PROJECT REPORT

Name: Tanmay Kale
Email: tkale1@binghamton.edu
Subject: CS458-Computer Security

Project Assignment 4

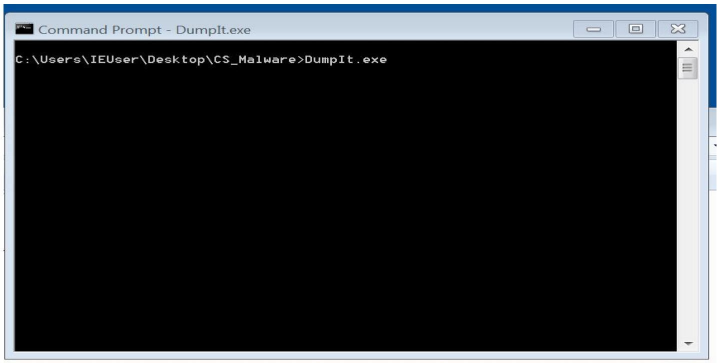
To learn how to find traces of malware infection using memory forensic tools(Volatility).

To Install Volatility and Necessary Software's:

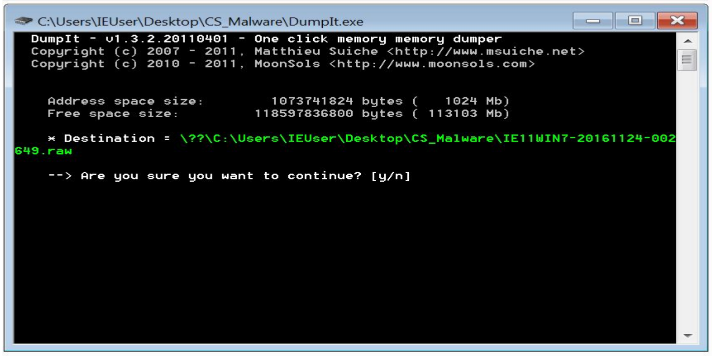
1. **Download Volatility.2.5-Standalone.exe:** This is a standalone application for Volatility software. It requires Python to run.
2. **Download DUMPIT:** The **DumpIt** provides an efficient way to acquire physical memory and save it on your disk. It saves the memory in raw file format.
3. **Python27:** It is required as a prerequisite for Volatility2.5-Standalone.exe

Procedure to Use Volatility:

1. Open terminal
2. Create a RAW File of the physical memory.
C:\Users\IRUser\Desktop\CS_Malware\DumpIt.exe



```
C:\Users\IEUser\Desktop\CS_Malware>DumpIt.exe
```



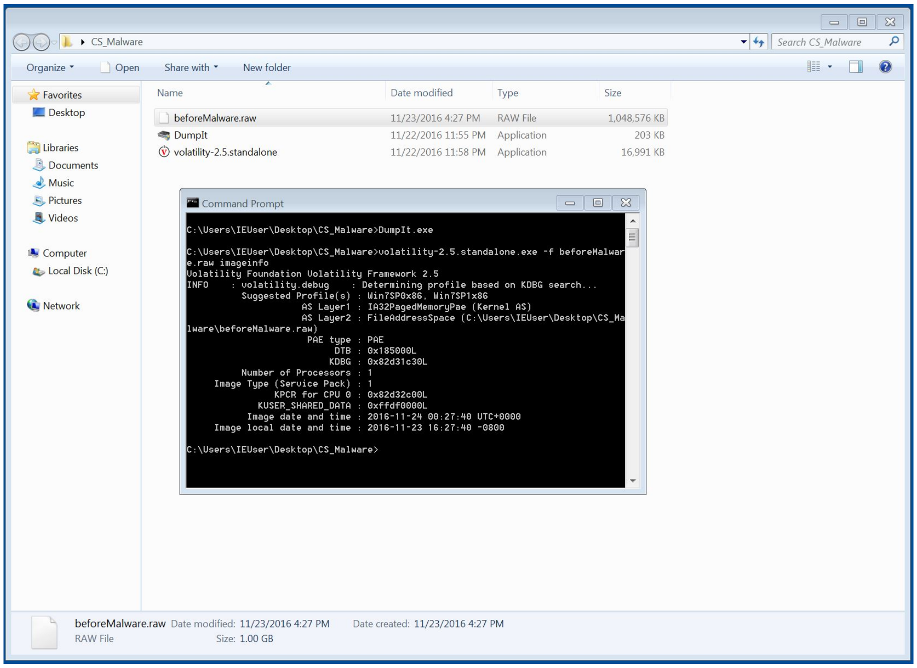
```
  DumpIt - v1.3.2.20110401 - One click memory memory dumper
  Copyright (c) 2007 - 2011, Matthieu Suiche <http://www.msuiche.net>
  Copyright (c) 2010 - 2011, MoonSols <http://www.moonsols.com>


    Address space size:        1073741824 bytes (   1024 Mb)
    Free space size:         118597836800 bytes ( 113103 Mb)

    * Destination = \??\C:\Users\IEUser\Desktop\CS_Malware\IE11WIN7-20161124-002
649.raw

    --> Are you sure you want to continue? [y/n]
```

3. Use the imageinfo on the generated raw file to determine the suggested profile for the operating system.
   C:\Users\IRUser\Desktop\CS_Malware\volatility-2.5.standalone.exe –f beforeMalware.raw imageinfo



Name	Date modified	Type	Size
beforeMalware.raw	11/23/2016 4:27 PM	RAW File	1,048,576 KB
DumpIt	11/22/2016 11:55 PM	Application	203 KB
volatility-2.5.standalone	11/22/2016 11:58 PM	Application	16,991 KB

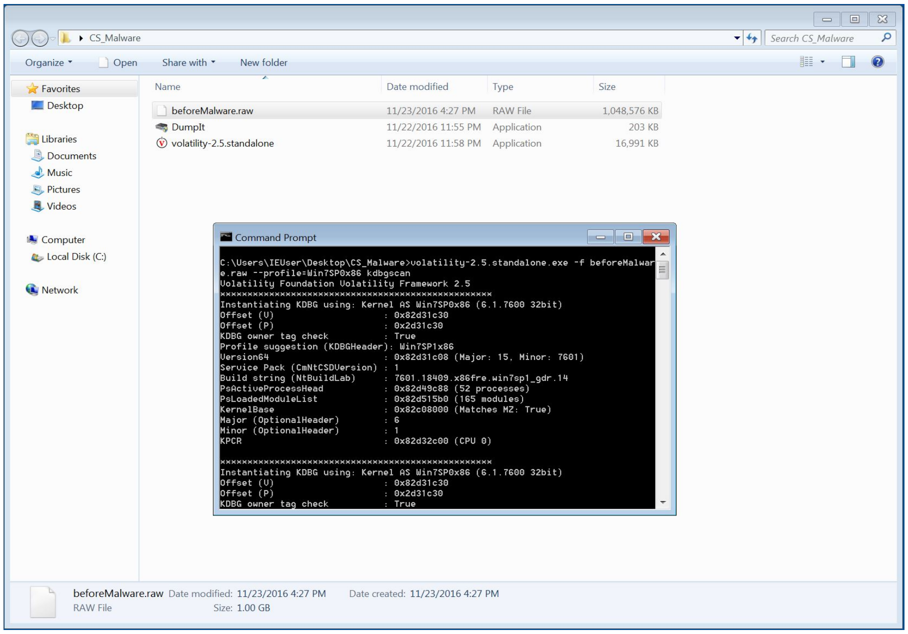
```
C:\Users\IEUser\Desktop\CS_Malware>DumpIt.exe

C:\Users\IEUser\Desktop\CS_Malware>volatility-2.5.standalone.exe -f beforeMalwar
e.raw imageinfo
Volatility Foundation Volatility Framework 2.5
INFO    : volatility.debug    : Determining profile based on KDBG search...
          Suggested Profile(s) : Win7SP0x86, Win7SP1x86
                     AS Layer1 : IA32PagedMemoryPae (Kernel AS)
                     AS Layer2 : FileAddressSpace (C:\Users\IEUser\Desktop\CS_Ma
lware\beforeMalware.raw)
                      PAE type : PAE
                           DTB : 0x185000L
                          KDBG : 0x82d31c30L
          Number of Processors : 1
     Image Type (Service Pack) : 1
                KPCR for CPU 0 : 0x82d32c00L
             KUSER_SHARED_DATA : 0xffdf0000L
           Image date and time : 2016-11-24 00:27:40 UTC+0000
     Image local date and time : 2016-11-23 16:27:40 -0800

C:\Users\IEUser\Desktop\CS_Malware>
```

beforeMalware.raw Date modified: 11/23/2016 4:27 PM Date created: 11/23/2016 4:27 PM
RAW File Size: 1.00 GB

4. The output of the imageinfo gives us the offset address of the suggested profile.
   C:\Users\IRUser\Desktop\CS_Malware\volatility-2.5.standalone.exe –f beforeMalware.raw –profile=Win7SP1x86 kdbgscan



Name	Date modified	Type	Size
beforeMalware.raw	11/23/2016 4:27 PM	RAW File	1,048,576 KB
DumpIt	11/22/2016 11:55 PM	Application	203 KB
volatility-2.5.standalone	11/22/2016 11:58 PM	Application	16,991 KB

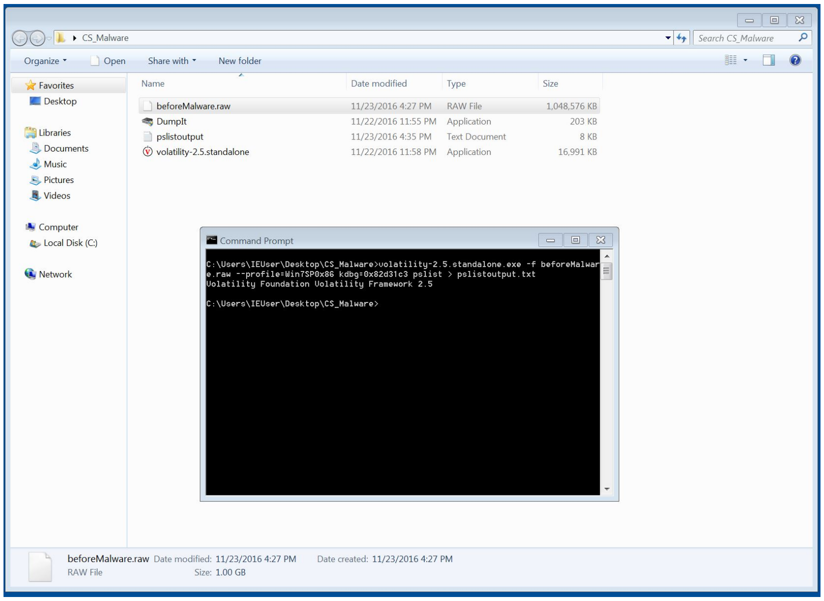
```
C:\Users\IEUser\Desktop\CS_Malware>volatility-2.5.standalone.exe -f beforeMalwar
e.raw --profile=Win7SP0x86 kdbgscan
Volatility Foundation Volatility Framework 2.5
**************************************************
Instantiating KDBG using: Kernel AS Win7SP0x86 (6.1.7600 32bit)
Offset (V)                    : 0x82d31c30
Offset (P)                    : 0x2d31c30
KDBG owner tag check          : True
Profile suggestion (KDBGHeader): Win7SP1x86
Version64                     : 0x82d31c08 (Major: 15, Minor: 7601)
Service Pack (CmNtCSDVersion) : 1
Build string (NtBuildLab)     : 7601.18409.x86fre.win7sp1_gdr.14
PsActiveProcessHead           : 0x82d49c88 (52 processes)
PsLoadedModuleList            : 0x82d515b0 (165 modules)
KernelBase                    : 0x82c08000 (Matches MZ: True)
Major (OptionalHeader)        : 6
Minor (OptionalHeader)        : 1
KPCR                          : 0x82d32c00 (CPU 0)

**************************************************
Instantiating KDBG using: Kernel AS Win7SP0x86 (6.1.7600 32bit)
Offset (V)                    : 0x82d31c30
Offset (P)                    : 0x2d31c30
KDBG owner tag check          : True
```

beforeMalware.raw Date modified: 11/23/2016 4:27 PM Date created: 11/23/2016 4:27 PM
RAW File Size: 1.00 GB

5. **Determine the effects of malware:** After this we use the offset address as an input to the kdbg along with the required Volatility command to scan the raw file and to analyze the system for any malware. Here I have used pslist which gives the list of all the processes which were running on the system before dumping the memory along with its details. C:\Users\IRUser\Desktop\CS_Malware\volatility-2.5.standalone.exe –f beforeMalware.raw –profile=Win7SP1x86 kdbg=0x82d31c3 pslist > pslistoutput.txt

5.1 pslist: store the output to pslistoutput.txt



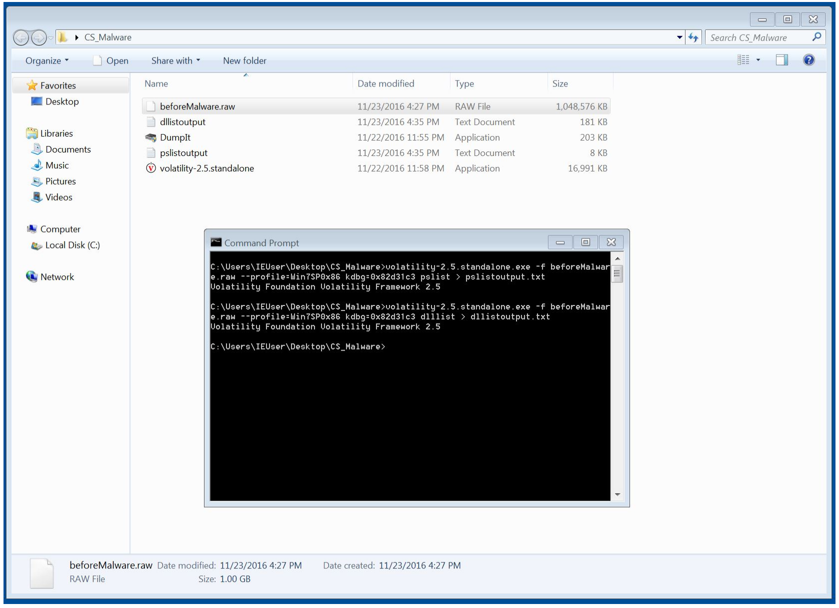
Name	Date modified	Type	Size
beforeMalware.raw	11/23/2016 4:27 PM	RAW File	1,048,576 KB
DumpIt	11/22/2016 11:55 PM	Application	203 KB
pslistoutput	11/23/2016 4:35 PM	Text Document	8 KB
volatility-2.5.standalone	11/22/2016 11:58 PM	Application	16,991 KB

```
C:\Users\IEUser\Desktop\CS_Malware>volatility-2.5.standalone.exe -f beforeMalwar
e.raw --profile=Win7SP0x86 kdbg=0x82d31c3 pslist > pslistoutput.txt
Volatility Foundation Volatility Framework 2.5

C:\Users\IEUser\Desktop\CS_Malware>
```

beforeMalware.raw Date modified: 11/23/2016 4:27 PM Date created: 11/23/2016 4:27 PM
RAW File Size: 1.00 GB

5.2 dlllist – store the output to dllistoutput.txt



Name	Date modified	Type	Size
beforeMalware.raw	11/23/2016 4:27 PM	RAW File	1,048,576 KB
dllistoutput	11/23/2016 4:35 PM	Text Document	181 KB
DumpIt	11/22/2016 11:55 PM	Application	203 KB
pslistoutput	11/23/2016 4:35 PM	Text Document	8 KB
volatility-2.5.standalone	11/22/2016 11:58 PM	Application	16,991 KB

```
C:\Users\IEUser\Desktop\CS_Malware>volatility-2.5.standalone.exe -f beforeMalwar
e.raw --profile=Win7SP0x86 kdbg=0x82d31c3 pslist > pslistoutput.txt
Volatility Foundation Volatility Framework 2.5

C:\Users\IEUser\Desktop\CS_Malware>volatility-2.5.standalone.exe -f beforeMalwar
e.raw --profile=Win7SP0x86 kdbg=0x82d31c3 dlllist > dllistoutput.txt
Volatility Foundation Volatility Framework 2.5

C:\Users\IEUser\Desktop\CS_Malware>
```

beforeMalware.raw Date modified: 11/23/2016 4:27 PM Date created: 11/23/2016 4:27 PM
RAW File Size: 1.00 GB

Malware analyzed:

1. **Keylogger Ardamax:** Ardamax Keylogger is a lite program that captures all activity of anyone using your computer and logs all keystrokes.
   Link: https://github.com/ytisf/theZoo/tree/master/malwares/Binaries

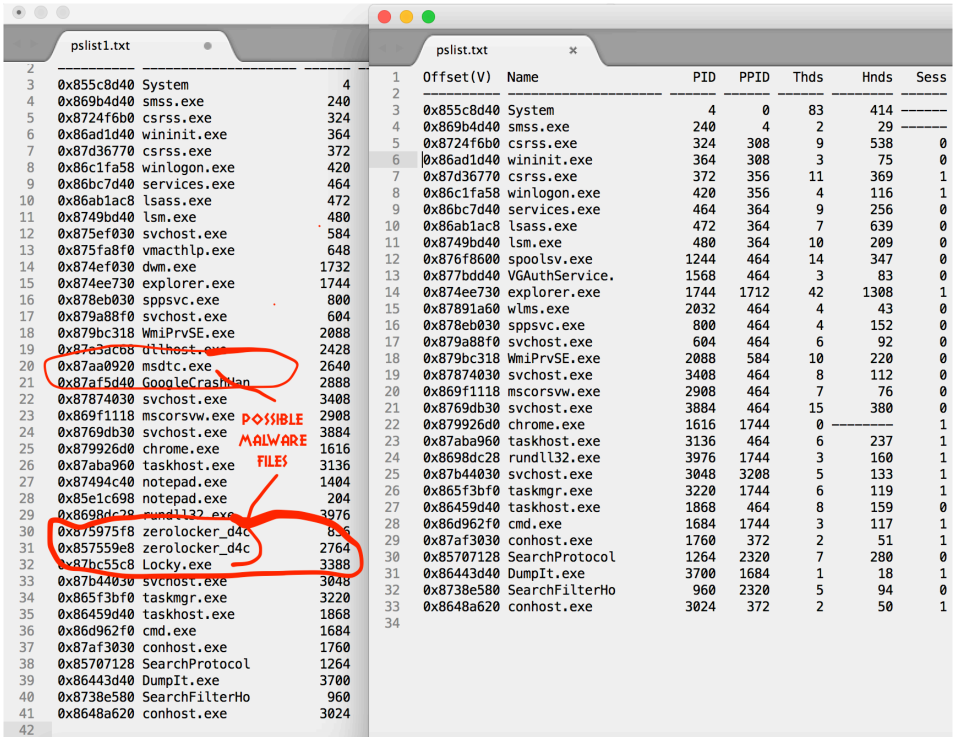
2. **Ransomware Locky:** But it's also the nickname of a new strain of ransomware, so-called because it renames all your important files so that they have the extension .locky
   Link: https://github.com/ytisf/theZoo/tree/master/malwares/Binaries/Ransomware.Locky

3. **Trojan Alienspy:** Alienspy is a Trojan horse that opens a back door on the compromised system.
   Link: https://github.com/ytisf/theZoo/tree/master/malwares/Binaries/Trojan.AlienSpy

4. **Zerolocker:** Zerolocker is new ransomware tool discovered by user which decrypts all computer data. It creates a folder zerolocker on your C:\ zerolocker drive which contains a dat file which has the ransom details stored in it.
   Link: https://github.com/ytisf/theZoo/tree/master/malwares/Binaries/ZeroLocker

Observations after running Malware:

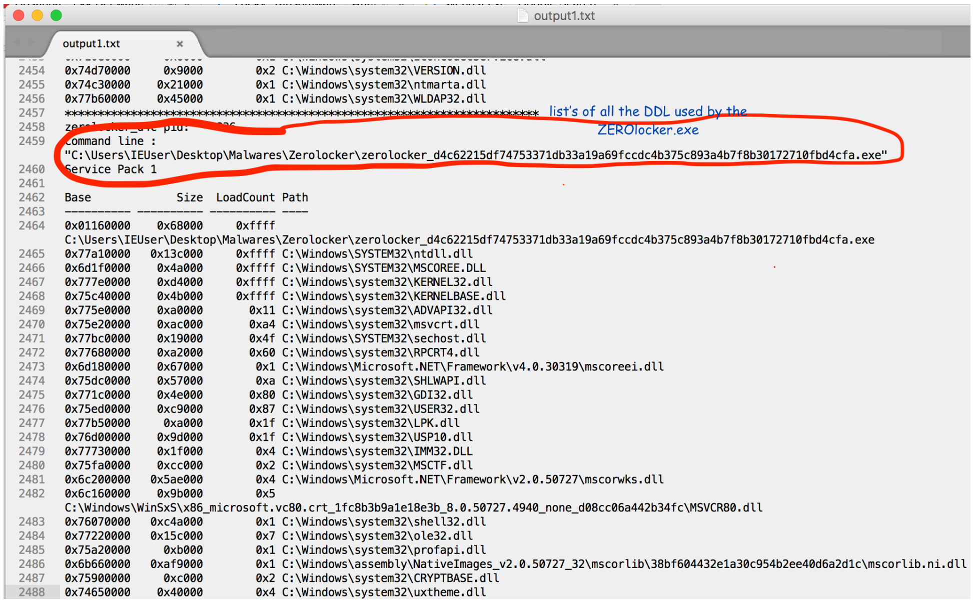
1. Comparing the output of pslist before and after running the zerolocker malware.



```
---------- -------------------- ------ -
0x855c8d40 System                    4
0x869b4d40 smss.exe                240
0x8724f6b0 csrss.exe               324
0x86ad1d40 wininit.exe             364
0x87d36770 csrss.exe               372
0x86c1fa58 winlogon.exe            420
0x86bc7d40 services.exe            464
0x86ab1ac8 lsass.exe               472
0x8749bd40 lsm.exe                 480
0x875ef030 svchost.exe             584
0x875fa8f0 vmacthlp.exe            648
0x874ef030 dwm.exe                1732
0x874ee730 explorer.exe           1744
0x878eb030 sppsvc.exe              800
0x879a88f0 svchost.exe             604
0x879bc318 WmiPrvSE.exe           2088
0x87a3ac68 dllhost.exe            2428
0x87aa0920 msdtc.exe              2640
0x87af5d40 GoogleCrashHan         2888
0x87874030 svchost.exe            3408
0x869f1118 mscorsvw.exe           2908
0x8769db30 svchost.exe            3884
0x879926d0 chrome.exe             1616
0x87aba960 taskhost.exe           3136
0x87494c40 notepad.exe            1404
0x85e1c698 notepad.exe             204
0x8698dc28 rundll32.exe           3976
0x875975f8 zerolocker_d4c          836
0x857559e8 zerolocker_d4c         2764
0x87bc55c8 Locky.exe              3388
0x87b44030 svchost.exe            3048
0x865f3bf0 taskmgr.exe            3220
0x86459d40 taskhost.exe           1868
0x86d962f0 cmd.exe                1684
0x87af3030 conhost.exe            1760
0x85707128 SearchProtocol         1264
0x86443d40 DumpIt.exe             3700
0x8738e580 SearchFilterHo          960
0x8648a620 conhost.exe            3024
```

```
Offset(V)  Name                    PID   PPID   Thds     Hnds   Sess
---------- -------------------- ------ ------ ------ -------- ------
0x855c8d40 System                    4      0     83      414 ------
0x869b4d40 smss.exe                240      4      2       29 ------
0x8724f6b0 csrss.exe               324    308      9      538      0
0x86ad1d40 wininit.exe             364    308      3       75      0
0x87d36770 csrss.exe               372    356     11      369      1
0x86c1fa58 winlogon.exe            420    356      4      116      1
0x86bc7d40 services.exe            464    364      9      256      0
0x86ab1ac8 lsass.exe               472    364      7      639      0
0x8749bd40 lsm.exe                 480    364     10      209      0
0x876f8600 spoolsv.exe            1244    464     14      347      0
0x877bdd40 VGAuthService.         1568    464      3       83      0
0x874ee730 explorer.exe           1744   1712     42     1308      1
0x87891a60 wlms.exe               2032    464      4       43      0
0x878eb030 sppsvc.exe              800    464      4      152      0
0x879a88f0 svchost.exe             604    464      6       92      0
0x879bc318 WmiPrvSE.exe           2088    584     10      220      0
0x87874030 svchost.exe            3408    464      8      112      0
0x869f1118 mscorsvw.exe           2908    464      7       76      0
0x8769db30 svchost.exe            3884    464     15      380      0
0x879926d0 chrome.exe             1616   1744      0 --------      1
0x87aba960 taskhost.exe           3136    464      6      237      1
0x8698dc28 rundll32.exe           3976   1744      3      160      1
0x87b44030 svchost.exe            3048   3208      5      133      1
0x865f3bf0 taskmgr.exe            3220   1744      6      119      1
0x86459d40 taskhost.exe           1868    464      8      159      0
0x86d962f0 cmd.exe                1684   1744      3      117      1
0x87af3030 conhost.exe            1760    372      2       51      1
0x85707128 SearchProtocol         1264   2320      7      280      0
0x86443d40 DumpIt.exe             3700   1684      1       18      1
0x8738e580 SearchFilterHo          960   2320      5       94      0
0x8648a620 conhost.exe            3024    372      2       50      1
```

2. Analyzing the dll’s used by the zerolocker.exe



```
0x74d70000     0x9000        0x2 C:\Windows\system32\VERSION.dll
0x74c30000    0x21000        0x1 C:\Windows\system32\ntmarta.dll
0x77b60000    0x45000        0x1 C:\Windows\system32\WLDAP32.dll
************************************************************************
zer[illegible]_d4c pid: [illegible]
Command line :
"C:\Users\IEUser\Desktop\Malwares\Zerolocker\zerolocker_d4c62215df74753371db33a19a69fccdc4b375c893a4b7f8b30172710fbd4cfa.exe"
Service Pack 1

Base             Size  LoadCount Path
---------- ---------- ---------- ----
0x01160000    0x68000     0xffff
C:\Users\IEUser\Desktop\Malwares\Zerolocker\zerolocker_d4c62215df74753371db33a19a69fccdc4b375c893a4b7f8b30172710fbd4cfa.exe
0x77a10000   0x13c000     0xffff C:\Windows\SYSTEM32\ntdll.dll
0x6d1f0000    0x4a000     0xffff C:\Windows\SYSTEM32\MSCOREE.DLL
0x777e0000    0xd4000     0xffff C:\Windows\system32\KERNEL32.dll
0x75c40000    0x4b000     0xffff C:\Windows\system32\KERNELBASE.dll
0x775e0000    0xa0000       0x11 C:\Windows\system32\ADVAPI32.dll
0x75e20000    0xac000       0xa4 C:\Windows\system32\msvcrt.dll
0x77bc0000    0x19000       0x4f C:\Windows\SYSTEM32\sechost.dll
0x77680000    0xa2000       0x60 C:\Windows\system32\RPCRT4.dll
0x6d180000    0x67000        0x1 C:\Windows\Microsoft.NET\Framework\v4.0.30319\mscoreei.dll
0x75dc0000    0x57000        0xa C:\Windows\system32\SHLWAPI.dll
0x771c0000    0x4e000       0x80 C:\Windows\system32\GDI32.dll
0x75ed0000    0xc9000       0x87 C:\Windows\system32\USER32.dll
0x77b50000     0xa000       0x1f C:\Windows\system32\LPK.dll
0x76d00000    0x9d000       0x1f C:\Windows\system32\USP10.dll
0x77730000    0x1f000        0x4 C:\Windows\system32\IMM32.DLL
0x75fa0000    0xcc000        0x2 C:\Windows\system32\MSCTF.dll
0x6c200000   0x5ae000        0x4 C:\Windows\Microsoft.NET\Framework\v2.0.50727\mscorwks.dll
0x6c160000    0x9b000        0x5
C:\Windows\WinSxS\x86_microsoft.vc80.crt_1fc8b3b9a1e18e3b_8.0.50727.4940_none_d08cc06a442b34fc\MSVCR80.dll
0x76070000   0xc4a000        0x1 C:\Windows\system32\shell32.dll
0x77220000   0x15c000        0x7 C:\Windows\system32\ole32.dll
0x75a20000     0xb000        0x1 C:\Windows\system32\profapi.dll
0x6b660000   0xaf9000        0x1 C:\Windows\assembly\NativeImages_v2.0.50727_32\mscorlib\38bf604432e1a30c954b2ee40d6a2d1c\mscorlib.ni.dll
0x75900000     0xc000        0x2 C:\Windows\system32\CRYPTBASE.dll
0x74650000    0x40000        0x4 C:\Windows\system32\uxtheme.dll
```

list’s of all the DDL used by the
ZEROlocker.exe