CAP797:CYBER FORENSICS-LABORATORY

Course Outcomes: Through this course students should be able to

CO1 :: understand the basic mechanisms of computer forensics

CO2 :: identify various mechanisms for carrying out computer forensic practices

CO3 :: employ various computer forensics tools to investigate cyber crime scene

CO4 :: conclude the cyber forensic investigation by creating investigative reports

List of Practicals / Experiments:

Analyzing storage devices and file system

- identifying disk layout
- partition table
- files system
- files
- directories
- time stamp
- unallocated space
- slack space

Creating disk imaging

- magnetic disk imaging
- USB disk imaging

Preserving integrity of forensic evidence

- cryptographic hashing
- evidence preservation
- error handling
- logging
- splitting and verification

Recovering deleted files

- recover deleted files from disk drives

Documentation

- generating report using FTK tool

Investigating network traffic

- live packet capturing and packet analysis

Tracking emails and investigating email crimes

- email forensics

Accruing data from ram

- volatile data collection

Text Books:

1. COMPUTER FORENSICS AND CYBER CRIME: AN INTRODUCTION by MARJIE T. BRITZ, Pearson Education India

References:

1. REAL DIGITAL FORENSICS: COMPUTER SECURITY AND INCIDENT RESPONSE by KEITH J. JONES, ADDISON-WESLEY