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

CHAPTER 1

1.1 OBJECTIVE OF THE PROJECT

Memory forensics is a crucial aspect of digital forensics, which involves analyzing the contents of a computer's volatile memory (RAM) to gain insights into the system's state at a particular point in time. The main objectives of memory forensics are to gather information that can help in identifying and analyzing security breaches, understanding malware behavior, investigating cybercrime incidents, and providing evidence in legal proceedings. In this article, we will discuss the objectives of memory forensics in detail.

1. Collecting evidence: Memory forensics is used to collect digital evidence from a computer's volatile memory that may not be available through traditional forensic techniques. This evidence may include system artifacts, malware, network connections, and user activity, which can help in reconstructing the events leading to a security breach or cybercrime incident.

2. Malware analysis: Memory forensics is a powerful technique for analyzing malware behavior. It can help in identifying the type of malware, the purpose of the malware, its capabilities, and the actions it has performed on the infected system. Memory forensics can also provide information about the presence of rootkits, backdoors, and other malicious programs that are difficult to detect through traditional antivirus software.

3. Incident response: Memory forensics plays a vital role in incident response. It enables the forensic analyst to quickly assess the extent of the damage caused by a security breach or malware infection and take appropriate action to mitigate the impact. Memory forensics can help in identifying the source of the attack, the vulnerability exploited, and the techniques used by the attacker.

4. Forensic analysis: Memory forensics is a critical tool in forensic analysis. It can provide valuable information about the system's state at the time of the incident, including the processes running, the files accessed, the network connections established, and the user activity. This information can be used to reconstruct the events leading to the incident and identify the individuals involved.

5. Root cause analysis: Memory forensics can help in identifying the root cause of a security breach or cybercrime incident. It can provide information about the

vulnerabilities exploited, the actions performed by the attacker, and the systems and networks affected. This information can be used to patch the vulnerabilities and prevent similar incidents in the future.

6. Legal evidence: Memory forensics can provide legally admissible evidence in court proceedings. The information collected from volatile memory can be used to reconstruct the events leading to the incident, identify the individuals involved, and prove their culpability. Memory forensics can also provide evidence of tampering or alteration of the system's volatile memory, which can help in proving the authenticity of the evidence.

In conclusion, memory forensics is an essential technique for investigating security breaches, malware infections, and cybercrime incidents. It enables the forensic analyst to collect valuable digital evidence, analyze malware behavior, respond to incidents quickly, perform forensic analysis, identify the root cause of the incident, and provide legally admissible evidence. Memory forensics is a complex and challenging field that requires expertise in computer architecture, operating systems, programming, and digital forensics. However, with the increasing sophistication of cyber threats, it is becoming increasingly important for organizations to invest in memory forensics capabilities to protect their assets and prevent cybercrime incidents.

CHAPTER 1

1.2 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)

FTK Imager is a forensic imaging and analysis software that is widely used in the digital forensic field. Developed by AccessData, FTK Imager is designed to create forensic images of hard drives, solid-state drives, and other digital storage media. The software can also be used for memory forensics to analyze the contents of a computer's volatile memory (RAM).

The FTK Imager user interface is user-friendly and intuitive, making it easy for both novice and experienced users to navigate. The software's features and capabilities include:

1. Imaging Capabilities

   FTK Imager allows users to create forensic images of physical and logical drives, as well as create image files in various formats, including E01, AFF, and RAW. The software supports both imaging and hashing of selected files and folders, and it can also image a running system and mount image files as logical drives.

2. Analysis Capabilities

   FTK Imager includes a wide range of analysis capabilities, including file analysis, hash calculation, search and filtering, and file carving. The software can identify and extract hidden files, recover deleted files, and identify and recover damaged files.

3. Memory Analysis Capabilities

   FTK Imager also includes memory analysis capabilities, allowing users to analyze the contents of a computer's volatile memory (RAM). The software can identify running processes, loaded DLLs, and open handles, as well as extract strings, analyze network connections, and search for malware.

4. Reporting Capabilities

   FTK Imager allows users to generate reports in various formats, including HTML, PDF, and RTF. Reports can include metadata, analysis results, and other relevant information.

5. User Interface

   The FTK Imager user interface is user-friendly and intuitive, making it easy for both novice and experienced users to navigate. The software provides a comprehensive view of the forensic image or memory dump being analyzed, with detailed information about the data and artifacts discovered.

Overall, FTK Imager is a comprehensive forensic imaging and analysis software that offers a wide range of capabilities for forensic investigators. Its user-friendly interface and powerful analysis tools make it a popular choice for both novice and experienced users.

CHAPTER 1

1.3 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. FTK Imager is widely used in legal and law enforcement investigations, where it is used to acquire forensic images of digital storage media, analyze the contents of those images, and generate reports for use in court proceedings. The software's powerful analysis capabilities and user-friendly interface make it a popular choice for investigators in these settings.

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.

CHAPTER 2

2.1 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

CHAPTER 2

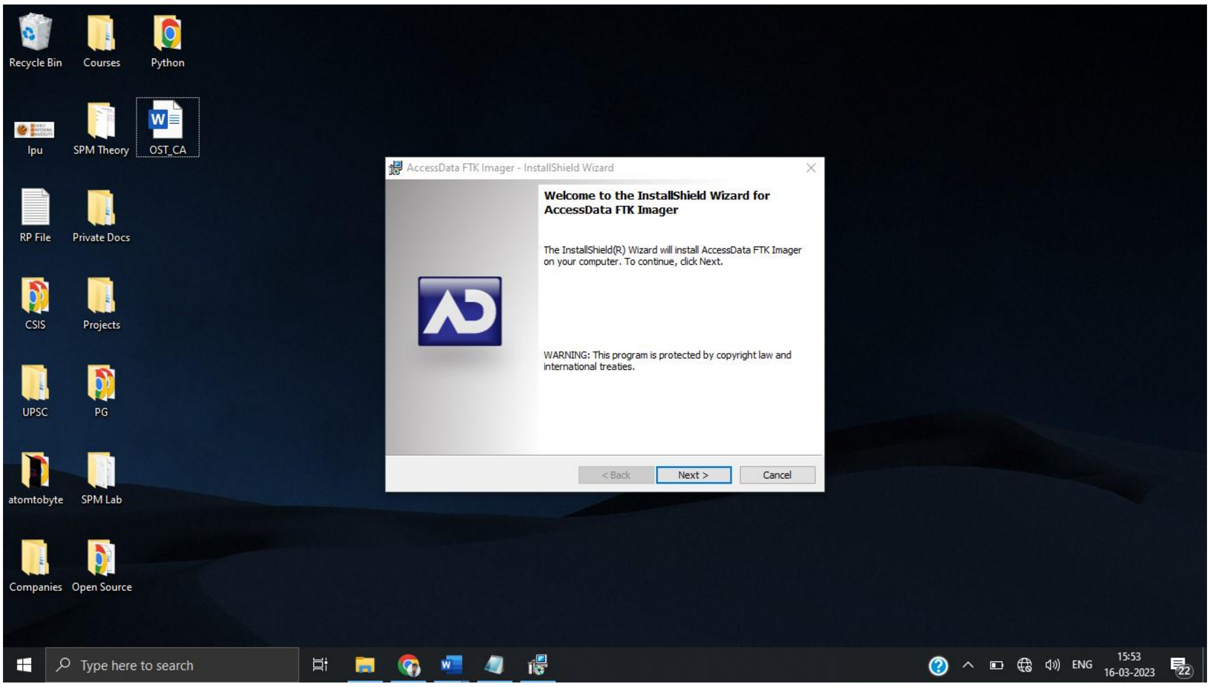
2.2 LINKS IN SUPPORT OF PROJECT

GITHUB	https://github.com/iareebahmad/CAsubmission
GOOGLE DRIVE FOR DUMP	https://drive.google.com/drive/folders/1DOaTClzc8iqjPrAhemVgAdbMu-dwQlQd?usp=sharing

CHAPTER 3

3.1 SNAPSHOTS AND ANALYSIS

1. Run the setup file and install FTK Imager.

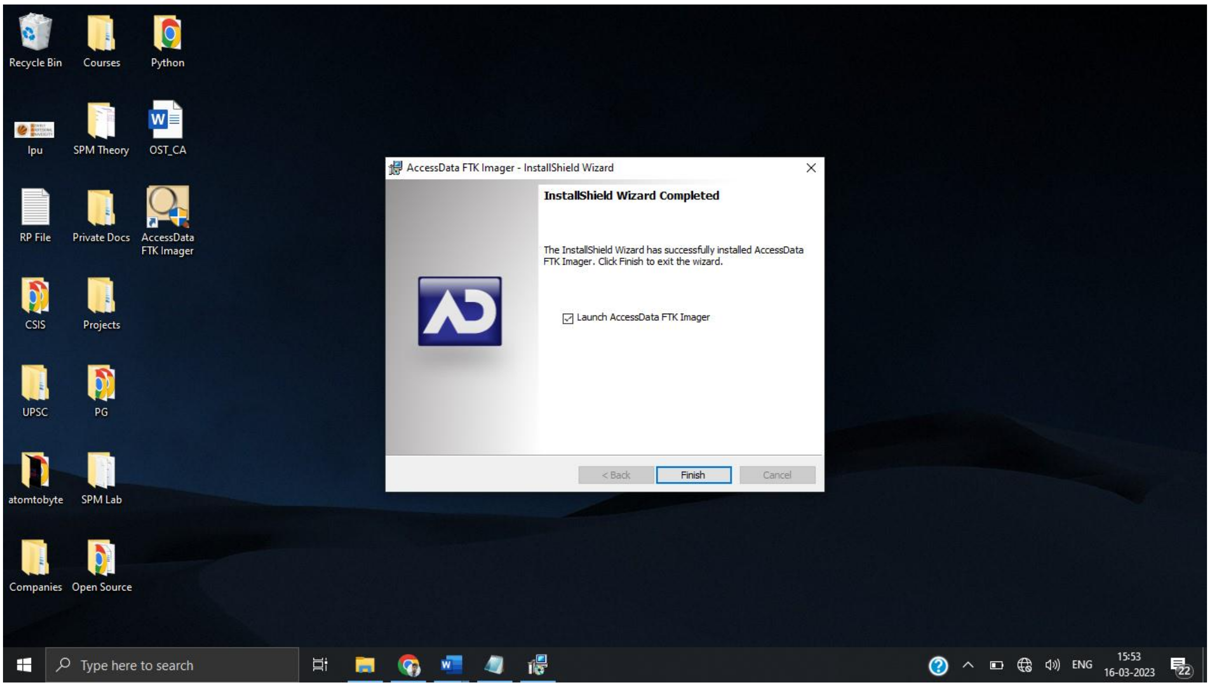


AccessData FTK Imager - InstallShield Wizard

Welcome to the InstallShield Wizard for AccessData FTK Imager

The InstallShield(R) Wizard will install AccessData FTK Imager on your computer. To continue, click Next.

WARNING: This program is protected by copyright law and international treaties.



AccessData FTK Imager - InstallShield Wizard

InstallShield Wizard Completed

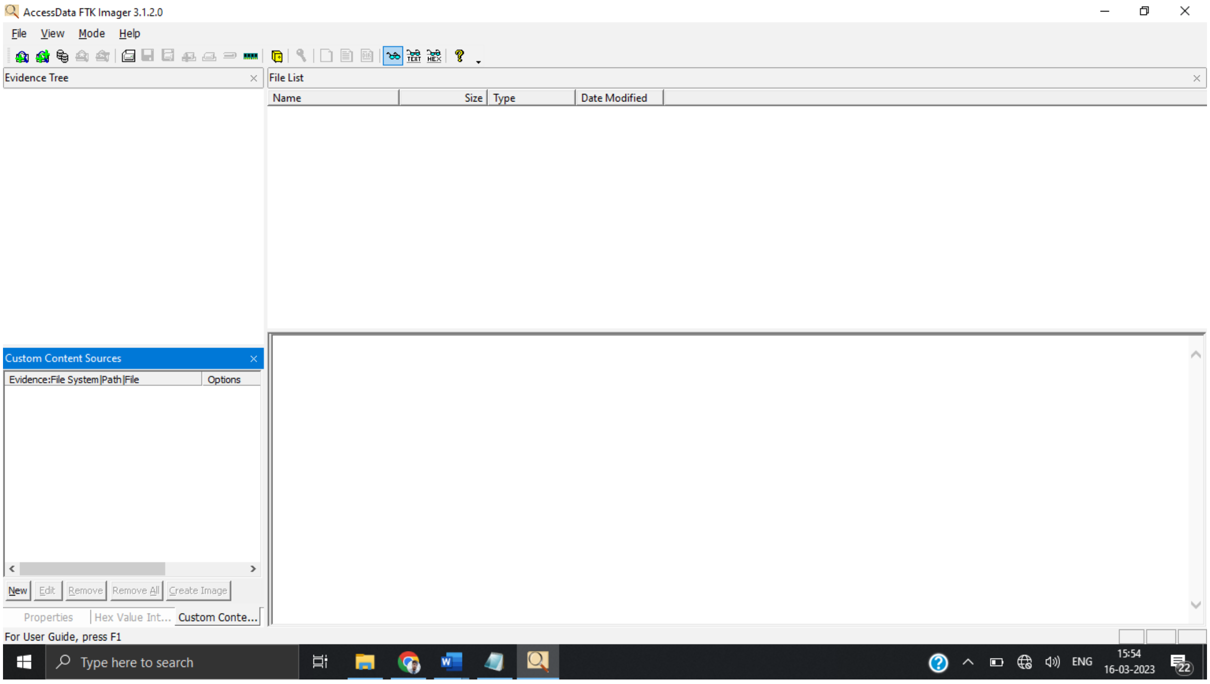
The InstallShield Wizard has successfully installed AccessData FTK Imager. Click Finish to exit the wizard.

☑ Launch AccessData FTK Imager

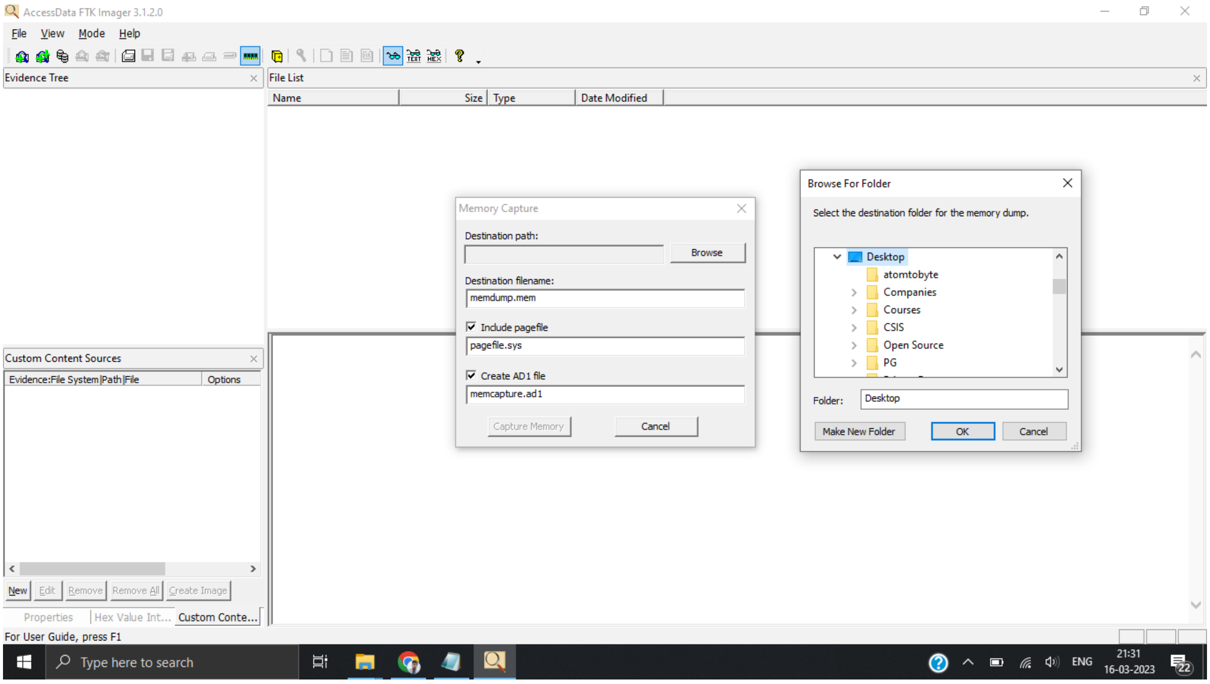
2. Open FTK Imager and navigate to the volatile memory icon (capture memory).
3. Due to physical random-access memory's limitations, Windows operating systems employ the pagefile (pagefile.sys) as volatile memory (RAM). It is situated under the "C" partition and is available for usage as volatile memory 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.



4. 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.”


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 21:31 16-03-2023

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

5. Image Formats by AccessData FTK Imager:

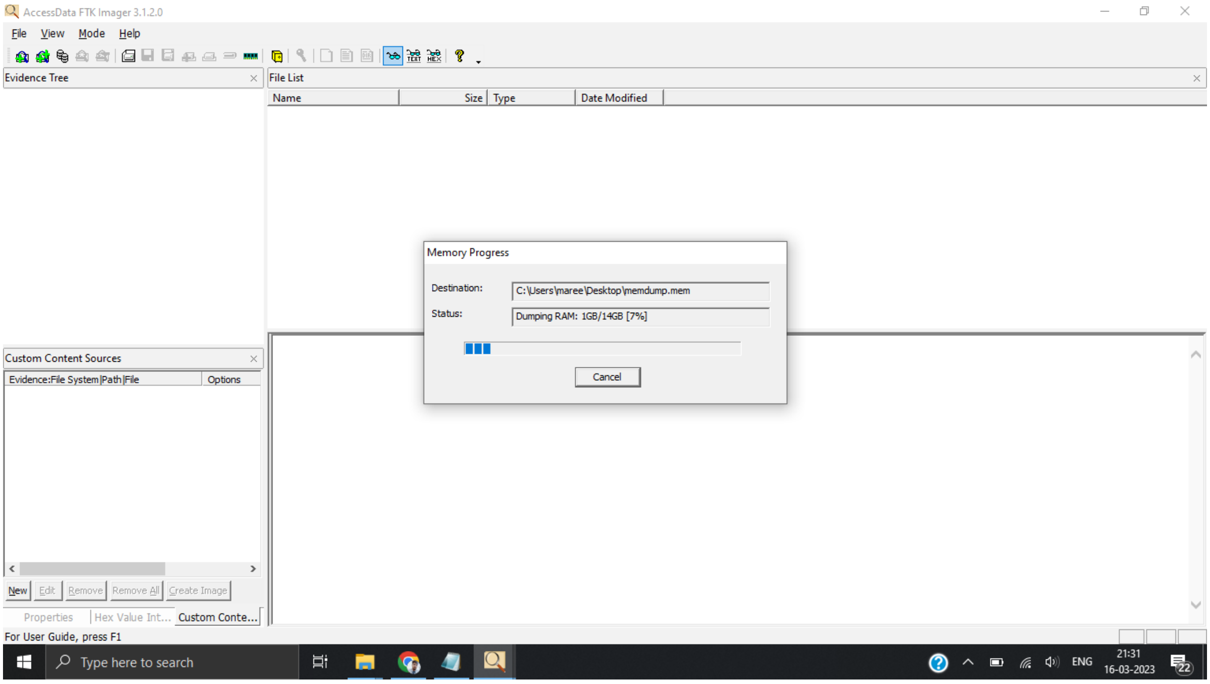
- RAW DD - The image format that modern analysis programmes most frequently employ is called raw (dd). There are no headers, metadata, or magic values in these raw file-formatted photos. For any memory ranges that were purposefully skipped (i.e., device memory) or that the acquisition tool was unable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

6. Now enter the case details.
7. Add image destination.
8. 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.
9. 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.
10. Click on “start” to start acquiring the evidence.

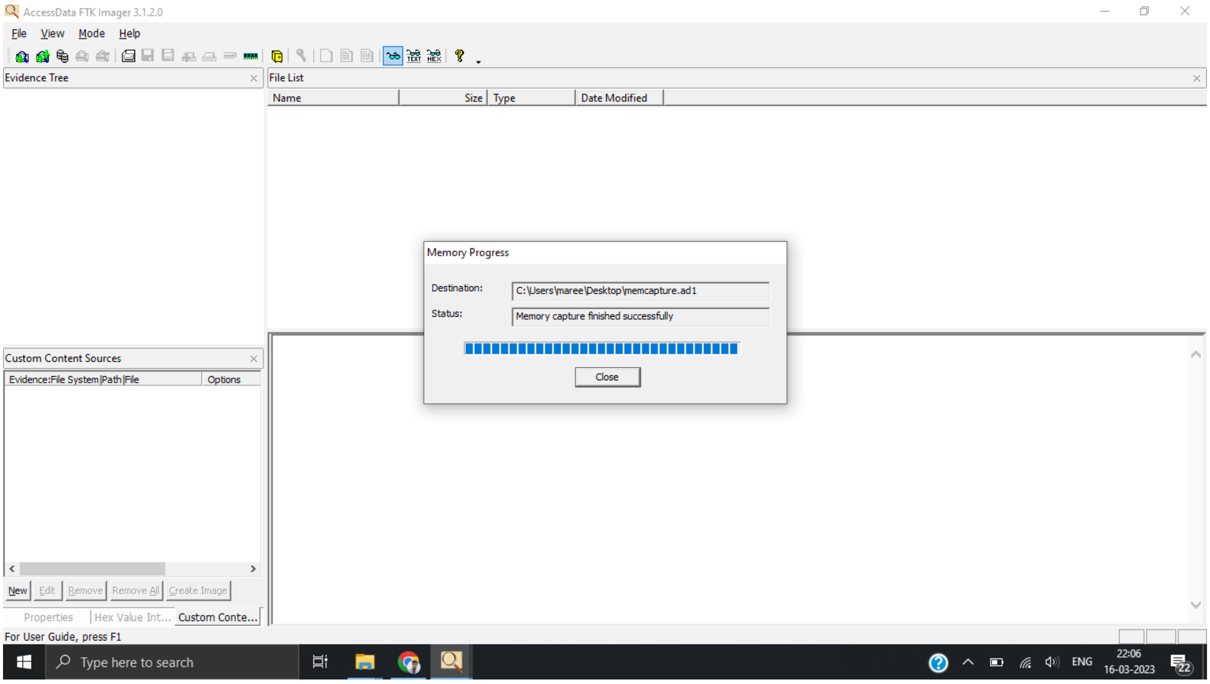


Memory Progress

Destination: C:\Users\maree\Desktop\memdump.mem

Status: Dumping RAM: 1GB/14GB [7%]

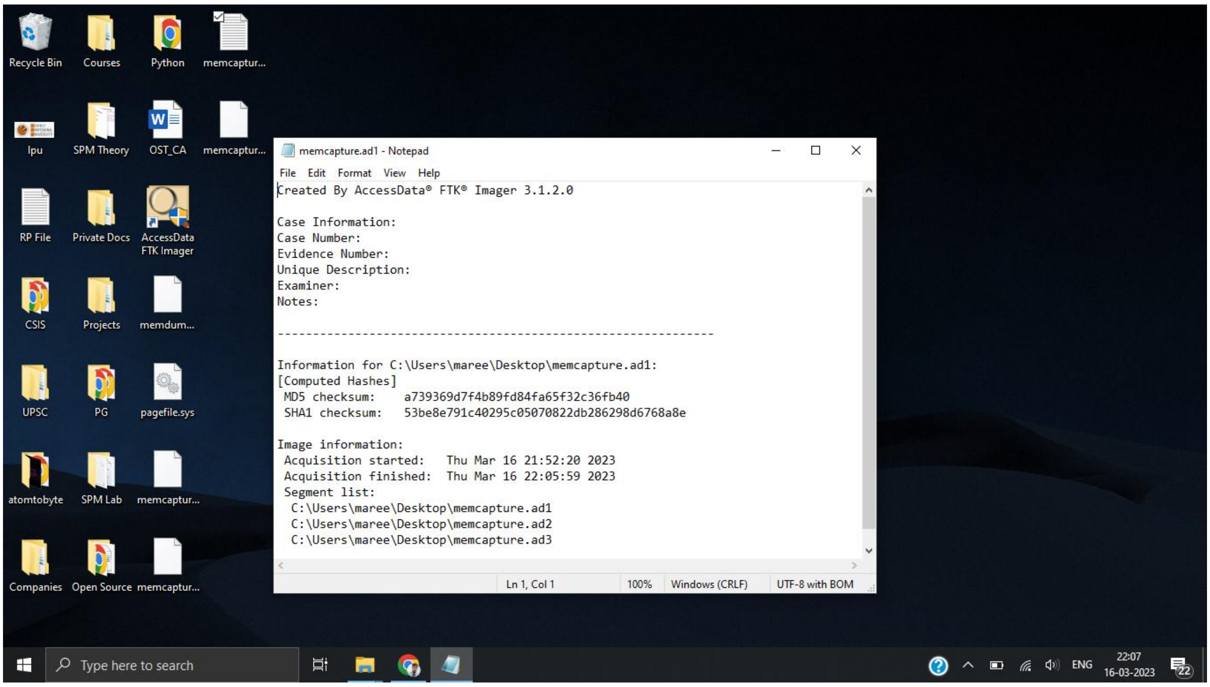
11. Once the acquiring is complete, it will generate a report text file to analyse the volatile data stored in the random access memory.


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
Close

Memory Progress

Destination: C:\Users\maree\Desktop\memcapture.ad1

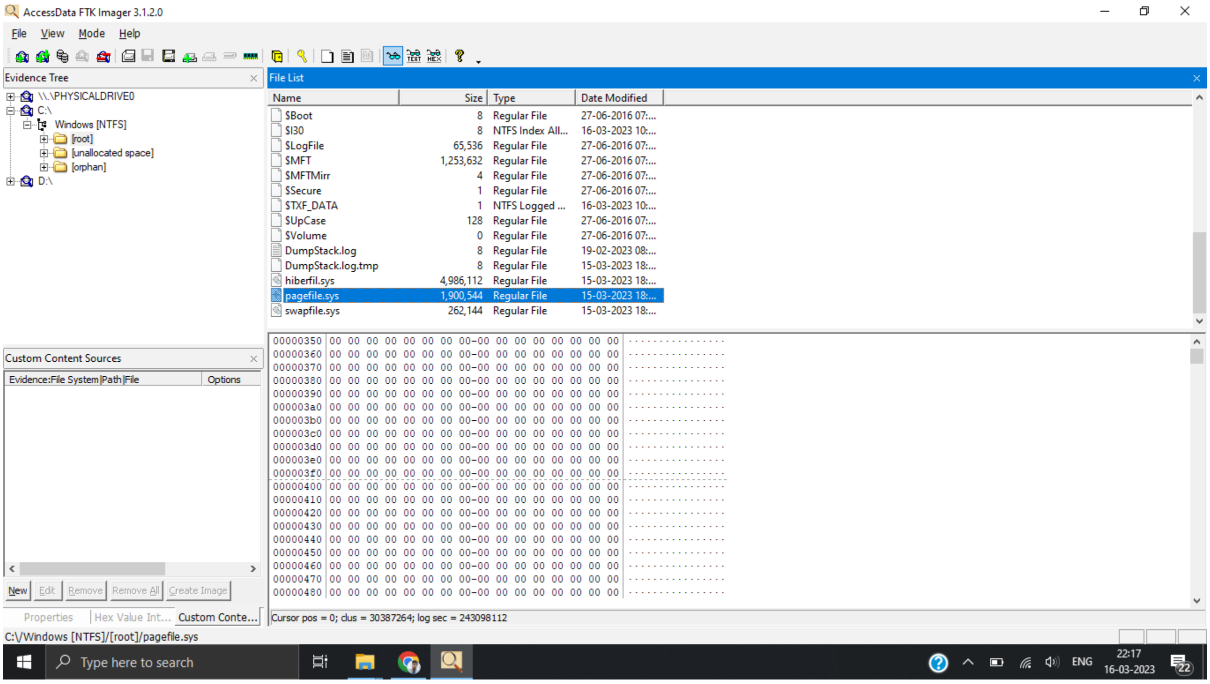
Status: Memory capture finished successfully


memcapture.ad1 - Notepad
File Edit Format View Help
Ln 1, Col 1 100% Windows (CRLF) UTF-8 with BOM

```
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
```

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

13. Open FTK Imager and got to files.



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:...

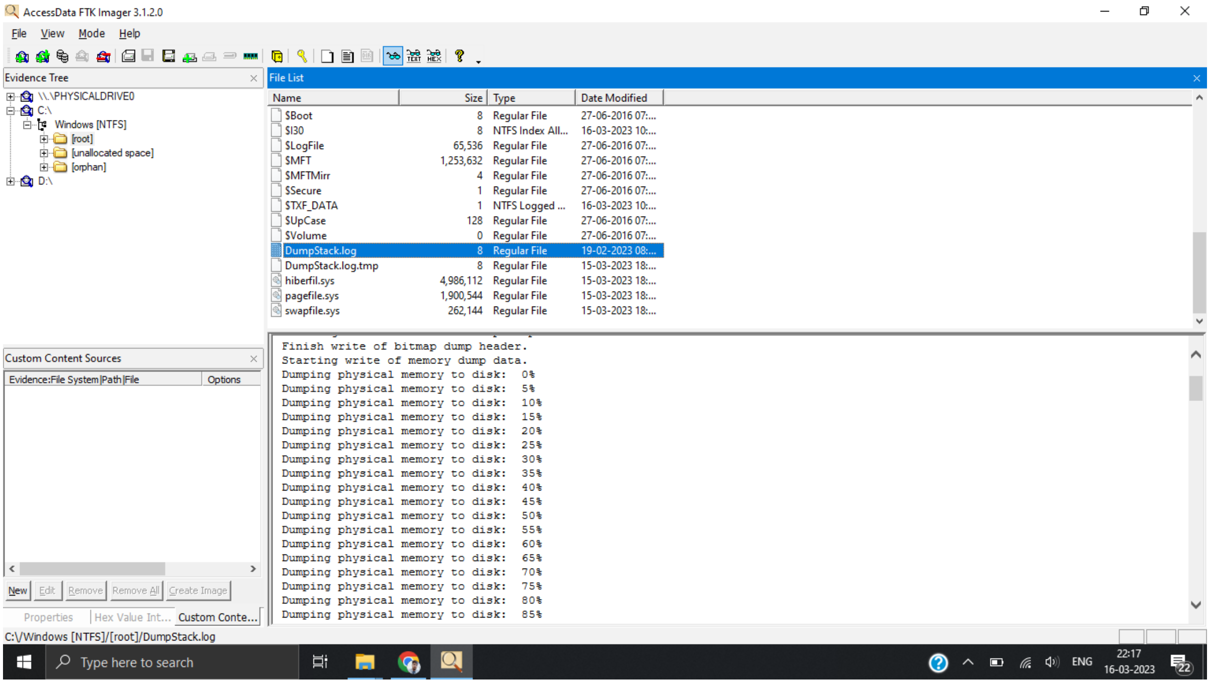
```
00000350 00 00 00 00 00 00 00 00-00 00 00 00 00 00 00 00 ................
00000360 00 00 00 00 00 00 00 00-00 00 00 00 00 00 00 00 ................
00000370 00 00 00 00 00 00 00 00-00 00 00 00 00 00 00 00 ................
00000380 00 00 00 00 00 00 00 00-00 00 00 00 00 00 00 00 ................
00000390 00 00 00 00 00 00 00 00-00 00 00 00 00 00 00 00 ................
000003a0 00 00 00 00 00 00 00 00-00 00 00 00 00 00 00 00 ................
000003b0 00 00 00 00 00 00 00 00-00 00 00 00 00 00 00 00 ................
000003c0 00 00 00 00 00 00 00 00-00 00 00 00 00 00 00 00 ................
000003d0 00 00 00 00 00 00 00 00-00 00 00 00 00 00 00 00 ................
000003e0 00 00 00 00 00 00 00 00-00 00 00 00 00 00 00 00 ................
000003f0 00 00 00 00 00 00 00 00-00 00 00 00 00 00 00 00 ................
00000400 00 00 00 00 00 00 00 00-00 00 00 00 00 00 00 00 ................
00000410 00 00 00 00 00 00 00 00-00 00 00 00 00 00 00 00 ................
00000420 00 00 00 00 00 00 00 00-00 00 00 00 00 00 00 00 ................
00000430 00 00 00 00 00 00 00 00-00 00 00 00 00 00 00 00 ................
00000440 00 00 00 00 00 00 00 00-00 00 00 00 00 00 00 00 ................
00000450 00 00 00 00 00 00 00 00-00 00 00 00 00 00 00 00 ................
00000460 00 00 00 00 00 00 00 00-00 00 00 00 00 00 00 00 ................
00000470 00 00 00 00 00 00 00 00-00 00 00 00 00 00 00 00 ................
00000480 00 00 00 00 00 00 00 00-00 00 00 00 00 00 00 00 ................
```

Cursor pos = 0; clus = 30387264; log sec = 243098112

C:\Windows [NTFS]/[root]/pagefile.sys

14. Click on “Add all attached drives.”

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



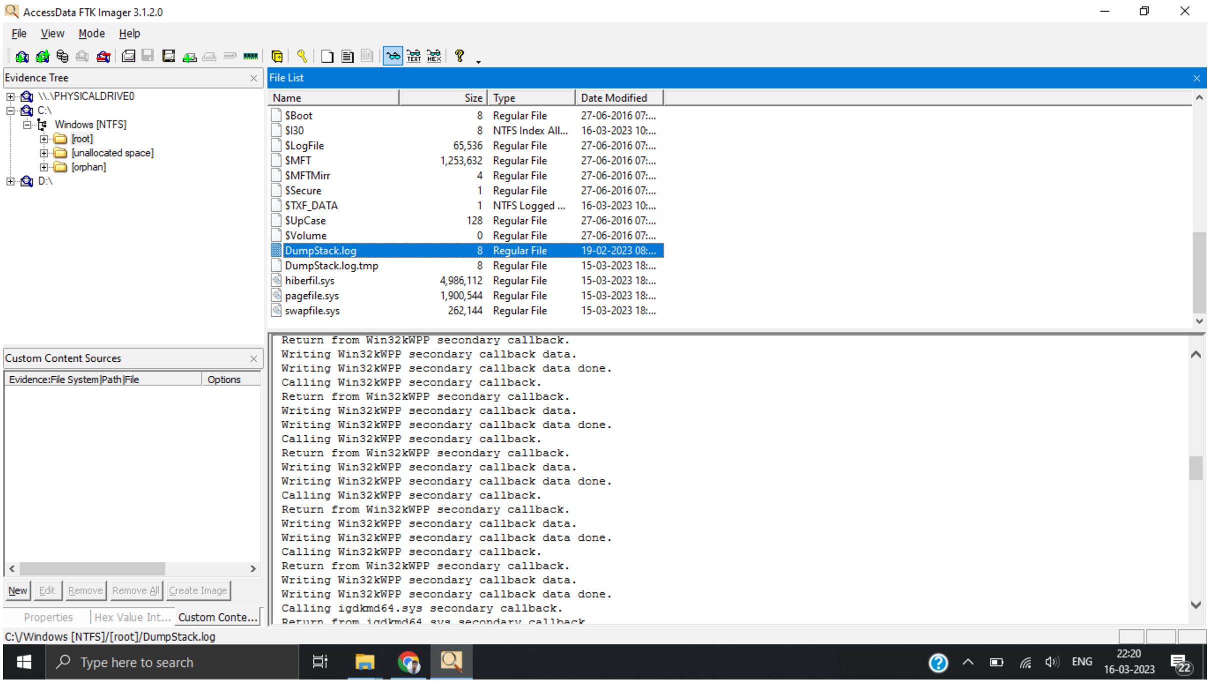
Name	Size	Type	Date Modified
$Boot	8	Regular File	27-06-2016 07:...
$I30	8	NTFS Index All...	16-03-2023 10:...
$LogFile	65,536	Regular File	27-06-2016 07:...
$MFT	1,253,632	Regular File	27-06-2016 07:...
$MFTMirr	4	Regular File	27-06-2016 07:...
$Secure	1	Regular File	27-06-2016 07:...
$TXF_DATA	1	NTFS 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:...

```
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

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

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



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:...

```
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.
Return from igdkmd64.sys secondary callback
```

C:\/Windows [NTFS]/[root]/DumpStack.log

CHAPTER 3

3.2 CONCLUSION

In conclusion, FTK Imager is a powerful and versatile tool that is widely used in the digital forensics field. With its ability to acquire forensic images of digital storage media, analyze the contents of those images, and generate reports for use in court proceedings, FTK Imager is an essential tool for investigators in both law enforcement and corporate settings.

FTK Imager's ability to quickly triage a system and identify indicators of compromise makes it a valuable tool for incident response situations, while its analysis capabilities make it a valuable tool for identifying and analyzing malicious code. Additionally, FTK Imager can be used for data recovery in situations where files have been accidentally deleted or lost due to hardware failure.

Overall, FTK Imager's powerful analysis capabilities and user-friendly interface make it a popular choice for investigators in a variety of settings. Whether it is being used in a digital forensic investigation, an incident response situation, or a legal or law enforcement investigation, FTK Imager provides investigators with the tools they need to quickly and accurately acquire and analyze digital evidence.

REFERENCES & BIBLIOGRAPHY

[01] N. Hiramoto, Y. Tsuchiya, Measuring dark web marketplaces via Bitcoin transactions: from birth to independence, Forensic Sci. Int.: Digit. Invest. 35 (2020), 301086.

[02] T. Thomas, M. Piscitelli, I. Shavrov, I. Baggili, Memory FORESHADOW: memory FOREnSics of HArDware CryptOcurrency wallets – a tool and visualization framework, Forensic Sci. Int.: Digit. Invest. 33 (2020), 301002.

[03] M. Frowis, T. Gottschalk, B. Haslhofer, C. Ruckert, P. Pesch, Safeguarding the evidential value of forensic cryptocurrency investigations, Forensic Sci. Int.: Digit. Invest. 33 (2020), 200902.

[04] S. Castell, Authored by AI- Here be crypto dragons: it's all about the evidence, Solicitors' J. 162 (2019) 42–45.

[05] W. Koerhuis, T. Kechadi, N.-A. Le-Khac, Forensic analysis of privacy-oriented cryptocurrencies, Forensic Sci. Int. 33 (2020), 200891.

[06] S. Dyson, W. Buchanan, L. Bell, Scenario-based creation and digital investigation of Ethereum ERC20 tokens, Forensic Sci. Int.: Digit. Invest. 32 (2020), 200894.

[07] A. Jones, S. Vidalis, Rethinking digital forensics, Ann. Emerg. Technol. Comput. 3 (2) (2019) 42–53.