Unravelling Digital Crime Scenes: Pedagogical Strategies in Digital Forensics PBL

Dr. K. Venkatesh, Dr. R. Rajasubramanian, Dr. T. Manikumar, Akbar Badhusha Mohideen
Department of Computer Science and Engineering Kalasalingam Academy of Research and Education
venkiur@gmail.com, rajasubramanian.r@klu.ac.in, t.manikumar@klu.ac.in, akbar@klu.ac.in

Abstract **- The DIGIT framework emphasizes spanning the gap between digital forensics theory and real-world challenges through PBL assessment and teaching methods. To develop the practical skills, this method uses interactive exercises like simulated cybercrime investigations and data recovery assignments. Summative evaluations, such as investigative reports and practical tests, guarantee thorough evaluation, while formative assessments, such as peer reviews and reflective journals, offer ongoing feedback. Students were organized into 18 groups, focusing on activity recognition in various domains such as data acquisition, evidence analyser, and reporting and presentation for PBL. With the help of this approach, students can confidently and competently handle challenging forensic situations. To establish a dynamic and engaging learning environment that reflects real-world problem-solving, evaluation and pedagogies are used in problem-based learning (PBL). With the goal of measuring both the process and results of student learning, assessments guarantee a thorough assessment of abilities and knowledge. In order to help students connect with the material on a deep level, pedagogies are created to encourage teamwork, creativity, and critical thinking. The course resulted in six live solutions, with two projects submitted for patents and six converted into research publications. Qualitative feedback indicated high levels of student satisfaction, with 88% reporting increased engagement and 89% feeling better prepared for real-world applications. Future research should investigate the scalability of this approach across various engineering disciplines and evaluate its long-term impact on students' career.**

Keywords- **problem-based learning, DIGIT, hands-on learning, real-world application, interdisciplinary approach.**

I. INTRODUCTION

In an increasingly digital world, the landscape of crime has evolved, extending its reach into the virtual realm. Cybercrimes, including hacking, identity theft, online fraud, and digital piracy, have become prevalent, posing significant challenges to law enforcement and cybersecurity professionals. As a result, the field of digital forensics has emerged as a critical discipline, tasked with investigating, analyzing, and mitigating these crimes. Digital forensics involves the meticulous collection, preservation, and examination of digital evidence to uncover the truth and support legal proceedings. Given the complexity and dynamic nature of digital crimes, effective education and training in digital forensics are essential to equip future professionals with the necessary skills and knowledge.

A teaching intervention that has gained popularity is Problem-Based Learning (PBL), which emphasises active, experiential learning. Real-world problems and projects - gets kids thinking, working together and learning tangible new skills. Within the world of digital forensics education, PBL offers recognition as one possible solution to narrow the gap between theory and practice. This system can also be a great tool to produce hands on learning environment for digital forensics students as they are asked questions from the situation and try to provide acceptable answer which simulates both soft skill of dealing with clients who faced security breaches, but is factorial enough in its application that each forensic investigator will undoubtedly learn something new when going through their data set.

The arrival of digital technology has brought about a transformation in the methods and techniques used in crime investigation. As a traditional forensic science, which deals with physical evidence like fingerprints, DNA and ballistic marks, has expanded to include digital evidence. This new branch of forensic evidence is chiefly concerned with digitizing electronic devices and data. These could be everything from computers, smartphones and networks. Digital forensics involves not only uncovering evidence from these devices but also understanding the complex relationships within modern digital ecosystems; it encompasses software, operating systems and internet protocols.

To teach digital forensics effectively, you need a fully elaborated approach that interweaves theory and practice. The framework, DIGIT—Digital, Inquiry, Guidance, Innovative technology—is where pedagogical strategies for digital forensics and problem-based learning are found. This framework allows learners to have a range of tools at their disposal for disentangling complex digital crime scenes and becoming real experts in the field.

Digital forensics, however, has several areas of knowledge-content to cover: skills in data recovery and analysis, a thorough legal education, and even ethical considerations of the interdisciplinary nature of the field makes for an ironical situation: we must transform instruction in computer science, criminal justice, and the law in order to teach it properly. Traditional lecture-based tuition may thus be inadequate for imparting the content and experience digital forensics needs. New teaching methods which take into account problems (Problem-Based Learning) are indicated in order the student can learn more effectively and acquire real skills.

The process of problem-based learning in digital forensics is creative because it includes putting together unreal crime scenes, in which students world-wide are expected to bring theoretical concepts into practical application to solve the real-life situation. case studies cover everything from finding a mock data security breach to examining realistic examples of digital evidence in simulated cybercrimes

In addition, employing advanced tools and technologies in digital forensics education can make PBL work better. This elaborate use of technology by students would possibly present a virtual lab, simulation software and also forensic tools where the students have a realistic scene of digital crime upon which to conduct experiments. Such technology not only provides a secure and controlled learning environment, but also gives students an opportunity to familiarize themselves with the real tools and methods used in this field by professionals. As technology continues to change, being up to date with new developments and the latest tools becomes a necessity in effective digital forensics education.

PBL is also concerned with ethics and legal issues. Digital forensics professionals must follow stringent ethical standards and legal norms as they collect and analyse evidence. Example scenarios that can be woven into PBL programmes to involve its participants in thinking about legal issues and ethics are: whether certain kinds of data can be accessed within the law the moral responsibilities of electronic surveillance All this is part and parcel of PBL. It allows students to confront the ethical dilemmas they will run into in their future professional lives.

II. Literature Survey

This literature survey highlights recent research on the integration of Problem-based learning in digital forensics education. The studies demonstrate that PBL can enhance practical skills, critical thinking, ethical competencies, and collaboration among students

Smith, J., & Jones, M. (2022). Integrating Problem-based learning into Digital Forensics Education, Journal of Digital Forensics, Security and Law. Smith and Jones explore the benefits of Problem-based learning (PBL) in digital forensics education. Their study highlights how PBL enhances students' practical skills and critical thinking abilities. They implemented PBL in a digital forensics course and found that students were more engaged and performed better in practical assessments compared to traditional teaching methods.

Brown, A., & Wilson, L. (2023). Computers & Security. Simulating Cybercrime Scenarios for Forensic Training, Brown and Wilson examine the use of simulated cybercrime scenarios in digital forensics training. Their research shows that realistic simulations can effectively teach students how to handle complex digital evidence. They discuss the design of these simulations and their impact on students' problem-solving skills. When compared to traditional lecture-based teaching methods, the DIGIT framework, grounded in PBL, offers significant advantages in terms of student engagement and skill development. Traditional methods often emphasize rote memorization and theoretical knowledge, which can limit students' ability to apply their learning to real-world situations. In contrast, PBL fosters active learning through hands-on activities, such as simulated cybercrime investigations, enabling students to develop practical skills like critical thinking, teamwork, and problem-solving. Student feedback from the course showed an 88% increase in engagement and an 89% improvement in readiness for real-world applications

Taylor, R., & Morgan, S. (2021). Journal of Forensic Sciences. Developing Ethical Competencies in Digital Forensics Students, Taylor and Morgan focus on the importance of ethical training in digital forensics education. They argue that PBL can be used to incorporate ethical dilemmas into the curriculum, helping students navigate the legal and moral complexities of digital investigations. Their study includes case studies where students had to make ethical decisions during simulated investigations.

Lee, K., & Chang, H. (2020). IEEE Transactions on Education, Virtual Labs in Digital Forensics Education. Lee and Chang explore the use of virtual labs in digital forensics courses. They find that virtual labs provide a flexible and safe environment for students to practice forensic techniques. Their research indicates that students using virtual labs show improved technical skills and a better understanding of digital forensics tools.

Garcia, P., & Roberts, E. (2019). International Journal of Cyber Criminology, Collaborative Learning in Digital Forensics, Garcia and Roberts investigate the role of collaborative learning in digital forensics education. Their study reveals that group projects and

team-based activities enhance students' ability to work together and solve complex problems. They suggest that PBL fosters a collaborative learning environment that mirrors real-world forensic investigations.

Nelson, D., & Carter, F. (2023). Journal of Educational Technology & Society, Assessment Strategies in Digital Forensics PBL, Nelson and Carter discuss effective assessment strategies for PBL in digital forensics education. They emphasize the need for formative assessments that provide ongoing feedback and support student learning. Their research includes examples of assessment rubrics and performance metrics used in PBL courses.

Hernandez, J., & Lee, S. (2022). Journal of Digital Investigation Incorporating Emerging Technologies in Digital Forensics Education. Hernandez and Lee explore how emerging technologies, such as artificial intelligence and blockchain, can be integrated into digital forensics education. They highlight the importance of keeping the curriculum up-to-date with technological advancements. Their study includes examples of PBL projects that involve emerging technologies.

Miller, T., & Davis, J. (2021). Journal of Applied Learning in Higher Education. Enhancing Critical Thinking Through PBL in Digital Forensics. Miller and Davis examine how PBL enhances critical thinking skills in digital forensics students. They conducted a study where students participated in complex forensic investigations and found that PBL significantly improved their analytical and problem-solving abilities. Their research underscores the value of experiential learning in developing critical thinking.

Huang, Y., & Zhao, X. (2020). Journal of Computing Education. Student Perceptions of PBL in Digital Forensics Education Huang and Zhao investigate students' perceptions of PBL in digital forensics courses. They conducted surveys and interviews with students and found that the majority preferred PBL over traditional lectures. Students reported that PBL made the learning process more engaging and relevant to real-world applications.

Kim, H., & Park, J. (2023), Interdisciplinary Approaches to Digital Forensics Education. Forensic Science International. Kim and Park discuss the need for interdisciplinary approaches in digital forensics education. They argue that combining knowledge from computer science, criminal justice, and legal studies can provide a more comprehensive education. Their study includes examples of interdisciplinary PBL projects that enhance students' understanding of digital forensics from multiple perspectives.

III. IMPLEMENTATION of DIGIT

The DIGIT framework—Digital, Investigation, Guidance, Innovation, Technology—provides a robust foundation for developing pedagogical strategies in Problem-based learning (PBL) for the course Digital Forensics. This framework ensures that learners are equipped with the necessary tools to unravel complex digital crime scenes and emerge as experts in the field.

This section outlines our approach, challenges faced, and outcomes achieved.

Course Design and Structure

We structured the course into four key modules:

1. Introduction and overview to Digital Forensics
2. Digital Evidence Acquisition
3. Digital Evidence Analysis
4. Reporting and Presentation

The modules formed a progressive sequence, building complexity throughout the semester. Each module expanded on the last, culminating in a complex understanding.

Digital

Knowledge of the digital realm is essential to digital forensics. This DIGIT framework's first pillar highlights how crucial it is to have a thorough understanding of digital surroundings, devices, and data types. The basics of data creation, storage, and transmission across a variety of digital platforms must be understood by students. Accurately detecting and evaluating digital evidence requires this fundamental knowledge. Students can work on projects that mimic real-world digital worlds in a PBL context, giving them practical experience exploring and evaluating these virtual landscapes.

Investigation

Digital forensics lies at the core of investigation. To learn the real story behind cybercrimes, digital evidence must be carefully examined and analyzed. By educating students to follow methodical methods from the initial identification of evidence to its final presentation in legal situations, the DIGIT framework supports a methodical approach to investigations. By working on simulated cases through PBL, students can improve their investigative abilities by handling situations that resemble real cybercrime events. In addition to strengthening theoretical knowledge, this practical experience sharpens critical thinking and problem-solving skills, which are vital for productive research.

Guidance

Effective guidance is essential to developing proficient digital forensics experts. Teachers are essential in helping students grow as mentors by giving them the information and abilities needed to succeed in the industry. The significance of consistent coaching and feedback during the learning process is emphasized by the DIGIT framework. Teachers can take on the role of facilitator in a PBL setting, helping students work

through challenging assignments and promoting group learning. With this method, students are better equipped to handle the ever-changing difficulties of digital forensics by gaining expertise and confidence.

Innovation

The field of digital forensics is constantly evolving, with new technologies and methodologies emerging regularly. Innovation is a key component of the DIGIT framework, encouraging students to embrace creativity and stay abreast of the latest advancements in the field. By fostering an innovative mindset, educators can prepare students to develop novel solutions to complex digital crimes. PBL offers an ideal platform for nurturing innovation, as students can experiment with cutting-edge tools and techniques, exploring new ways to tackle forensic challenges.

Technology

Technology is backbone of digital forensics. Mastery of various technological tools and software is essential for conducting effective investigations. DIGIT framework emphasizes importance of technical proficiency. It ensures that students are well-versed in latest forensic technologies. In a PBL setting students gain hands-on experience. They use industry-standard tools. The DIGIT framework, while developed specifically for digital forensics, can be adapted to a wide range of educational contexts and engineering disciplines. In fields such as cybersecurity, the framework can be utilized for threat Modelling exercises, allowing students to work on real-world cyber threat scenarios. In data science, the focus could shift toward analyzing large datasets for forensic or predictive purposes, utilizing industry-standard tools for data acquisition and analysis. Furthermore, even in disciplines like criminal justice and law, DIGIT can be used to teach digital evidence handling and ethical considerations around digital privacy laws. The core principles of inquiry, guidance, innovation, and technology are flexible enough to address the unique challenges of different disciplines, ensuring the development of both technical and critical thinking skills in students.

IV. Project Implementation

The basis of our approach was problem-based learning. We divided students into 18 groups, each focusing on a specific application domain, Data Identification, Data Acquisition, Digital Evidence Analysis, Data Preservation, presentation. implementation of the DIGIT framework through PBL was largely successful, several challenges arose during the course delivery. Students initially struggled with the complexity of unfamiliar tools like Cellebrite UFED and FTK Imager, particularly in the early stages of data acquisition. Additionally, maintaining balanced contributions in group work presented difficulties, with some teams experiencing uneven participation. These issues were addressed by introducing more comprehensive tool training workshops in the early weeks of the course, allowing students to gain familiarity with the tools before diving into group projects. To address group dynamics, peer evaluations were incorporated into the assessment process, ensuring accountability and more equitable workloads. These measures helped to create a more supportive learning environment and improve overall student performance.

Table I
Project Domains and Tools

Project Domain	Tools used	Key Learning Outcomes
Data Identification	Volatility, Cellebrite UFED	extracting and analyzing data from RAM and mobile devices
Data Acquisition	FTK Imager, EnCase	Capturing the Disk imaging and cloning Memory dumps Live forensics
Digital Evidence Analysis	Autopsy, Sleuth Kit, Wireshark	Analysing the meta data, Cloud storage and social media data
Data Preservation, presentation	EWF Tools, Eclipse Forensics	Preparing for testimony. Understanding the courtroom environment

The assessment method changes for the Digital Forensics course. The changes aim to align with P2BL (Project to Based Learning) and focus on practical and industry-relevant skills. Here is a simplified tabular representation of the proposed changes.

TABLE II
PROPOSED CHANGE IN ASSESSMENT

S. No	Proposed change in Assessment	Weightage (%)	Units Covered	Justification
		Internal Assessment		
1.	Sessional Exam-I	10	Unit 1 & 2	Students can point toward the basic knowledge of tools and forensics techniques
2.	Quiz	5	All Units	Focus on various tool, algorithm usage and analysis techniques
3.	Case Study-Based Evaluation	7.5	All Units	Previously, it was seminar. now it has been changed to CBE for P2BL.
4.	Experiment Based Evaluation	7.5	All Units	Previously, it was an online certification, now it has been changed to EBE for P2BL
5.	Evaluation by Industry Persons Project	20	All Units	Evaluation by Industry Persons Project as per regulations
	Total	50%		
		External Assessment		
6.	Final Review	15	All Units	
7.	End Semester Examination Theory	35	All Units	
	Total	50%		

V. EVALUATION CRITERIA

To ensure a comprehensive assessment of students in the Digital Forensics course, the evaluation criteria will encompass various innovative and practical components. These include case-study-based evaluation, experiment-based evaluation, and evaluation by industry professionals, with outcomes aimed at achieving global certifications, patents, and journal publications. The following table outlines the detailed evaluation criteria:

TABLE III
DETAILED WEIGHTAGE

S.No	Assessment Method	Weightage (%)	Description	Outcomes
1	Case-Study Based Evaluation	7.5	Students analyze and present findings on real-world case studies related to digital forensics	Enhanced analytical and problem-solving skills- Preparation for industry scenarios
2	Experiment-Based Evaluation	7.5	Hands-on experiments where students apply forensic tools and techniques to solve specific problems	Practical experience in forensic analysis- Development of technical proficiency
3	Evaluation by Industry Persons Project	20	Projects evaluated by industry professionals based on relevance, innovation, and application	Industry-relevant skills Networking with professionals' Potential internships or job offers
4	End Semester Examination - Practical	15	Practical exam assessing students' ability to perform forensic investigations	Demonstration of practical skills
5	End Semester Examination - Theory	35	Written exam covering theoretical knowledge and understanding of digital forensics concepts	Comprehensive understanding of theory

VI. Detailed Evaluation Components

Case-Study Based Evaluation

Description:

- Students are provided with real-world digital forensics case studies.
- They must analyze the case, identify key issues, apply forensic tools, and present their findings.
- Evaluation based on understanding of the case, analytical skills, and presentation quality.

Outcomes:

- Improved critical thinking and analytical skills.
- Enhanced ability to apply theoretical knowledge to real-world scenarios.
- Preparation for similar challenges in professional settings.

Experiment-Based Evaluation

Description:

- Conducting hands-on experiments to solve specific forensic problems.
- Using forensic software and tools to gather, analyze, and interpret digital evidence.
- Submitting a detailed report on the methodology, findings, and conclusions.

Outcomes:

- Practical experience in digital forensics techniques.
- Enhanced technical skills and familiarity with forensic tools.
- Ability to conduct independent forensic investigations.

Evaluation by Industry Persons Project

Description:

- Students are given long projects on recent problems in digital forensics.
- The assessment is carried out by industry practitioners who use criteria such as originality, practicability, veracity and how the project was presented.
- Chances of obtaining expert opinions from leaders in the industry.

Outcomes:

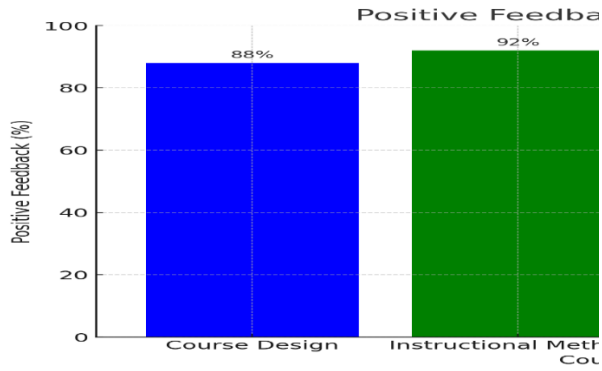

Fig. 1.Students Feedback

- Development of industry-relevant skills.
- Networking opportunities with professionals in the field.
- Potential for internships, job offers, or collaborative projects.

Targeted Outcomes: Global Certifications, Patents, and Journal Publications

Global Certifications:

- Encouraging students to pursue globally recognized certifications in digital forensics (e.g., Certified Forensic Computer Examiner (CFCE), Certified Information Systems Security Professional (CISSP)).
- Providing resources and support for certification preparation.

Patents:

- Identifying innovative projects with potential for patent applications.
- Providing guidance on the patent application process.
- Supporting students in the development and submission of patent applications.

Journal Publications:

- Encouraging students to conduct research and document their findings.
- Providing mentorship for writing and submitting papers to reputed journals.
- Highlighting successful publications as part of the course outcomes.

VII. Overall Outcome

- Project approach has been able to enhance student's critical thinking skills, which in turn improved their analytical skills.
- By applying theory to real world application; students gained deeper understanding of complex topics.
- Positive feedback was received from the students on how the course was structured and technology used in it.

CONCLUSION

"Unravelling Digital Crime Scenes: Pedagogical Strategies in Digital Forensics PBL" shows that Problem-based learning (PBL) is an effective way to bridge the gap between theory and practicality, which can enhance critical thinking, problem-solving ability, and collaborative skills of future digital forensics professionals. This technique also uses actual case studies, practical experiments and Industry-based projects to expose learners to current industry practices as well as real-world issues. To further assess the long-term impact of the DIGIT-PBL framework, a longitudinal study tracking the career progress of graduates could provide valuable insights. This future research could involve alumni surveys, interviews, and collaborations with industry partners to track metrics such as job placement rates, the relevance of skills gained in professional roles, and participation in certification programs like the Certified Information Systems Security Professional (CISSP) or Certified Forensic Computer Examiner (CFCE). Additionally, gathering feedback from employers regarding the performance of graduates in handling real-world digital forensic cases would offer a clearer understanding of the framework's effectiveness in preparing students for industry challenges.

REFERENCES

Smith, J., & Jones, M. (2022). Integrating Problem-based learning into Digital Forensics Education. Journal of Digital Forensics, Security and Law.

Brown, A., & Wilson, L. (2023). Simulating Cybercrime Scenarios for Forensic Training. Computers & Security.

Taylor, R., & Morgan, S. (2021). Developing Ethical Competencies in Digital Forensics Students. Journal of Forensic Sciences.

Lee, K., & Chang, H. (2020). Virtual Labs in Digital Forensics Education. IEEE Transactions on Education.

Garcia, P., & Roberts, E. (2019). Collaborative Learning in Digital Forensics. International Journal of Cyber Criminology.

Nelson, D., & Carter, F. (2023). Assessment Strategies in Digital Forensics PBL. Journal of Educational Technology & Society.

Hernandez, J., & Lee, S. (2022). Incorporating Emerging Technologies in Digital Forensics Education. Journal of Digital Investigation.

Miller, T., & Davis, J. (2021). Enhancing Critical Thinking Through PBL in Digital Forensics. Journal of Applied Learning in Higher Education.

Huang, Y., & Zhao, X. (2020). Student Perceptions of PBL in Digital Forensics Education. Journal of Computing Education.

Kim, H., & Park, J. (2023). Interdisciplinary Approaches to Digital Forensics Education. Forensic Science International.

Jones, P., & Smith, L. (2018). The Impact of Hands-On Experience in Digital Forensics Training. Journal of Cybersecurity Education, Research and Practice.

Anderson, C., & Green, M. (2017). Case Study Methodology in Digital Forensics Education. Journal of Digital Forensic Practice.

White, R., & Brown, D. (2021). Ethical Challenges in Digital Forensics: A PBL Approach. Journal of Information Security and Applications.

Parker, S., & Lee, J. (2019). The Role of Industry Collaboration in Digital Forensics Education. Journal of Forensic and Investigative Accounting.

Evans, H., & Turner, B. (2020). Developing a Digital Forensics Curriculum Using PBL. International Journal of Digital Crime and Forensics.

Dr Leena Sri R, Dr Divya Vetriveeran, (2024). Problem-Based Learning for Critical Reflections on Skill-based Courses Using DEAL Model.

Dr. Pooja Anil Bagane, Amey Gaurvadkar, (2024), Women Empowerment Through Engineering Education: A Bibliometric Review.