CSC303:DIGITAL FORENSICS

L:2 T:0 P:2 Credits:3

Course Outcomes: Through this course students should be able to

CO1 :: understand the fundamentals of computer forensics, cybercrimes, and the process of investigating cybercrimes.

CO2 :: cognize the fundamentals of hard disks, file systems, and data acquisition for computer forensics investigations.

CO3 :: review windows forensics investigations to recover digital evidence effectively from volatile and non-volatile sources.

CO4 :: determine the process of Linux and Mac forensics including network forensics.

CO5 :: demonstrate he fundamentals of web application, dark web, and cloud forensics to identify and investigate cybercrimes.

CO6 :: examine mail crimes and mobile forensics fundamentals.

Unit I

Computer forensics in today's world : Understand the fundamentals of computer forensics, Understand cyber crimes and their investigation procedures, Understand digital evidence, Understand forensic readiness, Incident response and the role of SOC (security operations center) in computer forensics, Identify the roles and responsibilities of a forensic investigator, Understand the challenges faced in investigating cyber crimes, Understand legal compliance in computer forensics

Computer forensics investigation process : Understand the forensic investigation process and its importance, Understand the pre-investigation phase, Understand first response, Understand the investigation phase, Understand the post-investigation phase

Unit II

Understanding hard disks and file systems : Describe different types of disk drives and their characteristics, Explain the logical structure of a disk, Understand booting process of windows, Linux and Mac operating systems, Understand various file systems of Windows, Linux and Mac operating systems, Examine file system using Autopsy and The Sleuth Kit tools, Understand storage systems, Understand encoding standards and hex editors

Data acquisition and duplication : Understand data acquisition fundamentals, Understand data acquisition methodology, Prepare an image file for examination

Unit III

Defeating anti-forensics techniques : Understand anti-forensics techniques, Discuss data deletion and recycle bin forensics, Illustrate file carving techniques and ways to recover evidence from deleted, Explore password cracking/bypassing techniques, Detect steganography, Hidden data in file system structures, Trail obfuscation, Understand techniques of artifact wiping, Overwritten data/metadata detection and encryption, Detect program packers and footprint minimizing techniques, Understand anti-forensics countermeasures

Windows forensics : Collect volatile and non-volatile information, Perform Windows memory and registry analysis, Examine the cache, Cookie and history recorded in web browsers, Examine Windows files and metadata, Understand shellbags, LNK files and jump lists, Understand text-based logs and Windows event logs

Unit IV

Linux and Mac forensics : Understand volatile and non-volatile data in Linux, Analyze filesystem images using The Sleuth Kit, Demonstrate memory forensics using Volatility & PhotoRec, Understand Mac forensics

Network forensics : Understand network forensics, Logging fundamentals and network forensic readiness, Summarize event correlation concepts, Identify Indicators of Compromise (IoCs) from network logs, Investigate network traffic, Perform incident detection and examination with SIEM tools, Monitor and detect wireless network attacks

Unit V

Investigating web attacks : Understand web application forensics, Understand Internet Information Services (IIS) logs, Understand Apache web server logs, Understand the functionality of intrusion detection system (IDS), Understand the functionality of web application firewall (WAF), Investigate web attacks on windows-based servers, Detect and investigate various attacks on web applications

Unit V

Dark web forensics : Understand the dark web, Determine how to identify the traces of tor browser during investigation, Perform Tor browser forensics

Cloud forensics : Understand the basic cloud computing concepts, Understand cloud forensics, Understand the fundamentals of Amazon Web Services (AWS), Determine how to investigate security incidents in AWS, Understand the fundamentals of Microsoft Azure, Determine how to investigate security incidents in Azure, Understand forensic methodologies for containers and microservices

Unit VI

Investigating email crimes : Understand email basics, Understand email crime investigation and its steps, U.S. laws against email crime

Mobile forensics : Understand the importance of mobile device forensics, Illustrate architectural layers and boot processes of Android and iOS Devices, Explain the steps involved in mobile forensics process, Investigate cellular network data, Understand sim file system and its data acquisition method, Illustrate phone locks and discuss rooting of android and jailbreaking of iOS devices, Perform logical acquisition on Android and iOS devices, Perform physical acquisition on Android and iOS devices, Discuss mobile forensics challenges and prepare investigation report

List of Practicals / Experiments:

List of practicals / experiments

- Disk imaging and data acquisition: Learn how to create forensic images of hard drives and other storage media to preserve evidence
- File system analysis: Analyze file systems to identify deleted files, hidden data, and file metadata
- Metadata examination: Extract and analyze metadata associated with files, such as creation and modification dates, file sizes, and user information
- Keyword searching: Conduct searches for specific keywords or phrases across various digital artifacts, including files, emails, and web browsing history
- Email header analysis: Examine email headers to gather information about sender, recipient, IP addresses, timestamps, and email routing paths
- Network traffic analysis: Analyze network packets and logs to identify communication patterns, potential intrusion attempts, or unauthorized activities
- Registry analysis: Investigate Windows registry entries to identify user activities, installed software, and system configurations
- Internet history analysis: Analyze web browser history and cache files to reconstruct a user's online activities and visited websites
- Mobile device forensics: Extract and analyze data from smartphones and tablets, including call logs, messages, application data, and location information.
- Live system analysis: Conduct forensic analysis on a running system to identify active processes, network connections, and volatile data

References:

1. DIGITAL FORENSICS AND INCIDENT RESPONSE by GERARD JOHANSEN, PACKT PUBLISHING