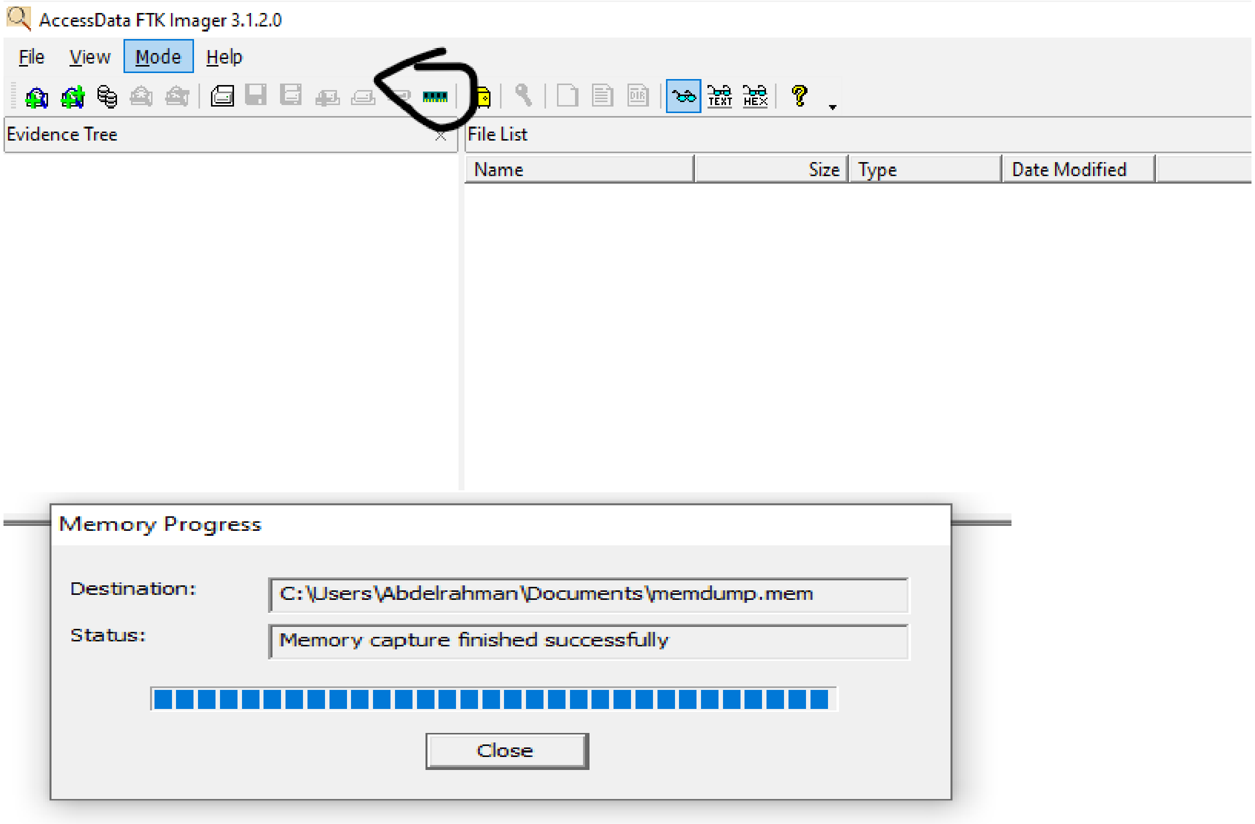
Forensics Assignment

Name: Abdelrahman Khaled Abdallah Hamed

ID: [redacted]14

1. Using FTK IMAGER to gather memory dump

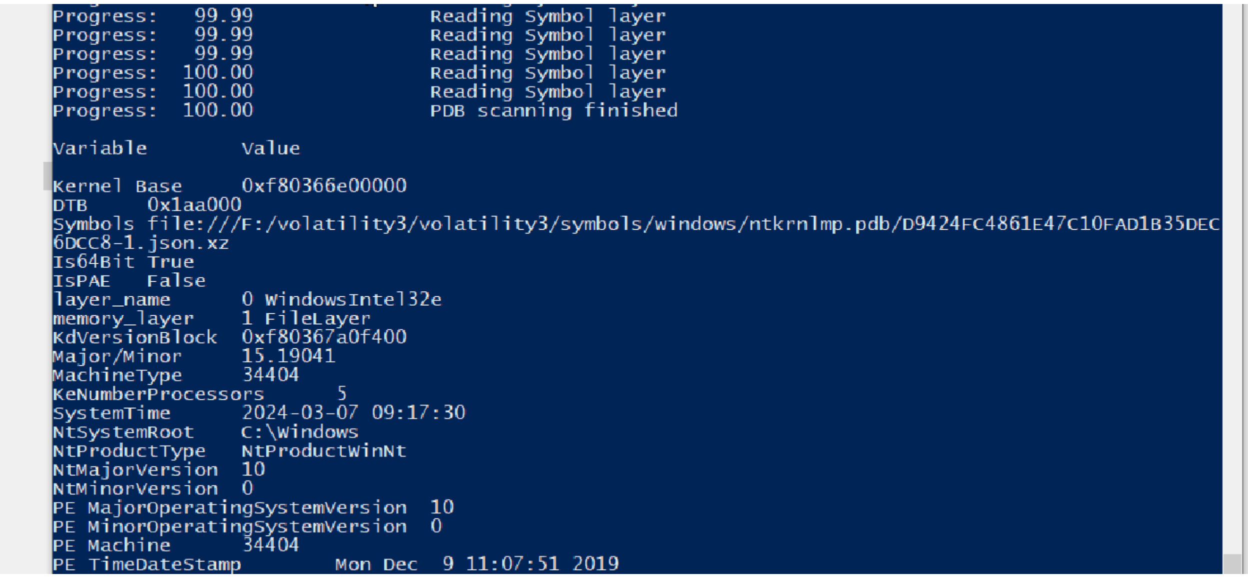


Destination: C:\Users\Abdelrahman\Documents\memdump.mem

Status: Memory capture finished successfully

2. Using volatility to analyze memory dump and process running on system

- **First command : Python.exe ./vol.py -f F:/memorydump.exe windows.info : for providing OS details →output:**

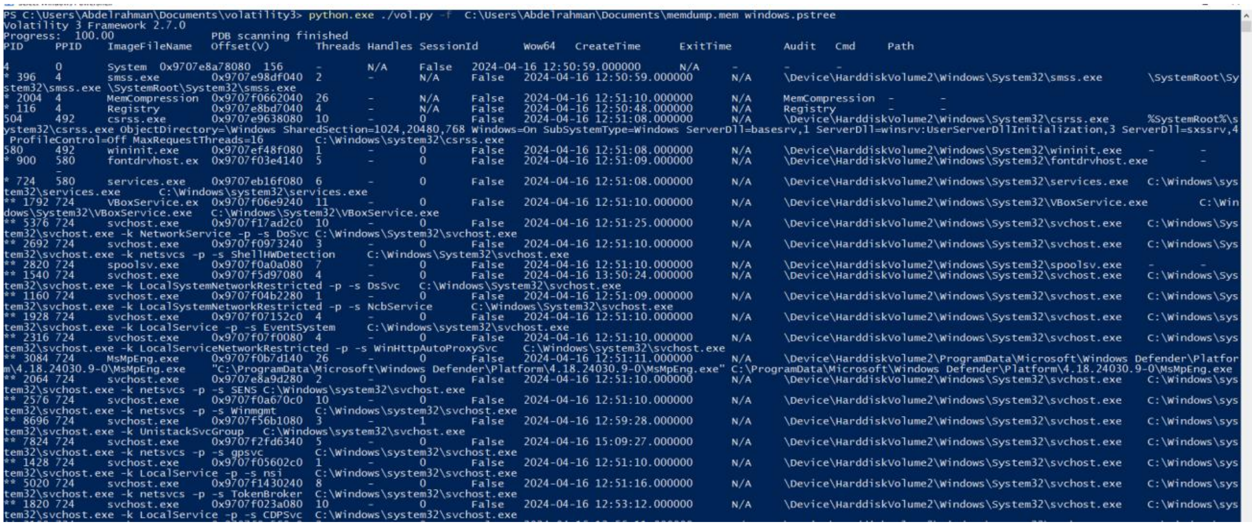


```
Progress:   99.99               Reading Symbol layer
Progress:   99.99               Reading Symbol layer
Progress:   99.99               Reading Symbol layer
Progress:  100.00               Reading Symbol layer
Progress:  100.00               Reading Symbol layer
Progress:  100.00               PDB scanning finished

Variable        Value

Kernel Base     0xf80366e00000
DTB     0x1aa000
Symbols file:///F:/volatility3/volatility3/symbols/windows/ntkrnlmp.pdb/D9424FC4861E47C10FAD1B35DEC
6DCC8-1.json.xz
Is64Bit True
IsPAE   False
layer_name      0 WindowsIntel32e
memory_layer    1 FileLayer
KdVersionBlock  0xf80367a0f400
Major/Minor     15.19041
MachineType     34404
KeNumberProcessors      5
SystemTime      2024-03-07 09:17:30
NtSystemRoot    C:\Windows
NtProductType   NtProductWinNt
NtMajorVersion  10
NtMinorVersion  0
PE MajorOperatingSystemVersion  10
PE MinorOperatingSystemVersion  0
PE Machine      34404
PE TimeDateStamp        Mon Dec  9 11:07:51 2019
```

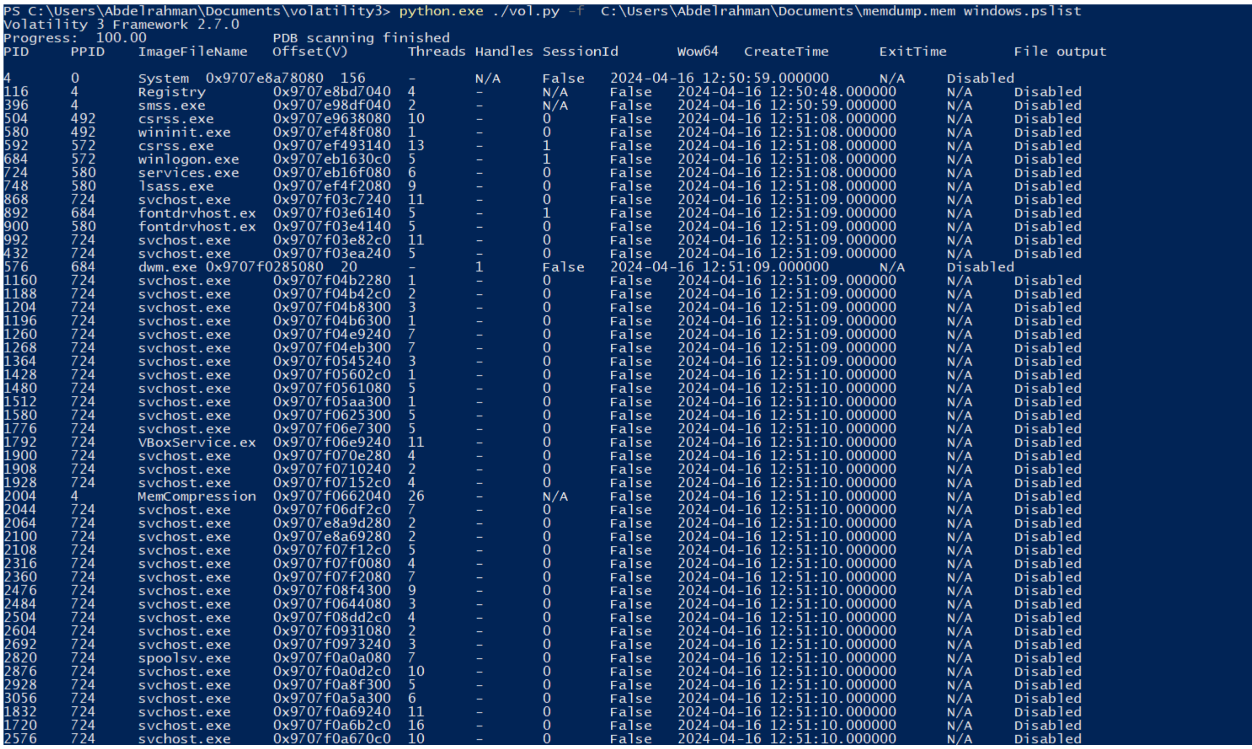
- **Second command : Python.exe ./vol.py -f F:/memorydump.exe windows.pstree : for generating a process tree which show the hierarchal relationship between process running in the memory**



```
PS C:\Users\Abdelrahman\Documents\volatility3> python.exe ./vol.py -f  C:\Users\Abdelrahman\Documents\memdump.mem windows.pstree
Volatility 3 Framework 2.7.0
Progress:  100.00               PDB scanning finished
PID     PPID    ImageFileName   Offset(V)       Threads Handles SessionId       Wow64   CreateTime      ExitTime        Audit   Cmd     Path

4       0       System  0x9707e8a78080  156     -       N/A     False   2024-04-16 12:50:59.000000      N/A     -       -       -
* 396   4       smss.exe        0x9707e98df040  2       -       N/A     False   2024-04-16 12:50:59.000000      N/A     \Device\HarddiskVolume2\Windows\System32\smss.exe       \SystemRoot\Sy
stem32\smss.exe \SystemRoot\System32\smss.exe
* 2004  4       MemCompression  0x9707f0662040  26      -       N/A     False   2024-04-16 12:51:10.000000      N/A     MemCompression  -       -
* 116   4       Registry        0x9707e8bd7040  4       -       N/A     False   2024-04-16 12:50:48.000000      N/A     Registry        -       -
504     492     csrss.exe       0x9707e9638080  10      -       0       False   2024-04-16 12:51:08.000000      N/A     \Device\HarddiskVolume2\Windows\System32\csrss.exe      %SystemRoot%\s
ystem32\csrss.exe ObjectDirectory=\Windows SharedSection=1024,20480,768 Windows=On SubSystemType=Windows ServerDll=basesrv,1 ServerDll=winsrv:UserServerDllInitialization,3 ServerDll=sxssrv,4
 ProfileControl=Off MaxRequestThreads=16        C:\Windows\system32\csrss.exe
580     492     wininit.exe     0x9707ef48f080  1       -       0       False   2024-04-16 12:51:08.000000      N/A     \Device\HarddiskVolume2\Windows\System32\wininit.exe    -       -
* 900   580     fontdrvhost.ex  0x9707f03e4140  5       -       0       False   2024-04-16 12:51:09.000000      N/A     \Device\HarddiskVolume2\Windows\System32\fontdrvhost.exe        -
        -
* 724   580     services.exe    0x9707eb16f080  6       -       0       False   2024-04-16 12:51:08.000000      N/A     \Device\HarddiskVolume2\Windows\System32\services.exe   C:\Windows\sys
tem32\services.exe      C:\Windows\system32\services.exe
** 1792 724     VBoxService.ex  0x9707f06e9240  11      -       0       False   2024-04-16 12:51:10.000000      N/A     \Device\HarddiskVolume2\Windows\System32\VBoxService.exe        C:\Win
dows\System32\VBoxService.exe   C:\Windows\System32\VBoxService.exe
** 5376 724     svchost.exe     0x9707f17ad2c0  10      -       0       False   2024-04-16 12:51:25.000000      N/A     \Device\HarddiskVolume2\Windows\System32\svchost.exe    C:\Windows\Sys
tem32\svchost.exe -k NetworkService -p -s DoSvc C:\Windows\System32\svchost.exe
** 2692 724     svchost.exe     0x9707f0973240  3       -       0       False   2024-04-16 12:51:10.000000      N/A     \Device\HarddiskVolume2\Windows\System32\svchost.exe    C:\Windows\Sys
tem32\svchost.exe -k netsvcs -p -s ShellHWDetection     C:\Windows\System32\svchost.exe
** 2820 724     spoolsv.exe     0x9707f0a0a080  7       -       0       False   2024-04-16 12:51:10.000000      N/A     \Device\HarddiskVolume2\Windows\System32\spoolsv.exe    -       -
** 1540 724     svchost.exe     0x9707f5d97080  4       -       0       False   2024-04-16 13:50:24.000000      N/A     \Device\HarddiskVolume2\Windows\System32\svchost.exe    C:\Windows\Sys
tem32\svchost.exe -k LocalSystemNetworkRestricted -p -s DsSvc   C:\Windows\System32\svchost.exe
** 1160 724     svchost.exe     0x9707f04b2280  1       -       0       False   2024-04-16 12:51:09.000000      N/A     \Device\HarddiskVolume2\Windows\System32\svchost.exe    C:\Windows\Sys
tem32\svchost.exe -k LocalSystemNetworkRestricted -p -s NcbService      C:\Windows\System32\svchost.exe
** 1928 724     svchost.exe     0x9707f07152c0  4       -       0       False   2024-04-16 12:51:10.000000      N/A     \Device\HarddiskVolume2\Windows\System32\svchost.exe    C:\Windows\sys
tem32\svchost.exe -k LocalService -p -s EventSystem     C:\Windows\system32\svchost.exe
** 2316 724     svchost.exe     0x9707f07f0080  4       -       0       False   2024-04-16 12:51:10.000000      N/A     \Device\HarddiskVolume2\Windows\System32\svchost.exe    C:\Windows\sys
tem32\svchost.exe -k LocalServiceNetworkRestricted -p -s WinHttpAutoProxySvc    C:\Windows\system32\svchost.exe
** 3084 724     MsMpEng.exe     0x9707f0b7d140  26      -       0       False   2024-04-16 12:51:11.000000      N/A     \Device\HarddiskVolume2\ProgramData\Microsoft\Windows Defender\Platfor
m\4.18.24030.9-0\MsMpEng.exe    "C:\ProgramData\Microsoft\Windows Defender\Platform\4.18.24030.9-0\MsMpEng.exe" C:\ProgramData\Microsoft\Windows Defender\Platform\4.18.24030.9-0\MsMpEng.exe
** 2064 724     svchost.exe     0x9707e8a9d280  2       -       0       False   2024-04-16 12:51:10.000000      N/A     \Device\HarddiskVolume2\Windows\System32\svchost.exe    C:\Windows\sys
tem32\svchost.exe -k netsvcs -p -s SENS C:\Windows\system32\svchost.exe
** 2576 724     svchost.exe     0x9707f0a670c0  10      -       0       False   2024-04-16 12:51:10.000000      N/A     \Device\HarddiskVolume2\Windows\System32\svchost.exe    C:\Windows\sys
tem32\svchost.exe -k netsvcs -p -s Winmgmt      C:\Windows\system32\svchost.exe
** 8696 724     svchost.exe     0x9707f56b1080  3       -       1       False   2024-04-16 12:59:28.000000      N/A     \Device\HarddiskVolume2\Windows\System32\svchost.exe    C:\Windows\sys
tem32\svchost.exe -k UnistackSvcGroup   C:\Windows\system32\svchost.exe
** 7824 724     svchost.exe     0x9707f2fd6340  5       -       0       False   2024-04-16 15:09:27.000000      N/A     \Device\HarddiskVolume2\Windows\System32\svchost.exe    C:\Windows\sys
tem32\svchost.exe -k netsvcs -p -s gpsvc        C:\Windows\system32\svchost.exe
** 1428 724     svchost.exe     0x9707f05602c0  1       -       0       False   2024-04-16 12:51:10.000000      N/A     \Device\HarddiskVolume2\Windows\System32\svchost.exe    C:\Windows\sys
tem32\svchost.exe -k LocalService -p -s nsi     C:\Windows\system32\svchost.exe
** 5020 724     svchost.exe     0x9707f1430240  8       -       0       False   2024-04-16 12:51:16.000000      N/A     \Device\HarddiskVolume2\Windows\System32\svchost.exe    C:\Windows\sys
tem32\svchost.exe -k netsvcs -p -s TokenBroker  C:\Windows\system32\svchost.exe
** 1820 724     svchost.exe     0x9707f023a080  10      -       0       False   2024-04-16 12:53:12.000000      N/A     \Device\HarddiskVolume2\Windows\System32\svchost.exe    C:\Windows\sys
tem32\svchost.exe -k LocalService -p -s CDPSvc  C:\Windows\system32\svchost.exe
```

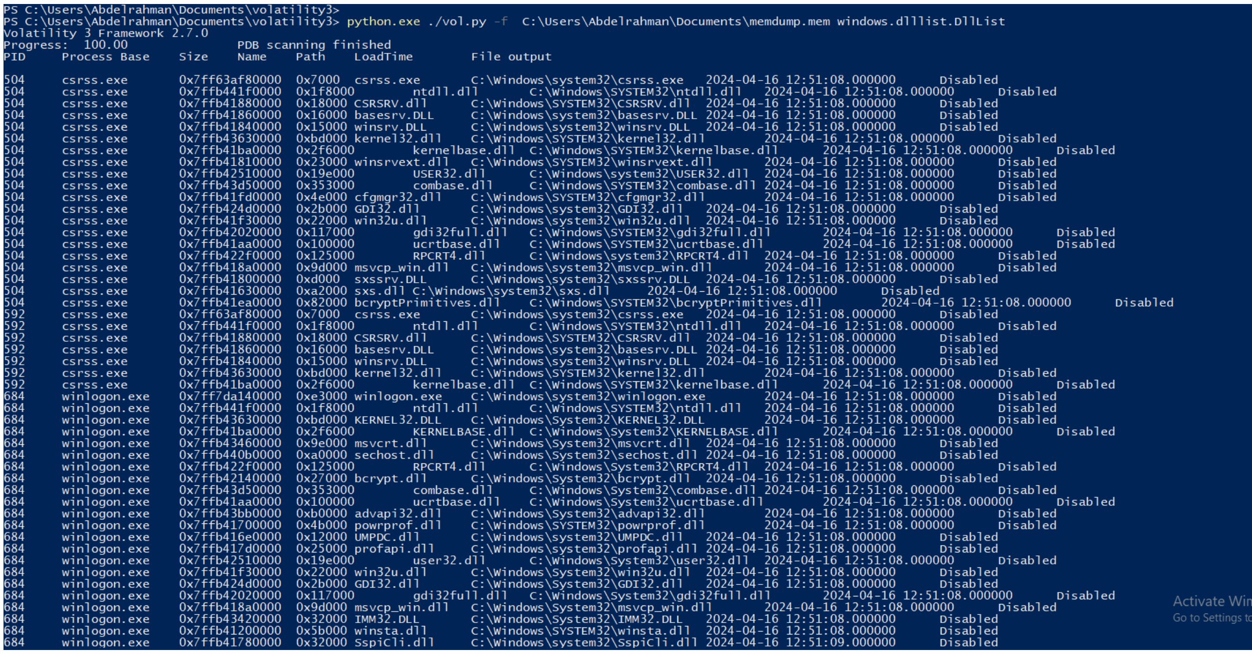
- **Third command : Python.exe ./vol.py -f F:/memorydump.exe windows.pslist : for providing details about every process running within memory dump**



```
PS C:\Users\Abdelrahman\Documents\volatility3> python.exe ./vol.py -f  C:\Users\Abdelrahman\Documents\memdump.mem windows.pslist
Volatility 3 Framework 2.7.0
Progress:  100.00               PDB scanning finished
PID     PPID    ImageFileName   Offset(V)       Threads Handles SessionId       Wow64   CreateTime      ExitTime        File output

4       0       System  0x9707e8a78080  156     -       N/A     False   2024-04-16 12:50:59.000000      N/A     Disabled
116     4       Registry        0x9707e8bd7040  4       -       N/A     False   2024-04-16 12:50:48.000000      N/A     Disabled
396     4       smss.exe        0x9707e98df040  2       -       N/A     False   2024-04-16 12:50:59.000000      N/A     Disabled
504     492     csrss.exe       0x9707e9638080  10      -       0       False   2024-04-16 12:51:08.000000      N/A     Disabled
580     492     wininit.exe     0x9707ef48f080  1       -       0       False   2024-04-16 12:51:08.000000      N/A     Disabled
592     572     csrss.exe       0x9707ef493140  13      -       1       False   2024-04-16 12:51:08.000000      N/A     Disabled
684     572     winlogon.exe    0x9707eb1630c0  5       -       1       False   2024-04-16 12:51:08.000000      N/A     Disabled
724     580     services.exe    0x9707eb16f080  6       -       0       False   2024-04-16 12:51:08.000000      N/A     Disabled
748     580     lsass.exe       0x9707ef4f2080  9       -       0       False   2024-04-16 12:51:08.000000      N/A     Disabled
868     724     svchost.exe     0x9707f03c7240  11      -       0       False   2024-04-16 12:51:09.000000      N/A     Disabled
892     684     fontdrvhost.ex  0x9707f03e6140  5       -       1       False   2024-04-16 12:51:09.000000      N/A     Disabled
900     580     fontdrvhost.ex  0x9707f03e4140  5       -       0       False   2024-04-16 12:51:09.000000      N/A     Disabled
992     724     svchost.exe     0x9707f03e82c0  11      -       0       False   2024-04-16 12:51:09.000000      N/A     Disabled
432     724     svchost.exe     0x9707f03ea240  5       -       0       False   2024-04-16 12:51:09.000000      N/A     Disabled
576     684     dwm.exe 0x9707f0285080  20      -       1       False   2024-04-16 12:51:09.000000      N/A     Disabled
1160    724     svchost.exe     0x9707f04b2280  1       -       0       False   2024-04-16 12:51:09.000000      N/A     Disabled
1188    724     svchost.exe     0x9707f04b42c0  2       -       0       False   2024-04-16 12:51:09.000000      N/A     Disabled
1204    724     svchost.exe     0x9707f04b8300  3       -       0       False   2024-04-16 12:51:09.000000      N/A     Disabled
1196    724     svchost.exe     0x9707f04b6300  1       -       0       False   2024-04-16 12:51:09.000000      N/A     Disabled
1260    724     svchost.exe     0x9707f04e9240  7       -       0       False   2024-04-16 12:51:09.000000      N/A     Disabled
1268    724     svchost.exe     0x9707f04eb300  7       -       0       False   2024-04-16 12:51:09.000000      N/A     Disabled
1364    724     svchost.exe     0x9707f0545240  3       -       0       False   2024-04-16 12:51:09.000000      N/A     Disabled
1428    724     svchost.exe     0x9707f05602c0  1       -       0       False   2024-04-16 12:51:10.000000      N/A     Disabled
1480    724     svchost.exe     0x9707f0561080  5       -       0       False   2024-04-16 12:51:10.000000      N/A     Disabled
1512    724     svchost.exe     0x9707f05aa300  1       -       0       False   2024-04-16 12:51:10.000000      N/A     Disabled
1580    724     svchost.exe     0x9707f0625300  5       -       0       False   2024-04-16 12:51:10.000000      N/A     Disabled
1776    724     svchost.exe     0x9707f06e7300  5       -       0       False   2024-04-16 12:51:10.000000      N/A     Disabled
1792    724     VBoxService.ex  0x9707f06e9240  11      -       0       False   2024-04-16 12:51:10.000000      N/A     Disabled
1900    724     svchost.exe     0x9707f070e280  4       -       0       False   2024-04-16 12:51:10.000000      N/A     Disabled
1908    724     svchost.exe     0x9707f0710240  2       -       0       False   2024-04-16 12:51:10.000000      N/A     Disabled
1928    724     svchost.exe     0x9707f07152c0  4       -       0       False   2024-04-16 12:51:10.000000      N/A     Disabled
2004    4       MemCompression  0x9707f0662040  26      -       N/A     False   2024-04-16 12:51:10.000000      N/A     Disabled
2044    724     svchost.exe     0x9707f06df2c0  7       -       0       False   2024-04-16 12:51:10.000000      N/A     Disabled
2064    724     svchost.exe     0x9707e8a9d280  2       -       0       False   2024-04-16 12:51:10.000000      N/A     Disabled
2100    724     svchost.exe     0x9707e8a69280  2       -       0       False   2024-04-16 12:51:10.000000      N/A     Disabled
2108    724     svchost.exe     0x9707f07f12c0  5       -       0       False   2024-04-16 12:51:10.000000      N/A     Disabled
2316    724     svchost.exe     0x9707f07f0080  4       -       0       False   2024-04-16 12:51:10.000000      N/A     Disabled
2360    724     svchost.exe     0x9707f07f2080  7       -       0       False   2024-04-16 12:51:10.000000      N/A     Disabled
2476    724     svchost.exe     0x9707f08f4300  9       -       0       False   2024-04-16 12:51:10.000000      N/A     Disabled
2484    724     svchost.exe     0x9707f0644080  3       -       0       False   2024-04-16 12:51:10.000000      N/A     Disabled
2504    724     svchost.exe     0x9707f08dd2c0  4       -       0       False   2024-04-16 12:51:10.000000      N/A     Disabled
2604    724     svchost.exe     0x9707f0931080  2       -       0       False   2024-04-16 12:51:10.000000      N/A     Disabled
2692    724     svchost.exe     0x9707f0973240  3       -       0       False   2024-04-16 12:51:10.000000      N/A     Disabled
2820    724     spoolsv.exe     0x9707f0a0a080  7       -       0       False   2024-04-16 12:51:10.000000      N/A     Disabled
2876    724     svchost.exe     0x9707f0a0d2c0  10      -       0       False   2024-04-16 12:51:10.000000      N/A     Disabled
2928    724     svchost.exe     0x9707f0a8f300  5       -       0       False   2024-04-16 12:51:10.000000      N/A     Disabled
3056    724     svchost.exe     0x9707f0a5a300  6       -       0       False   2024-04-16 12:51:10.000000      N/A     Disabled
1832    724     svchost.exe     0x9707f0a69240  11      -       0       False   2024-04-16 12:51:10.000000      N/A     Disabled
1720    724     svchost.exe     0x9707f0a6b2c0  16      -       0       False   2024-04-16 12:51:10.000000      N/A     Disabled
2576    724     svchost.exe     0x9707f0a670c0  10      -       0       False   2024-04-16 12:51:10.000000      N/A     Disabled
```

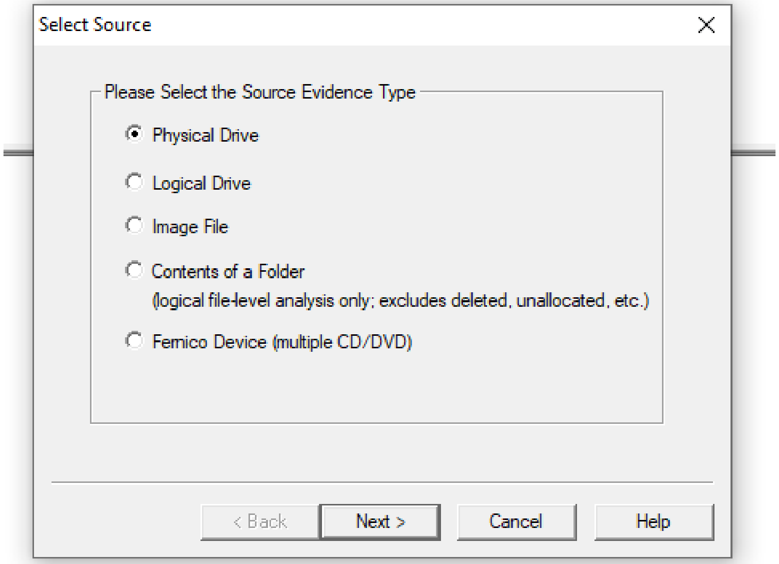
- **fourth command : Python.exe ./vol.py -f F:/memorydump.exe windows.dlllist.DLLlist : for providing details about every process running within memory dump along with dll associated with it**



```
PS C:\Users\Abdelrahman\Documents\volatility3>
PS C:\Users\Abdelrahman\Documents\volatility3> python.exe ./vol.py -f  C:\Users\Abdelrahman\Documents\memdump.mem windows.dlllist.DllList
Volatility 3 Framework 2.7.0
Progress:  100.00               PDB scanning finished
PID     Process Base    Size    Name    Path    LoadTime        File output

504     csrss.exe       0x7ff63af80000  0x7000  csrss.exe       C:\Windows\system32\csrss.exe   2024-04-16 12:51:08.000000      Disabled
504     csrss.exe       0x7ffb441f0000  0x1f8000        ntdll.dll       C:\Windows\SYSTEM32\ntdll.dll   2024-04-16 12:51:08.000000      Disabled
504     csrss.exe       0x7ffb41880000  0x18000 CSRSRV.dll      C:\Windows\SYSTEM32\CSRSRV.dll  2024-04-16 12:51:08.000000      Disabled
504     csrss.exe       0x7ffb41860000  0x16000 basesrv.DLL     C:\Windows\system32\basesrv.DLL 2024-04-16 12:51:08.000000      Disabled
504     csrss.exe       0x7ffb41840000  0x15000 winsrv.DLL      C:\Windows\system32\winsrv.DLL  2024-04-16 12:51:08.000000      Disabled
504     csrss.exe       0x7ffb43630000  0xbd000 kernel32.dll    C:\Windows\SYSTEM32\kernel32.dll        2024-04-16 12:51:08.000000      Disabled
504     csrss.exe       0x7ffb41ba0000  0x2f6000        kernelbase.dll  C:\Windows\SYSTEM32\kernelbase.dll      2024-04-16 12:51:08.000000      Disabled
504     csrss.exe       0x7ffb41810000  0x23000 winsrvext.dll   C:\Windows\SYSTEM32\winsrvext.dll       2024-04-16 12:51:08.000000      Disabled
504     csrss.exe       0x7ffb42510000  0x19e000        USER32.dll      C:\Windows\system32\USER32.dll  2024-04-16 12:51:08.000000      Disabled
504     csrss.exe       0x7ffb43d50000  0x353000        combase.dll     C:\Windows\SYSTEM32\combase.dll 2024-04-16 12:51:08.000000      Disabled
504     csrss.exe       0x7ffb41fd0000  0x4e000 cfgmgr32.dll    C:\Windows\SYSTEM32\cfgmgr32.dll        2024-04-16 12:51:08.000000      Disabled
504     csrss.exe       0x7ffb424d0000  0x2b000 GDI32.dll       C:\Windows\system32\GDI32.dll   2024-04-16 12:51:08.000000      Disabled
504     csrss.exe       0x7ffb41f30000  0x22000 win32u.dll      C:\Windows\system32\win32u.dll  2024-04-16 12:51:08.000000      Disabled
504     csrss.exe       0x7ffb42020000  0x117000        gdi32full.dll   C:\Windows\SYSTEM32\gdi32full.dll       2024-04-16 12:51:08.000000      Disabled
504     csrss.exe       0x7ffb41aa0000  0x100000        ucrtbase.dll    C:\Windows\SYSTEM32\ucrtbase.dll        2024-04-16 12:51:08.000000      Disabled
504     csrss.exe       0x7ffb422f0000  0x125000        RPCRT4.dll      C:\Windows\system32\RPCRT4.dll  2024-04-16 12:51:08.000000      Disabled
504     csrss.exe       0x7ffb418a0000  0x9d000 msvcp_win.dll   C:\Windows\system32\msvcp_win.dll       2024-04-16 12:51:08.000000      Disabled
504     csrss.exe       0x7ffb41800000  0xd000  sxssrv.DLL      C:\Windows\system32\sxssrv.DLL  2024-04-16 12:51:08.000000      Disabled
504     csrss.exe       0x7ffb41630000  0xa2000 sxs.dll C:\Windows\system32\sxs.dll     2024-04-16 12:51:08.000000      Disabled
504     csrss.exe       0x7ffb41ea0000  0x82000 bcryptPrimitives.dll    C:\Windows\SYSTEM32\bcryptPrimitives.dll        2024-04-16 12:51:08.000000      Disabled
592     csrss.exe       0x7ff63af80000  0x7000  csrss.exe       C:\Windows\system32\csrss.exe   2024-04-16 12:51:08.000000      Disabled
592     csrss.exe       0x7ffb441f0000  0x1f8000        ntdll.dll       C:\Windows\SYSTEM32\ntdll.dll   2024-04-16 12:51:08.000000      Disabled
592     csrss.exe       0x7ffb41880000  0x18000 CSRSRV.dll      C:\Windows\SYSTEM32\CSRSRV.dll  2024-04-16 12:51:08.000000      Disabled
592     csrss.exe       0x7ffb41860000  0x16000 basesrv.DLL     C:\Windows\system32\basesrv.DLL 2024-04-16 12:51:08.000000      Disabled
592     csrss.exe       0x7ffb41840000  0x15000 winsrv.DLL      C:\Windows\system32\winsrv.DLL  2024-04-16 12:51:08.000000      Disabled
592     csrss.exe       0x7ffb43630000  0xbd000 kernel32.dll    C:\Windows\SYSTEM32\kernel32.dll        2024-04-16 12:51:08.000000      Disabled
592     csrss.exe       0x7ffb41ba0000  0x2f6000        kernelbase.dll  C:\Windows\SYSTEM32\kernelbase.dll      2024-04-16 12:51:08.000000      Disabled
684     winlogon.exe    0x7ff7da140000  0xe3000 winlogon.exe    C:\Windows\system32\winlogon.exe        2024-04-16 12:51:08.000000      Disabled
684     winlogon.exe    0x7ffb441f0000  0x1f8000        ntdll.dll       C:\Windows\SYSTEM32\ntdll.dll   2024-04-16 12:51:08.000000      Disabled
684     winlogon.exe    0x7ffb43630000  0xbd000 KERNEL32.DLL    C:\Windows\System32\KERNEL32.DLL        2024-04-16 12:51:08.000000      Disabled
684     winlogon.exe    0x7ffb41ba0000  0x2f6000        KERNELBASE.dll  C:\Windows\System32\KERNELBASE.dll      2024-04-16 12:51:08.000000      Disabled
684     winlogon.exe    0x7ffb43460000  0x9e000 msvcrt.dll      C:\Windows\System32\msvcrt.dll  2024-04-16 12:51:08.000000      Disabled
684     winlogon.exe    0x7ffb440b0000  0xa0000 sechost.dll     C:\Windows\System32\sechost.dll 2024-04-16 12:51:08.000000      Disabled
684     winlogon.exe    0x7ffb422f0000  0x125000        RPCRT4.dll      C:\Windows\System32\RPCRT4.dll  2024-04-16 12:51:08.000000      Disabled
684     winlogon.exe    0x7ffb42140000  0x27000 bcrypt.dll      C:\Windows\System32\bcrypt.dll  2024-04-16 12:51:08.000000      Disabled
684     winlogon.exe    0x7ffb43d50000  0x353000        combase.dll     C:\Windows\System32\combase.dll 2024-04-16 12:51:08.000000      Disabled
684     winlogon.exe    0x7ffb41aa0000  0x100000        ucrtbase.dll    C:\Windows\System32\ucrtbase.dll        2024-04-16 12:51:08.000000      Disabled
684     winlogon.exe    0x7ffb43bb0000  0xb0000 advapi32.dll    C:\Windows\System32\advapi32.dll        2024-04-16 12:51:08.000000      Disabled
684     winlogon.exe    0x7ffb41700000  0x4b000 powrprof.dll    C:\Windows\SYSTEM32\powrprof.dll        2024-04-16 12:51:08.000000      Disabled
684     winlogon.exe    0x7ffb416e0000  0x12000 UMPDC.dll       C:\Windows\system32\UMPDC.dll   2024-04-16 12:51:08.000000      Disabled
684     winlogon.exe    0x7ffb417d0000  0x25000 profapi.dll     C:\Windows\system32\profapi.dll 2024-04-16 12:51:08.000000      Disabled
684     winlogon.exe    0x7ffb42510000  0x19e000        user32.dll      C:\Windows\System32\user32.dll  2024-04-16 12:51:08.000000      Disabled
684     winlogon.exe    0x7ffb41f30000  0x22000 win32u.dll      C:\Windows\System32\win32u.dll  2024-04-16 12:51:08.000000      Disabled
684     winlogon.exe    0x7ffb424d0000  0x2b000 GDI32.dll       C:\Windows\System32\GDI32.dll   2024-04-16 12:51:08.000000      Disabled
684     winlogon.exe    0x7ffb42020000  0x117000        gdi32full.dll   C:\Windows\System32\gdi32full.dll       2024-04-16 12:51:08.000000      Disabled
684     winlogon.exe    0x7ffb418a0000  0x9d000 msvcp_win.dll   C:\Windows\System32\msvcp_win.dll       2024-04-16 12:51:08.000000      Disabled
684     winlogon.exe    0x7ffb43420000  0x32000 IMM32.DLL       C:\Windows\System32\IMM32.DLL   2024-04-16 12:51:08.000000      Disabled
684     winlogon.exe    0x7ffb41200000  0x5b000 winsta.dll      C:\Windows\SYSTEM32\winsta.dll  2024-04-16 12:51:08.000000      Disabled
684     winlogon.exe    0x7ffb41780000  0x32000 SspiCli.dll     C:\Windows\system32\SspiCli.dll 2024-04-16 12:51:09.000000      Disabled
```

3-Using FTK IMAGER to take image from disk :



Select Source

Please Select the Source Evidence Type

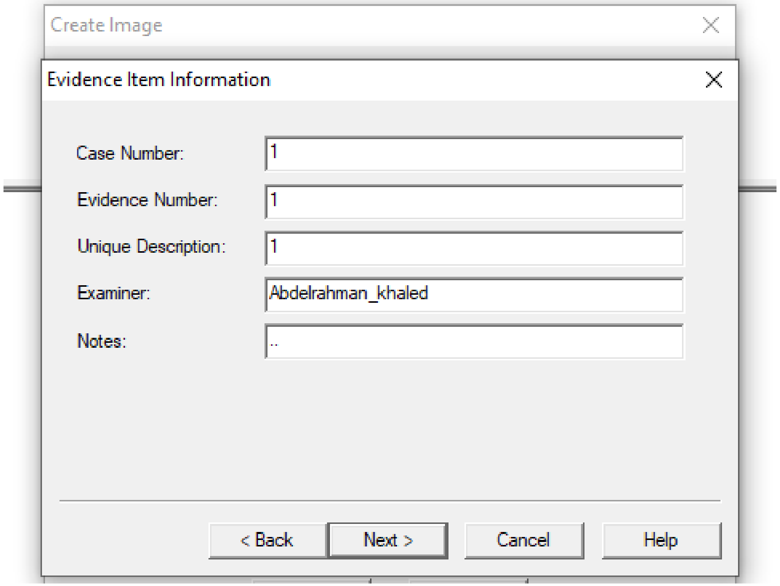
● Physical Drive

○ Logical Drive

○ Image File

○ Contents of a Folder
(logical file-level analysis only; excludes deleted, unallocated, etc.)

○ Femico Device (multiple CD/DVD)



Create Image

Evidence Item Information

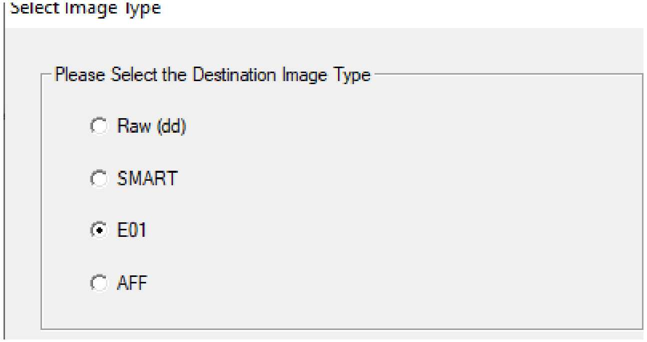
Case Number: 1

Evidence Number: 1

Unique Description: 1

Examiner: Abdelrahman_khaled

Notes: ..



Select Image Type

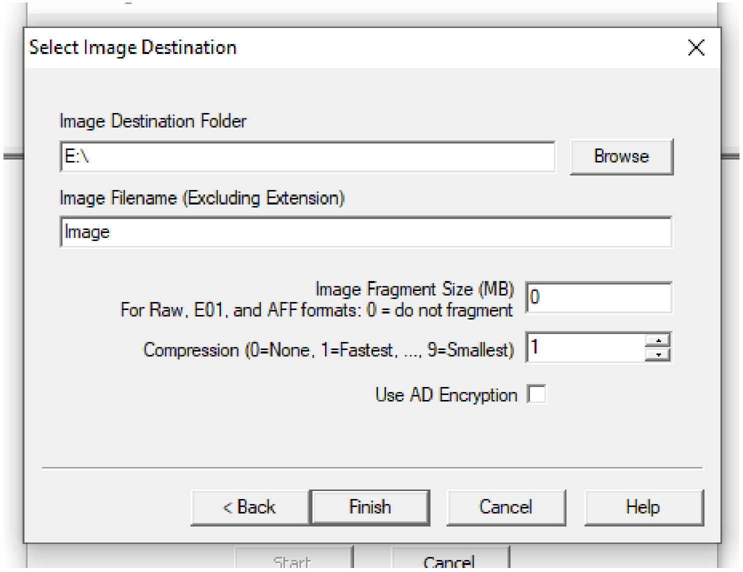
Please Select the Destination Image Type

○ Raw (dd)

○ SMART

● E01

○ AFF



Select Image Destination

Image Destination Folder: E:\

Image Filename (Excluding Extension): Image

Image Fragment Size (MB)
For Raw, E01, and AFF formats: 0 = do not fragment: 0

Compression (0=None, 1=Fastest, ..., 9=Smallest): 1

Use AD Encryption □

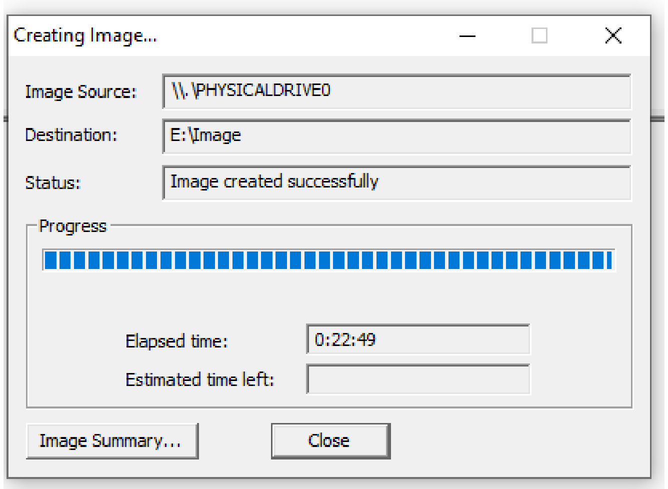

Creating Image...

Image Source: \\.\PHYSICALDRIVE0

Destination: E:\Image

Status: Image created successfully

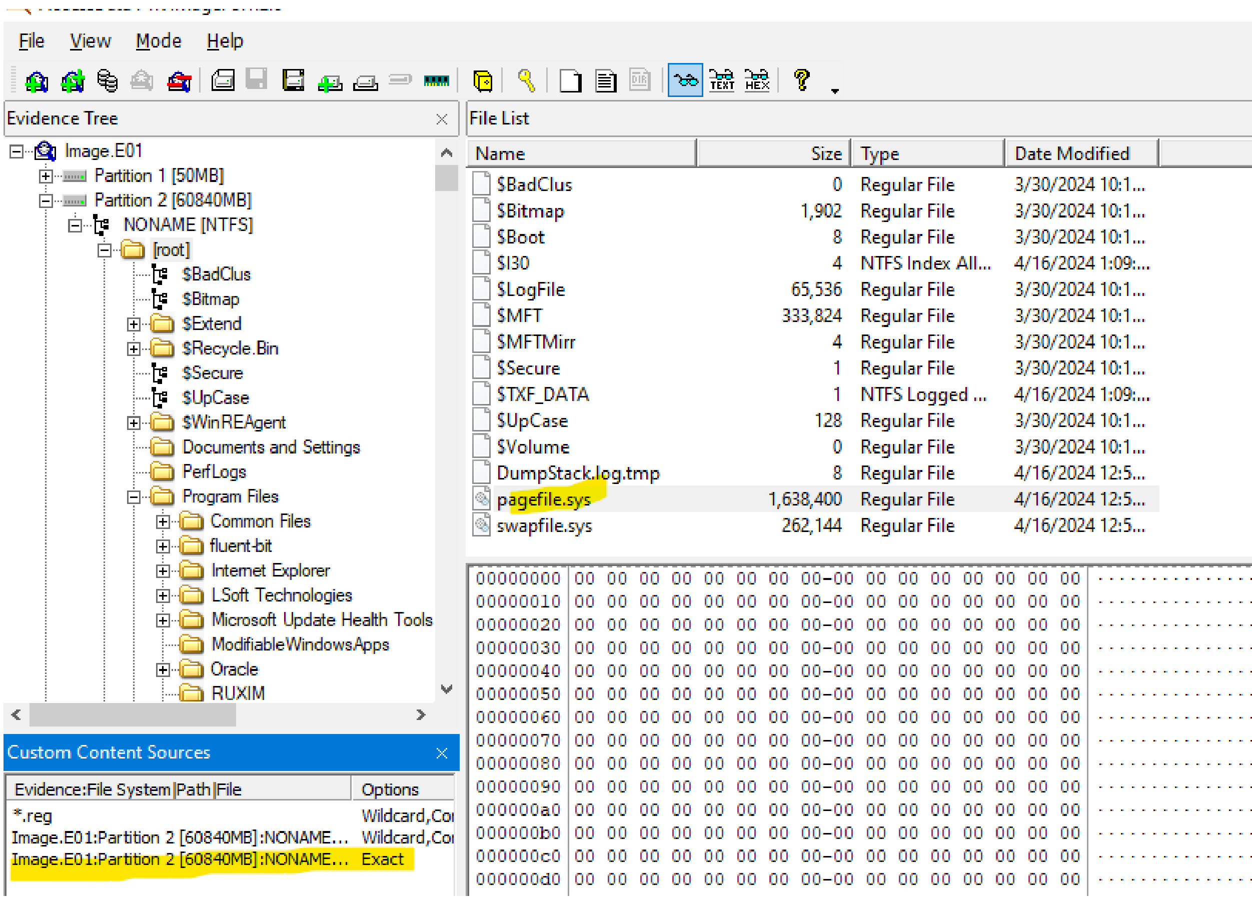
Progress

Elapsed time: 0:22:49

Estimated time left:

4-Analayzing Image using FTK IMAGER :

- **first extracting Pagefile**



```
Image.E01
  Partition 1 [50MB]
  Partition 2 [60840MB]
    NONAME [NTFS]
      [root]
        $BadClus
        $Bitmap
        $Extend
        $Recycle.Bin
        $Secure
        $UpCase
        $WinREAgent
        Documents and Settings
        PerfLogs
        Program Files
          Common Files
          fluent-bit
          Internet Explorer
          LSoft Technologies
          Microsoft Update Health Tools
          ModifiableWindowsApps
          Oracle
          RUXIM
```

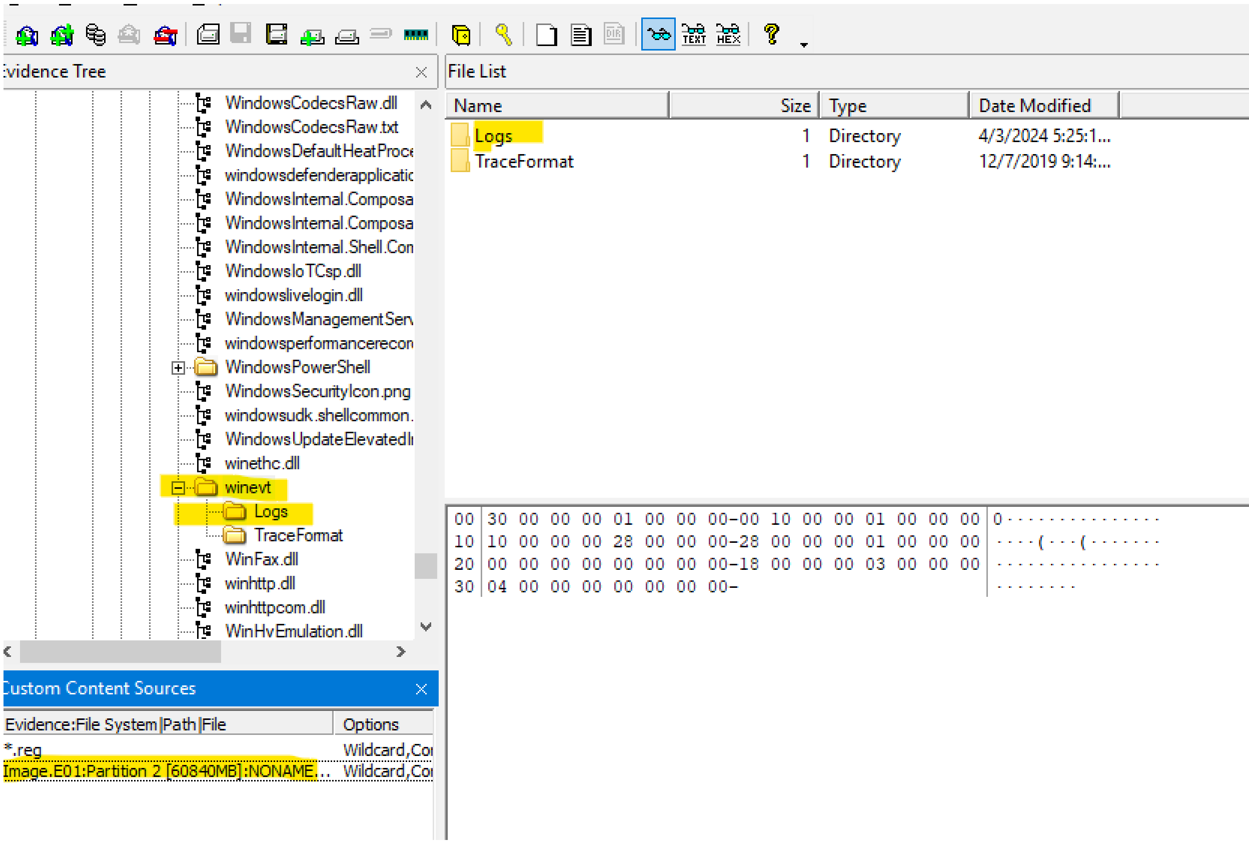
Name	Size	Type	Date Modified
$BadClus	0	Regular File	3/30/2024 10:1...
$Bitmap	1,902	Regular File	3/30/2024 10:1...
$Boot	8	Regular File	3/30/2024 10:1...
$I30	4	NTFS Index All...	4/16/2024 1:09:...
$LogFile	65,536	Regular File	3/30/2024 10:1...
$MFT	333,824	Regular File	3/30/2024 10:1...
$MFTMirr	4	Regular File	3/30/2024 10:1...
$Secure	1	Regular File	3/30/2024 10:1...
$TXF_DATA	1	NTFS Logged ...	4/16/2024 1:09:...
$UpCase	128	Regular File	3/30/2024 10:1...
$Volume	0	Regular File	3/30/2024 10:1...
DumpStack.log.tmp	8	Regular File	4/16/2024 12:5...
pagefile.sys	1,638,400	Regular File	4/16/2024 12:5...
swapfile.sys	262,144	Regular File	4/16/2024 12:5...

```
00000000  00 00 00 00 00 00 00 00-00 00 00 00 00 00 00 00  ................
00000010  00 00 00 00 00 00 00 00-00 00 00 00 00 00 00 00  ................
00000020  00 00 00 00 00 00 00 00-00 00 00 00 00 00 00 00  ................
00000030  00 00 00 00 00 00 00 00-00 00 00 00 00 00 00 00  ................
00000040  00 00 00 00 00 00 00 00-00 00 00 00 00 00 00 00  ................
00000050  00 00 00 00 00 00 00 00-00 00 00 00 00 00 00 00  ................
00000060  00 00 00 00 00 00 00 00-00 00 00 00 00 00 00 00  ................
00000070  00 00 00 00 00 00 00 00-00 00 00 00 00 00 00 00  ................
00000080  00 00 00 00 00 00 00 00-00 00 00 00 00 00 00 00  ................
00000090  00 00 00 00 00 00 00 00-00 00 00 00 00 00 00 00  ................
000000a0  00 00 00 00 00 00 00 00-00 00 00 00 00 00 00 00  ................
000000b0  00 00 00 00 00 00 00 00-00 00 00 00 00 00 00 00  ................
000000c0  00 00 00 00 00 00 00 00-00 00 00 00 00 00 00 00  ................
000000d0  00 00 00 00 00 00 00 00-00 00 00 00 00 00 00 00  ................
```

Custom Content Sources

Evidence:File System|Path|File	Options
*.reg	Wildcard,Coı
Image.E01:Partition 2 [60840MB]:NONAME...	Wildcard,Coı
Image.E01:Partition 2 [60840MB]:NONAME...	Exact

- **second extracting the event viewer files:**



:vidence Tree

- WindowsCodecsRaw.dll
- WindowsCodecsRaw.txt
- WindowsDefaultHeatProce
- windowsdefenderapplicatic
- WindowsInternal.Composa
- WindowsInternal.Composa
- WindowsInternal.Shell.Con
- WindowsIoTCsp.dll
- windowslivelogin.dll
- WindowsManagementServ
- windowsperformancerecon
- WindowsPowerShell
- WindowsSecurityIcon.png
- windowsudk.shellcommon.
- WindowsUpdateElevatedIi
- winethc.dll
- winevt
  - Logs
  - TraceFormat
- WinFax.dll
- winhttp.dll
- winhttpcom.dll
- WinHvEmulation.dll

File List

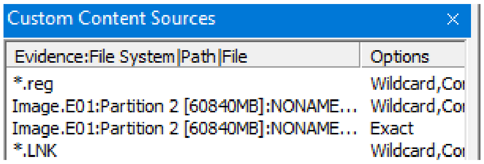
Name	Size	Type	Date Modified
Logs	1	Directory	4/3/2024 5:25:1...
TraceFormat	1	Directory	12/7/2019 9:14:...

```
00 30 00 00 00 01 00 00 00-00 10 00 00 01 00 00 00  0...............
10 10 00 00 00 28 00 00 00-28 00 00 00 01 00 00 00  ....(...(.......
20 00 00 00 00 00 00 00 00-18 00 00 00 03 00 00 00  ................
30 04 00 00 00 00 00 00 00-                         ........
```

:ustom Content Sources

Evidence:File System|Path|File	Options
*.reg	Wildcard,Coı
Image.E01:Partition 2 [60840MB]:NONAME...	Wildcard,Coı

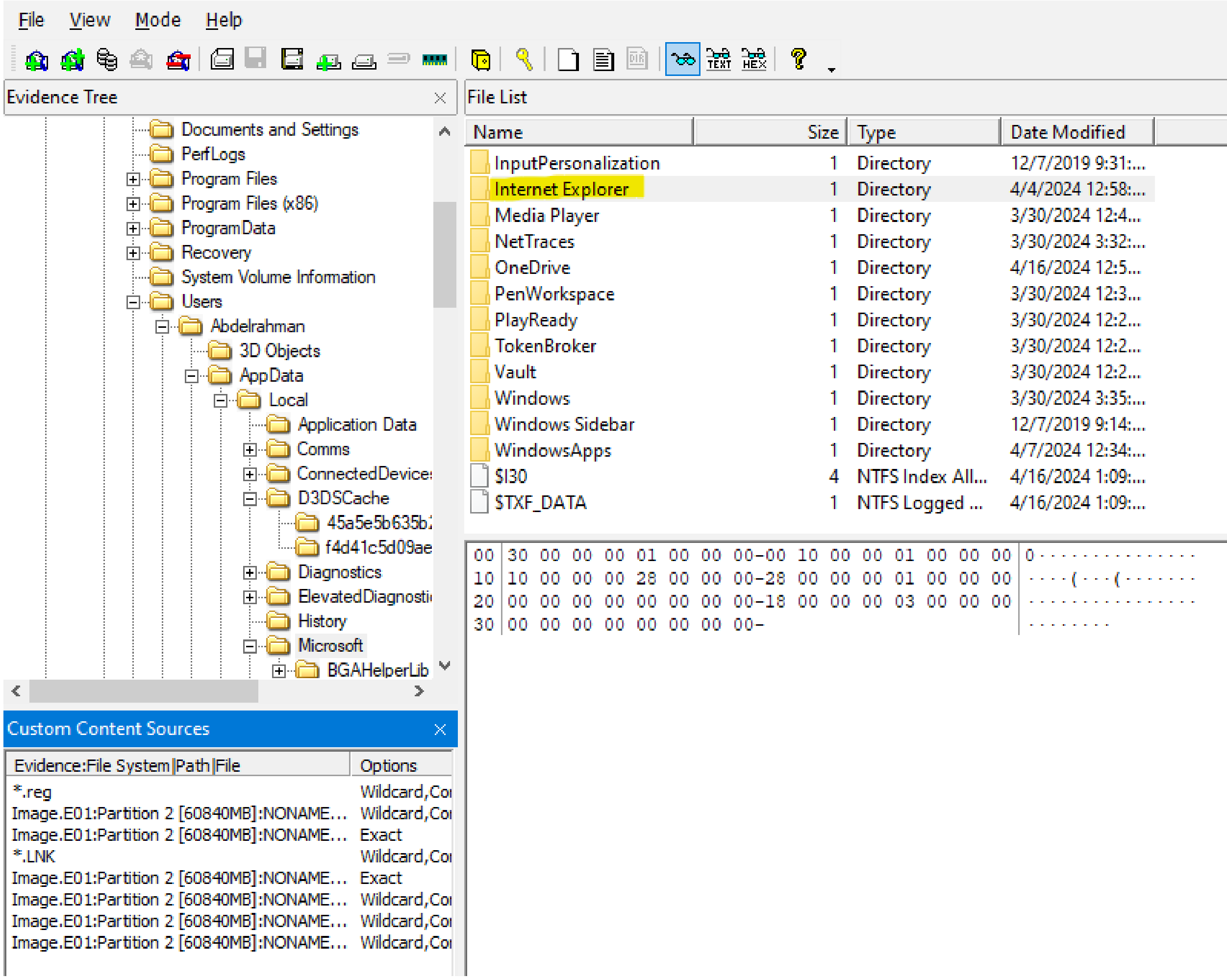
- **Third including all registry files (*.reg)**



Custom Content Sources

Evidence:File System|Path|File	Options
*.reg	Wildcard,Coı
Image.E01:Partition 2 [60840MB]:NONAME...	Wildcard,Coı
Image.E01:Partition 2 [60840MB]:NONAME...	Exact
*.LNK	Wildcard,Coı

- **Fourth including all browser related files:**

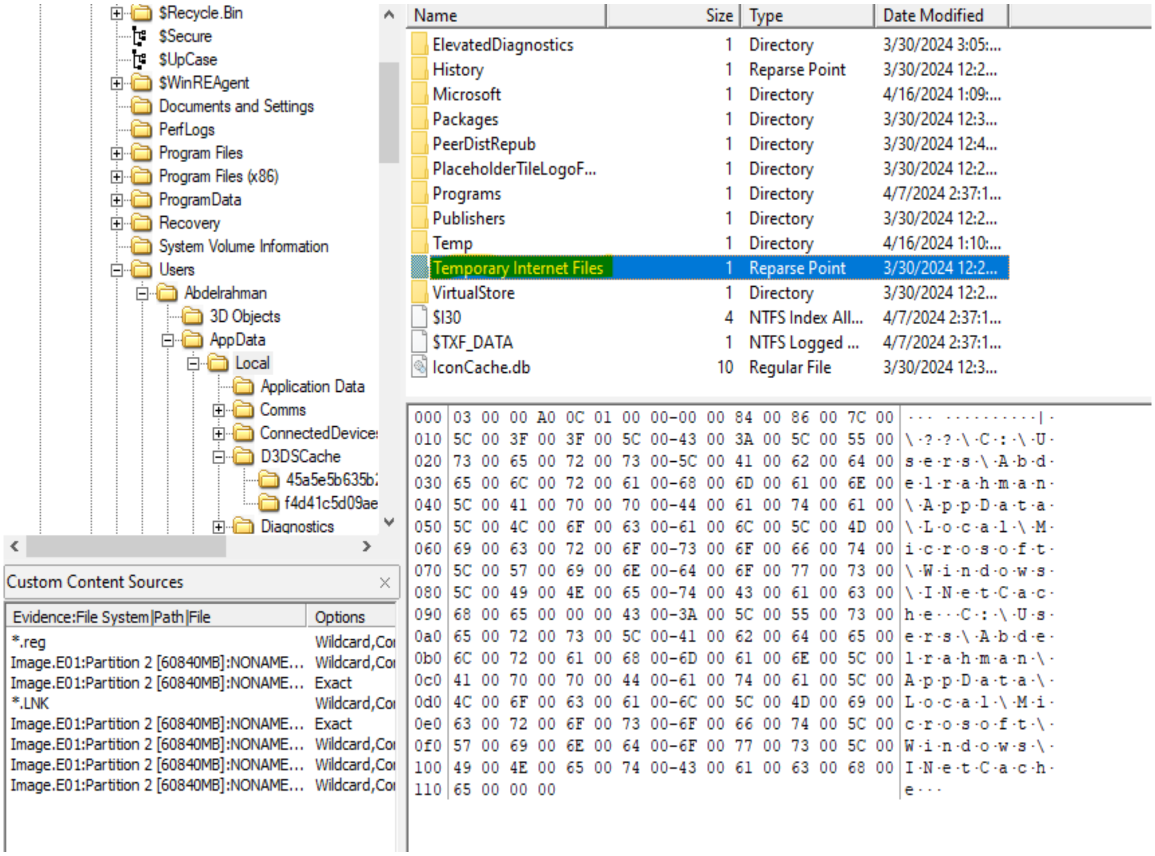


Name	Size	Type	Date Modified
InputPersonalization	1	Directory	12/7/2019 9:31:...
Internet Explorer	1	Directory	4/4/2024 12:58:...
Media Player	1	Directory	3/30/2024 12:4...
NetTraces	1	Directory	3/30/2024 3:32:...
OneDrive	1	Directory	4/16/2024 12:5...
PenWorkspace	1	Directory	3/30/2024 12:3...
PlayReady	1	Directory	3/30/2024 12:2...
TokenBroker	1	Directory	3/30/2024 12:2...
Vault	1	Directory	3/30/2024 12:2...
Windows	1	Directory	3/30/2024 3:35:...
Windows Sidebar	1	Directory	12/7/2019 9:14:...
WindowsApps	1	Directory	4/7/2024 12:34:...
$I30	4	NTFS Index All...	4/16/2024 1:09:...
$TXF_DATA	1	NTFS Logged ...	4/16/2024 1:09:...

```
00 30 00 00 00 01 00 00 00-00 10 00 00 01 00 00 00  0···············
10 10 00 00 00 28 00 00 00-28 00 00 00 01 00 00 00  ····(···(·······
20 00 00 00 00 00 00 00 00-18 00 00 00 03 00 00 00  ················
30 00 00 00 00 00 00 00 00-                         ········
```

Custom Content Sources

Evidence:File System|Path|File	Options
*.reg	Wildcard,Co
Image.E01:Partition 2 [60840MB]:NONAME...	Wildcard,Co
Image.E01:Partition 2 [60840MB]:NONAME...	Exact
*.LNK	Wildcard,Co
Image.E01:Partition 2 [60840MB]:NONAME...	Exact
Image.E01:Partition 2 [60840MB]:NONAME...	Wildcard,Co
Image.E01:Partition 2 [60840MB]:NONAME...	Wildcard,Co
Image.E01:Partition 2 [60840MB]:NONAME...	Wildcard,Co

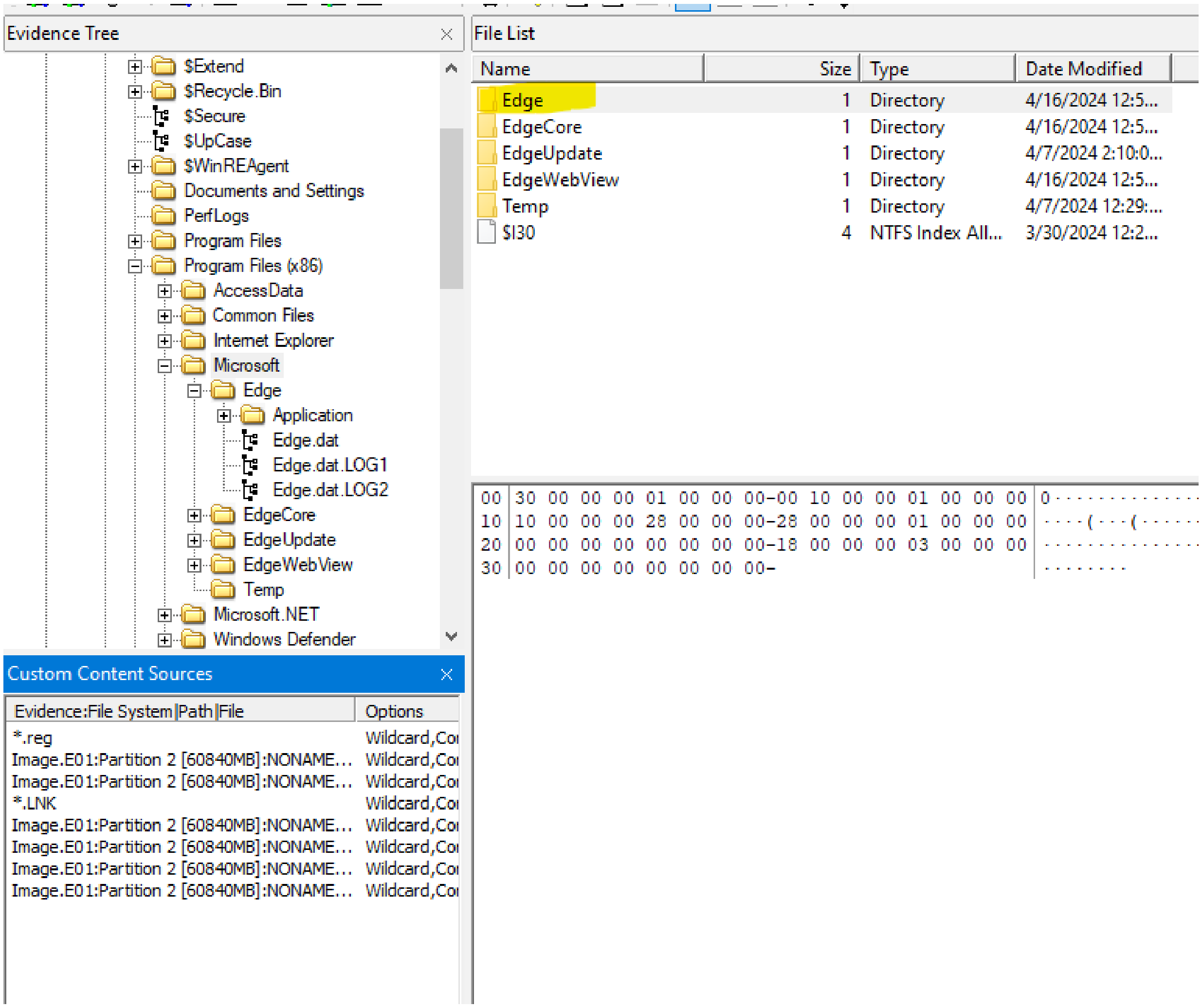


Name	Size	Type	Date Modified
ElevatedDiagnostics	1	Directory	3/30/2024 3:05:...
History	1	Reparse Point	3/30/2024 12:2...
Microsoft	1	Directory	4/16/2024 1:09:...
Packages	1	Directory	3/30/2024 12:3...
PeerDistRepub	1	Directory	3/30/2024 12:4...
PlaceholderTileLogoF...	1	Directory	3/30/2024 12:2...
Programs	1	Directory	4/7/2024 2:37:1...
Publishers	1	Directory	3/30/2024 12:2...
Temp	1	Directory	4/16/2024 1:10:...
Temporary Internet Files	1	Reparse Point	3/30/2024 12:2...
VirtualStore	1	Directory	3/30/2024 12:2...
$I30	4	NTFS Index All...	4/7/2024 2:37:1...
$TXF_DATA	1	NTFS Logged ...	4/7/2024 2:37:1...
IconCache.db	10	Regular File	3/30/2024 12:3...

```
000 03 00 00 A0 0C 01 00 00-00 00 84 00 86 00 7C 00  ··· ··········|·
010 5C 00 3F 00 3F 00 5C 00-43 00 3A 00 5C 00 55 00  \·?·?·\·C·:·\·U·
020 73 00 65 00 72 00 73 00-5C 00 41 00 62 00 64 00  s·e·r·s·\·A·b·d·
030 65 00 6C 00 72 00 61 00-68 00 6D 00 61 00 6E 00  e·l·r·a·h·m·a·n·
040 5C 00 41 00 70 00 70 00-44 00 61 00 74 00 61 00  \·A·p·p·D·a·t·a·
050 5C 00 4C 00 6F 00 63 00-61 00 6C 00 5C 00 4D 00  \·L·o·c·a·l·\·M·
060 69 00 63 00 72 00 6F 00-73 00 6F 00 66 00 74 00  i·c·r·o·s·o·f·t·
070 5C 00 57 00 69 00 6E 00-64 00 6F 00 77 00 73 00  \·W·i·n·d·o·w·s·
080 5C 00 49 00 4E 00 65 00-74 00 43 00 61 00 63 00  \·I·N·e·t·C·a·c·
090 68 00 65 00 00 00 43 00-3A 00 5C 00 55 00 73 00  h·e···C·:·\·U·s·
0a0 65 00 72 00 73 00 5C 00-41 00 62 00 64 00 65 00  e·r·s·\·A·b·d·e·
0b0 6C 00 72 00 61 00 68 00-6D 00 61 00 6E 00 5C 00  l·r·a·h·m·a·n·\·
0c0 41 00 70 00 70 00 44 00-61 00 74 00 61 00 5C 00  A·p·p·D·a·t·a·\·
0d0 4C 00 6F 00 63 00 61 00-6C 00 5C 00 4D 00 69 00  L·o·c·a·l·\·M·i·
0e0 63 00 72 00 6F 00 73 00-6F 00 66 00 74 00 5C 00  c·r·o·s·o·f·t·\·
0f0 57 00 69 00 6E 00 64 00-6F 00 77 00 73 00 5C 00  W·i·n·d·o·w·s·\·
100 49 00 4E 00 65 00 74 00-43 00 61 00 63 00 68 00  I·N·e·t·C·a·c·h·
110 65 00 00 00                                      e···
```

Custom Content Sources

Evidence:File System|Path|File	Options
*.reg	Wildcard,Coı
Image.E01:Partition 2 [60840MB]:NONAME...	Wildcard,Coı
Image.E01:Partition 2 [60840MB]:NONAME...	Exact
*.LNK	Wildcard,Coı
Image.E01:Partition 2 [60840MB]:NONAME...	Exact
Image.E01:Partition 2 [60840MB]:NONAME...	Wildcard,Coı
Image.E01:Partition 2 [60840MB]:NONAME...	Wildcard,Coı
Image.E01:Partition 2 [60840MB]:NONAME...	Wildcard,Coı



Evidence Tree

- $Extend
- $Recycle.Bin
- $Secure
- $UpCase
- $WinREAgent
- Documents and Settings
- PerfLogs
- Program Files
- Program Files (x86)
  - AccessData
  - Common Files
  - Internet Explorer
  - Microsoft
    - Edge
      - Application
      - Edge.dat
      - Edge.dat.LOG1
      - Edge.dat.LOG2
    - EdgeCore
    - EdgeUpdate
    - EdgeWebView
    - Temp
  - Microsoft.NET
  - Windows Defender

File List

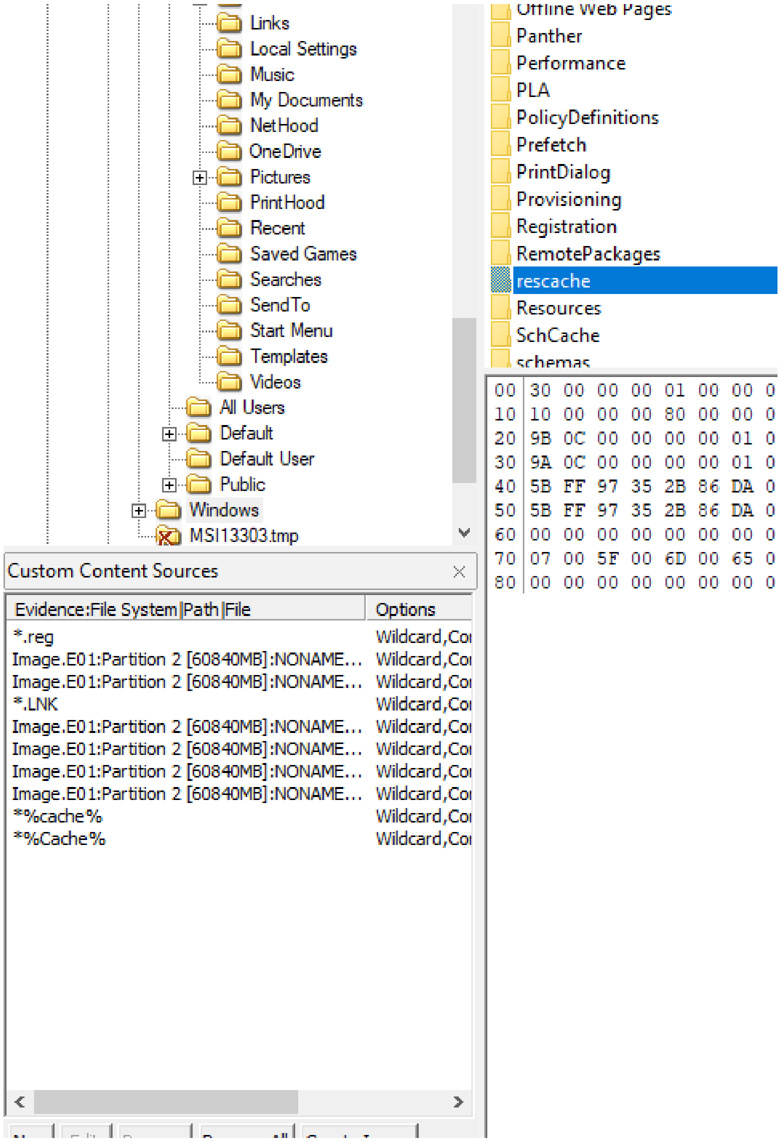
Name	Size	Type	Date Modified
Edge	1	Directory	4/16/2024 12:5...
EdgeCore	1	Directory	4/16/2024 12:5...
EdgeUpdate	1	Directory	4/7/2024 2:10:0...
EdgeWebView	1	Directory	4/16/2024 12:5...
Temp	1	Directory	4/7/2024 12:29:...
$I30	4	NTFS Index All...	3/30/2024 12:2...

```
00 30 00 00 00 01 00 00 00-00 10 00 00 01 00 00 00 0...............
10 10 00 00 00 28 00 00 00-28 00 00 00 01 00 00 00 ....(...(.......
20 00 00 00 00 00 00 00 00-18 00 00 00 03 00 00 00 ................
30 00 00 00 00 00 00 00 00-                        ........
```

Custom Content Sources

Evidence:File System|Path|File	Options
*.reg	Wildcard,Co
Image.E01:Partition 2 [60840MB]:NONAME...	Wildcard,Co
Image.E01:Partition 2 [60840MB]:NONAME...	Wildcard,Co
*.LNK	Wildcard,Co
Image.E01:Partition 2 [60840MB]:NONAME...	Wildcard,Co
Image.E01:Partition 2 [60840MB]:NONAME...	Wildcard,Co
Image.E01:Partition 2 [60840MB]:NONAME...	Wildcard,Co
Image.E01:Partition 2 [60840MB]:NONAME...	Wildcard,Co

- **Fifth including all cache files**

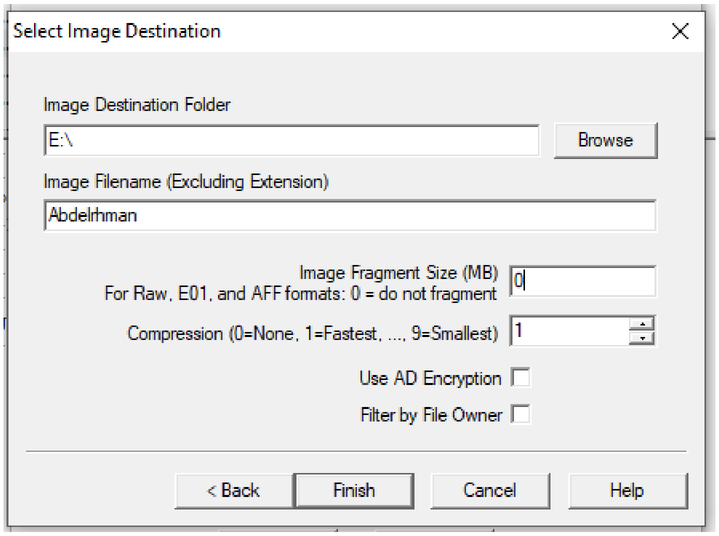


```
00 30 00 00 00 01 00 00 0
10 10 00 00 00 80 00 00 0
20 9B 0C 00 00 00 00 01 0
30 9A 0C 00 00 00 00 01 0
40 5B FF 97 35 2B 86 DA 0
50 5B FF 97 35 2B 86 DA 0
60 00 00 00 00 00 00 00 0
70 07 00 5F 00 6D 00 65 0
80 00 00 00 00 00 00 00 0
```

Custom Content Sources

Evidence:File System|Path|File	Options
*.reg	Wildcard,Co
Image.E01:Partition 2 [60840MB]:NONAME…	Wildcard,Co
Image.E01:Partition 2 [60840MB]:NONAME…	Wildcard,Co
*.LNK	Wildcard,Co
Image.E01:Partition 2 [60840MB]:NONAME…	Wildcard,Co
Image.E01:Partition 2 [60840MB]:NONAME…	Wildcard,Co
Image.E01:Partition 2 [60840MB]:NONAME…	Wildcard,Co
Image.E01:Partition 2 [60840MB]:NONAME…	Wildcard,Co
*%cache%	Wildcard,Co
*%Cache%	Wildcard,Co

- **Finally: extract in new image file :**



Select Image Destination

Image Destination Folder: E:\

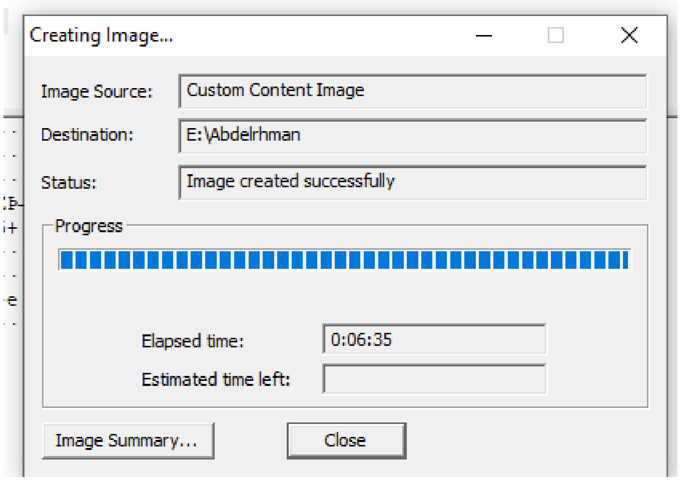
Image Filename (Excluding Extension): Abdelrhman

Image Fragment Size (MB)
For Raw, E01, and AFF formats: 0 = do not fragment: 0

Compression (0=None, 1=Fastest, ..., 9=Smallest): 1

Use AD Encryption □

Filter by File Owner □



Creating Image...

Image Source: Custom Content Image

Destination: E:\Abdelrhman

Status: Image created successfully

Progress

Elapsed time: 0:06:35

Estimated time left: