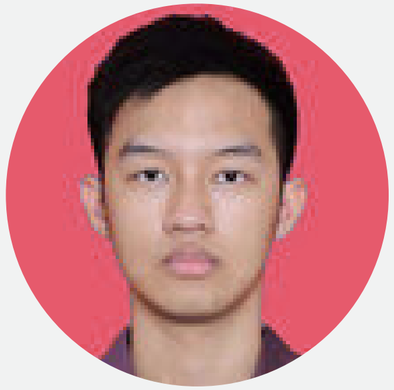
SHYLOCK ANALYSIS USING VOLATILITY

Computer Forensic | Shylock Analysis using Volatility

ANGGOTA KELOMPOK

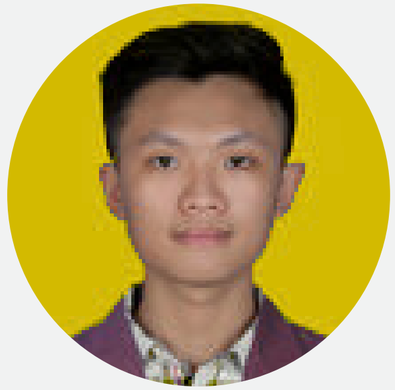
CHRISTINA
2502004235



HUGO
2501997016

MADE
2502005723

JONATHAN
2501986611



MAX
2502011360

FLOW

```
┌──(kali㉿kali)-[~/Documents/volatility_2.6_lin64_standalone]
└─$ ./volatility_2.6_lin64_standalone 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 (/home/kali/Documents/volatility_2.6_lin64_standalone/shylock.vmem)
                      PAE type : PAE
                           DTB : 0x319000L
                          KDBG : 0x80545b60L
          Number of Processors : 1
     Image Type (Service Pack) : 3
                KPCR for CPU 0 : 0xffdff000L
             KUSER_SHARED_DATA : 0xffdf0000L
           Image date and time : 2011-09-30 00:26:30 UTC+0000
     Image local date and time : 2011-09-29 20:26:30 -0400
```

- Menggunakan imageinfo untuk menampilkan properties dari memory image seperti date and time, operating system, service pack, hardware architecture, dan menampilkan profile volitility yang diperlukan.
- Pada command ini, profile yang ditemukan adalah Windows XP dengan ServicePack 2 pada x86 environment.

FLOW

```
┌──(kali㉿kali)-[~/Documents/volatility_2.6_lin64_standalone]
└─$ ./volatility_2.6_lin64_standalone pslist -f shylock.vmem
Volatility Foundation Volatility Framework 2.6
Offset(V)  Name                    PID   PPID   Thds     Hnds   Sess  Wow64 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
0x814a2cd0 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 msseces.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
0x81336638 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 msiexec.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   2011-09-30 00:26:30 UTC+0000
```

- Command pslist digunakan untuk menampilkan informasi terkait proses yang sedang berjalan.

FLOW

```
┌──(kali㉿kali)-[~/Documents/volatility_2.6_lin64_standalone]
└─$ ./volatility_2.6_lin64_standalone 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
```

- Command connscan digunakan untuk menampilkan koneksi TCP network yang sebelumnya sudah dihentikan. Sehingga, kita bisa menggunakan connscan untuk mendapatkan address yang sebelumnya terhubung ke jaringan tersebut.
- Pada command ini, ditemukan bahwa terdapat koneksi dengan PID 1752 (explorer.exe) dengan address 209.190.4.84 dan 184.172.252.227 menggunakan port 443.

FLOW

```
┌──(kali㉿kali)-[~/Documents/volatility_2.6_lin64_standalone]
└─$ ./volatility_2.6_lin64_standalone 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
```

- Command sockets digunakan untuk mendeteksi socket dari setiap protokol.

FLOW

```
┌──(kali㉿kali)-[~/Documents/volatility_2.6_lin64_standalone]
└─$ ./volatility_2.6_lin64_standalone 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    0xff000     0xffff C:\WINDOWS\Explorer.EXE
0x7c900000    0xb2000     0xffff C:\WINDOWS\system32\ntdll.dll
0x7c800000    0xf6000     0xffff C:\WINDOWS\system32\kernel32.dll
0x77dd0000    0x9b000     0xffff C:\WINDOWS\system32\ADVAPI32.dll
0x77e70000    0x93000     0xffff C:\WINDOWS\system32\RPCRT4.dll
0x77fe0000    0x11000     0xffff C:\WINDOWS\system32\Secur32.dll
0x75f80000    0xfd000     0xffff C:\WINDOWS\system32\BROWSEUI.dll
0x77f10000    0x49000     0xffff C:\WINDOWS\system32\GDI32.dll
0x7e410000    0x91000     0xffff C:\WINDOWS\system32\USER32.dll
0x77c10000    0x58000     0xffff C:\WINDOWS\system32\msvcrt.dll
0x774e0000   0x13e000     0xffff C:\WINDOWS\system32\ole32.dll
0x77f60000    0x76000     0xffff C:\WINDOWS\system32\SHLWAPI.dll
0x77120000    0x8b000     0xffff C:\WINDOWS\system32\OLEAUT32.dll
0x7e290000   0x173000     0xffff C:\WINDOWS\system32\SHDOCVW.dll
0x77a80000    0x95000     0xffff C:\WINDOWS\system32\CRYPT32.dll
0x77b20000    0x12000     0xffff C:\WINDOWS\system32\MSASN1.dll
0x754d0000    0x80000     0xffff C:\WINDOWS\system32\CRYPTUI.dll
0x5b860000    0x55000     0xffff C:\WINDOWS\system32\NETAPI32.dll
0x77c00000     0x8000     0xffff C:\WINDOWS\system32\VERSION.dll
0x3d930000    0xd1000     0xffff C:\WINDOWS\system32\WININET.dll
0x00400000     0x9000     0xffff C:\WINDOWS\system32\Normaliz.dll
0x3dfd0000    0x45000     0xffff C:\WINDOWS\system32\iertutil.dll
0x76c30000    0x2e000     0xffff C:\WINDOWS\system32\WINTRUST.dll
0x76c90000    0x28000     0xffff C:\WINDOWS\system32\IMAGEHLP.dll
0x76f60000    0x2c000     0xffff C:\WINDOWS\system32\WLDAP32.dll
0x7c9c0000   0x817000     0xffff C:\WINDOWS\system32\SHELL32.dll
0x5ad70000    0x38000     0xffff 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
0x77be0000    0x15000        0x1 C:\WINDOWS\system32\MSACM32.dll
0x769c0000    0xb4000       0x1c C:\WINDOWS\system32\USERENV.dll
0x76390000    0x1d000        0x5 C:\WINDOWS\system32\IMM32.DLL
0x773d0000   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\COMRes.dll
0x10000000    0x17000        0x4 C:\Documents and Settings\Administrator\Application Data\Dropbox\bin\DropboxExt.13.dll
```

- Untuk dapat menampilkan proses yang menggunakan DLL, kita bisa menggunakan command dlllist. DLL akan otomatis ditambahkan ke dalam list jika proses memanggil LoadLibrary dan tidak akan dihapus sampai FreeLibrary dipanggil dan jumlah reference mencapai nol.

FLOW

```
┌──(kali㉿kali)-[~/Documents/volatility_2.6_lin64_standalone]
└─$ ./volatility_2.6_lin64_standalone -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 e4 02 00 20 09 00   ..............
0x03380030  00 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 ff00            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
```

- Command malfind digunakan untuk menemukan code yang tersembunyi dan terinjeksi dalam user mode memory. Pada command yang kami gunakan, -p dipakai untuk menentukan proses spesifik yang ingin digunakan dan -D digunakan untuk menampilkan code yang terinjeksi ke hard drive. Ditemukan MZ header pada code yang terinjeksi dan -D akan menampilkan code yang terinjeksi ke hard drive untuk dapat dianalisis lebih lanjut.

```
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
```

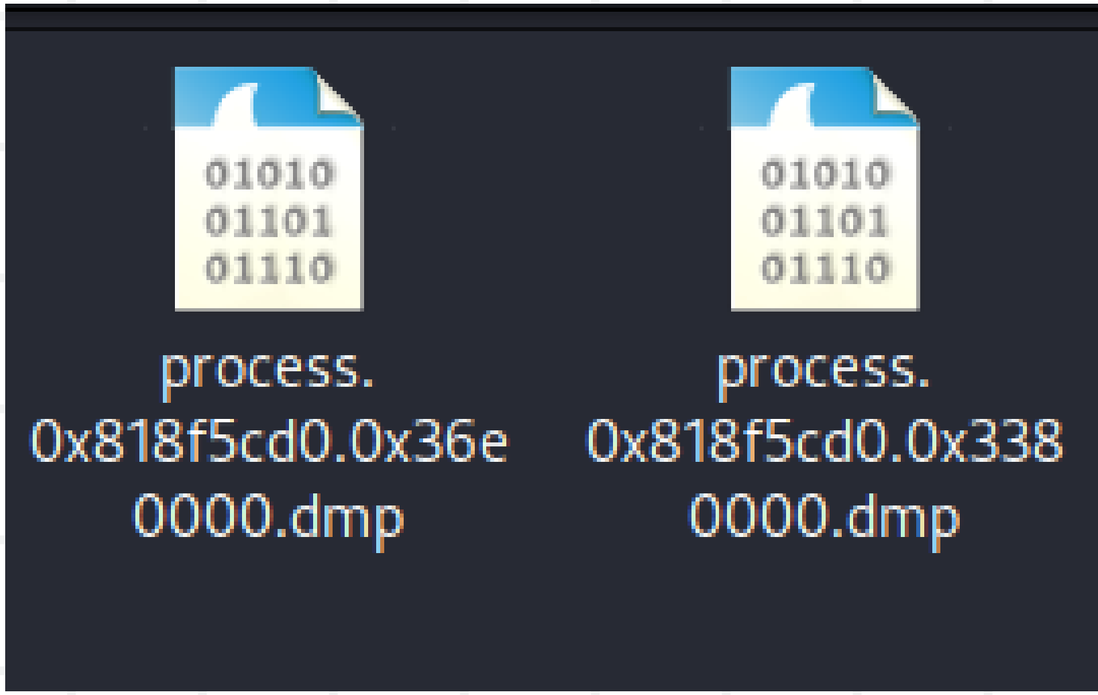
FLOW

- Pada command tersebut, ditemukan **2 malicious code** yang memperbolehkan akses **PAGE_EXECUTE_READWRITE** atau memory dapat mengeksekusi read dan write.
- Setelah itu kita mencoba melakukan memory dump untuk memory yang diinginkan menggunakan command dibawah.

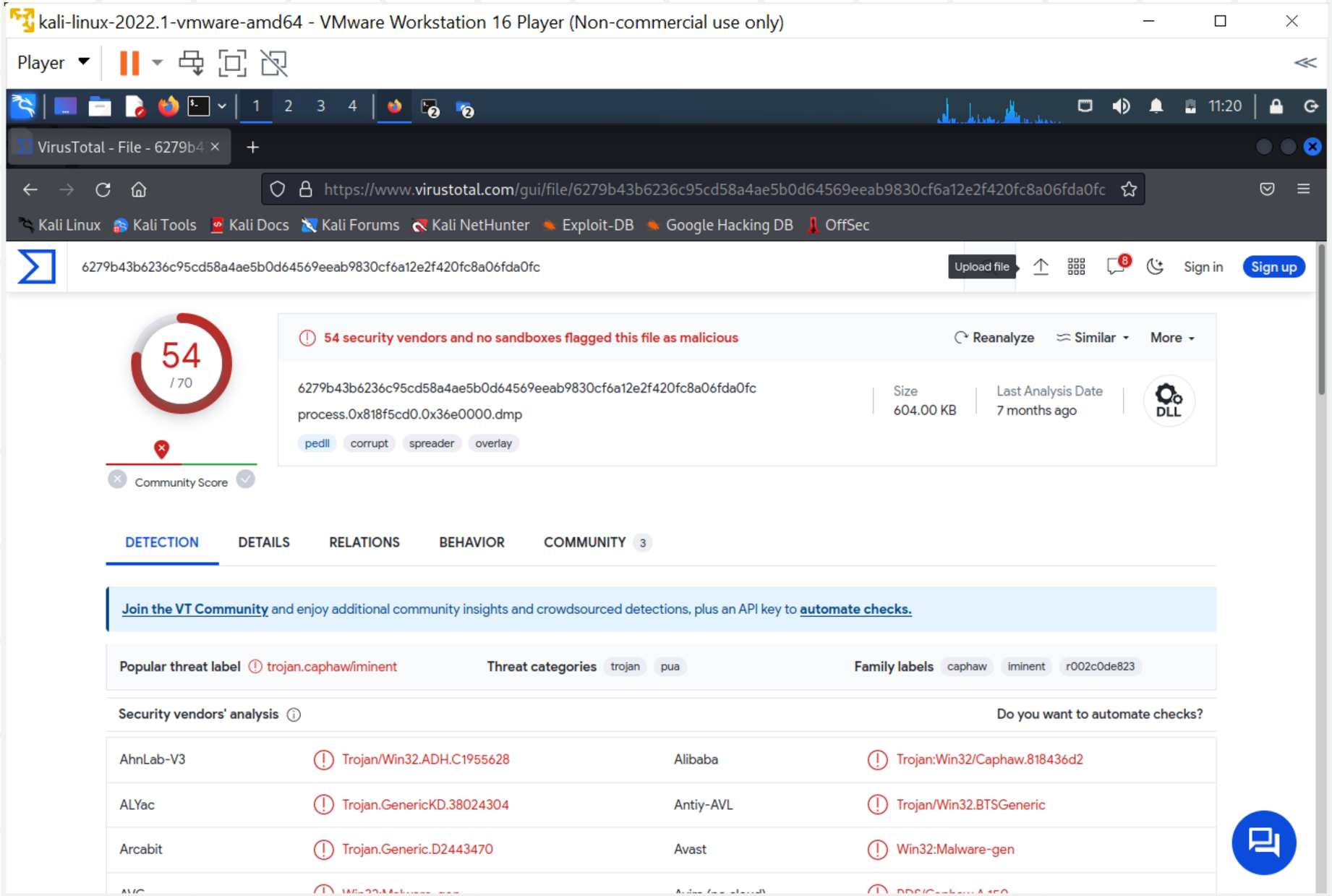
FLOW

```
┌──(root㉿kali)-[/home/kali/volatility_2.6_lin64_standalone]
└─# ./volatility_2.6_lin64_standalone memdump -f shylock.vmem -p 1752 --dump-dir ./
Volatility Foundation Volatility Framework 2.6
************************************************************************
Writing explorer.exe [  1752] to 1752.dmp
```

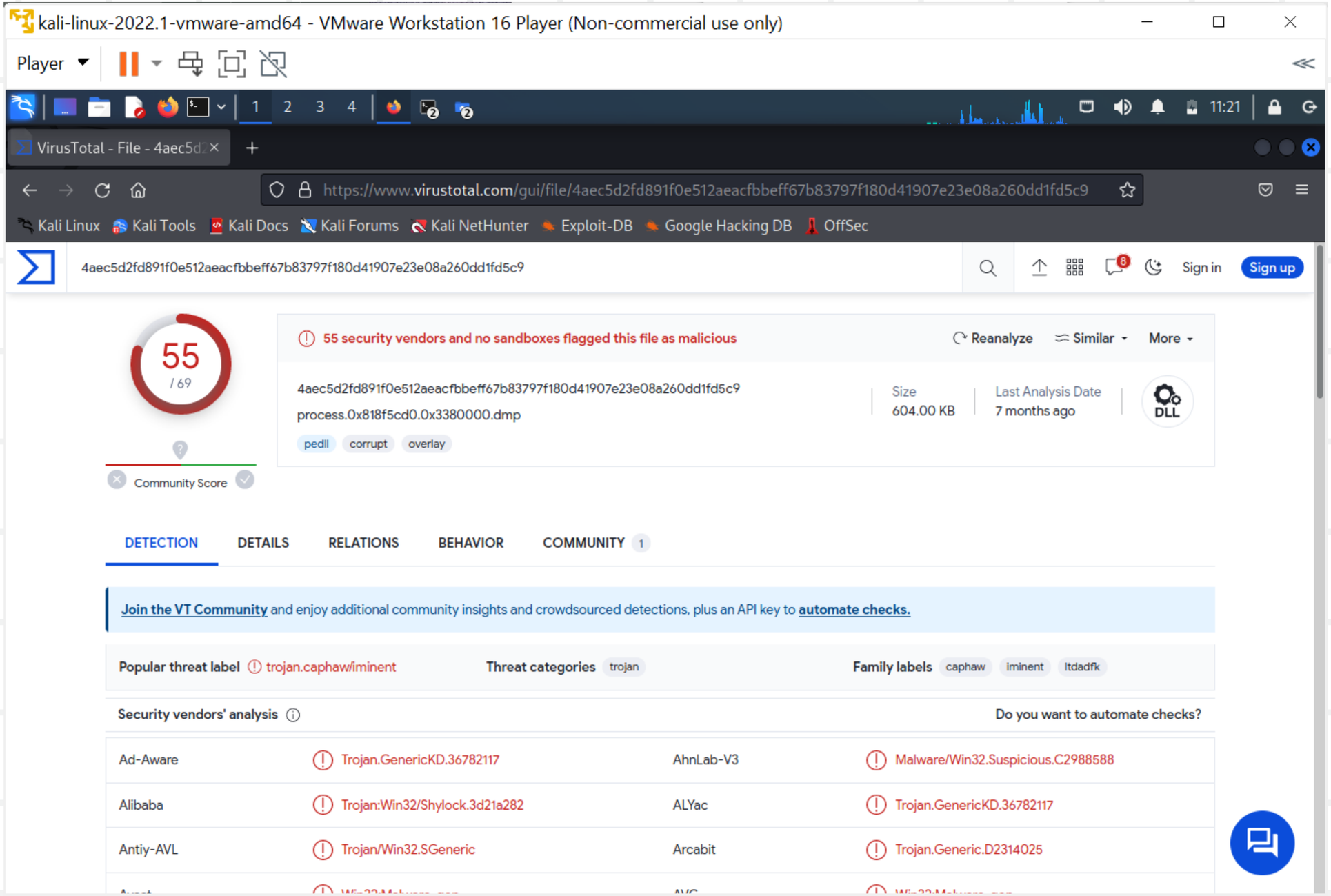
- Pada 2 proses tersebut, dilakukan pengecekan melalui VirusTotal dan didapatkan file tersebut merupakan malicious file.



PROOF OF MALICIOUS FILE1



PROOF OF MALICIOUS FILE2



THANK YOU