Journal of Information Systems Engineering and Management
2025, 10(28s)
e-ISSN: 2468-4376
https://www.jisem-journal.com/

Research Article

Design and Implementation of a Practical Training Platform in Digital Forensics: Case Study at the Higher Polytechnic School of Dakar

Okangondo Loshima Jr.[1*], Serigne Modou Kara Samb[2], Mohamed Kaba Keita[3], Doudou Fall[4], Idy Diop[5], Moussa Dethie Sarr[6]

[1] *Student, Mathematics and Computer Science Doctoral School, Faculty of Science and Technology, Cheikh Anta Diop University, Dakar, Senegal.*
[2] *Student, Mathematics, Computer Science and Technology, Faculty of Science and Technology, Iba Der Thiam University, Thiès, Senegal.*
[3] *Student, Computer Engineering Department, Higher Polytechnic School, Cheikh Anta Diop University, Dakar, Senegal.*
[4] *Professor in Computer Engineering, Computer Engineering Department, Higher Polytechnic School, Cheikh Anta Diop University, Dakar, Senegal.*
[5] *Professor in Computer Engineering, Computer Engineering Department, Higher Polytechnic School, Cheikh Anta Diop University, Dakar, Senegal.*
[6] *Professor in Computer Science, Mathematics, Computer Science and Technology Departement, Faculty of Science and Technology, Iba Der Thiam University, Thiès, Senegal.*
Email: [1] juniorokangondoloshima@esp.sn, [2] smkara.samb@univ-thies.sn, [3] keita.mohamed@esp.sn, [4] doudou.fall@esp.sn, [5] idy.diop@esp.sn, [6] mdsarr@univ-thies.sn

ARTICLE INFO

Received: 18 Dec 2024

Revised: 10 Feb 2025

Accepted: 28 Feb 2025

ABSTRACT

This study proposes the design of a platform for practical work in digital forensics within the computer engineering department of the Higher Polytechnic School of Dakar, Senegal. The aim is to reinforce students' training by providing them with practical skills in digital forensics. Using an approach combining questionnaires, interviews and secondary data analysis, we assessed the department's current capabilities and identified expert training needs in the face of rising cybercrime. Our results show the importance of developing this platform to bridge the gap in IT security expertise. This initiative aims to prepare a new generation of investigators capable of responding to digital challenges, both locally and sub-regionally.

Keywords: ESP, UCAD, Forensics, Criminalistics, AWS

INTRODUCTION

The rise in cyber-attacks in Africa, and particularly in Senegal, highlights the urgent need to train professionals capable of responding effectively to digital threats [1], [2]. As technologies rapidly evolve, cybercriminals are exploiting these advances to carry out increasingly sophisticated attacks [3]. Despite this context, African academic institutions, particularly in Senegal, lack practical training programs in digital forensics, creating a mismatch between the needs of the job market and the skills available [4].

To fill this gap, the Computer Engineering Department at the École Supérieure Polytechnique de Dakar is proposing to create a practical training platform in digital forensics. This platform will provide students with concrete tools to develop digital forensics skills through an interactive simulated environment. This study presents the design and implementation of this platform, assessing training needs through questionnaires and interviews with stakeholders, in order to prepare a new generation of digital investigators.

DIGITAL FORENSICS

Digital forensics is a sub-discipline of the forensic sciences dedicated to the identification, preservation, analysis and interpretation of digital evidence collected during computer investigations [5]. It aims to guarantee the integrity and authenticity of evidence so that it can be presented in a legal context.

The technologies employed in digital forensics have evolved significantly in recent years, particularly with the rise of connected objects (IoT), cloud systems and blockchain, which are introducing new challenges in the collection and analysis of evidence [5], [6]. Today, these devices and systems require constant adaptation of investigative methods and tools to remain effective in the face of increasingly complex threats [7].

Areas of specialization include:

1. File forensics: Analysis of logs and files to trace activities carried out on a system.
2. Mobile forensics: Investigation of data on mobile devices (call logs, messages, applications).
3. Network forensics: Monitoring and analysis of network traffic to detect and analyze security incidents [8], [9].

These different branches enable investigators to follow digital leads and establish strong links between criminal activities and digital evidence, an essential aspect in a context where cyberthreats continue to grow.

A. Process on digital Forensics

Digital forensics follows a structured process regulated by international standards such as ISO/IEC 27037, which guide the identification, collection and preservation of digital evidence [10].

Fig 1. Phases of digital forensics [11].

Figure 1 describes the different phases of digital investigation:

Identification: Define the systems or devices to be examined and the relevant data to be collected.

Preservation: Ensure that evidence is not altered during collection.

Analysis: Examine collected data in depth, identifying patterns or recovering deleted information.

Documentation: Rigorous traceability of all stages of the investigation.

Presentation: Communicate results in the form of reports or testimonials within a legal framework [12].

As cyber-attacks escalate and connected devices proliferate, digital forensics is gaining significance, requiring specialized training to equip cybersecurity professionals with the necessary skills to effectively address emerging threats.

B. Types of digital investigation

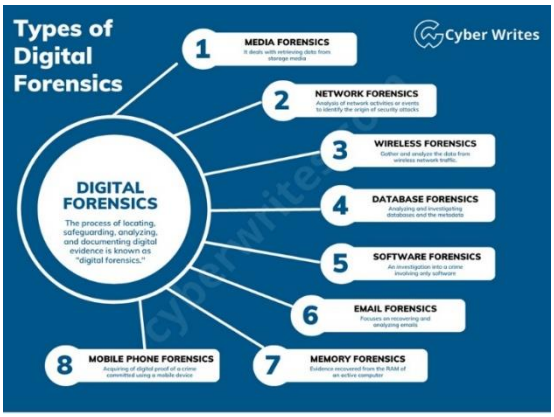

Fig 2. Types of digital Forensics [13]

Figure 2 shows the different types of digital investigation that have been studied to date.

C. Comparative table of digital Forensics learning platforms

To facilitate learning and skills development in this field, many platforms offer a variety of online courses, training and resources. This comparative table below, aims to provide an overview of the main digital forensics learning platforms, highlighting their key features, associated costs and an estimate of the number of users. This information is essential for cybersecurity professionals, students and anyone interested in acquiring digital forensics skills. The data presented is the result of an in-depth analysis based on the platforms' reputation and notoriety in the cyber security community, as well as a qualitative assessment of their offerings and online presence.

Table 1. Comparative Table of Digital Forensics Learning Platforms

Plateforms	Key features	Cost	Number of users
Pluralsight [14]	Extensive library of digital forensics and security courses	Monthly subscription	Several million
Udemy [15]	Offers a variety of courses on digital forensics	Price per course	Several million
Coursera [16]	Offers university courses in digital forensics	Monthly subscription	Several million
Cybrary[17]	Free and fee-based online cybersecurity courses	Free or premium	Several million
SANS Institute [18]	Advanced training in digital forensics and security	Training costs	Several thousand
Digital Forensic Foundations (DFF) [19]	Online course on the basics of digital forensics	Free	Several thousand
Forensic Focus[20]	Online resources, forums and articles on digital forensics	Free	Several thousand
Infosec Institute [21]	Courses and certifications in digital forensics	Training costs	Several thousand
SIFT [22]	Open-source platform for digital evidence analysis	Free	Several million
Offensive Security [23]	Advanced training in digital forensics and ethical hacking	Certification fees	Several thousand
eLearnSecurity [24]	Courses and training in digital forensics and cybersecurity	Training costs	Several thousand

Fig. 3. Comparative table of forensic learning platforms

Figure 3 presents a comparative analysis of 11 forensic learning platforms, highlighting their key features, associated costs, and user base. This comparison aims to provide insights into the strengths and accessibility of each platform for forensic learning purposes.

All these platforms offer high-quality training courses, but they are mainly oriented towards a commercial and theoretical approach, requiring paid subscriptions without providing an immersive practical environment. By contrast, our platform offers free access, but regulated by the computer engineering department of the polytechnic and partner universities, guaranteeing controlled academic use tailored to the specific needs of students. Thanks to the integration of virtualization via AWS, our platform enables students to run simulations in real time, an aspect that fundamentally differentiates it from competing solutions. This practical functionality, coupled with alignment with academic curricula, delivers a more complete and contextualized learning experience, meeting the demands of digital forensics training.

THE NEED FOR DIGITAL FORENSICS IN UNIVERSITIES

The integration of digital forensics into university curricula has become a priority due to the rapid expansion of technologies and the increase in cyberthreats. This need is particularly pressing in developing countries, where growth in the use of the Internet and digital technologies is associated with a rise in online criminal activity [25].

The demand for qualified professionals in digital forensics is rising sharply, whether in law enforcement, private companies or government agencies [26]. To meet this demand, universities need to offer specialized programs covering key topics such as digital evidence acquisition, computer systems analysis, and cybercrime detection. These programs must not only offer theoretical knowledge, but also include practical exercises to develop students' skills in simulated environments.

In addition, the rapid evolution of cyber threats requires digital security professionals to constantly update their skills. Universities can play a key role by offering continuing education and collaborative research opportunities with industries and governments, enabling them to keep pace with technological and criminal developments [27].

Digital forensics represents a unique opportunity for students interested in criminal justice and computer security. By combining digital forensics with other related disciplines, such as law or communication sciences, universities can train professionals better prepared to meet today's cybersecurity challenges. The addition of these programs will strengthen countries' ability to combat cybercrime, particularly in regions where IT security resources are still limited.

ANCILLARY WORKS

Digital forensics has made significant progress, thanks in particular to the development of platforms and tools facilitating the management and analysis of digital evidence. This section examines the main contributions in the field and highlights some of the limitations that justify the development of new approaches.

A. Digital Management and Investigation Platforms

S. Jeon and S. Lee [27] have proposed a management platform for digital forensics technologies, enabling efficient accumulation of resources for use in real investigations. This management system has proved useful for centralizing digital forensics knowledge, but focuses mainly on the operational aspect of investigations without offering a solution for the practical training of future professionals.

Another notable development is that of V. R. Silvarajoo et al [28], who have introduced a digital case management tool for collaborative investigations. This tool improves the traceability and efficiency of investigations by enabling the sharing and analysis of digital evidence between different investigators. However, this solution is limited to case management and does not offer an educational approach or user training.

B. Responses to Cyber Attacks in Developing Countries

In the context of developing countries, Ignus Swart et al [29] have explored the feasibility of visualizing information security on a national scale in South Africa. Their platform provides an overview of the country's security infrastructure, but does not address practical training in digital forensics, a crucial area for the development of IT security skills.

Anass Bayaga [30] has focused on the interoperability of security frameworks in developing countries, notably South Africa. His work stresses the importance of digital security policies, but does not include practical training, a fundamental aspect in strengthening the skills of professionals in this field.

C. Emerging Trends and Challenges in Digital Forensics

A. Tiwari et al [31] studied emerging trends in digital forensics, focusing on challenges such as the investigation of connected objects (IoT) and social network analysis. They highlighted the importance of adapting investigative tools and techniques to these new sources of evidence. However, their study does not propose any concrete solutions for training students or professionals in the analysis of these new technologies.

H. Yun et al [32] have proposed a Digital Forensics Services Platform (DFSP) for the detection of illegal content on the Internet, which can be a major asset given the advent of social networks. This solution, based on a distributed architecture and a content delivery network (CDN), is capable of processing large quantities of data in real time. Although this system is effective for industry, it is not suitable for teaching or training students in digital forensics.

METHODOLOGY

In this study, several methods were used to collect data and assess the feasibility and impact of a digital investigation training platform. The main objective of the methodology is to provide a rigorous analysis of student and teacher perceptions of the implementation of such a platform within the Computer Engineering Department of the École Supérieure Polytechnique de Dakar.

V. 1. Data collection

a) Questionnaire

The main data collection method was a structured questionnaire distributed to students and teachers. The questionnaire was designed to assess participants' knowledge, skills and needs in the field of digital investigation.

Il se divise en cinq sections :

- **Section A: General Information** - This section collects demographic information such as age, gender, and role (student or teacher).
- **Section B: Knowledge and Skills in Digital Investigation** - This section assesses participants' current skills in digital investigation, including whether they have taken courses or participated in practical work in this field.
- **Section C: Training Needs** - Participants are invited to express their perception of the importance of digital forensics skills for their future careers, and to identify the most interesting aspects of this discipline.
- **Section D: Perception of the Training Platform** - This section explores the anticipated benefits of a practical digital forensics training platform, as well as potential challenges to its implementation.
- **Section E: Suggestions and Comments** - Participants are invited to make suggestions for improving digital forensics training within the department.

The questionnaire was distributed to a sample of 300 students and teachers, and the responses were analyzed quantitatively.

b) Analysis of Questionnaire Responses

The responses were analyzed using statistical tools and Python scripts to visualize the results. The results of the questionnaire were represented in graphical form to visualize the following trends:

- Participation in practical digital investigation projects: 92% of respondents (276 out of 300) have already taken part in practical work, indicating a high level of involvement in this discipline.
- Skill levels: the majority of respondents consider themselves to be at beginner or intermediate level, underlining the need to reinforce practical training.
- Anticipated challenges: the main challenges identified include lack of financial resources, technical problems and insufficient teacher skills.

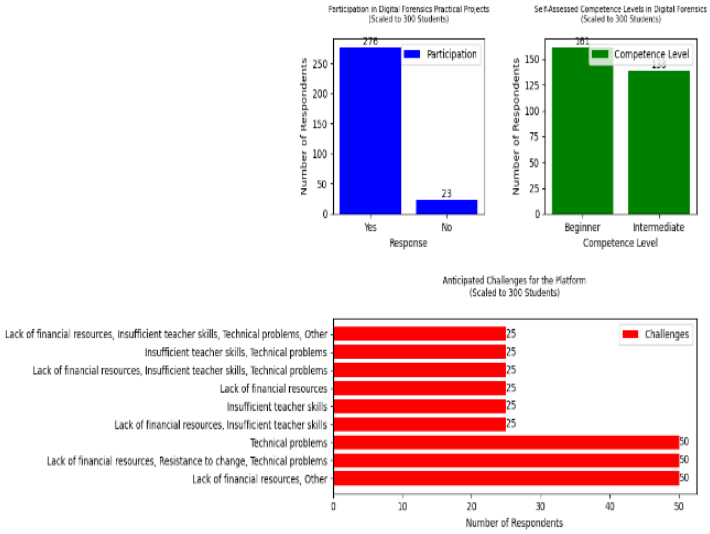

Fig 4. Results of the questionnaire

Figure 4 illustrates the participation, skill levels, and anticipated challenges in practical digital investigation projects. The data reveals a high level of involvement (92%), predominantly beginner or intermediate skill levels, and key obstacles such as financial constraints, technical issues, and limited teacher expertise.

c) Complementary Methods

In addition to the questionnaire, other techniques were used to enrich the analysis and provide a more comprehensive assessment of the platform:

- **Semi-structured interviews**: Interviews were conducted with a sample of teachers and students to gain a deeper insight into their perception of training needs and the challenges they anticipated in setting up the platform. These interviews provided detailed qualitative information, complementing the quantitative data from the questionnaire.
- **Literature review**: The study was based on an analysis of current digital investigation training programs at similar institutions worldwide. This analysis enabled us to compare current practices and identify opportunities for improvement for the proposed platform.

V.2. DATA PROCESSING AND ANALYSIS

The data was processed in three main stages:

- ***Data cleaning***: All incomplete or inconsistent responses were eliminated to ensure data quality.
- ***Quantitative analysis***: Questionnaire results were analyzed using statistical tools to identify key trends. The graphs generated facilitated the visualization of responses and the identification of student and teacher needs.
- ***Qualitative analysis***: Semi-structured interviews were transcribed and analyzed using a thematic approach, in order to identify recurring perceptions regarding the platform's implementation.

V.3. VISUALISATION DES RESULTATS

Quantitative results were represented using histograms and bar charts (see figure 4). These graphs illustrate the key trends observed in participants' responses, including:

- Participation in practical work.
- Skill levels in digital investigation.
- Anticipated challenges in setting up the platform.

SYSTEM ARCHITECTURE

The platform is based on a robust architecture integrating cutting-edge technologies such as Laravel, MySQL and AWS services for machine virtualization. Laravel, a powerful PHP framework, was used to create intuitive user interfaces combining HTML, CSS and JavaScript with the framework. Livewire for front-end dynamism, delivering a fluid, user-friendly experience. In addition, Livewire enables real-time communication with the MySQL database server, ensuring efficient management of user accounts and data. Each learner has a personal account validated by the administrator, guaranteeing secure access to the platform. Once authenticated, the user can access a pre-configured virtual machine, specially designed for practical work in Forensics. These virtual machines are hosted on AWS, offering reliable performance and optimum availability. Pre-configured virtual machines enable learners to concentrate on the practical aspects of digital forensics, without worrying about the technical details of deployment. Each user thus has the resources needed to carry out his or her forensic exercises, while benefiting from a secure environment isolated from the rest of the system.

The platform offers advanced tracking and reporting features, enabling administration to monitor learners' progress and identify areas requiring particular attention. Robust security mechanisms are also in place to protect data integrity and prevent unauthorized access. The Digital Forensics Platform offers a comprehensive and scalable solution for digital forensics training, responding to the growing need for forensic skills in the region. By combining a robust technological infrastructure with a practice-focused pedagogical approach, this solution effectively contributes to building digital resilience and combating cybercrime in Africa.

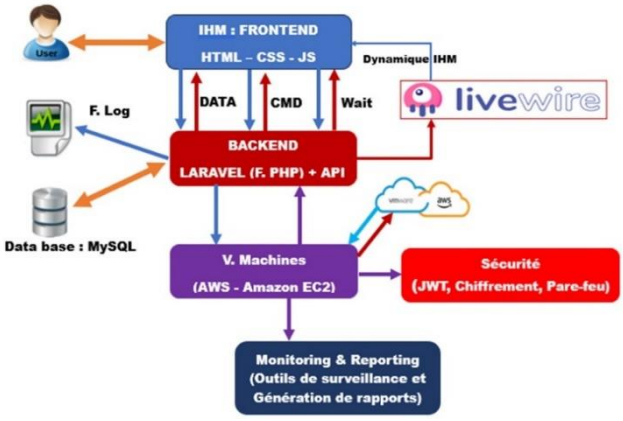

Fig 4. Platform architecture

Figure 4 describes the architecture of the platform, which consists of several interconnected layers. The frontend uses HTML, CSS, JavaScript and Livewire for a dynamic interface. The backend, developed with Laravel (PHP) and APIs, communicates with a MySQL database. Virtual machines are hosted on AWS (Amazon EC2), providing the necessary infrastructure. Security is managed by JWT, encryption and firewall. Monitoring and reporting tools enable performance to be monitored and reports to be generated. This architecture guarantees a robust, secure and scalable platform.

DESIGN AND MODELING

A. Class Diagram

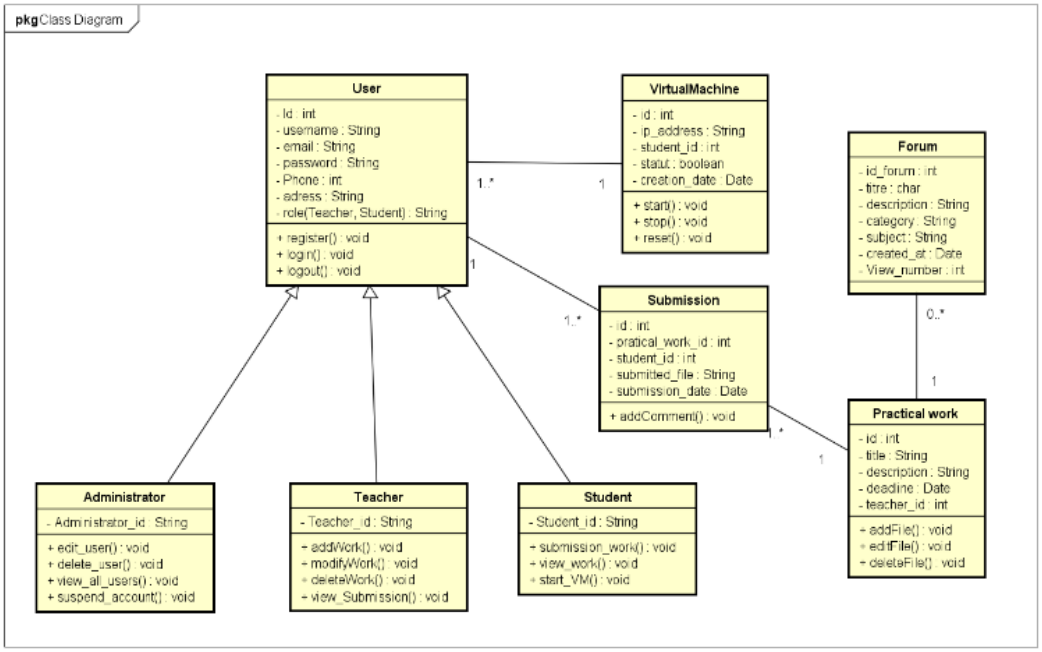

Fig 5. Class Diagram

Figure 5 shows a class diagram, illustrating the various entities and their relationships. The main classes include `User`, which specializes in `Student`, `Teacher`, and `Administrator`, each with specific methods such as practical assignment submission for students, assignment management for teachers, and user and virtual machine management for administrators. The `Submission` class captures details of submitted work, including the student and practical work IDs, and the submission date. The `Practical Work` class contains information on assigned practical work, while `VirtualMachine` manages the virtual machines used by students. Finally, the `Forum` class facilitates discussions between users, completing the platform system. The relationships between these classes are clearly defined, ensuring coherent, structured interaction between the various system components.

B. Sequence diagram

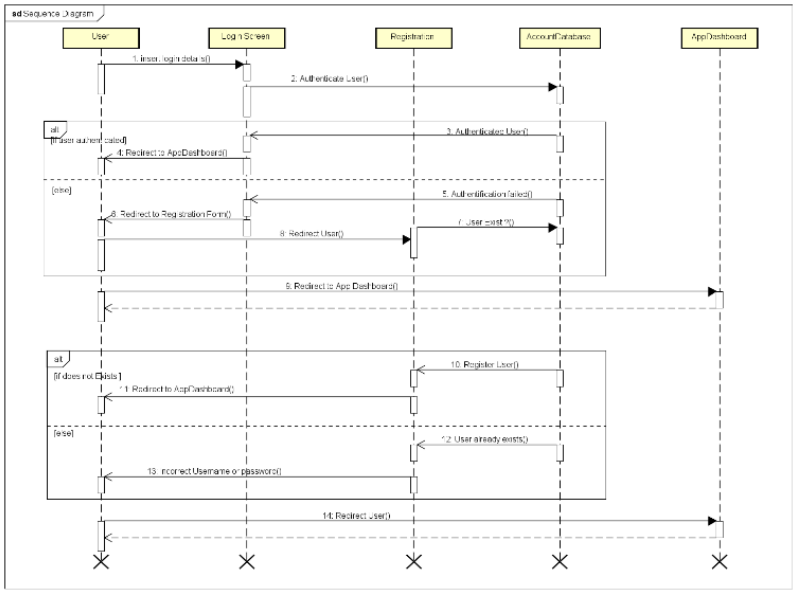

Fig 6. Authentication sequence diagram

Figure 6 is a sequence diagram demonstrating the login and registration process on the platform. The user enters his/her login details on the login screen, which verifies the details with the account database. If authentication is successful, the user is redirected to the dashboard corresponding to their profile. If authentication fails, the user is redirected to the registration form. The database check determines whether the user exists or not. If the user does not exist, he/she must register and be redirected to the dashboard.

C. Use case diagram

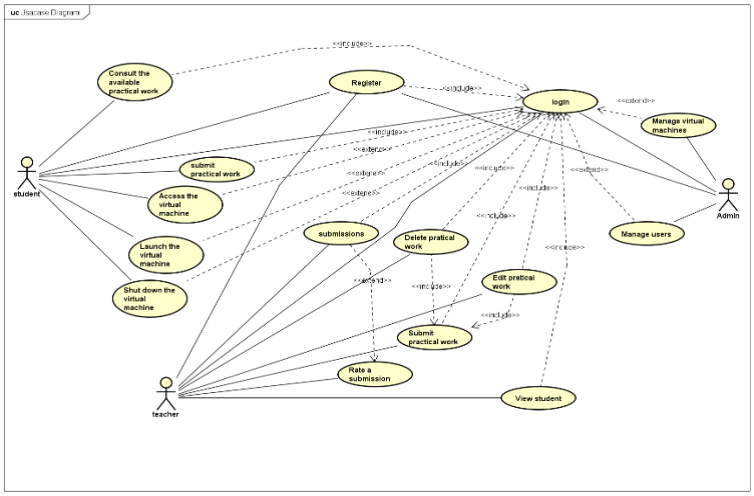

Fig 7. Use case Diagram

Figure 7 shows a use case diagram, highlighting the interactions between three main actors: `Student`, `Teacher`, and `Admin`. Students can register, log in, view and submit assignments, access, start and stop virtual machines. Teachers can log in, view and submit assignments, evaluate submissions, edit and delete assignments, and view student information. Administrators can log in, manage users and virtual machines. The diagram uses <<include>> and <<extend>> relationships to indicate dependencies and extensions between different use cases, providing a clear, structured view of the functionality available to each type of user on the platform.

CONCLUSION AND FUTURE WORK

This study highlights the importance of rigorous monitoring and continuous adaptation of the platform to align it with technological developments and new requirements in the field of digital forensics. It is crucial to ensure that training programs are regularly updated to meet the changing needs of the sector. In addition, collaboration with key players, such as technology industries and government institutions, could not only increase the relevance of the training, but also broaden the platform's impact beyond Senegal's borders. This will help to strengthen a more robust and adaptable digital security ecosystem, capable of responding to global cybercrime challenges.

REFERENCES

[1] Moussa Ngom, “Senegal: a “Mysterious Team” behind cyberattacks against the State”, lemonde.fr, May 29, 2023.
[2] INE Security, "INE Security," accessed July 28, 2024. [Online]. Available: https://security.ine.com/.
[3] Joël Rivière, Didier Lucas: "Criminalité et Internet, une arnaque à bon marché", Sécurité globale 2008/4 (N° 6), p. 67 - 82
[4] S. Jeon and S. Lee, "Digital Forensics Technology Management Platform," 2016 International Conference on Platform Technology and Service (PlatCon), Jeju, Korea (South), 2016, pp. 1-6, doi: 10.1109/PlatCon.2016.7456793.
[5] W. G. Kruse and J. G. Heiser, Computer Forensics: Incident Response Essentials, London, U.K.: Pearson, 2001.
[6] Interpol, "Digital forensics: Helping our member countries make the most of electronic evidence", Interpol.int, 2022.
[7] W. A. Jansen and A. Delaitre, Mobile Forensic Reference Materials: A Methodology and Reification, Gaithersburg, MD, USA: U.S.

[8] Valjarevic A., Venter H.S., «Analyses of the State-of-the-art Digital Forensic Investigation Process Models», The Southern Africa Telecommunication Networks and Applications Conference (SATNAC), Afrique du Sud, 2012.
[9] Valjarevic A., Venter H.S., «Harmonized Digital Forensic Investigation Process Model», International workshop on Digital Forensics in the Cloud (IWDFC), South Africa, 2012.
[10] ISO/IEC 27037 : 2012, Information technology - Security techniques - Guidelines for identification, collection, acquisition and preservation of digital evidence.
[11] Beebe N.L., Clark J.G.A., Hierarchical, "Objectives-Based Framework for the Digital Investigations Process". Digit. Invest. 2005.
[12] Pollitt M., «Applying Traditional Forensic Taxonomy to Digital Forensics», Advances in Digital Forensics IV, actes de la conférence du TC11.9 de l'IFIP, 2009
[13] Pluralsight, "Online Courses, Learning Paths, and Certifications - Pluralsight," accessed July 15, 2024. [Online]. Available: https://www.pluralsight.com
[14] Udemy, "Online Courses - Learn Anything, On Your Schedule," accessed July 17, 2024. [Online]. Available: https://www.udemy.com.
[15] Coursera, "Coursera | Degrees, Certificates, & Free Online Courses," accessed July 21, 2024. [Online]. Available: https://www.coursera.org/
[16] Cybrary, "Cybrary: Cybersecurity Courses & Cyber Security Training Online," accessed July 25, 2024. [Online]. Available: https://www.cybrary.it/.
[17] SANS, "Cybersecurity Training | SANS Certifications and Research," accessed July 25, 2024. [Online]. Available: https://www.sans.org/fr_fr/.
[18] Cellebrite, "Home," accessed July 25, 2024. [Online]. Available: https://cellebrite.com/en/home/.
[19] Forensic Focus, "Forensic Focus," accessed July 27, 2024. [Online]. Available: https://www.forensicfocus.com/.
[20] Infosec, "Cybersecurity Training & Certifications | Infosec," accessed July 26, 2024. [Online]. Available: https://www.infosecinstitute.com/.
[21] Sift, "Search for Public Funding & Public Aid," accessed September 29, 2024. [Online]. Available: https://www.sift-solutions.com/.
[22] O. Team, "Infosec & Cybersecurity Training," OffSec, accessed July 27, 2024. [Online]. Available: https://www.offsec.com/.
[23] INE Security, "INE Security," accessed July 28, 2024. [Online]. Available: https://security.ine.com/.
[24] W. A. Jansen and A. Delaitre, Mobile Forensic Reference Materials: A Methodology and Reification, Gaithersburg, MD, USA: U.S. Department of Commerce, National Institute of Standards and Technology, 2009.
[25] E. Casey, Handbook of Digital Forensics and Investigation, New York, NY, USA: Academic, 2009.
[26] Yassin Ciyow, "Cybersecurity: Africa under the threat of "digital chaos"", lemonde.fr, June 09, 2021
[27] S. Jeon and S. Lee, "Digital Forensics Technology Management Platform," 2016 International Conference on Platform Technology and Service (PlatCon), Jeju, Korea (South), 2016, pp. 1-6, doi: 10.1109/PlatCon.2016.7456793.
[28] Academie-plus, "The Information Portal on Education and Training in Senegal", [Online]. Available: https://www.academie-plus.com
[29] A. Bayaga, "Examining the integration and interoperability challenges of a security and privacy policy framework for e-government services: the case of South Africa," 2020 Conference on Information and Communication Technologies and Society (ICTAS), Durban, South Africa, 2020, pp. 1-6, doi: 10.1109/ICTAS47918.2020.233974.
[30] A. Tiwari, V. Mehrotra, S. Goel, K. Naman, S. Maurya and R. Agarwal, "Developing Trends and Challenges of Digital Forensics," 2021 5th International Conference on Information Systems and Computer Networks (ISCON), Mathura, India, 2021, pp. 1-5, doi: 10.1109/ISCON52037.2021.9702301
[31] V. R. Silvarajoo, S. Yun Lim and P. Daud, "Digital Evidence Case Management Tool for Collaborative Digital Forensics Investigation," 2021 3rd International Cyber Resilience Conference (CRC), Langkawi Island, Malaysia, 2021, pp. 1-4, doi: 10.1109/CRC50527.2021.9392497
[32] V. R. Silvarajoo, S. Yun Lim and P. Daud, "Digital Evidence Case Management Tool for Collaborative Digital Forensics Investigation," 2021 3rd International Cyber Resilience Conference (CRC), Langkawi Island, Malaysia, 2021, pp. 1-4, doi: 10.1109/CRC50527.2021.9392497