Experiment No .2

2.1 Aim: Investigative Procedures: Bag and Tag Evidence,Photographing Evidence, Transferring Photographs, Chain of Custody.

Example Scenario: A local IT company suspects one of its employees of unauthorized data exfiltration. The system administrator noticed unusual USB activity on a desktop computer used by the suspect (employee name: **Ravi Sharma**). You, as a junior digital forensic investigator, are called to **collect and preserve digital and physical evidence** from the suspect's workstation for further analysis.

2.2 Lab Outcome :

- Demonstrate practical skills in identifying, collecting, photographing, and preserving physical and digital evidence while maintaining the chain of custody.

2.3Learning Objectives:

- Identify potential physical and digital evidence at a cybercrime scene.
- Perform "bag and tag" procedures following standard forensic protocols.
- Photograph evidence maintaining proper angles and labeling for investigation.
- Transfer digital photographs securely using forensic best practices.
- Complete and maintain a chain of custody form to ensure evidence admissibility in legal proceedings.

2.4 Requirement:

- Desktop or laptop (as mock crime scene)
- USB drive (used as mock evidence)
- Camera or smartphone for photography

- External storage device or secure cloud folder

Materials:

- Anti-static or zip-lock evidence bags
- Tags/labels and markers
- Printed chain of custody form

Software:

- Image viewer
- Secure file transfer utility (optional, e.g., Google Drive, encrypted ZIP)

Documentation:

- Chain of Custody template (printed or digital)
- Evidence log sheet

2.5 Related Theory :

Bag and Tag Procedure:

- A critical process in evidence handling where each item is physically secured in a labeled bag to prevent contamination and tampering.
- Tags should contain metadata like time, date, collector's name, location, and evidence type.

Photographing Evidence:

- Must follow protocols: overall, mid-range, and close-up photos.

- Include scale (e.g., ruler) and labels in the image where possible.
- Maintain metadata (EXIF) to validate authenticity.

Transferring Photographs:

- Photos should be transferred securely using forensic copy methods.
- Any movement or duplication of files must be logged with timestamps.

Chain of Custody:

- A documented record of who collected, handled, transferred, and stored the evidence from the scene to the courtroom.
- Ensures accountability and integrity; any break can invalidate evidence in court.

Legal Relevance:

- Improper evidence handling may lead to the **inadmissibility of evidence** in court.
- Following proper procedures upholds **forensic soundness** and **legal admissibility** under rules of evidence (e.g., Indian Evidence Act or international equivalents).

2.6 Output:
(make chain of custody report by using this data.)

Date & Time	Evidence ID	Action Taken	By Whom	To Whom	Purpose/Notes

2.7 Conclusion: