SILVER OAK UNIVERSITY

Silver Oak College of Computer Application
Master of Science Cyber Security & Digital Forensics
Course Name: Practical-1(Cyber Crime Investigation & Forensic)
Course Code: 1040147203
Semester: 3rd

Prerequisite: Basic knowledge of system and mobile devices, Social Networking platforms, Types of web application functionality

Course Objective: To train the students about various types of Cyber Crimes and their investigation methodology, basic concepts of Cyber Law and use of Forensics tools for data processing.

Teaching Scheme:

Teaching Scheme				
L	T	P	Contact Hours	Credit
0	0	8	8	4

List of Experiments: **Total Hours: 112**

Sr. No.	Practical Name
1.	Create forensic images of hard disks and USB drives using tools like FTK Imager.
2.	Investigate a fake social media profile to identify impersonation and gather evidence.
3.	Recover browsing history and cookies from browsers using forensic tools.
4.	Analyze file systems to trace unauthorized access and data theft.
5.	Work with comprehensive forensic toolkits like FTK for various investigations.
6.	Extract and analyze email headers and IP addresses to trace email fraud.
7.	Use Hashcat to crack passwords efficiently with GPU acceleration.
8.	Analyze network traffic to identify sources and methods of DoS attacks.
9.	Recover deleted files and data from formatted partitions.
10.	Collect and analyze evidence from social media and blogs for defamation cases.
11.	Use EnCase Forensic Edition for in-depth digital investigations.
12.	Track emails and IP addresses, and recover deleted emails.
13.	Investigate transaction logs and digital evidence related to financial fraud.

14.	Recover data and analyze activities on mobile devices using forensic tools.
15.	Investigate network breaches by analyzing traffic and logs.
16.	Analyze infected systems to understand and document malware behavior.
17.	Conduct an in-depth investigation of a real-world cybercrime case using digital forensic techniques.
18.	Utilize advanced forensic tools and techniques to analyze digital evidence from a cybercrime case.
19.	Simulate a cyber incident response scenario to practice forensic investigation and response skills.
20.	Investigate emerging technologies and future trends in cyber forensics.

Course Outcomes:

Sr. No.	CO Statement
CO-1	Demonstrate proficiency in creating images of hard disks and removable storage media.
CO-2	Analyze internet usage data and perform recovery, extracting valuable information for forensic investigations.
CO-3	Apply forensic tools and techniques to track emails, IP addresses, and recover deleted emails, enhancing their ability to conduct thorough investigations.
CO-4	Develop an understanding of security measures to protect against data breaches and unauthorized access, applying password cracking techniques to assess the strength of password policies.
CO-5	Evaluate eDiscovery tool for forensic investigation.

Teaching & Learning Methodology:

1. The course includes a laboratory, where students have an opportunity to build an appreciation for the concepts being taught in lectures.
2. Lectures with live practical example using Projector and Computer
3. Experiments shall be performed in the laboratory related to course contents

Major Equipment:

1. Computer System
2. LAN cable

Books Recommended:

1. Lindsay, “International Domain Name Law:ICANN and the UDRP”, Oxford: Hart Publishing
2. Sharma J. P & Kanojia S., “Cyber Laws”, New Delhi:Ane Books Pvt. Ltd
3. Duggal P., “Cyber Laws”, Universal Law Publishing
4. Kamath N., “Law relating to computers, internet and e-commerce: A guide to Cyber Laws and the IT Act,2000 with rules, regulations and notifications” Delhi: Universal Law Publishing Co.
5. Prosise C., “Incident response & computer forensics”, McGraw-Hill Companies

CO-PO-PSO MATRIX:

Co. No	PO1	PO2	PO3	PO4	PO5	PO6	PO7	PSO1	PSO2
CO-1	2	2	3	1	2	1	2	2	2
CO-2	2		3	1			2	2	3
CO-3	2	1	2	3	2	1	2	3	1
CO-4	3	2		3			3	1	1
CO-5	3	3	3	2	3	2	3	3	2