MySQL Backup and Restore using Python**Implement back and restore for MySQL using Python.**
Mysql - CREATE DATABASE studentrepo; | USE studentrepo; | CREATE TABLE IF NOT EXISTS students (id INT AUTO_INCREMENT PRIMARY KEY, name VARCHAR(100), age INT, class VARCHAR(50), city VARCHAR(100), phoneno VARCHAR(20), email VARCHAR(100)); | INSERT INTO students (name, age, class, city, phoneno, email) VALUES ('John Doe', 20, 'Physics', 'New York', '555-1234', 'johndoe@example.com'), ('Jane Smith', 22, 'Computer Science', 'Los Angeles', '555-5678', 'janesmith@example.com'), | show databases | show table ADD MORE**python part-**import os | MY_SQL_PATH = "C:/Program Files (x86)/MySQL/MySQL Server 5.5/bin" | def backup (user, password, database_name, backup_path, backup_file_name): command = f"mysqldump -u{user} -p{password} {database_name} > {backup_path}/{backup_file_name}"; os.chdir(MY_SQL_PATH); os.system(command); print("Database Backup Successful") | def recovery(user, password, database_name, backup_path, backup_file_name): command = f"mysql -u{user} -p{password} {database_name}<{backup_path}/{backup_file_name}"; os.chdir(MY_SQL_PATH); os.system(command); print("Database Recovery successful") | print("Select Operation: \n1. Backup\n2. Recovery"); operation=int(input("Enter operation: ")); if operation==1: backup(input("\nEnter username: "), input("Enter password: "), input("Enter Database Name: "), input("Enter Backup Path: "), input("Enter Backup Name: "),) elif operation==2: recovery(input("\nEnter username: "), input("Enter password: "), input("Enter Database Name: "), input("Enter Backup Path: "), input("Enter Backup Name: "),) else: print("Invalid Operation") | #C:/Users/student/Documents/MYSQLBackup. **MYSQL**-drop database studentrepo

Data Acquisition**To perform Data Acquisition using FTK Imager tool and Encase Tool—**Download and install FTK Imager tool https://accessdata-ftk-imager.software.informer.com/download/ | Step 2: Add the evidence folder in the tool | Select File -> Add evidence Item -> Contents of a folder and click on next | Add path of the folder and click on finish | File has been added to the evidence tree | Step 3: Now click on File and add the folder or file to make its copy, for that click on Create Disk Image | Step 4: Choose the option "Contents of a folder" and click next | Click yes | Step 5: Browse the folder which we want to make a copy and click Finish | Step 6: Now add the location for the copy document to store it, for that click on Add | Step 7: Fill details | Step 8: After clicking Next, don't change anything, just add the filename and destination folder | Step 9: After Finish, we can see the below page | Step 10: Now click on Start to copy the document | Step 11: Now the new popup will appear where we can verify the HASH values | Step 12: We can see that the folder file is copied to the given location | In that file, we can see the details of the folder.

Encase Tool-Step 1: Download and install Encase tool | Step 2: Select File -> New or click on the new icon to create a new evidence file | Step 3: Enter case details | Step 4: | Step 5: Select File -> Add Device | Step 6: Select Local Drives | Step 7: Choose the drive to create its image (D drive, pendrive) and click Next | After this step, details about the drive will be displayed | Click on Finish | Interface after adding the drive | Step 8: Select Entries -> D | Right-click on D (Drive) and select Acquire | Step 9: Add to Case and click Next | Step 10: Name the case, enter the evidence number and password, and specify the output path | Note - It will take some time for the tool to image the drive depending on the drive size | After Acquisition | After Verification (happens by default after acquisition) | Step 11: Verify evidence file | Select Tools -> Verify Evidence Files | Step 12: Check the report.

Use FTK tool | Steps: Install FTK and after that choose "Start a New Case" | Enter the case details | Enter the following details | Click Next | Select all options | Click Next | Click Next | Add evidence | Click Finish and it will take some time to analyze | Click on Documents | Click on Unchecked Items | Right-click any file -> Create Bookmark | The bookmark will be added, click the Bookmark tab | Right-click the bookmark to delete it | Go to the Search tab -> Indexed Search tab and enter the following keywords | Click "View Cumulative Results" | Add a new keyword, click "Options" and select the following options | Click OK for all | Go to the Live Search tab and add the following keyword | Check "Regular Expression" | Start Search | Click File -> Report Wizard | Enter the following details | Click Next | Click Next | Click Next | Click Next | Click Next | Click Next | Click Next | Click Yes | View the report | Click Backup Case | Backup Folder | Open the backup case again. | Q.2] Using Autopsy | Aim: Using Autopsy for Case Investigation | Description: Case examination in cyber forensics involves collecting and analyzing digital evidence from devices to investigate cybercrimes. This includes recovering deleted files, analyzing logs, and using forensic tools like Autopsy and FTK to uncover relevant data. The evidence is then documented for use in legal proceedings, ensuring its integrity throughout the process.

Autopsy tool: Step 1: Download and install the Autopsy tool | Autopsy Interface | Step 2: Add New Case | Add Case Name and Base Directory | Step 3: Enter Case Information and click Finish | Case Database will be created | For Image 1 - precious.img file | Step 4: Select type of data source - Disk Image and click Next | Step 5: Select Data Source Path (Give Image's path) and click Next | After successfully adding the data source, the below message will be displayed | The tool is analyzing the file | Step 6: Click on the image to view the hexadecimal content of the file | Step 7: To perform a keyword search, select Tools -> Options -> Keyword Search | Step 8: Create a New Keyword List | Step 9: Add New Keywords | Step 10: Select type for keywords - Exact Match | Select type for keywords - Regular Expression | Select type for keywords - Substring Match | Click OK | Keyword List | Step 11: Right-click on precious.img and select "Run Ingest Modules" | Check if "Keyword Search" is selected and click Finish | Step 12: To test Keywords, select Analysis Result -> Keyword Hits -> List 1 (Keyword List Name) | Step 13: Generate a Report of the Examination | Step 14: Open Report File | For Image 2 - sample1.img file | Step 1: Select type of data source - Disk Image and click Next | Step 2: Select Data Source Path (Give Image's path) and click Next | After successfully adding the data source, the below message will be displayed | The tool is analyzing the file | Step 3: Click on the image to view the hexadecimal content of the file | Step 4: To perform a keyword search, select Tools -> Options -> Keyword Search | Step 5: Create a New Keyword List | Step 6: Add New Keywords | Step 7: Select type for keywords - Exact Match | Select type for keywords - Regular Expression | Select type for keywords - Substring Match | Click OK | Keyword List | Step 8: Right-click on sample1.img and select "Run Ingest Modules" | Check if "Keyword Search" is selected and click Finish | Step 9: To test Keywords, select Analysis Result -> Keyword Hits -> List 2 (Keyword List Name) | Step 10: Generate a Report of the Examination | Step 11: Open Report File.

Perform Email Forensics using Outlook and Forensic Tool 1.8.2 | Steps: Create an Outlook account | Send email to personal email | Click send | Check sent items | Check received email | Send email to Outlook | Check received email in Outlook | Delete email | Check deleted items | Click File and then click Open & Export | Click Export and select export to a file | Select .pst | Select Deleted Items, Inbox, and Sent Items | Specify path | Set password | Type the password again | Backup file is created | Open AccessData Forensic Tool | Start new case and enter case details | Enter the following details | Click next | Click next | Select email emphasis | Click next | Click add evidence and select individual file | Select the backup.pst file | Enter the following | Evidence is added | After the processing is done | Click Email Messages | Click any message | Go to Email tab and expand the backup.pst file | For jimsin.pst's inbox mails | Backup the case.

Perform Browser Forensics using Browser History Examiner Tool | Note: Clear browsing history from all browsers before starting (trial version displays only first 25 records) | Steps: Download, Install, and Open Browser History Examiner | Click File > Capture History | Click Next | Specify location | Click Capture | Search something in the browser | Dialog box appears, click Yes | Report is generated | Click File > Load History | Select the capture folder | Report preview | Explore all items | Click File > Export > Export as HTML | Click Export | Open the report | Add records to reports by marking the STAR | Click File > Report > Save as PDF | Open the report.

S-Tool Steps: Step 1: Download steg.zip (https://www.cs.vu.nl/~ast/books/mos2/steg.zip), unzip, and run S-Tools | Step 2: Download a .gif or .bmp image | Step 3: Drag and drop the image into S-Tools (add to steg folder) | Step 4: Create a text file, add content, and drag it onto the image | Step 5: Add a passphrase, select an encryption algorithm, and a new image (hidden data) will be created | Step 6: Decrypt the hidden message by right-clicking the file, selecting Reveal, and entering the same passphrase | Step 7: Right-click the text file, select Save As, and open it

SteganPEG Steps: Step 1: Install SteganPEG (https://www.softpedia.com/get/Security/Encrypting/SteganPEG.shtml) and select "Embed files into a JPEG image" | Step 2: Enter an encryption password, download a .jpg image, add its path, and click GO! | Step 3: Create a text file with content, add it, and save the stegged image | Step 4: Select "Read files from a JPEG image" for decryption and add the stegged image path | Step 5: Enter the same password, extract the file, and view its contents.