Designing a Linux Based Digital Forensics Course for Undergraduate Students

Dr. Lydia Ray

2025 CAE Community Symposium

Evolution of Digital Forensics

2025 CAE Community Symposium

1960-70

- Need to recover data from computers emerged for police and military

1980s

- The Computer Analysis and Response Team (CART) established by FBI.
- The he *Computer Fraud and Abuse Act* was passed.

1990s

- The International Organization on Computer Evidence (IOCE) was founded to develop digital forensics standards.
- The *Regional Computer Forensics Laboratory (RCFL) program* started by FBI

2000s

- The *Electronic Communications Privacy Act* was updated.
- The USA PATRIOT Act expanded surveillance and digital forensics capabilities.
- NIST developed guidelines for digital forensic tools.

2010s

- Mobile, cloud and social media forensics emerged.
- Ransomware and cybercrime surged.
- Digital forensics market expanded with increasing demands .

2020 onwards

- Blockchain forensics is introduced.
- IoT forensics is an emerging discipline.
- Gen AI tools bring assistance and new challenges in digital forensics.

Evolution of Digital Forensics Education

2025 CAE Community Symposium

- Informal and in-house training for law enforcement and IT people

- Standalone digital forensics courses within IT, cybersecurity, and criminal justice programs.
- Certification on forensic software
- NIST developed digital forensics education standards

- Bachelor's and master's programs in digital forensics
- Specialized courses on mobile, network and cloud forensics.

- More hands-on labs
- Virtual lab environment with eBooks
- Cyber range
- More research projects in higher education

2025 CAE Community Symposium

CSU Digital Forensics Timeline

2008

- Digital forensics course developed within BS in CS program
- Based on AccessData software

2016

- Cybersecurity track under BS in CS started
- Digital forensics course modified with EnCase knowledge

2018

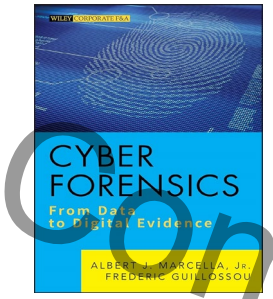
- Digital forensics course modified and expanded to include mobile forensics

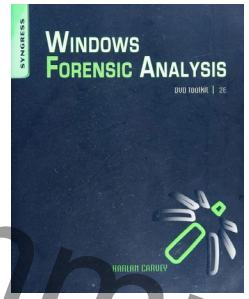
2021

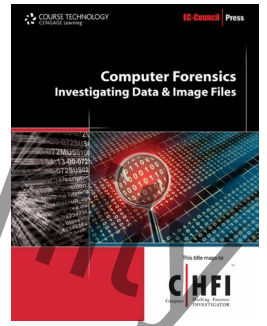
- eBook with virtual lab environment adopted

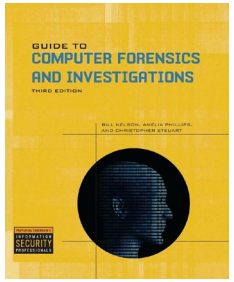
Textbooks and Labs Used in Digital Forensics Course

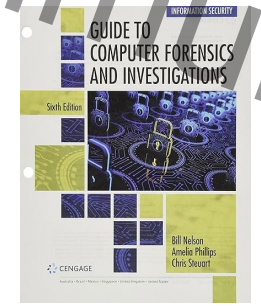
2025 CAE Community Symposium

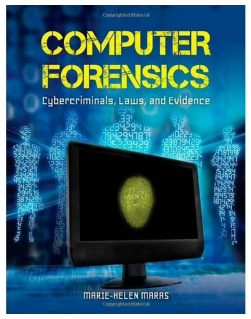


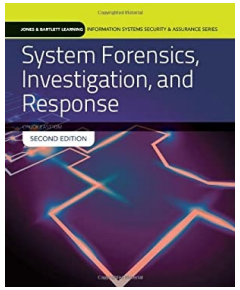


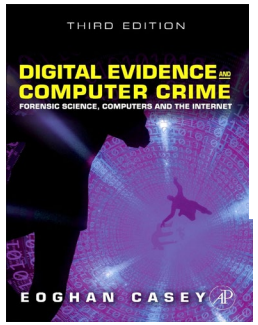












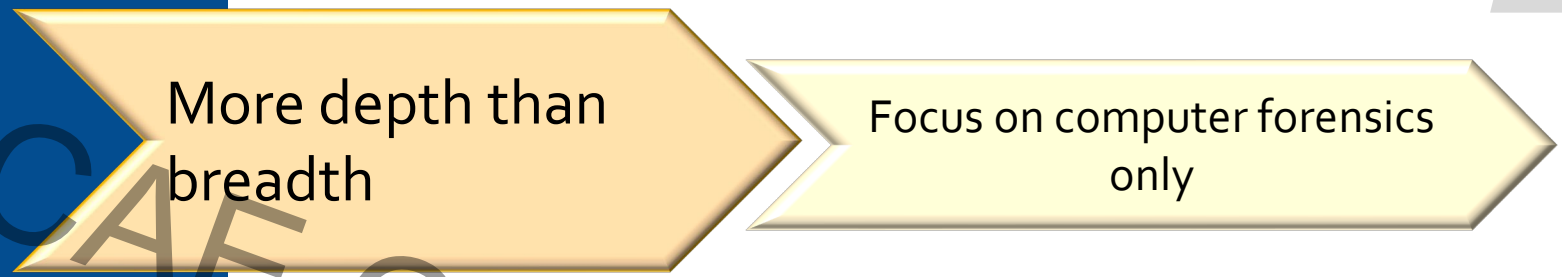
Small hands-on activities
No capstone case project

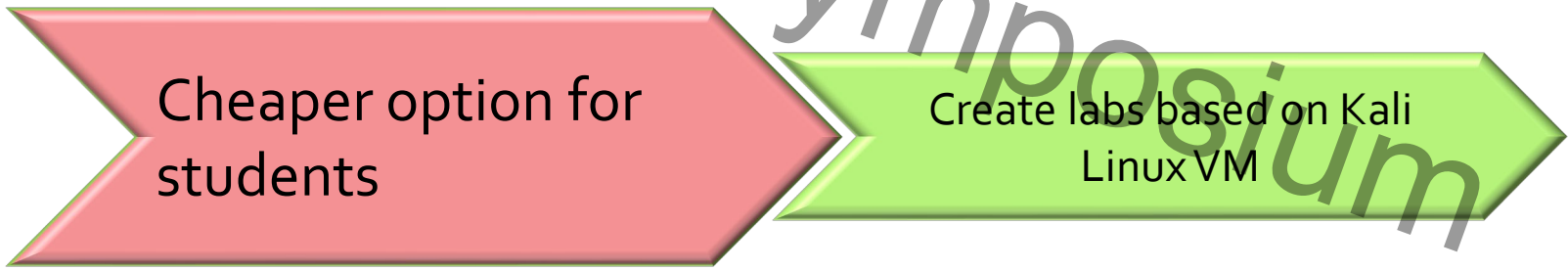
Hands-on activities for EnCase
No capstone case project

Netlab labs
Case project designed from a USB drive image from a divorce case

Mindtap labs
Case project from Digital Corpora

New Course Redesign Requirement





2025 CAE Community Symposium

CFCE Core Competencies

2025 CAE Community Symposium

- Pre-examination procedures
- Computer fundamentals
- Partition Schemes
- File Systems
- Windows Artifacts
- Data Recovery
- Presentation of Findings

Module 1: Overview of Digital Forensics Investigation

2025 CAE Community Symposium

Learning Outcome

After completing this lesson, students will be able to provide an overview of the digital forensic investigation process.

Assessment

Reading and class discussion on digital evidence recovery process in true crime cases.

Module 2: Fundamentals of Digital Data

2025 CAE Community Symposium

Learning Outcome

After completing this module, students will be able to:

- Describe the nature of digital data;
- Explain how different types of digital data is created;
- Identify raw digital data in hexadecimal format;
- Explain different measurements of digital data with examples

Assessment

Class discussions and activities to view the raw binary and hexadecimal forms of data contained in texts and multimedia files using an online hex viewer tool.

Module 3: Processing of Digital Evidence

2025 CAE Community Symposium

Learning Outcome

After completing this module, students will be able to:

- Describe the steps of digital investigation;
- Explain the importance of logging, chain of custody and data validation;
- Describe and implement data acquisition and validation techniques from a secondary storage media.

Lab

Set up a virtual machine with Kali Linux.

Module 4: Hardware Fundamentals

2025 CAE Community Symposium

Learning Outcome

After completing this module, students will be able to:

- Describe knowledge of which hardware components is essential for computer forensics investigation and why;
- Explain the functionalities of BIOS and UEFI;
- Explain the steps of booting an evidence computer using an external hard drive without changing any data on the evidence hard drive.
- Verify the system clock information.

Lab

A raw data and data integrity lab to create, modify, understand, and check the integrity of digital data using Linux.

Module 5: Traditional Hard Drive Geometry

2025 CAE Community Symposium

Learning Outcome

After completing this module, students will be able to:

- Describe the main components of a traditional hard drive;
- Describe CHS addressing and how it is used to store, access and retrieve data;
- Describe Logical Block Addressing scheme;
- Describe the Master Boot Record and its importance in computer forensics investigation.

Assessment

In-class activity on LBA and CHS addressing and their conversions.

Module 6: Solid State Drive Geometry

2025 CAE Community Symposium

Learning Outcome

After completing this lesson, students will be able to:

- Give a high-level description of how digital data is stored and accessed in a solid-state drive;
- Explain how SSD is fundamentally different from a traditional hard disk drive;
- Explain SSD's specific features relevant to digital forensics investigation and the challenges it brings to digital forensic investigation.

Lab

In this lab, students compare data recovery from two identical SSD drives with ExFAT formatting, one with TRIM enabled and the other with TRIM disable.

Module 7: Boot Process, MBR and GPT

2025 CAE Community Symposium

Learning Outcome

After completing this lesson, students will be able to:

- Give an overview of the boot process with an HDD and SSD in the context of digital forensics.
- Identify partition table in an MBR and extract partition information from partition table entries;
- Identify GPT and extract important information from GPT header and partition table entries.

Lab

In this lab, students extract important hard drive and partition information from a GPT.

Module 8: File System FAT

2025 CAE Community Symposium

Learning Outcome

After completing this lesson, students will be able to:

- Describe how FAT file system operates with directory and file allocation table;
- Recover file metadata and deleted files from a FAT file system.

Lab

In this lab, students recover deleted file along with its metadata from a bit-stream image of a USB drive formatted with FAT.

Module 9: File System NTFS

2025 CAE Community Symposium

Learning Outcome

After completing this lesson, students will be able to:

- Describe how NTFS stores and deletes files using the Master File Table (MFT);
- Extract existing and deleted file metadata from an MFT;
- Recover deleted file from an NTFS drive.

Labs

In one lab, students review an MFT with MFT viewer and identify various file attributes;

In another lab, students recover deleted file along with its metadata from a bit-stream image of a drive formatted with NTFS.

Module 10: File Systems of Linux and Mac

2025 CAE Community Symposium

Learning Outcome

After completing this lesson, students will be able to:

- Provide an overview of the basic file systems used by Linux and Mac;
- Identify Linux and Mac file systems from partition entries.

Labs

In this lab, students review the volume boot records of a Linux file system and a Mac file system.

Module 11: Data Recovery Techniques

2025 CAE Community Symposium

Learning Outcome

After completing this lesson, students will be able to:

- Extract various evidence using data recovery techniques such as signature analysis, password recovery, steganography file detection and extraction, decryption of an encrypted file etc. from a given bit-stream image.

Labs

In these labs, students recover various artifacts from the bit-stream image of carefully crafted hard drive using the techniques learnt in the module.

Module 12: Windows Registry Analysis

2025 CAE Community Symposium

Learning Outcome

After completing this lesson, students will be able to:

- Extract specific Windows registry files from a bit-stream image of an NTFS drive;
- Analyze the registry files to uncover user activity and account information, boot information, installed and uninstalled applications, network activity and evidence of malware from persistent mechanisms.

Lab

In this labs, students analyze various registry files extracted from a bit-stream image of a carefully crafted NTFS formatted drive to uncover various evidence.

Module 13: Email Header Analysis

2025 CAE Community Symposium

Learning Outcome

After completing this lesson, students will be able to:

- Analyze email headers to extract important metadata about the email's origin, routing, and potential signs of spoofing or phishing or scam.

Lab

In this labs, students analyze several different carefully crafted email headers with several spoofed header fields.

Module 14: Digital Forensics Report Writing

2025 CAE Community Symposium

Learning Outcome

After completing this lesson, students will be able to:

- Write a professional standard digital forensics report based on an investigation of a criminal case.

Final Capstone Project

In this final capstone project, students will solve a true crime case by analyzing bit-stream images of hard drives and USB drives to uncover various evidence using techniques learnt in the course. Students will write a professional forensics report and will also present the case in the class.

Our Work

- We built every lab from scratch;
- We are in the process of creating capstone projects with our own crime stories;
- We are in the process of combining all our teaching materials to publish an eBook.

Our labs: Digital Forensics Labs

2025 CAE Community Symposium

Questions?

This Photo by Unknown Author is licensed under CC BY

2025 CALE Community Symposium