PUNE INSTITUTE OF COMPUTER TECHNOLOGY, PUNE

ACADEMIC YEAR: 2023-24

DEPARTMENT OF COMPUTER ENGINEERING DEPARTMENT

CLASS: B.E. **SEMESTER: I**

SUBJECT: LP-IV

ASSIGNMENT NO.	A4
TITLE	Write a computer forensic application program for Recovering permanent Deleted Files and Deleted Partitions
PROBLEM STATEMENT /DEFINITION	Write a computer forensic application program for Recovering permanent Deleted Files and Deleted Partitions
OBJECTIVE	1)To learn different types of file system. 2)To understand the use of partitions and its structure. 3)To understand the importance of file recovery in forensics.
OUTCOME	Students will be able to - 1. Learn the different ways to recover a deleted file is studied.
S/W PACKAGES AND HARDWARE APPARATUS USED	1. 64 bit open source LINUX 2. Eclipse- 64 bit. 3. sleuth-kit installed.
REFERENCES	1. https://wiki.sleuthkit.org/index.php?title=FS_Analysis 2. https://www.therootuser.com/2017/11/recover-deleted-files-using-sleuthkit/
STEPS	Refer to theory, algorithm, test input, test output
INSTRUCTIONS FOR WRITING JOURNAL	1. Date 2. Assignment no. 3. Problem definition 4. Learning objective 5. Learning Outcome 6. Concepts related Theory 7. Algorithm 8. Test cases 9. Conclusion/Analysis

Prerequisites:

Concepts related Theory:

- **Introduction:**
  1. The Linux and Unix Trash is the equivalent of the Window?s Recicle
- Been. Every user has it?s own trash in Linux and Unix Systems.
- By default, the trash is located in the user?s /.local/share/Trash. The /.lo-
- cal/share/Trash directory contains two folders, les and info.
- The /.local/share/Trash/les folder contains all the les and folders inside

- the Trash.
- Example:
- ls -l les /.local/share/Trash/les
- -rw-rw-r 1 razvan razvan 0 2012-08-08 14:22 23
- -rwxrwxrwx 1 razvan razvan 220 2012-08-15 14:23 a
- drwxrwxrwx 2 razvan razvan 4096 2012-07-25 02:18 abc
- drwxrwxrwx 2 razvan razvan 4096 2012-08-10 00:26 abcd
- -rwxrwxrwx 1 razvan razvan 14 2012-07-04 01:28 b
- -rwxrwxrwx 1 razvan razvan 7 2012-07-04 01:28 b2
- 2. View the les inside the trash:
- You can easily nd out the les and folders inside the trash, with list-trash:
- list-trash
- 2012-08-15 15:10:27 /home/razvan/one
- 2012-08-15 15:09:59 /home/razvan/foo
- 2012-08-15 15:26:42 /home/razvan/1
- 3. Restoring les from trash:
- To restore les from trash, use restore-trash and type the number repre-
- senting the le you want to restore.
- Restore-trash

SLEUTH-KIT

The Sleuth Kit (TSK) is a library and collection of Unix- and Windows-based tools and utilities to allow for the forensic analysis of computer systems. It was written and maintained by digital investigator Brian Carrier. TSK can be used to perform investigations and data extraction from images of Windows, GNU/Linux and Unix computers. The Sleuth Kit is normally used in conjunction with its custom front-end application, Autopsy, to provide a user friendly interface. Several other tools also use TSK for file extraction.

The Sleuth Kit is a free, open source suite that provides a large number of specialized command-line based utilities.

It is based on The Coroner's Toolkit.

Journalling

A journaling file system is a file system that keeps track of the changes that will be made in a journal (usually a circular log in a dedicated area of the file system) before committing them to the main file system. In the event of a system crash or power failure, such file systems are quicker to bring back online and less likely to become corrupted**.**

Conclusion: successfully implemented the program for File recovery using the sleuth kit tool.

Review Questions:

1) What are different types of file system?
2) How to understand the use of partitions and its structure?
3) What are importance of file recovery in forensics?
4) Learn the different ways to recover a deleted file is studied.