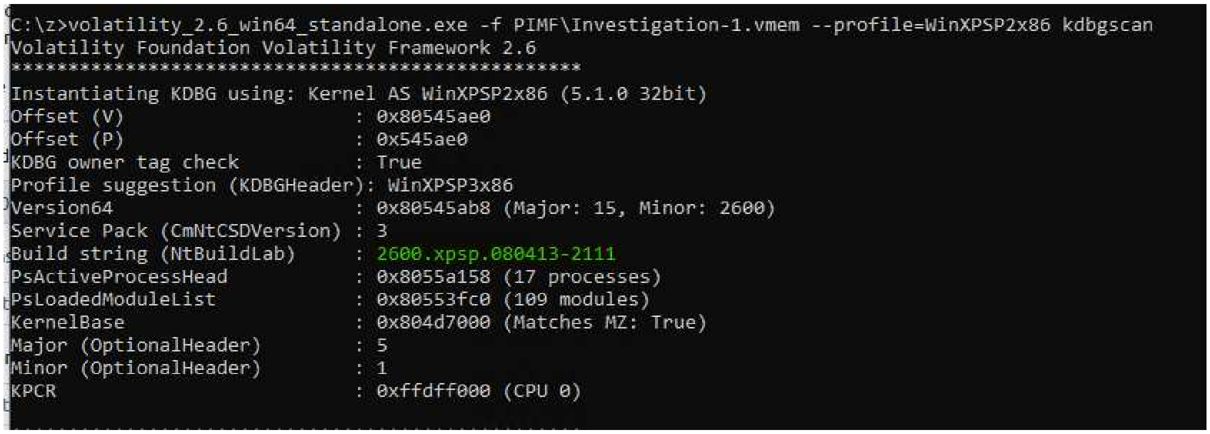
Volatility

martes, 6 de abril de 2021 19:33

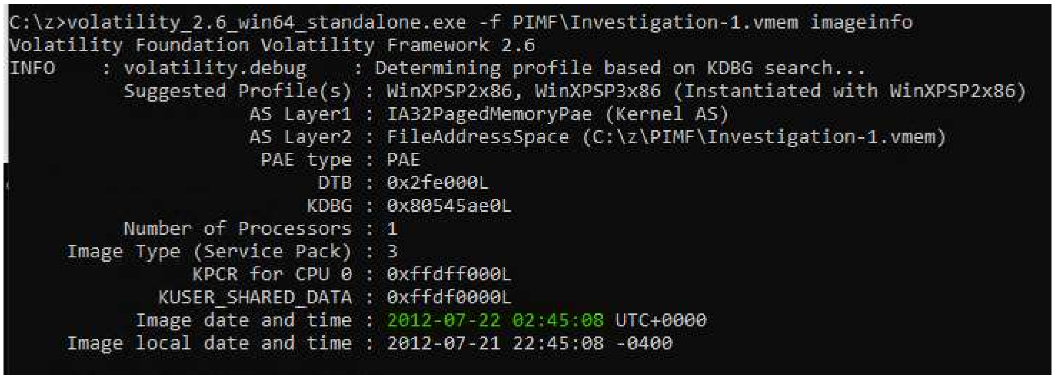
What is the build version of the host machine in Case 001?

Desde <https://tryhackme.com/room/volatility>



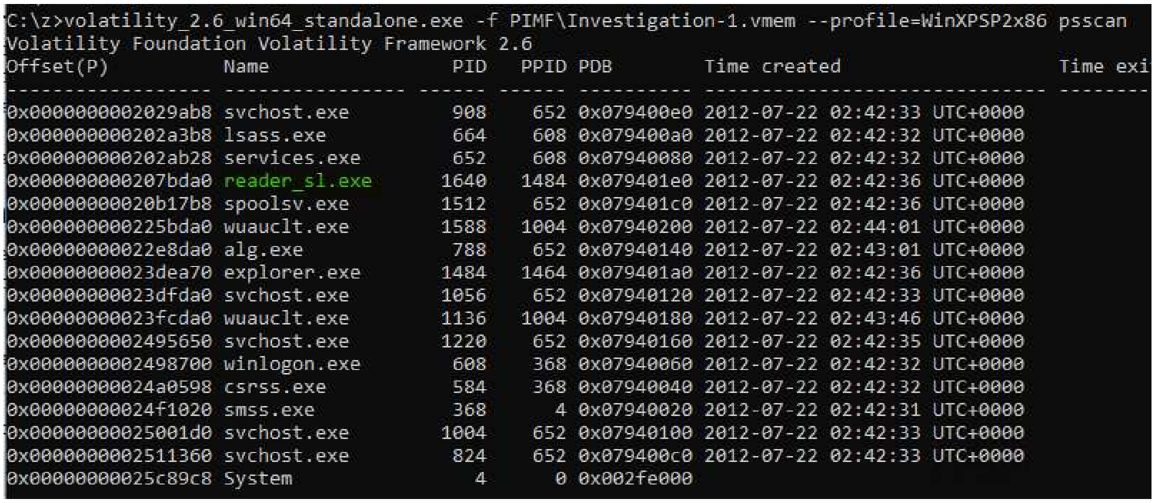
```
C:\z>volatility_2.6_win64_standalone.exe -f PIMF\Investigation-1.vmem --profile=WinXPSP2x86 kdbgscan
Volatility Foundation Volatility Framework 2.6
**************************************************
Instantiating KDBG using: Kernel AS WinXPSP2x86 (5.1.0 32bit)
Offset (V)                    : 0x80545ae0
Offset (P)                    : 0x545ae0
KDBG owner tag check          : True
Profile suggestion (KDBGHeader): WinXPSP3x86
Version64                     : 0x80545ab8 (Major: 15, Minor: 2600)
Service Pack (CmNtCSDVersion) : 3
Build string (NtBuildLab)     : 2600.xpsp.080413-2111
PsActiveProcessHead           : 0x8055a158 (17 processes)
PsLoadedModuleList            : 0x80553fc0 (109 modules)
KernelBase                    : 0x804d7000 (Matches MZ: True)
Major (OptionalHeader)        : 5
Minor (OptionalHeader)        : 1
KPCR                          : 0xffdff000 (CPU 0)
```

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



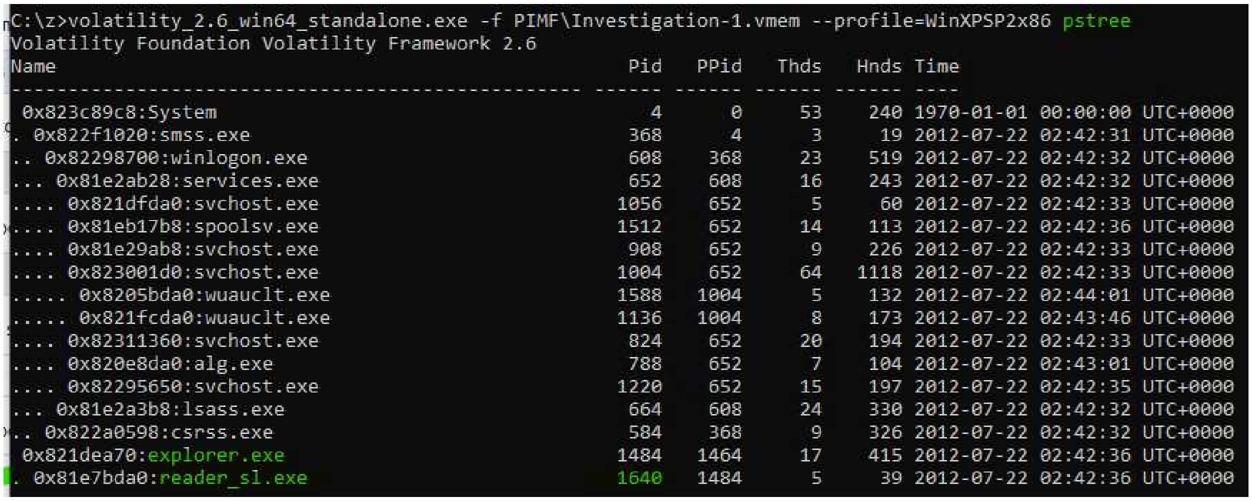
```
C:\z>volatility_2.6_win64_standalone.exe -f PIMF\Investigation-1.vmem imageinfo
Volatility Foundation Volatility Framework 2.6
INFO    : volatility.debug    : Determining profile based on KDBG search...
          Suggested Profile(s) : WinXPSP2x86, WinXPSP3x86 (Instantiated with WinXPSP2x86)
                     AS Layer1 : IA32PagedMemoryPae (Kernel AS)
                     AS Layer2 : FileAddressSpace (C:\z\PIMF\Investigation-1.vmem)
                      PAE type : PAE
                           DTB : 0x2fe000L
                          KDBG : 0x80545ae0L
          Number of Processors : 1
     Image Type (Service Pack) : 3
                KPCR for CPU 0 : 0xffdff000L
             KUSER_SHARED_DATA : 0xffdf0000L
           Image date and time : 2012-07-22 02:45:08 UTC+0000
     Image local date and time : 2012-07-21 22:45:08 -0400
```

What process can be considered suspicious in Case 001?



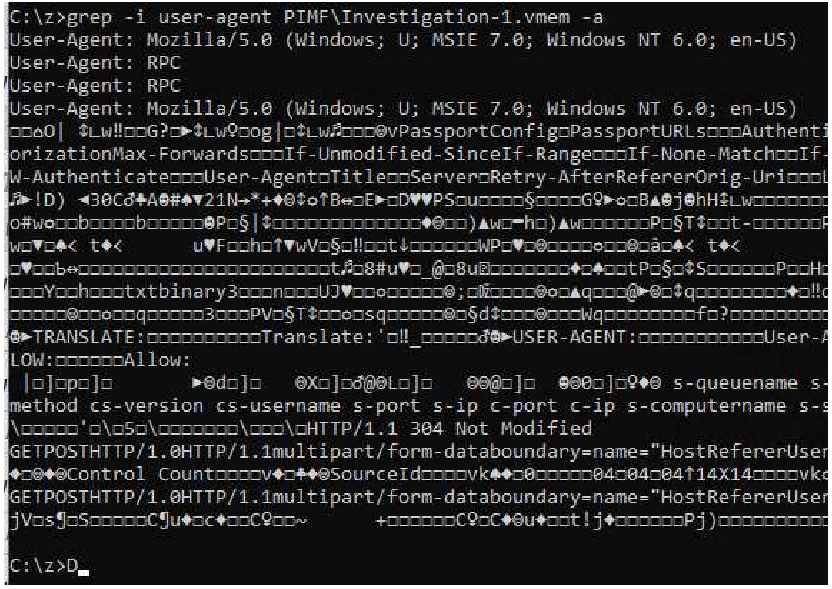
```
C:\z>volatility_2.6_win64_standalone.exe -f PIMF\Investigation-1.vmem --profile=WinXPSP2x86 psscan
Volatility Foundation Volatility Framework 2.6
Offset(P)          Name                PID   PPID PDB        Time created                   Time exi
------------------ ---------------- ------ ------ ---------- ------------------------------ --------
0x0000000002029ab8 svchost.exe         908    652 0x079400e0 2012-07-22 02:42:33 UTC+0000
0x000000000202a3b8 lsass.exe           664    608 0x079400a0 2012-07-22 02:42:32 UTC+0000
0x000000000202ab28 services.exe        652    608 0x07940080 2012-07-22 02:42:32 UTC+0000
0x000000000207bda0 reader_sl.exe      1640   1484 0x079401e0 2012-07-22 02:42:36 UTC+0000
0x00000000020b17b8 spoolsv.exe        1512    652 0x079401c0 2012-07-22 02:42:36 UTC+0000
0x000000000225bda0 wuauclt.exe        1588   1004 0x07940200 2012-07-22 02:44:01 UTC+0000
0x00000000022e8da0 alg.exe             788    652 0x07940140 2012-07-22 02:43:01 UTC+0000
0x00000000023dea70 explorer.exe       1484   1464 0x079401a0 2012-07-22 02:42:36 UTC+0000
0x00000000023dfda0 svchost.exe        1056    652 0x07940120 2012-07-22 02:42:33 UTC+0000
0x00000000023fcda0 wuauclt.exe        1136   1004 0x07940180 2012-07-22 02:43:46 UTC+0000
0x0000000002495650 svchost.exe        1220    652 0x07940160 2012-07-22 02:42:35 UTC+0000
0x0000000002498700 winlogon.exe        608    368 0x07940060 2012-07-22 02:42:32 UTC+0000
0x00000000024a0598 csrss.exe           584    368 0x07940040 2012-07-22 02:42:32 UTC+0000
0x00000000024f1020 smss.exe            368      4 0x07940020 2012-07-22 02:42:31 UTC+0000
0x00000000025001d0 svchost.exe        1004    652 0x07940100 2012-07-22 02:42:33 UTC+0000
0x0000000002511360 svchost.exe         824    652 0x079400c0 2012-07-22 02:42:33 UTC+0000
0x00000000025c89c8 System                4      0 0x002fe000
```

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



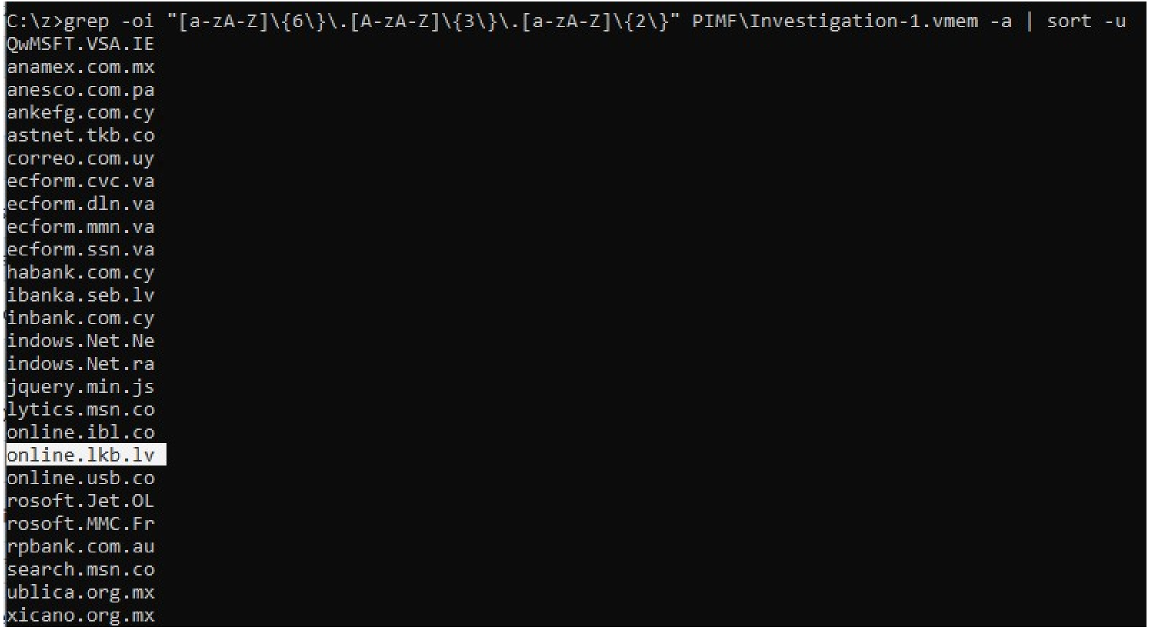
```
C:\z>volatility_2.6_win64_standalone.exe -f PIMF\Investigation-1.vmem --profile=WinXPSP2x86 pstree
Volatility Foundation Volatility Framework 2.6
Name                                                  Pid   PPid   Thds   Hnds Time
-------------------------------------------------- ------ ------ ------ ------ ----
 0x823c89c8:System                                      4      0     53    240 1970-01-01 00:00:00 UTC+0000
. 0x822f1020:smss.exe                                 368      4      3     19 2012-07-22 02:42:31 UTC+0000
.. 0x82298700:winlogon.exe                            608    368     23    519 2012-07-22 02:42:32 UTC+0000
... 0x81e2ab28:services.exe                           652    608     16    243 2012-07-22 02:42:32 UTC+0000
.... 0x821dfda0:svchost.exe                          1056    652      5     60 2012-07-22 02:42:33 UTC+0000
.... 0x81eb17b8:spoolsv.exe                          1512    652     14    113 2012-07-22 02:42:36 UTC+0000
.... 0x81e29ab8:svchost.exe                           908    652      9    226 2012-07-22 02:42:33 UTC+0000
.... 0x823001d0:svchost.exe                          1004    652     64   1118 2012-07-22 02:42:33 UTC+0000
..... 0x8205bda0:wuauclt.exe                         1588   1004      5    132 2012-07-22 02:44:01 UTC+0000
..... 0x821fcda0:wuauclt.exe                         1136   1004      8    173 2012-07-22 02:43:46 UTC+0000
.... 0x82311360:svchost.exe                           824    652     20    194 2012-07-22 02:42:33 UTC+0000
.... 0x820e8da0:alg.exe                               788    652      7    104 2012-07-22 02:43:01 UTC+0000
.... 0x82295650:svchost.exe                          1220    652     15    197 2012-07-22 02:42:35 UTC+0000
... 0x81e2a3b8:lsass.exe                              664    608     24    330 2012-07-22 02:42:32 UTC+0000
.. 0x822a0598:csrss.exe                               584    368      9    326 2012-07-22 02:42:32 UTC+0000
 0x821dea70:explorer.exe                             1484   1464     17    415 2012-07-22 02:42:36 UTC+0000
. 0x81e7bda0:reader_sl.exe                           1640   1484      5     39 2012-07-22 02:42:36 UTC+0000
```

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



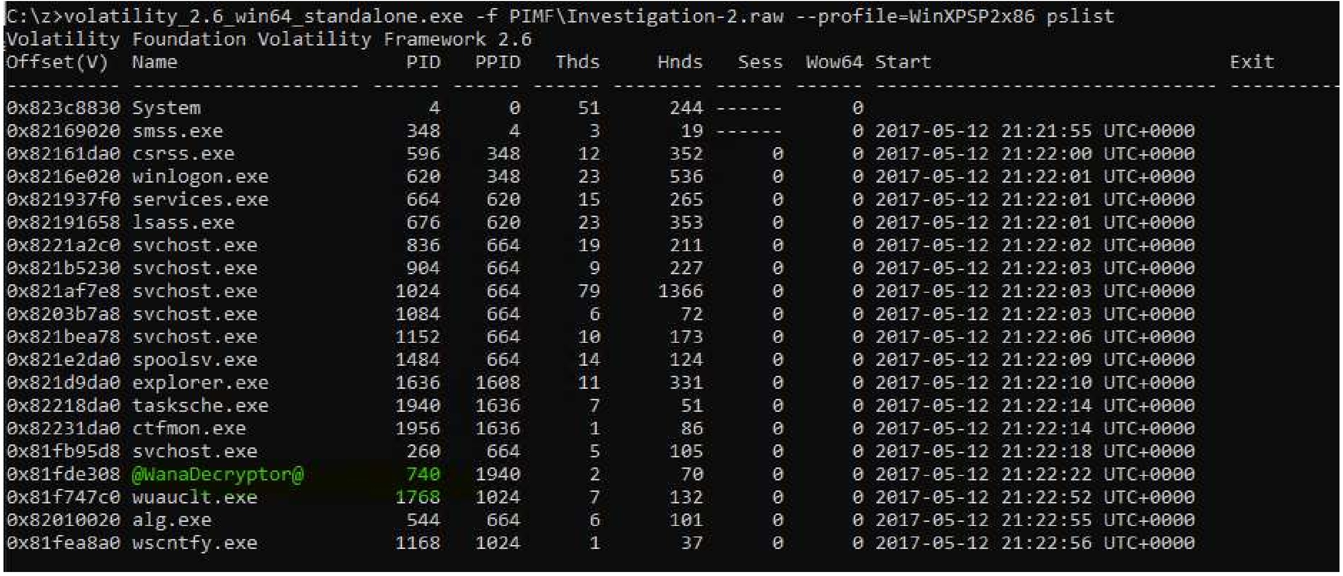
```
C:\z>grep -i user-agent PIMF\Investigation-1.vmem -a
User-Agent: Mozilla/5.0 (Windows; U; MSIE 7.0; Windows NT 6.0; en-US)
User-Agent: RPC
User-Agent: RPC
User-Agent: Mozilla/5.0 (Windows; U; MSIE 7.0; Windows NT 6.0; en-US)
□□⌂O| ↕Lw‼□□G?□►↕Lw♀□og|□↕Lw♫□□□@vPassportConfig□PassportURLs□□□Authenti
orizationMax-Forwards□□□If-Unmodified-SinceIf-Range□□□If-None-Match□□If-
W-Authenticate□□□User-Agent□Title□□Server□Retry-AfterRefererOrig-Uri□□□L
♫►!D) ◄30C♂♣A☻#♠▼21N→*+♦☺↕○↑B↔□E►□D♥♥PS□u□□□□§□□□□G♀►○□B▲☻j☻hH↕Lw□□□□□□□
o#w○□□b□□□□b□□□□□☻P□§|↕□□□□□□□□□□□□□□♦☺□□)▲w□▬h□)▲w□□□□□□P□§T↕□□t-□□□□□□P
w□▼□♠< t♦<      u♥F□□h□↑▼wV□§□‼□□t↓□□□□□□WP□♥□☺□□□□○□□☺□â□♠< t♦<
□♥□□b↔□□□□□□□□□□□□□□□□□□□□□□□t♫□8#u♥□_@□8u□□□□□□□□♦□♠□□tP□§□↕S□□□□□□P□□H□
□□□Y□□h□□□txtbinary3□□□n□□□UJ♥□□○□□□□□☺;□□□□□□☺○□▲q□□□@►☺□↕q□□□□□□□□♦□‼c
□□□□□☺□□○□□q□□□□□3□□□PV□§T↕□□○□sq□□□□□☺□§d↕□□□☺□□□Wq□□□□□□□□□f□?□□□□□□□□
☻►TRANSLATE:□□□□□□□□□□Translate:'□‼_□□□□□♂☻►USER-AGENT:□□□□□□□□□□□User-A
LOW:□□□□□□Allow:
 |□]□p□]□       ►☺d□]□   ☺X□]□♂@☺L□]□   ☺☺@□]□  ☻☺☺□]□♀♦☺ s-queuename s-
method cs-version cs-username s-port s-ip c-port c-ip s-computername s-s
\□□□□□'□\□5□\□□□□□□□\□□□\□HTTP/1.1 304 Not Modified
GETPOSTHTTP/1.0HTTP/1.1multipart/form-databoundary=name="HostRefererUser
♦□☺♦☺Control Count□□□□v♦□♣♦☺SourceId□□□□vk♠♦□0□□□□□04□04□04↑14X14□□□□vk
GETPOSTHTTP/1.0HTTP/1.1multipart/form-databoundary=name="HostRefererUser
jV□s¶□S□□□□□C¶u♦□c♦□□C♀□□~      +□□□□□□C♀□C♦☺u♦□□t!j♦□□□□□□Pj)□□□□□□□□□□

C:\z>D
```

What is the last suspicious bank domain found in Case 001?



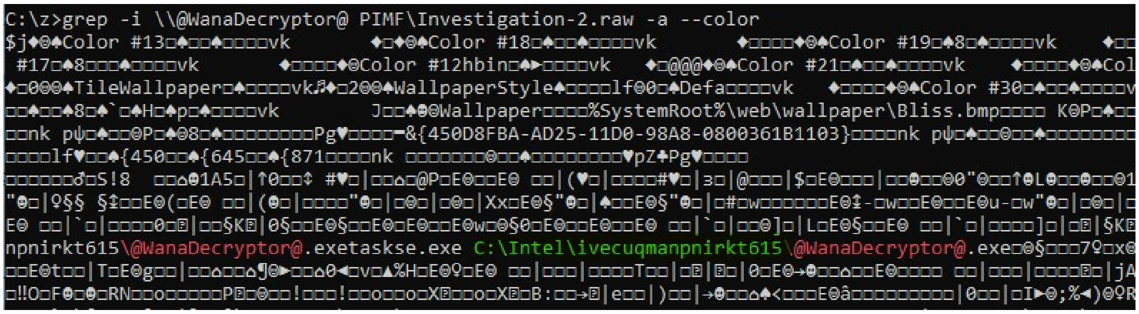
```
C:\z>grep -oi "[a-zA-Z]\{6\}\.[A-zA-Z]\{3\}\.[a-zA-Z]\{2\}" PIMF\Investigation-1.vmem -a | sort -u
QwMSFT.VSA.IE
anamex.com.mx
anesco.com.pa
ankefg.com.cy
astnet.tkb.co
correo.com.uy
ecform.cvc.va
ecform.dln.va
ecform.mmn.va
ecform.ssn.va
habank.com.cy
ibanka.seb.lv
inbank.com.cy
indows.Net.Ne
indows.Net.ra
jquery.min.js
lytics.msn.co
online.ibl.co
online.lkb.lv
online.usb.co
rosoft.Jet.OL
rosoft.MMC.Fr
rpbank.com.au
search.msn.co
ublica.org.mx
xicano.org.mx
```

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



```
C:\z>volatility_2.6_win64_standalone.exe -f PIMF\Investigation-2.raw --profile=WinXPSP2x86 pslist
Volatility Foundation Volatility Framework 2.6
Offset(V)  Name                    PID   PPID   Thds     Hnds   Sess  Wow64 Start                          Exit
---------- -------------------- ------ ------ ------ -------- ------ ------ ------------------------------ ---------
0x823c8830 System                    4      0     51      244 ------      0
0x82169020 smss.exe                348      4      3       19 ------      0 2017-05-12 21:21:55 UTC+0000
0x82161da0 csrss.exe               596    348     12      352      0      0 2017-05-12 21:22:00 UTC+0000
0x8216e020 winlogon.exe            620    348     23      536      0      0 2017-05-12 21:22:01 UTC+0000
0x821937f0 services.exe            664    620     15      265      0      0 2017-05-12 21:22:01 UTC+0000
0x82191658 lsass.exe               676    620     23      353      0      0 2017-05-12 21:22:01 UTC+0000
0x8221a2c0 svchost.exe             836    664     19      211      0      0 2017-05-12 21:22:02 UTC+0000
0x821b5230 svchost.exe             904    664      9      227      0      0 2017-05-12 21:22:03 UTC+0000
0x821af7e8 svchost.exe            1024    664     79     1366      0      0 2017-05-12 21:22:03 UTC+0000
0x8203b7a8 svchost.exe            1084    664      6       72      0      0 2017-05-12 21:22:03 UTC+0000
0x821bea78 svchost.exe            1152    664     10      173      0      0 2017-05-12 21:22:06 UTC+0000
0x821e2da0 spoolsv.exe            1484    664     14      124      0      0 2017-05-12 21:22:09 UTC+0000
0x821d9da0 explorer.exe           1636   1608     11      331      0      0 2017-05-12 21:22:10 UTC+0000
0x82218da0 tasksche.exe           1940   1636      7       51      0      0 2017-05-12 21:22:14 UTC+0000
0x82231da0 ctfmon.exe             1956   1636      1       86      0      0 2017-05-12 21:22:14 UTC+0000
0x81fb95d8 svchost.exe             260    664      5      105      0      0 2017-05-12 21:22:18 UTC+0000
0x81fde308 @WanaDecryptor@         740   1940      2       70      0      0 2017-05-12 21:22:22 UTC+0000
0x81f747c0 wuauclt.exe            1768   1024      7      132      0      0 2017-05-12 21:22:52 UTC+0000
0x82010020 alg.exe                 544    664      6      101      0      0 2017-05-12 21:22:55 UTC+0000
0x81fea8a0 wscntfy.exe            1168   1024      1       37      0      0 2017-05-12 21:22:56 UTC+0000
```

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



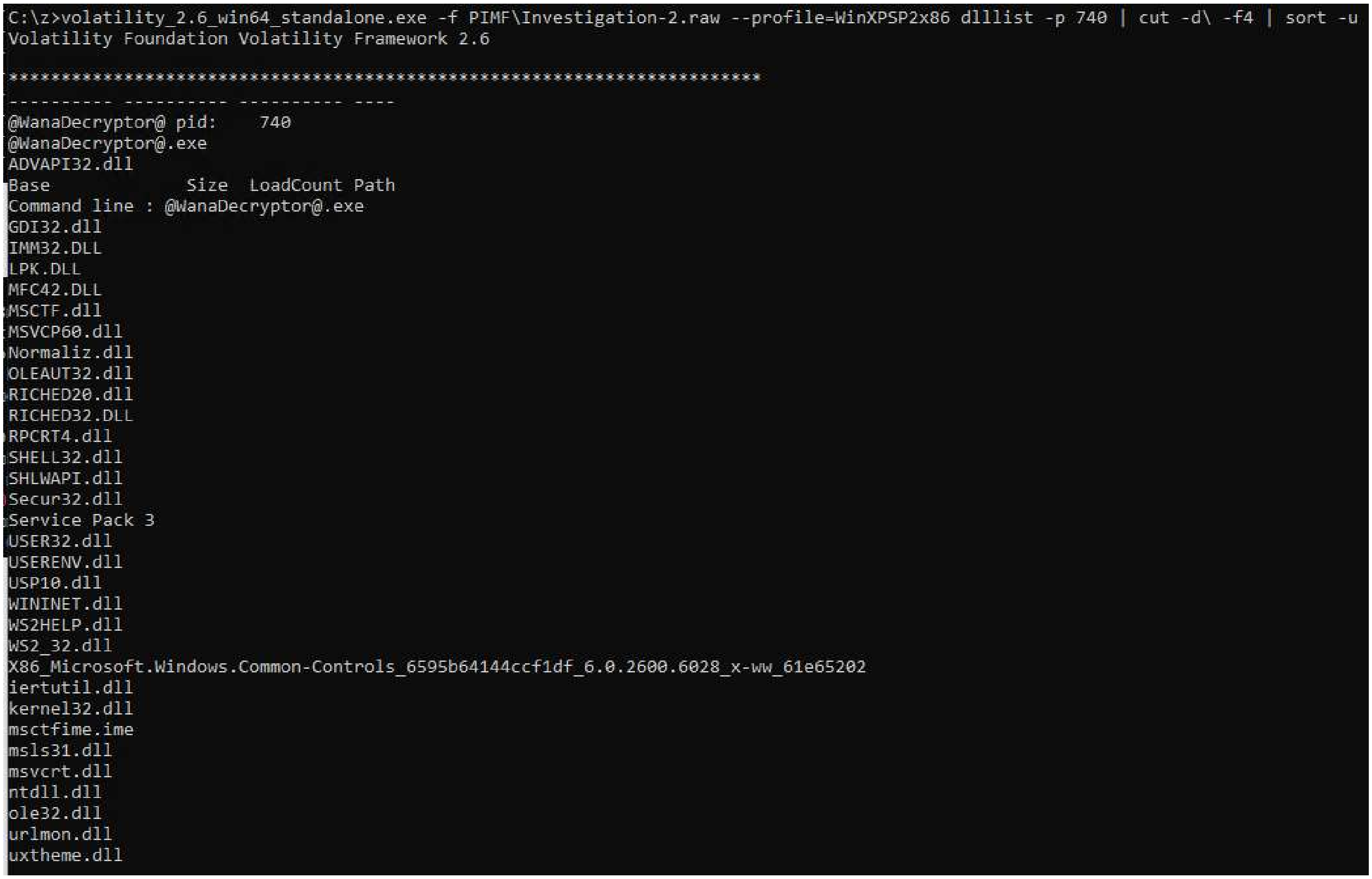
```
C:\z>grep -i \\@WanaDecryptor@ PIMF\Investigation-2.raw -a --color
$j♦☻♠Color #13□♠□□♠□□□□vk       ♦□♦☻♠Color #18□♠□□♠□□□□vk       ♦□□□□♦☻♠Color #19□♠8□♠□□□□vk     ♦□□
 #17□♠8□□□♠□□□□vk       ♦□□□□♦☻Color #12hbin□♠►□□□□vk    ♦□@@@♦☻♠Color #21□♠□□♠□□□□vk     ♦□□□□♦☻♠Col
♦□0☻☻♠TileWallpaper□♠□□□□vk♫♦□2☻☻♠WallpaperStyle♠□□□□lf☻0□♠Defa□□□□vk   ♦□□□□♦☻♠Color #30□♠□□♠□□□□v
□□♠□□♠8□♠`□♠H□♠p□♠□□□□vk        J□□♠☻☻Wallpaper□□□□%SystemRoot%\web\wallpaper\Bliss.bmp□□□□ K☻P□♠□□
□□nk pψ□♠□□☻P□♠☻8□♠□□□□□□□□Pg♥□□□□━&{450D8FBA-AD25-11D0-98A8-0800361B1103}□□□□nk pψ□♠□□☻□□♠□□□□□□□□
□□□□lf♥□□♠{450□□♠{645□□♠{871□□□□nk □□□□□□□☻□□♠□□□□□□□□♥pZ♣Pg♥□□□□
□□□□□□♂□S!8  □□⌂☻1A5□|↑0□□↕ #♥□|□□⌂□@P□E☻□□E☻ □□|(♥□|□□□□#♥□|з□|@□□□|$□E☻□□□|□□☻□□☻0"☻□□↑☻L☻□□☻□□☻1
"☻□|♀§§ §↨□□E☻(□E☻ □□|(☻□|□□□□"☻□|□☻□|□☻□|Xx□E☻§"☻□|♠□□E☻§"☻□|□#□w□□□□□□E☻↨-□w□□E☻□□E☻u-□w"☻□|□☻□|□
E☻ □□|`□|□□□□0□▣|□□§K▣|0§□□E☻§□□E☻□E☻□□E☻w□☻§0□E☻□□E☻□□E☻ □□|`□|□□☻]□|L□E☻§□□E☻ □□|`□|□□□□]□|□▣|§K▣
npnirkt615\@WanaDecryptor@.exetaskse.exe C:\Intel\ivecuqmanpnirkt615\@WanaDecryptor@.exe□☻§□□□7♀□x☻
□□E☻t□□|T□E☻g□□|□□⌂□□□⌂¶☻►□□⌂0◄□v□▲%H□E☻♀□E☻ □□|□□□|□□□□T□□|□▣|▣□|0□E☻→☻□□⌂□□E☻□□□□ □□|□□□|□□□□▣□|jA
□‼O□F☻□☻□RN□□o□□□□□P▣□☻□□!□□□!□□o□□□o□X▣□□□o□X▣□B:□□→▣|e□□|)□□|→☻□□⌂♠<□□□E☻â□□□□□□□□□□|0□□|□I►☻;%◄)☻♀R
```

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

What is the suspicious parent process PID connected to the decryptor in Case 002?
1940

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

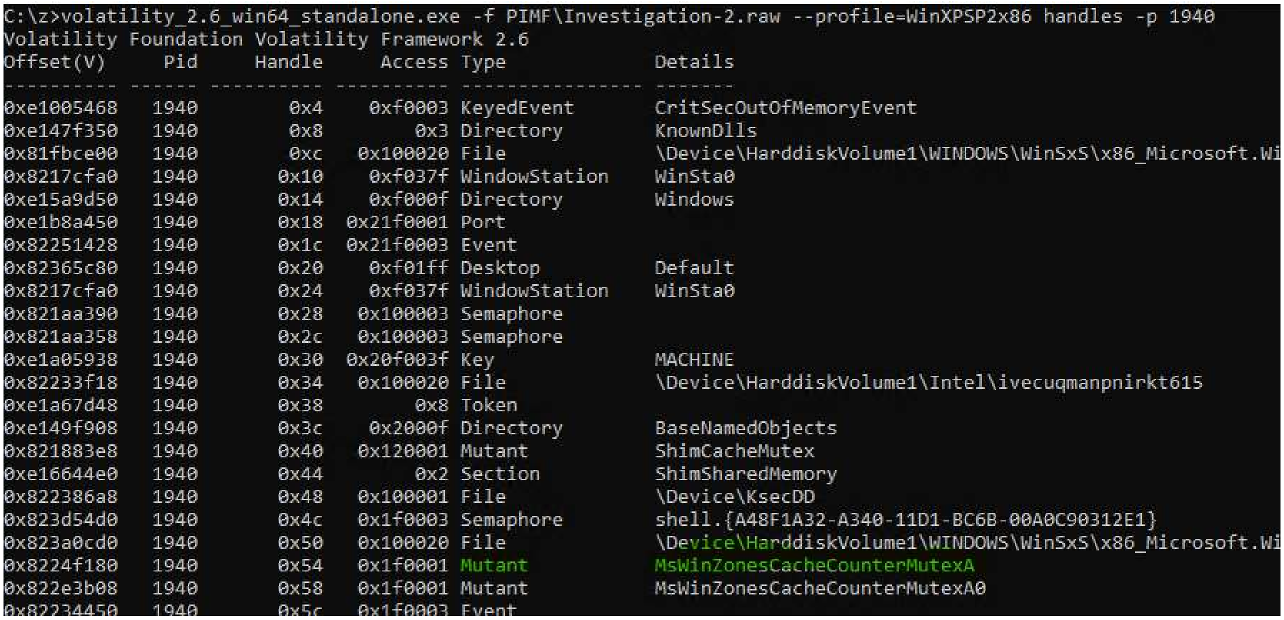
What DLL is loaded by the decryptor used for socket creation in Case 002?



```
C:\z>volatility_2.6_win64_standalone.exe -f PIMF\Investigation-2.raw --profile=WinXPSP2x86 dlllist -p 740 | cut -d\ -f4 | sort -u
Volatility Foundation Volatility Framework 2.6

************************************************************************
---------- ---------- ---------- ----
@WanaDecryptor@ pid:    740
@WanaDecryptor@.exe
ADVAPI32.dll
Base             Size  LoadCount Path
Command line : @WanaDecryptor@.exe
GDI32.dll
IMM32.DLL
LPK.DLL
MFC42.DLL
MSCTF.dll
MSVCP60.dll
Normaliz.dll
OLEAUT32.dll
RICHED20.dll
RICHED32.DLL
RPCRT4.dll
SHELL32.dll
SHLWAPI.dll
Secur32.dll
Service Pack 3
USER32.dll
USERENV.dll
USP10.dll
WININET.dll
WS2HELP.dll
WS2_32.dll
X86_Microsoft.Windows.Common-Controls_6595b64144ccf1df_6.0.2600.6028_x-ww_61e65202
iertutil.dll
kernel32.dll
msctfime.ime
msls31.dll
msvcrt.dll
ntdll.dll
ole32.dll
urlmon.dll
uxtheme.dll
```

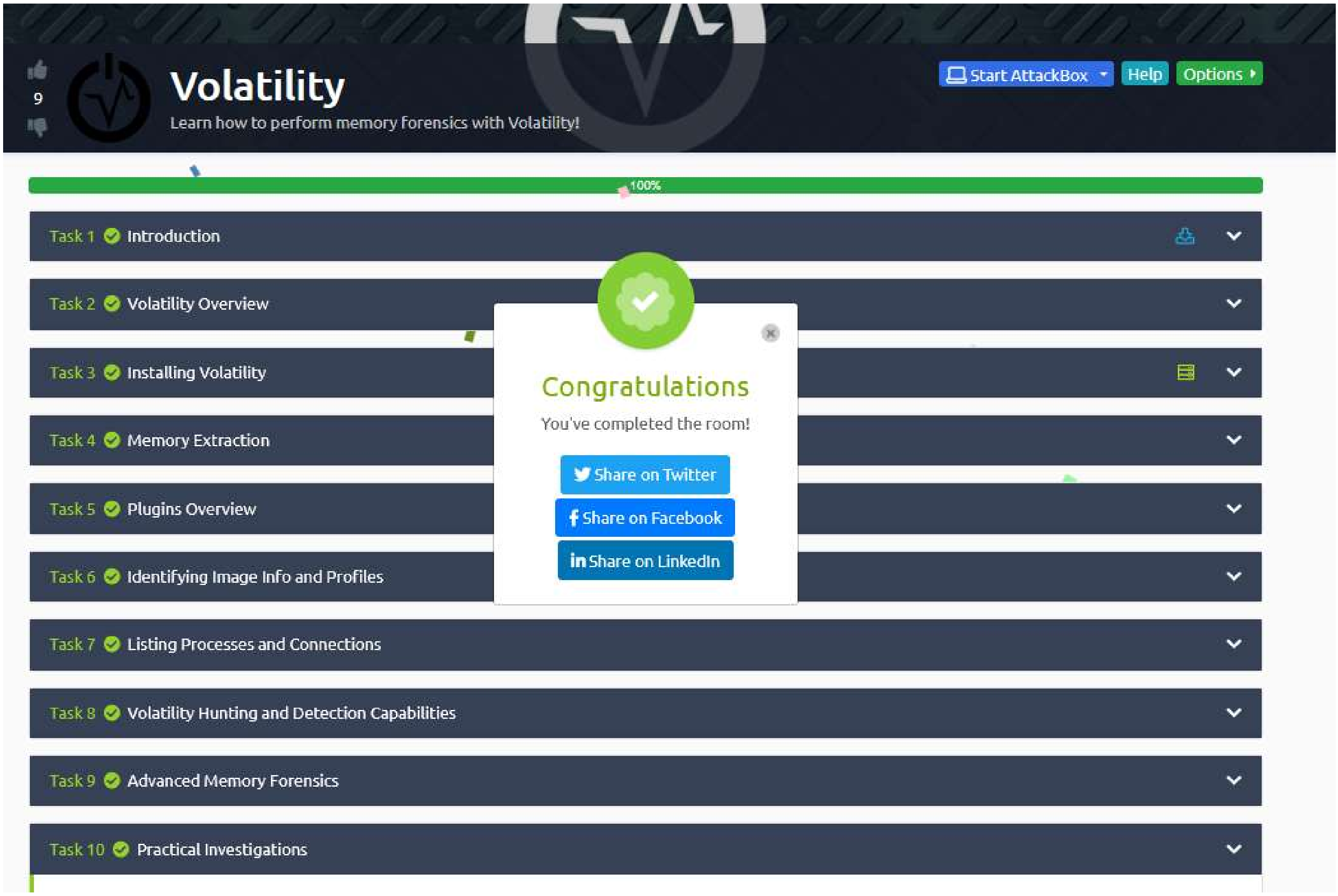
WS2_32.dll

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



```
C:\z>volatility_2.6_win64_standalone.exe -f PIMF\Investigation-2.raw --profile=WinXPSP2x86 handles -p 1940
Volatility Foundation Volatility Framework 2.6
Offset(V)     Pid     Handle     Access Type             Details
---------- ------ ---------- ---------- ---------------- -------
0xe1005468   1940        0x4    0xf0003 KeyedEvent       CritSecOutOfMemoryEvent
0xe147f350   1940        0x8        0x3 Directory        KnownDlls
0x81fbce00   1940        0xc   0x100020 File             \Device\HarddiskVolume1\WINDOWS\WinSxS\x86_Microsoft.Wi
0x8217cfa0   1940       0x10    0xf037f WindowStation    WinSta0
0xe15a9d50   1940       0x14    0xf000f Directory        Windows
0xe1b8a450   1940       0x18  0x21f0001 Port
0x82251428   1940       0x1c  0x21f0003 Event
0x82365c80   1940       0x20    0xf01ff Desktop          Default
0x8217cfa0   1940       0x24    0xf037f WindowStation    WinSta0
0x821aa390   1940       0x28   0x100003 Semaphore
0x821aa358   1940       0x2c   0x100003 Semaphore
0xe1a05938   1940       0x30  0x20f003f Key              MACHINE
0x82233f18   1940       0x34   0x100020 File             \Device\HarddiskVolume1\Intel\ivecuqmanpnirkt615
0xe1a67d48   1940       0x38        0x8 Token
0xe149f908   1940       0x3c    0x2000f Directory        BaseNamedObjects
0x821883e8   1940       0x40   0x120001 Mutant           ShimCacheMutex
0xe16644e0   1940       0x44        0x2 Section          ShimSharedMemory
0x822386a8   1940       0x48   0x100001 File             \Device\KsecDD
0x823d54d0   1940       0x4c   0x1f0003 Semaphore        shell.{A48F1A32-A340-11D1-BC6B-00A0C90312E1}
0x823a0cd0   1940       0x50   0x100020 File             \Device\HarddiskVolume1\WINDOWS\WinSxS\x86_Microsoft.Wi
0x8224f180   1940       0x54   0x1f0001 Mutant           MsWinZonesCacheCounterMutexA
0x822e3b08   1940       0x58   0x1f0001 Mutant           MsWinZonesCacheCounterMutexA0
0x82234450   1940       0x5c   0x1f0003 Event
```

What plugin could be used to identify all files loaded from the malware working directory in Case 002?
(reading the documentation)
windows.filescan



9

Volatility

Learn how to perform memory forensics with Volatility!

Start AttackBox | Help | Options

100%

Task 1 ✓ Introduction

Task 2 ✓ Volatility Overview

Task 3 ✓ Installing Volatility

Task 4 ✓ Memory Extraction

Task 5 ✓ Plugins Overview

Task 6 ✓ Identifying Image Info and Profiles

Task 7 ✓ Listing Processes and Connections

Task 8 ✓ Volatility Hunting and Detection Capabilities

Task 9 ✓ Advanced Memory Forensics

Task 10 ✓ Practical Investigations

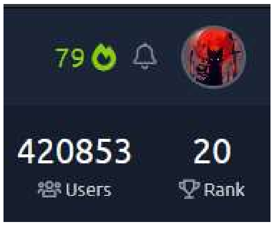
Congratulations

You've completed the room!

Share on Twitter

Share on Facebook

Share on LinkedIn



79

420853	20
Users	Rank