SCHEME OF COURSE WORK

Course Details:

Course Title	**:DIGITAL FORENSICS**		
Course Code	**:13CS2106**	**L T P C**	**:4 0 0 3**
Program:	**: M.Tech.**		
Specialization:	**: Cyber Security**		
Semester	**:2nd Semester**		
Prerequisites	**: Secure Protocols,Image Processing.**		
Courses to which it is a prerequisite	**: LINUX.**		

Course Outcomes (COs):

1	Utilize a systematic approach to computer investigations.
2	Utilize various forensic tools to collect digital evidence.
3	Perform digital forensics analysis upon windows,MAC and LINUX operating systems.
4	Perform email investigations.
5	Analyze and carve image files both logical and physical.

Program Outcomes (POs):

A graduate of Cyber Security Specializationwill be able to

1	Understand what are the common threats faced today.
2	The foundational theory behind Cyber security
3	The basic principles and techniques when designing a secure system,
4	How to think adversarial, how today's attacks and defenses work in practice, how to assess threats for their significance, and how to gauge the protections and limitations provided by today's technology
5	The basic principles and techniques in ethical hacking and overcome various hackers
6	Learn various security methodologies to enhance the security of web.
7	Basic principles of cyber laws and security policies
8	Various scripting languages to develop programs for security mechanisms.
9	Various tools and methodologies to analyze the various cyber crimes
10	Secure protocols inner mechanisms and their practical implementation
11	Various Forensic technologies and methodologies for security measurements analyzation.
12	.Intrusion detection techniques and image model security aspects in Android application developments.

Course Outcome versus **Program Outcomes:**

COs	PO1	PO2	PO3	PO4	PO5	PO6	PO7	PO8	PO9	PO10	PO11	PO12
CO-1			S			S						
CO-2	M	M	S							S		M
CO-3			M							S		M
CO-4		S		S								
CO-5												S

S - Strongly correlated, *M* - *Moderately* correlated, *Blank* - *No correlation*

Assessment Methods:	Assignment / Quiz / Seminar / Case Study / Mid-Test / End Exam

Teaching-Learning and Evaluation

Week	TOPIC / CONTENTS	Course Outcomes	Sample questions	TEACHING-LEARNING STRATEGY	Assessment Method & Schedule
1	Introduction & evidential potential of digital devices- key developments,digital devices in society,technology and culture,comment,closed vs open systems,evaluating digital evidence potential.	CO-1	Differentiate between closed system vs. open system?	▫ Lecture ▫ Demonstration	Assignment (Week 3 - 4)
2	Device handling & examination principles : seizure issues, Networked devices, contamination,previewing,imaging,continuity and hashing,evidence locations	CO-2	How can we evaluate digital evidence potential?	▫ Lecture / Discussion ▫ Programs implentation	Mid-Test 1 (Week 9)
3	Device handling & examination principles: Device identification	CO-2	Explain various device handling and examination principles?	▫ Lecture ▫ Programs implementation	Seminar (Week 3 - 6)
4	A Development model of digital systems,knowing,unknowing ,audit & logs, data content ,data context, internet & mobile devices the ISO/OSI model, the interner protocol suite, mobile phone PDAs,GPS,other personal technology	CO-2	Explain about ISO/OSI model		
5	A sevenelement security model, DNS,internet applications.	CO-2	Explain the following i) Seven Element Security Model ii) DNS Internet Applications		
6	Introduction to computer forensics, computer forensics assistance to human resources/employment proceedings, computer forensics services,benefits of professional forensics methodology ,steps taken by computer forensics specialists,Case histories ,case studies	CO-3,CO-4	Define Computer Forensics? Explain forensic services?		
7	use of computer forensics in law enforcement,computer forensics in law enforcement	C0-4	Explain the uses of computer forensics in law enforcement?		
8	who can use computer forensics	CO-4	Computer forensic services		

	evidence?		can be used by whom? Explain the problems with computer forensic evidences?		
9	**Mid-Test 1**	CO-1,CO-2			
10	Types of military computer forensic technology ,types of law enforcement :computer forensic technology, hidden data and how to find it, protecting data from being compromised , internet tracing method 65	CO-3	List out the primary uses of intelligent forensic filters?	▫ Lecture ▫ Discussion	Mid-Test 2 (Week 18)
11	Types of business computer forensic technology .	CO-3	Explain the different types of business computer forensic technology?		Seminar (Week 10 - 15)
12	specialized forensics techniques	CO-3	Explain specialized forensics techniques.		
13	spyware and adware,encryption methods and vulnerabilities	CO-3	Explain the following (i) spyware and adware (ii) Encryption methods and vulnerabilities?		
14	Homeland security systems,occurances of cyber crime,cyber detectives, course content ,case histories.	CO-5	Explain about homeland security systems?		
15	fighting cyber crime with risk management techniques.	CO-5	List out the different techniques for fighting cyber crime with risk management?		
16	computer forensics investigative services.	CO-5	Explain various computer forensic investigative services?		
17	Forensic process improvement.		Briefly discuss about forensic process improvement		
18	**Mid-Test 2**				
19/20	**END EXAM**				