Course Code	18CSE382T	Course Name	FORENSICS AND INCIDENT RESPONSE	Course Category	E	Professional Elective	L	T	P	C
							3	0	0	3

Pre-requisite Courses	Nil	Co-requisite Courses	Nil	Progressive Courses	Nil
Course Offering Department	Computer Science and Engineering	Data Book / Codes/Standards	Nil		

Course Learning Rationale (CLR):	*The purpose of learning this course is to:*
CLR-1 :	*Gain knowledge on the basics of procedures for identification, preservation of electronic evidence*
CLR-2 :	*Understand the purpose and usage of various forensic tools*
CLR-3 :	*Gain knowledge on how scientific evidence collection/extraction during investigation*
CLR-4 :	*Acquire knowledge on file systems and its innerworking*
CLR-5 :	*Understand the windows and linux investigation procedures*
CLR-6 :	*Introduce the report writingguidelines and principles*

Course Learning Outcomes (CLO):	*At the end of this course, learners will be able to:*	Learning			Program Learning Outcomes (PLO)														
		1	2	3	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15
		Level of Thinking (Bloom)	Expected Proficiency (%)	Expected Attainment (%)	Engineering Knowledge	Problem Analysis	Design & Development	Analysis, Design, Research	Modern Tool Usage	Society & Culture	Environment & Sustainability	Ethics	Individual & Team Work	Communication	Project Mgt. & Finance	Life Long Learning	PSO - 1	PSO - 2	PSO – 3
CLO-1 :	*Acquire the knowledge on basics of procedures for identification, preservation of electronic evidence*	*2*	*80*	*85*	*H*	-	-	-	-	-	-	-	-	-	-	-	-	-	-
CLO-2 :	*Acquire the ability to identify the purpose and usage of various forensic tools*	*2*	*75*	*80*	*H*	*H*	-	-	*H*	-	-	-	-	-	-	-	-	-	-
CLO-3 :	*Understand how scientific evidence collection/extraction during investigation*	*2*	*85*	*80*	*H*	-	-	-	-	-	-	-	-	-	-	-	-	-	-
CLO-4 :	*Appreciate the concepts of file systems and its importance in forensic science.*	*2*	*80*	*75*	*H*	-	-	-	-	-	-	-	-	-	-	-	-	-	-
CLO-5 :	*Apply the knowledge of windows and Linux investigation procedures*	*2*	*75*	*85*	*H*	-	-	*H*	-	-	-	-	-	-	-	-	-	-	-
CLO-6 :	*Acquire the knowledge on forensic report writing guidelines and principles*	*2*	*80*	*85*	*H*	-	-	-	-	*H*	-	-	-	-	-	-	-	-	-

Duration (hour)		9	9	9	9	9
S-1	SLO-1	*Introduction to Incident*	*Introduction to ACPO Principles*	*Introduction to File System Analysis*	*Introduction to Investigating Systems*	*Investigating Hacker Tools*
	SLO-2	*Goals of Incident Response*	*ACPO Principles of Computer Based Evidence*	*What is a File System?*	*Investigating Windows Systems*	*What are the goals of tool analysis?*
S-2	SLO-1	*Introduction to Incident Response Methodology (IRM)*	*Introduction to computer Storage Formats*	*Five Data Categories*	*Where Evidence resides on Windows Systems*	*How are files compiled?*
	SLO-2	*Steps in Incident Response Methodology*	*Understanding Storage Formats for Digital Evidence*	*FAT Concepts*	*Conducting a Windows Investigation I*	*Static Analysis of Hacker Tools I*
S-3	SLO-1	*IRM: Pre-incident preparation*	*Forensic Duplication*	*FAT Analysis*	*Conducting a Windows Investigation II*	*Static Analysis of Hacker Tools II*
	SLO-2	*IRM: Detection of incidents*	*Forensic Duplication tools*	*FAT - The Big Picture*	*File Auditing*	*Dynamic Analysis of Hacker Tools I*
S-4	SLO-1	*IRM: Initial Response*	*Forensic Duplicate creation of HDD*	*Introduction to NTFS*	*Theft of Information*	*Dynamic Analysis of Hacker Tools II*
	SLO-2	*IRM: Formulate a Response Strategy*	*Qualified Forensic Duplicate creation*	*Files in NTFS*	*Handling the departing employee*	*Evaluating Computer Forensics Tools*
S-5	SLO-1	*IRM: Investigate the Incident*	*Restored Image*	*MFT Concepts*	*Investigating Unix Systems*	*Types of Forensic Tools*
	SLO-2	*IRM: Reporting*	*Mirror Image*	*MFT Attribute Concepts*	*Overview of steps - Unix Investigation*	*Tasks performed by Forensic Tools*
S-6	SLO-1	*Creating response toolkit - Windows*	*Forensic Duplication Tool Requirements*	*Other MFT Attribute Concepts*	*Reviewing pertinent logs*	*Tool comparisons*
	SLO-2	*Volatile Data Collection - Windows*	*Creating a Forensic Duplicate of a Hard Drive*	*Indexes in NTFS*	*Performing keyword searches*	*Computer Forensics Software Tools*
S-7	SLO-1	*In-depth data collection - Windows*	*Evidence Handling*	*NTFS Analysis - File System Category*	*Reviewing relevant files*	*Computer Forensics Hardware Tools*
	SLO-2	*Storing collected data - Windows*	*Types of Evidence*	*NTFS Analysis - Content Category*	*Identifying unauthorized user accounts/groups*	*Validating and Testing Computer Forensics Software*
S-8	SLO-1	*Creating response toolkit - Unix*	*Challenges in Evidence Handling*	*NTFS Analysis - Metadata Category*	*Identifying rogue processes*	*Introduction to Forensic Report Writing*
	SLO-2	*Volatile Data Collection - Unix*	*Overview of Evidence Handling Procedure.*	*NTFS Analysis - File Name Category*	*Checking for unauthorized access points*	*Understanding the Importance of Reports*
S-9	SLO-1	*In-depth data collection - Unix*	*Evidence Handling Procedure*	*NTFS Analysis - Application Category*	*Analyzing trust relationships*	*Guidelines for Writing Reports*
	SLO-2	*Storing collected data - Unix*	*Evidence Handling reports*	*NTFS - The Big Picture*	*Detecting loadable kernel modules*	*A Template for Computer Forensics Reports*

Learning Resources	1. *KevinMandia,ChrisProsise,"IncidentResponseandcomputerforensics",TataMcGrawHill,2006.* 2. *Bill Nelson,Amelia Philips and Christopher Steuart, "Guide to computer forensics and investigations", coursetechnology,CengageLearning;4thedition,ISBN:1-435-49883-6,2009.*	3. *EoghanCasey,"HandbookComputerCrimeInvestigation'sForensicToolsandTechnology",Academic Press, 1st Edition,2001.* 4. *Brian Carrier, "File System Forensic Analysis", Addison-Wesley Professional; 1st edition 2005, ISBN-13: 978-0321268174*

Learning Assessment											
	Bloom's Level of Thinking	Continuous Learning Assessment (50%								Final Examination (50% weightage)	
		CLA – 1 (10%)		CLA – 2 (15%)		CLA – 3 (15%)		CLA – 4 (10%)#			
		Theory	Practice	Theory	Practice	Theory	Practice	Theory	Practice	Theory	Practice
Level 1	Remember	*40 %*	-	*30 %*	-	*30 %*	-	*30 %*	-	*30%*	-
	Understand										
Level 2	Apply	*40 %*	-	*40 %*	-	*40 %*	-	*40 %*	-	*40%*	-
	Analyze										
Level 3	Evaluate	*20 %*	-	*30 %*	-	*30 %*	-	*30 %*	-	*30%*	-
	Create										
	Total	100 %		100 %		100 %		100 %		100 %	

CLA – 4 can be from any combination of these: Assignments, Seminars, Tech Talks, Mini-Projects, Case-Studies, Self-Study, MOOCs, Certifications, Conf. Paper etc.,

Course Designers		
Experts from Industry	Experts from Higher Technical Institutions	Internal Experts
1. Mr.Balan C, Scientist F, CDAC, cbalan@cdac.in	*1.*	*1. Mr. A.R. Nagoor Meeran, SRMIST*
2.	*2.*	*2. Dr. C.N.S.Vinoth Kumar, SRMIST*