LOVELY PROFESSIONAL UNIVERSITY

PHAGWARA, PUNJAB

CONTINUOUS ASSESSMENT 3

OPEN-SOURCE TECHNOLOGY (INT 301)

SUBMITTED TO

DR. MANJOT KAUR

UID: 28925

SUBMITTED BY

MOHAMMAD AREEB AHMAD

REGISTRATION NUMBER: 11909058

INDEX TABLE

OBJECTIVE OF THE PROJECT

Use any open-source software to generate report to acquire and analyse the volatile data that is temporarily stored in random access memory of the machine.

DESCRIPTION OF THE PROJECT

Data acquisition device done on a system is usually just for the acquired data information that exists on the hard disk but in this project we are performing data acquisition for the acquired data in random access memory. The focus of this study is to acquire data in random access memory and generate report. In order to record and generate a report to analyse the data stored in the random access memory of the system, we shall be using AccessData FTK Imager.

AccessData produces the computer forensics software known as Forensic Toolkit or FTK. This is a commercial product that runs on Windows. This FTK Imager tool has the ability to both gather and examine digital forensic evidence.

There are two basic categories for the evidence that FTK Imager can gather. As follows:

1. Acquiring volatile memory (RAM)
2. Acquiring non – volatile memory (ROM)

This report focusses on the scope of acquiring volatile memory i.e. random access memory.

SCOPE OF THE PROJECT

The likelihood of cybercrime is rising along with the usage of computers in crimes. Cybercrime is committed not only to disable a network server but also to steal vital information from a person, group, or company. Now occurring cybercrime cases have already resulted in the theft of user id, also known as a username, email, and password, which some individuals attribute to protect their private personal information. Concerns regarding the Facebook account and online banking are two examples of this information. The lawful account owner could be harmed if the user id and password were misused by those who are not responsible for understanding how to steal other people's stuff. Moreover, the outcome of theft of bank accounts could lead to severe financial damages to the concerned individual or group.

Hence, we apply computer forensic tools in order to gather evidence and generate a report and analyse the data stored in volatile memory of the system.

Link Of Repository : https://github.com/iareebahmad/CAsubmission

TARGET SYSTEM DESCRIPTION

In order to implement digital forensics using FTK Imager, we need to decide the approach of attempt for the target system. This technology may be applied in one of two ways for acquiring forensic images:

1. Opening the FTK Imager portable version from the evidence machine via a USB flash drive or HDD. The evidence PC or laptop is turned on when using this method for live data gathering.

2. Setting up FTK Imager on the laptop of the investigator. In this situation, the investigator's laptop should mount the source disc using a write blocker.

The write blocker restricts access to the investigator's laptop to read-only operations while preventing data modification in the evidence source drive. The source disk's integrity is preserved as a result.

In this report we will be focusing on opening the FTK Imager portable version from the evidence machine via a USB flash drive or hard disk drive.

Clear with the approach of the target system, we are now in state to define other details of the target system.

Target System’s OS: Windows 10 Home

Target System’s RAM : 12.0 GB (11.9 GB Usable)

Target System’s Processor : Intel® Core™ i5-7200U CPU @ 2.50 GHz 2.71 GHz

STEPS & SNAPSHOTS

1. Open FTK Imager and navigate to the volatile memory icon (capture memory).
2. Due to physical random-access memory's limitations, Windows operating systems employ the pagefile (pagefile.sys) as volatile memory (RAM). It is situated under the "C" partition and is available for usage as volatile memory when the available RAM is full. Considering the volatile memory, this file may contain a significant amount of essential information. It is advised to record and gather this file during the acquisition.
   An AD1 file The FTK imager image file is called AD1. The option to make an AD1 file for subsequent usage is available to the investigator. The volatile memory will begin to be acquired once you click the "capture memory" button.
3. In this step, we select the source we need to acquire. Physical drives (physical hard drives), logical drives (partitions), image files, folder contents, and CDs/DVDs can all be acquired using FTK Imager. Investigators can utilise a write blocker to connect external HDDs to the collection machine and then choose the mounted HDD as a partition using the "logical drive" option.
   Collecting Physical Drives.
   Select the “Physical Drive” option.
   Select the drive you need to acquire and click “Finish.”
4. Image Formats by AccessData FTK Imager:

    - RAW DD - The image format that modern analysis programmes most frequently employ is called raw (dd). There are no headers, metadata, or magic values in these raw file-formatted photos. For any memory ranges that were purposefully skipped (i.e., device memory) or that the acquisition tool was unable to read, the raw format often

includes padding, which helps maintain spatial integrity (relative offsets among data).

- SMART: For Linux file systems, this file format is intended. With optional compression, this format maintains the disc images as pure bitstreams. A typical 13-byte header is followed by a number of sections in the file. Together with the actual data or information, each section also contains a type string, a 64-bit offset to the following section, a 64-bit size, padding, and a CRC.

- E01: EnCase, a proprietary format created by Guidance Software, uses this format. The image file is compressed using this format. The header and footer of an image in this format contain case information and an MD5 hash of the full bit stream. The name of the examiner, the date and time of acquisition, any special notes, and a password are all included in this case information.

- Advance Forensic Format (AFF) : It was created by Basis Technologies and Simson Garfinkel. AFF4 is the most recent implementation. The objective is to develop a disc image format that does not lock the user into a proprietary format that might impede their ability to adequately examine it.

5. Now enter the case details.
6. Add image destination.
7. Image Fragment Size (MB): By selecting this option, the image file will be divided into numerous images and saved to the same location. The image fragment size must be adjusted to "0" if you only need one file rather than several fragmented photos.
8. Go to the "verify photos when they are made" menu. Once the picture has been produced, this will check the hash values. It is advised to choose this option in order to guarantee honesty. But, if you're working with a high disc image size, this will lengthen the time it takes to gather your evidence.
9. Click on “start” to start acquiring the evidence.

10. Once the acquiring is complete, it will generate a report text file to analyse the volatile data stored in the random access memory.

11. After the acquiring is complete, we now shift towards analysation of the acquired file.

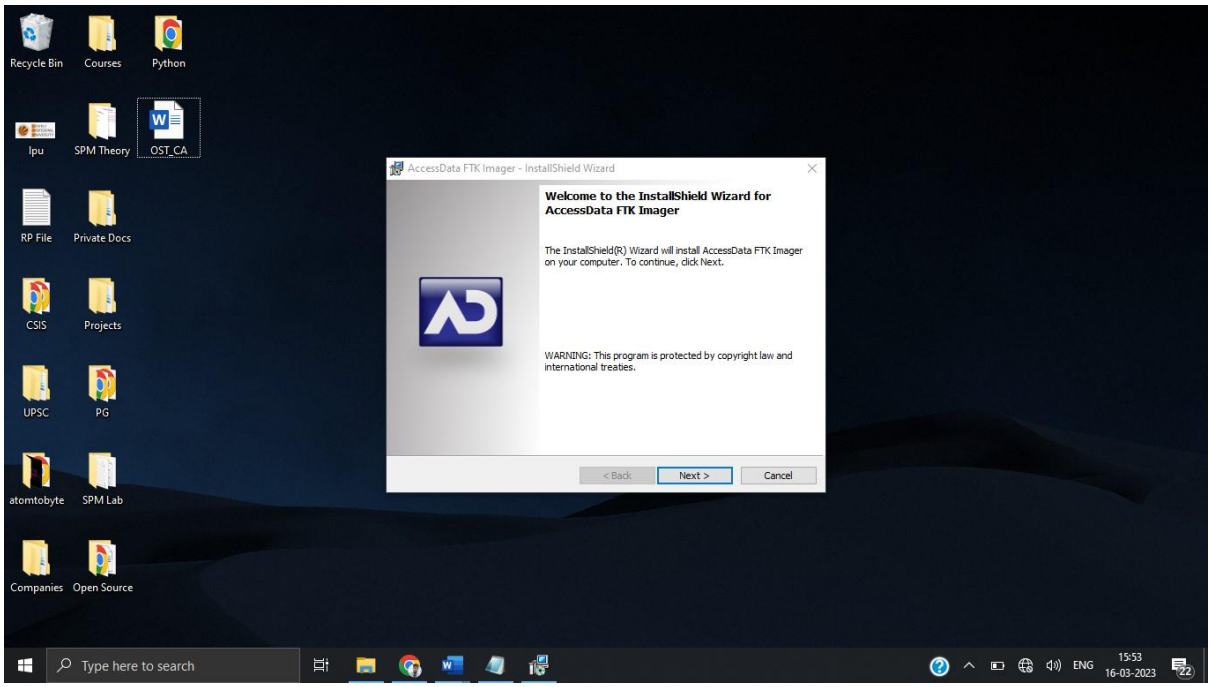
12. Open FTK Imager and got to files.

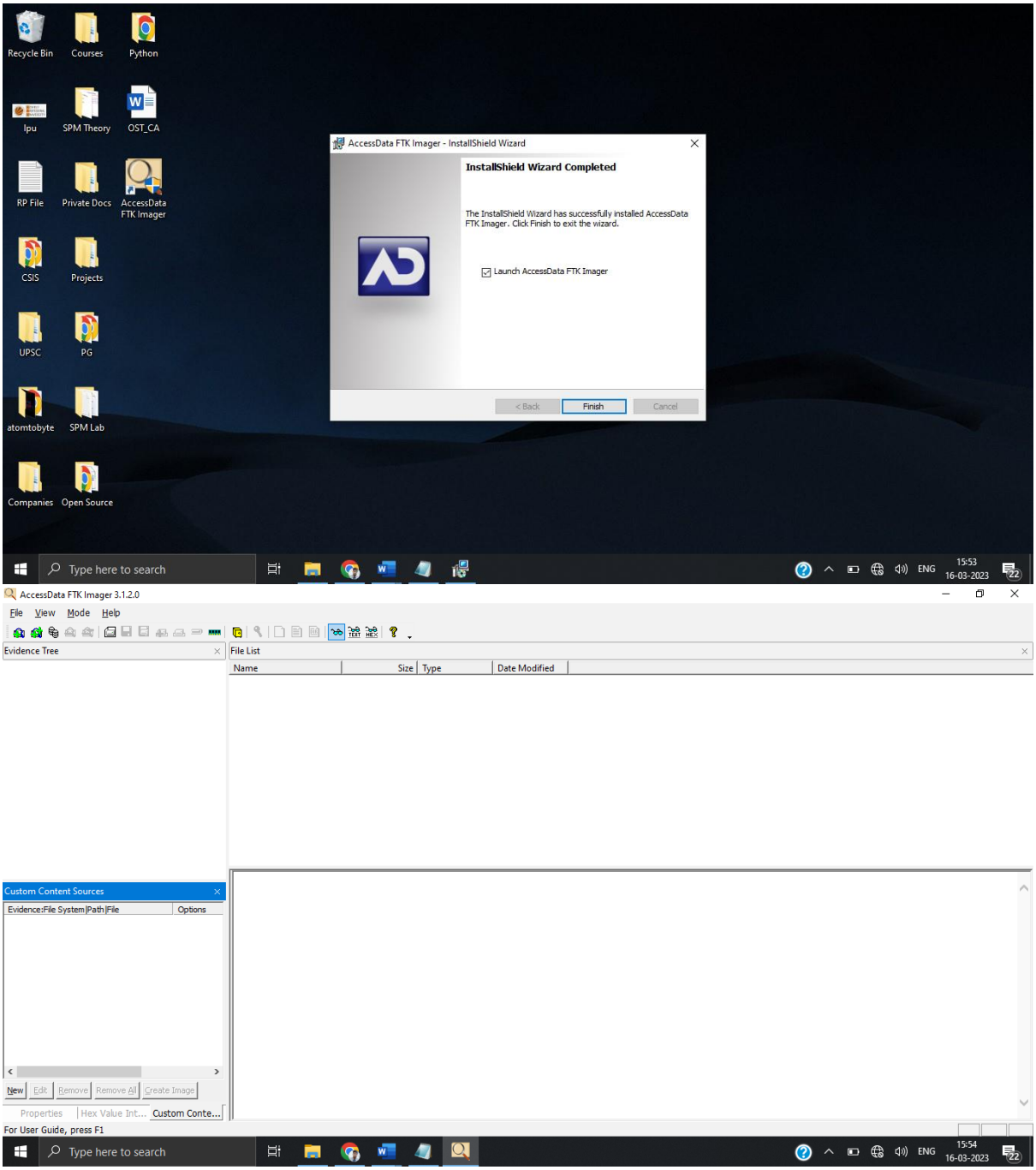
13. Click on “Add all attached drives.”

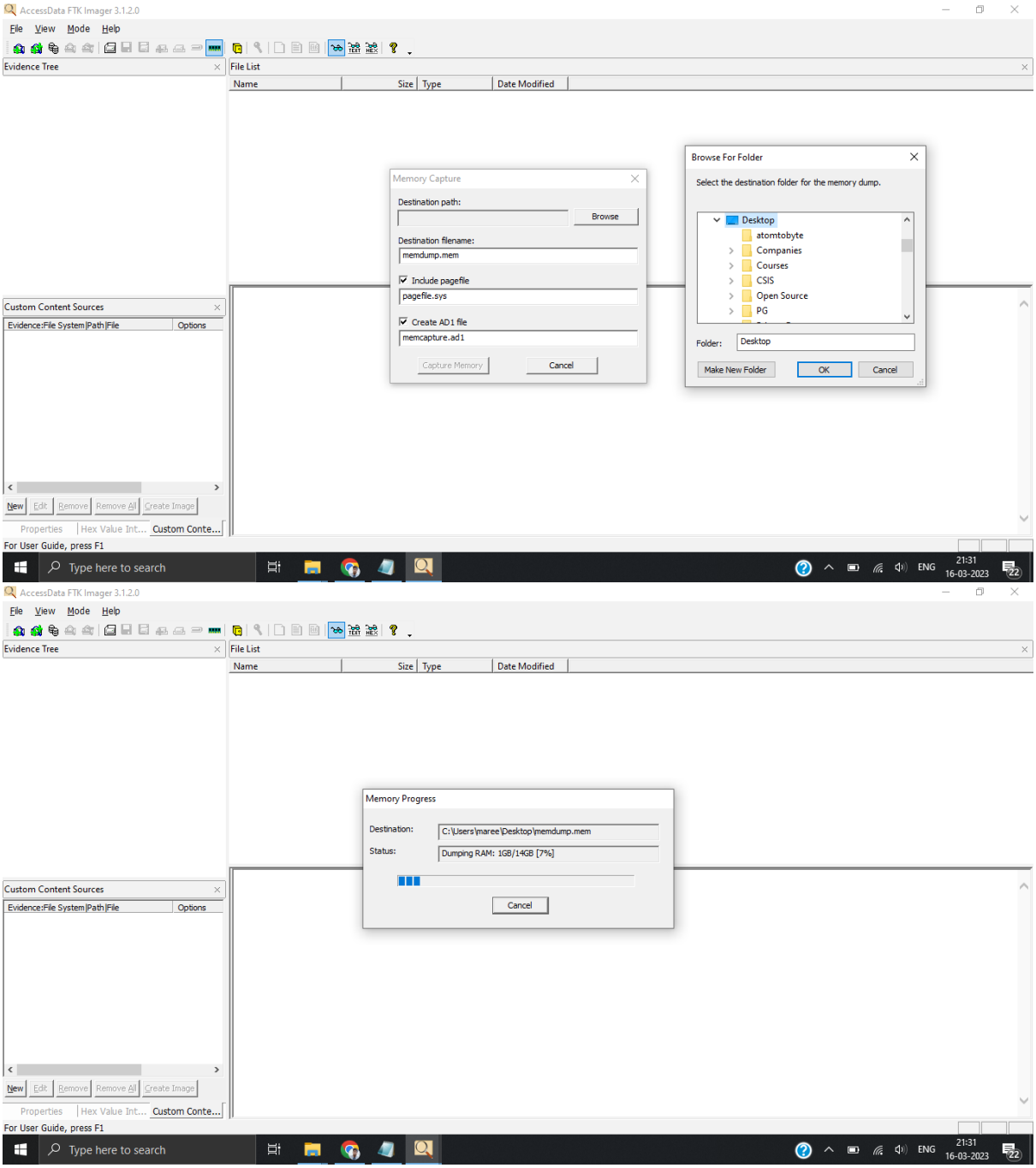
14. Click “C” Drive from the drop list and then select “root” folder.

15. Select “pagefile.sys” and in the bottom you get the report and that can be analysed.

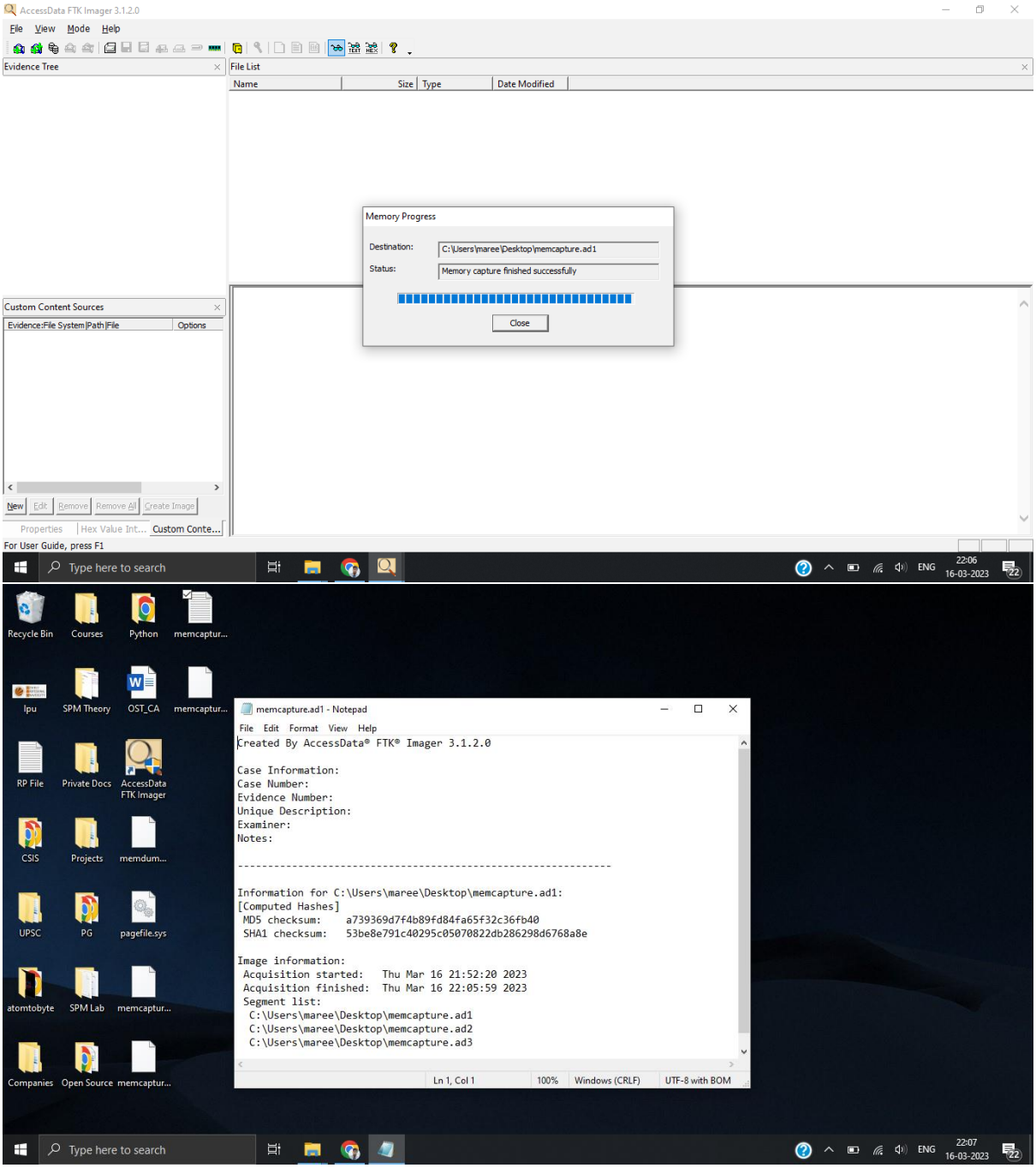
16. Also, select “DumpStack.log” for analysation purpose.

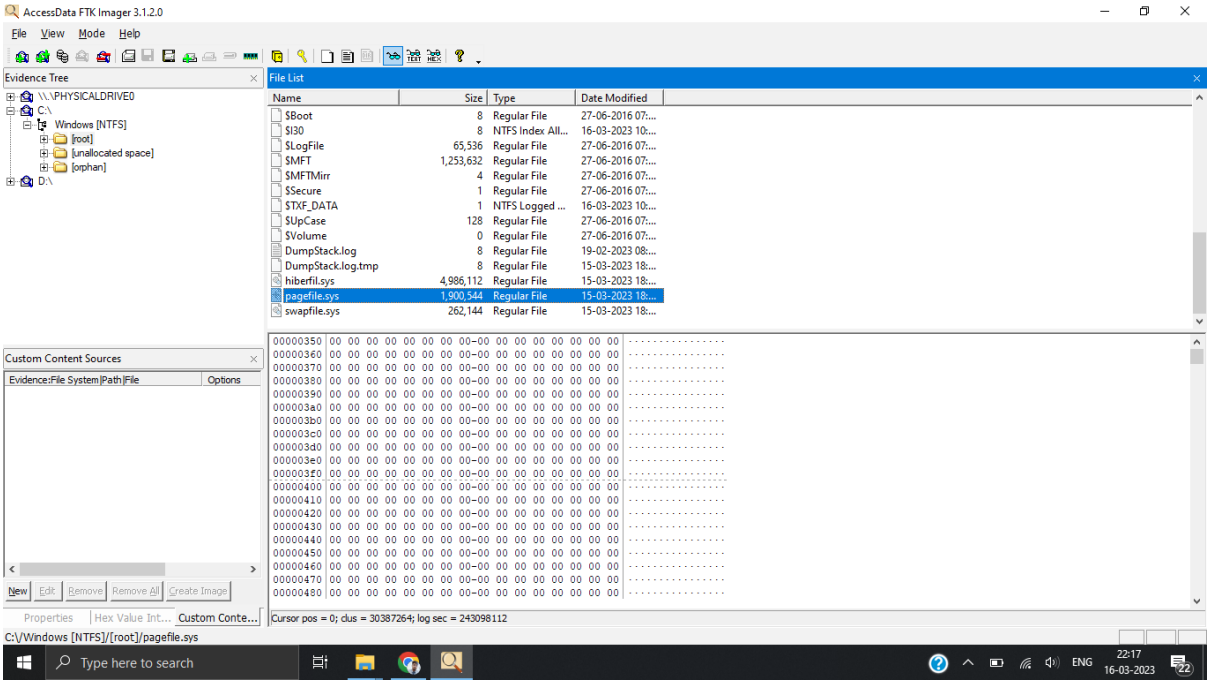


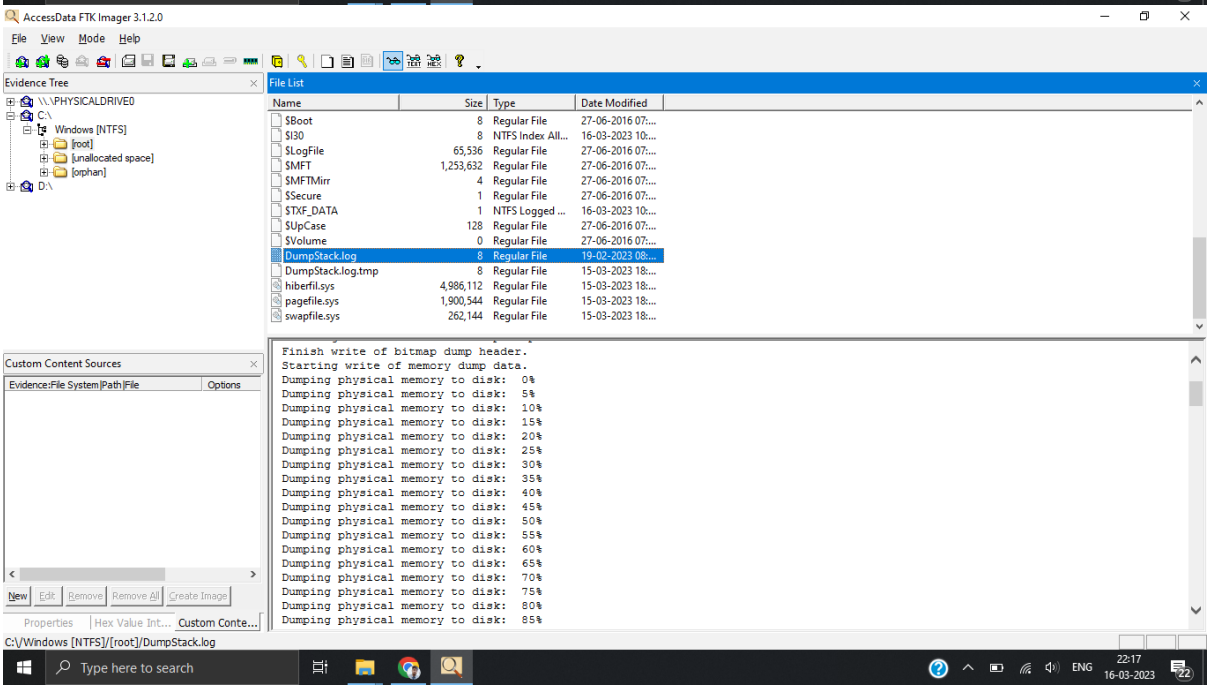

Recycle Bin
Courses
Python
Ipu
SPM Theory
OST_CA
RP File
Private Docs
AccessData FTK Imager
CSIS
Projects
UPSC
PG
atomtobyte
SPM Lab
Companies
Open Source
AccessData FTK Imager - InstallShield Wizard
InstallShield Wizard Completed
The InstallShield Wizard has successfully installed AccessData FTK Imager. Click Finish to exit the wizard.
Launch AccessData FTK Imager
< Back
Finish
Cancel
Type here to search
ENG
15:53
16-03-2023
AccessData FTK Imager 3.1.2.0
File View Mode Help
Evidence Tree
File List
Name
Size
Type
Date Modified
Custom Content Sources
Evidence:File System|Path|File
Options
New
Edit
Remove
Remove All
Create Image
Properties
Hex Value Int...
Custom Conte...
For User Guide, press F1
Type here to search
ENG
15:54
16-03-2023

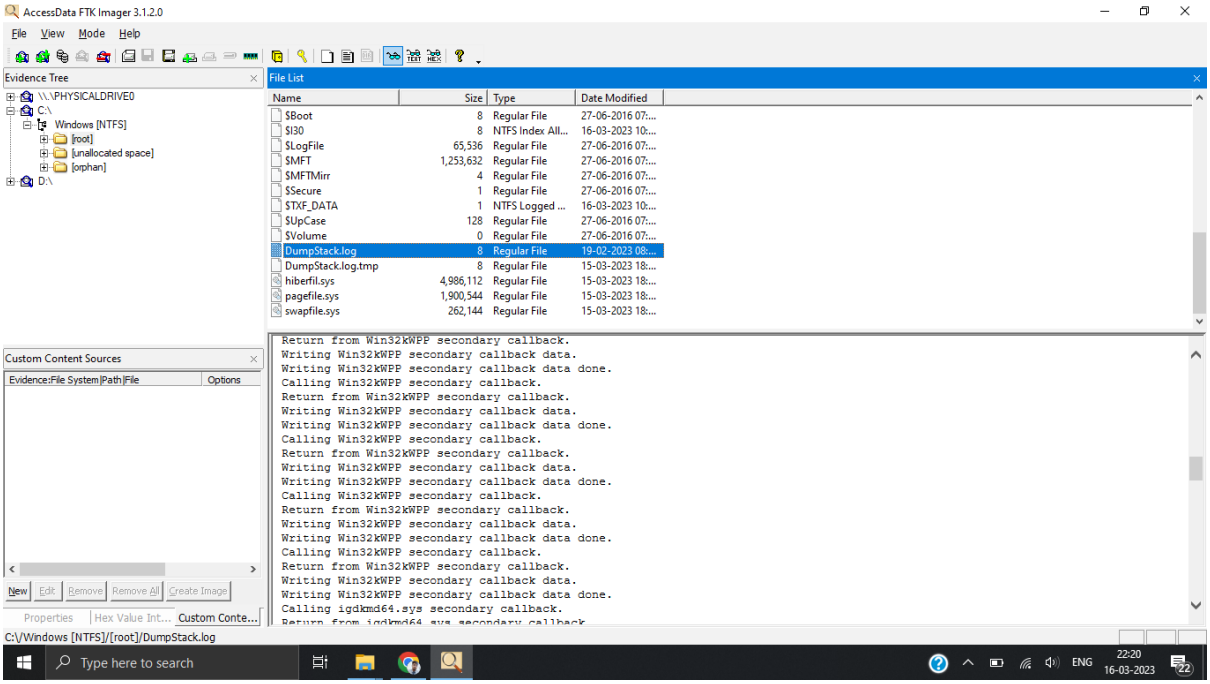

AccessData FTK Imager 3.1.2.0
File View Mode Help
Evidence Tree
File List
Name Size Type Date Modified
Memory Capture
Destination path:
Browse
Destination filename:
memdump.mem
Include pagefile
pagefile.sys
Create AD1 file
memcapture.ad1
Capture Memory
Cancel
Browse For Folder
Select the destination folder for the memory dump.
Desktop
atomtobyte
Companies
Courses
CSIS
Open Source
PG
Folder:
Desktop
Make New Folder
OK
Cancel
Custom Content Sources
Evidence:File System|Path|File
Options
New Edit Remove Remove All Create Image
Properties Hex Value Int... Custom Conte...
For User Guide, press F1
Type here to search
ENG
21:31
16-03-2023

AccessData FTK Imager 3.1.2.0
File View Mode Help
Evidence Tree
File List
Name Size Type Date Modified
Memory Progress
Destination:
C:\Users\maree\Desktop\memdump.mem
Status:
Dumping RAM: 1GB/14GB [7%]
Cancel
Custom Content Sources
Evidence:File System|Path|File
Options
New Edit Remove Remove All Create Image
Properties Hex Value Int... Custom Conte...
For User Guide, press F1
Type here to search
ENG
21:31
16-03-2023


AccessData FTK Imager 3.1.2.0
File View Mode Help
Evidence Tree
File List
Name Size Type Date Modified
Memory Progress
Destination: C:\Users\maree\Desktop\memcapture.ad1
Status: Memory capture finished successfully
Close
Custom Content Sources
Evidence:File System|Path|File Options
New Edit Remove Remove All Create Image
Properties Hex Value Int... Custom Conte...
For User Guide, press F1
Type here to search
ENG 22:06 16-03-2023
Recycle Bin Courses Python memcaptur...
lpu SPM Theory OST_CA memcaptur...
RP File Private Docs AccessData FTK Imager
CSIS Projects memdum...
UPSC PG pagefile.sys
atomtobyte SPM Lab memcaptur...
Companies Open Source memcaptur...
memcapture.ad1 - Notepad
File Edit Format View Help
Created By AccessData® FTK® Imager 3.1.2.0
Case Information:
Case Number:
Evidence Number:
Unique Description:
Examiner:
Notes:
Information for C:\Users\maree\Desktop\memcapture.ad1:
[Computed Hashes]
MD5 checksum: a739369d7f4b89fd84fa65f32c36fb40
SHA1 checksum: 53be8e791c40295c05070822db286298d6768a8e
Image information:
Acquisition started: Thu Mar 16 21:52:20 2023
Acquisition finished: Thu Mar 16 22:05:59 2023
Segment list:
C:\Users\maree\Desktop\memcapture.ad1
C:\Users\maree\Desktop\memcapture.ad2
C:\Users\maree\Desktop\memcapture.ad3
Ln 1, Col 1 100% Windows (CRLF) UTF-8 with BOM
Type here to search
ENG 22:07 16-03-2023


AccessData FTK Imager 3.1.2.0
File View Mode Help
Evidence Tree
\\.\PHYSICALDRIVE0
C:\
Windows [NTFS]
[root]
[unallocated space]
[orphan]
D:\
File List
Name Size Type Date Modified
$Boot 8 Regular File 27-06-2016 07:...
$I30 8 NTFS Index All... 16-03-2023 10:...
$LogFile 65,536 Regular File 27-06-2016 07:...
$MFT 1,253,632 Regular File 27-06-2016 07:...
$MFTMirr 4 Regular File 27-06-2016 07:...
$Secure 1 Regular File 27-06-2016 07:...
$TXF_DATA 1 NTFS Logged ... 16-03-2023 10:...
$UpCase 128 Regular File 27-06-2016 07:...
$Volume 0 Regular File 27-06-2016 07:...
DumpStack.log 8 Regular File 19-02-2023 08:...
DumpStack.log.tmp 8 Regular File 15-03-2023 18:...
hiberfil.sys 4,986,112 Regular File 15-03-2023 18:...
pagefile.sys 1,900,544 Regular File 15-03-2023 18:...
swapfile.sys 262,144 Regular File 15-03-2023 18:...
Custom Content Sources
Evidence:File System|Path|File Options
New Edit Remove Remove All Create Image
Properties Hex Value Int... Custom Conte...
Cursor pos = 0; clus = 30387264; log sec = 243098112
C:\Windows [NTFS]/[root]/pagefile.sys
Type here to search
ENG
22:17
16-03-2023


AccessData FTK Imager 3.1.2.0
File View Mode Help
Evidence Tree
\\.\PHYSICALDRIVE0
C:\
Windows [NTFS]
[root]
[unallocated space]
[orphan]
D:\
File List
Name Size Type Date Modified
$Boot 8 Regular File 27-06-2016 07:...
$I30 8 NTFS Index All... 16-03-2023 10:...
$LogFile 65,536 Regular File 27-06-2016 07:...
$MFT 1,253,632 Regular File 27-06-2016 07:...
$MFTMirr 4 Regular File 27-06-2016 07:...
$Secure 1 Regular File 27-06-2016 07:...
$TXF_DATA 1 NTFS Logged ... 16-03-2023 10:...
$UpCase 128 Regular File 27-06-2016 07:...
$Volume 0 Regular File 27-06-2016 07:...
DumpStack.log 8 Regular File 19-02-2023 08:...
DumpStack.log.tmp 8 Regular File 15-03-2023 18:...
hiberfil.sys 4,986,112 Regular File 15-03-2023 18:...
pagefile.sys 1,900,544 Regular File 15-03-2023 18:...
swapfile.sys 262,144 Regular File 15-03-2023 18:...
Custom Content Sources
Evidence:File System|Path|File Options
New Edit Remove Remove All Create Image
Properties Hex Value Int... Custom Conte...
Finish write of bitmap dump header.
Starting write of memory dump data.
Dumping physical memory to disk: 0%
Dumping physical memory to disk: 5%
Dumping physical memory to disk: 10%
Dumping physical memory to disk: 15%
Dumping physical memory to disk: 20%
Dumping physical memory to disk: 25%
Dumping physical memory to disk: 30%
Dumping physical memory to disk: 35%
Dumping physical memory to disk: 40%
Dumping physical memory to disk: 45%
Dumping physical memory to disk: 50%
Dumping physical memory to disk: 55%
Dumping physical memory to disk: 60%
Dumping physical memory to disk: 65%
Dumping physical memory to disk: 70%
Dumping physical memory to disk: 75%
Dumping physical memory to disk: 80%
Dumping physical memory to disk: 85%
C:\Windows [NTFS]/[root]/DumpStack.log
Type here to search
ENG
22:17
16-03-2023


AccessData FTK Imager 3.1.2.0
File View Mode Help
Evidence Tree
\\.\PHYSICALDRIVE0
C:\
Windows [NTFS]
[root]
[unallocated space]
[orphan]
D:\
File List
Name Size Type Date Modified
$Boot 8 Regular File 27-06-2016 07:...
$I30 8 NTFS Index All... 16-03-2023 10:...
$LogFile 65,536 Regular File 27-06-2016 07:...
$MFT 1,253,632 Regular File 27-06-2016 07:...
$MFTMirr 4 Regular File 27-06-2016 07:...
$Secure 1 Regular File 27-06-2016 07:...
$TXF_DATA 1 NTFS Logged ... 16-03-2023 10:...
$UpCase 128 Regular File 27-06-2016 07:...
$Volume 0 Regular File 27-06-2016 07:...
DumpStack.log 8 Regular File 19-02-2023 08:...
DumpStack.log.tmp 8 Regular File 15-03-2023 18:...
hiberfil.sys 4,986,112 Regular File 15-03-2023 18:...
pagefile.sys 1,900,544 Regular File 15-03-2023 18:...
swapfile.sys 262,144 Regular File 15-03-2023 18:...
Custom Content Sources
Evidence:File System|Path|File Options
New Edit Remove Remove All Create Image
Properties Hex Value Int... Custom Conte...
Return from Win32kWPP secondary callback.
Writing Win32kWPP secondary callback data.
Writing Win32kWPP secondary callback data done.
Calling Win32kWPP secondary callback.
Return from Win32kWPP secondary callback.
Writing Win32kWPP secondary callback data.
Writing Win32kWPP secondary callback data done.
Calling Win32kWPP secondary callback.
Return from Win32kWPP secondary callback.
Writing Win32kWPP secondary callback data.
Writing Win32kWPP secondary callback data done.
Calling Win32kWPP secondary callback.
Return from Win32kWPP secondary callback.
Writing Win32kWPP secondary callback data.
Writing Win32kWPP secondary callback data done.
Calling Win32kWPP secondary callback.
Return from Win32kWPP secondary callback.
Writing Win32kWPP secondary callback data.
Writing Win32kWPP secondary callback data done.
Calling igdkmd64.sys secondary callback.
C:\Windows [NTFS]/[root]/DumpStack.log
Type here to search
ENG
22:20
16-03-2023

CONCLUSION

The data stored in the random-access memory (RAM) was successfully acquired using FTK Imager which is an open source application. Furthermore, the report was generated successfully on the same for analysation purposes.

REFERENCES & BIBLIOGRAPHY

- https://www.geeksforgeeks.org/how-to-create-a-forensic-image-with-ftk-imager/
- https://www.exterro.com/ftk-imager