SARVAJANIK UNIVERSITY
INCLUSIVE | INTEGRATED | INNOVATIVE

SARVAJANIK UNIVERSITY
Sarvajanik College of Engineering and Technology
Bachelor of Technology

Year: B. Tech IV (Semester VII)

Subject Name: Digital Forensics **Subject Code:** BTEA19723
Type of course: Honors (Group: Cyber Security)
Prerequisite (if any): Operating system concepts, Computer Network, DBMS, Web Technology

Rationale: The purpose of this course is to introduce the principles of digital forensics in computers, wireless and wire line networks. The students are exposed to techniques and tools that allow the discovery, collection, preservation, and analysis of evidence with the purpose of understanding the weaknesses that made the attacks possible.

Teaching and Examination Scheme:

Teaching Scheme				Theory Marks			Practical Marks		Total
L	T	P	C	TEE	CA1	CA2	TEP	CA3	
3	0	2	4	60	25	15	30	20	150

CA1: Continuous Assessment (assignments / projects / open book tests / closed book tests) CA2: Sincerity in attending classes / class tests / timely submissions of assignments / self-learning attitude / solving advanced problems TEE: Term End Examination TEP: Term End Practical Exam (Performance and viva on practical skills learned in course) CA3: Regular submission of Lab work / Quality of work submitted / Active participation in lab sessions / viva on practical skills learned in course.

Contents:

Sr. No.	Contents	Total Hours
1	Introduction : Understanding of Forensic Science, Digital Forensic, The Digital Forensic Process, Lockard's Exchange Principle, Scientific Models. Computer Crime: Criminalistics as it relates to the Investigative Process, Analysis of Cyber-Criminalistics Area, Holistic Approach to Cyber-Forensics.	07
2	Understanding of the Technical Concepts : Basic Computer Organization, File system, Memory organization Concept, Data Storage Concepts	07
3	Digital Forensics Process Model: Introduction to Cybercrime Scene, Documenting the Scene and Evidence, Maintaining the Chain of Custody, Forensic Cloning of Evidence, Live and Dead System Forensic, Hashing concepts to maintain the Integrity of Evidence, Report Drafting.	07
4	Computer Forensics : Prepare a Case, Begin an Investigation, Understand Computer Forensics Workstations and Software, Conduct an Investigation, Complete a Case, Critique a Case Network Forensics : Open-source security tools for Network Forensic Analysis,	12

	Requirements for Preservation of Network Data. Mobile Forensics : Mobile Forensics Techniques, Mobile Forensics tools.	
5	Legal Aspects of Digital Forensics: Understanding of Legal Aspects and their impact on Digital Forensics, Electronics Discovery	04
6	Understanding of Digital Forensic Tools : Quality Assurance, Tool Validation, Tool Selection, Hardware, and Software tools	04
7	Case Study: Understanding of Internet Resources, Web Browser, Email Header Forensic, Social Networking Sites	04

Suggested Specification table with Marks (Theory): (For B. Tech only)

Distribution of Theory Marks					
R Level	**U Level**	**A Level**	**N Level**	**E Level**	**C Level**
15	20	20	05	-	-

Legends: R: Remembrance; U: Understanding; A: Application, N: Analyze and E: Evaluate C: Create (Revised Bloom's Taxonomy)

Reference Books:

Sr No	Title of book /article	Author(s)	Publisher and details like ISBN	Year of publication	Publication Edition
1	Cyber Security: Understanding Cyber Crimes, Computer Forensics and Legal Perspectives	Nina Godbole and Sunit Belpure	Wiley	2011	1st Edition
2	The Basics of Digital Forensics: The Primer for Getting Started in Digital Forensics	John Sammons	Syngress	April 2012	1st Edition
3	Practical Digital Forensics	Richard Boddington	Packt Publishing Limited	January 2016	1st Edition
4	Computer Forensics: Computer Crime Scene Investigation	John Vacca	Laxmi Publications	January 2015	1st Edition

5	Digital Forensic: The Fascinating World of Digital Evidence	Dr. Nilakshi Jain and Dr. Dhananjay Kalbande	Wiley Press	January 2016	1st Edition

Course Outcomes (CO):

Sr. No.	CO statements	Marks % weightage
CO-1	Describe Forensic science and Digital Forensic concepts	20
CO-2	Determine various digital forensic Operandi and motive behind cyber attacks	15
CO-3	Interpret the cyber pieces of evidence, Digital forensic process model and their legal perspective.	20
CO-4	Demonstrate various forensic tools to investigate the cybercrime and to identify the digital pieces of evidence	25
CO-5	Analyze the digital evidence used to commit cyber offences.	20

List of Open learning website:

List of Open-Source Software:

- Kali Linux
- Wireshark
- Recuva
- Last Activity tool
- AFLogical
- Whatsapp Extractor
- Free Hex Editor
- COFEE Tool
- Magnet RAM Capture
- RAM Capture
- NFI Defragger
- Toolsley
- Volatility

List of Experiments:

Sr. No.	Practical
1	To study detail working of boot process the operating system (Windows, Linux).
2	To study a case for digital evidence collection, retrieval, and presentation of cybercrime incidence.
3	To track the details of the computer in past using Last Activity view tool.
4	To perform data recovery of deleted files using Recuva in Windows.
5	To perform password cracking using any password cracking tool.
6	To perform detail inspection of different file formats using Hex editor.
7	To perform data extraction from android phone using AFLogical tool.
8	To perform forensics on WhatsApp using WhatsApp Extractor
9	To perform OS Backdoor using set toolkit
10	To perform Email Spoofing using SMTP servers