MITE

Invent Solutions

DIGITAL FORENSICS

23ICOE321

(COURSE HANDBOOK)

Department of CSE (IoT & Cyber Security with Blockchain Technology)

COURSE FACULTY:

Mr. Aneesh Kumar A

1. GENERAL INFORMATION

Welcome to Digital Forensics

Digital Forensics is a specialized field of cyber security that focuses on the identification, collection, preservation, analysis, and presentation of digital evidence in a legally acceptable manner. With the rapid growth of computers, mobile devices, cloud platforms, and the internet, digital systems have become central to both everyday activities and criminal investigations.

This course introduces students to the fundamental principles, tools, and techniques used in digital forensic investigations. It covers forensic processes for operating systems, storage media, mobile devices, networks, and cloud environments. Students will learn how cybercrimes are investigated, how digital evidence is handled without alteration, and how forensic findings are documented for legal and organizational use.

The course also emphasizes legal and ethical considerations, chain of custody, forensic standards, and compliance with cyber laws. By the end of the course, learners will gain practical skills to analyze digital incidents, support law enforcement or corporate investigations.

1.1. Course Objectives

This course is designed to:

1. Provide insights about the basic principles, methodologies, and tools used in computer forensics to investigate digital crimes.
2. Impart the various data acquisition methods, understand storage formats, and utilize appropriate tools to collect and analyze digital evidence effectively.
3. Equip the ability to navigate through the legal frameworks, privacy concerns, and ethical issues surrounding computer forensics, ensuring adherence to laws and professional standards during investigations.
4. Improve the knowledge about the processing of digital evidence from the incident scenes.

1.2..Course Outcomes

CO1. Explain the foundational principles, investigation processes, and key challenges involved in digital forensics for computer-based investigations.

CO2. Describe the procedures for planning and conducting corporate digital investigations, including incident scene protection and the seizure of digital evidence.

CO3. Identify and explain various data recovery workstations, acquisition methods, and tools used for RAID systems and remote network data acquisition.

CO4. Explain methods for storing, validating, and preserving digital evidence, including the role of digital hashing in ensuring evidence integrity.

CO5. Explain the fundamentals, commonly used tools, and techno-legal challenges of handheld device forensics in the context of digital evidence investigation.

1.3. Set Text and Suggested Sources

All the below mentioned books are available in the 1st Floor Library.

Key Text Books:

1. Nina Godbole, Sunit Belapure," Cyber Security : Understanding Cyber Crimes, Computer Forensics and Legal Perspectives",Wiley,2011, ISBN: 978-81-265-2179-1
2. Nelson, B, Phillips, A, Enfinger, F, Stuart, C., "Guide to Computer Forensics and Investigations, 4e ., Cengage Learning, 2014, ISBN: 978-81-315-1946-2.

Reference Books:

1. Vacca, J, "Computer Forensics, Computer Crime Scene Investigation", 2nd Ed, Charles River Media, 2005, ISBN: 1-58450-389.

2. THE COURSE

2.1. Course Description

Digital Forensics			
Semester	**VI**	CIE Marks	**50**
Course Code	**23ICOE321**	SEE Marks	**50**
Teaching Hours/Week (L:T:P)	**3:0:0**	Exam Hrs	**3**
Total Hours	**42**	Credits	**3**

The Digital Forensics course designed to provide students with core principles, tools, and techniques of digital forensic investigations, covering forensic procedures for operating systems, storage media, mobile devices, networks, and cloud environments. The course will run for 14 weeks during Semester 6 and consists of 5 modules that cover essential topics in Digital Forensics. Each week includes 3 lectures, delivered by Mr. Aneesh Kumar A. These lectures focus on theoretical concepts, practical applications, and course-related activities. Spanning a total of 42 hours, this 3-credit course is assessed through Continuous Internal Evaluation (CIE) for 50 marks and a Semester-End Examination (SEE) for 50 marks in the form of 3-hour exam duration. This structure ensures a balanced and engaging learning experience for students.

2.2. Initiating Contact with Staff and Other Students

We encourage open communication and welcome your questions regarding the course. However, given the large number of students enrolled, we request that you use email, office-hour appointments, and other forms of correspondence thoughtfully. Before contacting the course team with administrative queries, please check whether your question has already been addressed in previous communications, the course handbook, or the course website. Additionally, we encourage you to engage with your peers for discussion and collaborative learning, as this will enhance your understanding of the course content and help foster a supportive academic community.

2.3. Resources

Resources go beyond just books—they include dynamic tools like digital libraries, e-learning platforms, and research databases. These modern learning environments offer anytime, anywhere access to academic materials, interactive courses, and cutting-edge research, empowering students to explore knowledge and excel in their fields.

Students can access a variety of resources through the college website. These include the VTU Consortium, e-learning platforms, and additional sources like open-access repositories, government portals (e.g., NPTEL, NDLI), and these digital tools provide access to e-books, research papers, video lectures, and interactive tutorials, offering flexible and comprehensive learning environments.

E-learning and digital library can be accessed via the college website https://mite.ac.in/ (Campus Life section > Library > VTU Consortium/e-learning platforms/additional sources).

2.4. Staff

Course Convenor: Mr. Aneesh Kumar A
Cabin: Ground floor, PG Block
Email: aneesh@mite.ac.in

2.5. Topics and Reading materials for each module

Module 1 *No. of Hours: 08*

- **Topic: Introduction to Digital Forensics**

  Historical Background of Cyberforensics, Digital Forensics Science, The Need for Computer Forensics, Cyberforensics and Digital evidence, Digital Forensics Lifecycle, Chain of custody concept, Approaching a Computer Forensics Investigation, Relevance of the OSI 7 Layer Model to Computer forensics, Challenges in Computer Forensics: Technical and Legal Challenges.

Module 2 *No. of Hours: 09*

- **Topic: Computing Investigations**

  Preparing a Computer Investigation: An Overview of a Computer Crime, An overview of a Company Policy Violation. Systematic Approaches: Assessing the case, Planning the Investigation, Securing the Evidence, Procedure for corporate High-Tech investigations, Interviews and Interrogations in High-Tech, Understanding Data Recovery Work Station and Software: Setting a workstation for Computer Forensics, Conducting an Investigation: Gathering the Evidence, Understanding Bit-Stream Copies, Acquiring an Image of Evidence Media and completing the Case.

Module 3 *No. of Hours: 08*

- **Topic: Data acquisition**

  Understanding storage formats and digital evidence: Raw format, Proprietary Formats, Advanced Forensic Format. Determining the Best Acquisition Method, Contingency Planning for Image Acquisitions, Using Acquisition Tools, Validating Data Acquisitions, Performing RAID Data Acquisitions, Remote network acquisition tools, Other forensics acquisitions tools.

Module 4 *No. of Hours: 08*

- **Topic: Processing Crimes and Incident scenes**
  Identifying Digital Evidence: Understanding Rules of Evidence, Collecting Evidence in Private-Sector Incidence Scenes, Processing Law Enforcement Crime Scenes, Preparing for a Search, Securing a Computer Incident or Crime Scene, Seizing Digital Evidence at the Scene, Storing Digital Evidence, Obtaining Digital Hash, Reviewing a Case.

Module 5 *No. of Hours: 09*

- **Topic: Forensics of Hand-Held Devices**
  Personality, Definition, factors influencing personality, Big Five personality traits, Myers-Briggs personality Indicator (MBTI), Personality tools and tests, Motivation: Definition, Process of motivation, Cycle of motivation, Types, theories – Maslow's Hierarchy of needs, four drive theory of motivation.

3. ASSESSMENT

The assessment for the Digital Forensics is divided into two components: Continuous Internal Evaluation (CIE) and Semester End Examination (SEE), each accounting for 50% of the total marks.

Continuous Internal Evaluation (CIE) comprises two internal tests, scheduled for 8th and 14th week, which together contribute 30% of the total marks. Additionally, students can earn 20% through the completion of two assignments (10 marks for each assignment).

Semester End Examination (SEE) constitutes the remaining 50% of the total marks. Key information regarding examination dates and related details can be accessed via the college website (Academics and Courses section > Calendar of Events > B.E-Even Sem.)