KUSHAL RAHATKAR

2113202

INCIDENT MANAGEMENT AND FORENSICS COURSEWORK 2

CMM519

INDEX

TABLE OF CONTENTS

CWRAM.DD

BASIC ANALYSIS FINDINGS

Operating system – Windows XP

Service Pack – 2 / 3

System Architecture – x86 (32 bit)

Image date and time – 2020-11-09 23:33:29

```
C:\Coursework2>volatility_2.6_win64_standalone.exe -f cwRAM.mem 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:\Coursework2\cwRAM.mem)
                      PAE type : PAE
                           DTB : 0x31c000L
                          KDBG : 0x8054c2e0L
          Number of Processors : 2
     Image Type (Service Pack) : 2
                KPCR for CPU 0 : 0xffdff000L
                KPCR for CPU 1 : 0xf892a000L
             KUSER_SHARED_DATA : 0xffdf0000L
           Image date and time : 2020-11-09 23:33:29 UTC+0000
     Image local date and time : 2020-11-09 23:33:29 +0000
```

Figure 1

RUNNING TASKS ON THE SYSTEM

```
C:\Coursework2>volatility_2.6_win64_standalone.exe -f cwRAM.mem --profile=WinXPSP2x86 pslist
Volatility Foundation Volatility Framework 2.6
Offset(V)  Name                    PID   PPID   Thds     Hnds   Sess  Wow64 Start                          Exit
---------- -------------------- ------ ------ ------ -------- ------ ------ ------------------------------ ------------------------------
0x823c6830 System                    4      0     61      256 ------      0
0x822fc020 smss.exe                572      4      3       21 ------      0 2020-11-09 21:32:36 UTC+0000
0x821ab9d8 csrss.exe               636    572     11      387      0      0 2020-11-09 21:32:37 UTC+0000
0x82248020 winlogon.exe            660    572     21      638      0      0 2020-11-09 21:32:38 UTC+0000
0x81e98650 services.exe            704    660     16      352      0      0 2020-11-09 21:32:38 UTC+0000
0x8213f650 lsass.exe               716    660     25      367      0      0 2020-11-09 21:32:38 UTC+0000
0x8220f6d0 vmacthlp.exe            888    704      1       24      0      0 2020-11-09 21:32:38 UTC+0000
0x820dc020 svchost.exe             904    704     18      197      0      0 2020-11-09 21:32:38 UTC+0000
0x821e55c8 svchost.exe             968    704     10      284      0      0 2020-11-09 21:32:39 UTC+0000
0x82067c08 svchost.exe            1088    704     58     1243      0      0 2020-11-09 21:32:39 UTC+0000
0x81fd9b28 svchost.exe            1192    704      4       57      0      0 2020-11-09 21:32:39 UTC+0000
0x81ff2da0 svchost.exe            1244    704     14      208      0      0 2020-11-09 21:32:39 UTC+0000
0x82059978 spoolsv.exe            1364    704     10      136      0      0 2020-11-09 21:32:40 UTC+0000
0x81ffe020 explorer.exe           1672   1612     14      460      0      0 2020-11-09 21:32:46 UTC+0000
0x8224b780 VGAuthService.e         180    704      2       61      0      0 2020-11-09 21:32:46 UTC+0000
0x81f33020 vmtoolsd.exe            320   1672      5      134      0      0 2020-11-09 21:32:47 UTC+0000
0x81e7cda0 vmtoolsd.exe            384    704      7      246      0      0 2020-11-09 21:32:50 UTC+0000
0x82095b88 alg.exe                1296    704      5      103      0      0 2020-11-09 21:32:51 UTC+0000
0x81e41da0 wscntfy.exe             552   1088      1       27      0      0 2020-11-09 21:32:51 UTC+0000
0x82274558 wmiprvse.exe            764    904     13      308      0      0 2020-11-09 21:32:51 UTC+0000
0x81e28748 IEXPLORE.EXE           1024   1672      7      311      0      0 2020-11-09 23:20:57 UTC+0000
0x81fe5408 puttytel.exe           1564   1672      2       46      0      0 2020-11-09 23:22:04 UTC+0000
0x81e2c650 Tetris.exe             1276   1672      1       13      0      0 2020-11-09 23:27:37 UTC+0000
0x81fee6f8 msimn.exe               524   1672     12      323      0      0 2020-11-09 23:27:57 UTC+0000
0x81ef4da0 msmsgs.exe             1984    904      3      167      0      0 2020-11-09 23:27:57 UTC+0000
0x82119020 notepad.exe            1516   1672      1       33      0      0 2020-11-09 23:31:25 UTC+0000
0x81fbec08 RamCapture.exe         1164   1672      2       31      0      0 2020-11-09 23:33:12 UTC+0000
```

Figure 2

PROCESS TREE ON THE SYSTEM.

```
C:\Coursework2>volatility_2.6_win64_standalone.exe -f cwRAM.mem --profile=WinXPSP2x86 pstree
Volatility Foundation Volatility Framework 2.6
Name                                                  Pid   PPid   Thds   Hnds Time
-------------------------------------------------- ------ ------ ------ ------ ----
 0x823c6830:System                                      4      0     61    256 1970-01-01 00:00:00 UTC+0000
. 0x822fc020:smss.exe                                 572      4      3     21 2020-11-09 21:32:36 UTC+0000
.. 0x82248020:winlogon.exe                            660    572     21    638 2020-11-09 21:32:38 UTC+0000
... 0x81e98650:services.exe                           704    660     16    352 2020-11-09 21:32:38 UTC+0000
.... 0x81e7cda0:vmtoolsd.exe                          384    704      7    246 2020-11-09 21:32:50 UTC+0000
.... 0x82067c08:svchost.exe                          1088    704     58   1243 2020-11-09 21:32:39 UTC+0000
..... 0x81e41da0:wscntfy.exe                          552   1088      1     27 2020-11-09 21:32:51 UTC+0000
.... 0x820dc020:svchost.exe                           904    704     18    197 2020-11-09 21:32:38 UTC+0000
..... 0x81ef4da0:msmsgs.exe                          1984    904      3    167 2020-11-09 23:27:57 UTC+0000
..... 0x82274558:wmiprvse.exe                         764    904     13    308 2020-11-09 21:32:51 UTC+0000
.... 0x82095b88:alg.exe                              1296    704      5    103 2020-11-09 21:32:51 UTC+0000
.... 0x8224b780:VGAuthService.e                       180    704      2     61 2020-11-09 21:32:46 UTC+0000
.... 0x821e55c8:svchost.exe                           968    704     10    284 2020-11-09 21:32:39 UTC+0000
.... 0x82059978:spoolsv.exe                          1364    704     10    136 2020-11-09 21:32:40 UTC+0000
.... 0x81ff2da0:svchost.exe                          1244    704     14    208 2020-11-09 21:32:39 UTC+0000
.... 0x81fd9b28:svchost.exe                          1192    704      4     57 2020-11-09 21:32:39 UTC+0000
.... 0x8220f6d0:vmacthlp.exe                          888    704      1     24 2020-11-09 21:32:38 UTC+0000
... 0x8213f650:lsass.exe                              716    660     25    367 2020-11-09 21:32:38 UTC+0000
.. 0x821ab9d8:csrss.exe                               636    572     11    387 2020-11-09 21:32:37 UTC+0000
 0x81ffe020:explorer.exe                             1672   1612     14    460 2020-11-09 21:32:46 UTC+0000
. 0x81fee6f8:msimn.exe                                524   1672     12    323 2020-11-09 23:27:57 UTC+0000
. 0x81fe5408:puttytel.exe                            1564   1672      2     46 2020-11-09 23:22:04 UTC+0000
. 0x81e28748:IEXPLORE.EXE                            1024   1672      7    311 2020-11-09 23:20:57 UTC+0000
. 0x81e2c650:Tetris.exe                              1276   1672      1     13 2020-11-09 23:27:37 UTC+0000
. 0x81fbec08:RamCapture.exe                          1164   1672      2     31 2020-11-09 23:33:12 UTC+0000
. 0x81f33020:vmtoolsd.exe                             320   1672      5    134 2020-11-09 21:32:47 UTC+0000
. 0x82119020:notepad.exe                             1516   1672      1     33 2020-11-09 23:31:25 UTC+0000
```

Figure 3

TCP CONNECTIONS ON THE SYSTEM

```
C:\Coursework2>volatility_2.6_win64_standalone.exe -f cwRAM.mem --profile=WinXPSP2x86 connscan
Volatility Foundation Volatility Framework 2.6
Offset(P)  Local Address             Remote Address            Pid
---------- ------------------------- ------------------------- ---
0x021a73f8 192.168.1.11:1040         192.168.1.251:80          1024
0x022494e8 192.168.1.11:1041         192.168.1.250:23          1564
0x0224e3d8 192.168.1.11:1044         192.168.1.250:110         524
0x02348ab8 192.168.1.11:1039         192.168.1.251:80          1024
0x02389228 192.168.1.11:1042         192.168.1.250:110         524
0x038f0228 192.168.1.11:1042         192.168.1.250:110         524
0x1264fab8 192.168.1.11:1039         192.168.1.251:80          1024
0x14ca53d8 192.168.1.11:1044         192.168.1.250:110         524
0x17456228 192.168.1.11:1042         192.168.1.250:110         524
0x1cdd03d8 192.168.1.11:1044         192.168.1.250:110         524
0x1dff8228 192.168.1.11:1042         192.168.1.250:110         524
```

Figure 4

OPEN CONNECTIONS ON THE SYSTEM

```
C:\Coursework2>volatility_2.6_win64_standalone.exe -f cwRAM.mem --profile=WinXPSP2x86 connections
Volatility Foundation Volatility Framework 2.6
Offset(V)  Local Address             Remote Address            Pid
---------- ------------------------- ------------------------- ---
0x820494e8 192.168.1.11:1041         192.168.1.250:23          1564
```

Figure 5

OPEN PORTS ON THE SYSTEM WITH CONNECTION PROTOCOL

```
C:\Coursework2>volatility_2.6_win64_standalone.exe -f cwRAM.mem --profile=WinXPSP2x86 sockscan
Volatility Foundation Volatility Framework 2.6
Offset(P)          PID   Port  Proto Protocol        Address         Create Time
---------- -------- ------ ------ --------------- --------------- -----------
0x01bee3e0     1148   1026      6 TCP             127.0.0.1       2020-11-09 17:02:20 UTC+0000
0x02042338     1088    123     17 UDP             192.168.1.11    2020-11-09 21:32:50 UTC+0000
0x020424d0     1244   1900     17 UDP             127.0.0.1       2020-11-09 21:32:51 UTC+0000
0x020a73e0      716      0    255 Reserved        0.0.0.0         2020-11-09 21:32:47 UTC+0000
0x020bec20     1296   1029      6 TCP             127.0.0.1       2020-11-09 21:32:51 UTC+0000
0x020c4e98     1088    123     17 UDP             127.0.0.1       2020-11-09 21:32:50 UTC+0000
0x020fc008        4    445      6 TCP             0.0.0.0         2020-11-09 21:32:36 UTC+0000
0x02135c20     1088   1025     17 UDP             127.0.0.1       2020-11-09 21:32:50 UTC+0000
0x0219b978        4    138     17 UDP             192.168.1.11    2020-11-09 21:32:36 UTC+0000
0x021d4440      716    500     17 UDP             0.0.0.0         2020-11-09 21:32:46 UTC+0000
0x021d79c0     1564   1041      6 TCP             0.0.0.0         2020-11-09 23:24:21 UTC+0000
0x021d7b78     1024   1037     17 UDP             127.0.0.1       2020-11-09 23:21:00 UTC+0000
0x0223f3d0        4    139      6 TCP             192.168.1.11    2020-11-09 21:32:36 UTC+0000
0x02259e98        4    445     17 UDP             0.0.0.0         2020-11-09 21:32:36 UTC+0000
0x02310ce8     1244   1900     17 UDP             192.168.1.11    2020-11-09 21:32:51 UTC+0000
0x02319290      716   4500     17 UDP             0.0.0.0         2020-11-09 21:32:47 UTC+0000
0x0233fe98      968    135      6 TCP             0.0.0.0         2020-11-09 21:32:39 UTC+0000
0x024801d8        4    137     17 UDP             192.168.1.11    2020-11-09 21:32:36 UTC+0000
0x10fb63d0        4    139      6 TCP             192.168.1.11    2020-11-09 21:32:36 UTC+0000
0x123fbe98     1088    123     17 UDP             127.0.0.1       2020-11-09 21:32:50 UTC+0000
0x1251b440      716    500     17 UDP             0.0.0.0         2020-11-09 21:32:46 UTC+0000
0x126071d8        4    137     17 UDP             192.168.1.11    2020-11-09 21:32:36 UTC+0000
0x12683008        4    445      6 TCP             0.0.0.0         2020-11-09 21:32:36 UTC+0000
0x12ab5c20     1296   1029      6 TCP             127.0.0.1       2020-11-09 21:32:51 UTC+0000
0x12b66c20     1296   1029      6 TCP             127.0.0.1       2020-11-09 21:32:51 UTC+0000
0x12fcf008        4    445      6 TCP             0.0.0.0         2020-11-09 21:32:36 UTC+0000
0x13327ce8     1244   1900     17 UDP             192.168.1.11    2020-11-09 21:32:51 UTC+0000
0x137411d8        4    137     17 UDP             192.168.1.11    2020-11-09 21:32:36 UTC+0000
0x137e2978        4    138     17 UDP             192.168.1.11    2020-11-09 21:32:36 UTC+0000
0x1462e3e0      716      0    255 Reserved        0.0.0.0         2020-11-09 21:32:47 UTC+0000
0x14c853e0      716      0    255 Reserved        0.0.0.0         2020-11-09 21:32:47 UTC+0000
0x15e0dce8     1244   1900     17 UDP             192.168.1.11    2020-11-09 21:32:51 UTC+0000
0x1cea5008        4    445      6 TCP             0.0.0.0         2020-11-09 21:32:36 UTC+0000
0x1f735c20     1296   1029      6 TCP             127.0.0.1       2020-11-09 21:32:51 UTC+0000
```

Figure 6

OPEN SOCKETS ON THE SYSTEM

```
C:\Coursework2>volatility_2.6_win64_standalone.exe -f cwRAM.mem --profile=WinXPSP2x86 sockets
Volatility Foundation Volatility Framework 2.6
Offset(V)       PID   Port  Proto Protocol        Address         Create Time
---------- -------- ------ ------ ---------- ---------- ----------
0x81f9b978        4    138     17 UDP           192.168.1.11    2020-11-09 21:32:36 UTC+0000
0x81f35c20     1088   1025     17 UDP           127.0.0.1       2020-11-09 21:32:50 UTC+0000
0x81fd4440      716    500     17 UDP           0.0.0.0         2020-11-09 21:32:46 UTC+0000
0x81e42338     1088    123     17 UDP           192.168.1.11    2020-11-09 21:32:50 UTC+0000
0x81efc008        4    445      6 TCP           0.0.0.0         2020-11-09 21:32:36 UTC+0000
0x81fd7b78     1024   1037     17 UDP           127.0.0.1       2020-11-09 23:21:00 UTC+0000
0x8213fe98      968    135      6 TCP           0.0.0.0         2020-11-09 21:32:39 UTC+0000
0x81ebec20     1296   1029      6 TCP           127.0.0.1       2020-11-09 21:32:51 UTC+0000
0x81ea73e0      716      0    255 Reserved       0.0.0.0         2020-11-09 21:32:47 UTC+0000
0x81ec4e98     1088    123     17 UDP           127.0.0.1       2020-11-09 21:32:50 UTC+0000
0x82110ce8     1244   1900     17 UDP           192.168.1.11    2020-11-09 21:32:51 UTC+0000
0x8203f3d0        4    139      6 TCP           192.168.1.11    2020-11-09 21:32:36 UTC+0000
0x822801d8        4    137     17 UDP           192.168.1.11    2020-11-09 21:32:36 UTC+0000
0x81e424d0     1244   1900     17 UDP           127.0.0.1       2020-11-09 21:32:51 UTC+0000
0x82119290      716   4500     17 UDP           0.0.0.0         2020-11-09 21:32:47 UTC+0000
0x81fd79c0     1564   1041      6 TCP           0.0.0.0         2020-11-09 23:24:21 UTC+0000
0x82059e98        4    445     17 UDP           0.0.0.0         2020-11-09 21:32:36 UTC+0000
```

Figure 7

SYSTEM HIVES WITH KEYS

```
C:\Coursework2>volatility_2.6_win64_standalone.exe -f cwRAM.mem --profile=WinXPSP2x86 hivelist
Volatility Foundation Volatility Framework 2.6
Virtual    Physical   Name
---------- ---------- ----
0xe25a4410 0x0d341410 \Device\HarddiskVolume1\Documents and Settings\networkuser\Local Settings\Application Data\Microsoft\Windows\UsrClass.dat
0xe24fdb60 0x0c77db60 \Device\HarddiskVolume1\Documents and Settings\networkuser\NTUSER.DAT
0xe193c578 0x0aa04578 \Device\HarddiskVolume1\Documents and Settings\LocalService\Local Settings\Application Data\Microsoft\Windows\UsrClass.dat
0xe198a758 0x0b188758 \Device\HarddiskVolume1\Documents and Settings\LocalService\NTUSER.DAT
0xe1967758 0x0ad64758 \Device\HarddiskVolume1\Documents and Settings\NetworkService\Local Settings\Application Data\Microsoft\Windows\UsrClass.dat
0xe195c008 0x0ae40008 \Device\HarddiskVolume1\Documents and Settings\NetworkService\NTUSER.DAT
0xe140d758 0x08879758 \Device\HarddiskVolume1\WINDOWS\system32\config\software
0xe15cb368 0x085a6368 \Device\HarddiskVolume1\WINDOWS\system32\config\default
0xe179eb60 0x05808b60 \Device\HarddiskVolume1\WINDOWS\system32\config\SAM
0xe17bdb60 0x08400b60 \Device\HarddiskVolume1\WINDOWS\system32\config\SECURITY
0xe13c5008 0x02e5b008 [no name]
0xe1037008 0x02aea008 \Device\HarddiskVolume1\WINDOWS\system32\config\system
0xe102f008 0x02ae3008 [no name]
```

Figure 8

```
C:\Coursework2>volatility_2.6_win64_standalone.exe -f cwRAM.mem --profile=WinXPSP2x86 printkey
Volatility Foundation Volatility Framework 2.6
Legend: (S) = Stable   (V) = Volatile

----------------------------
Registry: \Device\HarddiskVolume1\Documents and Settings\networkuser\NTUSER.DAT
Key name: $$$PROTO.HIV (S)
Last updated: 2020-11-09 21:33:14 UTC+0000

Subkeys:
  (S) AppEvents
  (S) Console
  (S) Control Panel
  (S) Environment
  (S) Identities
  (S) Keyboard Layout
  (S) Printers
  (S) Software
  (S) UNICODE Program Groups
  (S) Windows 3.1 Migration Status
  (V) SessionInformation
  (V) Volatile Environment
```

Figure 7 (does not cover whole hive and key section)

NAME OF THE SYSTEM

```
C:\Coursework2>volatility_2.6_win64_standalone.exe -f cwRAM.mem --profile=WinXPSP2x86 printkey -o 0xe1037008 -K "ControlSet001\Control\ComputerName\ComputerName"
Volatility Foundation Volatility Framework 2.6
Legend: (S) = Stable   (V) = Volatile

----------------------------
Registry: \Device\HarddiskVolume1\WINDOWS\system32\config\system
Key name: ComputerName (S)
Last updated: 2019-12-03 13:39:22 UTC+0000

Subkeys:

Values:
REG_SZ        ComputerName    : (S) CSDM <----------
```

Figure 10(Process Described in Appendix)

DEVICES ATTACHED

```
C:\Coursework2>volatility_2.6_win64_standalone.exe -f cwRAM.mem --profile=WinXPSP2x86 printkey -o 0xe1037008 -K "ControlSet001\Enum\USBSTOR\Disk&Ven_USB2.0&Prod_Flash_Disk&Rev_2.60\20150511
165806718&0"
Volatility Foundation Volatility Framework 2.6
Legend: (S) = Stable   (V) = Volatile

----------------------------
Registry: \Device\HarddiskVolume1\WINDOWS\system32\config\system
Key name: 201505111658067 1&0 (S)
Last updated: 2020-11-09 23:26:55 UTC+0000

Subkeys:
  (S) Device Parameters
  (S) LogConf
  (V) Control

Values:
REG_SZ        DeviceDesc      : (S) Disk drive
REG_DWORD     Capabilities    : (S) 16
REG_DWORD     UINumber        : (S) 0
REG_MULTI_SZ  HardwareID      : (S) ['USBSTOR\\DiskUSB2.0__Flash_Disk_____2.60', 'USBSTOR\\DiskUSB2.0__Flash_Disk_____', 'USBSTOR\\DiskUSB2.0__', 'USBSTOR\\USB2.0__Flash_Disk_____2', 'US
B2.0__Flash_Disk_____2', 'USBSTOR\\GenDisk', 'GenDisk', '', '']
REG_MULTI_SZ  CompatibleIDs   : (S) ['USBSTOR\\Disk', 'USBSTOR\\RAW', '', '']
REG_SZ        ClassGUID       : (S) {4D36E967-E325-11CE-BFC1-08002BE10318}
REG_SZ        Service         : (S) disk
REG_DWORD     ConfigFlags     : (S) 0
REG_SZ        ParentIdPrefix  : (S) 8&314855ab&0
REG_SZ        Driver          : (S) {4D36E967-E325-11CE-BFC1-08002BE10318}\0001
REG_SZ        Class           : (S) DiskDrive
REG_SZ        Mfg             : (S) (Standard disk drives)
REG_SZ        FriendlyName    : (S) USB2.0 Flash Disk USB Device
```

Figure 11 (Process Described in Appendix)

LAST SHUTDOWN TIME OF MACHINE

```
C:\Coursework2>volatility_2.6_win64_standalone.exe -f cwRAM.mem --profile=WinXPSP2x86 printkey -o 0xe1037008 -K "ControlSet001\Control\Windows"
Volatility Foundation Volatility Framework 2.6
Legend: (S) = Stable   (V) = Volatile

----------------------------
Registry: \Device\HarddiskVolume1\WINDOWS\system32\config\system
Key name: Windows (S)
Last updated: 2020-11-09 21:32:20 UTC+0000

Subkeys:

Values:
REG_DWORD     CSDVersion      : (S) 512
REG_DWORD     CSDReleaseType  : (S) 0
REG_EXPAND_SZ Directory       : (S) %SystemRoot%
REG_DWORD     ErrorMode       : (S) 0
REG_DWORD     NoInteractiveServices : (S) 0
REG_EXPAND_SZ SystemDirectory : (S) %SystemRoot%\system32
REG_DWORD     ShellErrorMode  : (S) 1
REG_BINARY    ShutdownTime    : (S)
0x00000000  84 d8 31 ce df b6 d6 01        ..1.....
```

Figure 12 (Process Described in Appendix)

The shutdown time of the system is - Mon 9 November 2020 21:32:20 UTC

TIME ZONE OF THE SYSTEM SET WHILE INSTALLATION

```
C:\Coursework2>volatility_2.6_win64_standalone.exe -f cwRAM.mem --profile=WinXPSP2x86 printkey -o 0xe1037008 -K "ControlSet001\Control\TimeZoneInformation"
Volatility Foundation Volatility Framework 2.6
Legend: (S) = Stable   (V) = Volatile

----------------------------
Registry: \Device\HarddiskVolume1\WINDOWS\system32\config\system
Key name: TimeZoneInformation (S)
Last updated: 2019-12-03 14:08:11 UTC+0000

Subkeys:

Values:
REG_DWORD     Bias            : (S) 0
REG_SZ        StandardName    : (S) GMT Standard Time
REG_DWORD     StandardBias    : (S) 0
REG_BINARY    StandardStart   : (S)
0x00000000  00 00 0a 00 05 00 02 00 00 00 00 00 00 00 00 00   ................
REG_SZ        DaylightName    : (S) GMT Standard Time
REG_DWORD     DaylightBias    : (S) 4294967236
REG_BINARY    DaylightStart   : (S)
0x00000000  00 00 03 00 05 00 01 00 00 00 00 00 00 00 00 00   ................
REG_DWORD     ActiveTimeBias  : (S) 0
```

Figure 13 (Process Described in Appendix)

USERS ON THE SYSTEM "

```
C:\Coursework2>volatility_2.6_win64_standalone.exe -f cwRAM.mem --profile=WinXPSP2x86 printkey -o 0xe179eb60 -K "SAM\Domains\Account\Users\Names"
Volatility Foundation Volatility Framework 2.6
Legend: (S) = Stable   (V) = Volatile

----------------------------
Registry: \Device\HarddiskVolume1\WINDOWS\system32\config\SAM
Key name: Names (S)
Last updated: 2019-12-03 14:08:11 UTC+0000

Subkeys:
  (S) Administrator
  (S) Guest
  (S) HelpAssistant
  (S) networkuser
  (S) SUPPORT_388945a0

Values:
REG_DWORD                     : (S) 0
```

Figure 14

TETRIS.EXE

```
C:\Coursework2>volatility_2.6_win64_standalone.exe -f cwRAM.mem --profile=WinXPSP2x86 filescan | findstr Tetris
Volatility Foundation Volatility Framework 2.6
0x00000000021d68a0      1      0 R--r-d \Device\DP(1)0-0+5\Tetris.exe
0x0000000002295450      1      0 R--rw- \Device\DP(1)0-0+5\Tetris.exe
```

Figure 8

UNDERSTANDING AND FINDING INTERESTING THINGS

When working on Windows system, recovering Tetris.exe automatically got deleted by the system. This made a file suspicious to the investigator as the file must be malicious.

Downloading and using volatility on Linux platform made it possible to recover expected file without getting deleted. Because Linux Kernal do not execute .exe file and made the fie stable even after retrieving.

```
┌─[tryhard@Kushal]─[~/volatility_2.6_lin64_standalone]
└──╼ $./volatility_2.6_lin64_standalone -f cwRAM.mem profile=WinXPSP2x86 dumpfiles -Q 0x00000000021d68a0 --name file -D ~/volatility_2.6_lin64_standalone
Volatility Foundation Volatility Framework 2.6
ImageSectionObject 0x021d68a0   None   \Device\DP(1)0-0+5\Tetris.exe
DataSectionObject 0x021d68a0   None   \Device\DP(1)0-0+5\Tetris.exe
```

Figure 16 (Process can be accessed in Appendix)

```
C:\Coursework2>volatility_2.6_win64_standalone.exe -f cwRAM.mem --profile=WinXPSP2x86 -p 1276 dlllist
Volatility Foundation Volatility Framework 2.6
************************************************************************
Tetris.exe pid:   1276
Command line : "E:\Tetris.exe"
Service Pack 2

Base             Size  LoadCount Path
---------- ---------- ---------- ----
0x00400000    0x16000     0xffff E:\Tetris.exe
0x7c900000    0xb0000     0xffff C:\WINDOWS\system32\ntdll.dll
0x7c800000    0xf4000     0xffff C:\WINDOWS\system32\kernel32.dll
0x77c10000    0x58000     0xffff C:\WINDOWS\system32\MSVCRT.dll
0x77dd0000    0x9b000     0xffff C:\WINDOWS\system32\ADVAPI32.dll
0x77e70000    0x91000     0xffff C:\WINDOWS\system32\RPCRT4.dll
0x71ad0000     0x9000     0xffff C:\WINDOWS\system32\WSOCK32.dll
0x71ab0000    0x17000     0xffff C:\WINDOWS\system32\WS2_32.dll
0x71aa0000     0x8000     0xffff C:\WINDOWS\system32\WS2HELP.dll
0x77d40000    0x90000        0x6 C:\WINDOWS\system32\user32.dll
0x77f10000    0x46000        0x5 C:\WINDOWS\system32\GDI32.dll
0x5ad70000    0x38000        0x2 C:\WINDOWS\system32\uxtheme.dll
```

Figure 17

From the figure 16, the file has been retrieved and it can be seen in the folder.

```
┌─[tryhard@Kushal]─[~/volatility_2.6_lin64_standalone]
└──╼ $ls -la
total 538956
drwx------ 1 tryhard tryhard       276 Apr 17 02:13 .
drwxr-xr-x 1 tryhard tryhard       566 Apr 17 01:59 ..
-rwx------ 1 tryhard tryhard       778 Dec 27  2016 AUTHORS.txt
drwx------ 1 tryhard tryhard        20 Apr 17 02:01 Coursework2
-rwx------ 1 tryhard tryhard      3917 Dec 27  2016 CREDITS.txt
-rw-r--r-- 1 tryhard tryhard 536870912 Apr 17 01:57 cwRAM.mem
-rw-r--r-- 1 tryhard tryhard     73728 Apr 17 02:13 file.None.0x822f54b0.Tetris.exe.img
-rwx------ 1 tryhard tryhard       698 Jul  7  2016 LEGAL.txt
-rwx------ 1 tryhard tryhard     15127 Jul  7  2016 LICENSE.txt
-rwx------ 1 tryhard tryhard     31879 Dec 24  2016 README.txt
-rwx------ 1 tryhard tryhard  14937576 Dec 27  2016 volatility_2.6_lin64_standalone
```

Figure 18

The file size is 73728 bytes confirms the file is perfectly retrieved. Checking file on VirusTotal. It confirms the file is a strong Malware.

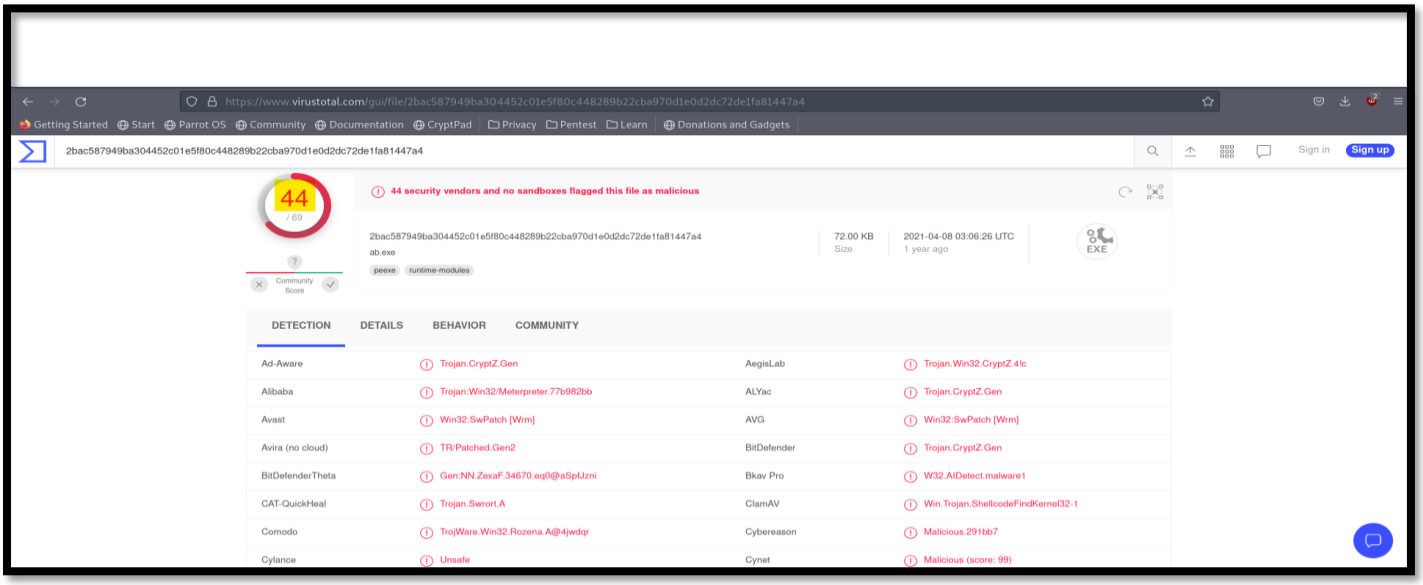


Figure 19

Following figure shows the mutex created by the IEXPLOR.exe file.

```
C:\Coursework2>volatility_2.6_win64_standalone.exe -f cwRAM.mem handles -p 1024 -t Mutant
Volatility Foundation Volatility Framework 2.6
Offset(V)     Pid      Handle     Access Type             Details
---------- ------ ---------- ---------- --------------- -------
0x81fa45e0   1024       0x3c   0x1f0001 Mutant
0x81f26ce8   1024       0x44   0x1f0001 Mutant
0x81e3b168   1024      0x138   0x100000 Mutant          _!MSFTHISTORY!_
0x81fd3550   1024      0x140   0x1f0001 Mutant          c:!documents and settings!networkuser!local settings!temporary internet files!content.ie5!
0x8206a588   1024      0x148   0x1f0001 Mutant          c:!documents and settings!networkuser!cookies!
0x81e31558   1024      0x150   0x1f0001 Mutant          c:!documents and settings!networkuser!local settings!history!history.ie5!
0x8204e748   1024      0x170   0x100000 Mutant          WininetStartupMutex
0x822f9270   1024      0x178   0x1f0001 Mutant          WininetConnectionMutex
0x822f2750   1024      0x17c   0x1f0001 Mutant
0x81e50aa8   1024      0x180   0x100000 Mutant          WininetProxyRegistryMutex
0x822f5b88   1024      0x198   0x120001 Mutant          ShimCacheMutex
0x81e31910   1024      0x1a4   0x1f0001 Mutant
0x82110228   1024      0x1b4   0x1f0001 Mutant
0x820da4a8   1024      0x1c0   0x1f0001 Mutant
0x82259688   1024      0x1c8   0x1f0001 Mutant
0x81fd3450   1024      0x28c   0x1f0001 Mutant
0x8214efe0   1024      0x294   0x100000 Mutant          RasPbFile
0x81ef3270   1024      0x420   0x1f0001 Mutant          CTF.LBES.MutexDefaultS-1-5-21-1614895754-261478967-839522115-1003
0x81e31998   1024      0x424   0x1f0001 Mutant          CTF.Compart.MutexDefaultS-1-5-21-1614895754-261478967-839522115-1003
0x81e2c600   1024      0x428   0x1f0001 Mutant          CTF.Asm.MutexDefaultS-1-5-21-1614895754-261478967-839522115-1003
0x81e2c5b0   1024      0x42c   0x1f0001 Mutant          CTF.Layouts.MutexDefaultS-1-5-21-1614895754-261478967-839522115-1003
0x8206a410   1024      0x430   0x1f0001 Mutant          CTF.TMD.MutexDefaultS-1-5-21-1614895754-261478967-839522115-1003
0x820d3d08   1024      0x438   0x1f0001 Mutant          HGFSMUTEX
0x81eec100   1024      0x488   0x1f0001 Mutant          _!SHMSFTHISTORY!_
0x8221f170   1024      0x490   0x1f0001 Mutant          _SHuassist.mtx
0x81f9e3f0   1024      0x4c0   0x1f0001 Mutant
0x81ff5880   1024      0x4c4   0x1f0001 Mutant
0x82147f18   1024      0x4c8   0x1f0001 Mutant
0x820d8fa0   1024      0x4d4   0x1f0001 Mutant
0x81e83f48   1024      0x4dc   0x1f0001 Mutant          MidiMapper_Configure
0x81fe6670   1024      0x4e0   0x1f0001 Mutant          MidiMapper_modLongMessage_RefCnt
0x8223f608   1024      0x508   0x1f0001 Mutant          c:!documents and settings!networkuser!local settings!history!history.ie5!mshist012020110920201110!
```

Figure 20

Mutex of msimn.exe

```
C:\Coursework2>volatility_2.6_win64_standalone.exe -f cwRAM.mem handles -p 524 -t Mutant
Volatility Foundation Volatility Framework 2.6
Offset(V)     Pid     Handle     Access Type             Details
---------- ------ ---------- ---------- ---------------- -------
0x821452c0    524       0x38   0x1f0001 Mutant           OutlookExpress_InstanceMutex_101897
0x81efc3e0    524       0x78   0x1f0001 Mutant
0x8206dd68    524       0x80   0x1f0001 Mutant
0x81e3b168    524       0xb4   0x100000 Mutant           _!MSFTHISTORY!_
0x81fd3550    524       0xbc   0x100000 Mutant           c:!documents and settings!networkuser!local settings!temporary internet files!content.ie5!
0x8206a588    524       0xc4   0x100000 Mutant           c:!documents and settings!networkuser!cookies!
0x81e31558    524       0xd0   0x100000 Mutant           c:!documents and settings!networkuser!local settings!history!history.ie5!
0x8204e748    524       0xf0   0x100000 Mutant           WininetStartupMutex
0x822f9270    524       0xf8   0x100000 Mutant           WininetConnectionMutex
0x8224f2b0    524       0xfc   0x1f0001 Mutant
0x81e50aa8    524      0x100   0x100000 Mutant           WininetProxyRegistryMutex
0x81fea690    524      0x17c   0x1f0001 Mutant           MSIdent Logon
0x821452c0    524      0x1a4   0x1f0001 Mutant           OutlookExpress_InstanceMutex_101897
0x81fc0a48    524      0x1b4   0x1f0001 Mutant
0x82099dd8    524      0x1bc   0x1f0001 Mutant
0x81ef5dd8    524      0x1c0   0x1f0001 Mutant
0x821ed770    524      0x1f0   0x1f0001 Mutant           microsoft_thor_folder_notifyinfo_mutex
0x81ef5268    524      0x1fc   0x1f0001 Mutant           c:_documents and settings_networkuser_local settings_application data_identities_{7ac41542-893c-40b2-9083-1dbbbb22a
af3}_microsoft_outlook express_folders.dbx_directdbmutex
0x820dcdc8    524      0x200   0x1f0001 Mutant
0x8206b1f8    524      0x228   0x1f0001 Mutant           c:_documents and settings_networkuser_local settings_application data_identities_{7ac41542-893c-40b2-9083-1dbbbb22a
af3}_microsoft_outlook express_offline.dbx_directdbmutex
0x821eb280    524      0x244   0x1f0001 Mutant           MPSWabDataAccessMutex
0x821e3a20    524      0x24c   0x1f0001 Mutant           MPSWABOlkStoreNotifyMutex
0x822475e0    524      0x278   0x1f0001 Mutant           Toolbar Notificationsmutex
0x821ed770    524      0x284   0x1f0001 Mutant           microsoft_thor_folder_notifyinfo_mutex
0x822f99d8    524      0x298   0x1f0001 Mutant           Outlook Express Outlook Bar Notifymutex
0x821e3a20    524      0x30c   0x1f0001 Mutant           MPSWABOlkStoreNotifyMutex
0x81f2c268    524      0x334   0x1f0001 Mutant
0x81ef3270    524      0x350   0x1f0001 Mutant           CTF.LBES.MutexDefaultS-1-5-21-1614895754-261478967-839522115-1003
0x81e31998    524      0x354   0x1f0001 Mutant           CTF.Compart.MutexDefaultS-1-5-21-1614895754-261478967-839522115-1003
0x81e2c600    524      0x358   0x1f0001 Mutant           CTF.Asm.MutexDefaultS-1-5-21-1614895754-261478967-839522115-1003
```

Figure 21

CWIMAGE.DD

DOCUMENTS FOUND

CARVED FILES

Carved files are the files recovered from the system.

Browsing files in the $CarvedFiles folder received one file shown in the figure 19

/img_cwimage.dd//$CarvedFiles 1 Results

Table Thumbnail Summary

Save Table as CSV

Name	S	C	O	Modified Time	Change Time	Access Time	Created Time	Size	Flags(Dir)	Flags(Meta)	Known	Location
f0000000.xls			0	0000-00-00 00:00:00	0000-00-00 00:00:00	0000-00-00 00:00:00	0000-00-00 00:00:00	25600	Unallocated	Unallocated	unknown	/img_cwimage.dd

Figure 22

The file contains data shown in the figure 20

BANK	ACC NUMBER	LOGIN	PIN	Value
RBS	557799	459454	4632	£15,600
Lloyds	468746168	67651	1188	£3,05,000
NatWest	874654	3146	6254	£2,57,766

Figure 23

The figure 20 clearly stats the file contains sensitive data. The data is about bank names, account numbers, login ids, pin and bank balance. According to the Metadata of the Autopsy, following information can be seen.

1. Author of the file is Harris
2. File was created at 2020-10-13T23:49:26
3. The file was last accessed by the same author that is Harris
4. The file was last modified at 2020-10-13T23:52:51
5. The file was last saved at 2020-10-13T23:52:51
6. The file was created by Harris

UNALLOCATED FILES

Unallocated Files are stored in Unalloc folder. The folder contains data from unallocated blogs of the system which are organised and can be found in folder Unalloc.

The file is large. In some readable texts, a file is containing information very similar to the information which was contained by CarvedFiles. The information can be seen in figure 21

BANK	ACC NUMBER	LOGIN	PIN	Value
RBS	557799		459454	4632
15,600				
Lloyds	468746168	67651	1188	
305,000				
NatWest	874654		3146	6254
257,766				

Figure 24

The file is 1057243136 bytes which is around 1057.243136 MB. To check the file whether it is a malware or not, the file was converted to SHA256 which can be seen in figure 22

```
C:\Coursework2>certutil -hashfile "Unalloc_Recovered" SHA256
SHA256 hash of Unalloc_Recovered:
38cff0ced34198fc09de59f44480f7936abe829b0aaefe034a13a3e3f5bca575
CertUtil: -hashfile command completed successfully.
```

Figure 25

Uploading the hash on the https://virustotal.com I found the following result. Hash used to find is **38CFF0CED34198FC09DE59F44480F7936ABE829B0AAEFE034A13A3E3F5BCA575**

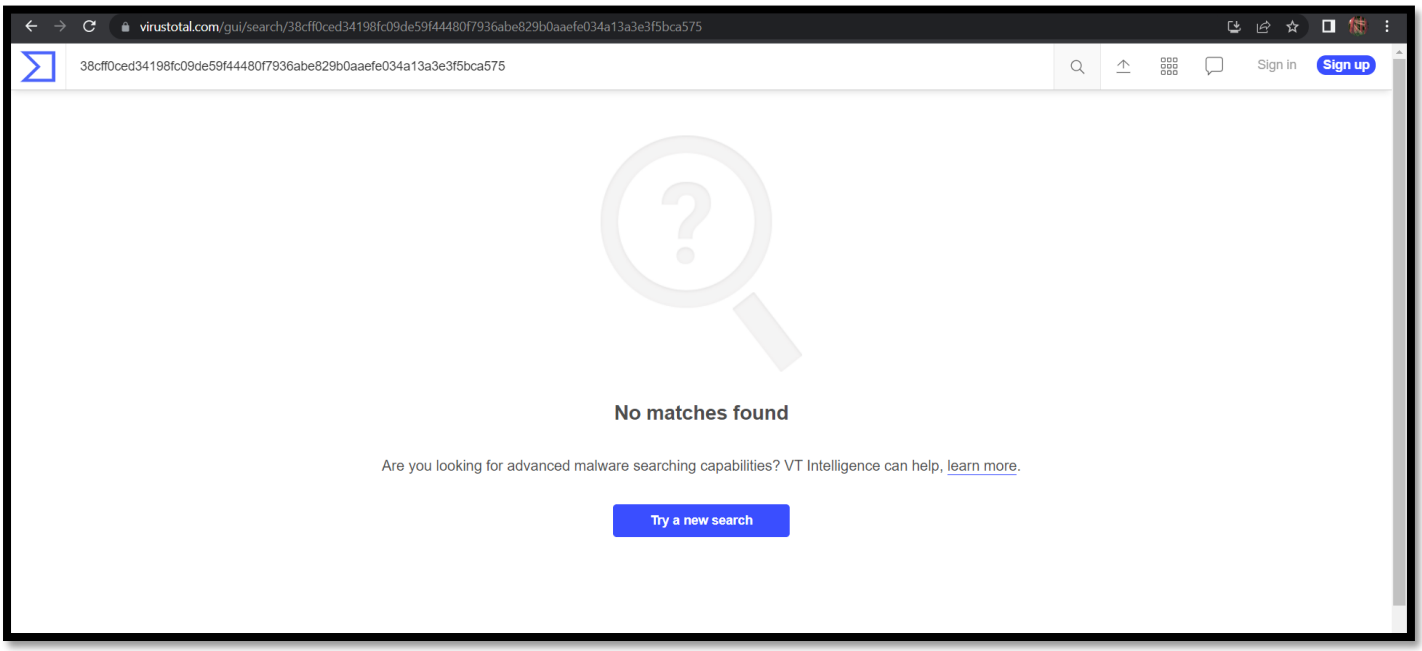


Figure 25

The hash wasn't found which can be confirmed as the file is not malware or any other virus.

EXECUTABLES FOUND ON IMAGE

There is only one executable found on the system. The file is shown in following figure 24

.exe 1 Results

Table Thumbnail Summary

Save Table as CSV

Name	S	C	O	Modified Time	Change Time	Access Time	Created Time	Size	Flags(Dir)	Flags(Meta)	Known	Locat
Tetris.exe			0	2020-11-09 23:25:50 GMT	0000-00-00 00:00:00	2020-11-09 00:00:00 GMT	2020-11-09 23:25:51 GMT	73802	Allocated	Allocated	unknown	/img_

Figure 26

As the file executable, the file seems suspicious. The name Tetris refers to one of the greatest and legendary computer games ever made. The game renders as figure 25

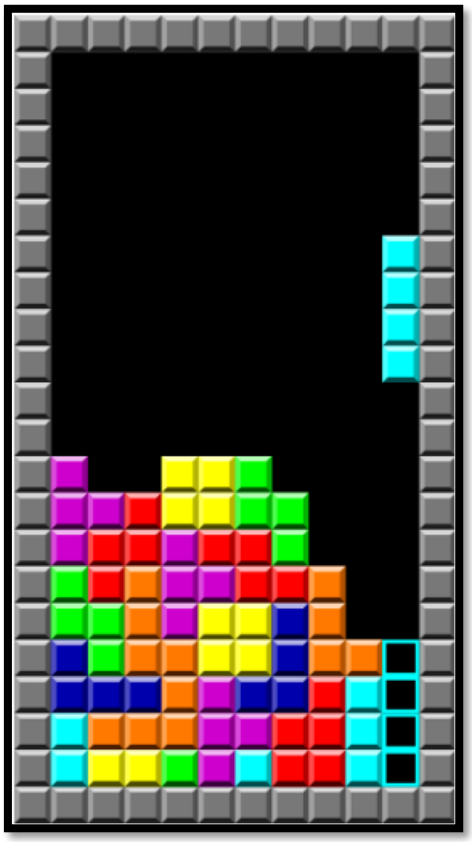


Figure 27

As the file is executable, it grabs some interest as it has high chances of being a virus or any malware. And the name must be given a person to trick and run the executable.

To check the file, the SHA256 of the file was searched on virustotal and it was found that the file is strong virus.

It can be seen in the figure 26

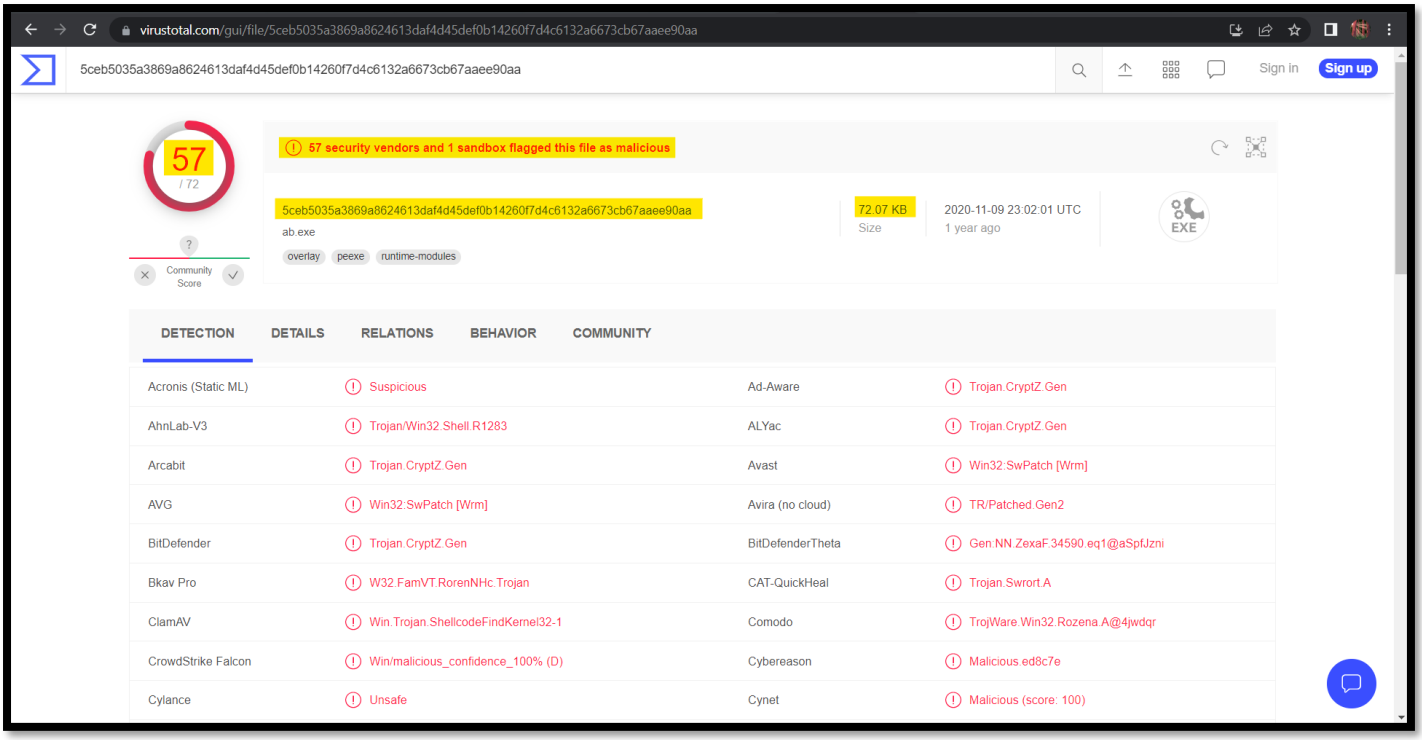
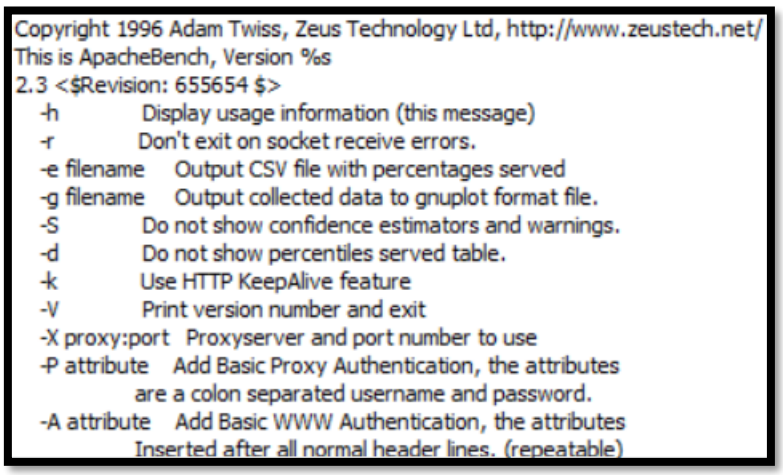


Figure 28

The file is a highly malicious.

The specifications of the file as follow

1. The file was created on 2020-11-09 23:25:51 GMT
2. The file was accessed on 2020-11-09 00:00:00 GMT
3. The file was modified on 2020-11-09 23:25:50 GMT
4. The file contains information related to Apache and also the usage is shown. For reference figure 27 can be referred.



```
Copyright 1996 Adam Twiss, Zeus Technology Ltd, http://www.zeustech.net/
This is ApacheBench, Version %s
2.3 <$Revision: 655654 $>
    -h          Display usage information (this message)
    -r          Don't exit on socket receive errors.
    -e filename     Output CSV file with percentages served
    -g filename     Output collected data to gnuplot format file.
    -S          Do not show confidence estimators and warnings.
    -d          Do not show percentiles served table.
    -k          Use HTTP KeepAlive feature
    -V          Print version number and exit
    -X proxy:port   Proxyserver and port number to use
    -P attribute    Add Basic Proxy Authentication, the attributes
                    are a colon separated username and password.
    -A attribute    Add Basic WWW Authentication, the attributes
                    Inserted after all normal header lines. (repeatable)
```

Figure 29

INTERESTING FILES

There is total three files in the Deleted Files. All the three files share the same contents. The files can be referred from figure 28. Interesting to know that the files are deleted files on the system

Name	S	C	O	Modified Time	Change Time	Access Time	Created Time	Size	Flags(Dir)	Flags(Meta)	Known
GreenAccounts.txt				2020-10-18 23:45:40 BST	0000-00-00 00:00:00	2020-11-09 00:00:00 GMT	2020-11-09 22:52:32 GMT	140	Unallocated	Unallocated	unknown
GreenAccounts.xls				2020-10-14 00:52:52 BST	0000-00-00 00:00:00	2020-11-09 00:00:00 GMT	2020-11-09 22:52:32 GMT	25600	Unallocated	Unallocated	unknown
f0000000.xls			0	0000-00-00 00:00:00	0000-00-00 00:00:00	0000-00-00 00:00:00	0000-00-00 00:00:00	25600	Unallocated	Unallocated	unknown

Figure 30

The contents of the file are as same as shown in the figure 21

1. GreenAccounts.txt

The file contains same information as shown in figure 21. The details are as same as figure 20.

2. GreenAccounts.xls

The file contains same information as shown in figure 21.The details are as same as figure 20.

3. f0000000.xls

The file contains same information as shown in figure 21. The details are as same as figure 20

Other than this, there are pdf, images, power point presentation but nothing is interesting.

EXPLAINING FORENSIC TECHNIQUE USED

SOFTWARES USED

1. RAM Image Processing (.mem)

   - volatility 2.6 win64 standaloneFile

2. Disk Image Processing (.dd)

   - Autopsy 4.19.3

QUERIES RUN

ID	Refer to	Query Fired	Result
1	Figure 1	volatility_2.6_win64_standalone.exe -f cwRAM.mem imageinfo	The result shows the information of an image. Contains basic information like time, date, architecture, profile, and basic system information
2	Figure 2	volatility_2.6_win64_standalone.exe -f cwRAM.mem --profile=WinXPSP2x86 pslist	The result shows the list of the tasks going on the system when the image was captured.
3	Figure 3	volatility_2.6_win64_standalone.exe -f cwRAM.mem --profile=WinXPSP2x86 pstree	The result shows the tree structure of the process going on the system. It shows the parent and child process behind ever process
4	Figure 4	volatility_2.6_win64_standalone.exe -f cwRAM.mem --profile=WinXPSP2x86 connscan	Shows the incoming and outgoing connections on the system at a time
5	Figure 5	volatility_2.6_win64_standalone.exe -f cwRAM.mem --profile=WinXPSP2x86 connections	Shows the current ongoing connectivity on the system
6	Figure 6	volatility_2.6_win64_standalone.exe -f cwRAM.mem --profile=WinXPSP2x86 sockscan	Scans the connections and displays the protocol of connections as well
7	Figure 7	volatility_2.6_win64_standalone.exe -f cwRAM.mem --profile=WinXPSP2x86 sockets	Shows active connections with protocol on the system connectivity
8	Figure 8	volatility_2.6_win64_standalone.exe -f cwRAM.mem --profile=WinXPSP2x86 hivelist	Shows the hives captured on the system
9	Figure 9	volatility_2.6_win64_standalone.exe -f cwRAM.mem --profile=WinXPSP2x86 printkey	Shows the keys on the system

10	Figure 10	cvolatility_2.6_win64_standalone.exe -f cwRAM.mem --profile=WinXPSP2x86 printkey -o 0xe1037008 -K "ControlSet001\Control\ComputerName\ComputerName"	Shows the name of the system
11	Figure 11	Volatility_2.6_win64.exe -f cwRAM.mem –profile=WinXPSP2x86 printkey -o 0xe1037008 -K "ControlSet001\Enum\USBSTOR\Disk&Ven_USB2.0&Prod_Flash_Disk&Rev_2.60\2015051116580671&0”	Shows the Devices attached to the system
12	Figure 12	volatility_2.6_win64_standalone.exe -f cwRAM.mem --profile=WinXPSP2x86 printkey -o 0xe1037008 -K "ControlSet001\Control\Windows"	Shows the last time the system was shutdown
13	Figure 13	volatility_2.6_win64_standalone.exe -f cwRAM.mem --profile=WinXPSP2x86 printkey -o 0xe1037008 -K "ControlSet001\Control\TimeZoneInformation"	Shows the time zone of the system
14	Figure 14	volatility_2.6_win64_standalone.exe -f cwRAM.mem --profile=WinXPSP2x86 printkey -o 0xe179eb60 -K "SAM\Domains\Account\Users\Names"	Shows User accounts on the system
15	Figure 17	>volatility_2.6_win64_standalone.exe -f cwRAM.mem handles -p <PID_of_file> -t Mutant	Finding Mutex of the executable files
16	Figure 16	./volatility_2.6_lin64_standalone -f cwRAM.mem profile=WinXPSP2x86 dumpfiles -Q 0x00000000021d68a0 --name file -D ~/volatility_2.6_lin64_standalone	Recovered Tetris.exe successfully from the system image.

From figure 4 PID 1024, 1564 and 524 are dealing with network activities and with the help of figure 2, we can see that the process is IEXPLORE.exe, PuTTytel.exe and minmn.exe. Going to the figure 3, IEXPLORE.exe, PuTTytel.exe and msimn.exe are the child process of explorer.exe.

As these processes are showing network activities, digging down in the mutual exclusion objects (mutex) created by these processes have possibility to reveal infection. While gathering the mutex of three processes, there were no mutex found for PuTTytel.exe.

From figure 5 and 2, its puttytl.exe which has open connection between these two IP addresses. This can be matched with the PID. PuTTytyl.exe is used for connectivity between two computers specially on windows PC.

From the mutex caught of PID 1024 that is IEXPLORE.exe, there are two suspicious mutex found which are ShimCacheMutex and WininetProxyRegistryMutex and there was no suspicious mutex found on PID 524.

Understanding ShimCacheMutex and WininetProxyRegistryMutex

1. ShimCacheMutex

Searching ShimCacheMutex on https://virustotal.com has given the following output. The SHA256 of ShimCacheMutex is as follow 5789793b9e2d83a895edace975cf5f970858b17b19166f4cacaf7b8719f286ab.

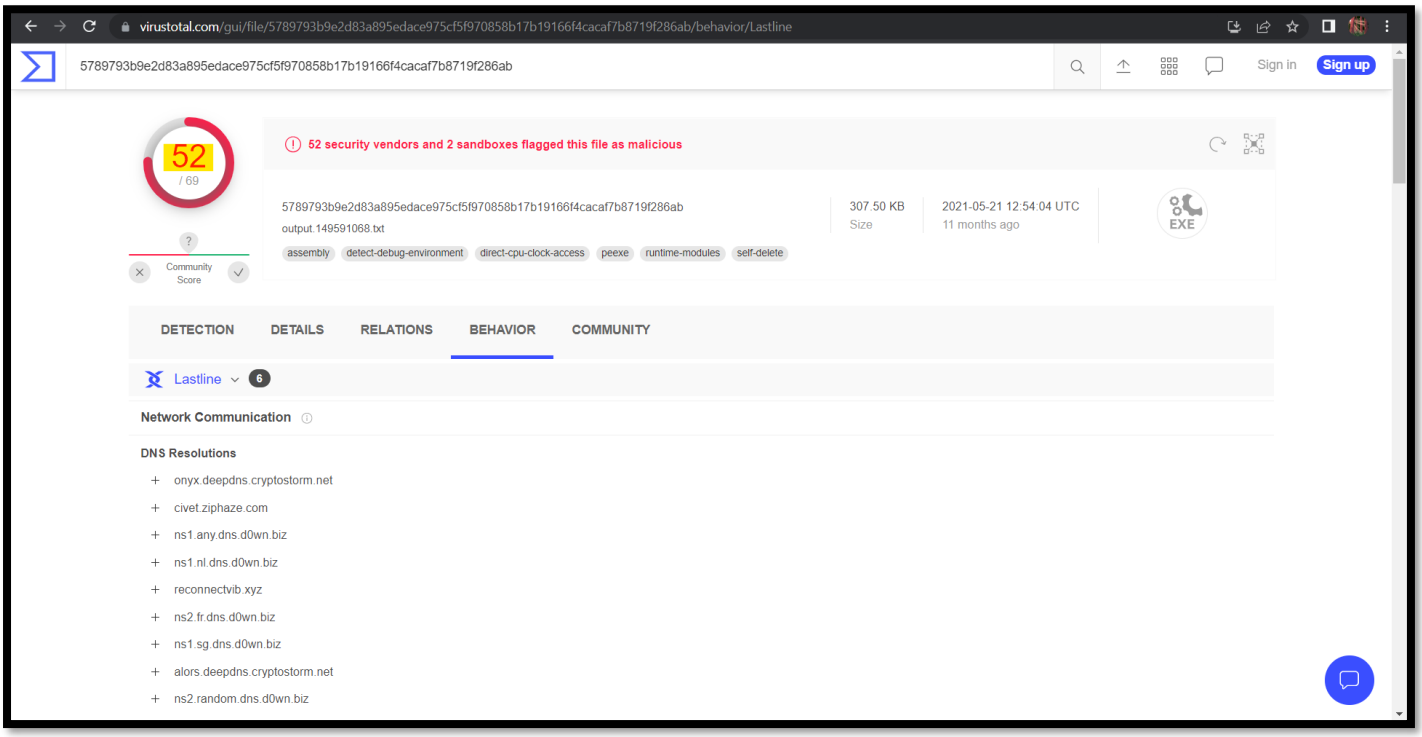


Figure 31

2. WininetProxyRegistryMutex

Searching WininetProxyRegistryMutex on https://virustotal.com has given the following output. Which ultimately confirms that the mutext WininetProxyRegistryMutex is a malware.

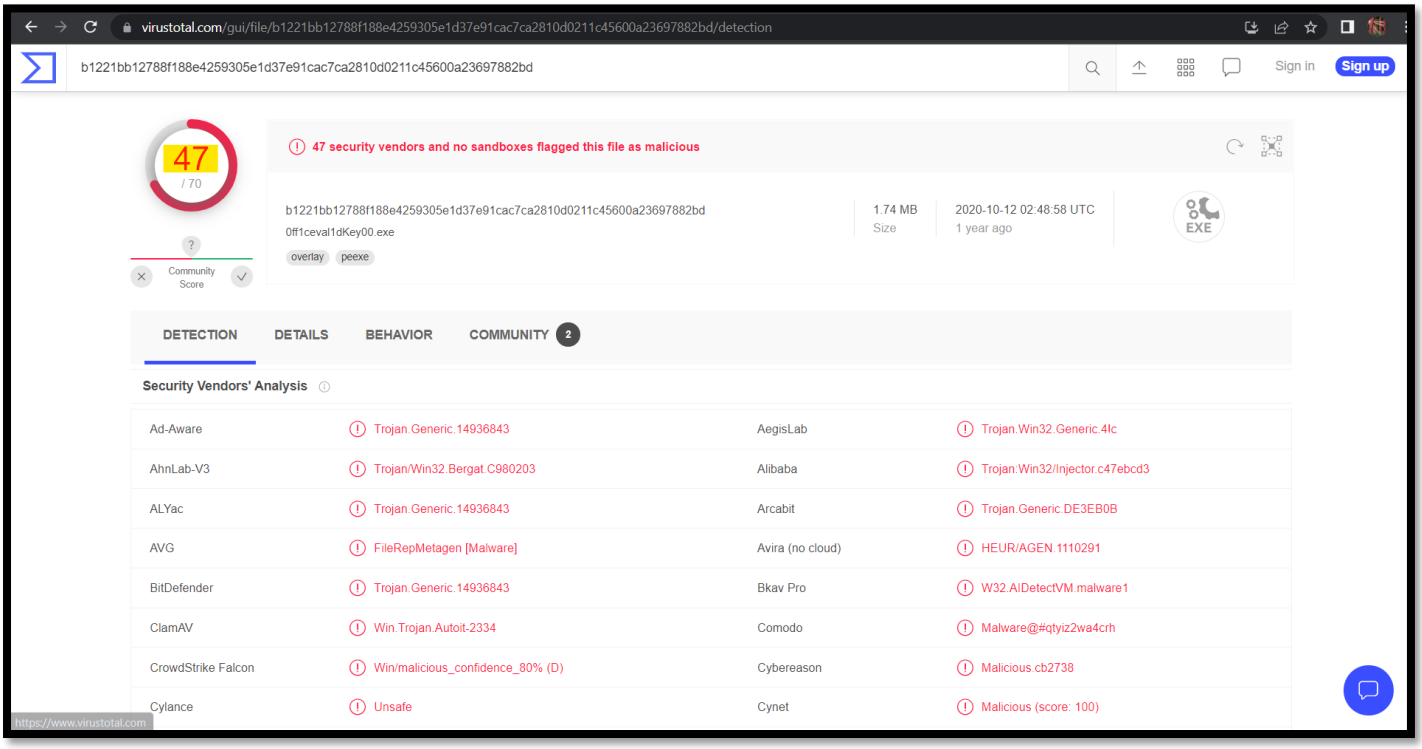


Figure 32

CONCLUSION

Considering all the above evidence, a conclusion can be formed.

A user named Harris has been read, write and accessed a file containing critical information called as GreenAccounts.txt. The file contains information related banking having account number, pin and bank balance as well. The file GreenAccounts appears in two formats which are .txt and .xls. The files are recovered from the Deleted file sections. There is also on executable file named Tetris.exe which is running on the system. The file Tetris.exe is a malware according to the https.//virustotal.com. Tetrix.exe contains an Apache Interactive flags which leads to the a confusion. Understanding the Text content of the file Tetris.exe it can also be said that the file is a backdoor. A user has been tricked to click and run the Tetris.exe on a system to establish a backdoor. Here the name Tetris.exe is given purposely because Tetris is the name of one of the legendary computer games ever created in the early stage of gaming.

Here the IP of the system is 192.168.1.11 and the connections going to the IP address of 192.168.1.251 and 192.168.1.250. From the Memory Image, the process called as PuTTytl.exe is running. The PuTTytl.exe is nothing but the connectivity between two computers using SSH or Telnet tunnelling. Here the connectivity under PuTTY can be see on IP address 192.168.1.11 and 192.168.1.250. Therefore it can be possible that the user has established a backdoor with the help of Tetris.exe or PuTTY is used to backdoor as well. But the PuTTY was not flagged as a malware in the system, the entire doubt goes on Tetrix.exe only.

Beyond Tetrix.exe and PuTTY, there are two malicious process going on the system which are IEXPLORE.exe and msimn.exe. Both the process are managing the network connectivity from the system to both the external IP addresses mentioned above.

Understanding the IEXPLORE.exe, this executable file is an malware according to the TotalVirus. This executable file is having multiple mutual exclusion objects. Two of them are highly dangerous. One belongs to the Malware and one as an Adware. This can be concluded as the Tetris.exe has downloaded this IEXPLORE.exe and the file is malicious.

Another executable file called msimn.exe also has the mutex, but none of them belongs to any suspicious behaviour.

Therefore, it can be said that, the user Harris has tricked a user to download and run Tetrix.exe which allowed him to enter in the victim’s machine unauthorisedly. Then the user Harris accessed critical information that is GreenAccounts.txt from the victim’s machine and deleted all the files having same data from the users system as well.

REFERENCE

1. HACKTRICKS.XYZ. (2016). VOLATILITY - CHEATSHEET - HACKTRICKS. [online] Available at: https://book.hacktricks.xyz/forensics/basic-forensic-methodology/memory-dump-analysis/volatility-examples [Accessed 20 Apr. 2022].

2. NEVES, V. (2019). [CTF] Getting values from Registry with Volatility. [online] !debugger present! Available at: https://dbgpresent.wordpress.com/2019/09/11/ctf-getting-values-from-registry-with-volatility/ [Accessed 20 Apr. 2022].

3. LUCIDEUS (2018). Windows Registry Forensic Analysis Part 1 — Windows Forensics Manual 2018. [online] Medium. Available at: https://medium.com/@lucideus/windows-registry-forensic-analysis-part-1-windows-forensics-manual-2018-2cb4da210125.

4. ACCESSDATA REGISTRY QUICK FIND CHART. (n.d.). [online] Available at: https://cryptome.org/isp-spy/access-data-spy1.pdf [Accessed 20 Apr. 2022].

5. EGNYTE. (n.d.). 365.pdf on Egnyte. [online] Available at: https://sansorg.egnyte.com/dl/LVvF5jRNLK [Accessed 20 Apr. 2022].

6. SLEUTHKIT.ORG. (n.d.). Autopsy User Documentation: PhotoRec Carver Module. [online] Available at: https://sleuthkit.org/autopsy/docs/user-docs/3.1/photorec_carver_page.html.

7. MALWARETIPS Community. (n.d.). Malware Writeup: Complete AutoIt Malware Analysis. [online] Available at: https://malwaretips.com/threads/malware-writeup-complete-autoit-malware-analysis.50496/ [Accessed 20 Apr. 2022].