CHAROTAR UNIVERSITY OF SCIENCE AND TECHNOLOGY
CHANDUBHAI S PATEL INSTITUTE OF TECHNOLOGY
K.D. PATEL DEPARTMENT OF INFORMATION TECHNOLOGY
ACADEMIC YEAR: 2022-23

List of Experiments

Subject: Cyber Security (IT382) (6th Semester)

Exp. No	Name of Experiment	Hours
1.	The computer forensics investigation process is a methodological approach of preparing for an investigation, collecting and analyzing digital evidence, and managing the case from the reporting of the crime until to the case's conclusion. This process takes place in a computer forensics lab. A computer forensic expert should be well-versed in how to use various tools for data recovery. By using tools such as EaseUS Data Recovery Wizard, MD5 Calculator, and HashCalc, it is possible to recover files that have been deleted even from a device's recycle bin, make a duplicate, and check the checksums to compare with the original data. A computer forensics lab (CFL) is a designated location for conducting computer-based investigations on collected evidence. It is an efficient computer forensics. Perform the following activities: 1. Recovering Data Using the EaseUS Data Recovery Wizard 2. Performing Hash, Checksum, or HMAC Calculations Using the HashCalc 3. Generating MD5 Hashes Using MD5 Calculator 4. Viewing Files of Various Formats Using the File Viewer 5. Handling Evidence Data Using the P2 Commander 6. Creating a Disk Image File of a Hard Disk Partition Using the R-Drive Image	06
2.	A hard disk drive is a non-volatile, random access digital data storage device used in most computer systems. A file system is a set of data types that is employed for storage, hierarchical categorization, management, navigation, access, and recovery of data. While investigating a computer-based crime, it is most important to understand hard disks and file systems, as these are the major sources of data storage. People usually delete their tracks after committing a crime with a computer in order to avoid being traced. That is why recovering the deleted files of hard disks and analyzing file systems is important when investigating a computer-based crime. Perform the following activities: 1. Recovering Deleted Files from Hard Disks Using WinHex 2. Analyzing File System Types Using The Sleuth Kit (TSK)	04

	3. Analyzing Raw image using Autopsy	
3.	Data acquisition is the process of gathering evidence or information. This can be done by using established methods to acquire data from a suspected storage media to get access to information about the crime or other incident, and potentially using that data as evidence to convict a suspect. Data duplication is a critical process in any computer forensic investigation. Many duplication tools are available that can duplicate create a copy of data. To start an investigation, a person who wants to examine data on a suspect machine needs to create an image of the disk. Perform the following activities: 1. Investigating NTFS Drive Using DiskExplorer for NTFS 2. Viewing Content of Forensic Image Using Access Data FTK Imager Tool	02
4.	There are different types of anti-forensics techniques such as data/file deletion, wiping/overwriting data and metadata, corruption / degaussing, cryptographic file systems, password protection, etc. Anti-forensics are the techniques the perpetrators use to avert detection through forensics investigation process. These techniques hinder proper forensics investigation process by reducing the quantity and quality of digital evidence. Perform the following activities: 1. Cracking Application Password (Passware Password Recovery Kit Forensic, Advanced Archive Password Recovery, and Advanced PDF Password Recovery) 2. Detecting Steganography (StegSpy, OpenStego, and DeepSound)	04
5.	Network forensics is the process of identifying criminal activity and the people behind the crime. Network forensics can be defined as sniffing, recording, acquisition, and analysis of the network traffic and event logs in order to investigate a network security incident. Perform the following activities: 1. Investigating System Log Data Using XpoLog Center Suite Tool 2. Investigating Network Attacks Using Kiwi Log Viewer 3. Investigating Network Traffic Using Wireshark	06
6.	Perform Windows Event Logs Analysis with Splunk/Event Manager.	04
7.	Demonstration of any security tool.	04