a61b8d06c03f92d0c13.exe

8. filescan – 메모리상에 실행, 생성, 삭제 된 파일들 흔적 확인



```
0x000000000233fb60    1      0 R--rw- ₩Device₩HarddiskVolume1₩Python25₩Lib₩sre_constants.py
0x0000000002340c30    1      0 R--r-d ₩Device₩HarddiskVolume1₩Documents and Settings₩Administrator
₩Desktop₩74ddc49a7c121a61b8d06c03f92d0c13.exe
0x0000000002340d18    1      0 R--r-- ₩Device₩HarddiskVolume1₩Program Files₩VMware₩VMware Tools
```

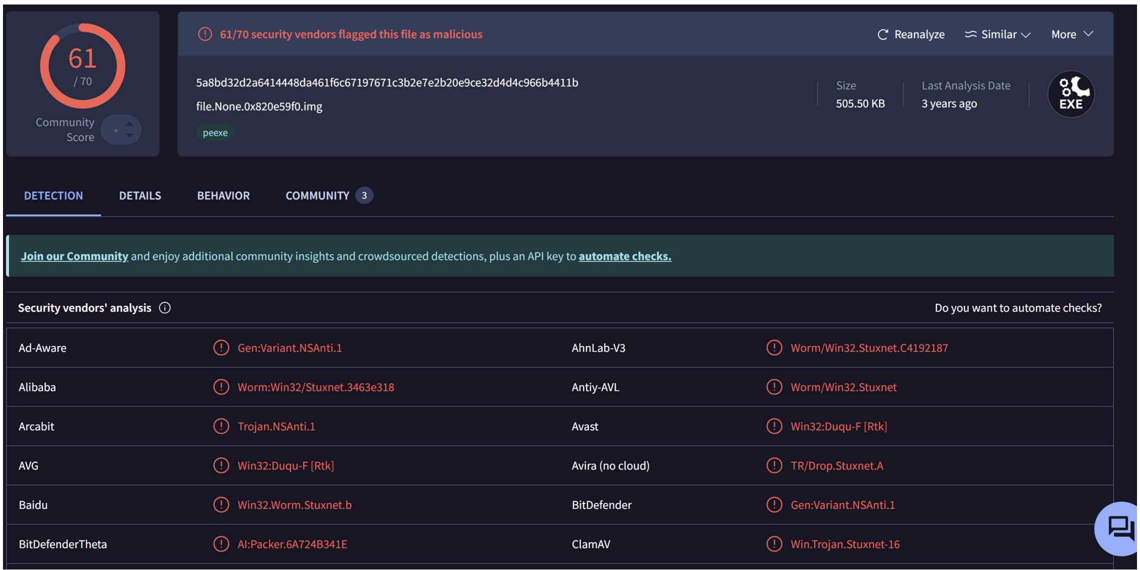
9. dumpfiles – 해당 파일 덤프(filescan 주소값으로) 복구



```
C:₩Python27₩Lib₩site-packages₩volatility-master>python2 vol.py --profile=WinXPSP2x86 -f C:₩df₩sample₩sample3.vmem dumpfi
les -Q 0x0000000002340c30 -D C:₩df₩sample3₩
Volatility Foundation Volatility Framework 2.6
ImageSectionObject 0x02340c30   None   ₩Device₩HarddiskVolume1₩Documents and Settings₩Administrator₩Desktop₩74ddc49a7c12
1a61b8d06c03f92d0c13.exe
DataSectionObject 0x02340c30   None   ₩Device₩HarddiskVolume1₩Documents and Settings₩Administrator₩Desktop₩74ddc49a7c121
a61b8d06c03f92d0c13.exe
```

의심 파일 : 74ddc49a7c121a61b8d06c03f92d0c13.exe

10. 바이러스 토탈



61/70 security vendors flagged this file as malicious

5a8bd32d2a6414448da461f6c67197671c3b2e7e2b20e9ce32d4d4c966b4411b

file.None.0x820e59f0.img

peexe

Size 505.50 KB

Last Analysis Date 3 years ago

DETECTION DETAILS BEHAVIOR COMMUNITY 3

Join our Community and enjoy additional community insights and crowdsourced detections, plus an API key to automate checks.

Security vendors' analysis

Do you want to automate checks?

Ad-Aware	Gen:Variant.NSAnti.1	AhnLab-V3	Worm/Win32.Stuxnet.C4192187
Alibaba	Worm:Win32/Stuxnet.3463e318	Antiy-AVL	Worm/Win32.Stuxnet
Arcabit	Trojan.NSAnti.1	Avast	Win32:Duqu-F [Rtk]
AVG	Win32:Duqu-F [Rtk]	Avira (no cloud)	TR/Drop.Stuxnet.A
Baidu	Win32.Worm.Stuxnet.b	BitDefender	Gen:Variant.NSAnti.1
BitDefenderTheta	AI:Packer.6A724B341E	ClamAV	Win.Trojan.Stuxnet-16

듀크와 비슷한 종류의 악성코드인 '스턱스넷'임을 확인