

Kelompok:

2501981270 - AGUSTINUS LEONARDO DWITAMA

2501989550 - MUHAMAD DWI APRIYANTO

2502001864 - RAVI DEEVAN SATYAKI

2501965052 - KEVIN MORRIS ARMANDO

2501983723 - NATANAEL FRANSISCO

Shylock via Volatility

Image Analysis

```
D:\DEEVAN\SEMESTER 5\Computer Forensic\volatility_2.6_win64_standalone\volatility_2.6_win64_standalone>.\volatility_2.6_win64_standalone.exe imageinfo -f shylock.vmem
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 (D:\DEEVAN\SEMESTER 5\Computer Forensic\volatility_2.6_win64_standalone\volatility_2.6_win64_standalone\shylock.vmem)
      PAE type : PAE
      DTB : 0x319000L
      KDBG : 0x80545b60L
      Number of Processors : 1
      Image Type (Service Pack) : 3
      KPCR for CPU 0 : 0xffdf000L
      KUSER_SHARED_DATA : 0xffdf000L
      Image date and time : 2011-09-30 00:26:30 UTC+0000
      Image local date and time : 2011-09-29 20:26:30 -0400
```

We have a Windows XP with ServicePack 2 on x86 environment.

Process Analysis

```
D:\DEEVAN\SEMESTER 5\Computer Forensic\volatility_2.6_win64_standalone\volatility_2.6_win64_standalone>.\volatility_2.6_win64_standalone.exe pslist -f shylock.vmem
Volatility Foundation Volatility Framework 2.6
Offset(V)  Name                PID  PPID  Thds  Hnds  Sess  Wom64  Start                Exit
-----
0x819cc830 System                4    0     60   209  -----  0
0x818efda0 smss.exe             384    4     3    19  -----  0 2011-09-26 01:33:32 UTC+0000
0x81616ab8 csrss.exe            612   384    12   473    0  0 2011-09-26 01:33:35 UTC+0000
0x814c9b40 winlogon.exe         636   384    16   498    0  0 2011-09-26 01:33:35 UTC+0000
0x81794d08 services.exe    680   636    15   271    0  0 2011-09-26 01:33:35 UTC+0000
0x814a2c00 lsass.exe      692   636    24   356    0  0 2011-09-26 01:33:35 UTC+0000
0x815c2630 vmacthlp.exe    852   680     1    25    0  0 2011-09-26 01:33:35 UTC+0000
0x81470020 svchost.exe     868   680    17   199    0  0 2011-09-26 01:33:35 UTC+0000
0x818b5248 svchost.exe     944   680    11   274    0  0 2011-09-26 01:33:36 UTC+0000
0x813a0458 MsMpEng.exe   1040   680    16   322    0  0 2011-09-26 01:33:36 UTC+0000
0x816b7020 svchost.exe    1076   680    87  1477    0  0 2011-09-26 01:33:36 UTC+0000
0x817f7548 svchost.exe    1200   680     6    81    0  0 2011-09-26 01:33:37 UTC+0000
0x8169a1d0 svchost.exe    1336   680    14   172    0  0 2011-09-26 01:33:37 UTC+0000
0x813685e0 spoolsv.exe    1516   680    14   159    0  0 2011-09-26 01:33:39 UTC+0000
0x818f5cd0 explorer.exe    1752  1696    32   680    0  0 2011-09-26 01:33:45 UTC+0000
0x815c9638 svchost.exe    1812   680     4   102    0  0 2011-09-26 01:33:46 UTC+0000
0x8192d7f0 VMwareTray.exe    1876  1752     3    84    0  0 2011-09-26 01:33:46 UTC+0000
0x818f6458 VMwareUser.exe 1888  1752     9   245    0  0 2011-09-26 01:33:47 UTC+0000
0x8164a020 mssecex.exe    1900  1752    11   205    0  0 2011-09-26 01:33:47 UTC+0000
0x81717370 ctfmon.exe        1912  1752     3    93    0  0 2011-09-26 01:33:47 UTC+0000
0x813a5b28 svchost.exe    2000   680     6   119    0  0 2011-09-26 01:33:47 UTC+0000
0x81336b28 vmtoolsd.exe     200   680     5   234    0  0 2011-09-26 01:33:47 UTC+0000
0x81329b28 VMUpgradeHelper 424   680     5   100    0  0 2011-09-26 01:33:48 UTC+0000
0x812d6020 wscntfy.exe       2028  1076     3    63    0  0 2011-09-26 01:33:55 UTC+0000
0x812c1718 TPAutoConnSvc.e 2068   680     5    99    0  0 2011-09-26 01:33:55 UTC+0000
0x812b03e0 alg.exe      2272   680     7   112    0  0 2011-09-26 01:33:55 UTC+0000
0x81324020 TPAutoConnect.e 3372  2068     3    90    0  0 2011-09-26 01:33:59 UTC+0000
0x814e7b38 msixexec.exe  2396   680     5   127    0  0 2011-09-26 01:34:45 UTC+0000
0x814db608 cmd.exe         3756  1752     3    56    0  0 2011-09-30 00:20:44 UTC+0000
0x812f59a8 cmd.exe         3128   200     0  -----  0  0 2011-09-30 00:26:30 UTC+0000
```

```
D:\DEEVAN\SEMESTER 5\Computer Forensic\volatility_2.6_win64_standalone\volatility_2.6_w
in64_standalone>.\volatility_2.6_win64_standalone.exe connscan -f shylock.vmem
Volatility Foundation Volatility Framework 2.6
Offset(P) Local Address Remote Address Pid
-----
0x014f6ab0 10.0.0.109:1072 209.190.4.84:443 1752
0x01507380 10.0.0.109:1073 209.190.4.84:443 1752
0x016c2b00 10.0.0.109:1065 184.173.252.227:443 1752
0x017028a0 10.0.0.109:1067 184.173.252.227:443 1752
0x01858cb0 10.0.0.109:1068 209.190.4.84:443 1752
```

```
D:\DEEVAN\SEMESTER 5\Computer Forensic\volatility_2.6_win64_standalone\volatility_2.6_win64_standalone>.\volatility_2.6_win64_standalone.exe sockets -f shylock.vmem
Volatility Foundation Volatility Framework 2.6
Offset(V) PID Port Proto Protocol Address Create Time
-----
0x812b15d0 4 0 47 GRE 0.0.0.0 2011-09-26 01:33:56 UTC+0000
0x812a8008 4 1030 6 TCP 0.0.0.0 2011-09-26 01:33:56 UTC+0000
0x813a5728 692 500 17 UDP 0.0.0.0 2011-09-26 01:33:47 UTC+0000
0x812a9b60 2272 1028 6 TCP 127.0.0.1 2011-09-26 01:33:56 UTC+0000
0x814c4008 1752 1073 6 TCP 0.0.0.0 2011-09-30 00:25:39 UTC+0000
0x818a3bf8 4 445 6 TCP 0.0.0.0 2011-09-26 01:33:32 UTC+0000
0x8179e730 944 135 6 TCP 0.0.0.0 2011-09-26 01:33:36 UTC+0000
0x812ade38 1076 1076 17 UDP 127.0.0.1 2011-09-30 00:26:30 UTC+0000
0x813a4e98 1752 1070 6 TCP 0.0.0.0 2011-09-30 00:25:34 UTC+0000
0x816711c8 1076 123 17 UDP 127.0.0.1 2011-09-30 00:26:30 UTC+0000
0x816757d0 692 0 255 Reserved 0.0.0.0 2011-09-26 01:33:47 UTC+0000
0x815bb708 1752 1067 6 TCP 0.0.0.0 2011-09-30 00:25:33 UTC+0000
0x812bb008 1336 1900 17 UDP 127.0.0.1 2011-09-30 00:26:30 UTC+0000
0x81904478 692 4500 17 UDP 0.0.0.0 2011-09-26 01:33:47 UTC+0000
0x814c9008 4 445 17 UDP 0.0.0.0 2011-09-26 01:33:32 UTC+0000
```

```
0x814c4008 1752 1073 6 TCP 0.0.0.0 2011-09-30 00:25:39 UTC+0000
0x813a4e98 1752 1070 6 TCP 0.0.0.0 2011-09-30 00:25:34 UTC+0000
0x815bb708 1752 1067 6 TCP 0.0.0.0 2011-09-30 00:25:33 UTC+0000
```

```
D:\DEEVAN\SEMESTER 5\Computer Forensic\volatility_2.6_win64_standalone\volatility_2.6_win64_standalone>.\volatility_2.6_win64_standalone.exe dlllist -f shylock.vmem -p 1752
Volatility Foundation Volatility Framework 2.6
*****
explorer.exe pid: 1752
Command line : C:\WINDOWS\Explorer.EXE
Service Pack 3

Base Size LoadCount Path
-----
0x01000000 0xffff000 0xfffff C:\WINDOWS\Explorer.EXE
0x7c900000 0xb2000 0xfffff C:\WINDOWS\system32\ntdll.dll
0x7c800000 0xf6000 0xfffff C:\WINDOWS\system32\kernel32.dll
0x77d00000 0x9b000 0xfffff C:\WINDOWS\system32\ADVAPI32.dll
0x77e70000 0x93000 0xfffff C:\WINDOWS\system32\RPCRT4.dll
0x77f80000 0x11000 0xfffff C:\WINDOWS\system32\Secur32.dll
0x775f0000 0xf4000 0xfffff C:\WINDOWS\system32\BROWSEUI.dll
0x77f10000 0x49000 0xfffff C:\WINDOWS\system32\GDI32.dll
0x7e410000 0x91000 0xfffff C:\WINDOWS\system32\USER32.dll
0x77c10000 0x58000 0xfffff C:\WINDOWS\system32\msvcrt.dll
0x774e0000 0x13e000 0xfffff C:\WINDOWS\system32\ole32.dll
0x77f60000 0x76000 0xfffff C:\WINDOWS\system32\SHLWAPI.dll
0x77120000 0x8b000 0xfffff C:\WINDOWS\system32\OLEAUT32.dll
0x7e290000 0x173000 0xfffff C:\WINDOWS\system32\SHDocVW.dll
0x77a00000 0x95000 0xfffff C:\WINDOWS\system32\CRYPT32.dll
0x77b20000 0x12000 0xfffff C:\WINDOWS\system32\MSASN1.dll
0x754d0000 0x80000 0xfffff C:\WINDOWS\system32\CRYPTUI.dll
0x5b860000 0x55000 0xfffff C:\WINDOWS\system32\NETAPI32.dll
0x77c00000 0x8000 0xfffff C:\WINDOWS\system32\VERSION.dll
0x3d930000 0xd1000 0xfffff C:\WINDOWS\system32\WININET.dll
0x00400000 0x9000 0xfffff C:\WINDOWS\system32\Normaliz.dll
0x3df40000 0x45000 0xfffff C:\WINDOWS\system32\iertutil.dll
0x76c00000 0x2e000 0xfffff C:\WINDOWS\system32\WINTRUST.dll
0x76c90000 0x28000 0xfffff C:\WINDOWS\system32\IMAGEHLP.dll
0x76f60000 0x2c000 0xfffff C:\WINDOWS\system32\WLDP32.dll
0x7c9c0000 0x817000 0xfffff C:\WINDOWS\system32\SHELL32.dll
0x5ad70000 0x38000 0xfffff C:\WINDOWS\system32\UxTheme.dll
0x5cb70000 0x26000 0x1 C:\WINDOWS\system32\ShimEng.dll
0x6f880000 0x1ca000 0x1 C:\WINDOWS\AppPatch\AcGenral.DLL
0x76b40000 0x2d000 0x7 C:\WINDOWS\system32\WINMM.dll
0x77b00000 0x15000 0x1 C:\WINDOWS\system32\MSACM32.dll
0x769c0000 0xb4000 0x1c C:\WINDOWS\system32\USERENV.dll
0x76390000 0x1d000 0x5 C:\WINDOWS\system32\IMM32.dll
0x77340000 0x103000 0x22 C:\WINDOWS\WinSxS\x86_Microsoft.Windows.Common-Controls_6595b64144ccf1df_6.0.2600.6028_x-ww_61e65202\comctl32.dll
0x5d090000 0x9a000 0x6 C:\WINDOWS\system32\comctl32.dll
0x755c0000 0x2e000 0x2 C:\WINDOWS\system32\msctfime.ime
0x77b40000 0x22000 0x4 C:\WINDOWS\system32\apphelp.dll
0x76fd0000 0x7f000 0x2 C:\WINDOWS\system32\CLBCATQ.DLL
0x77050000 0xc5000 0x2 C:\WINDOWS\system32\CORRES.dll
0x10000000 0x17000 0x4 C:\Documents and Settings\Administrator\Application Data\Dropbox\bin\DropboxExt.13.dll
```

```
0x4d4f0000 0x59000 0xd C:\WINDOWS\system32\WINHTTP.dll
0x76f20000 0x27000 0x3 C:\WINDOWS\system32\DNSAPI.dll
0x75e60000 0x13000 0xb C:\WINDOWS\system32\cryptnet.dll
```

0x662b0000 0x58000 0x2 C:\WINDOWS\system32\hnetcfg.dll
0x71a90000 0x8000 0x1 C:\WINDOWS\System32\wshtcpip.dll

```
C:\Users\Natan\Downloads\Compressed\volatility_2.6_win64_standalone>volatility_2.6_win64_standalone.exe -f shylock.vmem -p 1752 malfind -D ./
Volatility Foundation Volatility Framework 2.6
Process: explorer.exe Pid: 1752 Address: 0x3380000
Vad Tag: VadS Protection: PAGE_EXECUTE_READWRITE
Flags: CommitCharge: 151, MemCommit: 1, PrivateMemory: 1, Protection: 6

0x03380000 4d 5a 90 00 03 00 00 00 04 00 00 00 ff ff 00 00 MZ.....
0x03380010 b8 00 00 00 00 00 00 00 40 00 00 00 00 00 00 00 .....@.....
0x03380020 00 00 00 00 00 00 00 00 00 00 00 00 e4 02 00 20 .....
0x03380030 00 00 00 00 00 00 00 00 00 00 00 00 00 01 00 00 .....



0x03380000 4d          DEC EBP
0x03380001 5a          POP EDX
0x03380002 90          NOP
0x03380003 0003        ADD [EBX], AL
0x03380005 0000        ADD [EAX], AL
0x03380007 000400     ADD [EAX+EAX], AL
0x0338000a 0000        ADD [EAX], AL
0x0338000c ff         DB 0xff
0x0338000d fff0     INC DWORD [EAX]
0x0338000f 00b800000000 ADD [EAX+0x0], BH
0x03380015 0000        ADD [EAX], AL
0x03380017 004000     ADD [EAX+0x0], AL
0x0338001a 0000        ADD [EAX], AL
0x0338001c 0000        ADD [EAX], AL
0x0338001e 0000        ADD [EAX], AL
0x03380020 0000        ADD [EAX], AL
0x03380022 0000        ADD [EAX], AL
0x03380024 0000        ADD [EAX], AL
0x03380026 0000        ADD [EAX], AL
0x03380028 0000        ADD [EAX], AL
0x0338002a e402     IN AL, 0x2
0x0338002c 0020        ADD [EAX], AH
0x0338002e 0900        OR [EAX], EAX
0x03380030 0000        ADD [EAX], AL
0x03380032 0000        ADD [EAX], AL
0x03380034 0000        ADD [EAX], AL
0x03380036 0000        ADD [EAX], AL
0x03380038 0000        ADD [EAX], AL
0x0338003a 0000        ADD [EAX], AL
0x0338003c 0001        ADD [ECX], AL
0x0338003e 0000        ADD [EAX], AL
```

Process: explorer.exe Pid: 1752 Address: 0x36e0000
Vad Tag: VadS Protection: PAGE_EXECUTE_READWRITE
Flags: CommitCharge: 151, MemCommit: 1, PrivateMemory: 1, Protection: 6

```
0x036e0000  4d 5a 90 00 03 00 00 00 04 00 00 00 ff ff 00 00  MZ.....
0x036e0010  b8 00 00 00 00 00 00 00 40 00 00 00 00 00 00 00  .....@.....
0x036e0020  00 00 00 00 00 00 00 00 00 00 56 03 00 20 09 00  .....V.....
0x036e0030  00 00 00 00 00 00 00 00 00 00 00 00 00 01 00 00  .....
```

```
0x036e0000  4d          DEC EBP
0x036e0001  5a          POP EDX
0x036e0002  90          NOP
0x036e0003  0003        ADD [EBX], AL
0x036e0005  0000        ADD [EAX], AL
0x036e0007  000400      ADD [EAX+EAX], AL
0x036e000a  0000        ADD [EAX], AL
0x036e000c  ff          DB 0xff
0x036e000d  ff00        INC DWORD [EAX]
0x036e000f  00b800000000 ADD [EAX+0x0], BH
0x036e0015  0000        ADD [EAX], AL
0x036e0017  004000      ADD [EAX+0x0], AL
0x036e001a  0000        ADD [EAX], AL
0x036e001c  0000        ADD [EAX], AL
0x036e001e  0000        ADD [EAX], AL
0x036e0020  0000        ADD [EAX], AL
0x036e0022  0000        ADD [EAX], AL
0x036e0024  0000        ADD [EAX], AL
0x036e0026  0000        ADD [EAX], AL
0x036e0028  0000        ADD [EAX], AL
0x036e002a  56          PUSH ESI
0x036e002b  0300        ADD EAX, [EAX]
0x036e002d  2009        AND [ECX], CL
0x036e002f  0000        ADD [EAX], AL
0x036e0031  0000        ADD [EAX], AL
0x036e0033  0000        ADD [EAX], AL
0x036e0035  0000        ADD [EAX], AL
0x036e0037  0000        ADD [EAX], AL
0x036e0039  0000        ADD [EAX], AL
0x036e003b  0000        ADD [EAX], AL
0x036e003d  0100        ADD [EAX], EAX
0x036e003f  00          DB 0x0
```

▼ Today

 process.0x818f5cd0.0x36e0000.dmp	12/2/2023 6:40 PM	DMP File	604 KB
 process.0x818f5cd0.0x3380000.dmp	12/2/2023 6:40 PM	DMP File	604 KB


```
2003 NSPR4.DLL not found Inst.strNSPR4=%s
2004 |$$$}rstuvwxyz{$$$$$$>?@ABCDEFGHIJKLMNPQRSTUVWXYZ[\]^_`abcdefghijklmnopqrstuvwxyz
2005 IE_Hook::GetReplayInfo entry
2006 DIE_Hook::GetReplayInfo exit
2007 IE::Config=%s
2008 EMPTY
2009 IE::ReqFindRequest FOUND hOpenRequest=%08X m_hRequestFake=%d m_isBotInfo=%d m_isInject=%d m_isContentTextXml=%d
2010 IE::InternetReadFile (NATIVE) hOpenRequest=%08X size=%d
2011 IE::InternetReadFile (NATIVE) hOpenRequest=%08X size=%d domain=%s request=%s%s
2012 IE::InternetReadFileExA (NATIVE) hOpenRequest=%08X
2013 IE::InternetReadFileExA (NATIVE) hOpenRequest=%08X domain=%s request=%s%s
2014 IE::InternetReadFileExW (NATIVE) hOpenRequest=%08X
2015 IE::InternetReadFileExW (NATIVE) hOpenRequest=%08X domain=%s request=%s%s
2016 IE::InternetReadFile1() hOpenRequest=%08X domain=%s request=%s%s
2017 ERROR_IO_PENDING hOpenRequest=%08X timeout=%d
2018 ***ERROR::InternetQueryDataAvailable() GetLastError()=%d hOpenRequest=%08X dwSize=%d timeout=%d
2019 domain=%s request=%s%s
```

VAD node @ 0x81805108 Start 0x032c0000 End 0x032fffff Tag VadS
Flags: CommitCharge: 15, PrivateMemory: 1, Protection: 4
Protection: PAGE_READWRITE

VAD node @ 0x81623e58 Start 0x03380000 End 0x03416fff Tag VadS
Flags: CommitCharge: 151, MemCommit: 1, PrivateMemory: 1, Protection: 6
Protection: PAGE_EXECUTE_READWRITE

VAD node @ 0x817ad558 Start 0x03880000 End 0x038bffff Tag VadS
Flags: CommitCharge: 15, PrivateMemory: 1, Protection: 4
Protection: PAGE_READWRITE

VAD node @ 0x8150c728 Start 0x036e0000 End 0x03776fff Tag VadS
Flags: CommitCharge: 151, MemCommit: 1, PrivateMemory: 1, Protection: 6
Protection: PAGE_EXECUTE_READWRITE

VAD node @ 0x81780420 Start 0x03560000 End 0x035f1fff Tag VadS
Flags: CommitCharge: 146, MemCommit: 1, PrivateMemory: 1, Protection: 4
Protection: PAGE_READWRITE

```
C:\Windows\System32\cmd.e  X  +  v

C:\Users\natan\Downloads\Compressed\volatility_2.6_win64_standalone>volatility_2.6_win64_standalone.exe -f shylock.vmem -p 1752 apihooks
Volatility Foundation Volatility Framework 2.6
*****
Hook mode: Usermode
Hook type: Import Address Table (IAT)
Process: 1752 (explorer.exe)
Victim module: Explorer.EXE (0x1000000 - 0x10ff000)
Function: kernel32.dll!CreateProcessW
Hook address: 0x339e325
Hooking module: <unknown>

Disassembly(0):
0x339e325 55          PUSH EBP
0x339e326 8bec        MOV EBP, ESP
0x339e328 8b451c      MOV EAX, [EBP+0x1c]
0x339e32b 56          PUSH ESI
0x339e32c 8b752c      MOV ESI, [EBP+0x2c]
0x339e32f 57          PUSH EDI
0x339e330 56          PUSH ESI
0x339e331 ff7528      PUSH DWORD [EBP+0x28]
0x339e334 83c804      OR EAX, 0x4
0x339e337 ff7524      PUSH DWORD [EBP+0x24]
0x339e33a ff7520      PUSH DWORD [EBP+0x20]

*****
Hook mode: Usermode
Hook type: Import Address Table (IAT)
Process: 1752 (explorer.exe)
Victim module: Explorer.EXE (0x1000000 - 0x10ff000)
Function: kernel32.dll!HeapDestroy
Hook address: 0x339e231
Hooking module: <unknown>

Disassembly(0):
0x339e231 55          PUSH EBP
0x339e232 8bec        MOV EBP, ESP
0x339e234 51          PUSH ECX
0x339e235 e8ffa9feff  CALL 0x3388c39
0x339e23a ff7508      PUSH DWORD [EBP+0x8]
0x339e23d ff1548ff4003  CALL DWORD [0x340ff48]
0x339e243 59          POP ECX
0x339e244 5d          POP EBP
0x339e245 c20400      RET 0x4
0x339e248 55          PUSH EBP

*****
Hook mode: Usermode
Hook type: Import Address Table (IAT)
Process: 1752 (explorer.exe)
Victim module: Explorer.EXE (0x1000000 - 0x10ff000)
Function: user32.dll!ExitWindowsEx
Hook address: 0x33adb80
Hooking module: <unknown>

Disassembly(0):
0x33adb80 55          PUSH EBP
0x33adb81 8bec        MOV EBP, ESP
0x33adb83 51          PUSH ECX
0x33adb84 56          PUSH ESI
```

```
C:\Users\natan\Downloads\Compressed\volatility_2.6_win64_standalone>volatility_2.6_win64_standalone.exe -f shylock.vmem --pid 1752 dlldump -D ./
Volatility Foundation Volatility Framework 2.6
```

Process(V)	Name	Module Base	Module Name	Result
0x818f5cd0	explorer.exe	0x001000000	Explorer.EXE	OK: module.1752.1af5cd0.1000000.dll
0x818f5cd0	explorer.exe	0x07c900000	ntdll.dll	OK: module.1752.1af5cd0.7c900000.dll
0x818f5cd0	explorer.exe	0x07c300000	MSVCR71.dll	OK: module.1752.1af5cd0.7c300000.dll
0x818f5cd0	explorer.exe	0x078130000	urlmon.dll	OK: module.1752.1af5cd0.78130000.dll
0x818f5cd0	explorer.exe	0x077f60000	SHLWAPI.dll	OK: module.1752.1af5cd0.77f60000.dll
0x818f5cd0	explorer.exe	0x03dfd0000	iertutil.dll	OK: module.1752.1af5cd0.3dfd0000.dll
0x818f5cd0	explorer.exe	0x0767a0000	NTDSAPI.dll	OK: module.1752.1af5cd0.767a0000.dll
0x818f5cd0	explorer.exe	0x077fe0000	Secur32.dll	OK: module.1752.1af5cd0.77fe0000.dll
0x818f5cd0	explorer.exe	0x0755f0000	netcfgx.dll	OK: module.1752.1af5cd0.755f0000.dll
0x818f5cd0	explorer.exe	0x077c00000	VERSION.dll	OK: module.1752.1af5cd0.77c00000.dll
0x818f5cd0	explorer.exe	0x05f800000	Mp0Av.dll	OK: module.1752.1af5cd0.5f800000.dll
0x818f5cd0	explorer.exe	0x071a50000	mswsock.dll	OK: module.1752.1af5cd0.71a50000.dll
0x818f5cd0	explorer.exe	0x071c80000	NETRAP.dll	OK: module.1752.1af5cd0.71c80000.dll
0x818f5cd0	explorer.exe	0x07e290000	SHDOCVW.dll	OK: module.1752.1af5cd0.7e290000.dll
0x818f5cd0	explorer.exe	0x076eb0000	TAPI32.dll	OK: module.1752.1af5cd0.76eb0000.dll
0x818f5cd0	explorer.exe	0x077ad0000	POWRPROF.dll	OK: module.1752.1af5cd0.77ad0000.dll
0x818f5cd0	explorer.exe	0x075290000	wbemcomn.dll	OK: module.1752.1af5cd0.75290000.dll
0x818f5cd0	explorer.exe	0x077920000	SETUPAPI.dll	OK: module.1752.1af5cd0.77920000.dll
0x818f5cd0	explorer.exe	0x071c90000	NETUI1.dll	OK: module.1752.1af5cd0.71c90000.dll
0x818f5cd0	explorer.exe	0x071b20000	MPR.dll	OK: module.1752.1af5cd0.71b20000.dll
0x818f5cd0	explorer.exe	0x076390000	IMM32.DLL	OK: module.1752.1af5cd0.76390000.dll
0x818f5cd0	explorer.exe	0x077c10000	msvcrt.dll	OK: module.1752.1af5cd0.77c10000.dll
0x818f5cd0	explorer.exe	0x0755c0000	msctfime.ime	OK: module.1752.1af5cd0.755c0000.dll
0x818f5cd0	explorer.exe	0x0767f0000	schannel.dll	OK: module.1752.1af5cd0.767f0000.dll
0x818f5cd0	explorer.exe	0x07e410000	USER32.dll	OK: module.1752.1af5cd0.7e410000.dll
0x818f5cd0	explorer.exe	0x001210000	xpsp2res.dll	OK: module.1752.1af5cd0.1210000.dll
0x818f5cd0	explorer.exe	0x077a20000	cscui.dll	OK: module.1752.1af5cd0.77a20000.dll
0x818f5cd0	explorer.exe	0x073030000	WZCSDLL	OK: module.1752.1af5cd0.73030000.dll
0x818f5cd0	explorer.exe	0x076e80000	rtutils.dll	OK: module.1752.1af5cd0.76e80000.dll
0x818f5cd0	explorer.exe	0x073380000	zipfldr.dll	OK: module.1752.1af5cd0.73380000.dll
0x818f5cd0	explorer.exe	0x05dc00000	eappprxy.dll	OK: module.1752.1af5cd0.5dc00000.dll
0x818f5cd0	explorer.exe	0x001720000	vmhgfs.dll	OK: module.1752.1af5cd0.1720000.dll
0x818f5cd0	explorer.exe	0x076b20000	ATL.DLL	OK: module.1752.1af5cd0.76b20000.dll
0x818f5cd0	explorer.exe	0x076360000	WINSTA.dll	OK: module.1752.1af5cd0.76360000.dll
0x818f5cd0	explorer.exe	0x075f80000	BROWSEUI.dll	OK: module.1752.1af5cd0.75f80000.dll
0x818f5cd0	explorer.exe	0x05df10000	wzcdlg.dll	OK: module.1752.1af5cd0.5df10000.dll
0x818f5cd0	explorer.exe	0x010000000	DropboxExt.13.dll	OK: module.1752.1af5cd0.10000000.dll
0x818f5cd0	explorer.exe	0x0722b0000	sensapi.dll	OK: module.1752.1af5cd0.722b0000.dll
0x818f5cd0	explorer.exe	0x07c3a0000	MSVCP71.dll	OK: module.1752.1af5cd0.7c3a0000.dll
0x818f5cd0	explorer.exe	0x059a60000	dbghelp.dll	OK: module.1752.1af5cd0.59a60000.dll
0x818f5cd0	explorer.exe	0x076080000	MSVCP60.dll	OK: module.1752.1af5cd0.76080000.dll
0x818f5cd0	explorer.exe	0x077690000	NTMARTA.DLL	OK: module.1752.1af5cd0.77690000.dll
0x818f5cd0	explorer.exe	0x05dca0000	OneX.DLL	OK: module.1752.1af5cd0.5dca0000.dll
0x818f5cd0	explorer.exe	0x0662b0000	hnetcfg.dll	OK: module.1752.1af5cd0.662b0000.dll
0x818f5cd0	explorer.exe	0x0478c0000	dot3api.dll	OK: module.1752.1af5cd0.478c0000.dll
0x818f5cd0	explorer.exe	0x074ed0000	wbemsvc.dll	OK: module.1752.1af5cd0.74ed0000.dll