Refreshed view of Computer Security and E-Discovery Course Material

Miguel Ángel Rodríguez Delgado
Master in Computer Science
Alfredo Cruz, PhD
Polytechnic University of Puerto Rico
Graduate Project EXPO May 2025

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 that 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 walks students through the learning process.*

Key Terms *— Computer-Security, Cyber-Security-Exercise, E-Discovery and Digital Evidence.*

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 and 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.

In today's digital landscape, the rapid pace at which cyber threats and investigative techniques evolve means that traditional curricula often become outdated before they are even taught. To address this, our courses integrate current industry practices and technological advancements, ensuring that every exercise is relevant and reflective of contemporary challenges. For instance, the exercises in E-Discovery and Digital Evidence focus on practical processes such as forensic imaging, metadata analysis, and packet capture analysis—techniques that are indispensable in legal investigations and digital forensic investigations. Each exercise is meticulously designed to simulate realistic scenarios, demanding that students not only understand the underlying theory but also apply their knowledge to identify, analyze, and resolve complex issues encountered in actual investigations.

LITERATURE REVIEW

E-Discovery and Digital Evidence

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 that students are well-equipped to handle complex digital investigations and legal challenges.

Computer Security

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.

Importance of Updating Educational Material

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]. This project aligns with this objective by creating exercises reflecting contemporary practices and challenges, ensuring students receive a relevant and robust education.

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 covered provided students with a comprehensive learning experience. Table 1 shows the topic distribution for the E-Discovery and Digital Evidence course.

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

Table 2 shows the exercise distribution for the course Computer Security.

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

Forensic Imaging

Forensic imaging is a critical process in digital forensics, involving the creation of an exact bit-by-bit copy of digital storage media for analysis and investigation. This technique ensures the integrity and preservation of original evidence, allowing investigators to uncover crucial data without altering the original source.

Forensic Imaging Exercise 1

In the context of a cybersecurity investigation involving the website, forensic imaging was applied by capturing a full snapshot of the website's contents, network requests, and loaded scripts to analyze potential malware distribution. Using tools like WebPageTest, students examined how the website loads, identify any unexpected JavaScript files, track redirects to malicious domains, and detect unauthorized third-party content. This forensic snapshot ensured that evidence was preserved for further analysis without altering the original data, enabling cybersecurity professionals to reconstruct and understand the attack vector.

Metadata

Metadata, often described as data about data, plays a crucial role in digital forensics and information management. It provides essential information about digital file creation, modification, and access history, which can be pivotal in legal investigations and cybersecurity audits.

Understanding and analyzing metadata allows investigators to trace actions, establish timelines, and verify the authenticity of digital evidence.

Metadata Exercise 1

Online tools could be used to capture a snapshot of the certificate's metadata, including the issuer, validity period, encryption strength, and domain information, to verify the authenticity and security of an SSL certificate from a suspected phishing website. By using tools like SSL Labs' SSL Test, students assessed whether the certificate was self-signed, issued by an untrusted Certificate Authority (CA), or had other discrepancies that suggested fraudulent activity. By collecting and preserving this digital evidence, forensic analysts established a link between the phishing website and the data breach, supporting legal and cybersecurity actions.

Metadata Exercise 2

In a copyright infringement case, metadata provided essential details about an image, including the camera model, date and time of capture, geolocation data, and file modifications. Using tools like Metadata2Go, forensic analysts analyzed the metadata of the image1.jpeg file to determine its origin and verified whether it matched the client's original photograph. Key metadata attributes, such as the camera make and model, helped establish ownership and detect unauthorized usage. If the metadata confirmed that the image had been captured using a device registered to the photographer, this evidence strengthened the legal case against the unauthorized use.

These exercises allowed students to work through metadata analysis in digital forensics. The first exercise focused on extracting metadata from an image to gather information about its origin, which was crucial in copyright infringement cases. The second exercise extended this concept to digital documents, emphasizing the importance of analyzing metadata to understand document history and identify any anomalies. The third exercise delved deeper into metadata analysis of a PDF in a legal context, highlighting the role of metadata in verifying document authenticity and detecting tampering. Together, these exercises covered a broad range of applications for metadata analysis, from image files to PDF documents, reinforcing the importance of metadata in digital forensic investigations.

Recovery

Recovery in the context of E-Discovery and Digital Evidence refers to the process of retrieving deleted, hidden, or inaccessible data from digital devices for legal and investigative purposes. This process involves advanced techniques and tools to ensure that crucial electronic information is accurately restored and preserved. Effective recovery is essential for uncovering relevant evidence that can significantly impact the outcome of legal proceedings and investigations.

Recovery Exercise 1

In a phishing campaign investigation targeting employees of a financial institution, recovery involved identifying and mitigating malicious infrastructure, such as fraudulent domains and fake login pages. Using DNSDumpster, investigators performed DNS reconnaissance on the suspicious domain (pupr.edu) to gather information about its IP addresses, subdomains, MX records, and other DNS entries. Identifying these records helped in blocking malicious servers, reporting fraudulent domains to registrars, and implementing security controls such as email filtering and domain takedown requests. By mapping the phishing domain's infrastructure, cybersecurity teams enhanced their incident response and prevented future attacks.

Large Forensics & Filtering

Large data forensics involves analyzing and investigating extensive datasets to uncover digital evidence and insights. As organizations generate vast amounts of data, efficiently processing and analyzing these large datasets becomes critical in forensic investigations. Techniques such as data mining, machine learning, and advanced analytics are employed to sift through massive volumes of

data, identify relevant patterns, and extract actionable intelligence. This approach ensures that investigators can handle the scale and complexity of modern digital environments while maintaining the accuracy and integrity of their findings.

Large Forensics & Filtering Exercise 1

Filtering was a crucial process in forensic investigations that helped analysts isolate relevant digital evidence by eliminating noise and focusing on key indicators of compromise. In an e-Discovery investigation involving a phishing campaign, filtering was applied to analyze a set of suspicious URLs extracted from emails and chat logs. By using online URL analysis tools like VirusTotal, investigators examined these URLs for malicious behavior, checked for malware distribution, phishing content, and reputation-based security warnings. This process helped identify fraudulent websites and determined whether the URLs were used to steal financial credentials or deploy malware within the company's network. Effective filtering ensured that only high-risk links were prioritized for further investigation, improving response efficiency in cybersecurity incidents.

Large Forensics & Filtering Exercise 2

Examining a suspected executable file recovered from a compromised server was crucial in determining whether it was used as a malware dropper. By leveraging an online virus scanning tool like VirusTotal, forensic investigators uploaded the file, scanned it against multiple antivirus engines, and analyzed the report for signs of malware, trojans, or other threats. If flagged as malicious, the analysis provided insights into its potential impact, such as unauthorized access, data exfiltration, or system compromise, aiding in the investigation of the cybersecurity breach.

Large Forensics & Filtering Exercise 3

Email header analysis was a crucial step in e-discovery for uncovering fraud, email spoofing, or unauthorized access. During a corporate fraud investigation, forensic analysts extracted metadata from email headers to determine the origin, relay path, timestamps, and security validation mechanisms (such as DKIM, SPF, and DMARC). Using tools like Google Apps Toolbox Message Header Analyzer, investigators traced the sender's IP address, email routing details, and potential anomalies that might indicate spoofing, tampering, or unauthorized email relay. By carefully examining these headers, forensic experts verified the authenticity of emails and established a digital chain of custody, ensuring that the collected evidence remained admissible in legal proceedings.

Together, these exercises offered a comprehensive understanding of the e-discovery process. The first exercise focused on filtering out irrelevant documents, providing a foundation for narrowing down large datasets to relevant information. The second exercise built on this by emphasizing the review of large sets of emails, highlighting the importance of efficient and collaborative review processes. The third exercise addressed the initial step of collecting emails, ensuring that the data was gathered accurately and preserved for subsequent filtering and review. Together, these exercises covered the critical stages of e-discovery, from data collection and filtering to detailed review and documentation, demonstrating the integrated workflow necessary for effective legal investigations.

Sensitive Information Handling

Handling sensitive information in digital forensics requires strict adherence to privacy laws, ethical guidelines, and security protocols to protect the integrity and confidentiality of the data. This involves employing encryption, access controls, and secure storage methods to prevent unauthorized access and data breaches. Proper handling ensures that sensitive information is safeguarded throughout the forensic process, maintaining the trust and privacy of individuals and organizations involved.

Sensitive Information Handling Exercise 1

In a corporate fraud investigation involving the now-defunct e-commerce website shopnow.com,

forensic investigators carefully retrieved and analyzed archived web pages using the Wayback Machine. This allowed them to examine fraudulent sale offers, discrepancies in terms and conditions, and any relevant customer feedback from March 2022. However, during the documentation of findings, it was essential to redact sensitive customer information, such as names, addresses, payment details, and login credentials, before sharing reports with stakeholders. This ensured compliance with data protection regulations while maintaining the evidentiary value of the investigation.

Packet Capture Analysis

Packet capture analysis involves collecting and examining data packets transmitted over a network to identify and investigate security incidents, performance issues, and other network-related anomalies. By capturing and analyzing network traffic, forensic experts can uncover unauthorized activities, pinpoint sources of attacks, and understand the data flow within a network. This detailed inspection of packet data is essential for maintaining network security, troubleshooting problems, and ensuring compliance with regulatory requirements.

Packet Capture Analysis Exercise 1

In a potential data breach at a financial institution, forensic analysts examined a packet capture file (network_traffic.pcap) to reconstruct network communication over a specified period. By using online PCAP analysis tools such as Dynamite Analytics, investigators inspected the captured packets to identify suspicious traffic patterns, unauthorized connections, and potential exfiltration of sensitive data. Key aspects of the analysis included checking protocols, IP addresses, and payload contents to determine if an external attacker had infiltrated the network.

Hashing

Hashing is a cryptographic technique that converts data into a fixed-size string of characters, uniquely representing the original data. In digital forensics, hashing is essential for verifying the integrity and authenticity of digital evidence, ensuring that data has not been altered or tampered with during the investigation process. Common hashing algorithms include MD5, SHA-1, and SHA-256, which produce unique hash values that serve as digital fingerprints for files and data.

Hashing Exercise 1

In a corporate litigation case, where a JPEG file (image1.jpeg) was a key piece of evidence, computing an MD5 hash allowed investigators to verify that the file had not been altered throughout the legal proceedings. If even a single byte was changed, the resulting hash would be entirely different, providing proof of tampering or authenticity. Using tools like the MD5 checksum generator, forensic analysts created and compared hashes to confirm that the digital evidence remained unmodified from its original state, ensuring its admissibility in court.

Risk Management

In computer security, Annualized Loss Expectancy (ALE) is a risk management metric that estimates the potential annual financial loss from security threats. It combines the likelihood of a security incident occurring with the expected loss per incident, helping organizations prioritize and justify their security investments.

Risk Management Exercise 1

This exercise involved assessing the potential financial impact of a cybersecurity breach on a company's network infrastructure. The task was to calculate the Annualized Loss Expectancy (ALE) based on the asset value of the network infrastructure, the likelihood of a breach occurring, and the estimated recovery cost.

Risk Management Exercise 2

This exercise involved analyzing images of various security controls and identifying the appropriate classification for each. The classifications to choose from were Preventative,

Detective, Corrective, and Deterrent. The goal was to match each security control with its correct classification and explain how it mitigated the associated threat.

Cryptography

Secure communication involves protecting data transmission between parties to prevent unauthorized access, interception, or tampering. Techniques such as encryption, digital certificates, and secure protocols ensure that information remains confidential and unaltered during transit.

Cryptography Exercise 1

This exercise involved identifying the cipher used to encrypt a message and decrypting it based on the given clue. The clue pointed to Caesar's Cipher, which involved shifting the alphabet by a specific number of places.

Public Key Infrastructure

Secure communication involves protecting data transmission between parties to prevent unauthorized access, interception, or tampering. Techniques such as encryption, digital certificates, and secure protocols ensure that information remains confidential and unaltered during transit.

Public Key Infrastructure Exercise 1

A public key and a private key. In the scenario where Alice encrypted a message for Dave using PKI, Alice used Dave's public key to encrypt the plaintext message, ensuring that only Dave could decrypt it using his private key, which was securely kept confidential. This process guaranteed the confidentiality of the communication, as no one else could decrypt the message without access to Dave's private key. PKI enabled secure, authenticated exchanges in organizations by leveraging trust hierarchies, ensuring that encryption keys were tied to verified digital identities.

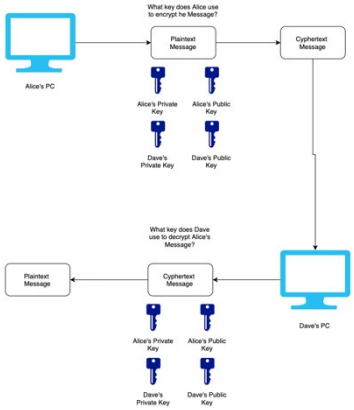

Figure 1
Communication Encryption Diagram for PKI

Signing

Secure communication involves protecting data transmission between parties to prevent unauthorized access, interception, or tampering. Techniques such as encryption, digital certificates, and secure protocols ensure that information remains confidential and unaltered during transit.

Secure Communication Exercise 1

This exercise focused on the process of signing a message to ensure its authenticity. Alice had to sign a message, and Dave had to verify the signature. The task was to identify the appropriate keys used for signing and verification. Figure 2 shows the diagrams used for Secure Communications Exercise 3.

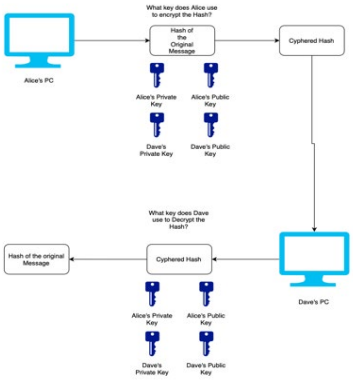

Figure 2
Communication Encryption Diagram for Hashing

These exercises collectively provided a comprehensive understanding of cryptography and Public Key Infrastructure (PKI). The first exercise emphasized the basics of encryption and decryption using Caesar's Cipher, highlighting the concept of symmetric key encryption. The second exercise introduced asymmetric encryption, explaining how public and private keys ensured secure communication between two parties. The third exercise built on this by explaining digital signatures, demonstrating how PKI could also be used to verify the authenticity and integrity of a message. Together, these exercises covered essential aspects of cryptography, from basic encryption techniques to the complexities of PKI, showcasing their roles in ensuring secure and authentic communication in the digital world.

Hashing

Hashing in computer security refers to the process of converting data into a fixed-size, unique string of characters using a cryptographic algorithm. This technique is crucial for verifying data integrity, ensuring that the original content has not been altered.

Hashing Exercise 1

This exercise involved identifying the original passwords from a set of leaked hashed passwords using an online SHA1 tool. The task was to compare the provided hashed passwords with the hashes generated from the given options to find the matching original password.

Non-Repudiation

Non-repudiation is a security principle ensuring that a party in a digital transaction cannot deny the authenticity of their signature or the sending of a message. This is typically achieved through digital signatures and cryptographic methods, providing proof of origin and integrity.

Non-Repudiation Exercise 1

This exercise involved ensuring non-repudiation in communication between Alice and Dave using asymmetric encryption. Alice sent an encrypted message, and Dave needed to verify if the message was altered during transit. The exercise involved using Alice's public and private keys, along with SHA-1 and RSA encryption, to check the integrity of the message.

File Integrity

Network security involves implementing measures to protect a computer network from unauthorized access, misuse, or theft. This includes the use of firewalls, intrusion detection systems, and encryption to safeguard data and maintain the integrity of connected systems.

Network Security Exercise 1

A hex analysis of the file, using tools like HexEd.it, revealed its true file type, metadata, and potential embedded data. Attackers often used steganography to conceal confidential information within seemingly harmless files, such as images, making forensic examination critical in detecting unauthorized data exfiltration. By analyzing the hexadecimal structure, investigators determined whether malicious modifications had been made, uncovered hidden data, and traced the source of the leak, aiding in a comprehensive cybersecurity investigation.

File Analysis

Attacks in computer security refer to malicious actions aimed at compromising the security of information systems. These can include a variety of methods, such as phishing, malware, denial-of-service (DoS), and man-in-the-middle attacks, each designed to exploit vulnerabilities.

File Analysis Exercise 1

File integrity verification was a crucial aspect of digital forensics, ensuring that files had not been altered or tampered with during transmission or storage. In the context of a corporate merger case, verifying the integrity of critical images exchanged between companies helped maintain the authenticity of digital evidence. By using cryptographic hashing

tools, such as the MD5 checksum calculator, forensic analysts generated and compared the hash values of Hash_Image_1 and Hash_Image_2. If both files produced the same hash value, it confirmed that the images were identical and had not been modified. However, if the hash values differed, it indicated potential tampering or corruption, which could have impacted the due diligence process and raised concerns about the legitimacy of the exchanged files. This process ensured transparency and security in high-stakes legal and corporate investigations.

CONCLUSION

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.

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.

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/S2352484721007289. [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].