BCA-5-03T-EC-B2: Digital Forensics

Total Marks: 100
External Marks: 70
Internal Marks: 30
Credits: 4
Pass Percentage:40%

INSTRUCTIONS FOR THE PAPER SETTER/EXAMINER

1. The syllabus prescribed should be strictly adhered to.
2. The question paper will consist of three sections: A, B, and C. Sections A and B will have four questions from the respective sections of the syllabus and will carry 10 marks each. The candidates will attempt two questions from each section.
3. Section C will have fifteen short answer questions covering the entire syllabus. Each question will carry 3 marks. Candidates will attempt any ten questions from this section.
4. The examiner shall give a clear instruction to the candidates to attempt questions only at one place and only once. Second or subsequent attempts, unless the earlier ones have been crossed out, shall not be evaluated.
5. The duration of each paper will be three hours.

INSTRUCTIONS FOR THE CANDIDATES

Candidates are required to attempt any two questions each from the sections A and B of the question paper and any ten short questions from Section C. They have to attempt questions only at one place and only once. Second or subsequent attempts, unless the earlier ones have been crossed out, shall not be evaluated.

Course Name: Digital Forensics **Course Code: BCA-5-03T-EC-B2**	
Course Outcomes (COs) After the completion of this course, the students will be able to:	
CO 1	Understand the principles and concepts of digital forensics.
CO 2	Understand various types of cyber crimes
CO 3	Analyze computer architectures, file systems, and operating systems relevant to digital forensics investigations.
CO 4	Understand the legal and ethical considerations associated with digital forensics, including the admissibility of digital evidence in court.
CO 5	Utilize popular forensic tools and software for digital investigations.

Detailed Contents:

Module No.	Module Name	Module Contents
Section-A		
Module I	**Introduction to Digital Forensics and Cyber Crime**	• Introduction to digital forensics, definition and scope of digital forensics • Different Branches of Digital Forensics • Importance and applications of digital forensics in law enforcement and cybersecurity. • Definition and types of cybercrimes • Electronic evidence and handling, electronic media, collection, searching and storage of electronic media, • Introduction to internet crimes • Hacking and cracking, credit card and ATM frauds, web technology, cryptography, emerging digital crimes and modules
Module II	**Legal aspects of Digital Forensics**	• Understanding of legal aspects and their impact on digital forensics, Electronics discovery • Overview of legal and ethical issues in digital forensics. • Types of digital evidence (e.g., documents, emails, logs). • Collection, preservation, and documentation of digital evidence. • Preparing forensic reports. • Providing expert testimony in court. • Admissibility of digital evidence in court.
Section-B		
Module III	**Forensic Tools**	• Introduction to Forensic Tools • Usage of Slack space • Tools for Disk Imaging, Data Recovery, Vulnerability • Assessment Tools, Encase and FTK tools • Anti-Forensics and probable counters • Retrieving information
Module VI	**Processing of Electronic Evidence**	• Process of computer forensics and digital investigations • Processing of digital evidence, digital images, damaged SIM and data recovery, multimedia evidence • Retrieving deleted data: desktops, laptops and mobiles

		• Retrieving data from slack space, renamed file, ghosting, compressed files • Techniques for analysing and extracting information from computer memory • Forensic analysis of smartphones and tablets.

Books

1. C. Altheide & H. Carvey, “Digital Forensics with Open Source Tools”, Syngress
2. John Sammons “The Basics of Digital Forensics”, Syngress
3. Brain Carrier “File System Forensic Analysis”, Addison-Wesley
4. Harlan Carvey “Advanced Digital Forensic Analysis of the Windows Registry”, Syngress
5. Diane Barrett “Virtualization and Forensics - A Digital Forensic Investigator’s Guide to Virtual Environments”, Syngress
6. B. Nelson, A. Phillips, and C. Steuart “Guide to Computer Forensics and Investigations”, Cengage