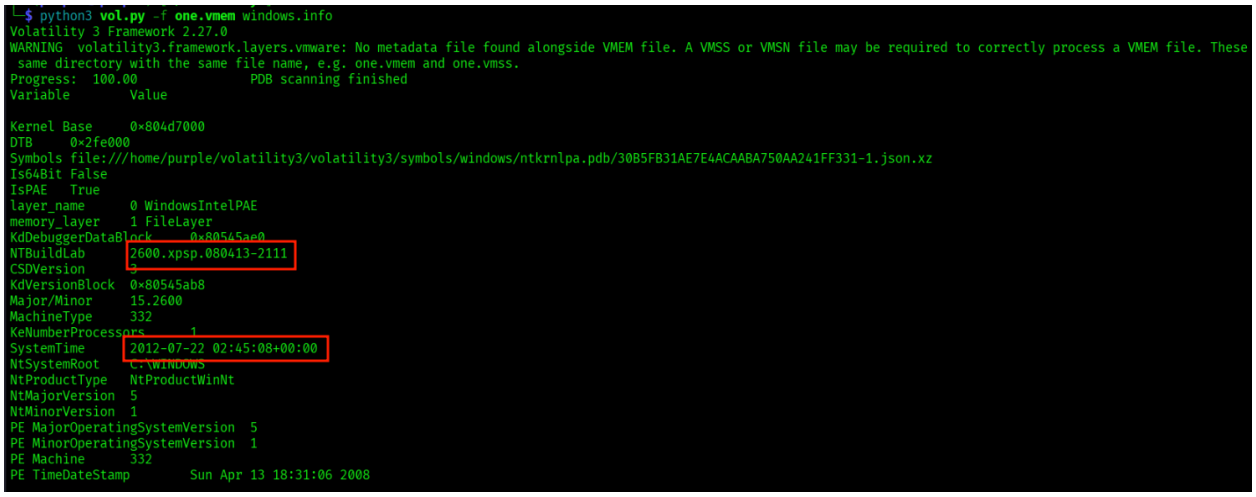
Volatility

Task 10 Practical Investigations

I have downloaded the task files into my vm and i changed the names as one and two for case 1 and case 2

What is the build version of the host machine in Case 001?

Use python3 vol.py -f one.vmem windows.info



2600.xpsp.080413-2111

At what time was the memory file acquired in Case 001?

2012-07-22 02:45:08

What process can be considered suspicious in Case 001?
Note: Certain special characters may not be visible on the provided VM. When doing a copy-and-paste, it will still copy all characters.

python3 vol.py -f one.vmem windows.psscan

```
└─$ python3 vol.py -f one.vmem windows.psscan
Volatility 3 Framework 2.27.0
WARNING  volatility3.framework.layers.vmware: No metadata file found alongside VMEM file. A VMSS or VMSN file may be required to correc
 same directory with the same file name, e.g. one.vmem and one.vmss.
Progress:  100.00               PDB scanning finished
PID     PPID    ImageFileName   Offset(V)       Threads Handles SessionId       Wow64   CreateTime      ExitTime        File output

908     652     svchost.exe     0×2029ab8       9       226     0       False   2012-07-22 02:42:33.000000 UTC  N/A     Disabled
664     608     lsass.exe       0×202a3b8       24      330     0       False   2012-07-22 02:42:32.000000 UTC  N/A     Disabled
652     608     services.exe    0×202ab28       16      243     0       False   2012-07-22 02:42:32.000000 UTC  N/A     Disabled
1640    1484    reader_sl.exe   0×207bda0       5       39      0       False   2012-07-22 02:42:36.000000 UTC  N/A     Disabled
1512    652     spoolsv.exe     0×20b17b8       14      113     0       False   2012-07-22 02:42:36.000000 UTC  N/A     Disabled
1588    1004    wuauclt.exe     0×225bda0       5       132     0       False   2012-07-22 02:44:01.000000 UTC  N/A     Disabled
788     652     alg.exe 0×22e8da0       7       104     0       False   2012-07-22 02:43:01.000000 UTC  N/A     Disabled
1484    1464    explorer.exe    0×23dea70       17      415     0       False   2012-07-22 02:42:36.000000 UTC  N/A     Disabled
1056    652     svchost.exe     0×23dfda0       5       60      0       False   2012-07-22 02:42:33.000000 UTC  N/A     Disabled
1136    1004    wuauclt.exe     0×23fcda0       8       173     0       False   2012-07-22 02:43:46.000000 UTC  N/A     Disabled
1220    652     svchost.exe     0×2495650       15      197     0       False   2012-07-22 02:42:35.000000 UTC  N/A     Disabled
608     368     winlogon.exe    0×2498700       23      519     0       False   2012-07-22 02:42:32.000000 UTC  N/A     Disabled
584     368     csrss.exe       0×24a0598       9       326     0       False   2012-07-22 02:42:32.000000 UTC  N/A     Disabled
368     4       smss.exe        0×24f1020       3       19      N/A     False   2012-07-22 02:42:31.000000 UTC  N/A     Disabled
1004    652     svchost.exe     0×25001d0       64      1118    0       False   2012-07-22 02:42:33.000000 UTC  N/A     Disabled
824     652     svchost.exe     0×2511360       20      194     0       False   2012-07-22 02:42:33.000000 UTC  N/A     Disabled
4       0       System  0×25c89c8       53      240     N/A     False   N/A     N/A     Disabled
```

reader_sl.exe

What is the parent process of the suspicious process in Case 001?
python3 vol.py -f one.vmem windows.pstree

```
WS\system32\svchost.exe C:\WINDOWS\system32\svchost -k DcomLaunch        C:\WINDOWS\system32\svchost.exe
1484    1464    explorer.exe    0×821dea70      17      415     0       False   2012-07-22 02:42:36.00000
rer.exe C:\WINDOWS\Explorer.EXE C:\WINDOWS\Explorer.EXE
* 1640  1484    reader_sl.exe   0×81e7bda0      5       39      0       False   2012-07-22 02:42:36.00000
\Adobe\Reader 9.0\Reader\reader_sl.exe  "C:\Program Files\Adobe\Reader 9.0\Reader\Reader_sl.exe"        C
```

1484 is the pid of parent
explorer.exe

What is the PID of the suspicious process in Case 001?

It is available from the previous question

1640

What is the parent process PID in Case 001?

1484

What user-agent was employed by the adversary in Case 001?

First we need to dump the memory based on the suspicious process , then need to extract the user-agent using strings

python3 vol.py -f one.vmem -o output_dir windows.memmap.Memmap --pid 1640 --dump

```
└─$ ls
pid.1640.dmp

┌──(purple㉿purple)-[~/volatility3/output_dir]
└─$ strings pid.1640.dmp | grep -i  "user-agent"
User-Agent
User-Agent: Mozilla/5.0 (Windows; U; MSIE 7.0; Windows NT 6.0; en-US)
 cs(User-Agent)
USER-AGENT:
User-Agent:

┌──(purple㉿purple)-[~/volatility3/output_dir]
└─$ _
```

Mozilla/5.0 (Windows; U; MSIE 7.0; Windows NT 6.0; en-US)

Was Chase Bank one of the suspicious bank domains found in Case 001? (Y/N)

Search for the case in the dumps of the suspicious process

strings pid.1640.dmp | grep -i "chase"

```
ges//spacer.gif" alt="Step three of three has not been completed." width="1" height="1
head">Confirm your personality <img src="https://chaseonline.chase.com/content/ecpweb/
https (S S L) 128-bit Encryption" title="Your information is securely transmitted via
rder="0" cellspacing="0" cellpadding="0" class="fullwidth" summary="terms of use link
 style="width:30%; vertical-align:top"> </td><td align="center" width="40%" valign="to
ent.location.href='http://www.chase.com//ccp/index.jsp?pg_name=ccpmapp/shared/assets/p
ver="window.status='';return true" onFocus="window.status='';return true" onMouseOut="
 ⟶<a id="TermsLink" href="JavaScript:document.location.href='http://www.chase.com//c
.status='';return true" onMouseOver="window.status='';return true" onFocus="window.sta
Use</a> ⇐!— mp_trans_remove_end —⟶⇐!— mp_trans_add<a id="TermsLink" href="JavaScrip
pp/spanish/resources/page/terms';" onBlur="window.status='';return true" onMouseOver="
MouseOut="window.status='';return true">Terms of Use</a> ⟶</span></td><td style="tex
class="printable"><table border="0" cellspacing="0" cellpadding="0" class="fullwidth">
ertext">
 Co.</td></tr><tr><td class="spacerh10"> </td></tr></table></div>⇐!—END Footer⟶
="ifr2" src="https://www.chase.com/online/Home/images/chaseNewlogo.gif" frameborder="0

 name="ge93Zid02L5" action="https://www.chase.com/online/Home/images/chaseNewlogo.gif"
  url:  "https://chaseonline.chase.com/gw/secure/ena",
```

Yes

What suspicious process is running at PID 740 in Case 002?

python3 vol.py -f two.raw windows.pslist

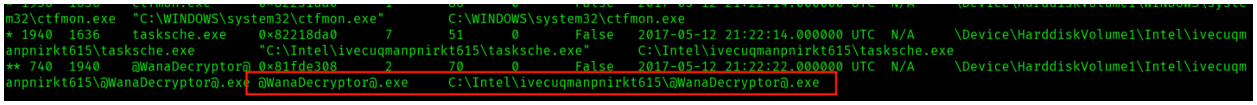
```
└─$ python3 vol.py -f two.raw windows.pslist
Volatility 3 Framework 2.27.0
Progress:  100.00               PDB scanning finished
PID     PPID    ImageFileName   Offset(V)       Threads Handles SessionId       Wow64   CreateTime      ExitTime        File outpu

4       0       System  0×823c8830      51      244     N/A     False   N/A     N/A     Disabled
348     4       smss.exe        0×82169020      3       19      N/A     False   2017-05-12 21:21:55.000000 UTC  N/A     Disabled
596     348     csrss.exe       0×82161da0      12      352     0       False   2017-05-12 21:22:00.000000 UTC  N/A     Disabled
620     348     winlogon.exe    0×8216e020      23      536     0       False   2017-05-12 21:22:01.000000 UTC  N/A     Disabled
664     620     services.exe    0×821937f0      15      265     0       False   2017-05-12 21:22:01.000000 UTC  N/A     Disabled
676     620     lsass.exe       0×82191658      23      353     0       False   2017-05-12 21:22:01.000000 UTC  N/A     Disabled
836     664     svchost.exe     0×8221a2c0      19      211     0       False   2017-05-12 21:22:02.000000 UTC  N/A     Disabled
904     664     svchost.exe     0×821b5230      9       227     0       False   2017-05-12 21:22:03.000000 UTC  N/A     Disabled
1024    664     svchost.exe     0×821af7e8      79      1366    0       False   2017-05-12 21:22:03.000000 UTC  N/A     Disabled
1084    664     svchost.exe     0×8203b7a8      6       72      0       False   2017-05-12 21:22:03.000000 UTC  N/A     Disabled
1152    664     svchost.exe     0×821bea78      10      173     0       False   2017-05-12 21:22:06.000000 UTC  N/A     Disabled
1484    664     spoolsv.exe     0×821e2da0      14      124     0       False   2017-05-12 21:22:09.000000 UTC  N/A     Disabled
1636    1608    explorer.exe    0×821d9da0      11      331     0       False   2017-05-12 21:22:10.000000 UTC  N/A     Disabled
1940    1636    tasksche.exe    0×82218da0      7       51      0       False   2017-05-12 21:22:14.000000 UTC  N/A     Disabled
1956    1636    ctfmon.exe      0×82231da0      1       86      0       False   2017-05-12 21:22:14.000000 UTC  N/A     Disabled
260     664     svchost.exe     0×81fb95d8      5       105     0       False   2017-05-12 21:22:18.000000 UTC  N/A     Disabled
740     1940    @WanaDecryptor@ 0×81fde308      2       70      0       False   2017-05-12 21:22:22.000000 UTC  N/A     Disabled
1768    1024    wuauclt.exe     0×81f747c0      7       132     0       False   2017-05-12 21:22:52.000000 UTC  N/A     Disabled
544     664     alg.exe 0×82010020      6       101     0       False   2017-05-12 21:22:55.000000 UTC  N/A     Disabled
1168    1024    wscntfy.exe     0×81fea8a0      1       37      0       False   2017-05-12 21:22:56.000000 UTC  N/A     Disabled
```

@WanaDecryptor@

What is the full path of the suspicious binary in PID 740 in Case 002?

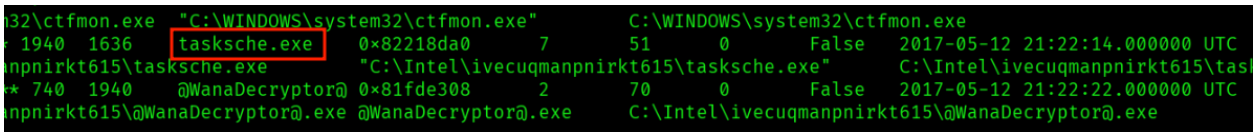
python3 vol.py -f two.raw windows.pstree



C:\Intel\ivecuqmanpnirkt615\@WanaDecryptor@.exe

What is the parent process of PID 740 in Case 002?

It is easy to find from the last question



tasksche.exe

What is the suspicious parent process PID connected to the decryptor in Case 002?

Front the past question ：1940

From our current information, what malware is present on the system in Case 002?

Do some online research with the information that we have

Wannacry

What DLL is loaded by the decryptor used for socket creation in Case 002?

```
└─$ python3 vol.py -f two.raw windows.dlllist | grep  "740"
1024resssvchost.exe     0x5f740000      0x0e000  ncprov.dll      C:\WINDOWS\system32\wbem\ncprov.dll     1
740     @WanaDecryptor@ 0x400000        0x3d000 @WanaDecryptor@.exe     C:\Intel\ivecuqmanpnirkt615\@WanaDecr
740     @WanaDecryptor@ 0x7c900000      0xb2000 ntdll.dll       C:\WINDOWS\system32\ntdll.dll   -1      N/A
740     @WanaDecryptor@ 0x7c800000      0xf6000 kernel32.dll    C:\WINDOWS\system32\kernel32.dll        -1
740     @WanaDecryptor@ 0x73dd0000      0xf2000 MFC42.DLL       C:\WINDOWS\system32\MFC42.DLL   -1      N/A
740     @WanaDecryptor@ 0x77c10000      0x58000 msvcrt.dll      C:\WINDOWS\system32\msvcrt.dll  -1      N/A
740     @WanaDecryptor@ 0x77f10000      0x49000 GDI32.dll       C:\WINDOWS\system32\GDI32.dll   -1      N/A
740     @WanaDecryptor@ 0x7e410000      0x91000 USER32.dll      C:\WINDOWS\system32\USER32.dll  -1      N/A
740     @WanaDecryptor@ 0x77dd0000      0x9b000 ADVAPI32.dll    C:\WINDOWS\system32\ADVAPI32.dll        -1
740     @WanaDecryptor@ 0x77e70000      0x93000 RPCRT4.dll      C:\WINDOWS\system32\RPCRT4.dll  -1      N/A
740     @WanaDecryptor@ 0x77fe0000      0x11000 Secur32.dll     C:\WINDOWS\system32\Secur32.dll -1      N/A
740     @WanaDecryptor@ 0x7c9c0000      0x818000        SHELL32.dll     C:\WINDOWS\system32\SHELL32.dll -1
740     @WanaDecryptor@ 0x77f60000      0x76000 SHLWAPI.dll     C:\WINDOWS\system32\SHLWAPI.dll -1      N/A
740     @WanaDecryptor@ 0x773d0000      0x103000        COMCTL32.dll    C:\WINDOWS\WinSxS\X86_Microsoft.Windo
8_x-ww_61e65202\COMCTL32.dll    -1      N/A     Disabled
740     @WanaDecryptor@ 0x77120000      0x8b000 OLEAUT32.dll    C:\WINDOWS\system32\OLEAUT32.dll        -1
740     @WanaDecryptor@ 0x774e0000      0x13e000        ole32.dll       C:\WINDOWS\system32\ole32.dll   -1
740     @WanaDecryptor@ 0x78130000      0x134000        urlmon.dll      C:\WINDOWS\system32\urlmon.dll  -1
740     @WanaDecryptor@ 0x3dfd0000      0x1ec000        iertutil.dll    C:\WINDOWS\system32\iertutil.dll
740     @WanaDecryptor@ 0x76080000      0x65000 MSVCP60.dll     C:\WINDOWS\system32\MSVCP60.dll -1      N/A
740     @WanaDecryptor@ 0x71ab0000      0x17000 WS2_32.dll      C:\WINDOWS\system32\WS2_32.dll  -1      N/A
740     @WanaDecryptor@ 0x71aa0000      0x8000  WS2HELP.dll     C:\WINDOWS\system32\WS2HELP.dll -1      N/A
740     @WanaDecryptor@ 0x3d930000      0xe7000 WININET.dll     C:\WINDOWS\system32\WININET.dll -1      N/A
740     @WanaDecryptor@ 0x340000        0x9000  Normaliz.dll    C:\WINDOWS\system32\Normaliz.dll        -1
740     @WanaDecryptor@ 0x76390000      0x1d000 IMM32.DLL       C:\WINDOWS\system32\IMM32.DLL   4       N/A
740     @WanaDecryptor@ 0x629c0000      0x9000  LPK.DLL C:\WINDOWS\system32\LPK.DLL     1       N/A     Disab
740     @WanaDecryptor@ 0x74d90000      0x6b000 USP10.dll       C:\WINDOWS\system32\USP10.dll   2       N/A
```

WS2_32.dll

What mutex can be found that is a known indicator of the malware in question in Case 002?

python3 vol.py -f two.raw windows.handles | grep "1940"

```
1940    tasksche.exe    0x823d54d0      0x4c    Semaphore       0x1f0003        shell.{A48F1A32-A340-11D
1940    tasksche.exe    0x823a0cd0      0x50    File    0x100020        \Device\HarddiskVolume1\WINDOWS\
44ccf1df_6.0.2600.6028_x-ww_61e65202
1940    tasksche.exe    0x8224f180      0x54    Mutant  0x1f0001        MsWinZonesCacheCounterMutexA
1940    tasksche.exe    0x822e3b08      0x58    Mutant  0x1f0001        MsWinZonesCacheCounterMutexA0
1940    tasksche.exe    0x82234450      0x5c    Event   0x1f0003        -
1940    tasksche.exe    0x821dbdd8      0x60    Semaphore       0x100003        -
1940    tasksche.exe    0x822398f8      0x64    Semaphore       0x100003        -
```

MsWinZonesCacheCounterMutexA

What plugin could be used to identify all files loaded from the malware working directory in Case 002?

```
└─$ python3 vol.py -h | grep windows | grep file
    windows.dumpfiles.DumpFiles
    windows.filescan.FileScan
                        Scans for file objects present in a particular windows
```

windows.filescan