|  |  |  |  |
| --- | --- | --- | --- |
| **Course Name:** | **Information Security (116U01L602)** | **Semester:** | **VI** |
| **Date of Performance:** | **23/ 04 / 2025** | **DIV/ Batch No:** | **A-3** |
| **Student Name:** | **Kashish Mamania** | **Roll No:** | **16010122104** |

|  |
| --- |
| **Title: Digital Forensic investigation using Encase forensic tool** |

|  |
| --- |
| **Objectives:** |
| **CO5** Interpret legal and ethical issues in security |

|  |
| --- |
| **Expected Outcome of Experiment:** |
| * Understanding the process and methodology for conducting a digital forensic investigation using EnCase Forensic Tool. * Familiarity with the key features of EnCase, such as data acquisition, analysis, and reporting. * Ability to use EnCase to gather and analyze evidence from digital devices. * Understanding of how to ensure the integrity and validity of digital evidence during an investigation. * Gaining practical experience in analyzing digital evidence for possible legal use. * Developing insights into the application of digital forensic principles in real-world investigations. |

|  |
| --- |
| **Books/ Journals/ Websites referred:** |
| <https://www.opentext.com/products/encase-forensic>  Technical articles, tips, and troubleshooting -  <https://forums.opentext.com/forums/support/categories/encase>  Creation of forensic image - <https://www.youtube.com/watch?v=qoOuhrvJgV8>  Process and analyse forensic image -  <https://www.youtube.com/watch?v=DxjBq4vPNA0>  Keyword Search - <https://www.youtube.com/watch?v=NduzWIvr4oI>  Access Windows Registry - <https://www.youtube.com/watch?v=be2EYmo_tiQ> |

|  |
| --- |
| **Pre Lab/ Prior Concepts:** |
| **Basic Computer Forensics:**   * Understanding of computer hardware and software. * Concepts of digital evidence and its importance in investigations. * The basics of file systems (FAT, NTFS, exFAT) and how they store and manage data.   **Digital Evidence Integrity:**   * Chain of custody procedures. * The concept of imaging, hashing, and ensuring data integrity during the forensic process.   **Data Acquisition Techniques:**   * Methods to acquire data from storage media (hard drives, USBs, network devices). * Write-blocking techniques to prevent altering data during the acquisition process.   **File Analysis and Recovery:**   * Concepts of file signatures and file carving. * Recovery of deleted files and hidden data. |

|  |
| --- |
| **New Concepts to be learned:** |
| **EnCase Tool Features:**   * Using EnCase to create forensic images of digital media. * Data analysis and investigation features of EnCase, including keyword searches, filtering, and timeline analysis. * Creating and managing cases in EnCase.   **Forensic Report Generation:**   * Creating and understanding detailed forensic reports using EnCase. * Generating evidence logs and preparing reports for legal proceedings.   **File System Forensics:**   * In-depth knowledge of how file systems operate and how to analyze them for digital evidence in EnCase. * Techniques for reconstructing deleted or hidden files using EnCase.   **Data Carving and Extraction:**   * Using EnCase to perform data carving for recovering fragmented or incomplete files. * Extraction of metadata, system logs, and artifacts useful in investigations.   **Handling Encrypted Data:**   * Using EnCase for investigating encrypted data and applying decryption methods when possible. |

|  |
| --- |
| **Abstract:** |
| Digital forensics plays a crucial role in investigating cybercrimes, data breaches, and incidents involving the misuse of digital devices. The EnCase Forensic Tool is one of the leading software applications used in digital forensics for evidence acquisition, analysis, and reporting. This experiment aims to demonstrate the process of using EnCase to conduct a digital forensic investigation. The primary objective is to acquire digital evidence, analyze it for relevant data, and generate a detailed forensic report. The experiment will also explore techniques for data recovery, file analysis, and ensuring evidence integrity throughout the investigation process. |

|  |
| --- |
| **Related Theory:** |
| **Digital Forensics Fundamentals:**   * Digital forensics refers to the process of collecting, preserving, analyzing, and presenting data in a manner that is legally acceptable in a court of law. * The investigation of digital evidence requires specialized tools, methodologies, and adherence to strict protocols to ensure the authenticity and integrity of the data.   **EnCase Tool Overview:**   * EnCase is a powerful tool used for forensic investigations and is known for its capabilities in acquiring, analyzing, and reporting digital evidence. * It supports various types of digital media and file systems, making it versatile in investigating computers, mobile devices, and networks.   **The Importance of Data Integrity:**   * In digital forensics, ensuring the integrity of data is paramount. Investigators must follow procedures such as hashing and write-blocking to avoid altering the original evidence during the acquisition and analysis stages.   **Digital Evidence Analysis:**   * The analysis phase involves searching for specific data related to an investigation, recovering deleted or hidden files, and piecing together evidence in a manner that helps reconstruct events.   **Legal Aspects of Digital Forensics:**   * Digital forensics investigations must comply with legal frameworks such as the Fourth Amendment (U.S.) and data protection laws to ensure that evidence is admissible in court. Evidence handling and documentation must adhere to legal standards for chain of custody and preservation. |

|  |
| --- |
| **Implementation Details:** |
|  |

|  |
| --- |
| **Conclusion:** |
| In this experiment we learned EnCase tool. |

|  |
| --- |
| **Post-Lab Questions:** |
| **1. How does EnCase handle evidence integrity? What role does hashing play in this?**  EnCase ensures evidence integrity by creating a cryptographic hash (commonly MD5 or SHA-1) of the evidence file when it is first added. This hash acts like a digital fingerprint of the file.  Any changes to the evidence (even a single bit) would result in a different hash, alerting the investigator to possible tampering.  EnCase recalculates and compares the hash at different stages (e.g., during import, export, or verification) to confirm authenticity and maintain a proper chain of custody.  In essence, hashing guarantees that the evidence remains unaltered throughout the investigation.  **2. What filters or search tools did you use to locate potentially relevant files?**    Keyword Search: Entered terms like "password", "confidential", "meeting" to find sensitive or relevant content.  File Extension Filter: Narrowed down results to specific types such as .jpg, .png, .docx, .pdf, .eml, and .pst.  Time Range Filter (if applicable): Used to analyze activity within a specific timeframe.  File Path/Metadata View: Helped explore locations like user documents, downloads, and email archives.  These tools made it easier to quickly isolate important files from large volumes of data.  **3. What is file signature analysis, and how did it help identify suspicious files?**  File signature analysis compares a file’s internal signature (magic number) with its extension to confirm it’s not disguised or corrupted.  For example, a file named photo.jpg should begin with the JPEG file header FFD8. If it starts with a ZIP header instead, it’s suspicious.  In my analysis, this feature:  Exposed files with mismatched extensions (e.g., a .jpg that was actually a .exe).  Highlighted corrupted files that could be attempts to hide or manipulate evidence.  It is essential for detecting file masquerading, a common method used to conceal malicious files.  **4. Why is it important to follow ethical guidelines during forensic analysis?**  Forensic investigators handle sensitive and potentially incriminating data, so adhering to ethical guidelines is crucial because:  It protects the rights and privacy of individuals involved.  It ensures evidence remains admissible in court — any misconduct could lead to evidence being dismissed.  It helps maintain professional integrity and trust.  Actions like fabricating, modifying, or accessing personal data without cause could result in legal consequences and reputational damage.  Following ethical protocols upholds the credibility and legality of the forensic investigation. |