

Course No.	Title of the Course	Credits	Course Structure	Pre-Requisite
ITIT E 602	Digital Forensics	4	3L-0T-2P	Number Theory and Cryptography
COURSE OUTCOMES:				
CO1: To understand the fundamentals of digital forensics and different kinds of cyber-crimes.				
CO2: To apply different types of data acquisition tools				
CO3: To analyze the digital investigation scene				
CO4: To learn about the digital forensics software and hardware tools				
CO5: To understand the virtual machine and network forensics				
Unit No.	Topics			
Unit 1	Introduction: Digital Forensics Fundamentals, Computer Crimes, Understanding Digital Investigations, Procedures for Private-Sector High-Tech Investigations, Understanding Data Recovery Workstation and Software, Conducting an Investigation, Investigator’s Office and Laboratory			
Unit 2	Data Acquisition: Understanding Storage Formats for Digital Evidence, Determining the Best Acquisition Method, Acquisition tools, Validating Data Acquisitions, Performing RAID Data Acquisitions, Remote Network Acquisition Tools, Other Forensics Acquisition Tools			
Unit 3	Processing Crimes and Incident Scenes: Identifying Digital Evidence, Collecting Evidence in Private-Sector Incident Scenes, Processing Law Enforcement Crime Scenes, Preparing for a Search, Securing a Digital Incident or Crime Scene, Seizing Digital Evidence at the Scene, Storing Digital Evidence, Obtaining Digital hash, Reviewing case			
Unit 4	Current Digital Forensics Tools: Digital Forensics Software Tools, Digital Forensics Hardware Tools, Validating and Testing Forensic Software, Digital Forensics Examination Protocol, Digital Forensics Analysis and Validation,			
Unit 5	Virtual Machine and Network Forensics Overview of Virtual Machine Forensics, Live Acquisitions, Network Forensics Overview, Email and Social Media Investigations, Investigating Email Crimes and Violations, Understanding E-Mail Servers, Specialized E-Mail Forensics Tools, Social Media Forensics on Mobile Devices, Forensics Tools for Social Media Investigations			
Suggested Readings:				
1. Warren G. Kruse II and Jay G. Heiser, “Computer Forensics: Incident Response Essentials”, Addison Wesley, 2002.				

2. Nelson, B, Phillips, A, Enfinger, F, Stuart, C., "Guide to Computer Forensics and Investigations", 2nd edition, Thomson Course Technology, 2006, ISBN: 0-619-21706-5.
3. John R. Vacca, Computer Forensics, "Computer Crime Scene Investigation", 2ndEd, Charles River Media, 2005.
4. Anthony T. S. Ho and Shujun Li, "Handbook of Digital Forensics of Multimedia Data and Devices", IEEE Press, John Wiley & Sons, 2015.