Design of Experimental Teaching System of "Network Crime Investigation" Based on Virtual Simulation

Guangxuan Chen[1,a], Qiang Liu[1,b], Anan Huang[1,c], Bo Hu[1,d], Guangxiao Chen[2,*]

{chenguangxuan@zjjcxy.cn[a], liuqiang@zjjcxy.cn[b], huanganan@zjjcxy.cn[c], hubo@zjjcxy.cn[d], ericcgx@163.com[*]}

Zhejiang Police College, Hangzhou, China[1], Wenzhou Public Security Bureau, Wenzhou, China[2]

Abstract. As a highly practical course, the teaching design of "Network Crime Investigation" should pay more attention to the design of experimental content. This article designs a virtual simulation based experimental teaching platform for the teaching needs of conducting online crime investigation experiments, and designs a student-centered experimental teaching system based on the platform, providing platform support for the effective implementation of the "Network Crime Investigation" course teaching.

Keywords: Investigative experiment, curriculum design, experimental teaching

1 Introduction

The Cybersecurity and Law Enforcement major mainly studies the basic knowledge and skills of cybersecurity, cybercrime investigation, and criminal law enforcement. It ensures cybersecurity in departments such as public security and prosecution, and prevents and investigates cyber crimes such as illegal intrusions and malicious attacks. Especially in recent years, the rampant forms of new types of cybercrime have highlighted the importance of cybersecurity and law enforcement.

At present, courses in the field of cybersecurity and law enforcement mainly include three major parts: first, basic courses in public security, such as criminal investigation, criminology, criminal psychology, introduction to public security, public security management, and crime scene investigation; The second is professional basic courses, such as advanced language programming, data structure, operating system principles, computer networks, database principles and applications, etc; The third is professional compulsory and elective courses, such as information security technology, digital forensics technology, mobile forensics technology, data recovery technology, big data technology principles and applications, artificial intelligence and applications, network crime investigation, etc. Due to the fact that most of these courses are modular, conventional experimental training teaching cannot cover all types of experiments, especially some unreachable or irreversible experimental types (such as digital forensics, online crime scene investigation, etc.), which have not been well integrated and form a complete practical experimental training course system, making it difficult to replicate experimental scenes and weak coherence of experimental modules in various practical teaching links. On the other hand, due to the continuous development and iterative upgrading of the models of cybercrime and new types of crime, their means and

ICMEIM 2023, September 08-10, Wuhan, People's Republic of China

DOI 10.4108/eai.8-9-2023.2340079

technologies are also constantly evolving. Traditional and dispersed cybercrime investigation experimental training modules are difficult to respond to the diverse and diverse needs of practical experiments in the new business environment in a timely and effective manner, making it difficult for students to carry out practical operations in actual on-site experimental environments, and unable to effectively integrate theory with practice.

Therefore, focusing on the practical needs of crime investigation and exploring the construction of a practical network crime investigation experimental training system is of great significance for connecting various course modules and improving the teaching level and practical training level of network security law enforcement in public security colleges.

2 Investigative experiment

2.1 Overview of investigation experiments

"Investigative experiment" can have different meanings depending on the context, but generally it refers to a type of experiment that is designed to investigate a particular hypothesis or question. In the context of scientific research, an investigative experiment involves the systematic testing of a hypothesis or theory by manipulating variables and observing the outcomes. This type of experiment is often conducted in a controlled environment, such as a laboratory, to ensure that the results are reliable and valid [1].

In the context of criminal investigations, an investigative experiment may refer to a simulation or reconstruction of a crime scene to test various hypotheses or to gather evidence. This type of experiment is often conducted by forensic experts and law enforcement agencies to help solve crimes and identify suspects [2].

Regardless of the context, an investigative experiment typically involves careful planning, attention to detail, and the use of appropriate tools and techniques to ensure accurate and reliable results.

2.2 Conducting investigation experiments

The process of conducting an investigative experiment can vary depending on the specific context and research question, but here are some general steps that can be followed:

Formulate a research question or hypothesis: Identify the question or hypothesis that you want to investigate. This should be a clear and testable statement that you can use to guide your experiment.

- Design the experiment: Decide on the experimental design that you will use, including the variables that you will manipulate and measure, and the procedures that you will follow. Make sure that your design is appropriate for your research question and that it will allow you to obtain reliable and valid results.
- Gather materials and equipment: Collect all of the materials and equipment that you will need to conduct your experiment. This may include chemicals, instruments, or other specialized tools.

- Conduct the experiment: Follow the procedures that you have designed and carry out the experiment. Be sure to record all of your observations and measurements accurately.
- Analyze the data: Once you have collected your data, analyze it to determine whether your hypothesis has been supported or not. This may involve statistical analysis or other methods, depending on the nature of your experiment.
- Draw conclusions and report your findings: Based on your analysis, draw conclusions about your research question or hypothesis. Write up your findings in a report or manuscript, including a description of your experimental design, methods, results, and conclusions.
- Evaluate your experiment: Reflect on your experimental design and procedures to identify any limitations or weaknesses. Consider how you might improve your experiment in the future to obtain more reliable or valid results.

Overall, conducting an investigative experiment requires careful planning, attention to detail, and a thorough understanding of the research question or hypothesis that you are investigating.

2.3 Steps of conducting investigation experiments for cyber crime

how to carry out investigative experiment for cyber crime?

Investigative experiments for cyber crimes involve collecting and analyzing digital evidence to identify the source and nature of the crime. Here are some steps to follow for carrying out an investigative experiment for cybercrime:

- Secure the Scene: If possible, isolate and secure the affected system and network. This can help prevent further damage and preserve evidence.
- Document: Document everything that you find, including the date, time, location, and details of the incident. Take screenshots, photos, and videos of any suspicious activity or evidence.
- Identify Evidence: Collect all possible evidence related to the cybercrime. This can include log files, network traffic data, system files, and any physical evidence related to the crime.
- Analyze the Evidence: Analyze the evidence that you have collected to identify the nature of the crime, the source of the attack, and any other relevant details. Use forensic tools to extract and analyze digital evidence.
- Report: Prepare a report detailing your findings and conclusions. This report should include a summary of the incident, the methods used to investigate the crime, the evidence collected, and your conclusions.
- Prosecute: If the evidence suggests that a crime has been committed, you may need to work with law enforcement to bring the perpetrator to justice.

It's important to note that investigating cyber crimes can be complex and challenging. If you're not experienced in cyber forensics, it's recommended that you seek the help of a qualified professional to ensure that the investigation is conducted correctly and legally.

3 Design of investigation experiment teaching platform

In order to better carry out online crime investigation experiments, it is necessary to first have specialized laboratories and experimental platforms. The design concept of the laboratory is as follows.

3.1 Design ideas

The laboratory will focus on security evaluation, malicious code detection, case tracing analysis, APP security evaluation, mobile security evaluation, remote case consultation, data cooperation investigation, data analysis and visualization, network security defense and emergency response drills, and other dimensions of WEB application operation. It will collect multi-level, multi-dimensional, and diversified cyberspace security data, and based on massive data analysis technology, algorithm models, artificial intelligence and other analytical technologies to achieve the goals of teaching, research, and training.

The construction of the laboratory is divided into three levels: firstly, the construction of the laboratory hardware platform; The second is to deploy various platforms based on the teaching, research, and practical application needs of public security and law enforcement and data analysis; The third is the construction of a curriculum system for teaching and practical training.

(1) In terms of experimental environment technology architecture, an open, scalable, and interrelated technology architecture is adopted. The internal experimental modules of each experimental environment can be flexibly organized, and through configuration expansion and tailoring, they can adapt to different scale, distribution levels, deployment flexibility, and structural system system validation operating environments; The experimental environments can be interconnected to support integrated experiments of software and hardware systems and has necessary external interconnection capabilities and can achieve interoperability with other related systems under the same technical standard, meeting the requirements for system access and verification based on different technical standards.

(2) Construct an experimental environment by combining virtual and real methods. Select products that comply with international standard technical systems, take into account future technological development, and have the technical means of "hardware solidification and software upgrade" to achieve reduced investment, economic applicability, and keeping up with the forefront.

(3) In terms of operational control of the experimental environment, it is equipped with experimental control and management methods, capable of controlling and managing the state of the experimental process and nodes, collecting, managing, and statistically analyzing experimental data, and has system performance evaluation methods to complete system performance evaluation. On the basis of completing daily teaching and practical training, professional courses and training courses related to the subject can also be developed.

3.2 Overall framework

The overall framework of the laboratory platform is developed and designed in a multi-level and progressive manner, mainly divided into five levels: resource layer, data layer, interface layer, application layer, and display layer.

The resource layer includes the design of virtualization management platform, deployment of virtual machines, configuration of physical devices such as network facilities and firewalls; The data layer includes courseware library, scenario library, sample library, and other related data; The interface layer includes data storage interfaces, security device interfaces, and resource layer platform interfaces; The application layer includes training module design, competition module design, WEB application security supervision and operation security evaluation for various scenarios, malicious code detection and case tracing analysis, APP security supervision and mobile security evaluation, remote case consultation and data cooperation investigation, data analysis module, etc; The display layer mainly displays the achievements of teaching, learning, training, scientific research, etc., including multi-dimensional visualization display and large screen front-end display. The overall framework is shown in Figure 1.

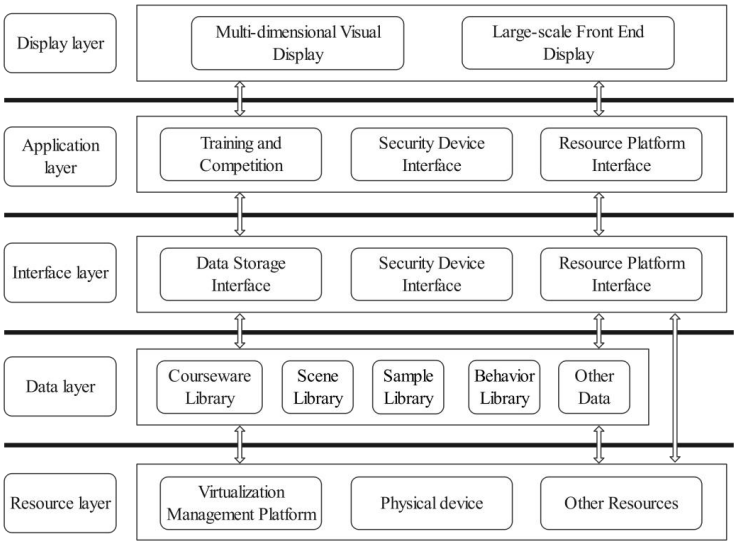

Fig. 1. Overall framework of the laboratory

3.3 Design of virtualization platform architecture

With teaching as the center and practice as the purpose, the virtualization platform covers the functions of cyberspace security, distributed cluster laboratory, topology application, digital forensics, network security event knowledge base, system and application virtual template library, courseware system library, tool set, environment customization, environment reproduction, course upgrading, virtual-real combination, etc., while closely tracking the latest technologies domestic and abroad and upgrading the corresponding systems and equipment and present them in the course [3], [4].

Through dedicated network virtualization devices, the scenarios required for network security cases are virtualized, including baseline scanning, threat analysis, WEB security, Trojan horse analysis, virus analysis, data mining, vulnerability analysis, host security, cloud security, wireless security, firewall, intrusion detection, disaster recovery backup and recovery, cryptography and applications, and security programming [5]. At the same time, it provides students with relevant guidance and experimental environment scenes to meet the teaching needs.

4 Curriculum design

As a highly practical course, the "Cybercrime Investigation" course emphasizes a student-centered approach, allowing students to acquire preview abilities from numerous course resources, internalize them in classroom activities, evaluate their learning, and ultimately continuously improve on the basis of evaluation to achieve refinement and sublimation.

Learner centered curriculum design is a product of human centered philosophical thinking. This curriculum design emphasizes individual development and emphasizes that the organizational form of the curriculum should be based on the needs, interests, and goals of students. The course design follows the process of "resource development, learning first, classroom internalization, evaluation feedback, and discussion summary". Course resource development, mainly including the development of video tutorials, electronic documents, PPTs, audio tutorials, etc; Learning first mainly refers to students' independent learning, collaborative learning, literature review, online learning, and problem-solving activities that are carried out on the premise of fully utilizing various learning media such as books, the internet, and e-books [6]. At the same time, in the classroom stage, knowledge internalization is achieved through channels such as teacher questioning, student experiments, collaborative communication, and knowledge and skill updates. Afterwards, evaluation and feedback will be provided on experimental reports, papers, assessments, collective tutoring, and personalized guidance. Finally, the discussion and summary were conducted through critical reflection, optimization of experimental plans, supplementation of course resources, and group interaction. Classroom internalization and evaluation feedback can promote students' development, while teachers can benefit from discussions and summaries, thereby promoting their own development and further promoting students' development.

5 Conclusion

This article designs a virtual simulation based experimental teaching platform for the teaching needs of conducting network crime investigation experiments. The experimental platform is developed through five layers: resource layer, data layer, interface layer, application layer, and display layer, achieving the aggregation and fusion of multiple resources. At the same time, a student-centered experimental teaching system has been designed based on the platform, gradually advancing from four steps: course resource development, classroom activity development, learning evaluation, and refinement, providing platform support for the effective implementation of the "Network Crime Investigation" course teaching.

Acknowledgments. In this paper, the research was sponsored by the Teaching Demonstration Team of Graduation Morality Cultivation of Zhejiang Province's "14th Five Year Plan" Graduate Education Reform Program under Grant No.47 and 2022 Education and Teaching Reform Program of Zhejiang Police College under Grant No. 20220101.

References

[1] PengK, J.: Research on the Improvement of China's Investigation Experiment System. Journal of Changzhou Institute of Technology(Social Science Edition). Vol. 39, No. 3, pp. 5-9 (2021)

[2] Zavialova, D.V.: Internet Governance, Borders and Jurisdiction in the Context of Crime Investigation. Courier of Kutafin Moscow State Law University , Vol. 2, pp. 155-161(2021)

[3] XiaoQ, D.: Experimental Teaching of Information Security Based on Virtual Simulation. Hindawi Limited. Vol. 1, pp. 1-9 (2021)

[4] MingJ, W.: Enhancing the Course Teaching of Power System Analysis with Virtual Simulation Platform. International Journal of Electrical Engineering & Education. Vol. 60, No.3, pp. 289-312 (2023)

[5] Jin, Z.: Construction and Exploration of Virtual Simulation Experimental Teaching Platform for Network Security and Computer Technology. Journal of Physics Conference Series. Vol. 2173 (2021)

[6] Munna, A.S.: Application of Theories, Principles and Models of Curriculum Design: A Literature Review. International Journal of Multidisciplinary and Current Educational Research, Vol. 3, No. 1, pp. 147-153 (2021)