

Forensic Analysis of the NIST Hacking Case: Integrating Autopsy Tools and Artificial Intelligence in Teaching Digital Forensics

Damir Delija, Goran Sirovatka, Marinko Žagar
Zagreb University of Applied Sciences, Zagreb, Croatia
damir.delija@tvz.hr, goran.sirovatka@tvz.hr, marinko.zagar@tvz.hr

Abstract — This article examines the forensic analysis of the NIST Hacking Case, where an abandoned laptop was found with potential traces of hacking. Through the use of the forensic tool Autopsy and consultation with ChatGPT, students conducted in-depth analysis, identifying artifacts, clues, and attempting to link the computer to the suspect. The results of the analysis, the methodology used during the research and the identified challenges provide insight into contemporary approaches to digital forensics.

Keywords - Digital forensics; The NIST Hacking Case; Autopsy tool; ChatGPT;

I. INTRODUCTION

The NIST Hacking Case, employed as an educational case study in the field of digital forensics, simulates a real-world scenario where investigators encounter an abandoned laptop with potential hacking traces. This case acquaints students with the challenges and techniques of forensic analysis, preparing them for real-life situations in cyber forensics. It is one of the older forensic images accessible on the NIST web site, as part of an effort to provide training and testing materials for digital forensic practitioners. The case is located on "<https://cfreds.nist.gov/all/NIST/HackingCase>" where it is possible to download disk images, case description, test questions and correct answers. On the first glance it is outdated since it is based on Windows XP machine seized in 2004, but in this specific situation it is adequate and even has some simple but important advantages against other more up-to-date forensic images available. Students of the Information Security and Digital Forensic study program (ISDF) [1] on the Zagreb University of Applied Sciences were tasked with solving this forensic problem as a final part of an exam in Digital Forensic lectures. It is supposed to be a homework task which should result in a report about analysis results and tools and methods used. Students were instructed to use ChatGPT as an additional tool, if they feel safe with it, but also to document in detail how they were using ChatGPT and how useful it was in answering questions in the NIST hacking case. Due to technical limitations ISDF cannot provide students with reliable powerful computers suitable for handling modern forensic cases so the NIST hacking case with its small size and moderate processing requirements is acceptable, especially since it covers all important digital forensic topics in an adequate way. In other words, students were able to work on the NIST hacking case on their own personal computers or at resources available in the ISDF online laboratory [2],[3]. All infrastructure for

accessing NIST hacking case data and handling reports were provided through the TVZ learning management system LMS-2020.

Utilizing Autopsy, an open source free and advanced forensic tool, students conducted a thorough analysis of the computer system, including file review, user activity inspection, and extraction of key information. Concurrently, the use of artificial intelligence, in the form of consultations with ChatGPT, provided students with access to additional information and clarifications, further enriching their educational experience.

This article focuses on analyzing how students used Autopsy and artificial intelligence in solving the NIST Hacking Case as part of their education. The collected data on student works offer insights into the methodologies employed and the challenges faced by the students. The goal is to understand the effectiveness of this approach in digital forensics education.

Further in the article, we thoroughly explore the methodology applied by the students, analyze their results, discuss the challenges, and conclude with a reflection on the implications of these findings for educational practices in digital forensics.

In this exploration of the NIST Hacking Case, a notable aspect is the integration of ChatGPT in the data analysis process and the preparation of the academic paper. ChatGPT served as a useful tool for students, offering guidance in dissecting complex digital evidence and aiding in the interpretation of forensic data. Its role extended to assisting in the structuring of their findings and providing insights on how to effectively present their analyses. The use of such advanced artificial intelligence in educational settings not only facilitated a deeper understanding of the case study but also exemplified the potential of AI-assisted learning in enhancing the analytical skills required in the field of digital forensics. Also, ChatGPT was used to speed up and empower the analyses of report papers from students.

II. METHODOLOGY

A. Overview

This paper adopts a comprehensive approach to analyze the NIST Hacking Case, focusing on the application of digital forensic tools and artificial intelligence in an educational setting. The methodology is designed to

evaluate the effectiveness of these tools in enhancing the students' learning experience and their ability to conduct thorough digital investigations.

The students involved in the NIST Hacking Case study completed their tasks by February 1st 2024, with 46 out of 49 students submitting their papers on time. This commendable rate of timely submission reflects the students' commitment and the effectiveness of the assignment in engaging them with the subject matter.

The dataset for analysis comprised papers from 44 students, amounting to approximately 880 pages of raw text. This substantial volume of text included a total of 1,364 answers, providing a rich source of data for evaluating student understanding and application of digital forensic concepts.

The short period between the completion of the students' papers and the required date for this paper, posed a significant challenge in conducting a more detailed analysis. Given the extensive volume of text and the depth of answers provided, the time constraints limited the scope of analysis that could be undertaken. This limitation was particularly felt in the ability to conduct a more nuanced and in-depth evaluation of each individual response, even with help of ChatGPT.

This situation underscores the challenges faced in educational research, especially when dealing with large volumes of qualitative data. It highlights the need for efficient data analysis methods and the potential role of AI tools in aiding such processes. However, it also emphasizes the importance of allowing sufficient time for thorough analysis to gain comprehensive insights from student submissions..

B. Forensic Tool Utilization: Autopsy

Autopsy, a leading open-source digital forensics platform, was the primary tool used by the students in this case study. It facilitated the in-depth analysis of the digital image of the abandoned laptop, enabling the extraction and examination of critical data such as file systems, deleted files, and system logs. The students were tasked with using Autopsy to identify key forensic artifacts, trace evidence of hacking activities, and gather potential leads about the suspect.

C. Artificial Intelligence Assistance: ChatGPT

Alongside Autopsy, ChatGPT played a significant role in the students' research process. It was used as a supplementary tool for data analysis and interpretation. Students consulted ChatGPT for additional insights, clarifications on complex forensic concepts, and guidance in navigating through the intricacies of digital evidence. Furthermore, ChatGPT assisted in the structuring and preparation of their final reports, ensuring a coherent and comprehensive presentation of their findings.

D. Data Collection and Analysis

The core of the study involved collecting and analyzing the students' reports on their findings. Each report was examined to assess the accuracy of the forensic analysis, the depth of understanding of digital forensic principles,

and the effectiveness of integrating Autopsy and ChatGPT in the research process. The reports were also evaluated for their structure, clarity, and adherence to academic and digital forensic standards.

E. Ethical Considerations

Throughout the study, ethical considerations were important. The use of digital forensic tools and AI assistance was conducted within the boundaries of academic integrity and ethical research practices. The confidentiality and privacy of the students' work were maintained, with all analyses and discussions being purely educational and hypothetical in nature.

III. ANALYSIS RESULTS

The analysis of student responses to the NIST Hacking Case revealed significant insights into their proficiency in utilizing digital forensic tools and understanding the process of forensic investigations. The results highlighted varied levels of expertise and provided a window into the effectiveness of integrating traditional forensic tools with AI-driven methodologies in an educational context. The use of ChatGPT as a supplementary tool was another focal point of the study. The analysis indicated that students frequently consulted ChatGPT for complex forensic queries, reflecting an innovative approach to problem-solving. ChatGPT's role in aiding the structuring and development of their reports was also noteworthy, enhancing the overall quality of their submissions. As part of preparation students were introduced into SANS articles about usage of AI tools in analyzing data [4].

A key finding from the analysis was the students' ability to effectively use the Autopsy tool and enhance usage through AI guidance and consulting.. For instance students successfully identified the hash value of the forensic image, with approximately 20.45% accurately matching the hash value. Similarly, around 25% correctly identified the operating system as Windows XP through various means without help of AI, demonstrating a solid understanding of key forensic analysis techniques.

The varied responses to questions related to the installation date of the operating system and the timezone settings indicated a range of understanding. While students identified the timezone correctly, there were inconsistencies in pinpointing the exact installation date (approximately 18.18% accuracy), highlighting areas for further emphasis in future curriculum development.

2. Koji je operativni sustav korišten na računalu?

Operacijski sustav na računalu je Windows XP.

ChatGPT odgovor:

Analizirajte System Artifacts:

- U oknu za navigaciju, idite na odjeljak koji se odnosi na sustavne artefakte ili "System Artifacts".
- Pregledajte datoteke ili mape koje se odnose na informacije o operativnom sustavu.

Ispitajte Datoteke sa Sustavskim Informacijama:

- Proučite datoteke poput "system.log", "winlogon.log" ili sličnih koje bi mogle sadržavati informacije o operativnom sustavu.

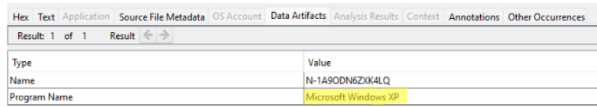
Prikaz Informacija:

- Kada pronađete relevantne datoteke, desnim klikom otvorite ih u Autopsyju.
- Pogledajte unutar tih datoteka kako biste pronašli informacije o operativnom sustavu.

Figure 1. Example of how student use ChatGPT in solving case.

2. Koji je operativni sustav korišten na računalu?

Na slici 2 možemo vidjeti da se na računalu koristi operativni sustav Microsoft Windows XP.



Zadatak 2. Koji je operativni sustav korišten na računalu?

Korišteni OS je Windows XP Professional. Informacija je zapisana unutar boot ini datoteke. Slika 2 prikazuje korišteni OS.

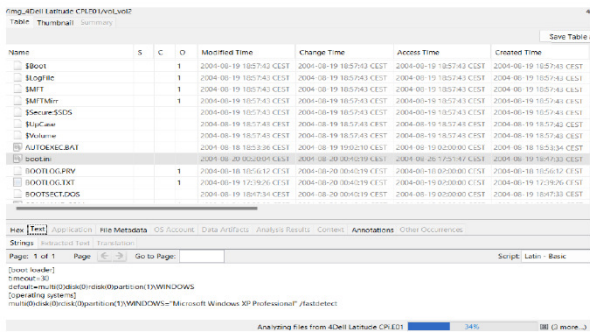


Figure 2. Two examples of another way of finding solution to question without AI help

In the Figure 1 and 2 various examples of possible answers in students reports are present, giving the idea there are more than a one correct method to get answer, even with using AI for support. In some situations answers are presented as screenshots of forensic tool, what is also accepted as correct.

The analysis of all 44 seminar papers, it was found that ChatGPT was not used or only referenced in 11 instances, explicitly stated by the students. In contrast, ChatGPT was utilized for suggestions or guidance in 24 papers, where it provided various insights or pathways for the students' research and analysis tasks. The remaining 9 papers did not clearly indicate whether ChatGPT was used or not. This distribution highlights that while ChatGPT served as a valuable tool for guidance in over half of the cases, its application was not uniform across all submissions. More detailed breakdown of how ChatGPT was used per paper and per question is presented in Tables I and Tables II.

TABLE I. USAGE OF CHATGPT PER EACH QUESTION, QUESTION NOT USING IT AT ALL ARE OMITTED

Question	ChatGPT Usage
2	Guidance for accessing registry dana
3	Provided registry location for Windows installation date
4	For time zone settings
5	For identifying registered owner
6	Suggested reviewing user metadata in artifacts, Provided registry location for user account name
7	Suggested reviewing "System Information"

	and Registry, Provided registry location for domain name
8	Provided suggestions, but the user found a more efficient solution
9	Provided exact location of data
10	For most frequent user account
11	Used for last logged-in user
13	Used for listing network cards
16	Used - Suggested finding data in artifacts
17	Used for SMTP address
18	Used - Suggested reviewing artifacts and Registry
19	Used - Provided suggestions for reviewing installed e-mail and news clients
20	Used for listing news groups subscribed by Mr. Evil
26	Used - Suggested reviewing web history
27	Used for reviewing webmail and network-related artifacts
31	Used - Provided instructions for finding mIRC logs

TABLE II. BREAKDOWN BY STUDENT PAPER IN WHICH WAY CHATGPT WAS USED, PAPERS NOT USING IT AT ALL ARE OMITTED.

Paper	Summary of ChatGPT usage
6	Used for Internet history and other options
7	Used for reviewing artifacts related to webmail and network
9	Used for finding data in artifacts
11	Used for reviewing artifacts and Registry
12	Most profitable to search key words
13	Provided full path to data after detailed search
14	Provided exact location of last shutdown time data
15	Suggested looking at \Users and related artifacts
18	Suggested reviewing artifacts and Registry
19	Suggested searching key words as most profitable method
20	Provided full path to data after detailed search
23	Suggested looking at \Users and "System Information"
24	Suggested looking at "System Information" and Registry
25	Provided exact location of last shutdown time data
26	Suggested looking at \Users and related artifacts

28	Corrected from system to software; provided location for data
30	Recognized hexadecimal value but not the time value
31	Provided instructions for finding mIRC logs
32	Provided information on Ethereal (now known as Wireshark)
33	Identified MAC address manufacturer as 3Com Corporation
34	Could not fully identify hacking programs
37	Identified number of user accounts
38	Found that Mr. Evil was the most frequent user
39	Identified the last user who logged in as Mr. Evil
40	Analyzed installed programs for hacking purposes
41	Used keyword search for finding SMTP
42	Used keyword search for NNTP settings
43	Identified MS Outlook Express
44	Opened Outlook Express file for subscribed news groups

Based on the data the following conclusions can be drawn:

- **Selective Use of ChatGPT:** ChatGPT was not uniformly used across all papers. It was utilized in specific instances where the students needed guidance or clarification on digital forensics concepts, methods, or tools.
- **Varied Dependence on AI Assistance:** The frequency of ChatGPT usage varied significantly across different papers. This indicates a varied level of dependence or trust in AI assistance among students. Some relied on it for critical insights, while others either did not use it or used it minimally.
- **Task-Specific Queries:** Where ChatGPT was used, it often focused on specific tasks like identifying file locations, interpreting hexadecimal values, or suggesting methods for analyzing digital artifacts. This suggests that students used ChatGPT as a supplementary tool for specific technical challenges rather than for overall analysis.
- **Learning and Exploration Tool:** The usage of ChatGPT appears to be more exploratory and educational, aiding students in navigating complex digital forensics tasks. It served as a learning tool, providing additional information and guiding students through the process.
- **Independence in Analysis:** The majority of the papers did not use ChatGPT, indicating a preference for independent analysis. This reflects the students' ability to handle complex digital forensic investigations without relying heavily on AI assistance.

- **Integration of AI in Education:** The document showcases an interesting integration of AI in educational settings. It highlights how AI tools like ChatGPT can augment learning and research, particularly in technical fields like digital forensics.

Also the students' adherence to ethical standards and academic rigor was commendable. Their reports showed a high level of integrity and respect for ethical guidelines.

A. Detailed Analysis by Specific Question

Only subset of questions is presented in the paper:

- **Question 1 - Hash Value Identification:** 7 students correctly identified the forensic image hash value.
- **Question 2 - Operating System Used:** 34 students accurately identified the operating system as Windows XP, demonstrating strong skills in identifying system information.
- **Question 3 - Installation Date:** 8 students pinpointed the correct installation date, indicating proficiency in interpreting system metadata.
- **Question 4 - Time Zone Settings:** All 44 students correctly identified the time zone settings, showing a comprehensive understanding of system configurations.
- **Question 5 - Registered Owner:** Similarly, all 44 students correctly identified the registered owner, indicating effective analysis skills in user information retrieval.
- **Question 6 - User Account Name:** 37 students accurately identified the user account name, reflecting their ability in user account analysis.
- **Question 7 - Primary Domain Name:** 8 students correctly identified the primary domain name, suggesting a more nuanced understanding of network settings.
- **Question 9 - Total Number of Recorded Accounts:** 8 students correctly stated the total number of user accounts, highlighting their capability in account management analysis.
- **Question 10 - Account Name of Frequent User:** 8 students accurately identified 'Mr. Evil' as the frequent user, showing effectiveness in user behavior analysis.
- **Question 11 - Last User Logged in:** 34 students correctly identified the last user logged in, demonstrating their proficiency in tracking user activities.
- **Question 14 - Network Cards Used:** 20 students correctly listed the network cards, indicating their understanding of network interfaces and settings.
- **Question 17 - Installed Programs for Hacking:** All 44 students successfully identified programs that could be used for hacking, showcasing a broad understanding of potential hacking tools.

- Question 18 - SMTP Email Address for Mr. Evil: 30 students correctly identified Mr. Evil's SMTP email address, showing their skill in analyzing email configurations.
- Question 19 - NNTP Settings for Mr. Evil: 16 students accurately identified the NNTP settings, indicating a deeper dive into advanced configuration analysis.
- Question 22 - Installed IRC Programs: 21 students listed installed IRC programs, revealing their ability to identify communication tools.
- Question 23 - IRC User Settings: 39 students correctly identified user settings in IRC programs, demonstrating their ability to analyze user preferences and settings.
- Question 24 - IRC Chat Session Logging: Another 39 students correctly identified details about IRC chat session logging, showing their capability in analyzing communication records.
- Question 25 - File Containing Intercepted Data: 22 students identified the file with intercepted data, indicating proficiency in analyzing data capture and storage.
- Question 31 – Malware installed on the image: All 44 students demonstrated strong overall comprehension and effective reporting, indicating the successful integration of forensic tools and AI in their educational process.

B. Interpretation of Results

The analysis of the NIST Hacking Case study provides valuable insights into the students' understanding and application of digital forensic principles. The results indicate a varying degree of proficiency among students. For instance, high accuracy in identifying basic system information like the operating system and registered owner (Questions 2, 5) contrasts with less accuracy in more complex tasks such as network configuration (Question 7) and NNTP settings (Question 19). This disparity suggests that while students are comfortable with foundational concepts, they face challenges when dealing with more intricate aspects of digital forensics.

C. Challenges in Analysis

One of the primary challenges observed in the study was the students' ability to interpret complex forensic data accurately. For example, the varied responses to the installation date (Question 3) highlight the need for a deeper understanding of system metadata and its implications. Additionally, the integration of AI tools like ChatGPT, while beneficial in some aspects, also raises questions about the students' reliance on external tools for analysis and interpretation, potentially impacting their independent problem-solving skills.

D. Implications

The findings from this study have implications for digital forensic education and for ISDF. They underscore the necessity of a balanced curriculum that not only focuses

on basic forensic skills but also emphasizes advanced topics and practical problem-solving abilities. The use of AI tools in education, as shown in this study, can be a double-edged sword, offering significant benefits in understanding complex concepts but also potentially leading to over-reliance if not properly integrated with hands-on forensic skills.

E. Comparison with Current Trends and Practices

Comparing the results with current trends and practices in digital forensics reveals a gradual shift towards incorporating advanced technologies and AI into forensic investigations. The students' use of Autopsy and ChatGPT aligns with the industry's movement towards more technologically integrated approaches. However, the varying degrees of accuracy across different tasks highlight the importance of ensuring that foundational forensic skills are not overshadowed by technological advancements.

F. The Role of ChatGPT in Analyzing the NIST Hacking Case

• Integration of AI in Forensic Education

In the analysis of the NIST Hacking Case, ChatGPT played a important role, demonstrating the practical application of artificial intelligence in forensic education. Its integration into the study provided a perspective on how AI can complement traditional forensic tools and methodologies.

• Facilitating Data Analysis and Interpretation

ChatGPT was utilized extensively for data analysis and interpretation. It assisted in breaking down complex forensic concepts, offering clarifications and insights that enriched students' understanding of the case. This AI-driven approach allowed for a more in-depth exploration of the forensic data, aiding students in identifying key artifacts and understanding their significance within the broader context of the case.

• Enhancing Research and Reporting Skills

Beyond data analysis, ChatGPT contributed significantly to the development of research and reporting skills among students. It guided them in structuring their findings, ensuring that their reports were coherent and comprehensive. This aspect of AI assistance was crucial in helping students articulate their analysis clearly and effectively, reflecting a higher standard of academic rigor.

• Reflection on AI's Impact on Learning

The utilization of ChatGPT in this study reflects a broader trend in educational practices, where AI tools are increasingly being used to enhance learning experiences. In digital forensics, where the analysis of complex data sets is paramount, AI can serve as a powerful ally, helping students navigate through challenging aspects of their research. However, it also raises important considerations about the balance between AI assistance and independent analytical skills, a balance that is crucial in the development of competent forensic professionals.

IV. CONCLUSION

The incorporation of ChatGPT in the NIST Hacking Case study underscores the potential of AI in forensic education. Its role in assisting with data analysis, enhancing research skills, and improving report quality highlights the benefits of integrating AI tools in academic settings. As the field of digital forensics continues to evolve, the use of AI in education will likely become an increasingly important aspect of preparing students for the demands of the profession.

This comprehensive analysis of student responses across various questions demonstrates a diverse range of understanding and skill levels in digital forensics. The results underscore the effectiveness of combining practical forensic tools with AI methodologies in education, highlighting areas of strength and potential improvement [5].

A. Key Takeaways from the Study

The analysis of the NIST Hacking Case study offers several key takeaways in the context of digital forensic education:

- **Effective Integration of Tools:** The integration of traditional forensic tools like Autopsy with advanced AI tools such as ChatGPT proved to be highly effective. This combination enhanced students' learning experience, providing them with comprehensive insights into forensic analysis.
 - **Varied Student Proficiency:** The study revealed varying levels of proficiency among students in digital forensics. While foundational concepts were well grasped, more complex tasks highlighted areas requiring deeper focus in the curriculum.
 - **Importance of AI in Education:** ChatGPT's role in aiding students through complex forensic concepts and in structuring their reports underscores the growing importance of AI in education. However, it also highlights the necessity to balance AI assistance with the development of independent analytical skills [5].
 - **Challenges in Data Analysis:** The large volume of data and the short time frame for analysis presented challenges, underscoring the need for efficient data processing methods in educational research.
- **Potential for Future Research:** The study opens avenues for future research, particularly in exploring the optimal integration of AI in forensic education and developing methods for efficient analysis of large-scale educational data.
 - **This exploration of the NIST Hacking Case** demonstrates the dynamic nature of digital forensic education and the potential of integrating traditional methodologies with modern technological advancements. As the field continues to evolve, the balance between technological reliance and foundational forensic skills will remain a key consideration in shaping competent digital forensic professionals.
 - **As deeper insight from this research** it is possible to see ChatGPT has been able to act as teaching assistant/lecturer in a role of helping students when real persons were not physically available.

REFERENCES

- [1] D.Delija,G.Sirovatka,D.Tuličić,M.Žagar,"Comparison of graduate specialist study of computing and specialist study of information security and digital forensics at the Zagreb University of Applied Sciences" // 42th International Convention on Information, Communication and Electronic Technology (MIPRO) - proceedings / Skala, Karolj (ur.). Rijeka: Hrvatska udruga za informacijsku i komunikacijsku tehnologiju, elektroniku i mikroelektroniku - MIPRO, 2019. str. 1423-1426 doi: 10.23919/MIPRO.2019.8756891
- [2] D.Delija,G.Sirovatka,D.Tuličić,M.Žagar,K.Hausknecht,D.Topolčić, S.Gruičić, "Implementation of virtual digital forensic class and laboratory for training, education and investigation" // 42th International Convention on Information, Communication and Electronic Technology (MIPRO) - proceedings / Skala, Karolj (ur.). Rijeka: Hrvatska udruga za informacijsku i komunikacijsku tehnologiju, elektroniku i mikroelektroniku - MIPRO, 2019. str. 49-54 doi: 10.23919/mipro.2019.8756801
- [3] TVZ „ELABORAT Specijalistički diplomski stručni studij Informacijska sigurnost i digitalna forenzika „, TVZ 2017,
- [4] L.Spitzer, "Leveraging Artificial Intelligence (AI) to Manage Human Risk“, SANS Blog, 7.10.2023, visted 10.10.2023 <https://www.sans.org/blog/leveraging-artificial-intelligence-ai-to-manage-human-risk-part-6-analyzing-documents-charts-and-spreadsheets/>
- [5] M.Scanlon,F.Breitinger,C.Hargreaves,J.Hilgert,J.Sheppard, "ChatGPT for digital forensic investigation: The good, the bad, and the unknown, Forensic Science International: Digital Investigation, Volume 46, Supplement, preprint, 2023, <https://www.sciencedirect.com/science/article/pii/S266628172300121X>, visited 2nd April 2024.