INT 301 Project

NAME: M. Vishnu Vardhan

REGNO: 11908323

SECTION:KE022

Faculty: Dr. Manjot Kaur

Name of the University: Lovely Professional University

Name of the city: Phagwara (Punjab)

Date of submission: 22nd March 2023

Use any open source tool to find partial and full multimedia files(video files) in DataStream. Explore any other five features from the same software.

I-INTRODUCTION:

The Sleuth Kit, a suite of command-line tools for digital forensic investigation, may be used to discover partial and full multimedia files (video files) in a DataStream using open-source technologies. The Sleuth Kit works with a variety of file systems and can extract files and data from disc images, live systems, and other storage devices.

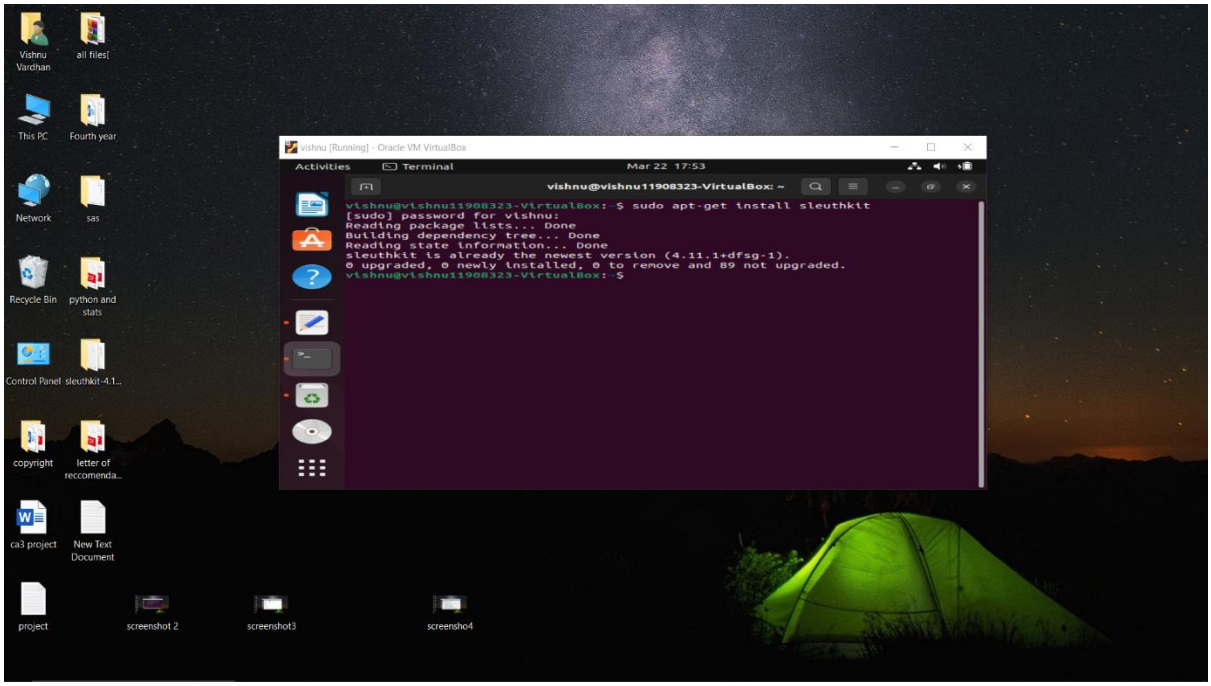
DESCRIPTION:

This project is asking for guidance on how to find partial and full multimedia files (specifically video files) within a DataStream using an open-source tool. It is not specified what the DataStream is, or its size or format. The question also asks for exploration of five additional features of the open-source tool used.

SCOPE:

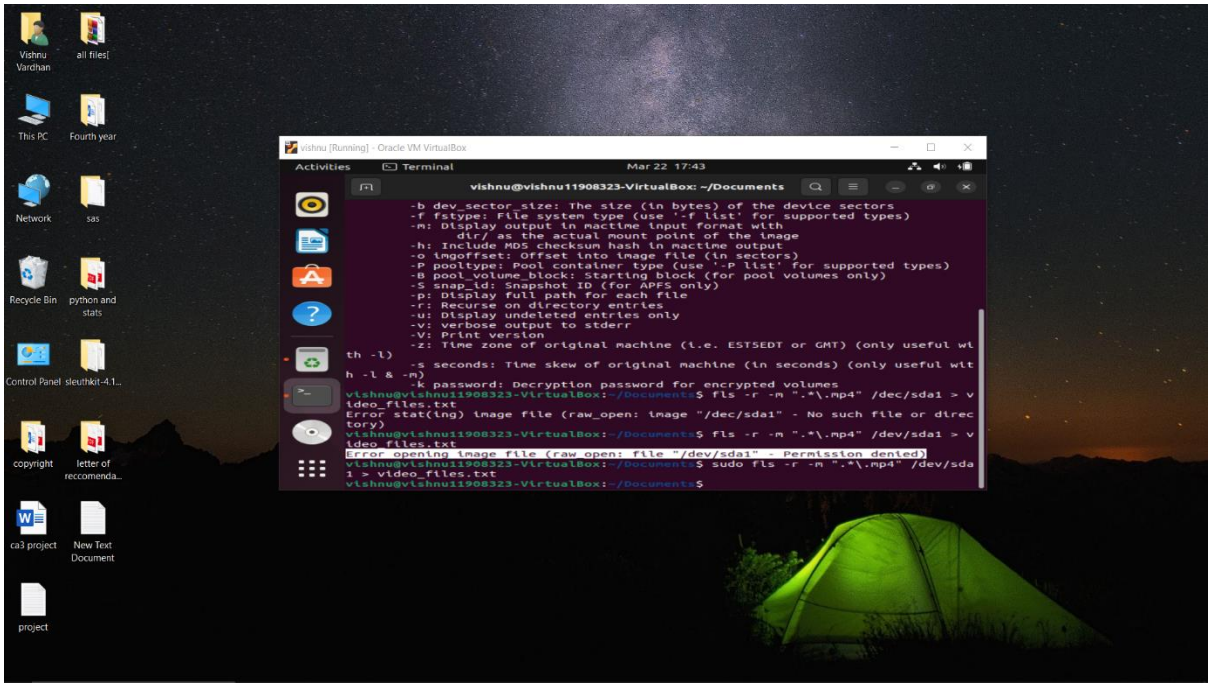
The scope of the project is to use any open-source tool to find partial and full multimedia files (video files) in a DataStream and explore five other features of the same software. The question does not provide any specific details about the DataStream, such as the size or format of the data, or the operating system being used.

II- Analysis Report:



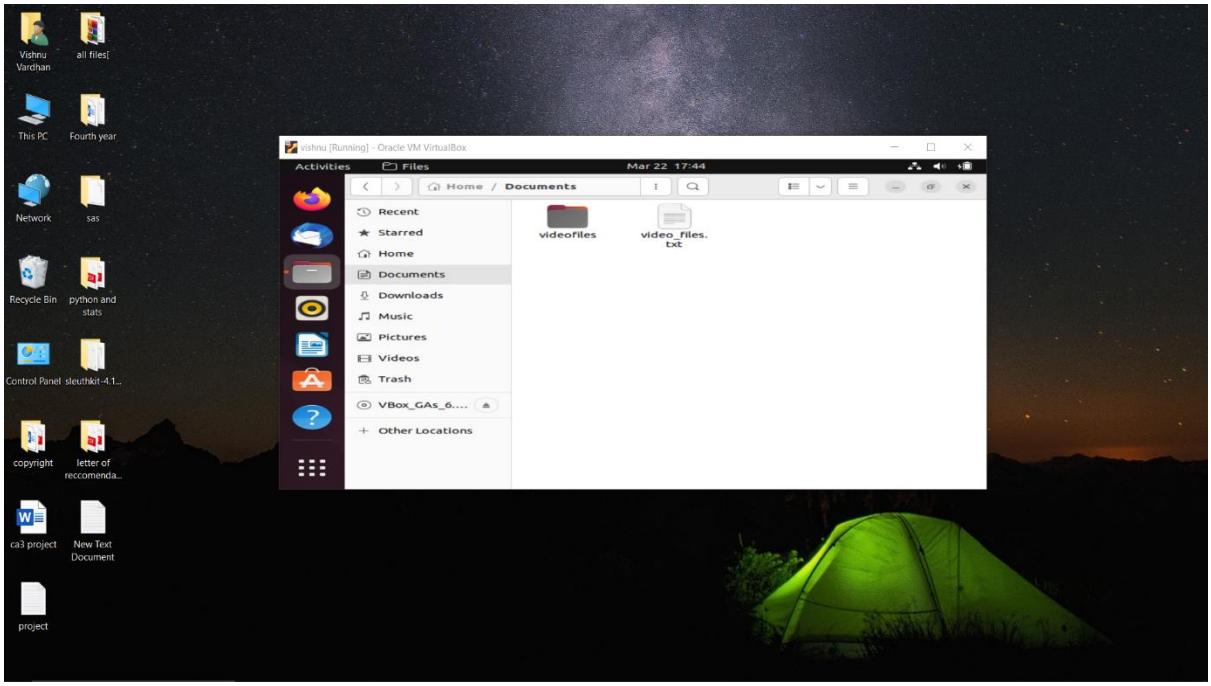
In this we are installing the sleuth kit in ubuntu using

sudo apt-get install sleuth kit

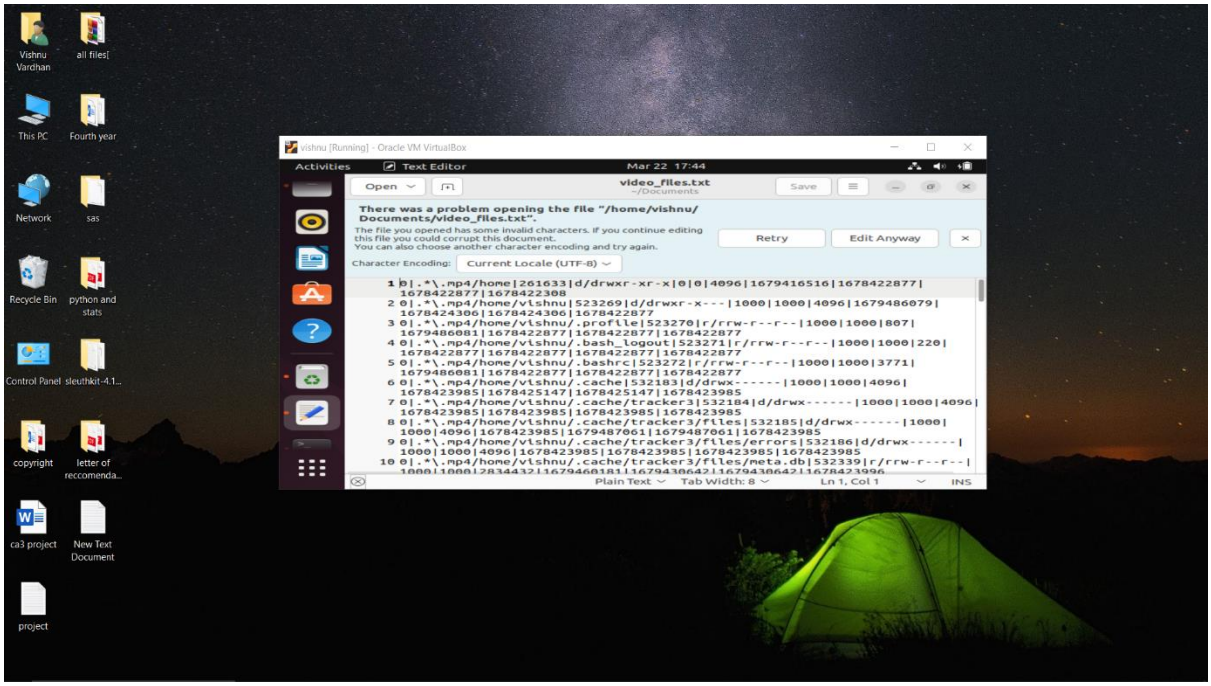


The "fls" command may be used to discover partial and full multimedia files (video files) in DataStream using Sleuth Kit. The "fls" command can display a list of all the files in a given DataStream, including deleted and incomplete files. Here's an example of how to discover video files in a DataStream using the "fls" command:

With the above command, we use the "-r" option to search all directories and subdirectories recursively, and the "-m" option to define the regular expression pattern to find video files. We are also sending the output to a text file named "video files.txt".



Here is the file where the output video_files.txt is located.



This is the output of the command used in the project.

Sleuth Kit also has the following handy features:

1. "fsstat" command: The "fsstat" command may display file system statistics such as file system size, block size, number of free and utilised blocks, and last mount time.

2. "mactime" command: Based on the timestamps of the files in a DataStream, the "mactime" command can provide a timeline of file activity. This can help forensic investigators identify the order of events.

3. The "istat" command displays precise information on a given file in a DataStream, such as the inode number, creation time, modification time, and access time.

4. The "img cat" command can display the contents of a given file in a DataStream. This is handy for inspecting the contents of deleted files or retrieving lost data.

5. The "blkls" command displays the contents of a specified block in a DataStream. This can be useful for studying raw disc data or rescuing data from a corrupted file system.