PES UNIVERSITY

UE19CS336
Digital Forensics

Name : Suhan B Revankar
SRN : PES2UG19CS412
Section : G Section

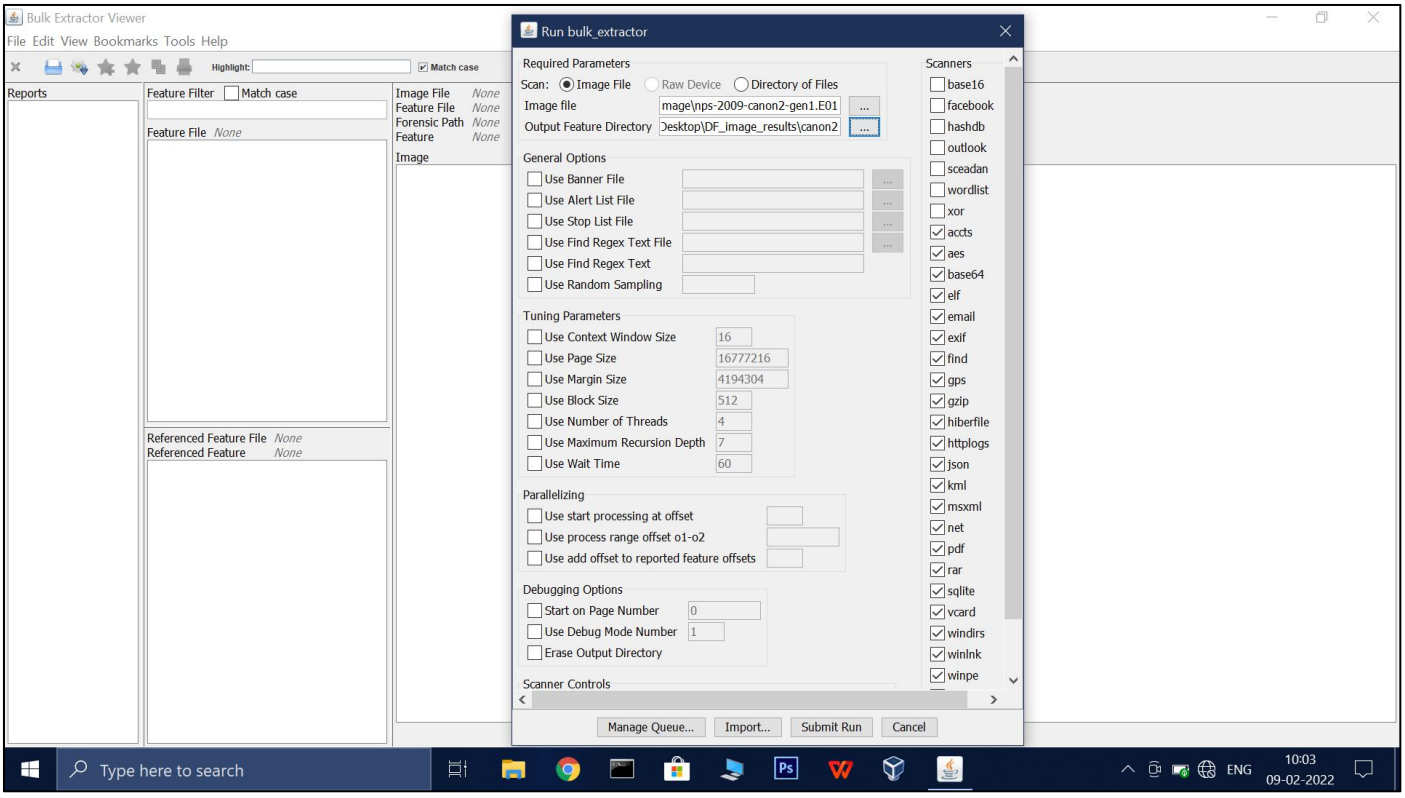
Table of Contents :

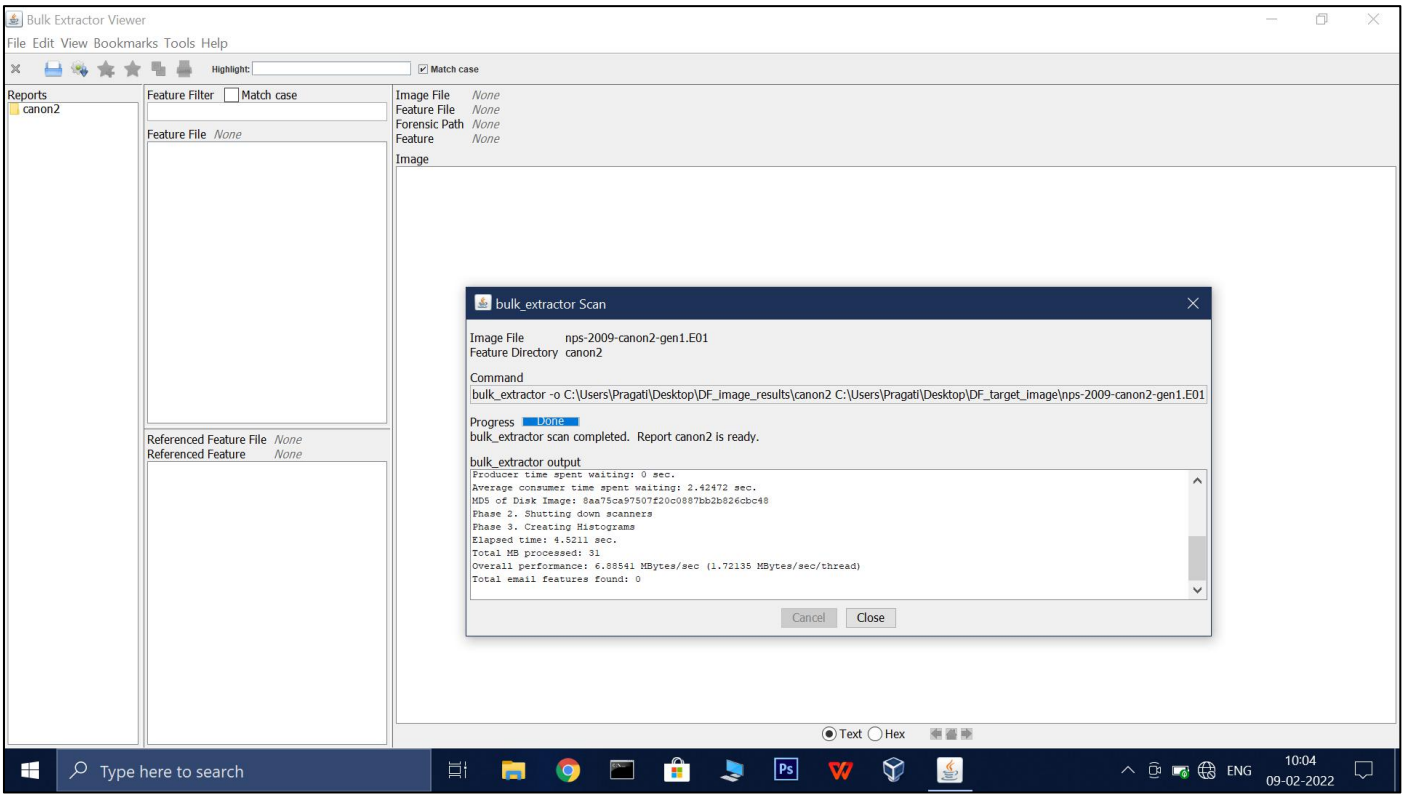
Activity 1

Bulk Extractor retrive data of digital device

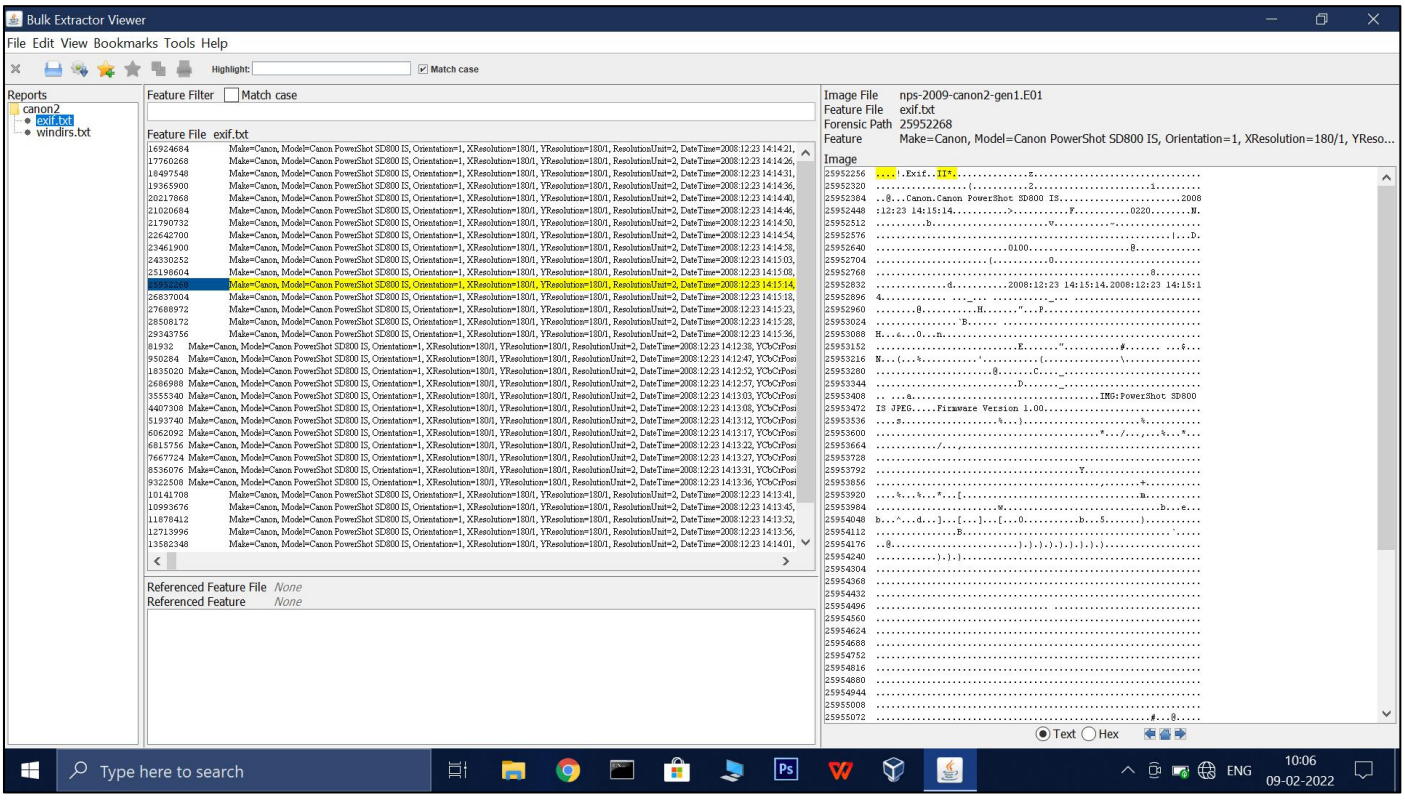
Part 1: Image evidence

1. Open Bulk extractor (requires java 6 for running mandatory)
2. Navigate to Tools -> Run bulk extractor
3. Following window appears
4. Select the source image file for analysis and destination folder to store report
5. Click on ‘Submit run’





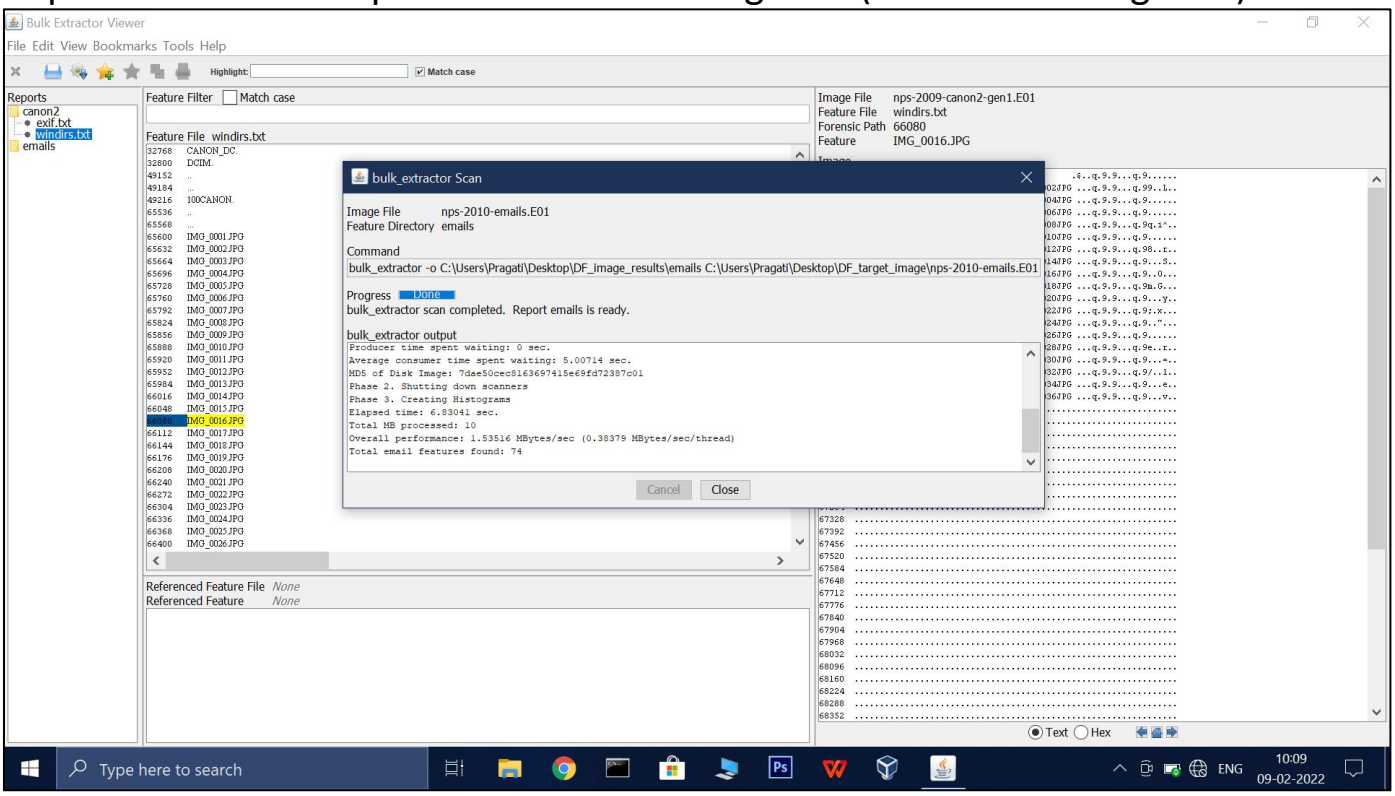
Wait for the process to complete , then click on ‘close’



Then you can see the evidence tree on left-top corner , navigate through them

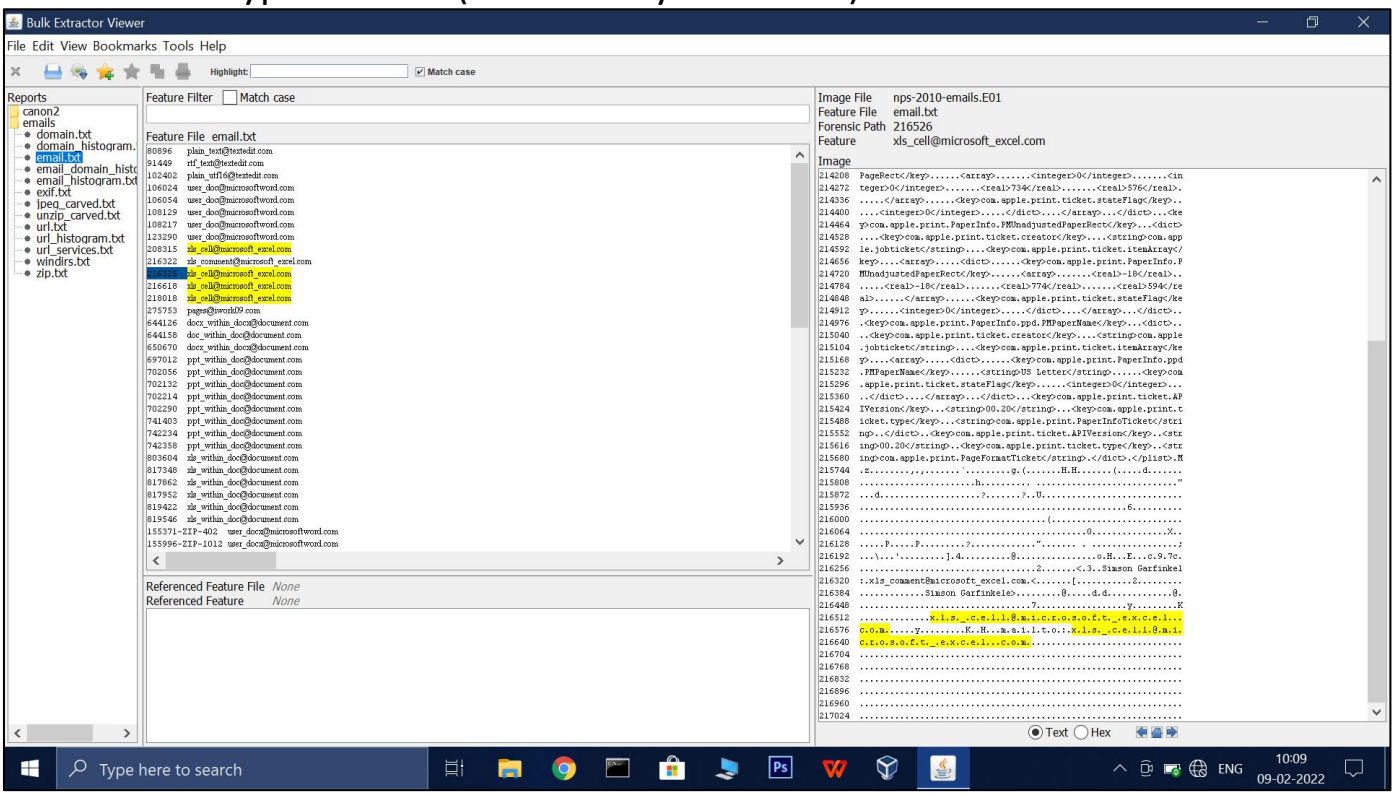
Part 2: Email Evidence

Repeat the above steps but with other image file (here email image file)



Click on ‘close’ once its done
You can see the structure once again

1. Select the type of drive (here its Physical Drive).



Report is also generated in the selected target folder

Email image anaysis Report generated

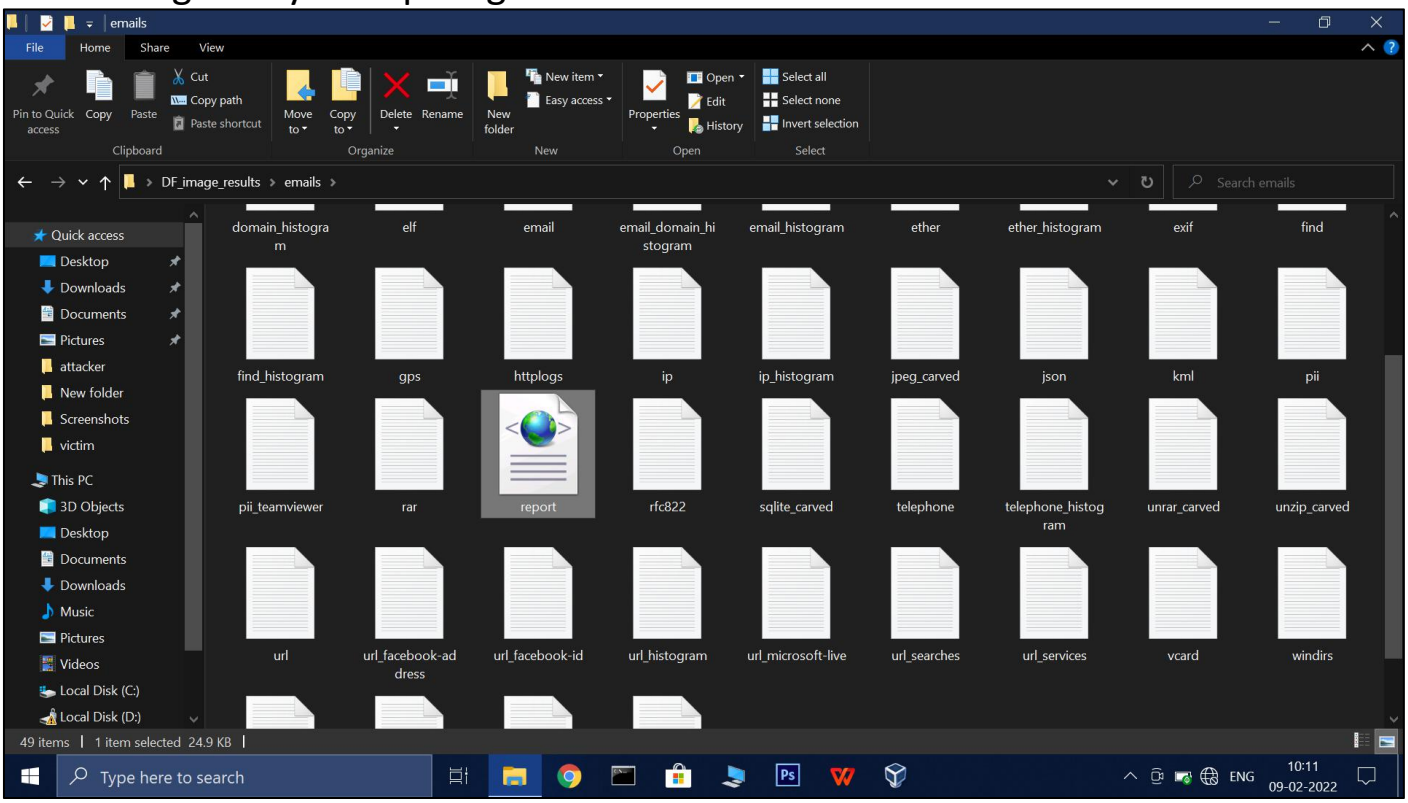
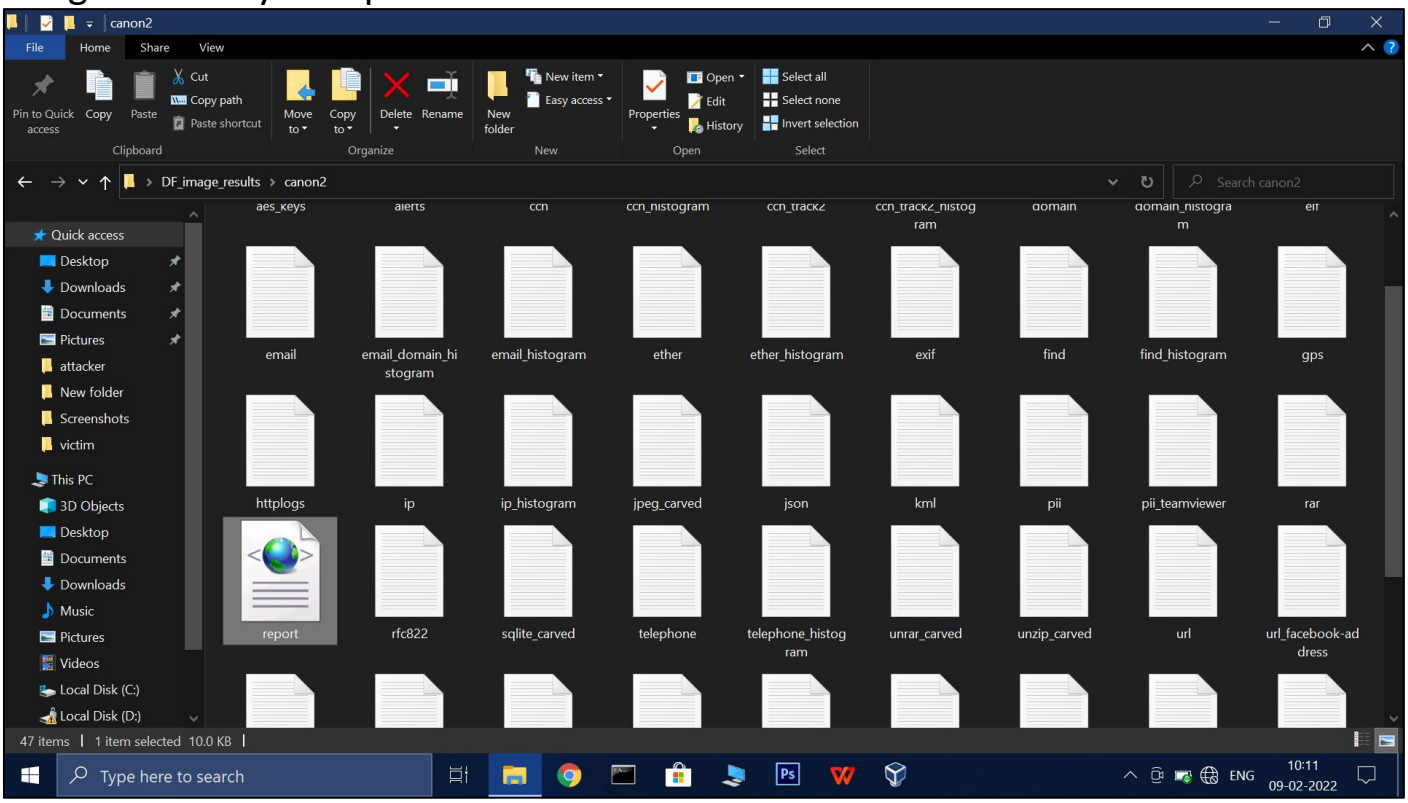


Image file analysis report

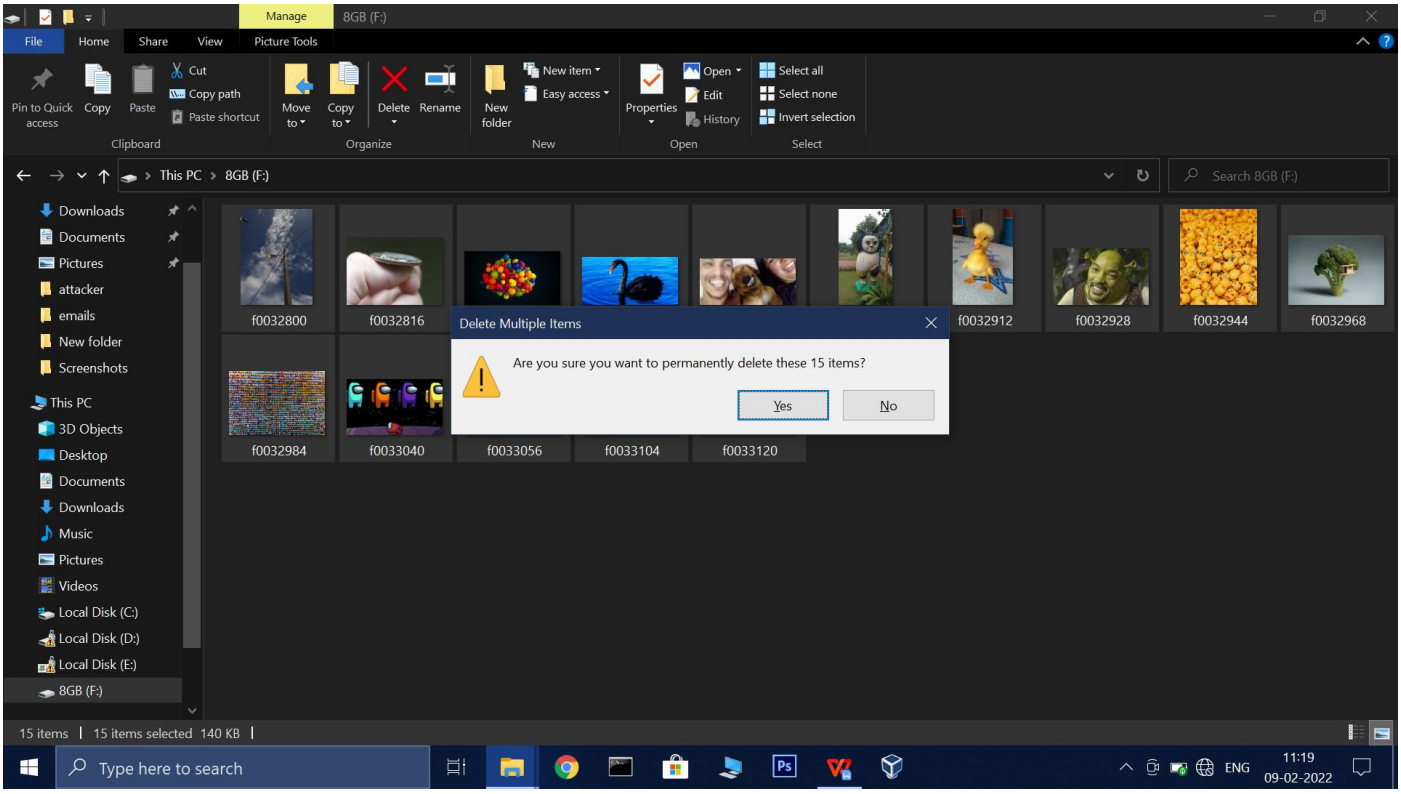


Activity 2

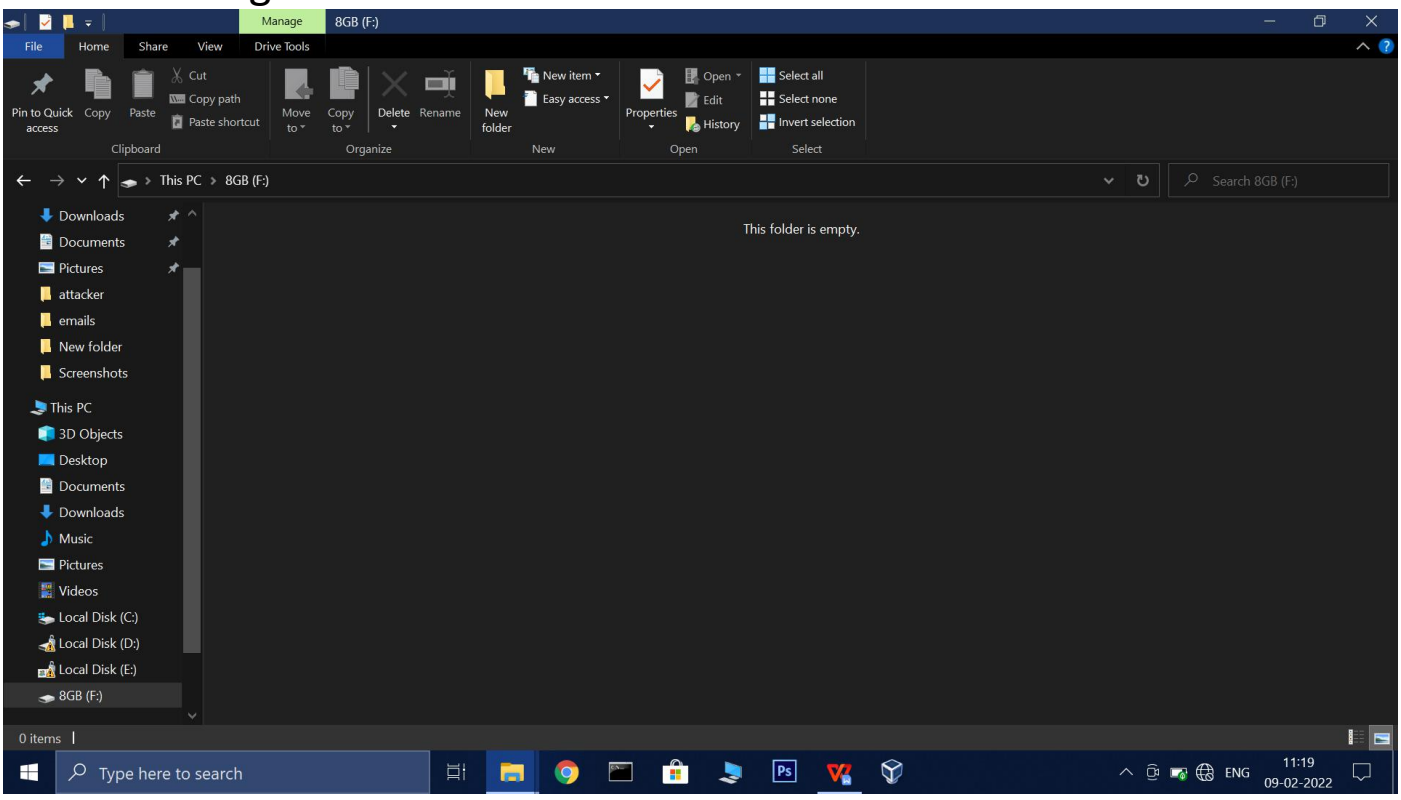
Photorec tool used to recover deleted files from a physical drive as pendrive

Part 1:

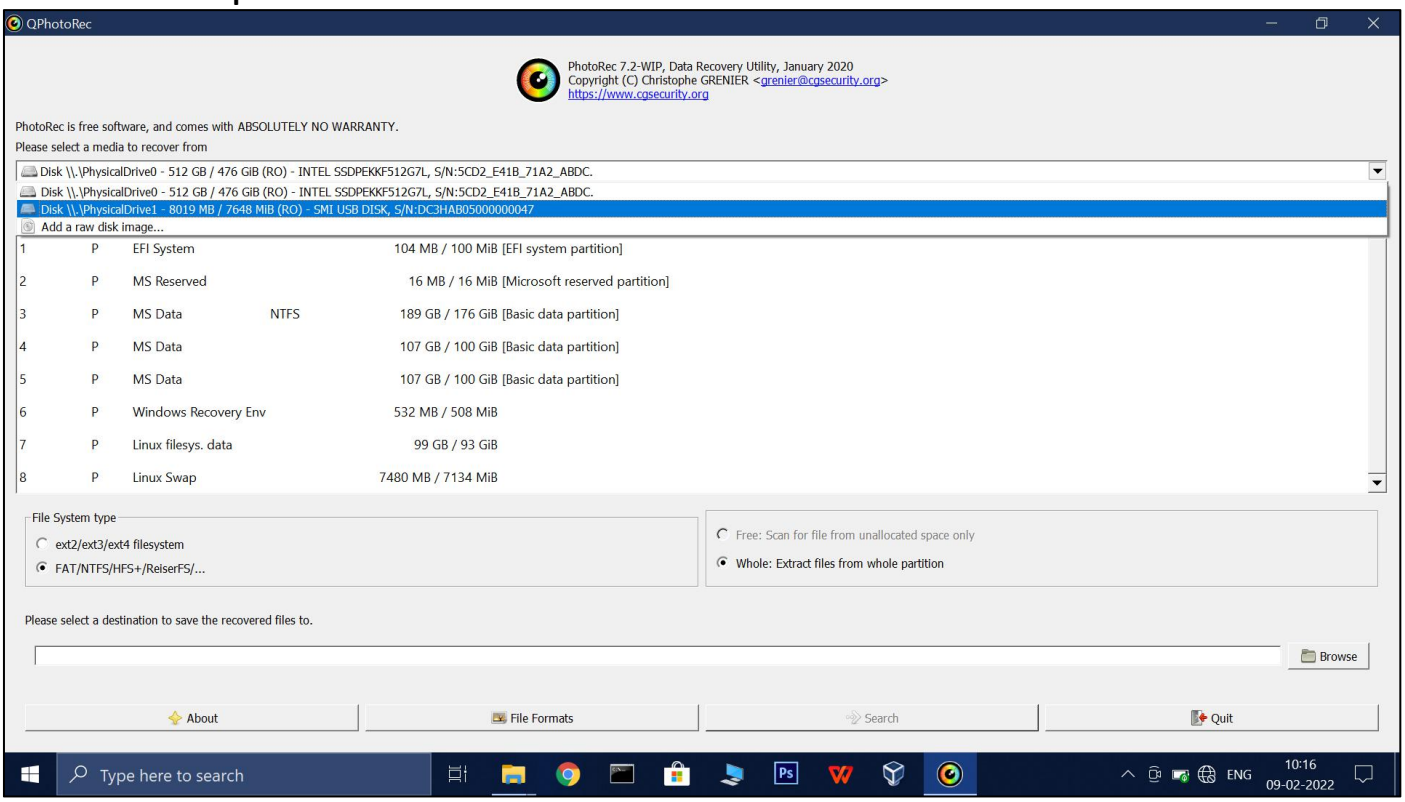
Place images in the physical drive … Delete those files



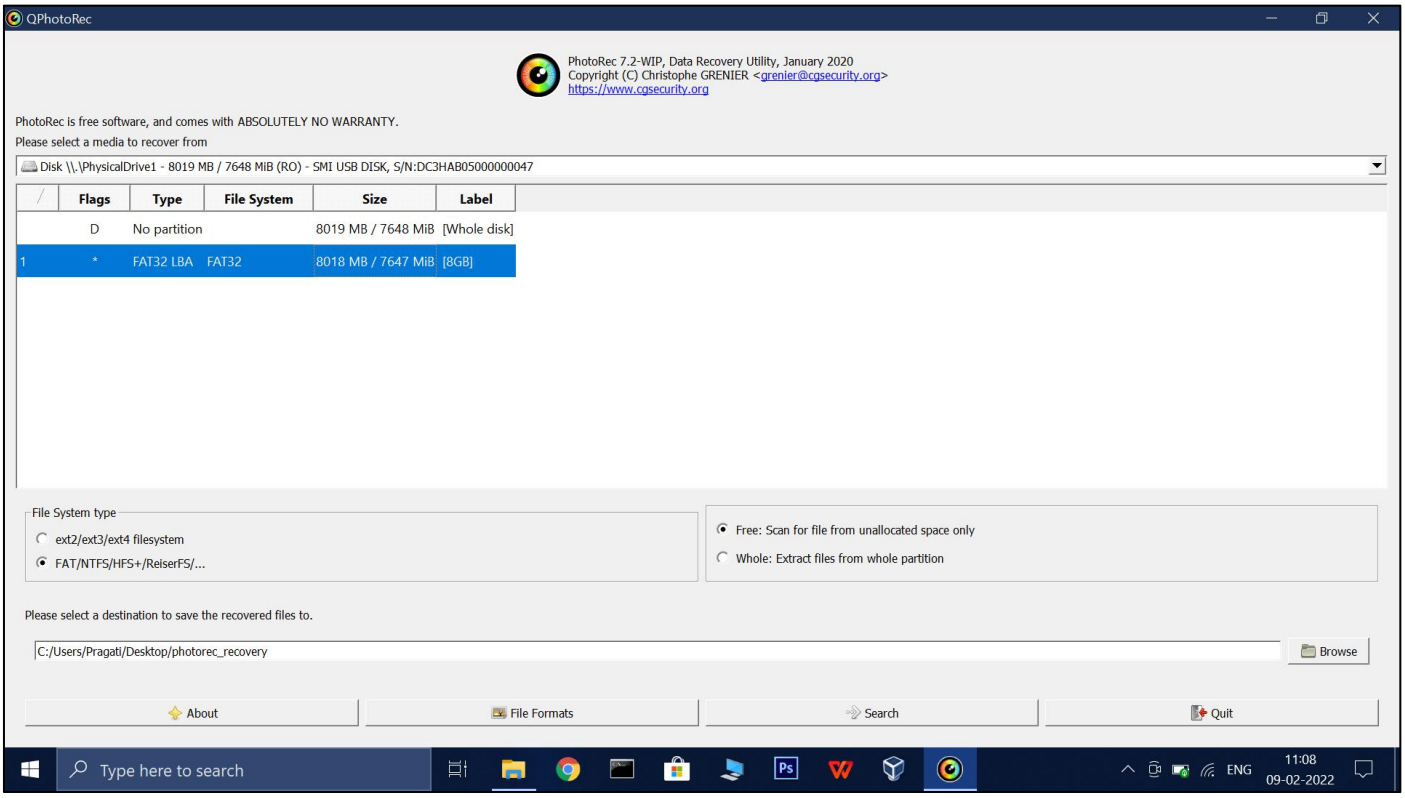
After deleting



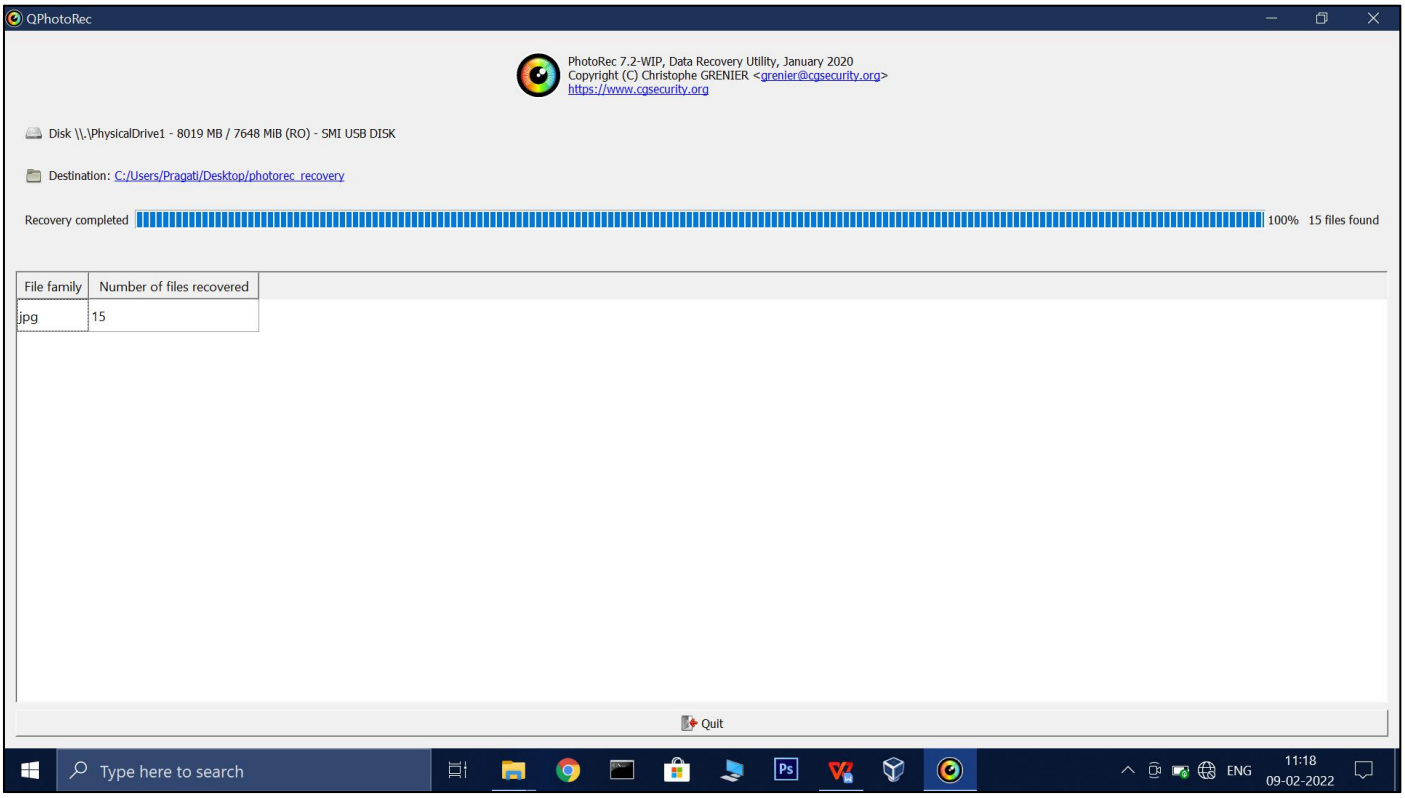
2. Start the photorec tool



Select the target physical drive

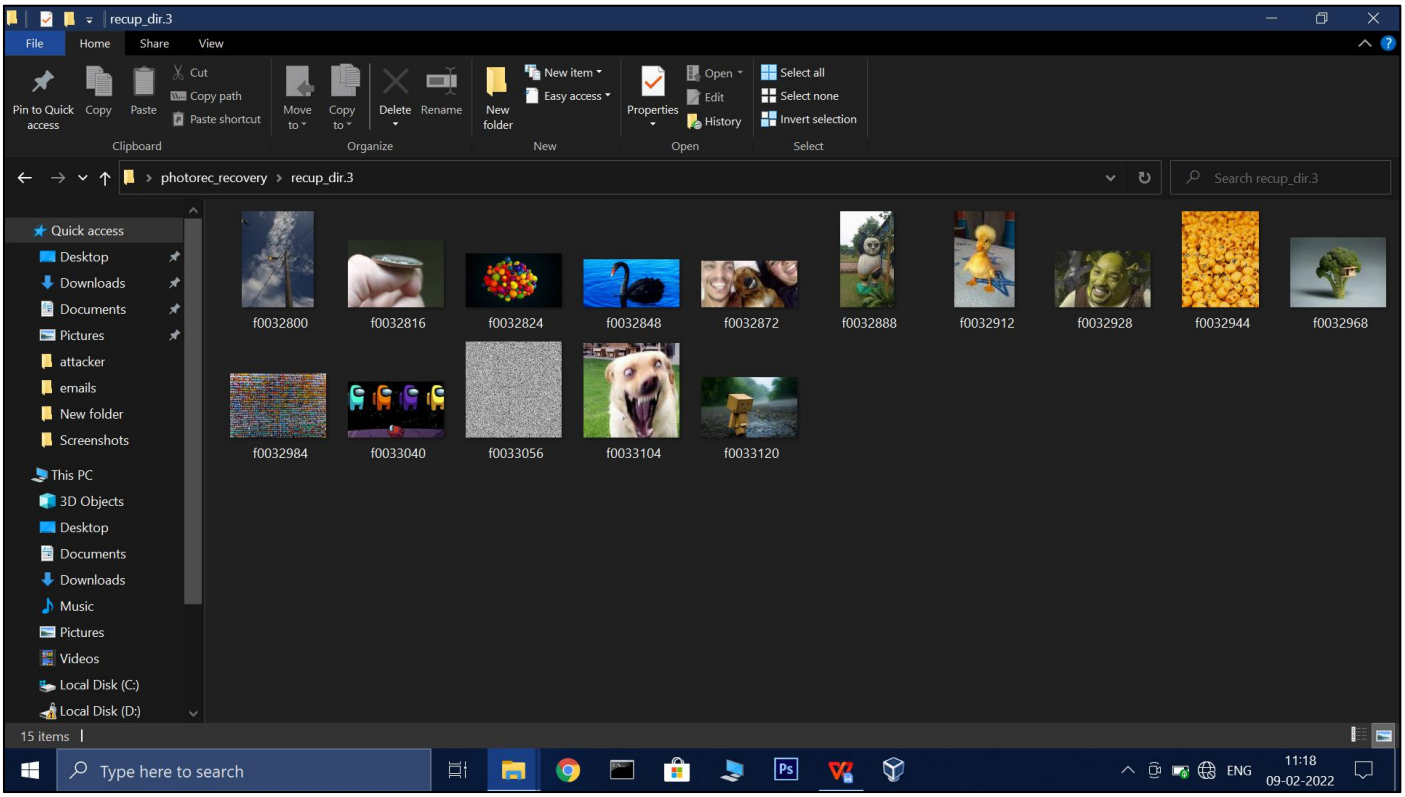


Select the destination folder to restore the deleted files . then click on ‘search’



Once process is finished click on ‘quit’

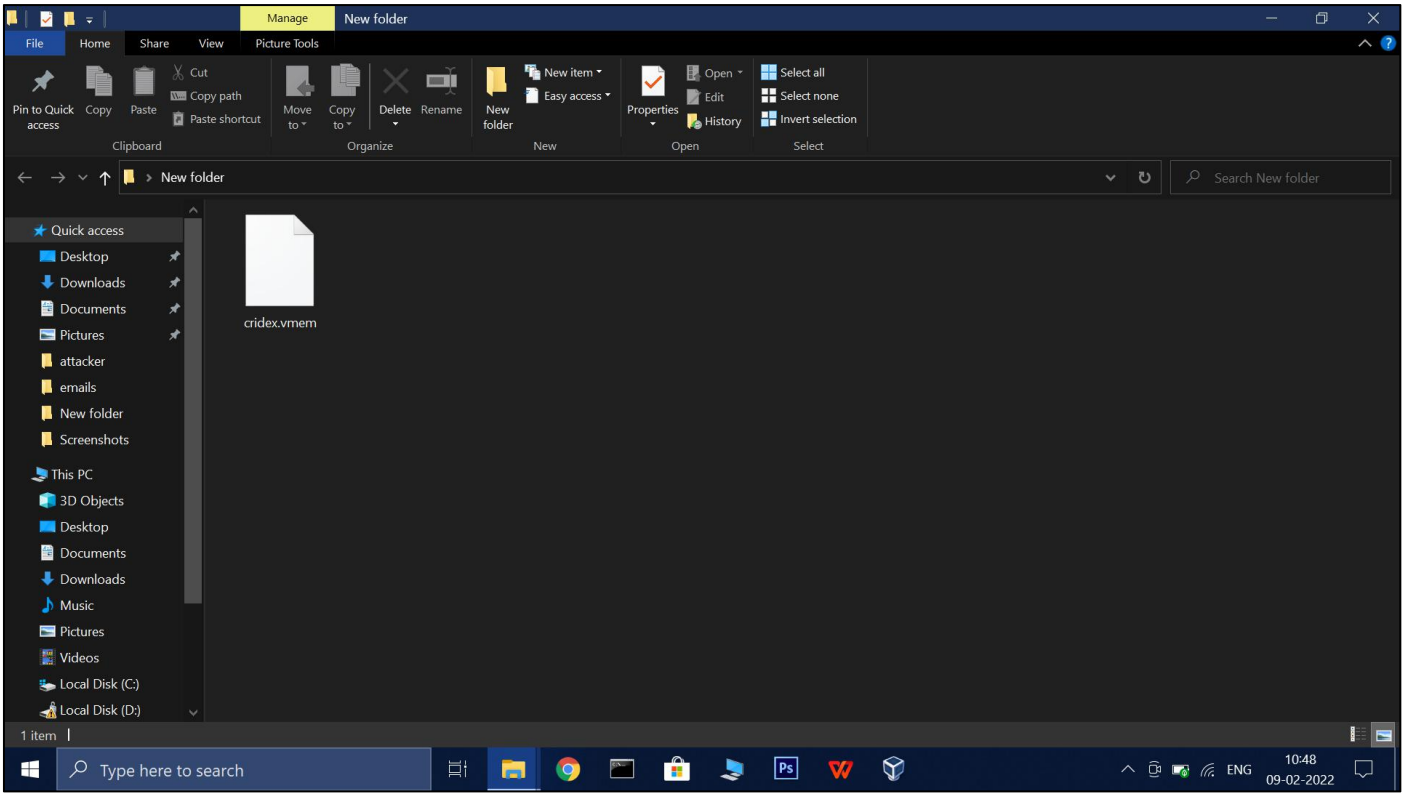
After the process is completed go to the destination folder selected earlier and you will see the directory has contains recovered files .



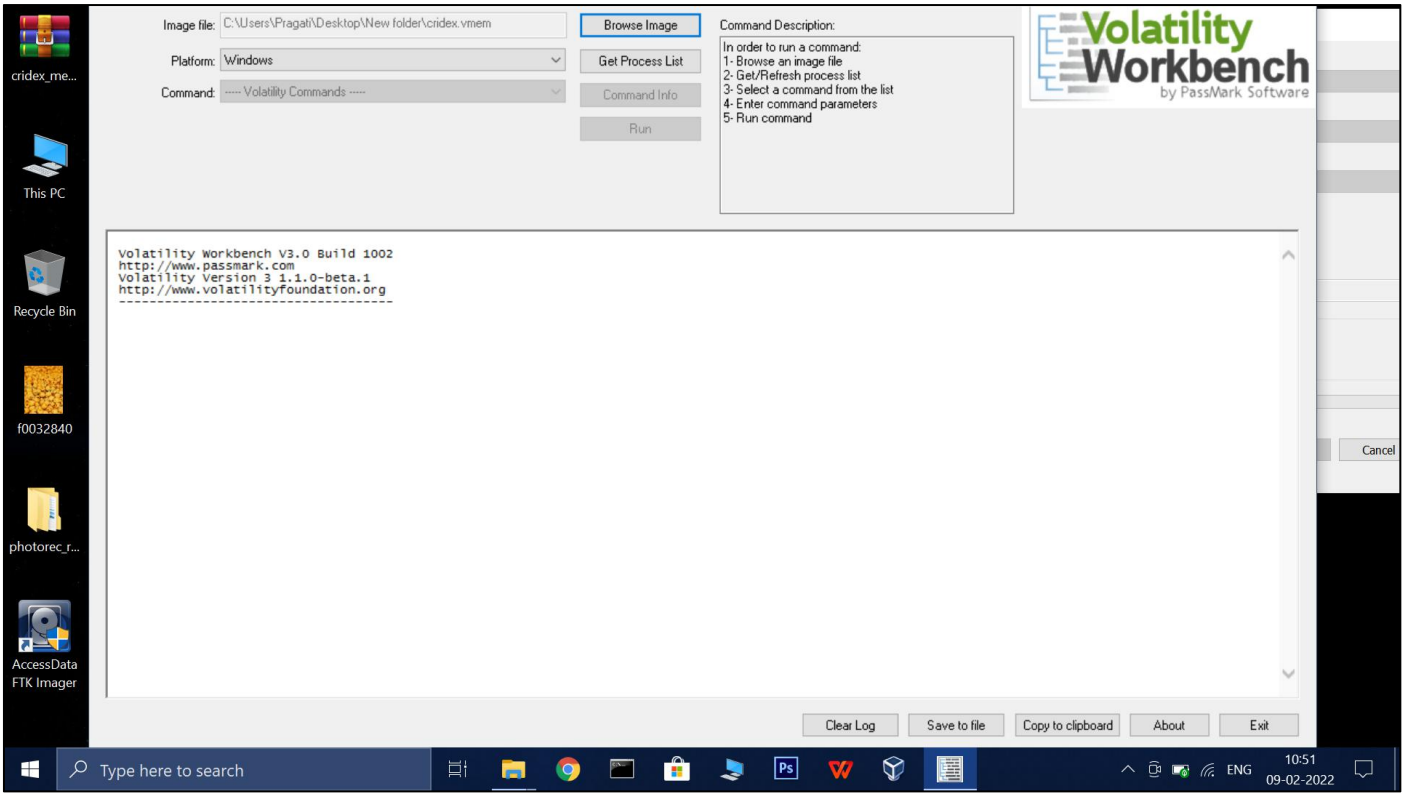
Activity 3

Volatility Workbench , perform memory analysis of a computer

1. Obtain a sample memory dump from the internet and extract it place it in a folder



2. Launch the volatility workbench choose the target file placed in above folder and click on ‘Get process list’



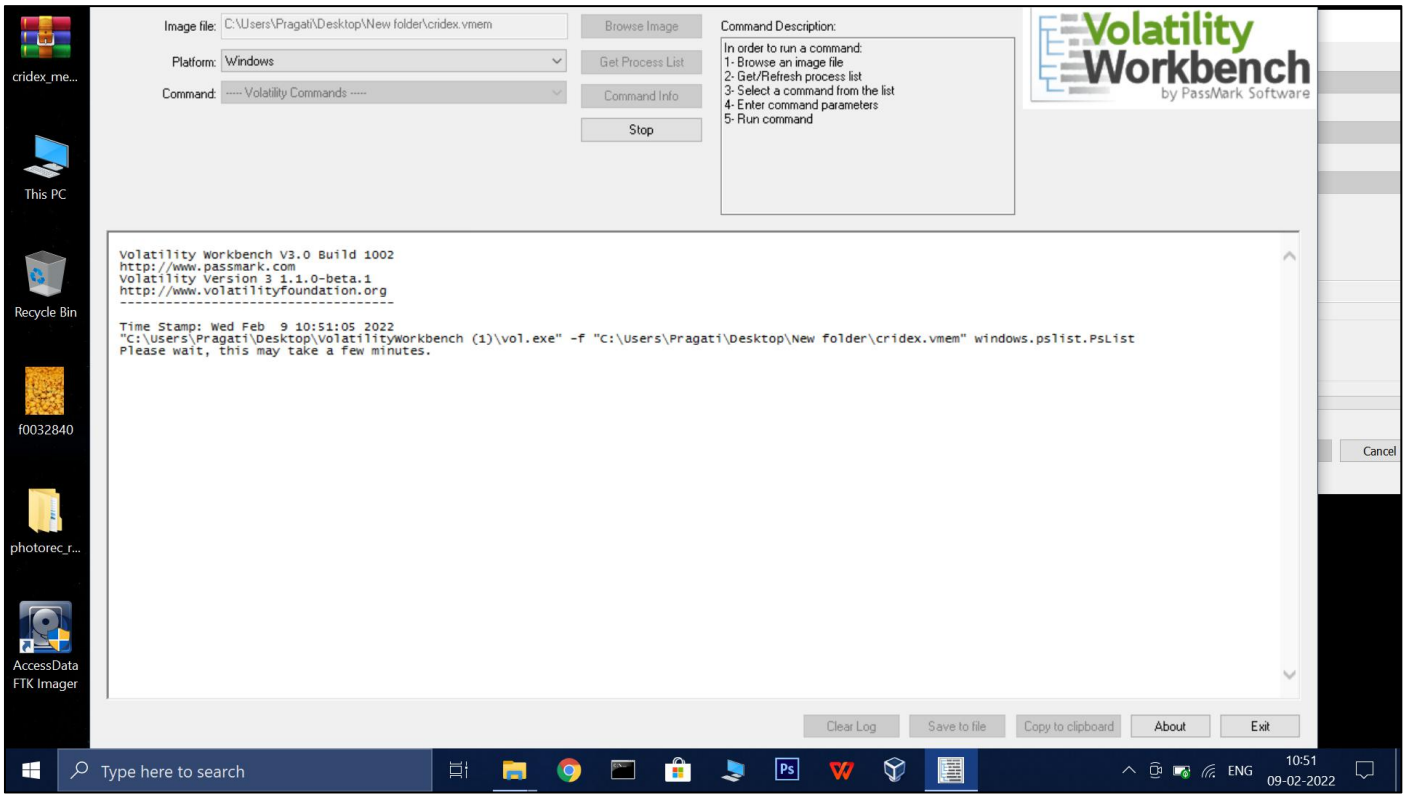


Image file: C:\Users\Pragati\Desktop\New folder\cridex.vmem
Browse Image
Platform: Windows
Get Process List
Command: ----- Volatility Commands -----
Command Info
Stop
Command Description:
In order to run a command:
1- Browse an image file
2- Get/Refresh process list
3- Select a command from the list
4- Enter command parameters
5- Run command
Volatility Workbench
by PassMark Software
Volatility Workbench V3.0 Build 1002
http://www.passmark.com
Volatility Version 3 1.1.0-beta.1
http://www.volatilityfoundation.org
Time Stamp: Wed Feb 9 10:51:05 2022
"C:\Users\Pragati\Desktop\VolatilityWorkbench (1)\vol.exe" -f "C:\Users\Pragati\Desktop\New folder\cridex.vmem" windows.pslist.PsList
Please wait, this may take a few minutes.
Clear Log
Save to file
Copy to clipboard
About
Exit
Cancel
cridex_me...
This PC
Recycle Bin
f0032840
photorec_r...
AccessData FTK Imager
Type here to search
ENG
10:51
09-02-2022

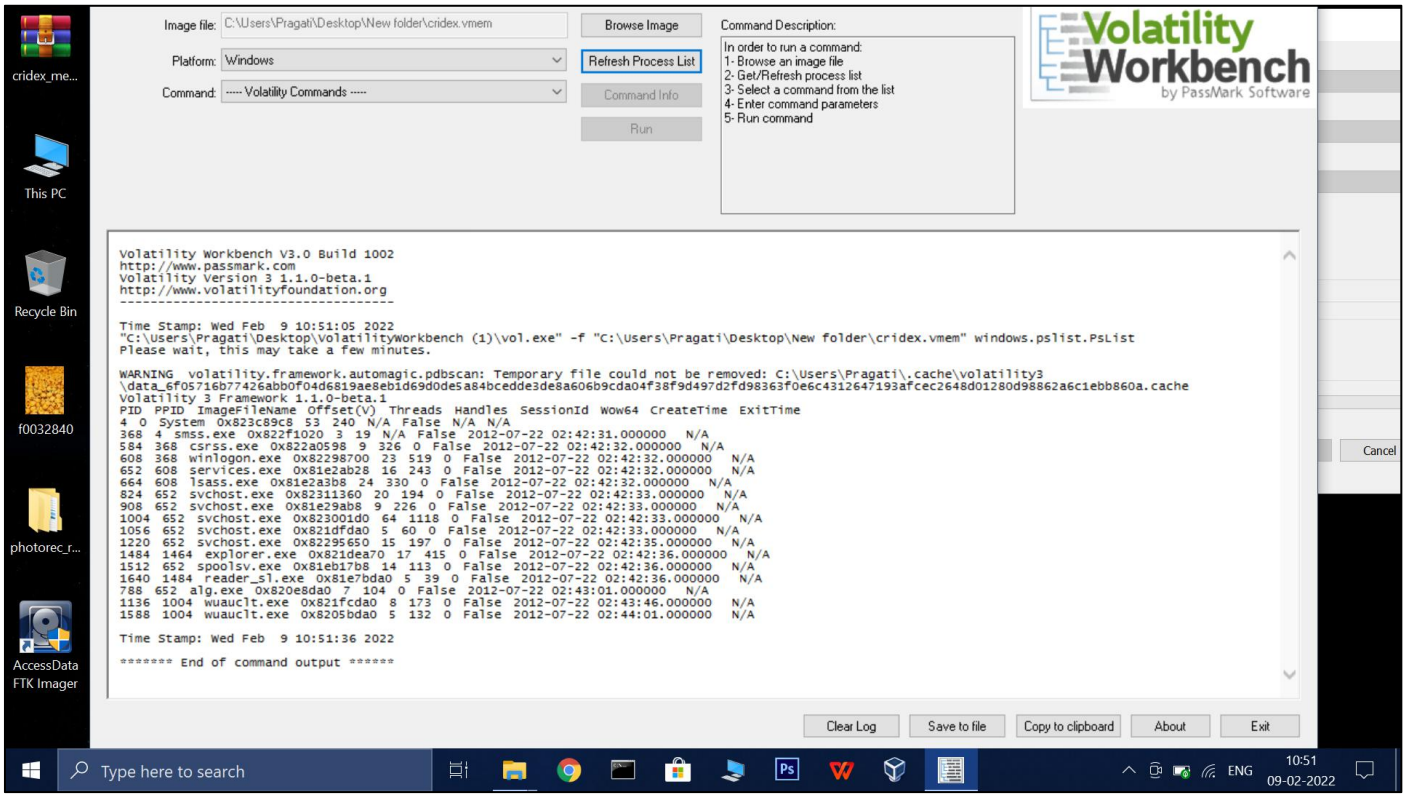
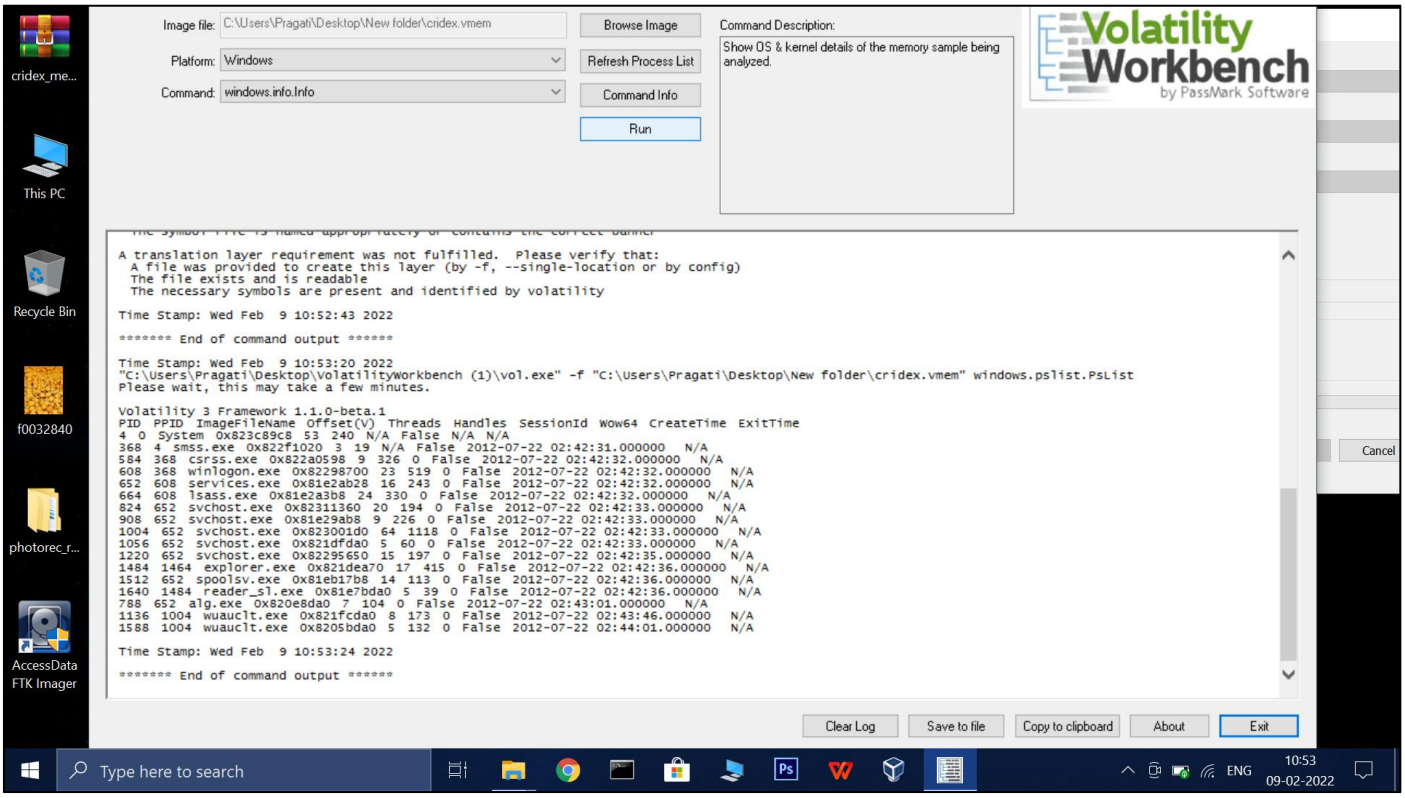
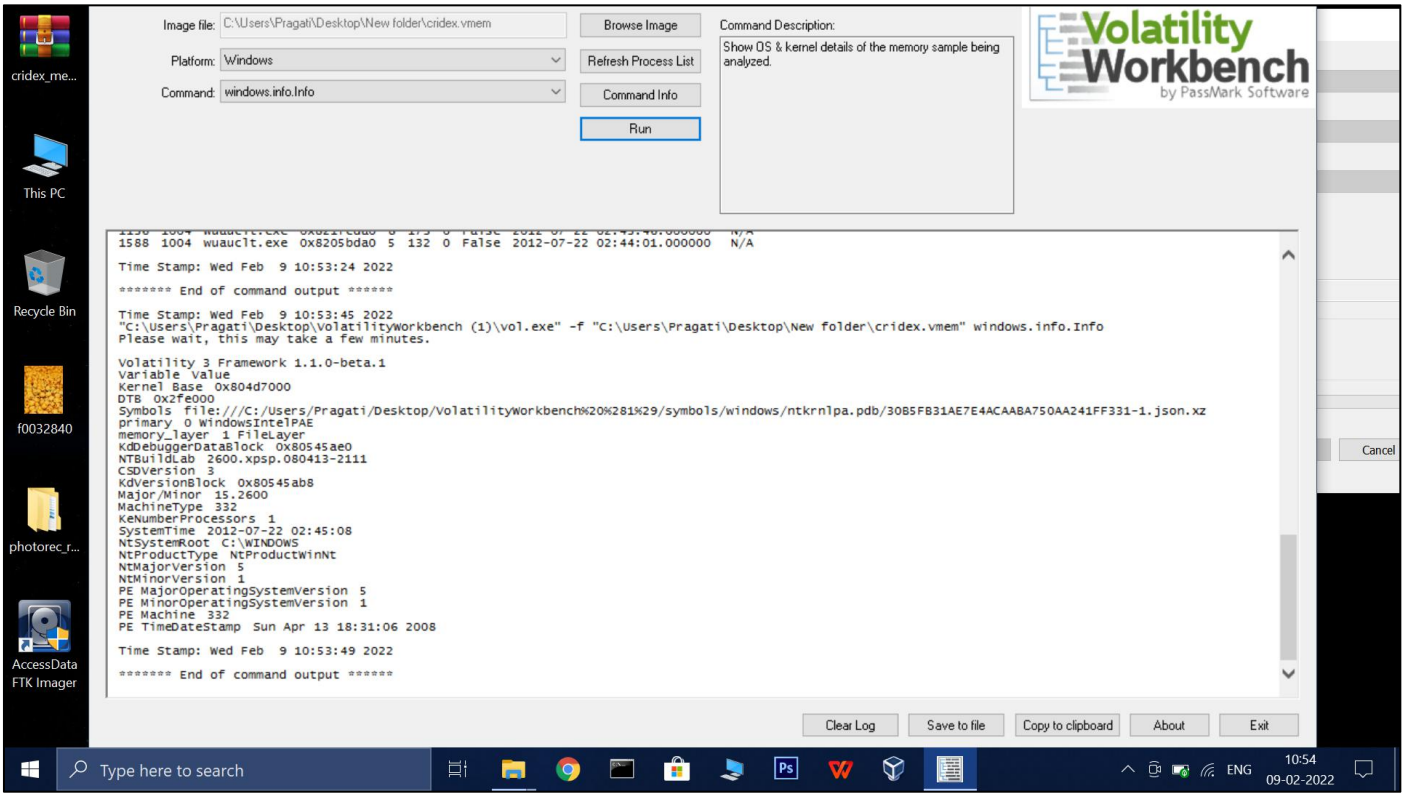


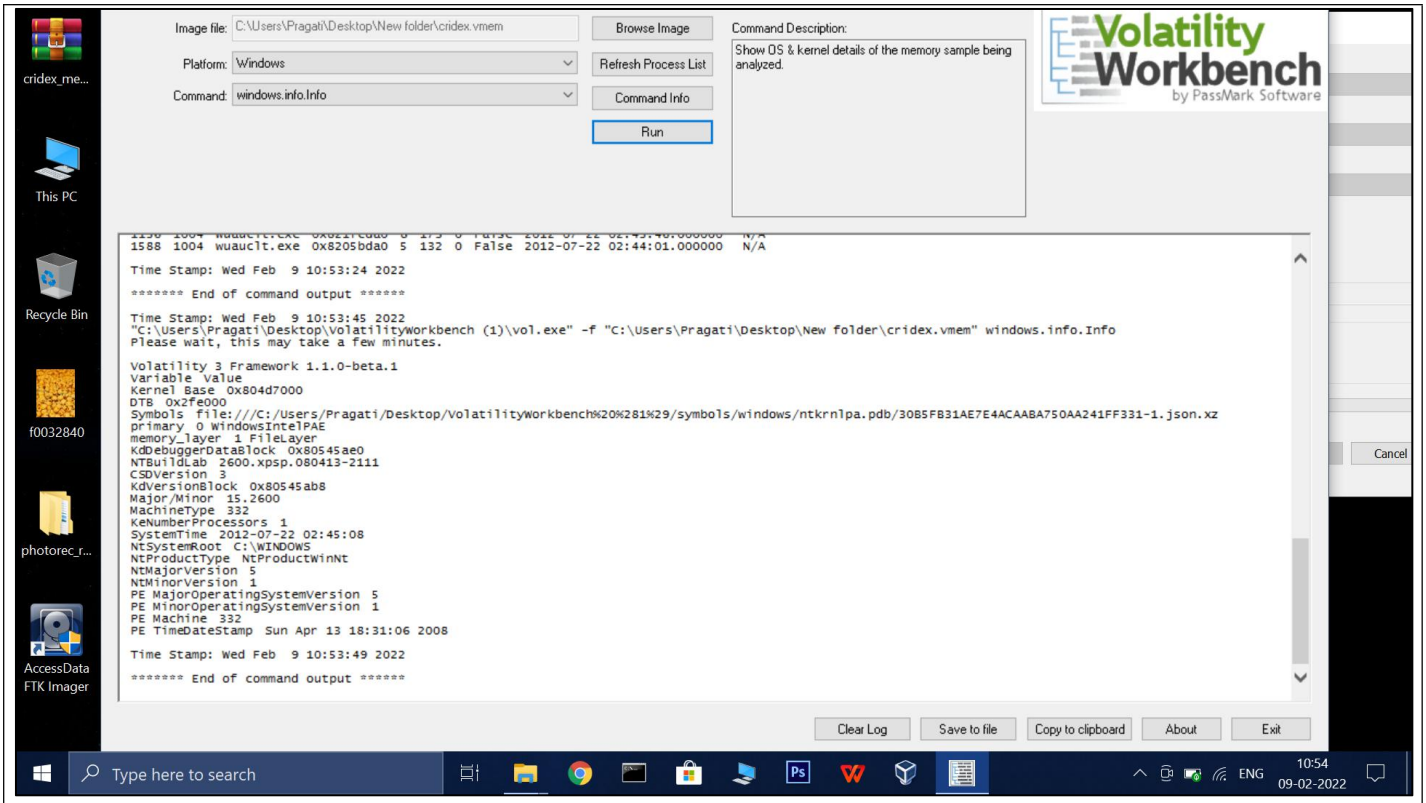
Image file: C:\Users\Pragati\Desktop\New folder\cridex.vmem
Browse Image
Platform: Windows
Refresh Process List
Command: ----- Volatility Commands -----
Command Info
Run
Command Description:
In order to run a command:
1- Browse an image file
2- Get/Refresh process list
3- Select a command from the list
4- Enter command parameters
5- Run command
Volatility Workbench
by PassMark Software
Volatility Workbench V3.0 Build 1002
http://www.passmark.com
Volatility Version 3 1.1.0-beta.1
http://www.volatilityfoundation.org
Time Stamp: Wed Feb 9 10:51:05 2022
"C:\Users\Pragati\Desktop\VolatilityWorkbench (1)\vol.exe" -f "C:\Users\Pragati\Desktop\New folder\cridex.vmem" windows.pslist.PsList
Please wait, this may take a few minutes.
WARNING volatility.framework.automagic.pdbscan: Temporary file could not be removed: C:\Users\Pragati\.cache\volatility3\data_6f057 16b7426abb0f04d6819ae8eb1d69d0de5a84bcedde3de8a606b9cda04f38f9d497d2fd98363f0e6c4312647193afcec2648d01280d98862a6c1ebb860a.cache
Volatility 3 Framework 1.1.0-beta.1
PID PPID ImageFileName Offset(V) Threads Handles SessionId Wow64 CreateTime ExitTime
4 0 System 0x823c89c8 53 240 N/A False N/A N/A
368 4 smss.exe 0x822f1020 3 19 N/A False 2012-07-22 02:42:31.000000 N/A
584 368 csrss.exe 0x822a0598 9 326 0 False 2012-07-22 02:42:32.000000 N/A
608 368 winlogon.exe 0x82298700 23 519 0 False 2012-07-22 02:42:32.000000 N/A
652 608 services.exe 0x81e2ab28 16 243 0 False 2012-07-22 02:42:32.000000 N/A
664 608 lsass.exe 0x81e2a3b8 24 330 0 False 2012-07-22 02:42:32.000000 N/A
824 652 svchost.exe 0x82311360 20 194 0 False 2012-07-22 02:42:33.000000 N/A
908 652 svchost.exe 0x81e29ab8 9 226 0 False 2012-07-22 02:42:33.000000 N/A
1004 652 svchost.exe 0x823001d0 64 1118 0 False 2012-07-22 02:42:33.000000 N/A
1056 652 svchost.exe 0x821dfda0 5 60 0 False 2012-07-22 02:42:33.000000 N/A
1220 652 svchost.exe 0x82295650 15 197 0 False 2012-07-22 02:42:35.000000 N/A
1484 1464 explorer.exe 0x821dea70 17 415 0 False 2012-07-22 02:42:36.000000 N/A
1512 652 spoolsv.exe 0x81eb17b8 14 113 0 False 2012-07-22 02:42:36.000000 N/A
1640 1484 reader_sl.exe 0x81e7bda0 5 39 0 False 2012-07-22 02:42:36.000000 N/A
788 652 alg.exe 0x820e8da0 7 104 0 False 2012-07-22 02:43:01.000000 N/A
1136 1004 wuauclt.exe 0x821fcda0 8 173 0 False 2012-07-22 02:43:46.000000 N/A
1588 1004 wuauclt.exe 0x8205bda0 5 132 0 False 2012-07-22 02:44:01.000000 N/A
Time Stamp: Wed Feb 9 10:51:36 2022
******* End of command output ******
Clear Log
Save to file
Copy to clipboard
About
Exit
Cancel
cridex_me...
This PC
Recycle Bin
f0032840
photorec_r...
AccessData FTK Imager
Type here to search
ENG
10:51
09-02-2022

Under command section various commands are available and then click on run as per your needs

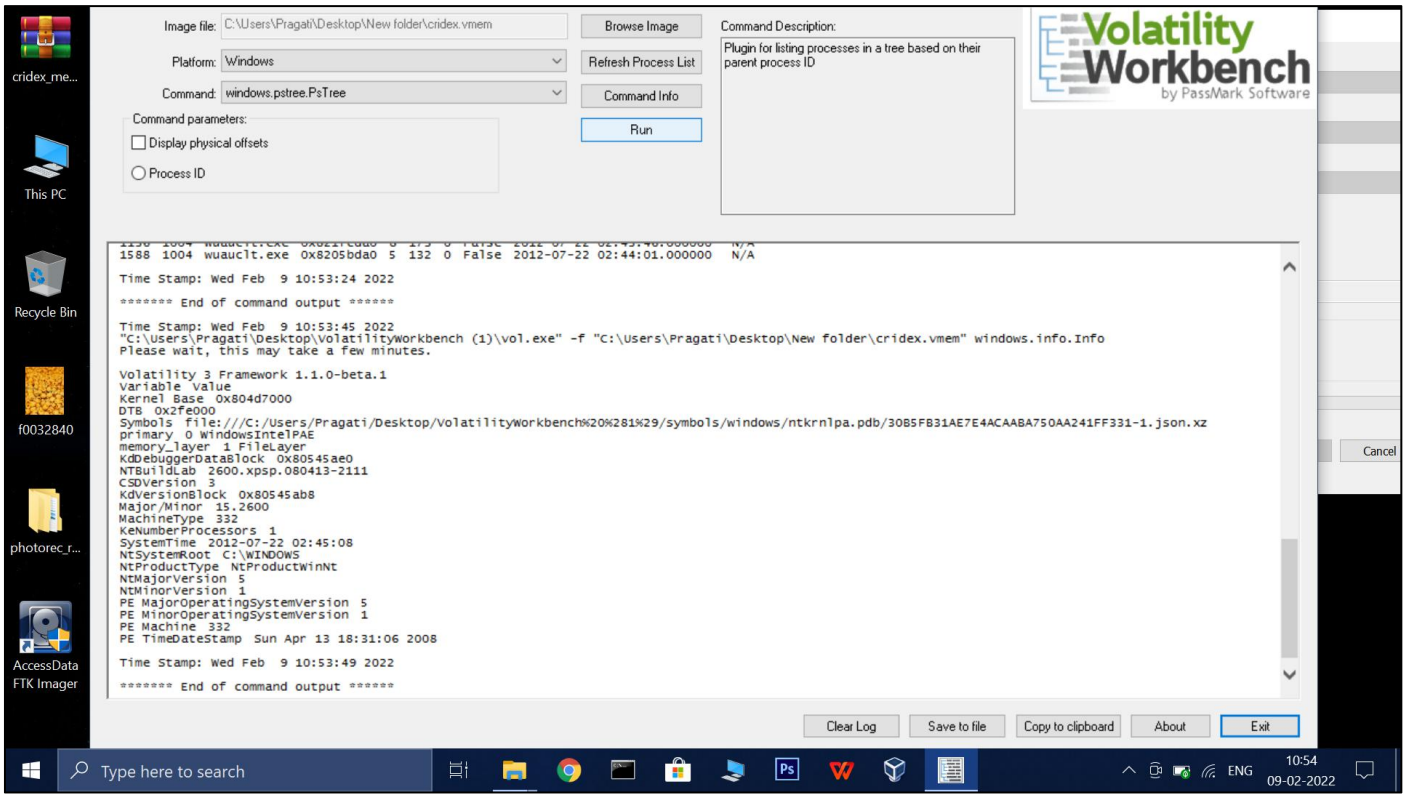
I. windows.info.info

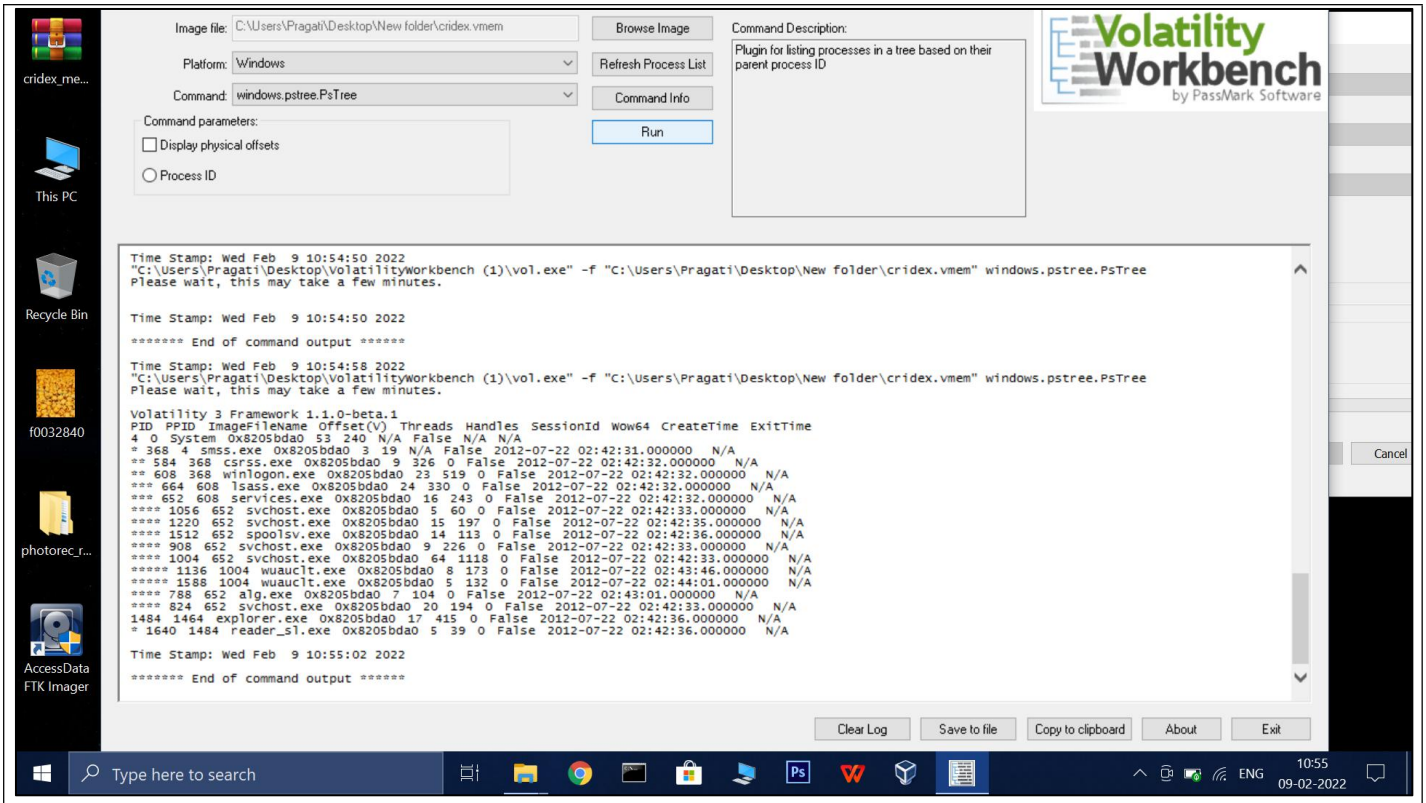




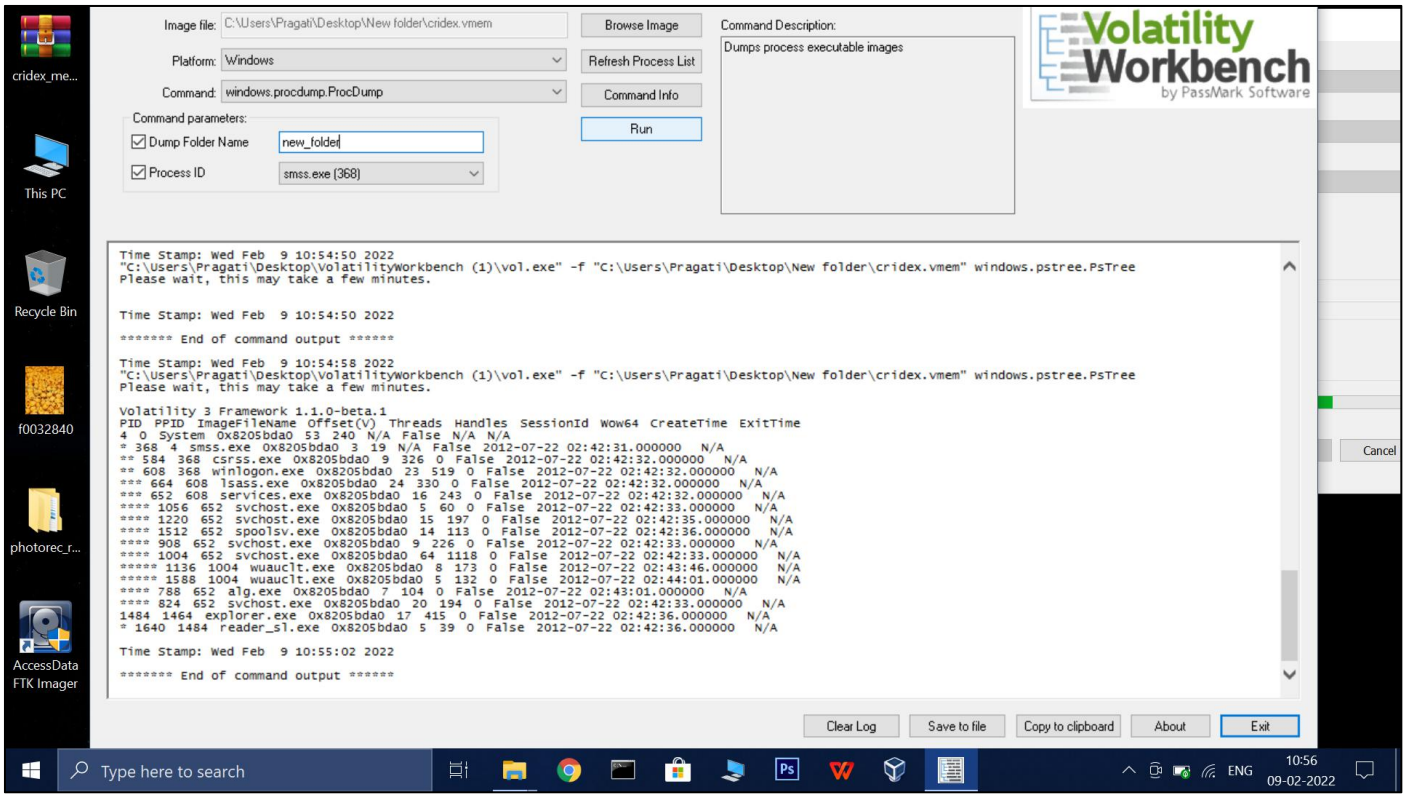


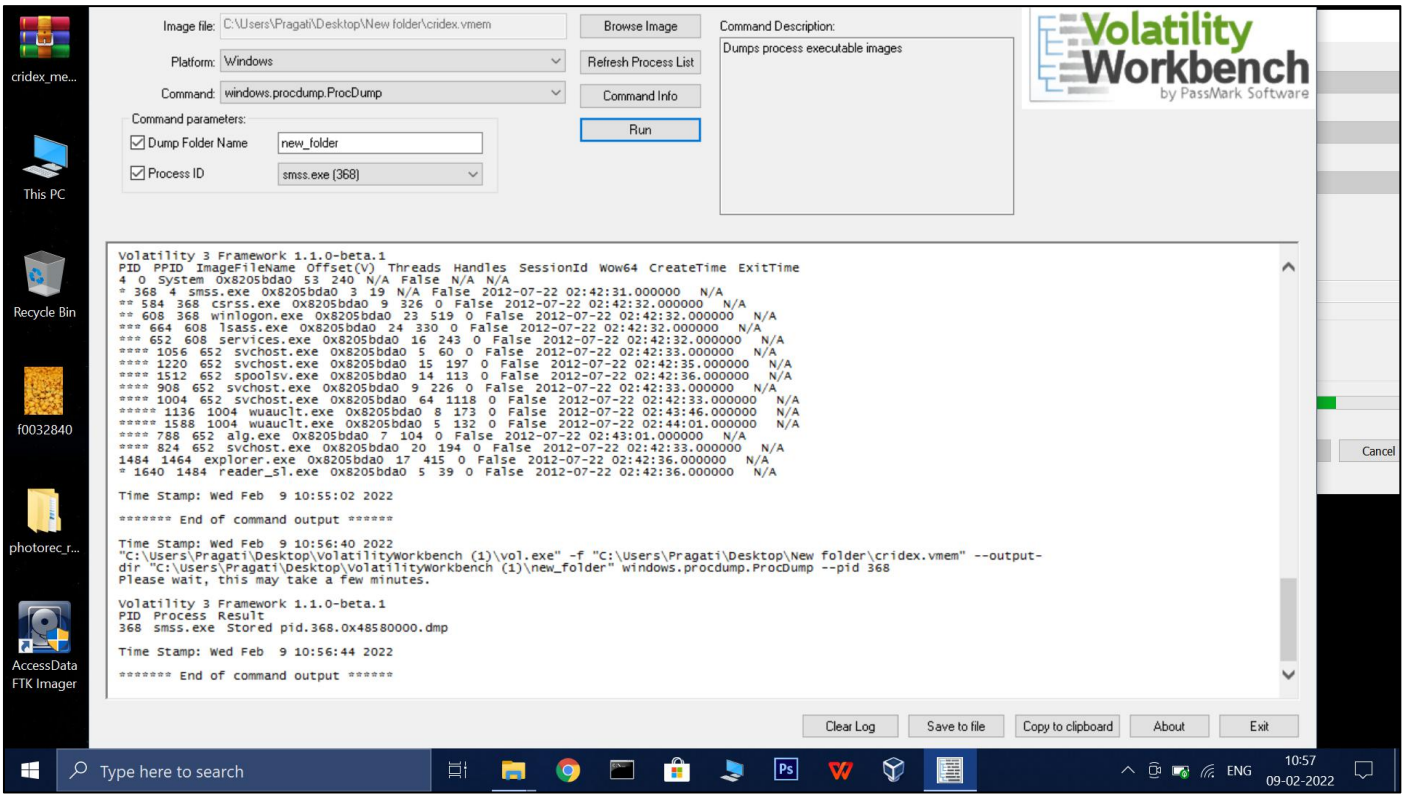
Ii. Windows.pstree.PsTree



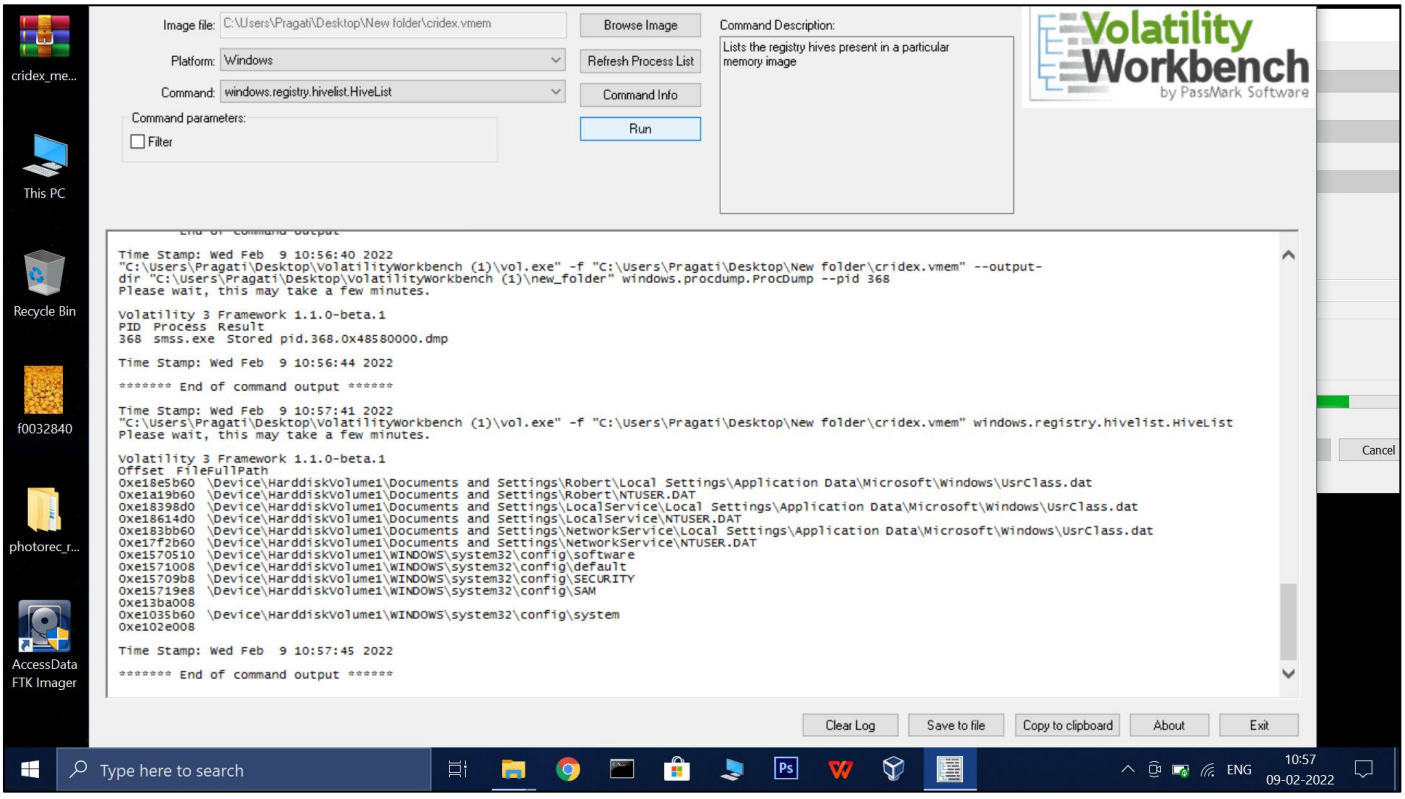


Iii. Windows.procdump.ProcDump





lv.windows.registry.hivelist.HiveList



******