

## DCS-2-01T: Digital Forensics

Total Marks: 100  
External Marks: 70  
Internal Marks: 30  
Credits: 6  
Pass Percentage:40%

<b>Course Name: Digital Forensics</b>	
<b>Course Code: DCS-2-01T</b>	
<b>Course Outcomes (COs)</b>	
After the completion of this course, the students will be able to:	
<b>CO 1</b>	Understand the principles and concepts of digital forensics.
<b>CO 2</b>	Understand various types of cyber crimes
<b>CO 3</b>	Analyze computer architectures, file systems, and operating systems relevant to digital forensics investigations.
<b>CO 4</b>	Understand the legal and ethical considerations associated with digital forensics, including the admissibility of digital evidence in court.
<b>CO 5</b>	Utilize popular forensic tools and software for digital investigations.

### Detailed Contents:

<b>Module No.</b>	<b>Module Name</b>	<b>Module Contents</b>
<b>Module I</b>	<b>Introduction to Digital Forensics</b>	<ul style="list-style-type: none"><li>• Introduction to digital forensics, definition and scope of digital forensics</li><li>• Different Branches of Digital Forensics</li><li>• Importance and applications of digital forensics in law enforcement and cybersecurity.</li></ul>
<b>Module II</b>	<b>Cyber Crime and Computer Crime</b>	<ul style="list-style-type: none"><li>• Definition and types of cybercrimes</li><li>• Electronic evidence and handling, electronic media, collection, searching and storage of electronic media,</li><li>• Introduction to internet crimes</li><li>• Hacking and cracking, credit card and ATM frauds, web technology, cryptography, emerging digital crimes and modules</li></ul>
<b>Module III</b>	<b>Computer Fundamentals for Digital Forensics</b>	<ul style="list-style-type: none"><li>• Basic Computer Organization</li><li>• Analysis of File systems and Data Structures</li><li>• Memory organization concept</li><li>• Data storage concepts</li><li>• Basics of operating systems and their role in digital forensics.</li><li>• Investigating network-based attacks.</li><li>• Analysing network traffic and logs.</li><li>• Understanding volatile memory.</li><li>• Windows Systems and Artifacts</li><li>• Linux Systems and Artifacts</li></ul>

<b>Module IV</b>	<b>Legal aspects of Digital Forensics</b>	<ul style="list-style-type: none"> <li>• Understanding of legal aspects and their impact on digital forensics, Electronics discovery</li> <li>• Overview of legal and ethical issues in digital forensics.</li> <li>• Types of digital evidence (e.g., documents, emails, logs).</li> <li>• Collection, preservation, and documentation of digital evidence.</li> <li>• Preparing forensic reports.</li> <li>• Providing expert testimony in court.</li> <li>• Admissibility of digital evidence in court.</li> </ul>
<b>Module V</b>	<b>Forensic Tools</b>	<ul style="list-style-type: none"> <li>• Introduction to Forensic Tools</li> <li>• Usage of Slack space</li> <li>• Tools for Disk Imaging, Data Recovery, Vulnerability</li> <li>• Assessment Tools, Encase and FTK tools</li> <li>• Anti-Forensics and probable counters</li> <li>• Retrieving information</li> </ul>
<b>Module VI</b>	<b>Processing of Electronic Evidence</b>	<ul style="list-style-type: none"> <li>• Process of computer forensics and digital investigations</li> <li>• Processing of digital evidence, digital images, damaged SIM and data recovery, multimedia evidence</li> <li>• Retrieving deleted data: desktops, laptops and mobiles</li> <li>• Retrieving data from slack space, renamed file, ghosting, compressed files</li> <li>• Techniques for analysing and extracting information from computer memory</li> <li>• Forensic analysis of smartphones and tablets.</li> </ul>

## Books

<ol style="list-style-type: none"> <li>1. C. Altheide &amp; H. Carvey, "Digital Forensics with Open Source Tools", Syngress</li> <li>2. John Sammons "The Basics of Digital Forensics", Syngress</li> <li>3. Brain Carrier "File System Forensic Analysis", Addison-Wesley</li> <li>4. Harlan Carvey "Advanced Digital Forensic Analysis of the Windows Registry", Syngress</li> <li>5. Diane Barrett "Virtualization and Forensics - A Digital Forensic Investigator's Guide to Virtual Environments", Syngress</li> <li>6. B. Nelson, A. Phillips, and C. Steuart "Guide to Computer Forensics and Investigations", Cengage</li> </ol>
--