INFER: Enhancing Digital Forensics Education through Ready-to-Use Hands-on Labs with Portable Operating Environments

Tran Ngoc Bao Huynh, Haowen Xu, Brian Almaguer, Jun Dai, and Xiaoyan Sun(✉)

Worcester Polytechnic Institute, Worcester MA 01609, USA
{nhuynh1,hxu4,baalmaguer,jdai,xsun7}@wpi.edu

Abstract. As cybercrime increases annually, digital forensics, a subsection of cybersecurity that involves identifying, preserving and analyzing digital evidence, has seen a surge in demand over the years. Despite the need, there is a large shortage in the cybersecurity workforce, including digital forensics. Meanwhile, the community also faces a lack of free, interactive, and quality instructional resources for digital forensics education. In this paper, we introduce INFER (INstructional Forensics Education Resource), which develops a set of hands-on labs for digital forensics education. These labs were designed on different and essential topics from the basic to advanced levels. The hands-on activities are portable, comprehensive, expandable, adjustable, and easy to follow with step-by-step instructions and accompanying lab environments. We evaluated the effectiveness of these labs through students' surveys. A faculty development workshop was also hosted to disseminate the INFER materials and assess the usability. Based on the evaluation results, INFER is a valuable resource for providing quality digital forensics education.

Keywords: Digital Forensics Education, Hands-on Labs, Experiential Learning.

1 Introduction

Digital Forensics (DF) is a subsection of cybersecurity that focuses on identifying, collecting, analyzing, and preserving digital evidence for various digital systems and platforms, including mobile devices, networks, databases, and IoT devices. DF is essential not only for recovering deleted or damaged files from disks and devices but also plays a crucial role in criminal investigations, particularly in cases involving cybercrime.

Despite the growing demand and potential, there is a significant shortage of professionals in the cybersecurity field. Digital forensics, being a specialized subset of cybersecurity, is also facing a growing need for experts in this area. In 2024, the global cybersecurity workforce gap is nearing 5 million professionals, a 19.1% increase from 2023 [1]. This gap is expected to widen as new digital systems rapidly evolve. As society becomes increasingly reliant on technology and the threat of cyberattacks intensifies annually, the need for skilled cybersecurity professionals to defend against digital threats and investigate the cyber attacks has never been more critical.

Traditional training methods in digital forensics primarily emphasize theory and certifications. However, these approaches may not expose learners to sufficient practical exercises and hands-on experiences. High-quality digital forensics education stresses the importance of gaining practical experience with relevant forensics tools and platforms. Experiential learning, extensively studied in STEM fields, has demonstrated a positive impact on student learning outcomes. Yet, its effectiveness has not been thoroughly studied in the digital forensics field due to lack of systematic, comprehensive hands-on labs that are readily available and easily adaptable for in-depth research. As it stands, the most advanced hands-on training in digital forensics remains limited to a small audience.

Several recent digital forensics education projects [2–5] contribute to the field by developing specific courses (inherently a recipe of lectures and labs to fulfill learning outcomes) that cover one or more sub-branches (such as IoT forensics), or by pedagogically enhancing digital forensics education with specific technology (such as Augmented Reality). However, the lack of high quality labs remains a challenge. Besides, the impact of experiential learning in digital forensics education is still unclear.

Therefore, this paper presents a comprehensive instructional resource for digital forensics education and studies the impact of experiential learning based on a pool of newly developed hands-on labs. Specifically, this work develops an ***INstructional Forensics Education Resource (INFER)*** in the form of step-by-step hands-on labs with accompanying instructional operating environments, and research the labs' impact on student learning in digital forensics. The work in the paper answers the research question: *To what extent will the INFER labs impact student knowledge, skills, and attitudes regarding digital forensics?* More specifically, what is the impact towards the student learning outcomes in regards to the breadth of knowledge, skills, interest in forensics, and career readiness?

In this work, the designed INFER labs come with the required instructional operating environments so that instructors do not need to prepare them from scratch. The INFER labs are portable, comprehensive, expandable, and adjustable: 1) they systematically and comprehensively cover a number of forensics sub-areas in depth; 2) they are ready-to-use with the required lab environments and materials; and 3) they can be adopted for different levels of digital forensics education, such as the undergraduate and graduate level courses. Like SEED Labs [6], INFER can be adopted with proper adjustment by other courses in high school education and workforce development such as: summer academies or summer camps (e.g., GenCyber [7]); community college courses; and trainings for digital forensics practitioners, law enforcement personnel, and IT professionals from nonprofit organizations and government agencies.

2 Background and Related Work

2.1 Cybersecurity Education

There are several approaches to teach and introduce cybersecurity concepts to new learners, including courses, workshops, games, and cyber ranges. Traditional methods often rely on lectures focused on theoretical knowledge and the concepts of cybersecurity [8]. Cyber ranges are valuable tools for simulating real-time cyber scenarios [9–11]; however, they can be costly and often complex and challenging for beginners. Hands-on labs [6], workshops [12, 13], and serious games [8, 14, 15] are effective tools for engaging new learners. These methods allow learners to gain practical experience through real-world use cases, fostering deeper engagement with the material, skill development, and a better understanding of core concepts. While games offer interactive and visually appealing experiences, they often lack the depth necessary to build proficiency with the tools used in the field. For all the above mentioned methods, most of them are for general cybersecurity education and not directly designed for digital forensics education

2.2 Digital Forensics Education

There remains a notable lack of comprehensive curricular and teaching materials for digital forensics, particularly at the undergraduate and postgraduate levels. While some efforts have been made to enhance digital forensics education through hands-on labs and activities [16–19], they might have various limitations. Some works do not provide sufficient comprehensiveness or depth to cover the different topics in digital forensics. Some provides a limited set of forensics tools or platforms. Most do not provide a step-by-step instruction to guide students in the learning process. In addition, these labs often do not come with the accompanying environment that is already configured with proper operating systems, software, and required lab materials (such as acquired images of disks, text/audio/video files, etc). Setting up the lab environment and creating the lab materials from scratch can often be very time consuming.

3 INFER - Hands-on Labs for Forensic Education

3.1 Why

The absence of quality hands-on labs renders many digital forensics courses impractical and superficial. For example, students completing a course may understand the concept of data acquisition (acquiring evidence), but they may not know how to actually zero-out (completely wipe) a target disk, construct a brand-new file system on it, and then perform data acquisition in a Linux environment. Similarly, they may have learned the concept of file carving (recovering the files from unallocated areas), but they may not know how to manually locate the file fragments on the disk and reassemble them to recover the file. Hence, well-designed hands-on labs will be indispensable for helping students delve into digital forensics and gain practical experience. Moreover, the delivery of these labs can help strengthen our understanding of the distinctive impact of experiential learning in digital forensics education.

Therefore, the INFER labs are designed to address gaps in current digital forensics education by being portable, comprehensive, expandable, adaptable, and ready for use by anyone with the provided lab environments and materials. By creating a structured learning framework, we can effectively convey advanced concepts to new learners while keeping them engaged through practical, real-world applications and exercises.

3.2 How

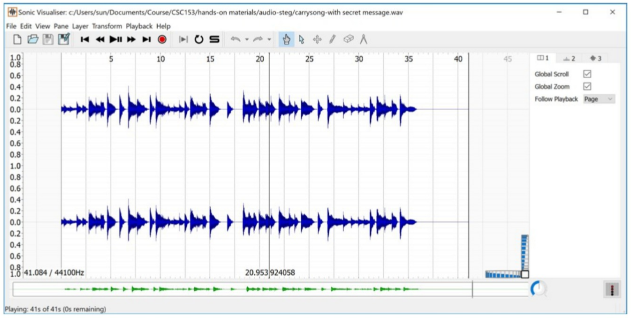
Our work contains 18 step-by-step, hands-on exercises covering 12 essential topics in digital forensics. These topics are categorized and range from foundational concepts, such as data acquisition, to advanced and contemporary areas, including social network forensics, memory forensics, and reverse engineering. Foundational labs are estimated to take about an hour. Intermediate problems will require approximately two to four hours to complete, while advanced activities will take four hours or more. Most labs can be divided into multiple modules to alleviate complexity and allow students to work on a smaller task at a time.

Recognizing that students and learners are often highly motivated to explore the real-world role of a digital forensics investigator [20], we have designed many of the labs to be problem-based and centered around authentic digital forensics cases. As exemplified by Fig. 1, each lab includes detailed step-by-step instructions with corresponding screenshots so that students can work on the labs following these instructions, requiring minimum help or guidance from the instructors. The instructions and needed lab materials (virtual machine images, artifact files, etc.) are accessible through the project website [21] and GitHub [22].

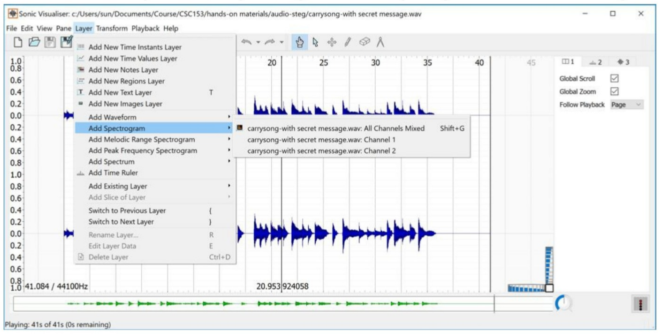
To provide a comprehensive learning experience, the labs utilize CAINE, Windows, and Kali Linux operating systems (OS). This variety ensures learners are prepared to navigate different OS environments they may encounter in professional practice. Windows, as one of the world's most widely used desktop operating systems, is a critical platform for digital forensic investigations. Familiarity with its essential tools and mechanisms is indispensable for effective forensic analysis. Kali Linux is an open-source distribution specifically tailored for penetration testing, computer forensics, ethical hacking, and reverse engineering [23]. Similarly, CAINE (Computer Aided INvestigative Environment) is an open-source Linux distribution designed to support digital forensic investigations [24]. Both operating systems come equipped with an extensive array of pre-installed forensic tools, enabling tasks such as disk imaging, analysis, and memory forensics. These tools provide the foundational capabilities required for collecting and analyzing digital evidence.

In addition to the pre-installed tools, the labs incorporate other free and readily accessible software such as WinPMem, Ghidra, and FTK Imager. For

Step 21: Start Sonic Visualiser program. Click on **File**->**Open** to open the carrysong-with secret message.wav file.


Sonic Visualiser: c:/Users/sun/Documents/Course/CSC153/hands-on materials/audio-steg/carrysong-with secret message.wav
File Edit View Pane Layer Transform Playback Help
Global Scroll
Global Zoom
Follow Playback Page
41.084 / 44100Hz
20.953|924058
Playing: 41s of 41s (0s remaining)

Step 22: Click on **Layer**->**Add Spectrogram**-> **carrysong-with secret message.wav: All Channels Mixed**.


Sonic Visualiser: c:/Users/sun/Documents/Course/CSC153/hands-on materials/audio-steg/carrysong-with secret message.wav
File Edit View Pane Layer Transform Playback Help
Add New Time Instants Layer
Add New Time Values Layer
Add New Notes Layer
Add New Regions Layer
Add New Text Layer T
Add New Images Layer
Add Waveform
Add Spectrogram
Add Melodic Range Spectrogram
Add Peak Frequency Spectrogram
Add Spectrum
Add Time Ruler
Add Existing Layer
Add Slice of Layer
Switch to Previous Layer {
Switch to Next Layer }
Rename Layer... R
Edit Layer Data E
Delete Layer Ctrl+D
carrysong-with secret message.wav: All Channels Mixed Shift+G
carrysong-with secret message.wav: Channel 1
carrysong-with secret message.wav: Channel 2
Global Scroll
Global Zoom
Follow Playback Page
41.084 / 44100Hz
20.953|924058
Playing: 41s of 41s (0s remaining)

Step 23: You can move around to display the secret message.

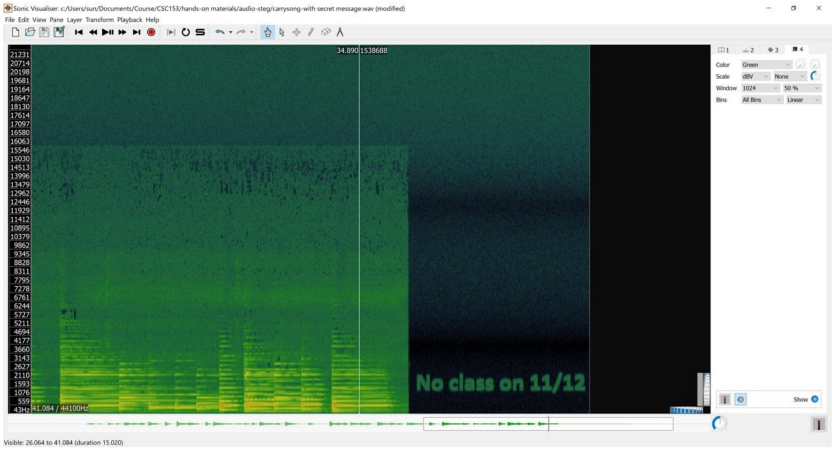
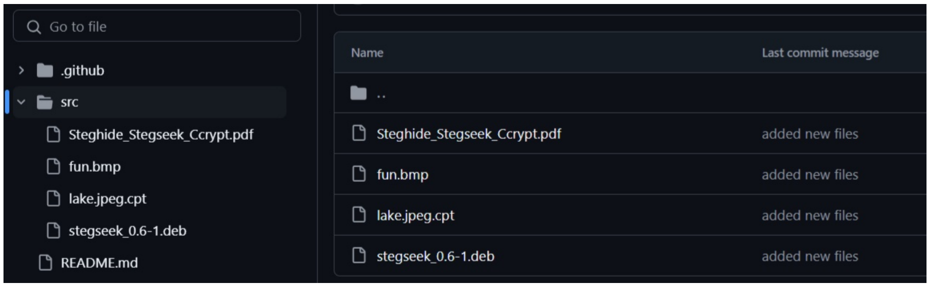

Sonic Visualiser: c:/Users/sun/Documents/Course/CSC153/hands-on materials/audio-steg/carrysong-with secret message.wav (modified)
File Edit View Pane Layer Transform Playback Help
34.890|1538688
Color Green
Scale dBV None
Window 1024 50 %
Bins All Bins Linear
No class on 11/12
41.084 / 44100Hz
Show
Visible: 26.064 to 41.084 (duration 15.020)

Fig. 1. An excerpt of step-by-step instructions from example INFER Lab: Steganography with Audio File.

tools requiring separate installation, we provide detailed installation links and setup instructions within the lab documentation.

Each lab directory in the GitHub repository contains comprehensive materials, including lab instructions, relevant files, and tools for practice. For instance, Fig. 2 highlights a steganography-focused repository. This repository includes a PDF file with lab instructions, input files such as “fun.bmp” and “lake.jpeg.cpt,” and the tool “stegseek_06.1.deb” for practice. To reinforce learning, each lab concludes with review questions and optional bonus challenges. These challenges are designed to deepen the learner’s understanding and encourage independent problem-solving. While step-by-step instructions are provided for the primary tasks, the bonus challenges require learners to apply the knowledge and skills gained during the lab to complete the tasks independently.



Name	Last commit message
..	
Steghide_Stegseek_Ccrypt.pdf	added new files
fun.bmp	added new files
lake.jpeg.cpt	added new files
stegseek_0.6-1.deb	added new files

Fig. 2. Steganography hands-on repository.

4 Evaluation

4.1 Student Perspective

Studies were conducted towards students who used INFER labs to assess the impact of these labs on students’ learning effectiveness and their attitude towards digital forensics. The participants were from digital forensics courses at different levels: the undergraduate level and the graduate level. The majority of the students are pursuing majors in computer science, cybersecurity, or related fields. Our data collection and processing procedures adhered to ethical guidelines for human subject research, and has obtained the Institutional Review Board (IRB) approval. We conducted different surveys with approximately 50 college students (ages 18 and older). This include the pre-course and post-course surveys that evaluate aspects such as students’ level of knowledge, interest, confidence, and career readiness, and also surveys on each hands-on lab that they’ve work on to evaluate the effectiveness for each individual lab. Please note that the surveys for individual labs were conducted with only a subset of labs due to the limited time allocated for labs within the courses. It is not feasible to incorporate all the designed labs, as each course requires specific topics to be covered.

In the pre-course survey, students were asked to rate their interest in Digital Forensics on a scale from 1 (low) to 5 (high). We found that 98% of the students expressed interest in the topic. Over half of the students were considering or interested in pursuing a career related to digital forensics. However, most students were initially unfamiliar with the digital forensics and perceived it as a complex subject. When being asked about their confidence in their skills and career readiness in digital forensics, only 15 out of 51 students reported average or high confidence, with just 3 students selecting a rating of 4 or 5.

More than 60% of the students were unfamiliar with how to set up a Virtual Machine (VM) for a digital forensic workstation, a fundamental yet critical step in forensics and many other cybersecurity tasks. Most undergraduate students were unable to perform this task, while 60% of the graduate students were comfortable preparing a VM environment before the course. In all labs, we emphasize the importance of ensuring the integrity of the evidence data. Since the evidence data and devices might contain malware, opening them on the host machine is risky. Additionally, data on the investigator's host machine could interfere with the evidence, compromising its integrity. Therefore, understanding how to set up a sandbox, such as the VM environment, to handle potentially harmful data is essential in cybersecurity, as well as in digital forensics.

Only 15% of the students had experience with Linux or Windows data acquisition, the first and most crucial step in collecting and retrieving valid data. Unlike Network Forensics, which involves tools like Wireshark and is typically covered in Computer Network courses, most other topics in digital forensics were unfamiliar to the students.

In the surveys for individual hands-on activities, we gathered student feedback through rating scale questions and short-answer responses to assess the labs' impact on their learning in Digital Forensics. Specifically, we ask questions such as: *Do you feel Activity 6 was effective in helping you learn digital forensics concepts such as how to use Winhex to recover graphics files? Does Activity 6 make you interested in the topic of using Winhex to recover graphic files?*

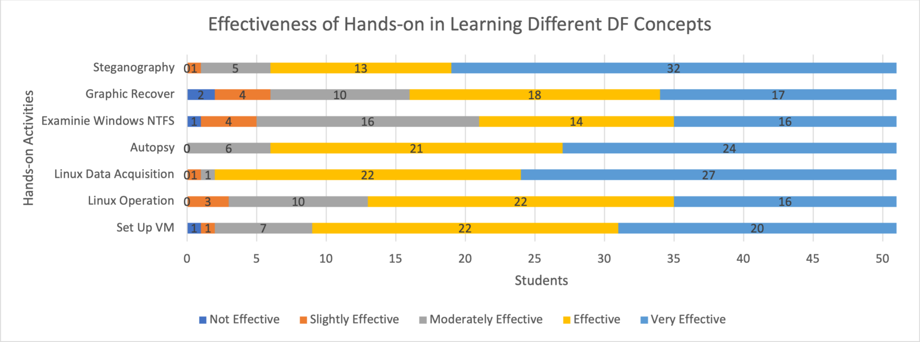


Fig. 3. Effectiveness of INFER labs for learning different DF concepts.

As shown in Fig. 3, when students were asked if the hands-on labs helped them effectively learn digital forensic concepts, most participants found the activities helpful. However, there were often students who ran into technical challenges for some labs. For example, some students encountered challenges during the "Set Up VM" task, particularly when setting up the virtual environment on Mac machines. Due to Apple's proprietary silicon chips, many x86_64 VM images are incompatible with Mac's unique architecture. We recognize this issue and have worked to develop additional instructions for these special cases. For Mac machines, alternative software and setup steps may be required. For example, VMware Fusion or Workstation can be used on Mac as alternatives to VirtualBox, which is no longer supported on mac OS. However, VMs must be compatible with Mac processors (i.e., ARM architecture) to run on Mac, even when using VMware. For VM images incompatible with Mac processors, the QEMU emulator [25] provides an effective solution. QEMU is a free, open-source software that is easy to install and can be managed efficiently through the command line in the terminal.

In addition to the "Set Up VM" activity, students who rated other tasks as "Not Effective" or "Slightly Effective" suggested the inclusion of instructional videos. While we indeed provide videos to instructors to better support the teaching, we encourage students to first attempt the exercises on their own. Working on the lab independently by following the instructions, addressing the technical challenges, and answering the lab questions can promote better comprehension and retention compared to simply replicating steps from a video.

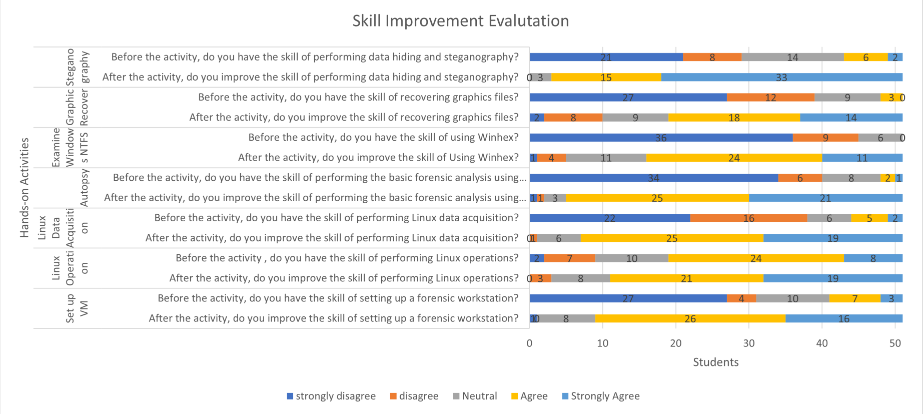


Fig. 4. Students' skill improvement through INFER labs.

The improvement in students' skills before and after participating in the activities is significant, as illustrated in Fig. 4. For instance, in the "Examine Windows NTFS" activity, none of the students initially possessed the skill to use WinHex. However, after completing the hands-on lab, this number surged to 35 students, reflecting an almost 70% improvement. Similarly, activities such as “Steganography” and “Set Up VM” demonstrated nearly 100% skill enhancement rates. Upon examining the cases where students reported no improvement in their skills, their short-answer feedback revealed that these instances were primarily due to technical issues with Mac machines, as previously explained.

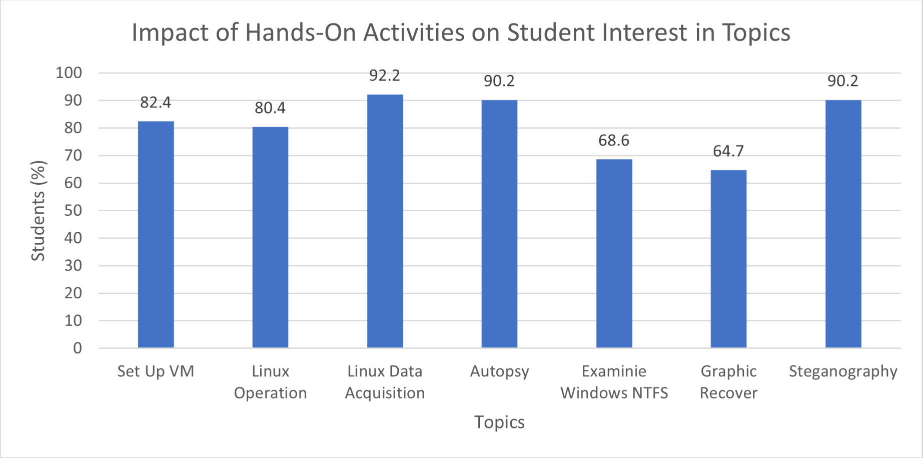


Fig. 5. Impact of INFER labs on student interest in learning DF.

As shown in Fig. 5, the INFER hands-on activities significantly boosted students’ interest in digital forensics, while effectively enhancing their skills across various topics and tasks. Students were asked to rate their interest levels on a scale from 1 (Not Interested) to 5 (Very Interested) in response to whether the activities increased their capability of using the tools and performing digital forensic tasks. The activities that garnered the most interest included steganography, data acquisition, and real-world case-based autopsy labs. On the other hand, activities such as “Windows NTFS” and “Graphic Recovery” required extensive understanding and interaction with hex data files, which proved to be more challenging for many undergraduate students. Consequently, these topics received lower interest ratings among this group. However, the inspiration rates among graduate students for these two topics were notably higher, at 90% and 70%, respectively.

After completing the course, students also completed a post-course survey. As shown in Fig. 6, there was a significant increase in the number of students who somewhat agreed or strongly agreed that their ability to understand and perform digital forensic tasks had improved. Nearly all students were now able to set up their own VM for forensic investigations and perform data acquisition in both Windows and Linux, compared to just 10–20% at the start of the course.

For advanced topics such as “Android Forensics” and “Drone Forensics”, none of the students had prior experience with the material before the course. This

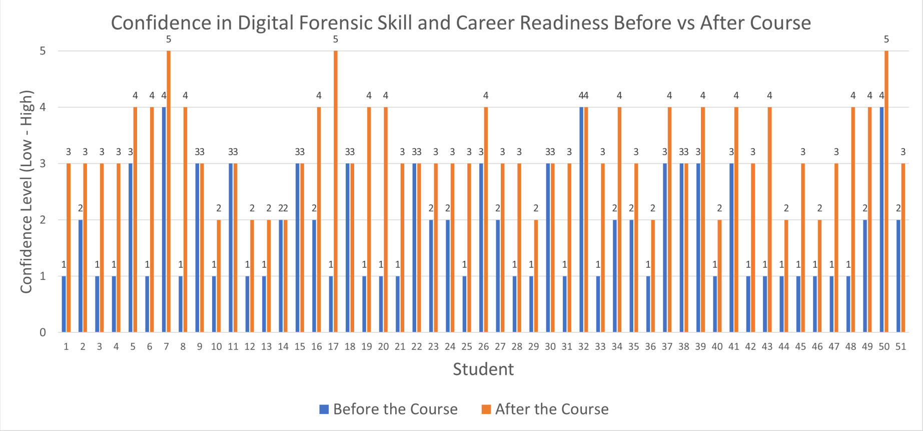


Fig. 6. Students' confidence in DF skill and career readiness before vs. after the course.

is partly due to the fact that many of the tools involved are not free, and not everyone has access to expensive smartphone or drone technology.

Additionally, we found that labs focusing on binary analysis or assembly code, such as "Reverse Engineering", as well as labs requiring a combination of various digital forensics skills and knowledge—such as "Social Network Forensics", "Memory Forensics", and "Drone Forensics"—proved to be more challenging for students. As a result, the understanding and confidence levels for these exercises were generally lower compared to those for other labs.

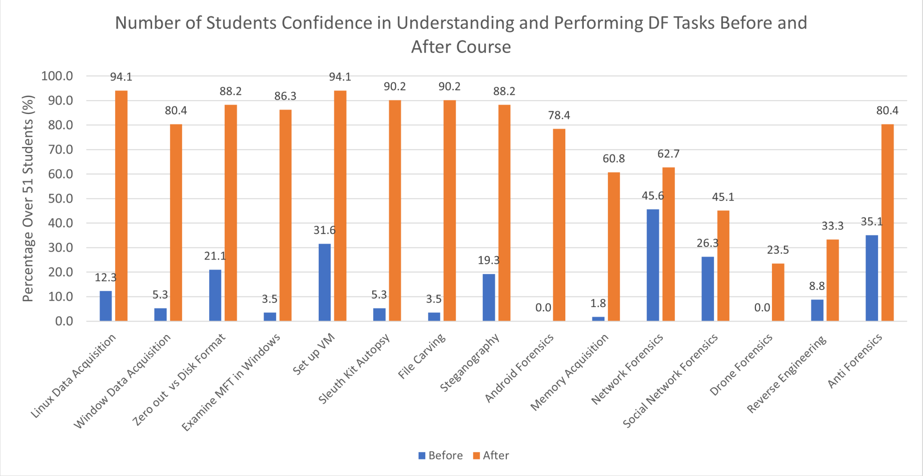


Fig. 7. Number of students confident in performing DF tasks before vs. after the course.

Nonetheless, the feedback we received from students after completing the hands-on tasks was largely positive. Below are some of the comments from students following the course and their hands-on lab experiences:

> *"It is a truly enriching experience to learn more about digital forensics through hands-on activities with different tools, such as how to recover deleted or hidden data and bypass security measures on Android."*
> *"Much more interested now than I was before. May choose this as my career path. Thanks for the introduction!"*
> *"This was a phenomenal experience. I look forward to implementing what I've learned in the future. I look to brush up on a few more concepts and skills before applying them to a job. This class is a wonderful stepping stone".*
> *"Overall, a great and engaging class. Really enjoyed the activities and gained a greater knowledge in digital forensics".*
> *"Very interesting and allows you to explore different areas of forensics".*

4.2 Educator Perspective

This project was also evaluated from the educator's perspective by collecting feedback from two groups: K-12 teachers and college faculty. Two major efforts were made to gather their feedback: 1) we used the INFER labs in a graduate-level summer course in digital forensics for K-12 teachers (mostly high school teachers); 2) we hosted a 2-day faculty development workshop to disseminate the labs to college professors.

The graduate level summer course in digital forensics has approximately 20 teachers from K-12 schools (mostly high schools) nationwide. All participants were teaching or planning to teach courses in cybersecurity, or other courses related to computer science, engineering, or similar disciplines. Before participating in the hands-on labs, most teachers had little to no familiarity with digital forensics, with only about 30% having prior experience or confidence in the subject. Considering that most teachers were teaching at the high school level, the course used only a small subset of INFER labs as the hands-on activities: "Linux Data Acquisition", "Zero and Disk Formatting", "Setting Up Virtual Machines for Digital Forensics Investigations", and "Steganography". The feedback collected from teachers on confidence is presented in Fig. 8 below. Despite not covering all topics, hands-on lab practice based on INFER significantly improved participants' confidence, with 100% reporting confidence in performing Digital Forensics tasks by the end of the course. This indicates that the teachers gained sufficient technical background to teach their students in these topics confidently.

A two-day development workshop was also hosted for faculty from community colleges and four-year universities to disseminate the designed labs. The event brought together 11 faculty members and professors from various institutions across the United States. We provided an introduction of the INFER project and also a training on how to use the labs in digital forensics courses. Participants also received a in-depth guided walkthrough of five hands-on labs

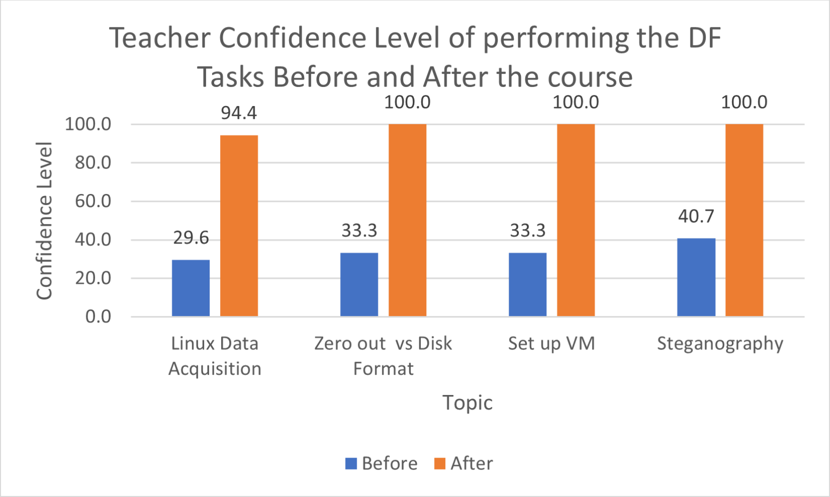


Fig. 8. Teachers' confidence level in performing DF tasks before vs. after the course.

during the workshop, and then they were given the opportunity to work on the labs independently taking the students' role. These five labs, including "Linux Data Acquisition with Zero Out and Disk Formatting", "Sleuth Kit Autopsy", "Image Steganography", "Audio Steganography", and "Reverse Engineering", are examples demonstrating how the faculty can use them in their own class. With these examples, they also know how to access and use the materials for the remaining labs. At the end of the workshop, participant surveys were conducted to get the faculty's opinions on INFER labs' design and effectiveness. All participants (100%) found the INFER labs valuable and would recommend them to colleagues or friends teaching cybersecurity or digital forensics-related courses. Many of them have plans to adopt INFER labs in their own courses or start a digital forensics course in their institution.

Below are reflections and feedback from some teachers and professors who participated in the course and workshop:

> *"The synchronous instructions coupled with the hands-on labs offered the best of both worlds."*
> *"The hands-on labs are really useful in my teaching and research."*
> *"I really liked the accessibility of the labs and being able to continue to work with them outside of the workshop."*
> *"We would like to use the labs in our digital forensics courses."*
> *"The INFER labs offer multiple opportunities for advancing digital forensics (DF) research and education. We can create new courses for undergraduate and graduate students, integrating selected DF labs into these new courses as well as existing ones. Additionally, we can conduct DF research to develop new techniques that enhance current DF methodologies and skills."*

4.3 Limitations and Future Work

Keeping software up to date is essential for rapid technological advancements. For instance, Android, IoT, and drone software evolve very quickly, making some lab tools potentially obsolete for current or future applications. Continuous effort and dedicated human resources are required to track and update tools accordingly.

Additionally, some software, such as Belkasoft X and WinHex, offer limited-time free access or restrict advanced features in their free versions, which may hinder long-term learning and the ability to perform complex tasks. To enhance accessibility, we are working on extending lab instructions to Mac environments, particularly in preparing virtual machines and images, as several tools are not Mac-compatible and require alternative setup procedures.

For future work, we aim to integrate more real-world attack scenarios and case studies, as suggested by [18, 20]. This will provide students with a more practical, engaging, and effective learning experience. We will periodically review and update the tools and software to ensure they remain up-to-date and accessible for use.

5 Conclusion

The demand for a highly skilled cybersecurity workforce, particularly in digital forensics, continues to grow. INFER labs aim to bridge this gap by offering a practical, interactive, comprehensive, and readily-available resource for digital forensic education. Survey results from students, teachers, and college faculty provided very positive feedback, reinforcing the project's usability, effectiveness, and potential to enhance digital forensics training. As INFER is free and open source, future collaborations and contributions can further expand and refine the materials, ensuring they remain practical and aligned with real-world applications.

6 Acknowledgment

Drs. Xiaoyan Sun and Jun Dai are supported by NSF DGE-2409851. Dr. Jun Dai is also supported by NSF DGE-1934285/2403603.

References

1. ISC2 Cyber Security Workforce Study, "Global Cybersecurity Workforce Prepares for an AI-Driven World," (2024), last accessed 2025/01/27.
2. Cybersecurity Education Workshop 2019. CyberEd 2019. https://sceweb.sce.uhcl.edu/cybercorps/workshop.html, last Accessed 2025/4/1.
3. CFEAR: Cyber Forensics Education via Augmented Reality - NSF Award Research: SaTC-EDU: EAGER: CFEAR: Cyber Forensics Education via Augmented Reality. https://www.nsf.gov/awardsearch/showAward?AWD_ID=1500055&Historical Awards=false, last accessed 2025/1/27.

4. Expanding Digital Forensics Education with Artifact Curation and Scalable - NSF Award Research: SaTC: EDU: Expanding Digital Forensics Education with Artifact Curation and Scalable, Accessible Artifact Exercises. https://www.nsf.gov/awardsearch/showAward?AWD_ID=1900210&Historical Awards=false, last accessed 2025/1/27.
5. Online Digital Forensics Courses and Labs for Students and Professionals - NSF Award Research: SaTC: EDU: Online Digital Forensics Courses and Labs for Students and Professionals. https://www.nsf.gov/awardsearch/showAward?AWD_ID=1802701&Historical Awards=false, last accessed 2025/1/27.
6. Du, W., Wang, R.: SEED: A suite of instructional laboratories for computer security education. Journal on Educational Resources in Computing (JERIC), 8(1), 1-24 (2008). https://doi.org/10.1145/1348713.1348716
7. GenCyber. https://public.cyber.mil/gencyber/, last accessed 2025/1/27.
8. Friedl, S., Glas, M., Englbrecht, L., Bohm, F., Pernul, G.: ForCyRange: An Educational for IoT Cyber Range for Live Digital Forensics. IFIP WISE (June, 2022). https://doi.org/10.1007/978-3-031-08172-9_6
9. Katsantonis, M.N., Manikas, A., Mavridis, I., Gritzalis, D.: Cyber range design framework for cyber security education and training. Int. J. Inf. Secur. 22, pp. 1005–1027 (2023). https://doi.org/10.1007/s10207-023-00680-4
10. Leitner, M., Frank, M., Hotwagner, W., Langner, G., Maurhart, O., Pahi, et al.: AIT Cyber Range: Flexible Cyber Security Environment for Exercises, Training, and Research. In Proceedings of the 2020 European Interdisciplinary Cybersecurity Conference (EICC '20). Association for Computing Machinery, New York, NY, USA, Article 2, 1–6 (2021). https://doi.org/10.1145/3424954.3424959
11. Oh, S. K., Stickney, N., Hawthorne, D., Matthews, S. J.: Teaching Web-Attacks on a Raspberry Pi Cyber Range. In Proceedings of the 21st Annual Conference on Information Technology Education (SIGITE '20). Association for Computing Machinery, New York, NY, USA, 324–329. https://doi.org/10.1145/3368308.3415364
12. Yuan, X., Williams, K., Yu, H., Rorrer, A., Chu, B. T., Yang, et al.: Developing faculty expertise in information assurance through case studies and hands-on experiences. 2014 47th Hawaii International Conference on System Sciences. IEEE, 2014. https://doi.org/10.1109/HICSS.2014.606
13. Englbrecht, L., Pernul, G.: A serious game-based peer-instruction digital forensics workshop. In: Drevin, L., Von Solms, S., Theocharidou, M. (eds.) WISE 2020. IAICT, vol. 579, pp. 127–141. Springer, Cham (2020). https://doi.org/10.1007/978-3-030-59291-2_9
14. Friedl, S., Reittinger, T., Pernul, G.: Digital Detectives: A Serious Point-and-Click Game for Digital Forensics. In: Drevin, L., Leung, W.S., von Solms, S. (eds) Information Security Education - Challenges in the Digital Age. WISE 2024. IFIP Advances in Information and Communication Technology, vol 707. https://doi.org/10.1007/978-3-031-62918-1_9
15. Pan, Y., Schwartz, D., Mishra, S.: Gamified digital forensics course modules for undergraduates. 2015 IEEE Integrated STEM Education Conference. IEEE (2015). https://doi.org/10.1109/ISECon.2015.7119899
16. Chi, H., Jones, E. L., Chatmon, C., Evans, D.: Design and implementation of digital forensics labs: A case study for teaching digital forensics to undergraduate students. In Proceedings of the Conference (Vol. 672, No. 057, p. 193) (2009).
17. Ward, P.: Development of a Small Cybersecurity Program at a Community College. Information Systems Education Journal, 19(3), 4-10 (2021).

18. Xu, W., Deng, L., Xu, D.: Towards Designing Shared Digital Forensics Instructional Materials. IEEE COMPSAC (2022). https://doi.org/10.1109/COMPSAC54236.2022.00025
19. Wang, X., Bhuse, V., Sutton, S.: The Design and Development of Hands-on Activities for Digital Forensics Education. Journal of The Colloquium for Information Systems Security Education, Volume 11, No. 1 (2024). https://doi.org/10.53735/cisse.v11i1.187
20. Wang, X., Bai, Y., Goda, B.: Project Design and Implementation for Digital Forensics Education. In Proceedings of the 20th Annual SIG Conference on Information Technology Education (SIGITE '19). Association for Computing Machinery, New York, NY, USA, 33–38 (2019). https://doi.org/10.1145/3349266.3351402
21. INFER Project Website, https://wp.wpi.edu/infer/, last accessed 2025/4/2.
22. INFER Project Github Repository, https://github.com/WPI-LIONS-Group/INFER.git, last accessed 2025/4/2.
23. Kali Linux, https://www.kali.org/, last accessed 2024/12/21.
24. Caine, https://www.caine-live.net/, last accessed 2024/12/21.
25. QEMU, https://www.qemu.org/download/, last accessed 2025/1/27.