Refreshed View of Computer Security and E-Discovery Course Material

Author: Miguel Angel Rodriguez Delgado
Advisor: Alfredo Cruz, PhD
Department of Computer Science

Abstract

Developing comprehensive educational exercises for E-Discovery and Digital Evidence and Computer Security courses is important for enhancing students' practical skills in two relevant cybersecurity fields. These exercises incorporate current industry practices and technological advancements, preparing students for real-world cybersecurity challenges. Students thoroughly understand theoretical concepts and practical implementations by focusing on hands-on applications, critical thinking, and problem-solving. Updating educational material in these fields ensures students are well-equipped to address the evolving landscape of digital threats and legal investigations. For this purpose, 14 exercises and 1 presentation were developed for each course that walk students through the learning process.

Introduction

The dynamic and ever-evolving nature of cybersecurity, driven by rapid technological advancements and increasingly sophisticated digital threats, presents an ongoing challenge for educators striving to prepare students for real-world scenarios. Recognizing the critical need to bridge the gap between theoretical knowledge and practical application, this project has been dedicated to developing a comprehensive suite of educational exercises designed specifically for two pivotal areas: E-Discovery, Digital Evidence, and Computer Security. These courses are structured not only to introduce cutting-edge concepts and methodologies but also to immerse students in the hands-on experiences necessary to tackle actual cybersecurity challenges.

Background

Lawton et al. [1] suggest that E-Discovery and Digital Evidence are critical components of modern legal and investigative processes. The importance of this field has grown exponentially with the proliferation of digital data [2]. Effective e-discovery practices are essential for managing the vast amounts of electronically stored information (ESI) encountered in legal proceedings. According to Hosny et al. [3], integrating updated educational materials in this domain ensures students can handle complex digital investigations and legal challenges. Computer Security is foundational to protecting information systems from cyber threats, according to Abdollahi et al. [4]. The dynamic nature of cybersecurity necessitates continuous learning and adaptation. A NIST study highlights [5] the importance of incorporating current security practices and emerging technologies into cybersecurity education. By developing realistic and up-to-date exercises, this project aims to bridge the gap between academic knowledge and industry requirements, providing students with the skills needed to secure information systems effectively. Craig and DeVoss suggest [6] the importance of updating educational material in cybersecurity cannot be overstated. Outdated educational content fails to prepare students for the current and future demands of the cybersecurity landscape. Educational institutions must prioritize continuously revising curricula to incorporate the latest research, tools, and methodologies, as suggested by George et al. [7].

Problem

There exists a critical gap between theoretical knowledge and practical skill in both E-Discovery/Digital Evidence and Computer Security education, as emerging threats and investigative techniques outpace static course materials. Moreover, educators often struggle to keep lab exercises aligned with rapidly evolving legal standards and forensic tools, which can leave graduates ill-prepared for compliance-driven e-discovery workflows.

Methodology

The exercises were developed in a format that provides increasing difficulty. Each course had 14 exercises divided into two sections: beginner and complex exercises. Each exercise was built on the previous one, creating broad coverage for the topics , providing students with a comprehensive learning experience. Table 1 shows the topic distribution for the E-Discovery and Digital Evidence course. The development centered on crafting two parallel, fourteen-step exercise sequences—one for E-Discovery and Digital Evidence, the other for Computer Security—each organized into introductory and advanced sections that build progressively on one another. By spacing exercises from fundamental tasks like forensic imaging and metadata extraction to more complex scenarios such as large-scale data filtering and packet capture analysis, students are guided through a scaffolded learning path that reinforces earlier concepts as they advance. Topics were distributed deliberately to ensure comprehensive coverage of both legal-forensic workflows and core security practices, with each new activity relying on skills honed in preceding exercises. This structured, layered approach not only clarifies theoretical principles but also immerses learners in realistic, real-time problem solving, thereby bridging the gap between academic study and professional application.

Table 1: General Exercise Topic Distribution for E-Discovery Course

# of Exercises	Topics
1	Forensic Imaging
2	Metadata Analysis
1	Recovery
3	Large Data Set Forensics & Filtering
1	Sensitive Information handling
1	Packet Capture Analysis
1	Hashing and File Integrity

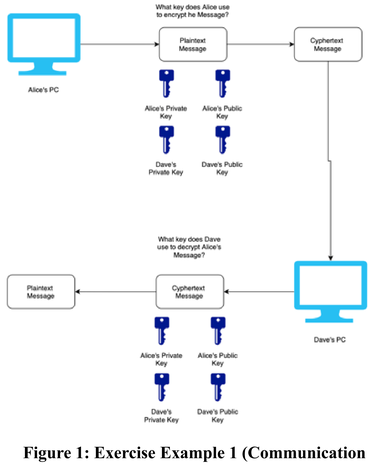

Figure 1: Exercise Example 1 (Communication Encryption Diagram for PKI)

Results and Discussion

A total of 28 hands-on exercises were developed—14 for the E-Discovery and Digital Evidence course and 14 for the Computer Security course, each organized into beginner and advanced sections that build upon one another. Topic distribution tables demonstrate balanced coverage across core domains: forensic imaging, metadata analysis, data recovery, large-scale forensics and filtering, sensitive information handling, and packet capture analysis in the E-Discovery sequence; and risk management, cryptography, public key infrastructure, hashing, file integrity, and file analysis in the Computer Security sequence . The scaffolded design ensures that each exercise reinforces previously acquired skills while introducing new concepts, creating a cohesive progression from foundational techniques to complex, real-world scenarios. This structured exercise framework directly addresses the mismatch between static curricula and evolving cybersecurity challenges by embedding current industry tools and legal-forensic workflows into every module. The deliberate progression—from basic data collection and integrity verification to sophisticated analysis and risk mitigation—promotes both conceptual understanding and practical proficiency. Moreover, the dual-course approach fosters interdisciplinary thinking, preparing students to navigate the intersection of legal requirements and security operations. Future refinements could incorporate AI-assisted analysis and cloud-native forensics to further align the exercises with emerging professional practices.

Table 2: General Exercise Topic Distribution for Computer Security Course

# of Exercises	Topics
2	Risk Management
1	Cryptography
1	Public Key Infrastructure
1	Signatures
1	Non-Repudiation
1	Hashing
2	File Integrity
1	File Analysis

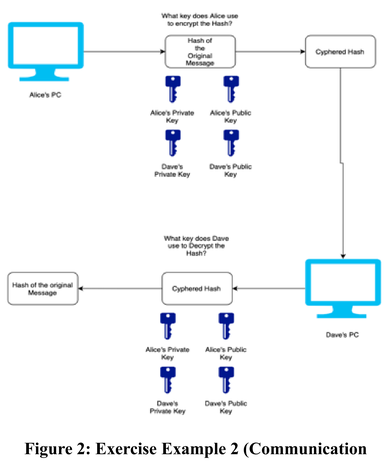

Figure 2: Exercise Example 2 (Communication Encryption Diagram for Hashing)

Conclusions

Developing comprehensive educational exercises for E-Discovery and Digital Evidence and Computer Security courses significantly enhances students' practical skills in cybersecurity. These meticulously crafted exercises, encompassing 14 distinct scenarios for each course, integrate current industry practices and technological advancements. Students gain a robust understanding of theoretical concepts and practical implementations by emphasizing hands-on applications, critical thinking, and problem-solving. This initiative ensures that students are well-prepared to tackle real-world cybersecurity challenges, effectively manage digital threats, and conduct legal investigations precisely. The continuous update of educational material in these domains is crucial for maintaining relevance and equipping students with the necessary skills to navigate the evolving landscape of cybersecurity. These exercises represent a significant step forward in bridging the gap between academic knowledge and industry requirements, fostering a new generation of cybersecurity professionals' adept at addressing contemporary issues.

Future Work

The courses could further benefit from the incorporation of AI and machine learning tools for automated analysis, threat detection, and predictive modeling, reflecting the growing importance of these technologies in cybersecurity. Additionally, partnering with cybersecurity professionals and legal experts ensures exercises remain up to date with the latest practices, tools and regulatory requirements of the field.

Acknowledgements

Thank you to my advisor Dr. Alfredo. Cruz and the wonderful staff of the Polytechnic University's graduate school.

References

1. D. Lawton, R. Stacey, & G. Dodd, "eDiscovery in Digital Forensic Investigations," *U.K. Ministry of Justice*, Sept. 2014. [Online]. Available: https://assets.publishing.service.gov.uk/media/5a7e427ded915d74e33f1185/ediscovery-digital-forensic-investigations-3214.pdf. [Accessed: November 14, 2024].
2. The Sedona Conference, "ESI Evidence & Admissibility," Second Edition, *22 SEDONA CONF. J.*, 83 2021. Available: https://thesedonaconference.org/sites/default/files/publications/2_ESI_Evidence_and_Admissibility_0.pdf. [Accessed: November 14, 2024].
3. A. Hosny, S. Abd-Elkader, and M. H. Amer, "Challenges and opportunities in forensic DNA databases and DNA data banking systems," *Egyptian Journal of Forensic Sciences*, vol. 14, no. 1, 2023, Art. no. 13. Available: https://ejfs.springeropen.com/articles/10.1186/s41935-023-00375-w. [Accessed: December 23, 2024].
4. M. Abdollahi, A. Masoumzadeh, S. Ahmadi, and P. R. Malek, "The emergence of forensic chemistry in the investigation of wildlife crimes: A review," *Forensic Chemistry*, vol. 26, 2021, Art. no. 100354. Available: https://www.sciencedirect.com/science/article/pii/S2352248472100728 9. [Accessed: December 23, 2024].
5. P. A. Redmond, J. G. Richer, L. J. Johnson, and K. D. Scarfone, "NIST Special Publication 800-181: National Initiative for Cybersecurity Education (NICE) Cybersecurity Workforce Framework," *National Institute of Standards and Technology*, Gaithersburg, MD, USA, NIST SP 800-181, Nov. 2019. Available: https://www.nist.gov/system/files/documents/2019/11/08/nist.sp._800-181.pdf. [Accessed: December 23, 2024].
6. J. Craig and D. DeVoss, "Strategic Approaches to Cybersecurity Learning: A Study of Educational Models and Outcomes," *Information*, vol. 15, no. 2, p. 117, Feb. 2024. DOI:10.3390/info15020117. [Accessed: January 01, 2025].
7. S. E. George, S. A. Paschall, and J. D. Nunnery, "Evidence-based practices for supporting students with disabilities: Review of research and implications for education," *U.S. Department of Education*, Institute of Education Sciences, National Center for Education Evaluation and Regional Assistance, Regional Educational Laboratory Northeast & Islands, REL 2021014, Dec. 2020. Available: https://ies.ed.gov/ncee/edlabs/regions/northeast/pdf/REL_2021014.pdf. [Accessed: January 01, 2025].