GURU NANAK INSTITUTIONS TECHNICAL CAMPUS
(AUTONOMOUS)

B.Tech. (Minor in Cyber Security)

L	T	P	C
3	0	0	3

SECURITY INCIDENT & RESPONSE MANAGEMENT (18MD0CS14)

COURSE OBJECTIVE:
A brief explanation of the objective is to provide digital evidences which are obtained from digital media and to understand the objectives of computer forensics, first of all, people have to recognize the different roles computer plays in a certain crime

UNIT-I
Real-World Incidents: Factors Affecting Response, International Crime, Introduction to the Incident Response Process,
Preparing for Incident Response: Overview of Pre-incident Preparation, Identifying Risk, Preparing Individual Hosts , Preparing a Network , Establishing Appropriate Policies and Procedures, Creating a Response Toolkit , Establishing an Incident Response Team.

UNIT-II
Data Collection: Live Data Collection from Windows Systems, Creating a Response Toolkit, Storing Information Obtained during the Initial Response, Obtaining Volatile Data, Performing an In-Depth Live Response, Is Forensic Duplication Necessary?
Live Data Collection from Unix Systems: Creating a Response Toolkit , Storing Information Obtained During the Initial Response, Obtaining Volatile Data Prior to Forensic Duplication.

UNIT-III
Forensic Duplication: Forensic Duplicates As Admissible Evidence, Forensic Duplication Tool Requirements, Creating a Forensic Duplicate of a Hard Drive , Creating a Qualified Forensic Duplicate of a Hard Drive.
Collecting Network-based Evidence: What is Network-based Evidence, What Are the Goals of Network Monitoring? , Types of Network Monitoring, Setting Up a Network Monitoring System, Performing a Trap-and-Trace.

UNIT-IV
Evidence Handling: What Is Evidence?, The Challenges of Evidence Handling, Overview of Evidence-Handling Procedures, Evidence System Description, Digital Photos, Evidence Tags, Evidence Labels, Evidence Storage, The Evidence Log, Working Copies, Evidence Backups, Evidence Disposition, Evidence Custodian Audits.

UNIT-V
Data Analysis: Computer System Storage Fundamentals, Hard Drives and Interfaces, Preparation of Hard Drive Media, Introduction to File Systems and Storage Layers.
Data Analysis Techniques: Preparation for Forensic Analysis, Restoring a Forensic Duplicate, Preparing a Forensic Duplication for Analysis In Linux, Reviewing Image Files with Forensic Suites.

TEXT BOOKS:

1. Incident Response and computer forensics, Kevin Mandia, Chris Prosise, Tata McGrawHill, 2006.
2. Computer Forensics, Computer Crime Investigation, John R. Vacca, Firewall Media, New Delhi.
3. Computer Forensics and Investigations, Nelson, Phillips Enfinger, Steuart, cengage Learning.

REFERENCE BOOKS:

1. Real Digital Forensics, Keith J. Jones, Richard Bejtiich, Curtis W. Rose, Addison- Wesley Pearson Education.
2. Forensic Compiling, A Tractitioneris Guide by Tony Sammes and Brian Jenkinson, Springer International Edition.

COURSE OUTCOMES:

By the end of the course, students will be able to

CO 1: realize real world security incidents
CO 2: perform live data collection from unix systems / windows systems
CO 3: apply techniques for collecting network-based evidence
CO 4: describe evidence handling methods
CO 5: discuss data analysis techniques

Dr. J. Rajeshwar Chairman, BOS	Dr. B. Kranthi Kiran JNTUH Nominee	Dr. G. Narsimha Academic Council Nominee	Dr. Aruna Malapati Academic Council Nominee

Dr. Rishi Sayal Member, BOS	Dr. M.V. Narayana Member, BOS	Dr. Ch. Subbalakshmi Member, BOS	Dr. S. Madhu Member, BOS	Dr. E. Madhusudhana Reddy Member, BOS

Mr. V. Devasekhar Member, BOS	Mr. K. Chandra Shekar Member, BOS	Mr. Roop Kumar Raju Industry Representative	Mr. D. Saidulu Alumni