LAB Manual

PART A

(PART A : TO BE REFERRED BY STUDENTS)

**Experiment No.09**

**Aim:**

Study of any five tools for e-mail forensics.

**Theory:**

Digital forensics is the field of determining who was responsible for a digital intrusion

or other computer crime. It uses a wide range of techniques to gain attribution to the

perpetrator.

It relies upon the fundamental concept that whenever a digital intrusion or crime is

committed, the perpetrator inadvertently leaves a bit of themselves behind for the

investigator to find. These "bits" could be entries in log files, changes to the registry,

hacking software, malware, remnants of deleted files, etc. All of these can provide

clues and evidence to determine their identity and lead to the capture and arrest of the

hacker.

As a hacker, the more you know and understand about digital forensics, the better you

can evade the standard forensic techniques and even implement anti-forensic measures

to throw off the investigator.

PART B

(PART B : TO BE COMPLETED BY STUDENTS)

***(Students must submit the soft copy as per following segments within two hours of the practical slot. The soft copy must be uploaded on the Blackboard or emailed to the concerned lab in charge faculties at the end of the practical in case the there is no Black board access available)***

|  |  |
| --- | --- |
| Roll No. | Name: |
| Class : | Batch : |
| Date of Experiment: | Date of Submission |
| Grade : | Time of Submission: |
| Date of Grading: | |

**B.1 Features of Software tools studied by student:**

***(Paste your java code completed during the 2 hours of practical in the lab here)***

**B.2 Advantages and limitations of each tool:**

***(Paste your program input and output in following format, If there is error then paste the specific error in the output part. In case of error with due permission of the faculty extension can be given to submit the error free code with output in due course of time. Students will be graded accordingly.)***

**B.3 Observations and learning:**

***(Students are expected to comment on the output obtained with clear observations and learning for each task/ sub part assigned)***

**B.4 Which tool did you like the most and why?:**

*(****Students must write the conclusions based on their learning)***