VR Cybercrime Scene Investigation Lab

Dolar Paddhariya[1], Prasann Bhatlawande[1], Vaibhav Tarte[1], Prof. Chiranjit Das[1] and Dr. Deepika Ajalkar[1]

[1]G H Raisoni College of Engineering & Management, Pune, India

Abstract: The VR Cybercrime Scene Investigation Lab is an innovative project that aims to connect theoretical knowledge with practical skills in digital forensics training. Traditional methods like lectures and case studies provide limited chances for hands-on investigation. To fix this, the Cybercop Project creates an immersive virtual reality environment where students take on the role of investigators dealing with advanced cybercrimes. Learners can explore realistic simulated crime scenes, including hacker workspaces and compromised offices. They collect and analyze digital evidence such as USB drives, phishing emails, and suspicious server logs. The lab also includes a live-mode forensic kit management system with real-time feedback, which helps students understand the correct procedures. By combining VR technology, interactive content, and scenario-based learning, the project offers a cost-effective, scalable, and engaging platform that not only improves forensic skills but also develops critical thinking, problem-solving abilities, and readiness for real-world cybersecurity challenges.

Keywords: Virtual Reality, Cybercrime Investigation, Digital Forensics, Cybersecurity Education, Immersive Training, Forensic Skill Gap

1. Introduction

Basically, a cybercrime refers to unauthorized access to a computer, network, or internet without any legal permission. It has evolved significantly since the 1970s, when incidents largely involved unauthorized access to mainframe systems. Today, advanced threats such as ransomware, phishing, identity theft, and large-scale intrusions pose serious risks to governments, industries, and individuals worldwide. This rapid escalation has highlighted the importance of Digital Forensics, which is about finding and protecting digital information, studying it carefully, and then presenting it in a way that can be trusted and used in legal cases.

1.1 Problem, Motivation, and Proposed Work Overview

Cybercrime, encompassing unauthorized access, data theft, and sophisticated malware attacks, has evolved rapidly since the 1970s, now posing severe economic and national security threats globally [11, 12]. This escalation underscores the critical role of Digital Forensics, which is the rigorous process of preserving, identifying, extracting, documenting, and interpreting digital evidence for legal proceedings. Despite this necessity, forensic education in most academic institutions is predominantly theory-driven and logistically constrained by the high cost and limited scalability of maintaining physical, up-to-date forensic laboratories [14]. This creates a critical disconnect between theoretical knowledge and the practical, hands-on competencies required by professional investigators, contributing to a growing skills gap in the cybersecurity sector [8, 9].

To address this challenge, we propose and develop the VR Cybercrime Scene Investigation Lab. This innovative, scalable, and affordable platform utilizes immersive Virtual Reality (VR) to replicate complex cybercrime incidents in a realistic, risk-free virtual environment. The core motivation is to transform passive learning into active, scenario-based practice. Learners step into simulated crime scenes, such as a breached corporate office or a hacker's workstation, to perform end-to-end digital investigations. The proposed work provides a comprehensive overview of the system's architecture, development workflow, and the design of embedded forensic tools for analyzing digital artifacts like phishing emails, malicious USB drives, and manipulated server logs. By fully embedding a chain-of-custody workflow and automated performance feedback, the platform offers a uniquely practical training solution that is both cost-efficient and easily updated to reflect emerging cyber threats.

1.2 Comparative Analysis and Research Gap

Virtual Reality has been widely recognized for its potential in forensic science and crime scene investigation (CSI) training [2]. Studies have demonstrated that VR simulations significantly enhance student engagement and skill acquisition [2, 7] and offer powerful opportunities for collaborative investigation in digitized scenes [3]. Extended Reality (XR) tools, including VR, improve accessibility and reproducibility in educational settings [4].

However, a comparative analysis of existing research reveals a critical limitation. As summarized in Table 1, the majority of successful VR applications in forensics, such as those discussed by Rinaldi et al. [3] and Lee and Park [9], overwhelmingly concentrate on physical evidence (e.g., blood spatter, ballistics, scene reconstruction) or the analysis of VR device artifacts themselves [5, 6]. While valuable, these systems do not provide a practical, immersive experience in digital evidence handling and analysis. For instance, existing educational tools often teach the theory of examining a phishing email or server log, but rarely place the learner in a scenario where they must physically locate the source, secure the digital file, and use an in-VR tool to perform the analysis while maintaining an authentic chain of custody.

Feature	**Physical Forensics VR [2, 10]**	**Digital Forensics Training (Traditional) [14]**	**VR Cybercrime Investigation Lab (Proposed)**
Focus	Physical evidence (e.g., blood, objects, scene layout)	Theoretical knowledge, case studies, and command-line usage	**Hands-on Digital Evidence Workflow**

Scalability	Medium (Requires scanning/modeling new scenes)	Low (Requires physical lab resources, high maintenance)	**High (Modular scene/case design in Unity)**
Evidence Type	Physical artifacts	Static data sets, documents	**Interactive digital artifacts (Emails, logs, USBs)**
Workflow	Scene reconstruction, physical evidence tagging	Reading about the procedure	**Full, immersive *collect-analyze-report* loop**
Cost	High (Specialized hardware/photogrammetry)	High (Physical lab setup and maintenance)	**Low (Basic VR headset and software)**

Table 1: Comparative analysis of existing training approaches and the proposed VR lab.

Our work directly addresses this research gap by creating a novel system that integrates a high-fidelity VR environment with the complete digital forensics workflow. We extend the concept of immersive training by focusing specifically on the interaction with digital artifacts within a physically realized virtual space, a feature largely absent in current training systems. This combination of immersive location-based learning and practical digital tool usage offers a unique and more effective preparation method for future cyber investigators.

1.3 Architecture and Paper Structure

The proposed system utilizes a modular architecture designed for scalability and real-time interaction, as illustrated in Figure 1. The framework is divided into five main functional domains: VR Environment Design, Evidence and Interaction Logic, Backend Simulation, Scoring and Feedback, and Iterative Testing and Deployment. The core functionality is built using Unity 2022 LTS, leveraging the XR Interaction Toolkit for immersive interaction.

The remainder of this paper is structured as follows: Section 2 details the related work, formally defining the research gap. Section 3 outlines the modular system architecture and component design. Section 4 describes the materials, methods, and the in-VR tools implemented. Section 5 presents the demonstrative results and prototype findings. Finally, Section 6 concludes the paper and discusses future enhancement directions.

2. Related Work

[1] Virtual reality has been extensively employed in forensic training to enhance realism and engagement. Mayne and Green [2] confirmed that VR simulations significantly boost student involvement and practical skill development. The potential for collaborative investigation in digitized CSI environments was highlighted by Rinaldi et al. [3], emphasizing multi-user capability. Furthermore, a review of extended reality (XR) tools by Change et al. [4] indicated that immersive platforms improve the accessibility and reproducibility of forensic educational content. Studies have also explored the forensic analysis of artifacts from VR devices, such as the Meta Quest 2 [5], and the potential of web-based VR worlds for digital forensics training [6].
However, the prevailing focus remains centered on physical elements. While systems exist for VR device analysis, few provide an integrated, hands-on environment for practicing the

core workflow of digital evidence collection and analysis (phishing, log analysis, malware traces) within a simulated crime scene setting. Patel and Singh's work [13] addressed the teaching of Chain of Custody using VR, but the scope was limited to procedural understanding. Our work distinguishes itself by combining a fully immersive crime scene investigation environment with interactive, scenario-specific digital artifacts and embedded forensic tools, establishing a crucial link between theoretical chain-of-custody concepts and the practical execution of digital forensics. This deliberate fusion is the key differentiator and fills the gap identified in Table 1.

3. VR Model and System Architecture

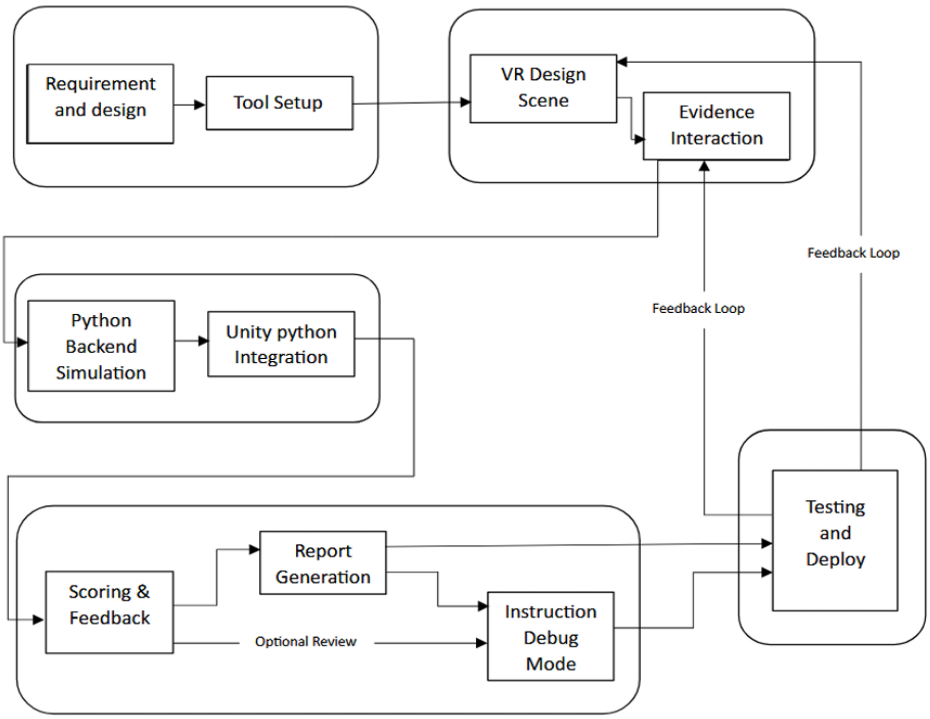


Figure 1: Workflow of the VR Cybercrime Scene Investigation Lab. The design integrates VR scene creation, evidence interaction, backend simulation, scoring, and feedback, and final deployment with iterative feedback loops [16].

3.1. Architecture

Figure 1 shows the system of the VR Cybercrime Scene Investigation Lab. The development of the VR Cybercrime Scene Investigation Lab followed a clear process to create an effective training tool that can grow with user needs. We began by defining the investigation goals and setting up the required software and hardware. We used Unity along with the XR Interaction Toolkit to build the VR environment. Next, we designed immersive 3D scenes that mimic real workspaces where users can interact with digital evidence, such as phishing emails, USB drives, and server logs. We built the backend simulation directly in Unity using C# scripts, with some Python modules that support real-time forensic analysis to simulate attacker behavior. To monitor user performance, we added a scoring and feedback system that logs interactions and evaluates how accurately users make decisions based on forensic methods. At the end of each case, the system automatically generates detailed investigation reports. An

optional debug mode also allows instructors to review user actions and give targeted feedback. The whole development process was iterative and included testing and deployment phases with user feedback to improve the VR experience, backend logic, and evidence handling.

3.2. VR Training Model and Assumptions

We assume:

• Trainees understand how to operate VR devices and engage with the simulation.
• The virtual environment mimics real-world scenarios, with objects and hazards acting realistically.
• VR hardware and software work properly, offering real-time feedback for effective learning.
• Skills practiced in VR are expected to transfer safely to real-world situations.

4. Materials and Methods

4.1. Tools and Technologies Used

• Unity 2022.3 LTS with XR Interaction Toolkit is used for immersive VR development and interaction design.
• Meta Quest 2 or PC VR serves as the primary hardware platform for testing and deployment.
• Pro Builder and Unity Asset Store packages are used to model office spaces, server rooms, and virtual workstations.
• C# scripting is used to manage evidence logic, scene interactions, and in-VR forensic analysis.
• Text Mesh Pro supports clear, scalable UI rendering within VR environments.
• Blender is optionally used to design custom 3D assets such as USB drives, laptops, and terminals.
• Audacity and Eleven Labs may be used for voiceover creation and immersive audio integration.

4.2. System Architecture

The system has a modular and flexible structure. Each forensic case scenario is contained within its own Unity scene. This setup provides a clear separation of responsibilities and allows for independent development and testing. A centralized Evidence Manager class keeps track of collected evidence, storing details like source, type, and analysis status. Meanwhile, a Score Manager module calculates task accuracy and creates a final performance score. All processing occurs locally in Unity, so there is no need for external APIs or cloud services. Voice guidance uses event-triggered audio playback, and immersive in-VR interfaces are available for analysis tasks such as log review, email inspection, and hash verification.

4.3. Development Workflow

The development workflow for the VR Cybercrime Scene Investigation Lab was carefully planned to ensure scalability and user engagement. It began with designing specific forensic scenarios, such as phishing investigations, suspicious USB analysis, and unauthorized server access. Using Unity and Pro Builder, we built detailed 3D virtual environments that replicate realistic office and server room settings. Interactive props were placed to encourage natural user interaction.

Key development steps included:

- Designing immersive scenes (e.g., computer labs, classrooms) with appropriate lighting and spatial audio.

- Implementing XR Grab Interactable components and Unity Events to enable grabbing and interacting with evidence.
- Developing modular logic for evidence collection through C# scripts, including tracking collected evidence and listing it.
- Creating in-VR UI panels for forensic tools, such as an email analyzer, a log viewer with time-based filtering, and a hash checker.
- Building automated reports that summarize user actions and investigation outcomes.
- Testing and preparing the system for deployment on Meta Quest.

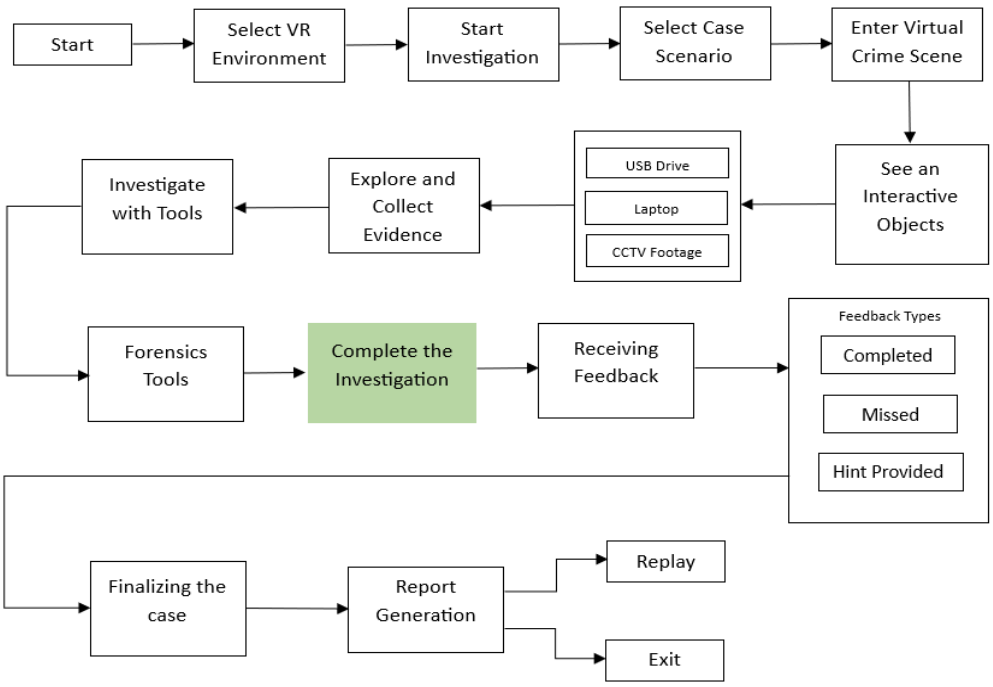


Figure 2: Overview of the VR case report generation process, from evidence collection to in-VR report display.

4.4. Case Flow (Game Flow)

Each case follows the general flow:
VR briefing
→ scene exploration
→evidence collection
→ in-VR analysis
→ decision making
→ score evaluation
→ case report.
This structure allows for modular scaling, enabling new cases to be added easily without modifying the core logic.

4.5. Scoring and Feedback Mechanism

To track user performance during investigations, we implemented a modular scoring system in Unity. The Score Manager script awards or deducts points based on how accurately users collect and analyze evidence. For instance, identifying a phishing email correctly gives +10 points; while mislabeling it results in a penalty. Real-time feedback is displayed using a Text Mesh Pro-based UI overlay that updates the score and highlights correct/incorrect decisions. This immediate response helps reinforce learning while maintaining immersion.

4.6. Voice Interaction and Narration

To reduce reliance on on-screen instructions, we used AI-generated voice narration from Eleven Labs. Audio cues activate through Unity Events at crucial points, like case briefings, hints, and mission completions. For instance, when entering the phishing case, users hear: "Investigate the email and determine if it is legitimate." This helps guide users, especially those who are new, and improves overall accessibility and immersion.

4.7. Report Generation

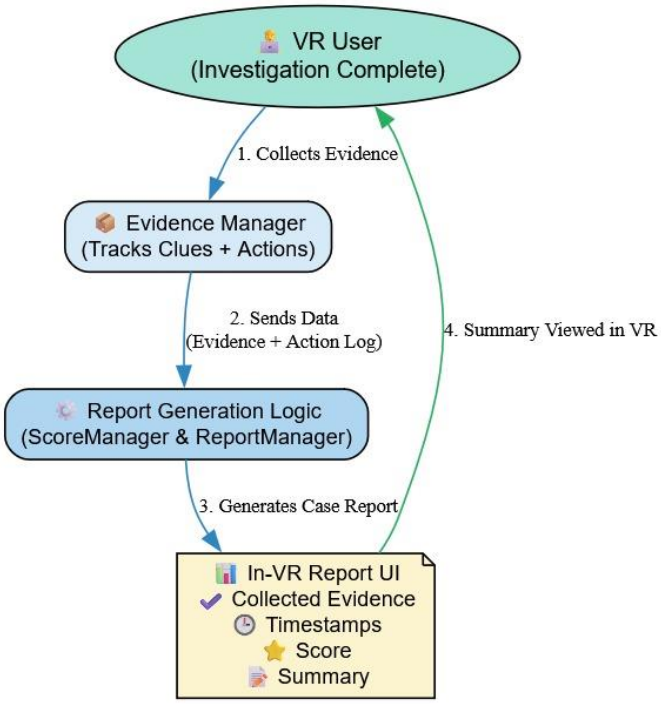


Figure 3: In-VR report display: the final case report appears on a scrollable canvas inside the scene.

At the end of each case, the application generates a dynamic case report that summarizes the user's performance. Instead of exporting to external formats like PDF or JSON, we display the report inside VR on a scrollable canvas. It includes key details such as evidence collected, timestamps of actions, correct and missed clues, and total score. The design was kept minimal to avoid overwhelming the user and maintain immersion

4.8. Modular Scene Design and Future Growth

To support future growth, each forensic case was built as a separate Unity scene. Evidence items were created as prefabs with standard fields such as evidence Name, evidence Type,

and clue Weight. Forensic tools, such as the email analyzer and log viewer, are modular and reusable. New scenarios can be added by duplicating existing scenes and linking them to shared managers like Score Manager and Evidence Manager. The system is also designed to support future extensions, including multiplayer investigation.

5. Methodology

5.1. Overview

The VR Cybercrime Scene Investigation Lab features a structured process for solving cases that closely mimics a real-world digital forensics workflow. It guides the learner through an engaging investigation where they can find, examine, and record clues using specially designed in-VR tools. All interactions and logic are implemented within Unity, utilizing the XR Interaction Toolkit and C# scripting to provide seamless and interactive functionality.

5.2. Investigation Flow (User Perspective)

The VR application uses a modular "investigate–analyze–report" loop that remains consistent across all scenarios. Each case proceeds through the following phases:

- Case Briefing– Provides background and objectives of the investigation.
- Scene Exploration– Allows the learner to explore the virtual environment.
- Evidence Interaction– Engages with digital artefacts such as emails, USBs, or logs.
- In-VR Forensic Analysis– Analyzes collected evidence using embedded forensic tools.
- Decision-Making– Learners make choices based on analysis outcomes.
- Final Report Generation– Produces a structured forensic report.

5.3. Scene Design and Navigation

Each scenario is designed as a separate Unity scene (e.g., office, server room). XR Teleportation and Ray Interactor components are used for navigation and interaction. Scene design focuses on realism, with appropriate spatial audio and lighting to simulate the investigation environment.

5.4. Evidence Management System

All clues are tagged with metadata using a custom Evidence Item script. These items are collected via XR Grab Interactable and stored in a runtime Evidence Manager singleton, which tracks interaction state, status (analyzed/unanalyzed), and forensic relevance.

5.5. Built-in Forensic Tools

To improve the educational experience and give learners chances to practice real-life digital investigations, the system provides a set of interactive forensic tools in the VR environment. Each tool is designed as a reusable UI panel in Unity and becomes active when the user interacts with specific evidence elements.

5.6. Scoring and Feedback System

To make the investigation more engaging and measurable, we added a scoring system in the VR lab. Correct actions earn points, while missing or mishandling evidence lowers the score. Instant feedback messages (e.g., "Correct Evidence Found") help learners recognize their mistakes and improve immediately.

5.7. Report Generation

At the end of every case, the system automatically creates an investigation report within the VR environment. This report summarizes the learner's work, including evidence collected, analysis steps, decisions, and the final score. The report appears on a scrollable 3D panel in

front of the user, providing a clear summary while keeping the user in VR.

5.8. Scalability and Future Enhancements

The project is designed to be extensible. Crime scenes are created as separate Unity scenes, and evidence items and tools are stored as reusable prefabs. Future work includes handling more complex cases, implementing multiplayer support, addressing AI-driven threats, and offering optional cloud case updates.

6. Result

6.1 Findings Related to Research Gap

- Traditional digital forensics education is primarily theory-focused and provides very limited opportunities for practical, hands-on training.
- Physical forensic laboratories are costly to establish, require continuous updates, and lack scalability to meet the rising demand for cybersecurity education.
- As a result, students often have minimal scope for realistic, hands-on investigation practice

6.2 How Our Project Overcomes It

- To bridge the gap created by traditional theory-based learning, our VR Cybercrime Scene Investigation Lab gives students the chance to step into a simulated investigation environment. Inside this space, they can collect evidence, analyze logs, and generate reports similar to real forensic work.
- In response to the high cost of physical labs, our project introduces a low-cost, repeatable, and easily accessible training platform that can be set up in any institution with basic
- VR equipment.
- To tackle the lack of practical investigation practice, the system creates a safe and risk-free environment where students can experiment, learn from mistakes, and still follow proper forensic procedures without the risk of damaging real systems.

6.3 Prototype Demonstration

6.3.1. Asset Creation: Environment Design

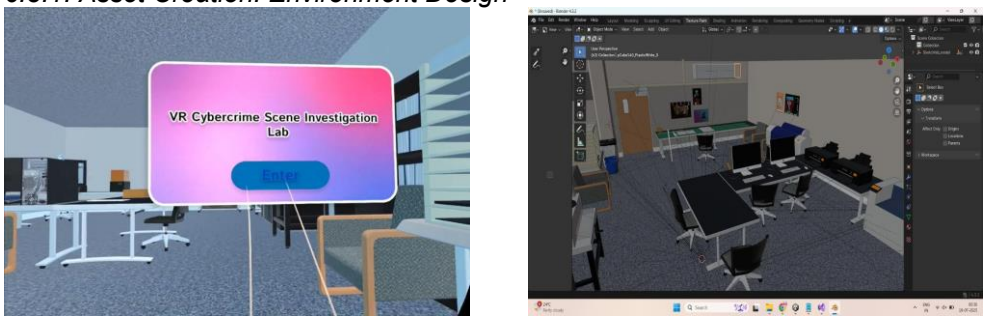
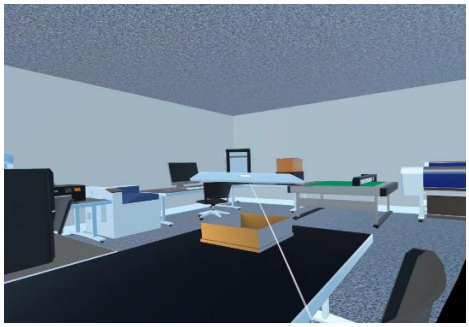


Figure 4: As shown in Figure 3, the VR Cybercrime Scene Investigation Lab opens with a simple and interactive entry screen. This acts as the starting point for learners, making it easy for them to enter the virtual environment and begin exploring forensic training activities.

6.3.2. Evidence Collection Phase: Report generated on the collected evidence.



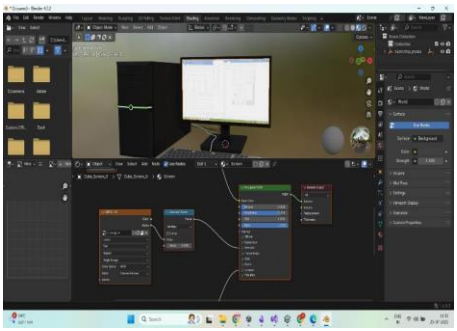


Figure.5: In this step, the VR Cybercrime Scene Investigation Lab lets users move beyond just collecting evidence to exploring it in detail. The system offers a computer interface where learners can interact with digital files, system logs, and other artifacts. This hands-on method helps students practice identifying suspicious data, tracing potential security breaches, and understanding how real-world investigations are conducted. By simulating the analysis process, the lab makes it easier for learners to link theory with practical skills in a safe and controlled setting.

6.3.3 Report Generation: Final Output

Figure.6: At the end of the investigation, the system creates a report that summarizes the user's performance. It shows important details like the task completed, time taken, and overall score. This feedback helps learners assess their progress, pinpoint areas that need improvement, and understand how well they managed the evidence collection process.

7. Discussion

The results demonstrate the feasibility and promise of leveraging Virtual Reality to significantly enhance digital forensics training, offering a substantial improvement over traditional, theory-heavy methods. Our analysis confirms the growing gap between the escalating number of cybercrime incidents and the slow pace of trained professional production [8, 9]. The VR Cybercrime Scene Investigation Lab directly addresses this need by offering a training method that is both highly effective and scalable.

The core strength of this platform is the creation of a safe, repeatable, and practical environment for investigation. Learners actively engage with the full forensic lifecycle—from scene entry and evidence collection to in-VR analysis and formal report generation—under simulated pressure but without real-world risk. This active approach is significantly more practical and engaging than traditional classroom instruction [15]. Furthermore, the system resolves the logistical barriers of physical labs by providing an affordable and easily updatable alternative that only requires basic VR hardware.

While the system successfully validates the concept of immersive digital forensics training, a few challenges remain. Current implementation relies on platforms like the Meta Quest 2, which may present an accessibility barrier for some institutions. Large-scale empirical testing

with diverse student cohorts is essential to validate the effectiveness of skill transfer to real-world scenarios quantitatively.

Overall, this VR-based training platform represents a promising shift towards making cybersecurity education more practical and accessible. With continued refinement, it holds the potential to substantially reduce the skills gap in the digital forensics field.

8. Conclusion

The primary objective of this project was the successful development of the VR Cybercrime Scene Investigation Lab, a platform that effectively merges theoretical knowledge with practical experience in digital forensics education. Our study successfully demonstrated that Virtual Reality provides an engaging, low-cost, and highly scalable solution for providing an authentic cybercrime case investigation experience.

In contrast to traditional, costly physical laboratories and passive learning methods, our VR platform offers a safe and repeatable setting where learners can diligently practice evidence collection, perform log analysis, and author formal reports, all while strictly adhering to proper forensic procedures. The results suggest that VR-based labs can be a valuable addition to universities, corporate training centers, and law enforcement academies globally, making cybersecurity education more dynamic, accessible, and ultimately, more practical.

For future work, we recommend several key extensions: incorporating more complex forensic scenarios (e.g., memory analysis, mobile device forensics), implementing multi-user collaboration features to enable team investigations, and conducting rigorous large-scale efficacy studies in real classroom settings to formally assess learning outcomes.

9. Acknowledgment

We express our sincere gratitude to our guide and faculty at the Department of Cybersecurity, G.H. Raisoni College of Engineering and Management, Pune, for their continuous guidance and encouragement. Their essential advice and support throughout the project were instrumental in translating our conceptual ideas into a fully functional system. We also thank our classmates and friends who contributed valuable suggestions, tested early versions of the VR Cybercrime Scene Investigation Lab, and motivated our iterative improvements. Lastly, we are grateful to our college for providing the necessary facilities and resources for this work.

References

1. E. Casey, Digital Evidence and Computer Crime: Forensic Science, Computers, and the Internet, 4th ed. (Elsevier Academic Press, 2019).
2. J. Mayne and I. Green, “Virtual Reality in Crime Scene Training: Enhancing Engagement and Learning,” Forensic Science International, 310, 110–119 (2020).
3. F. Rinaldi, M. Conti, and G. Dini, “Collaborative Forensic Investigation in Virtual Environments: Opportunities and Challenges,” Journal of Digital Forensics, Security and Law, 17 (1), 23–40 (2022).
4. L. Chango, S. Vega, and M. Perez, “Extended Reality Tools for Forensic Education: A Review,” Computers & Education: XR Special Issue, 185, 104–118 (2023).
5. T. Raymer, “Forensic Artifact Analysis in VR Devices: Case Study of Meta Quest 2,” in Proc. Int. Workshop on Emerging Cybersecurity, IEEE, 77–86 (2023).
6. C. Silva, A. Romero, and L. Ortega, “Exploring Web-based Virtual Reality Worlds for Digital Forensics Training,” Forensic Science International: Digital Investigation, 45, 301–312 (2023).

7. S. Farrell and D. Holmes, "Immersive Learning for Cybersecurity Education: A VR-based Approach," in Proc. ACM Conf. on Computing Education Research, 199–210 (2021).
8. A. Smith and P. Johnson, "The Rising Skills Gap in Cybersecurity: Causes and Solutions," Cybersecurity Journal, 12 (2), 101–118 (2019).
9. INTERPOL, "Global Cybercrime Report 2022: Emerging Trends and Skills Gap," Interpol Cybercrime Directorate, Tech. Rep. (2022).
10. H. Lee and S. Park, "Virtual Reality for Police Training: Case Study in Digital Evidence Handling," in IEEE VR Conference, 112–121 (2021).
11. D. Kaplan and R. Miller, "Cybercrime Trends 2020: Global Challenges and Future Outlook," Journal of Cyber Policy, 5 (3), 275–292 (2020).
12. M. McGuire, "The Hidden Costs of Cybercrime," Centre for Strategic and International Studies (CSIS), 1–56 (2021).
13. N. Patel and R. Singh, "Using Virtual Reality to Teach Chain of Custody in Digital Forensics," in Proc. ACM SIGCSE Conference, 455–462 (2021).
14. S. Green, "Limitations of Traditional Digital Forensics Education," Education and Information Technologies, 23 (4), 1725–1738 (2018).
15. R. Bahl and D. Sharma, "Gamification and Immersive Learning for Cybersecurity Training," Computers & Security, 112, 102512 (2022).
16. Weiss Jr., E.G., "The Future of Forensic Training: Why Virtual Reality Is Here to Stay." LinkedIn Pulse, Aug. 18, 2025.