1. **Study of Digital Forensics and different tools used for forensic investigation.**

**Experiment using Autopsy.**

* Install Autopsy: Autopsy is a free, open-source digital forensics platform that can be installed on Windows, MacOS, and Linux.
* Acquire Evidence: Obtain a forensic image of the suspect device or hard drive, either through physical acquisition or logical acquisition.
* Add Image to Autopsy: Import the acquired image into Autopsy, creating a new case and specifying the details of the image.
* Select Analysis Options: Choose the appropriate analysis options, including hash databases, file system type, and specific modules to run.
* Analyse the Image: Start the analysis process, which may take several hours to complete, depending on the size of the image and the selected modules.
* Review Results: Review the results of the analysis, including a list of files and folders, hash sets, keyword searches, and timeline analysis.
* Bookmark and Tag Evidence: Bookmark and tag evidence items for further analysis or to include in a report.
* Create a Report: Create a comprehensive report of the findings, including evidence items, analysis results, and conclusion.
* Present the Evidence: Present the evidence and report to relevant parties, including law enforcement or legal teams.

1. **How to Recover Deleted Files using Forensics Tools.**

* Acquire a copy of the storage device: Create a forensic image of the storage device where the deleted files are located. This ensures that the original data is not altered during the recovery process.
* Analyse the storage device: Use a digital forensics tool such as Autopsy, FTK Imager, or EnCase to analyse the storage device and determine if the deleted files can be recovered.
* Search for deleted files: Use the tool's search or recovery functions to locate the deleted files. These functions typically look for unallocated space on the storage device where the deleted files may still reside.
* Preview the recovered files: Preview the recovered files to confirm that they are the correct ones and that they are in a usable state.
* Save the recovered files: Save the recovered files to a separate storage device, such as a USB drive or external hard drive, to avoid overwriting any of the deleted data.
* Document the recovery process: Document the steps taken during the recovery process, including the tools used and any relevant settings. This documentation can be used as evidence in a court of law if necessary.

Additional Software: Recuva

1. **Study the steps for hiding and extract any text file behind an image file/ Audio file using Command Prompt.**

* Select an Image to Be Used for Hiding File Behind the Image. E.g.; kumar.jpg
* Now Select a File to Hide Behind the Image and Make It in .RAR Format. (e.g.: secret.rar) With the Help of the WinRAR.
* Go to Command Prompt and browse to that directory and run this command
* ***Copy /b kumar.jpg + secret.rar finalimage.jpg***
* Finalimage.jpg is the image file which will have secret.rar hidden.
* To Open Hidden Files:
* Open winrar
* Now locate your image (finalimage.jpg) and open it or simply drag your image in WinRAR.
* Extract the file and done.

1. **How to Extract Exchangeable image file format (EXIF) Data from Image Files using Exif reader Software.**

* Download and install Exifreader software on your computer.
* Open Exifreader software.
* Click on the "File" menu and select "Open."
* Select the image file from which you want to extract EXIF data.
* The EXIF data of the selected image will be displayed in the main window of Exifreader software.
* You can save the EXIF data by clicking on the "File" menu and selecting "Save As."
* Select the desired file format for saving the EXIF data and click on "Save."

1. **How to make the forensic image of the hard drive using FTK**

* Connect the hard drive to the computer where FTK is installed.
* Launch FTK Forensics and select Create disk image
* Select Physical Drive from the list of acquisition options.
* Select the hard drive you want to image and click "Next."
* Choose the "Create Image File" option and select the destination for the forensic image.
* Set the desired imaging options, such as compression, encryption, and hash calculation.
* Click "Start" to begin the imaging process.
* FTK will create a bit-by-bit image of the hard drive and save it to the specified location.
* Verify the integrity of the image by comparing the hash value of the original drive and the created image.

1. **How to Restore the Evidence Image using Autopsy**

* Launch Autopsy and select "New Case"
* Enter case Information and Base Directory
* Input details of the Examiner, the case directory will be created
* Select the disk image or VM file and choose the image file.
* Select the source image file.
* Configure the ingest modules (Select all by default).
* Click on finish.

1. **(A) How to Collect Email Evidence in Victim PC**

* Secure the computer and preserve the evidence by disconnecting it from the network and avoiding further use.
* Make a forensic image of the hard drive using a reliable forensic tool, such as EnCase Forensics, to preserve the original data.
* Launch the forensic tool and examine the image to locate and extract the email evidence.
* Look for email client software, such as Microsoft Outlook or Mozilla Thunderbird, and their associated data files, such as PST or MBX files.
* Extract the email client data files and any associated attachments or email messages.
* Use the forensic tool to analyse the extracted data and recover deleted or hidden email messages, if necessary.
* Document the process and store the extracted email evidence in a secure location.

**(B) How to Extract Browser Artifacts.**

* Secure the computer and preserve the evidence by disconnecting it from the network and avoiding further use.
* Make a forensic image of the hard drive to preserve the original data.
* Launch the forensic tool and examine the image to locate and extract the browser artifacts.
* Look for the browser's cache, history, and cookie files, which are typically stored in specific locations on the hard drive. Look for SQLite Database.
* Extract the relevant browser files and use the forensic tool to analyse the data.
* Analyse the browser cache, history, and cookie files to recover web pages visited, login information, and other relevant artifacts.
* Document the process and store the extracted browser artifacts in a secure location.

1. **(A) How to View Last Activity of Your PC.**

* Press the "Windows" key and the "R" key on your keyboard to open the Run dialog.
* Type "eventvwr.msc" and press "Enter" to open the Event Viewer.
* In the Event Viewer window, expand the "Windows Logs" section and select the "System" log.
* Scroll through the log entries to view the recent activity on the computer, including system start-up and shut-down, software installation, and other system events.
* You can also view the "Application" log to see the activity of specific software applications.
* Use utility from Nirsoft : <https://www.nirsoft.net/utils/computer_activity_view.html>

1. **Find Last Connected USB on your system (USB Forensics)**

* Press the "Windows" key and the "R" key on your keyboard to open the Run dialog.
* Type "eventvwr.msc" and press "Enter" to open the Event Viewer.
* In the Event Viewer window, expand the "Windows Logs" section and select the "System" log.
* Scroll through the log entries to find the entry for the last connected USB device. The entry should have a description like "USB Mass Storage Device connected."
* The entry will include the date and time the USB device was connected, as well as the device name and manufacturer.

Using Registry:

* Press the "Windows" key and the "R" key on your keyboard to open the Run dialog.
* Type "regedit" and press "Enter" to open the Registry Editor.
* In the Registry Editor, navigate to the following key: HKEY\_LOCAL\_MACHINE\SYSTEM\CurrentControlSet\Enum\USB
* In the USB key, you will see multiple subkeys, each representing a connected USB device.
* The subkeys are named based on the device's identifier, such as "VID\_XXXX&PID\_XXXX". The "XXXX" represents the vendor and product IDs of the device.
* To determine the last connected USB device, look at the "LastWrite" time of each subkey. The subkey with the most recent "LastWrite" time represents the last connected USB device.
* You can also view the "FriendlyName" value of the subkey to get the device name.

1. **Comparison of two Files for forensics investigation by Compare IT software**

* Install Compare It software on your computer.
* Launch the Compare It software and select the two files you want to compare.
* The software will compare the files and display the differences in a graphical format, such as highlighting the differences in red and green.
* Review the differences between the two files and make note of any changes or modifications that may be relevant to the forensic investigation.
* If desired, you can also save the comparison results as a report or export them to another file format.

1. **Live Forensics Case Investigation using Autopsy**

* Obtain the live system: Acquire a physical or network-based image of the live system that you want to investigate.
* Install Autopsy: Download and install Autopsy on a separate forensics’ workstation. Autopsy is a free and open-source digital forensics platform.
* Create a case: In Autopsy, create a new case and provide the case details, such as the case name and the date the case was created.
* Add the image to the case: In Autopsy, add the image of the live system to the case. Autopsy supports multiple image formats, including EnCase and raw image formats.
* Configure data sources: In Autopsy, configure the data sources you want to analyse, such as the file system, the registry, and the memory dump.
* Run Autopsy: Run Autopsy and let the software analyse the data sources and extract relevant information, such as file system artifacts, registry keys, and memory dumps.
* Review the results: In Autopsy, review the results of the analysis, including the file system artifacts, registry keys, and memory dumps. You can also use the built-in search functionality to find specific files, artifacts, or keywords.
* Document findings: Document the findings of the investigation in a report, including the relevant artifacts and other evidence.