Development of a Digital Forensics Lab for Incident Response, Criminal Investigation, and Host Analysis Training

William Meredith · **Thomas Devine, PhD**

West Virginia University · wm00026@mix.wvu.edu · thomas.devine@mail.wvu.edu

Introduction

- Digital forensics is a core cyber defense skill — yet most academic programs lack realistic, scenario-based lab experiences that mirror professional practice.
- Existing curricula emphasize tool familiarity over investigative process, leaving students underprepared for the analytical reasoning required in incident response and criminal investigation roles.
- This work presents a modular, open-source forensics lab framework built for CAE-CD curricula — reusable and adoptable across undergraduate cyber defense programs without specialized infrastructure.

> *"This lab was designed around open-ended investigation. Students receive a scenario and a disk image, not step-by-step instructions."*

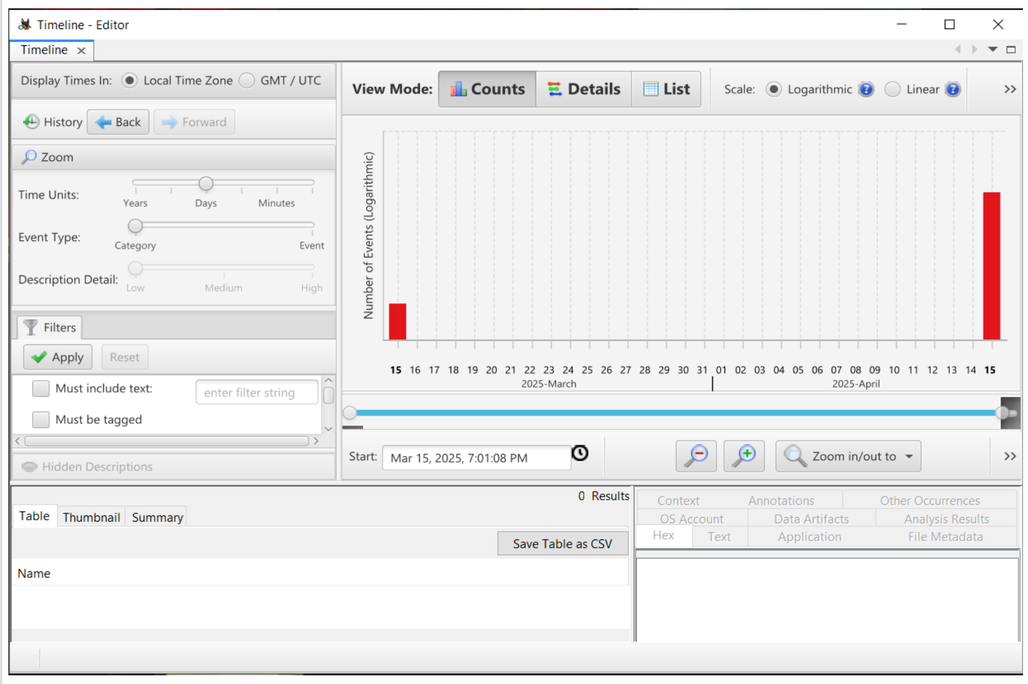

Fig. 1 | Autopsy Timeline Editor — used in Case 2 to reconstruct when files were modified, deleted, and accessed during the simulated enterprise attack.

Lab Design

- **Tool**: Autopsy (free, open-source, Windows-compatible) used by law enforcement, military, and corporate investigators worldwide. No licensing cost; runs on standard lab hardware.
- **Case 1** — "*Scavenger Hunt*" (Flash Drive): Recover deleted files and images from a prepared drive image, identify the file owner via metadata, and produce a concise forensic report (≤150 words). Estimated time: ~60 min.
- **Case 2** — "*Enterprise Compromise*" (Linux Server): Examine a VM disk image to identify privilege escalation, uncover hardcoded credentials embedded in attacker-planted scripts, trace deleted auth logs, and reconstruct the attack timeline. Estimated time: ~90 min.
- **Deliverables**: documented findings recorded throughout+ a formal forensic report; mirroring professional expectations.

Learning Objectives

- ***Apply forensic methodology:*** conduct structured evidence acquisition, artifact analysis, and timeline reconstruction following professional investigative standards.
- ***Recover deleted digital artifacts:*** retrieve deleted files from a prepared flash drive image and determine user identity and activity from file system metadata.
- ***Investigate an enterprise compromise:*** examine a Linux server disk image to identify privilege escalation, trace deleted authorization and credential logs, and document indicators of compromise.
- ***Produce forensic documentation:*** record investigative findings throughout the lab and author a concise report consistent with professional digital forensics standards.

At a Glance

LEVEL **Upper-Division Cybersecurity**	**DURATION** **~2–3 Hours (2 Cases)**
TOOL **Autopsy (Free / Open Source)**	**PLATFORM** **Windows Lab Hardware**

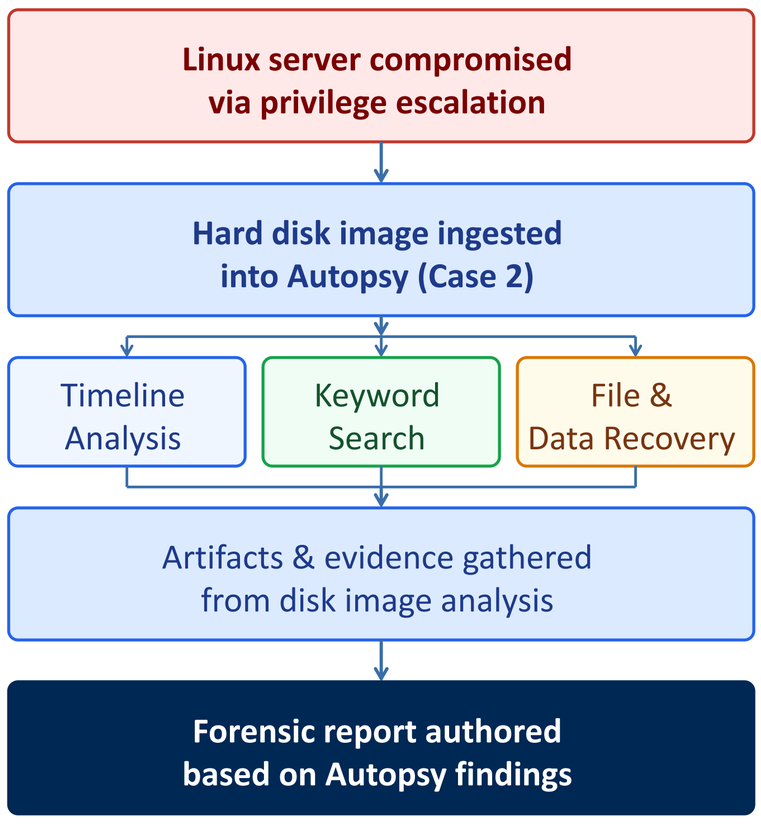

Fig. 2 | Case 2 — Enterprise Compromise Investigation Workflow

CAE-CD Alignment & Assessment

Work Role	Core Tasks Practiced
212 Cyber Defense Forensics Analyst	Perform file system forensic analysis (T0286) · Analyze log files and evidence to identify intrusion perpetrators (T0027) · Provide technical summary per reporting procedures (T0075) · Use forensic tool suites including Sleuth Kit (S0071)
221 Cyber Crime Investigator	Examine recovered data for evidentiary value (T0103) · Gather and preserve evidence for prosecution (T0430) · Identify elements of proof of the crime (T0114) · Prepare reports per legal standards (T0523)

- **Case 1** targets the criminal investigation track (DCWF 221): identifying and recovering deleted evidence, and producing reports consistent with legal documentation standards.
- **Case 2** targets the incident response / defense track (DCWF 212): tracing a host-based compromise, recovering deleted logs, and reconstructing attacker actions.
- Post-lab surveys using standardized questions assess perceived learning gains and confidence in applying forensics competencies to realistic investigative scenarios. Currently in deployment — results forthcoming.

Lab Materials & Availability

- **Disk images** — two purpose-built forensic images (FAT32 flash drive for Case 1; Linux VM image for Case 2) prepared to contain realistic planted artifacts, deleted files, and investigative evidence.
- **Case scenario packets** — written scenario briefs for each case describing the investigative context, role, and deliverables. No step-by-step instructions included by design.
- **Assessment instruments** — pre/post survey instruments aligned to DCWF competency confidence measures, plus a structured forensic report rubric used for grading.
- **Instructor materials** — facilitation guide covering Autopsy setup, case loading, common student sticking points, and debrief discussion prompts for both cases.
- All materials will be **released openly to the CAE community**.

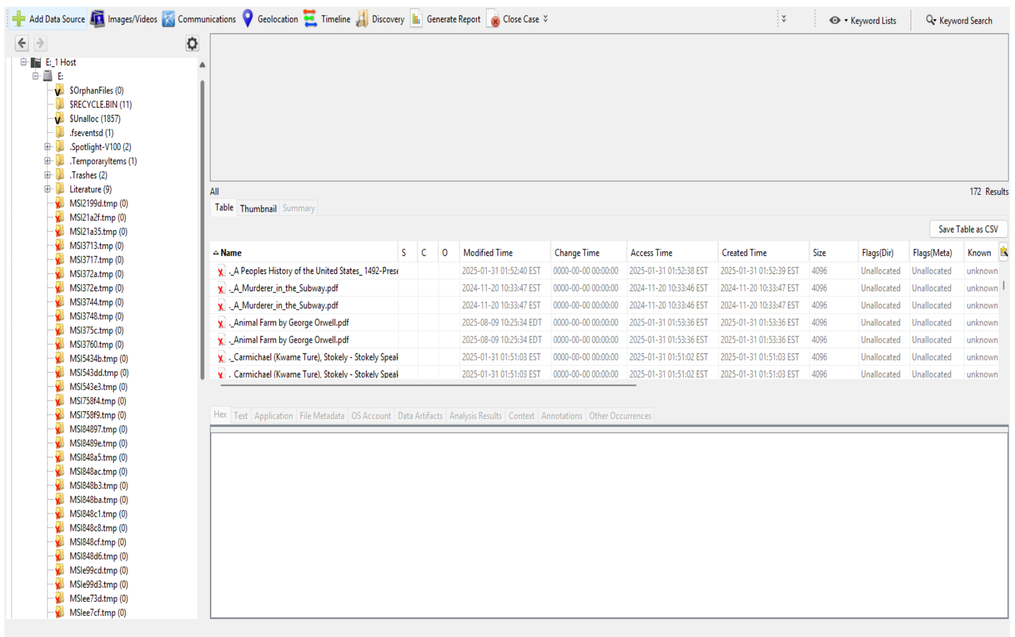

Fig. 3 | Autopsy file tree and recovered deleted files — Case 1 (Scavenger Hunt). Red X marks indicate deleted files recovered from unallocated space; timestamps and metadata are used to identify the drive owner.

Significance

- Most CAE programs lack scenario-based forensics labs. This open-source framework requires no specialized infrastructure, no licensing fees, and runs on standard Windows lab hardware — **immediately adoptable**.
- Emphasizing investigative process over tool mechanics builds transferable analytical reasoning skills applicable to real incident response and criminal investigation roles — **the skills employers actually need**.
- The dual-scenario structure covers both career tracks in a single lab: criminal investigation (Case 1) and enterprise incident response (Case 2), broadening **relevance across diverse CAE program offerings**.
- Releasing all materials to the CAE community enables shared refinement and seeds a **common forensics curriculum** across CAE-CD designated programs.

Conclusion

- This framework demonstrates that high-quality, scenario-based forensics education is achievable with only open-source tools and prepared disk images — removing the infrastructure barriers that prevent most CAE programs from offering realistic forensics labs.
- The open-ended, investigation-centered design develops the *analytical reasoning* and *professional documentation skills* that DCWF roles 212 and 221 require — skills that step-by-step tool tutorials do not build.
- Early classroom deployments show *strong student engagement and perceived learning gains*, validating an investigation-centered pedagogy for upper-level forensics and security coursework (~2–3 hours).
- We are actively seeking *CAE community partners* to pilot these materials. Speak with us at this session or contact us directly to be notified when lab materials are released.

Future Work

- Post-lab *surveys targeting DCWF-aligned competency* confidence are currently in deployment. Results will be used to validate instructional effectiveness and guide scenario refinements.
- All lab materials — pre-built disk images, case scenario files, lab instructions, and assessment instruments — will be *released openly to the CAE community* for adoption, adaptation, and collaborative improvement.
- Additional forensic modules are planned using this framework as a replicable model: *network forensics, mobile device forensics, and memory analysis* — expanding coverage of DCWF 212 competencies.
- Long-term goal: *establish a shared CAE forensics curriculum library* that programs can draw from, contribute to, and build upon cooperatively as a community resource.

West Virginia University
BENJAMIN M. STATLER COLLEGE OF ENGINEERING AND MINERAL RESOURCES