CAP796:CYBER FORENSICS

Course Outcomes: Through this course students should be able to

CO1 :: understand the basic mechanisms of computer forensics

CO2 :: identify various mechanisms for carrying out computer forensic practices

CO3 :: employ various computer forensics tools to investigate cyber crime scene and prepare investigative reports

CO4 :: apply cyber investigations fundamentals for the protection of computer network resources from unauthorized activity

Unit I

Key Technical Concepts : bits, bytes and number system, file extensions and file segments, storage and memory concept, computing environment, data types, file systems

Introduction to Cyber Forensics : introduction, need and uses of cyber forensics, locard's exchange principle, organization of forensic notes, role of forensic examiner in judicial system, cyber forensics tools

Unit II

Collecting Evidence : cyber investigation, crime scenes and evidence, investigating methodology, documenting the scene, chain of custody, cloning, live system versus dead system, hashing

Challenges and concerns of Cyber Forensic : standards and controls, cloud forensics, SSDs

Unit III

Windows System Artifacts : deleted data, volatile information, non-volatile information, windows memory analysis, inside the windows registry, cache, cookies, history analysis in web browser, hibernation file, registry, print spooling, metadata, link files, restore points and shadow copy concept

Antiforensics : hiding data, passwords attacks, password cracking methods, default password database, steganography, data destruction

Unit IV

Investigative reports : introduction to investigative reports, report specifications, layout of an investigative report, guidelines for writing a report, importance of consistency, important aspects of a good report, dos and don’ts of forensic computer investigations

Legal : electronic discovery, searches with warrants, expert testimony, searches without warrants

Unit V

Internet and Email Forensics : internet overview, role of web browser in cyber forensics, email and cyber forensics, investigating e-mail crimes and violations, role of social networking sites in cyber forensics

Network Forensics : social engineering, network fundamentals, network security tools, network attacks, incident response, network evidences and investigations

Unit VI

Mobile Device Forensics : cellular networks, operating systems, cell phone evidence, cell phone forensics tools, global positioning system

Text Books:

1. COMPUTER FORENSICS AND CYBER CRIME: AN INTRODUCTIO by MARJIE T. BRITZ, Pearson Education India
2. INVESTIGATING THE CYBER BREACH: THE DIGITAL FORENSICS GUIDE FOR THE NETWORK ENGINEER by JOSEPH MUNIZ AND AAMIR LAKHANI, Pearson Education India

References:

1. REAL DIGITAL FORENSICS: COMPUTER SECURITY AND INCIDENT RESPONSE by KEITH J. JONES, ADDISON-WESLEY