School:		**School of Engineering and technology**	
Department		**Department of Computer Science and Engineering**	
Program:		**B.Tech**	
Branch:		**Computer Science & Engineering with Specialization in Cyber Security and Forensics**	
1	Course Code	CSCR2201	
2	Course Title	**Digital Forensics**	
3	Credits	3	
4	Contact Hours (L-T-P)	3-0-0	
	Course Status	CORE	
5	Course Objective	Provide the students with practice on applying digital forensics techniques and enhance their skills regarding practical applications of digital forensics.	
6	Course Outcomes	On successful completion of this module students will be able to **CO1:**Demonstrate the principles of Digital Forensics and how resultant evidence can be applied within legal cases. **CO2:**Illustrate their competence in recovering files, network forensics, password cracking **CO3:**Evaluate the effectiveness of available digital forensics tools and use them in a way that optimizes the efficiency and quality of digital forensics investigations. CO4: apply a solid foundational grounding in computer networks, operating systems, file systems, hardware, and mobile devices to digital investigations and to the protection of computer network resources from unauthorized activity CO5: access and critically evaluate relevant technical and legal information and emerging industry trends CO6:Adapt effectively the results of a computer, network, and/or data forensic analysis verbally, in writing, and in presentations to both technical and lay audiences.	
7	Course Description	This course introduces students to basics of Digital Forensics. Make them apply appropriate skills and knowledge in solving computer forensics problems.	
8	Outline syllabus		CO Mapping
	Unit 1	**INTRODUCTION TO COMPUTER FORENSICS**	
	A	History of Forensics – Computer Forensic Flaws and Risks	CO1
	B	Rules of Computer Forensics – Legal issues – Digital Forensic Principles	CO1, CO2
	C	Digital Environments – Digital Forensic Methodologies	CO1, CO2,CO4
	Unit 2	**AN OVERVIEW OF DIGITAL FORENSICS INVESTIGATION**	
	A	Live forensics and investigation –digital evidence	CO1, CO2
	B	seizure methodology factors limiting the whole sale seizure of hardware- Demystifying computer/ cyber crime	CO1, CO2

	C	explosion of networking – explosion of wireless networks – interpersonal communication	CO1, CO2,CO5,CO6
	Unit 3	**DATA FORENSICS**	
	A	Recovering deleted files and deleted partitions – deleted file recovery tools –	CO1,CO2,CO3
	B	deleted partitioned recovery tools – data acquisition and duplication	CO1,CO2,CO3
	C	data acquisition tools – hardware tools – backing up and duplicating data.	CO1,CO2,CO3
	Unit 4	**ROUTER FORENSICS AND NETWORK FORENSICS**	
	A	overview of Routers – Hacking Routers – Investigating Routers	CO2,CO3,CO4
	B	Investigating Wireless Attacks – Basics of wireless - Wireless Penetration Testing	CO3,CO4
	C	Direct Connections to Wireless Access Point – Wireless Connect to a Wireless Access Point.	CO2, CO4,CO5
	Unit 5	**E-MAIL FORENSICS AND STEGANOGRAPHY**	
	A	Forensics Acquisition – Processing Local mail archives –	CO2,CO5,
	B	Processing server level archives – classification of steganography	CO3,CO5,CO6
	C	categories of steganography in Forensics – Types of password cracking.	CO4,CO5,CO6
	Mode of examination	Theory	
	Weightage Distribution	CA / CA / CA	
		30% / 30% / 30%	
	Text book/s*	• Anthony Reyes, Jack Wiles, "Cybercrime and Digital Forenscis", Syngress Publishers, Elsevier 2007. • John Sammons, "The Basics of Digital Forensics", Elsevier 2012	
	Other References	• Linda Volonins, Reynalds Anzaldua, "Computer Forensics for dummies", Wiley Publishing 2008.	

CO and PO Mapping

S. No.	Course Outcome	Program Outcomes (PO) & Program Specific Outcomes (PSO)
1.	**CO1:** Demonstrate the principles of Digital Forensics and how resultant evidence can be applied within legal cases.	PO1,PO2, PO5, PO8,PO12,PSO3
2.	**CO2:** Illustrate their competence in recovering files, network forensics, password cracking	PO1, PO2, PO3, PSO3
3.	**CO3:** Evaluate the effectiveness of available digital forensics tools and use them in a way that optimizes the efficiency and quality of digital forensics investigations.	PO1, PO2, PO3, PO5, PO9, PO12, PSO1
4.	CO4: apply a solid foundational grounding in computer networks, operating systems, file	PO1, PO2, PO4, PO5, PO6, PO8, PSO2

	systems, hardware, and mobile devices to digital investigations and to the protection of computer network resources from unauthorized activity	
5.	CO5: access and critically evaluate relevant technical and legal information and emerging industry trends	PO1, PO2, PO3,PO8,PO9,PSO2,
6.	CO6:Adapt effectively the results of a computer, network, and/or data forensic analysis verbally, in writing, and in presentations to both technical and lay audiences.	PO1, PO2, PO4, PO5, PO6,PO7,PO10,PO11,PSO1

PO and PSO mapping with level of strength for Course Name Digital Forensics (Course Code CSC201)

Course Code_ Course Name	CO's	PO 1	PO 2	PO 3	PO 4	PO 5	PO 6	PO 7	PO 8	PO 9	PO 10	PO 11	PO 12	PSO 1	PSO 2	PSO3
Digital Forensics (CSC201)	CO1	3	3	-	-	2	-	-	3	-	-	-	3	-	-	3
	CO2	3	3	2	-	-	-	-	-	-	-	-	-	-	-	3
	CO3	3	3	2	-	2	-	-	-	2	-	-	2	3	-	-
	CO4	3	3	-	3	2	3	-	2	-	-	-	-	-	3	-
	CO5	3	2	3	-	-	-	-	3	3	-	-	-	-	3	-
	CO6	3	3	-	3	3	3	3	-	-	3	3	-	3	-	-

Average of non-zeros entry in following table (should be auto calculated).

Course Code	Course Name	PO 1	PO 2	PO 3	PO 4	PO 5	PO 6	PO 7	PO 8	PO 9	PO 10	PO 11	PO 12	PSO 1	PSO 2	PSO 3
CSC201	Digital Forensics	3	2.7	1.1	1	1.5	1	.5	1.3	.8	.5	.5	.8	1	1	1

Strength of Correlation

1. Addressed to***Slight (Low=1)******extent******2.*** Addressed to***Moderate (Medium=2)*** ***extent***
3. Addressed to***Substantial (High=3)*** ***extent***