iJRASET
International Journal For Research in Applied Science and Engineering Technology

INTERNATIONAL JOURNAL FOR RESEARCH

IN APPLIED SCIENCE & ENGINEERING TECHNOLOGY

Volume: 13 **Issue:** XII **Month of publication:** December 2025

DOI: https://doi.org/10.22214/ijraset.2025.76050

www.ijraset.com

Call: 08813907089 | E-mail ID: ijraset@gmail.com

International Journal for Research in Applied Science & Engineering Technology (IJRASET)
ISSN: 2321-9653; IC Value: 45.98; SJ Impact Factor: 7.538
Volume 13 Issue XII Dec 2025- Available at www.ijraset.com

Dual-Role Group Dynamics as a Practical and Inclusive Framework for Teaching Digital Forensic Analysis - Think Like a Hacker and Think Like an Investigator

Ivo Ricardo Dias Rosa
ISTEC - Instituto Superior de Tecnologias Avançadas - Lisbon, Portugal.

Abstract: ***Cybersecurity is one of the most dynamic and challenging fields today, with constantly evolving digital threats. Digital forensic analysis, a subfield of forensic science, focuses on the examination of digital media and components to report, explain, and justify events that occur in a digital context. As a subfamily of forensic sciences, digital forensic analysis applies specific methods, techniques, and procedures to ensure that the collected evidence is valid and unquestionable. To prepare future information security professionals, hands-on education that goes beyond theory and emphasizes realism and engagement is essential. Traditional teaching approaches in this area are often limited to theoretical instruction, lacking the immersive and investigative dimensions required to address real-world challenges. This paper presents an innovative dual-role, group-based methodology - Think like a hacker, think like an investigator - that integrates collaborative learning, gamification, and standard-based forensic practice. Students alternate between designing attack scenarios and performing forensic investigations, following internationally recognized frameworks, such as NIST SP 800-86 and ISO/IEC 27037:2012. This bidirectional learning process develops both adversarial and investigative thinking, enhancing critical analysis, teamwork, and methodological rigor in the research process. The methodology was applied in the Digital Forensic Analysis course at ISTEC - Instituto Superior de Tecnologias Avançadas (Lisbon, Portugal), where it demonstrated promising outcomes. Students reported greater motivation, a deeper conceptual understanding, and improved readiness for professional cybersecurity environments. By combining open-source and no-cost tools with a dual-role group dynamic, this approach contributes to a more inclusive, engaging, and practice-oriented cybersecurity education.***

Keywords: Digital Forensic Analysis, Cybersecurity, Cybersecurity Education, Framework for Teaching Digital Forensic Analysis, Digital Investigation, Teaching Strategies in Cybersecurity, Group Dynamics, Dual-Role Learning, Gamification, NIS800-86, ISO/IEC 27037:2012

I. INTRODUCTION

Digital forensics, a critical subfield of forensic science, applies scientific techniques to acquire, preserve, and analyse digital evidence with unquestionable validity for legal proceedings [1]. However, traditional teaching methods often fail to prepare professionals for the dynamic challenges of this field, highlighting the need for innovative pedagogical approaches such as the dual-role methodology presented in this paper.

Digital Forensic Analysis corresponds to the acquisition, preservation, identification, extraction, restoration, analysis, and documentation of computer evidence, whether physical components or data that have been processed electronically and stored on computer media [2]. Digital forensics is a critical discipline in cybersecurity that involves the collection, preservation, and analysis of digital evidence to investigate cyber incidents. To empower future information security professionals, it is crucial to provide a learning experience that goes beyond theory and offers practical opportunities to apply this knowledge. In this context, a technical-practical experience was developed to provide students with a hands-on exposure of digital forensics analysis in challenging attack scenarios.

II. DIGITAL EVIDENCE

Evidence is expected to have probative validity before a court and a judge, therefore, digital evidence follows the same principles that are used in the context of physical evidence, ensuring that it remains Admissible, Authentic, Complete, Reliable, and Believable [1] [3]:

1) Admissible - respects the principles and guidelines in accordance with the law applicable to that context, business sector, or region.
2) Authentic - ensuring the proper relationship between the incident and evidence collected.
3) Complete - guaranteeing its integrity, that is, that it has not been contaminated or compromised during handling.
4) Reliable: Any handling of digital evidence must be properly documented so that it cannot be contested.
5) Believable: The information must be understandable and plausible.

III. DIGITAL FORENSIC ANALYSIS METHODOLOGY AND FRAMEWORK

The field of digital forensic analysis is governed by numerous methodologies and frameworks. This paper focuses on **NIST SP 800-86** and **ISO/IEC 27037:2012** due to their foundational roles in integrating forensic techniques into incident response and guiding the collection and preservation of digital evidence. Understanding their interplay is essential for developing a comprehensive pedagogical framework.

The NIST 800-86, Guide to Integrating Forensic Techniques into Incident Response [4], , is a document published by the National Institute of Standards and Technology in the United States. This guide offers recommendations for effectively integrating digital forensic techniques into incident responses. The goal is to assist organizations in collecting, analyzing, and presenting information that can be used to comprehend the course of a security incident, identify potential future threats, and enhance the overall security of the organization [4].

In contrast, ISO 27037:2012, "Information technology - Security techniques - Guidelines for identification, collection, acquisition, and preservation of digital evidence," is an international standard that provides directives for the identification, collection, acquisition, and preservation of digital evidence. This standard is part of the ISO 27000 family, which focuses on information security. ISO 27037:2012 is particularly beneficial for organizations that require the collection and preservation of digital evidence in a manner suitable for use in a court of law [5].

A comparative analysis of the NIST SP 800-86 and ISO/IEC 27037:2012 references revealed notable differences in their approaches to digital forensic analysis.

The NIST SP 800-86 stands out for its emphasis on the stages of digital forensics, suggesting a comprehensive framework for conducting digital investigations. However, this reference reveals a deficiency in the instructions for securing evidence, which could compromise the effectiveness of preserving the integrity of the evidence during the investigation process [4] [6].

In contrast, ISO/IEC 27037:2012 is distinct for its emphasis on instructions for collecting evidence, suggesting a focus on ensuring the integrity of the evidence collected during the digital investigation. However, this reference reveals a deficiency in the stages of digital forensics, which could limit its applicability to comprehensive digital investigations [5] [6].

These differences underscore the need for an integrated approach to digital forensics analysis. For an effective digital investigation, both a comprehensive framework for conducting the investigation (as provided by NIST SP 800-86) and robust instructions for collecting evidence (as provided by ISO/IEC 27037:2012) are crucial. Thus, the combined use of these references may offer a more holistic and effective approach to digital forensics analysis [6].

Both standards, NIST 800-86 and ISO 27037:2012, address the collection and analysis of digital evidence, albeit in slightly different manners. NIST 800-86 places a strong emphasis on incident response and the integration of forensic techniques into this process. In contrast, ISO 27037:2012 focuses more on the collection and preservation of digital evidence for use in legal proceedings.

IV. PROPOSED METHODOLOGY: TEACHING METHODOLOGY DEVELOPED AND EVALUATED

A methodology was developed to enhance the teaching of digital forensic analysis. This methodology is organized into **macro activities** that have sequentially interconnected micro steps at a lower level of detail. There are **two** macro activities in the methodology and **five** micro-steps.

Considering the name given to the exercise, *Think like a hacker and Think like an investigator*, the two macro activities are:

1) Think like a hacker : This phase is essentially where attack scenarios are developed, such as whether it is an actual cyber attack or cyber incident. Malicious and suspicious behaviors are generated and analyzed during the second activity of the proposed methodology.
2) Think like an investigator : This activity can only begin once the *Think like a hacker activity* has been completed. This is the main activity because it is when the entire digital forensic investigation process begins, applying the typical processes and procedures of an investigation and following standards.

The five interconnected micro-steps are as follows and have the following purpose:

- Formation of Working Groups: Students are organized into groups, each tasked with creating a digital attack scenario. Each scenario was designed to simulate realistic attack behaviors , challenging the skills of budding digital forensic investigators.
- Creation of Attack Scenarios: Student groups are encouraged to employ a variety of techniques, including the use of malware, encryption, steganography, and strategic evidence elimination, to make their attack scenarios challenging and realistic.
- Forensic Imaging: After creating the scenarios, groups follow recognized best practices and methodologies, such as NIST 800-86 [4], ISO 27037:212 [5] to create forensic images of the affected systems. This involves copying system images to external drives to ensure evidence preservation. At this stage, the recommendation was to use the FTK Imager software [7].
- Exchange of Forensic Images: A fundamental part of the experience is the exchange of forensic images among groups. Each group receives an image from an attack scenario created by another group and assumes the role of a digital forensic investigator.
- Analysis and Presentation: During the investigation, students applied digital forensic analysis techniques to reconstruct the events of the assigned scenario. At this stage, the recommendation was to use **Autopsy** software [8]. The goal was to retell the story of the incident based on the available evidence. Each group presents its findings, promoting knowledge exchange among the students.

In this methodology, the first two steps are part of the Think like a hacker activity, and the remaining three steps can be mapped to the Think like an investigator activity.

The Figure 1 graphically represents the different activities, stages, and relationships between them in this methodology applied to the technical/practical teaching of digital forensic analysis.

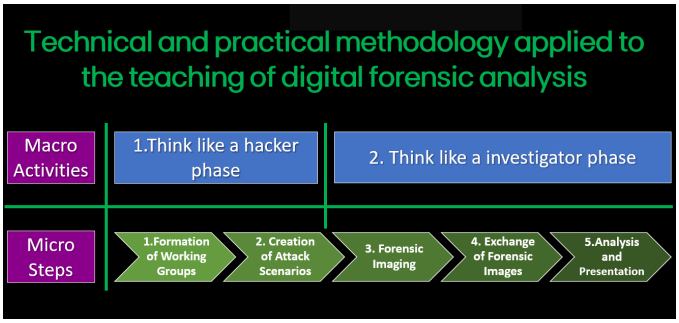


Figure 1 - Graphical representation of the methodology developed applied to the technical/practical teaching of digital forensic analysis. Image developed by the author.

V. CHARACTERIZATION AND EVALUATION OF SCENARIOS: ANALYSIS BASED ON THE DATA COLLECTED

To critically assess the effectiveness and benefits of the methodology, data were collected based on three key metrics: incident classification and typology, information-hiding techniques, and technologies used or tested. These metrics enabled an evaluation of the complexity and realism of the scenarios, directly informing the analysis of pedagogical advantages.

The metrics adopted include the following:

1) Incident Classification and Typology : This metric assessed the nature and classification of the incidents incorporated into the scenarios created and assessed by students.

2) Information Hiding Techniques : This metric examines the techniques used to hide information in the scenarios, providing insights into the camouflage strategies employed.

Of the different scenarios analysed so far, the following information-hiding techniques have already been identified:

Information Hiding Techniques	Scope
Encryption	Content Communications
Steganography	Content Communications
Anonymization	Identities
Delete	Content

Encoding	Content
Rootkits	Processes Files Content Communications
Time Stomping	Metadata (Time) Content
Data Carving	Content
Memory Dumping	Volatile Memory (RAM)
Virtualization Techniques and Isolated Execution Environments	Processes Execution Environments
Log Alteration	Logs Metadata Content
Use of Anonymous Networks	Communications Identities
Use of Volatile Artifacts	Volatile Memory (RAM) Temporary Files Content

Table 1 - information hiding techniques and their scope of application, taking into account the scenarios identified

3) Technologies Used/Tested: This metric examined the specific technologies employed or tested in the scenarios, highlighting the tools and technological resources involved. In terms of technological tools, we can also identify the use of a set and experience with a significant number of tools:

Technological Tools	Description
FTK Imager [7]	Is a tool that creates a forensic image of the hard disk for detailed analysis of files, including deleted and hidden files.
Autopsy [8]	Is an open source forensic tool that provides a graphical interface for detailed analysis of systems and recovery of digital evidence.
Volatility [9]	Is a forensic analysis tool that allows you to extract valuable information from the memory of operating systems.
StegSecret	Is an application that detects and extracts information hidden in image files, revealing messages or data not visible to the naked eye.
StyleSuxx	Is a tool that helps analyze steganography, allowing you to identify and recover information hidden in media files.
StegHide	Is a tool that allows confidential data to be hidden within image files, providing additional security to digital communication.
OpenPuff	OpenPuff is an open-source steganography and watermarking tool that supports a variety of file formats such as JPEG, BMP, PNG, MP3, WAV, 3GP, and MP4, offers military-grade encryption, and allows the concealment of data in up to 16 of these media carriers simultaneously.
Message Header Analyzer	Is a tool that analyzes email headers to trace the origin and route of messages.
olevba	Extracts and analyzes VBA macros from Microsoft Office documents. Used to detect potential macro-based malware in phishing scenarios.
Binwalk	Assists in reverse engineering and extraction of firmware and binary images. Particularly relevant in IoT and embedded system cases.
Binary Ninja	A powerful static analysis and reverse engineering platform, enabling disassembly and control flow analysis of binaries.

any.run	An interactive online malware sandbox used for dynamic behavioral analysis of potentially malicious executables or scripts.
VirusTotal	Online platform aggregating antivirus scan results and behavioral analysis; useful for file triage and intelligence correlation.
Event Log Explorer	Facilitates deep analysis of Windows Event Logs to reconstruct user or attacker activity.
Blockchain.com Explorer	Web-based tool used to trace Bitcoin wallet activity and transactions; commonly used in investigations involving ransomware payments, fraud, and money laundering through cryptocurrency.
SilentEye / OpenStego	Additional tools used for steganographic encoding/decoding across various media formats.

Table 2 - Variety of technologies used/tested considering the various works developed and which were part of this study

These metrics provide a solid basis for the critical analysis of the scenarios developed by the students, allowing for a detailed assessment of the characteristics and complexity of each case.

VI. BENEFITS AND IMPACTS

This approach to teaching, based on technical and practical challenges, offers several benefits:

1) Hands-on Learning: Students gain valuable practical experience in investigating cyber incidents, preparing them for real-world cybersecurity environments .

2) Collaboration: The exchange of forensic images promotes collaboration among groups, allowing students to learn from different approaches and perspectives.

3) Critical Skill Development: Students develop critical skills as future cybersecurity professionals, including:

- Digital evidence analysis;
- Data preservation;
- Incident reconstruction is an essential skill.
- Handling different technological tools applicable to the specific context of digital forensic analysis, and others applicable to a more transversal context of cybersecurity

4) Gamification : Healthy competition among groups, with the challenge of retelling the story of the attack, motivates students to excel and enhances their skills.

5) Variety of scenarios : The variety of scenarios allows students to gain diverse experiences , preparing them to face a wide range of real-world situations and stimulating creativity.

6) Scenarios with varying complexity : The varying complexity of the scenarios allows students to develop skills gradually, starting with simpler cases and progressing to more complex challenges, thereby ensuring comprehensive and adaptable training.

VII. INNOVATION AND DISCUSSION

The Think like a hacker, think like an investigator methodology introduces an innovative dual-role framework that expands the traditional boundaries of cybersecurity education. Although group-based exercises and Capture-the-Flag challenges are widely used, the proposed model distinguishes itself through the simultaneous integration of offensive and investigative mindsets within the same pedagogical structure.

This duality requires each student group to act as both an attacker and a digital investigator. In doing so, learners experience the full lifecycle of a cyber incident, from intrusion design and data hiding to evidence collection, analysis, and reporting. Such cognitive switching strengthens analytical reasoning and provides a deeper understanding of adversarial thinking, incident reconstruction and the evidential chain.

Compared with previous educational frameworks in digital forensics [10], [11], [12], this approach extends the learning paradigm by emphasizing bidirectional learning and inclusivity of the learning process. The methodology relies exclusively on open-source and no-cost forensic tools such as Autopsy [8], FTK Imager [7], and Volatility [9], ensuring accessibility for institutions with limited resources and contributing to the reduction of the digital divide.

From a standards perspective, the simultaneous application of NIST SP 800-86 [4] and ISO/IEC 27037:2012 [5] in a classroom context provides a unique opportunity to align educational outcomes with both process- and evidence-oriented frameworks.

This alignment promotes students' awareness of the distinct yet complementary legal and procedural dimensions of digital forensic practice.

Initial classroom feedback suggests that the gamified dual-role dynamic enhances motivation and engagement compared to traditional lecture-based formats. Students reported higher confidence in using forensic tools and a better understanding of the rationale behind the procedural standards. Nevertheless, further quantitative validation is needed to assess measurable learning outcomes, which is an avenue proposed for future research.

VIII. FUTURE WORK

To continue this work and deepen the application of this teaching and training methodology in digital forensic analysis, the following lines of research and development can be explored:

1) Validation in Different Scenarios and Complexities:

- The methodology should be tested with a wide range of students, considering different attack scenarios and variability in complexity.
- Evaluate the effectiveness of the methodology in scenarios ranging from simple attacks to those involving advanced cyber security techniques.
- Collect feedback from students and instructors to improve the methodology based on real-world classroom experiences.
- A knowledge base was created with the results of the different scenarios analyzed and the respective feedback, providing a comparative observatory over the years and editions of the course.
- The application of this methodology in scenarios that include IoT artifacts should be tested and evaluated to ensure its effectiveness and adaptability to different environments and technologies.
- The methodology was applied and evaluated in scenarios where AI was used to generate cyberattacks or cyber incident scenarios and to support forensic investigations for analyzing and discovering the root cause of the cybersecurity incident.

2) Extension to Other Cybersecurity Courses:

The methodology can be expanded to other areas, disciplines or even other academic courses in cybersecurity, including:

- *Ethical Hacking*
  - Explore how ethical hacking knowledge can be integrated into the methodology.
  - Develop more realistic, complex and challenging **Think like a hacker** scenarios, taking into account real attack techniques and tactics.
- *Vulnerability management*
  - Consider integrating vulnerability analysis into the methodology.
  - Evaluate the strategy for identifying vulnerabilities in the "Think like a hacker" scenarios and in the "think like an investigator" activity as an investigator who can discover and evaluate these vulnerabilities.
- *Security Incident Management*
  - Broaden the focus of digital forensic analysis methodology for security incident management by incorporating a standardized incident taxonomy. The application of taxonomic classification frameworks, such as those proposed by the European Union Agency for Cybersecurity (ENISA) [13], supports a structured categorization of incidents (e.g., malware infection, data exfiltration, denial of service, etc.), improving incident triage, response prioritization, and post-incident analysis. This structured approach enhances the integration of forensic analysis and incident response workflows.
  - Explore in the Think like an investigator activity the application of other compliance standards, such as ISO/IEC 27035 (Information Security Incident Management) [14] and NIST 800-61 (Computer Security Incident Handling) [15] in the methodology.
  - Classify the security incidents generated in the Think like a hacker activity based on the MITRE ATT&CK framework (Adversarial Tactics, Techniques, and Common Knowledge) [16] for a more comprehensive analysis of the tactics and techniques used by attackers.

These lines of research and development represent exciting opportunities to further expand and improve the teaching and training methodology in digital forensic analysis in cybersecurity towards a transversal theoretical-practical teaching methodology. This allows for a more holistic and integrated approach to prepare students for the real and constantly evolving challenges in the field of information security.

IX. CONCLUSIONS

In 2016, researchers from University College Dublin [12] identified five major challenges faced by digital forensic analysis professionals when handling digital evidence in a rapidly evolving technological environment.

The five challenges identified are as follows [12]:

1) Data Complexity : Managing large volumes of heterogeneous data requires advanced data reduction and filtering techniques before analysis.

2) Diversity of Sources : The lack of standardization in the analysis of diverse data sources, such as operating systems, file formats, and devices, makes analysis difficult.

3) Consistency and Correlation : Current forensic tools often identify fragmented evidence but fail to support effective correlation and contextualization of the evidence .

4) Data Volume: The exponential growth of storage capacity and connected devices demands increased automation to process information efficiently.

5) Temporal Synchronization : Unifying time references from multiple sources, timestamps, and other temporal aspects is challenging in digital forensic analysis.

Despite living in an era of constant technological evolution and transformation, which at certain times enhances the activity of the investigator and at other times enhances the activity of the hacker, these challenges are still very relevant and applicable today.

The dual-role teaching methodology presented in this study directly addresses several of these challenges in a controlled academic context. By engaging students as both attackers and investigators, this approach fosters a deeper comprehension of digital evidence, adversarial behaviour, and procedural rigor. This bidirectional dynamic enables learners to experience the entire investigative lifecycle, from data generation and concealment to evidence extraction, correlation, and timeline reconstruction, effectively mirroring the complexity, diversity, and synchronization problems faced by real-world professionals.

Furthermore, the framework integrates hands-on, standard-based learning through the use of NIST SP 800-86 [4] and ISO/IEC 27037:2012 [5], ensuring consistency with industry and legal best practices. The exclusive use of open and no-cost forensic tools promotes inclusiveness and accessibility, preparing students from diverse academic and socio-economic backgrounds for realistic cybersecurity challenges.

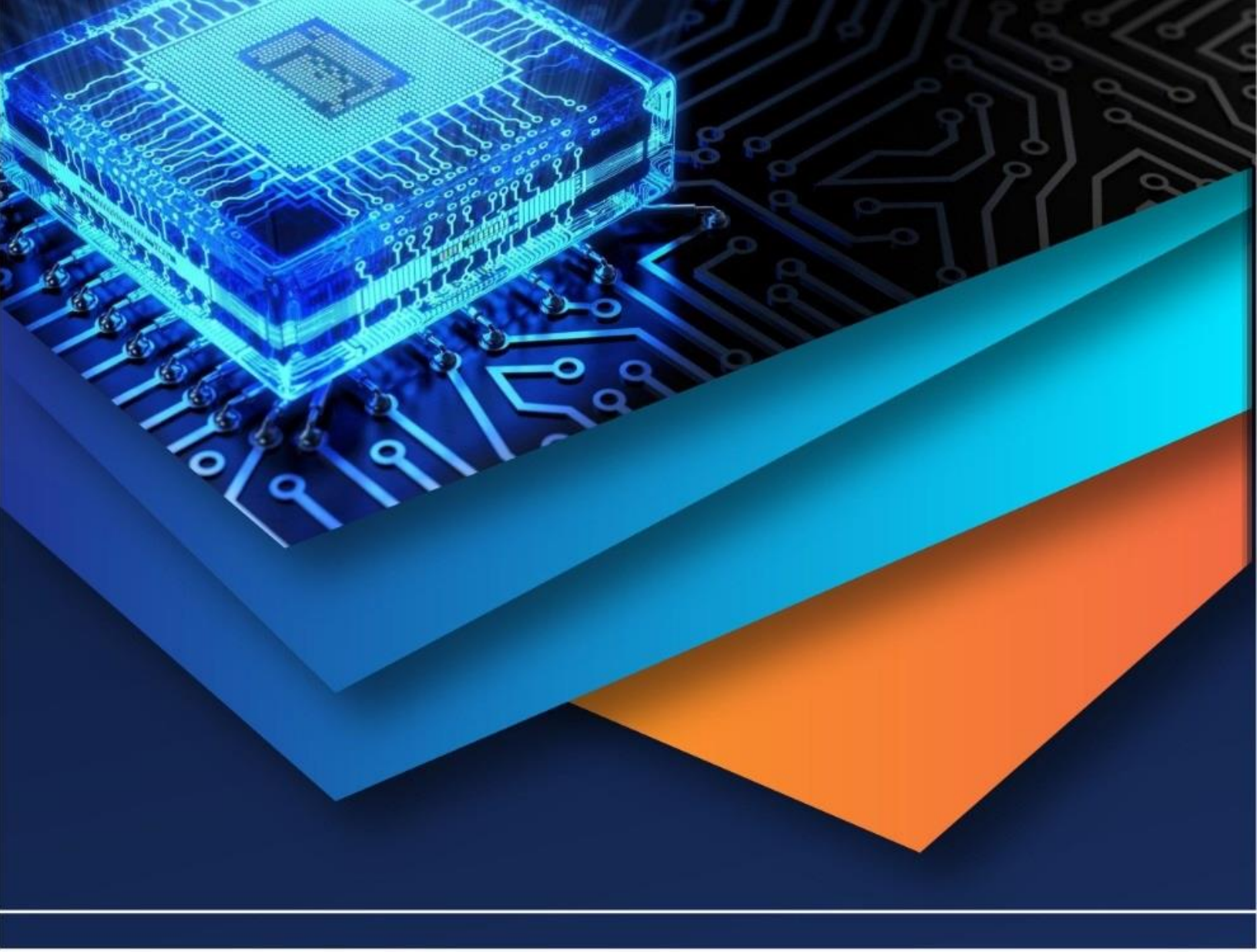
Beyond its pedagogical innovation, the model helps overcome traditional limitations in digital forensics education, such as insufficient engagement, lack of realism, and fragmented understanding between theory and practice. Preliminary implementations indicate that the methodology not only motivates students but also develops analytical reasoning, collaboration, and methodological discipline.

The Think like a hacker, Think like an investigator methodology represents an innovative, practical, and inclusive framework for digital forensic education. By integrating recognised standards (NIST SP 800-86 and ISO/IEC 27037:2012) and open-source tools, it equips students with both technical competence and investigative mindset, preparing them to address the evolving challenges and threat in the modern cybersecurity landscape.

REFERENCES

[1] M. Antunes and B. Rodrigues, INTRODUÇÃO À CIBERSEGURANÇA - A INTERNET, OS ASPETOS LEGAIS E A ANÁLISE DIGITAL FORENSE, Lisbon: FCA, 2018.
[2] J. G. Heiser and W. G. Kruse, Computer Forensics: Incident Response Essentials, 1st Edition, Addison-Wesley, 2001, p. 392.
[3] A. Yeboah-Ofori, "Digital Forensics Investigation Jurisprudence: Issues Of Admissibility Of Digital Evidence," Journal of Forensic, Legal & Investigative Sciences, vol. 6, pp. 1-8, 5 2020.
[4] K. Kent, S. Chevalier, T. Grance and H. Dang, Guide to Integrating Forensic Techniques into Incident Response, NIST Special Publication, 2006.
[5] ISO/IEC 27037, ISO/IEC 27037:2012 Information technology - Security techniques - Guidelines for identification, collection, acquisition, and preservation of digital evidence, International Organization for Standardization (ISO), 2012.
[6] R. Ramadhan, P. Setiawan and D. Hariyadi, "Digital Forensic Investigation for Non-Volatile Memory Architecture by Hybrid Evaluation Based on ISO/IEC 27037:2012 and NIST SP800-86 Framework," IT Journal Research and Development, no. 10.25299/itjrd.2022.8968, pp. 162-168, 2022.
[7] Exterro, "FTK Imager - Exterro," Exterro, [Online]. Available: https://www.exterro.com/ftk-imager.
[8] "Autopsy - Digital Forensics," Autopsy, [Online]. Available: https://www.autopsy.com/.
[9] The Volatility Foundation, "The Volatility Framework: Advanced Memory Forensics," [Online]. Available: https://www.volatilityfoundation.org.
[10] G. Palmer, "A Road Map for Digital Forensic Research," Digital Forensic Research Workshop (DFRWS), Baltimore, MD, 2001.
[11] M. Pollitt, "A History of Digital Forensics," in Advances in Digital Forensics VI, Springer, Ed., New York, IFIP International Conference., 2010.
[12] D. Lillis, B. Becker, T. O'Sullivan and M. Scanlon, "Current Challenges and Future Research Areas for Digital Forensic Investigation," in The 11th ADFSL Conference on Digital Forensics, Security and Law (CDFSL 2016), Daytona Beach, FL, USA, 2016.

[13] ENISA, "Reference Incident Classification Taxonomy, European Union Agency for Cybersecurity," 2018. [Online]. Available: https://www.enisa.europa.eu/publications/reference-incident-classification-taxonomy.
[14] ISO/IEC 27035, ISO/IEC 27035-1:2016 Information technology - Security techniques - Information security incident management - Part 1: Principles of incident management., International Organization for Standardization (ISO), 2023.
[15] NIST, NIST Special Publication 800-61 Revision 2: Computer Security Incident Handling Guide, National Institute of Standards and Technology, 2012.
[16] M. Corporation, "MITRE ATT&CK Framework," MITRE, [Online]. Available: https://attack.mitre.org. [Accessed 3 September 2025].



10.22214/IJRASET

45.98

IMPACT FACTOR: 7.129

IMPACT FACTOR: 7.429

INTERNATIONAL JOURNAL FOR RESEARCH

IN APPLIED SCIENCE & ENGINEERING TECHNOLOGY