

SARDAR PATEL UNIVERSITY
Programme & Subject: Master of E-Business (M.Eb)
Semester: III
Syllabus with Effect from: June-2010

Paper Code: PM03EMEB05	Total Credit: 4
Title Of Paper: Forensic Investigation	

Unit	Description in Detail	Weightage (%)
I	Introduction: History of Forensics – Objectives of Computer Forensics – Computer facilitated Crimes and Reasons for Cyber Attacks – Computer Forensics: Rules, Procedures and Legal Issues – Types of Investigations – Role of the Investigator – Forensic Process	25%
II	Collecting Evidence: Systems, Disks, and Media: File Systems and Hard Disks, Digital Media Devices, Image File Forensics – Evidence collection from a single system – Remote Investigations and collections	25%
III	Windows and Linux Forensics: Windows and Linux Boot Process – Windows System Analysis – Linux System Analysis – Windows and Linux Forensics – Acquiring Data, Duplicating Data and Recovering Deleted Files	25%
IV	Advanced Forensics: Steganography and Application Password Crackers – Investigating Email Crimes – Tracking User Activity – Documenting the Investigation	25%

Basic Text & Reference Books:-

- The Official CHFI Guide: By Dave Kleiman, Syngress Publications
- Hacking Exposed: Computer Forensic – Secrets and Solutions By Aaron Philipp, David Cowen, Chris Davis
- Fundamental Computer Investigation Guide for Windows: Microsoft Corporation

