RK.UNIVERSITY

SYLLABUS

Course Title	Cyber Forensic (Elective - II)
Course Code	CP909
Course Credit	Lecture : 03
	Practical : 01
	Tutorial : 00
	Credit : 04

Course Learning Outcomes

At the end of the course, students will be able to:

1. **Understand** the ethics and legality of hacking.
2. **Understand** Computer forensic and **describe** important and role of forensic specialist.
3. **Identify** different computer forensic technology.
4. **Comparison** of different types of computer forensics systems.
5. **Analyzing** Evidence collection techniques.

Detailed Syllabus

Sr. No.	Name of chapter & Details	Hours Allotted
	Section – I	
1	**Introduction to Ethical Hacking, Ethics, and Legality** Ethical Hacking Terminology, Different Types of Hacking Technologies, Different Phases Involved in Ethical Hacking and Stages of Ethical Hacking: Passive and Active Reconnaissance, Scanning, Gaining Access, Maintaining Access, Covering Tracks, Hacktivism, Types of Hacker Classes, Skills Required to Become an Ethical Hacker, Vulnerability Research, Ways to Conduct Ethical Hacking, Creating a Security Evaluation Plan, Types of Ethical Hacks, Testing Types, Ethical Hacking Report.	**5**
2	**Computer forensics fundamentals** Introduction to computer forensics, use of computer forensics in law enforcement, computer forensics assistance to human resources/employment proceedings, computer forensics services, benefits of professional forensics methodology, steps taken by computer forensics specialists	**8**

3	**Types of Computer Forensics Technology** Types of Military Computer Forensic Technology, Types of Law Enforcement: Computer Forensic Technology, Types of Business Computer Forensic Technology, Specialized Forensics Techniques, Hidden Data and How to Find It, Spyware and Adware, Encryption Methods and Vulnerabilities, Protecting Data from Being Compromised Internet Tracing Methods, Security and Wireless Technologies, Avoiding Pitfalls with Firewalls Biometric Security Systems	**8**
4	**Types of Computer Forensics Systems** Internet Security Systems, Intrusion Detection Systems, Firewall Security Systems, Storage Area Network Security Systems, Network Disaster Recovery Systems, Public Key Infrastructure Systems, Wireless Network Security Systems, Satellite Encryption Security Systems, Instant Messaging (IM) Security Systems, Net Privacy Systems, Identity Management Security Systems, Identity Theft, Biometric Security Systems	**7**
5	**Evidence Collection and Data Seizure** Why Collect Evidence, Collection Options Obstacles, Types of Evidence, The Rules of Evidence, Volatile Evidence, General Procedure, Collection and Archiving, Methods of Collection, Artifacts, Collection Steps, Controlling Contamination: The Chain of Custody, Reconstructing the Attack, The digital crime scene, Investigating Cybercrime, Duties Support Functions and Competencies.	**7**
6	**Identification of Data** Timekeeping, Forensic Identification and Analysis of Technical Surveillance Devices, Reconstructing Past Events: How to Become a Digital Detective, Useable File Formats, Unusable File Formats, Converting Files, Investigating Network Intrusions and Cyber Crime, Network Forensics and Investigating logs, Investigating network Traffic, Investigating Web attacks, Router Forensics. Cyber forensics tools and case studies.	**7**

Instructional Method and Pedagogy
• Lectures will be conducted with the aid of multi –media projector, blackboard. • The course includes tutorials, where students have an opportunity to practice the examples for the concepts being taught in lectures. • Assignments based on course content will be given to the students at the end of each unit/topic and will be evaluated at regular interval.

Reference Books
• John R. Vacca, Computer Forensics: Computer Crime Scene Investigation, 2nd Edition, Charles River Media, 2005 • Christo Paar, Jan Pelzl, Understanding Cryptography: A Textbook for Students and Practitioners, 2nd Edition, Springer, 2010 • Ali Jahangiri, Live Hacking: The Ultimate Guide to Hacking Techniques & Countermeasures for Ethical Hackers & IT Security Experts, Published by Dr. Ali Jahangiri, 2009 • Computer Forensics: Investigating Network Intrusions and Cyber Crime (EC-Council Press), Cengage Learning, 2010