Towards Development of Ready-to-Use Hands-on Labs with Portable Operating Environments for Digital Forensics Education

Tran Ngoc Bao Huynh
Department of Computer Science
Worcester Polytechnic Institute
Massachusetts, USA
nhuynh1@wpi.edu

Haowen Xu
Department of Computer Science
Worcester Polytechnic Institute
Massachusetts, USA
hxu4@wpi.edu

Brian Almaguer
Department of Computer Science
Worcester Polytechnic Institute
Massachusetts, USA
baalmaguer@wpi.edu

Jun Dai
Department of Computer Science
Worcester Polytechnic Institute
Massachusetts, USA
jdai@wpi.edu

Xiaoyan Sun*
Department of Computer Science
Worcester Polytechnic Institute
Massachusetts, USA
xsun7@wpi.edu

***Abstract*—Digital forensics is a critical field that plays an essential role in investigating cyber crimes, security incidents, and other crimes utilizing digital devices. Despite the heightened need for more experts in this field, the workforce faces constant shortages. For effective workforce development, the field currently lacks accessible, engaging, and valuable educational materials. To combat this issue, we propose INFER, a set of instructional hands-on labs for digital forensics education. In these labs, we designed an experiential learning experience that is a comprehensive program that is easily accessible for different levels of education in a portable environment and can be used on different operating systems. We conducted a study with students and had them take surveys before and after the labs to determine the value of the labs. We also hosted a workshop to invite professors and educators in the field to evaluate the usability of the materials. Based on the results, INFER is a beneficial resource that can help develop a future workforce of digital forensics professionals.**

***Index Terms*—digital forensic education, hands-on, labs**

I. Introduction

Cybersecurity threats have evolved into a critical national security challenge in today's increasingly interconnected world. Nearly everything—from simple household appliances like lights and toasters to complex transportation systems such as cars and aircraft—is connected to the internet or cloud infrastructure. This hyper-digital ecosystem demands robust security measures to protect against vulnerabilities, requiring highly skilled professionals and continuous technological innovation and talent development.

As cyber threats undergo rapid iteration and technological advancement, digital forensics (DF) becomes an indispensable field that plays a core role in both network defense and incident response. Beyond cybersecurity, its applications span multiple fields such as criminal investigations, financial security, and cybercrime prevention. For instance, in cybersecurity, digital forensics enables the identification of attack vectors, tracking adversaries, and restoring compromised systems. In other domains, it can extract critical evidence from electronic devices for criminal cases, provide a scientific basis for judicial decisions, and enable real-time monitoring of suspicious activities, such as suspicious transactions in the financial sector. These examples highlight the growing importance of digital forensics across disciplines. However, the rapid growth of cyber threats is met with a severe talent shortage in digital forensics. Globally, an estimated 4.8 million cybersecurity professionals are needed to ensure organizational security [1], and this shortage poses significant risks. Statistics reveal that 58% of cybersecurity professionals believe skill gaps put their organizations at high risk [1]. This talent deficit exacerbates the risks of data breaches, delayed incident responses, and financial losses, underscoring the urgent need for systematic workforce development.

Addressing this challenge requires high quality training in digital forensics to enhance workforce development. To equip future digital forensics professionals with the skills to address evolving challenges, it is critical to design practical and sound educational resources. However, practical hands-on experiences for digital forensics education and professional training remain limited for several reasons: 1) Most mature training avenues for digital forensics are mainly profit-driven; 2) Some free avenues emphasize basic concepts of digital forensics, but do not offer comprehensive hands-on labs. 3) Scattered resources provide coarse-grained labs with minimal instruction yet lack systematic coverage and depth for education and training purposes. 4) In cases where lab instructions are available, the environment setups and troubleshooting can be

*Corresponding author: Xiaoyan Sun (xsun7@wpi.edu)

daunting and time consuming. The absence of quality hands-on labs makes many DF courses impractical and superficial.

Therefore, in this paper, we introduce the design of a lab suite, INFER (INstructional Forensics Education Resource), for digital forensics education. The INFER suite includes hand-on labs with step-by-step instructions, as well as the accompany operating environment for the labs. The designed INFER labs are comprehensive, ready-to-use, expandable, and adjustable to educate students at various levels. The main contributions of this paper are as follows:

- Design rationale of INFER labs. This paper presents the design rationale behind the INFER labs and explain how the labs are developed based on theoretical principles. We provide a detailed description for developing digital forensics educational materials, covering key steps from resource design to implementation to support educators in creating more effective learning tools. The design rationale presented in this paper can inspire the development of other education resources.
- Portable Operating System Integration. This paper presents the development of the accompanying portable instructional operating environments for the INFER labs. The integration of portable operating systems into the educational resources enables practice-oriented learning experiences and significantly saves instructors efforts to prepare the lab environments.
- Evaluating usability of designed labs. This paper also assesses the usability of the designed INFER labs by integrating the INFER labs into related undergraduate and graduate level digital forensics courses, and disseminating the labs to other faculty through a faculty development workshop. We presents the feedback collected from students and faculty on aspects such as the instruction clarity and difficulty level of labs.

II. Background and related work

A. Digital Forensics

Digital Forensics is a subfield within cybersecurity that involves recovering, preserving, and analyzing data from electronic devices and digital traces, ensuring the integrity and admissibility of the evidence. It is important for fields such as criminal investigations, regulatory compliance, incident response, and cybercrime prevention. By uncovering hidden, deleted, or encrypted data, digital forensics provides actionable insights that guide legal and organizational decision-making.

The process of Digital Forensics generally consists of four main steps, as shown in Fig. 1:

1) Preparation: Proper planning and setup of tools, protocols, and permissions are critical to ensure a compliant and efficient investigation. This includes defining the investigation scope and securing the chain of custody.
2) Data Acquisition: Investigators use specialized tools to collect data from devices, such as imaging hard drives or extracting mobile device data. This step focuses on creating unaltered copies of the data while verifying their integrity using hash values.
3) Data Analysis: Forensic experts analyze the acquired data to uncover meaningful insights. Techniques include recovering deleted files, decoding encrypted data, and correlating logs. Advanced methods, such as timeline analysis and AI-driven tools, enhance the efficiency of this stage, particularly when handling large datasets.
4) Reporting: Findings are documented in a legally defensible report, summarizing methodologies, evidence, and conclusions. Clear visualizations and structured summaries are often included to aid non-technical associates.

The evolution of digital forensic tools has significantly enhanced the field. Tools such as EnCase [2], FTK (Forensic Toolkit) [3], and open-source platforms (e.g. Autopsy [4]) have become industry standards, enabling professionals to process diverse evidence types systematically. Meanwhile, integrating AI and big data analytics has further streamlined the analysis of complex cases. Despite these advancements, most tools require substantial expertise and are not readily adaptable for educational purposes, highlighting the need for simplified, practice-oriented resources.

As technology evolves, so do the challenges in digital forensics. Investigations now encompass mobile devices, Internet of Things (IoT), cloud computing, and encrypted environments, all introducing new complexities. Additionally, attackers employ anti-forensics techniques, such as data obfuscation or deletion, to hinder investigations.

Another pressing challenge is the shortage of structured and inclusive educational materials. Many current resources are either overly specialized, too generic, or lack practical components. For example, free resources like the Federal Virtual Training Environment [5] focus on basic concepts but provide limited hands-on experience. This lack of accessible and practice-oriented materials leaves learners unprepared for real-world challenges, widening the talent gap in the field.

This paper aims to create educational materials that integrate practical labs and easy-to-adopt operating environments. By providing accessible, cost-effective, and adaptable resources, we aim to bridge the talent gap and equip aspiring professionals with the skills necessary to tackle the complexities of digital forensics problems.

B. Current Research in the Digital Forensics Education

Practical hands-on experiences for digital forensics education and professional training remain limited, particularly in the availability of publicly accessible, hands-on instructional materials tailored for digital forensics education.

Most existing training programs cater to specific audiences or are driven by profit motives. For example, mature training programs offered by organizations such as SANS, Cyber5W, TCM Security, and EC Council [6]–[9] primarily target industry professionals. They are often priced very high, making them inaccessible to a broader audience. While some free training options exist, they are often restricted. For instance, Nw3C training [10] is exclusively available to specific regulatory agencies, such as law enforcement. Additionally, free programs supported by competitive scholarships, like

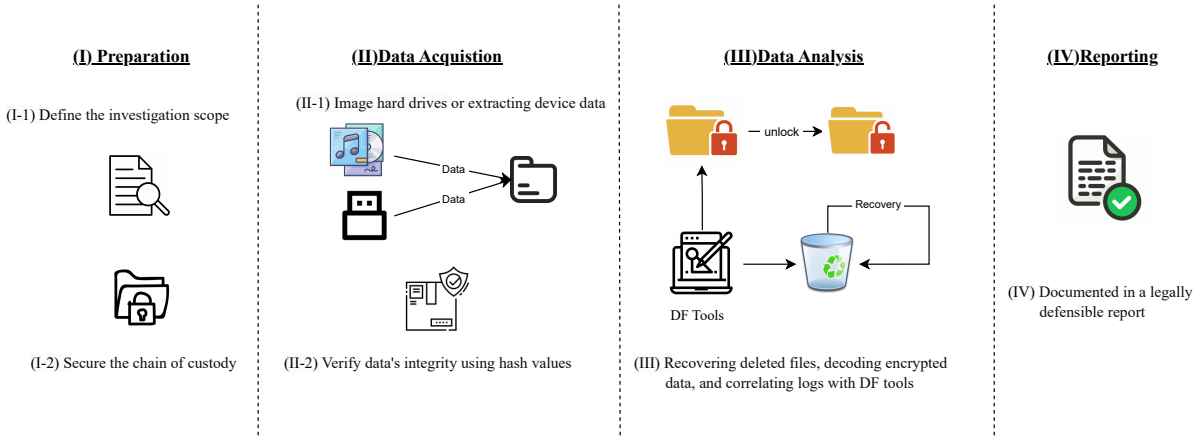

Fig. 1. Steps of the process of Digital Forensic.

those offered by SANS Scholarships, SWSIS, and Women in Cybersecurity, [11]–[13] benefit only a small, selected group of participants.

Free resources that are more widely available tend to lack depth and hands-on components. For instance, platforms like the Federal Virtual Training Environment [5] primarily focus on basic digital forensics concepts without providing the comprehensive, practical labs necessary for effective skill development. Similarly, scattered resources such as Wonderhowto [14] offer coarse-grained labs with minimal instruction, lacking the systematic structure and depth required for robust education and training purposes.

Another critical issue is inclusivity and adaptability. Many existing resources are either too generic or overly specialized, making them unsuitable for learners from diverse backgrounds or with varying experience levels. This disparity limits access to thorough and practical knowledge in digital forensics and underscores the pressing need for structured, inclusive, and practice-oriented educational materials.

To address these challenges, training resources must evolve alongside the rapid advancements in cybersecurity threats. Educational materials should provide theoretical knowledge and emphasize hands-on experiences, clear, step-by-step guidance, and practical labs. These components are essential to prepare students to tackle real-world scenarios effectively.

By developing well-structured and comprehensive training resources, we can close the gap in digital forensics education. Such materials will empower aspiring digital forensic experts, enabling them to build the skills required to protect critical digital infrastructures and address the growing complexity of cyber threats. Ultimately, these efforts will contribute to creating a stronger, more capable workforce that can meet the demands of an ever-evolving digital landscape.

III. Design and Development of the INFER Labs

A. Knowledge Units

The CAE-CD (National Centers of Academic Excellence - Cyber Defense) [15] provided a number of Knowledge units (KUs) [16] as guidelines to standardize and streamline the learning process in cybersecurity. Educators focus on these topics to ensure they can provide the most essential materials to prepare their students for what they will encounter in the field in the present and future.

For the Digital Forensics focus area, the KUs equip students with the abilities and skills necessary to apply DF techniques throughout an investigation cycle. Following the KUs, students and trainers will be able to apply DF tools and tasks, such as data acquisition, memory extraction, etc., to analyze different computer systems (host, server, network components) and report and detect the impact of cybercrime on the system.

There are five main disciplines (KUs) requirement from CAE-CD: Device Forensics (DVF), Digital Forensics (DFS), Host Forensics (HOF), Media Forensics (MEF) and Network Forensics (NWF). For Device Forensics, students will learn how to perform forensics to investigate devices such as mobile phones and tablets. Digital Forensics KUs will teach students the procedures, rules, and formal processes in a digital forensics investigation. Host Forensics covers topics such as Steganography, File System, and File Carving. In Media Forensics, students will learn about the different methods and approaches to analyze specified media, verification and validations, when to perform live or static acquisition, etc. Finally, Network Forensics covers topics related to network traffic analysis, for example, packet capture and analysis and identifying anomalous or malicious network activities.

B. Experiential Learning

Digital Forensics is a practical field, so hands-on experiments are required to achieve the best outcome. Research has shown that these activities can increase students' interest in the subject [17] and improve their comprehension [18]. Although many studies have proven the effectiveness of experiential learning in STEM and that hands-on experiment is the most important qualification valued by employers [19], most students receive little practical training and thus lack the skill set needed for the job [20]. In cybersecurity, experiential learning approaches usually focus on competitions [21], virtual

labs [22], [23], and remote labs [24]. At the same time, digital forensics tends to provide experiential learning through semester-long projects [25], [26], cyber range [27], [28], or, more recently, serious games [29], [30]. The cyber range provides a real-time simulation of cyber scenarios. Serious games and semester-long projects that are based on real-world cases offer an engaging environment with valuable hands-on experiments. Nevertheless, these approaches could be complex and challenging; they require students to have prior knowledge of the field to maximize their learning experience. The gamified approach provides an appealing visual and interactive experience. However, they usually fail to cover the materials in depth to build proficiency with the tools used in digital forensics. Hence, small hands-on labs with detailed instructions are crucial in building students' fundamental skills for beginning-level digital forensics courses. These labs allow students to acquire the prerequisite skills for working on larger projects. This proposed project aims to provide such practical skill-gaining labs and study their impact on student learning.

C. INFER Labs

Based on the KUs required for CAE-CD and experiential learning, we developed INFER, a series of step-by-step hands-on labs with accompanying instructional operating environments. INFER is a systematic and comprehensive set of materials covering several forensic sub-areas in depth. They are portable, ready to use, and can easily be adapted for different levels of education. The INFER labs are carefully scaffolded to accommodate different difficulty levels, from introductory to advanced. Early labs focus on foundational skills, including virtual machine setup, basic digital forensics (DF) concepts, the DF process, and data acquisition. Intermediate and advanced hands-on activities cover more sophisticated topics, including steganography, memory forensics, reverse engineering, and anti-forensics. Each lab includes step-by-step instructions with visual guidance, allowing students with or without prior DF experience to engage meaningfully. In some hands-on, Additional optional tasks are available (especially for advanced or higher-skilled learners), encouraging deeper exploration and promoting skill transfer. These design elements address the lack of accessible, practice-oriented educational resources in the field of DF. The list of covered topics, their domain-specific knowledge units (KUs), and estimated time to completion is shown in Table I below.

TABLE I
LIST OF INFER TOPICS AND HANDS-ON LABS

Domain Specific KUs	**Topics**	**Hands-on Lab**	**Estimate Completion Time**
DFS, MEF	Data Acquisition	H1: Data Acquisition using dd/dcfldd	1-2 hours
		H2: Windows Acquisition Tools	1-2 hours
DFS, MEF	Windows Forensics	H3: Examine Windows NTFS using*Winhex*	2-6 hours
DFS, MEF	Linux Forensics	H4: Virtual Linux Forensics Workstation Set up and Forensics Analysis with *Autopsy*	2-4 hours
DFS, HOF	File Carving	H5: File Carving	1-2 hours
		H6: Recover Graphic File	$\geq$ 4 hours
HOF	Data Hiding and Steganography	H7: Basic Data Hiding Techniques	1-2 hours
		H8: Steganography with Audio File	1-2 hours
		H9: Steganography with Image File	1-2 hours
		H10: Developing Your Own Image Steganography Tool	$\geq$ 4 hours
DVF	Mobile Forensics	H11: Android Forensics	2-4 hours
DFS	Memory Forensics	H12: Memory Forensics	$\geq$ 4 hours
NWF	Network Forensics	H13: Network Forensics with *Xplico*	2-4 hours
DFS, MEF	Social Network Forensics	H14: Forensics on Discord	1-2 hours
DVF	CPS/IoT Forensics	H15: Drone Forensics	2-4 hours
DFS	Reverse Engineering	H16: Reverse Engineering with IDA	$\geq$ 4 hours
		H17: Reverse Engineering with Ghidra	$\geq$ 4 hours
DFS, MEF	Anti-Forensics	H18: Anti-Forensics Techniques	2-4 hours

As discussed in section III-B, experiential learning greatly promotes comprehension, motivates student interest, and fosters workforce development; this project applied Kolb's experiential learning cycle (ELC) [22] to develop hands-on labs. Kolb's ELC is a widely used experiential learning approach that has been applied to field studies, training projects, and classroom activities [22], [31]. Kolb's ELC (Fig. 2) includes four stages: 1) concrete experience when the learner actively experiments with a concept; 2) reflective observation when the learner consciously reflects back on the experience; 3) abstract conceptualization when the learner attempts to generalize a model of what is experienced; and 4) active experimentation when the learner applies the model to a new experiment.

Previous studies have shown that Kolb's ELC can be applied to provide effective hands-on experiences. Abdulwahed and Nagy discussed the benefits of designing engineering labs based on Kolb's ELC [32]. In cybersecurity, Konak et al. [22] studied applying the ELC to improve student learning in virtual computer labs.

Taking this into account, INFER applies Kolb's ELC by following its four stages:

Stage 1: Concrete experience requires performing a new task to gain direct practical experience. This project provides step-by-step instructions with screenshots to provide direct guidance to students while completing the tasks. An example of the Android Forensics lab's instruction is shown in Fig. 3. Operations and interactions with the forensics tools and platforms are part of the learning process. Without detailed tutorial-like instructions, students may experience a steep learning curve. They do not know the "how-to," even if they

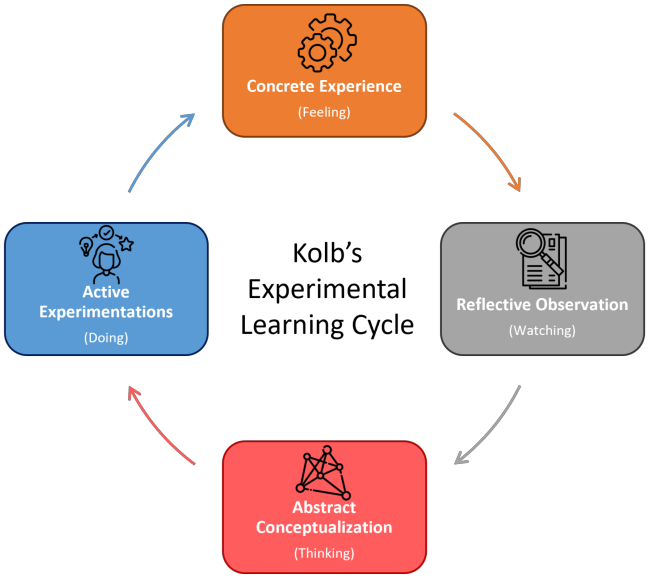

Fig. 2. Kolb's Experiential Learning Cycle.

understand the concepts and goals of the labs. Preparing detailed instructions with sufficient screenshots requires documenting every step of the labs in advance. It is also important to envision the potential technical problems that students may encounter and include them in the lab instructions. Otherwise, the debugging and troubleshooting can significantly eat up instructors' and students' lab time.

Stage 2: Reflective observation stresses students reflecting on their experiences. An INFER lab can be divided into modules, wherein reflective questions be provided to facilitate self-reflection or group discussions.

Stage 3: Abstract conceptualization expects students to generalize the experience or construct a theoretical model. Inspiring post-activity questions are provided at the end of each INFER lab instruction to not only verify the artifacts that students have discovered but also help students reflect on critical concepts and the entire lab's procedures, principles, and methodologies. Instructors can also use these questions for in-class discussions if they want to intervene. They will be provided with the ground truth and answers to those questions in the instructor's manual.

Stage 4: Active experimentation asks students to apply the concepts to another concrete experience. The implementation in this stage can vary depending on the instructors' preference. For this stage, INFER follows the two strategies employed by Konak et al. [22]: 1) combine related topics so that a later topic is based on the former one; or 2) provide a new task. In some INFER labs, some modules will repeat a former module towards different objects (e.g. datasets, drives) for a special purpose, such as comparing the approaches or results. The repeat allows students to try another concrete experience. Instructors can also provide a new lab without step-by-step instructions for students to try out.

We also utilized case studies to enhance students' interest

Fig. 3. An Excerpt of Step-by-step Instructions from example INFER Lab: Android Forensics.

and clearer define the objectives of digital forensic investigation. For example, in the Autopsy lab, we create a scenario where a USB drive was seized by a campus police officer and students are asked to perform investigation on content of the USB. By applying problems and cases that exist in real-world scenarios to the hands-on lab instructions, students will have a chance to implement their understanding and skills in a real-world context. Other studies by Gupta et al. [33] and Xu et al. [34] also shows that this approach can boost the student's interest and active experimentation and help the student effectively learn the objectives from the labs.

IV. The Designed Environment for Digital Forensics Training

A. Operating System Used in the hands-on

The hands-on labs in INFER use three operating systems: Windows, Caine [35], and Kali Linux [36].

Students and instructors can easily set up the Virtual Machine to host these operating systems (OS) in VMware Workstation Pro 17 by Broadcom or Oracle VirtualBox. The project's GitHub and website also provide details on downloading and setting up the software and OSes.

When it comes to choosing operating systems, as shown in Table II, each has its unique advantages.

- Windows is widely used and familiar to many, making it an excellent choice for general computer forensics.

TABLE II
COMPARISON OF OPERATING SYSTEMS USED IN DIGITAL FORENSICS LABS

Feature	Windows	Caine	Kali Linux
Primary Use	General computer forensics, file system analysis.	Comprehensive digital forensics tasks with specialized tools.	Network forensics and penetration testing.
Pre-installed Tools	Limited; requires manual installation of forensic tools.	Built-in suite of forensic tools such as Autopsy and Sleuth Kit.	Extensive security and forensic tools (e.g., Wireshark, Nmap).
Advantages	Widely used; familiar to most users.	User-friendly interface; tailored for forensic tasks.	Excellent for exploring cyber threats and simulating attacks.
Limitations	Lacks specialized forensic environment by default.	Limited support for advanced penetration testing.	Requires more technical knowledge; not beginner-friendly.
User Friendliness	High; suitable for beginners.m	Moderate; simple for forensic tasks.	Low; requires experience with Linux commands.

- Caine is a specialized distribution featuring a comprehensive collection of digital forensics tools and a user-friendly interface.
- Kali Linux, on the other hand, is well-known for its extensive suite of security and penetration testing tools, which are perfect for exploring and understanding security threats.

B. Portable OS Environment and Labs Material

INFER also develops portable instructional environments, mainly in Linux Virtual Machines (VMs), pre-configured, tested, and loaded with required lab materials such as software, disk images, files, and skeleton code. To facilitate dissemination, the project will minimize the number of developed VMs by hosting multiple INFER labs on one VM. For labs that involve attacks, the attack and victim VMs will be provided along with the network configuration instructions. The Virtual Machine can be set up in two ways: by the students themselves or by using pre-configured, ready-to-use Virtual Machines. Setting up the VM from scratch allows students to learn the installation and configuration processes needed for our specific forensics lab; this provides valuable insights into the workings of the OS and Virtual Machine environments.

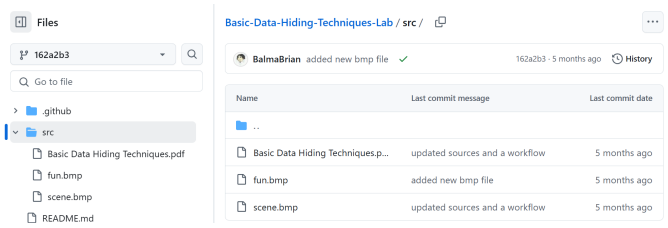

Fig. 4. Basic Data Hiding Hands-on Repository.

No matter if students want to set up their Virtual Machines or not, easy-to-use VMs are available for those who prefer to dive into the practical aspects of the labs without doing the environment setup. These machines already have the lab materials baked into the system, or the files can be sideloaded into the system using ISO files and the virtual CD Drive. The latter method enables just one standard lab to be used as a base, and labs can be cycled based on which ISO is loaded.

Using VMware Workstation or VirtualBox, students can run several different Operating Systems simultaneously on a single host machine, facilitating a comprehensive learning environment. VMware's robust platform supports snapshots and cloning, enabling students to take multiple snapshots of their Virtual Machines at different setup stages and easily revert to previous states if needed. Virtualbox also has some but not all the features available on VMware, but it has been a free and open-source software since the beginning. Unlike Virtual Box, VMware recently became a free software via personal licensing. Students or instructors can choose the software they prefer based on their past experiences and available resources.

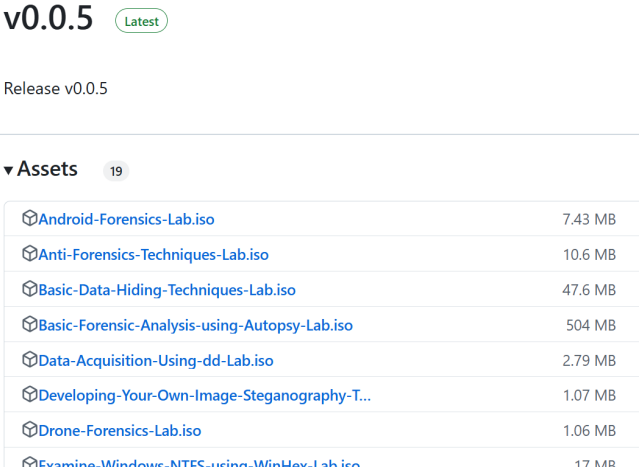

Fig. 5. Released ISO Image of Hands-on Labs.

The lab materials are published on GitHub [37]. Each lab includes step-by-step PDF instructions and any additional materials needed for the lab (Fig. 4). These materials can be sourced from GitHub when a student creates their own Virtual Machine or these materials can be mounted to a ready-to-use Virtual Machine by using the released ISO on GitHub's release page as shown in Fig. 5. Each lab created has all its source files in Github; each has all its source files copied over into an ISO file for distribution.

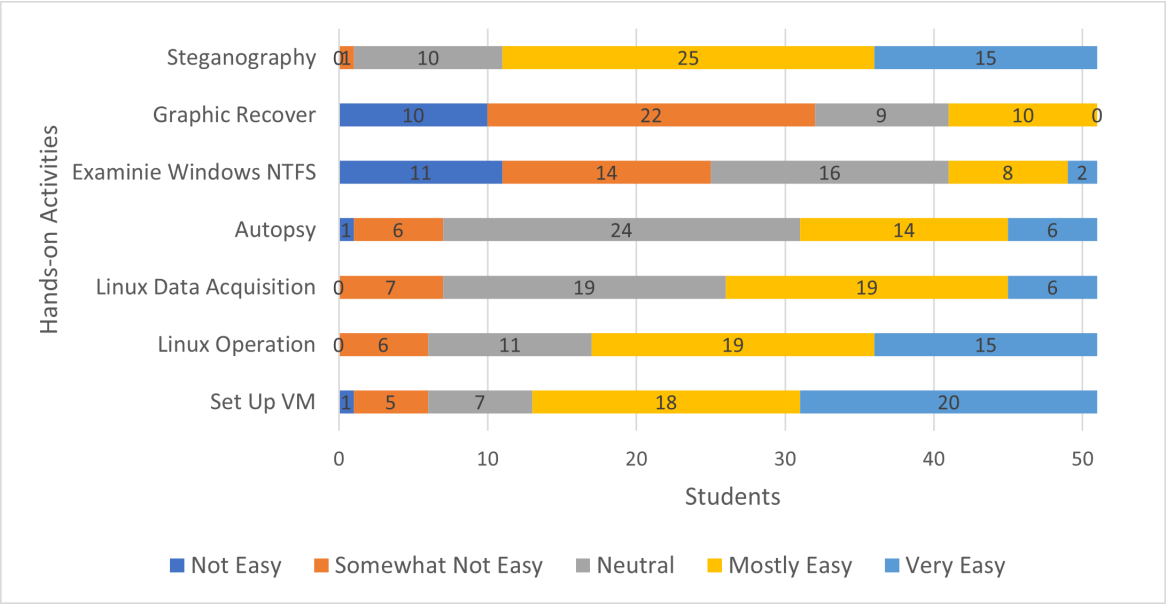

Fig. 6. Evaluation of the Hands-on Labs Difficulty by Students.

V. Evaluation

To evaluate this project, we have deployed hands-on labs for Computer Science courses, totaling about 50 students, at two different levels: undergraduate and graduate. We recorded student surveys before the courses, during certain hands-on activities, and after the courses. According to the post-course survey feedback, most students became interested in the subject, and many are considering pursuing a career in this field. Students' background knowledge about Digital Forensics varies; however, most of these students are unfamiliar with digital forensics, find this area complex, and lack the confidence and skills necessary to work in the field.

Fig. 6 shows the evaluation results on the difficulty level of hands-on labs. The first three labs: "Set up VM", "Linux Operation", and "Linux Data Acquisition" were considered easy, with the majority of students marking them as "Mostly Easy" and "Very Easy". These first three labs are really straightforward, with structured processes, and easy to follow. Besides that, many students might use Linux in other coursework or personal projects, which could be a significant factor in their ease with these lab environments. However, some students encountered challenges in the first two tasks, especially 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 recognized this issue and developed additional instructions for these specific cases. For Mac machines, alternative software and setup steps may be necessary.

Autopsy hands-on has a mixed distribution difficulty spread. About half of the students found it manageable, while others thought the activity was neutral or challenging. This hands-on involved applying knowledge learned from previous activities. Before analyzing the file system using Autopsy tool [4], students will have to import the image file system into the VM workspace - this process was taught and practiced in the first three labs. Some of the students did not consider the size of the evidence disk beforehand, and they did not provide enough memory for the VM, which ended up crashing or failing to import the evidence drive. Compared to the first three hands-on, very few students had experience with the tool (Autopsy) and material before doing this lab.

"Examine Windows NTFS" and "Graphic Recover" are the most difficult labs. These hands-on activities require technical knowledge about recovery tools and extensive understanding and interaction with the file system by analyzing the raw hex data. As a result, many students found these labs overwhelming. Meanwhile, most students are interested and rate the "Steganography" activity as easy, with only one rating it as "Somewhat Not Easy". This is because the steganography lab involves simple and easy installation tools such as steghide [38], stegseek [39], etc. Many of these tools have straightforward interfaces and simply require dragging/dropping the file, choosing embed or extract secret messages, and verifying the results. Unlike the previous two labs, steganography does not require students to deeply understand the hex file system or programming. Students can follow the step-by-step instructions and immediately see the results.

Feedback for hands-on instructions' clarity is collected and shown in Fig. 7. Clarity of the instruction greatly impacts the difficulty of the hands-on activities since unclear instructions will increase cognitive load, and step-by-step guidance could ease the complexity. If the students spend time guessing or interpreting the instructions, they perceive the labs as more difficult. On the other hand, activities with detailed, logical instructions will help the students feel more approachable and less overwhelmed. From the difficulty and clarity evaluation,

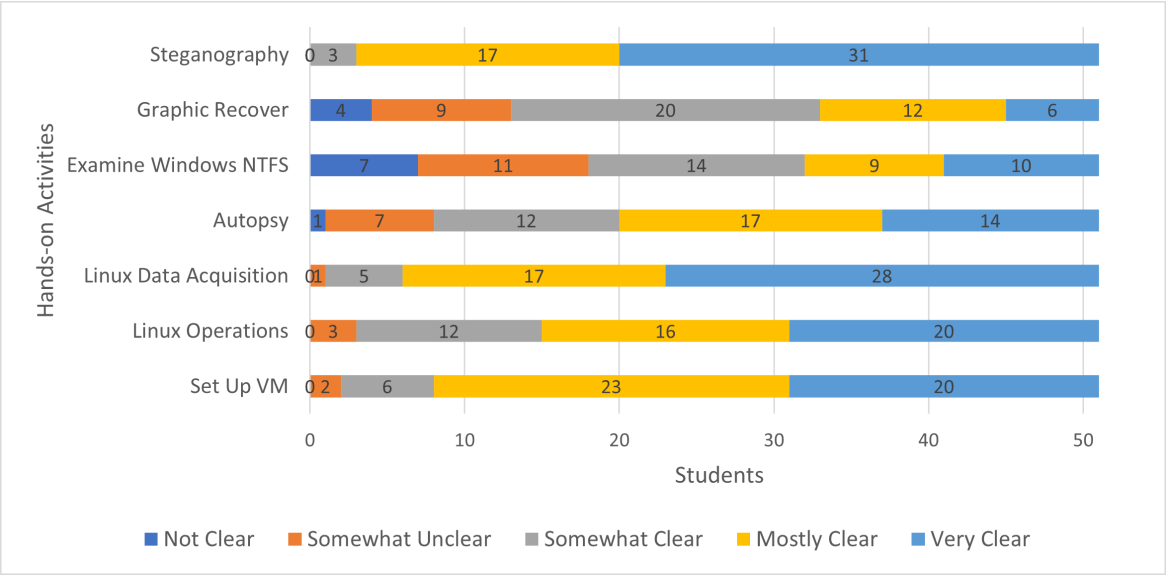

Fig. 7. Evaluation of the Hands-on Labs Instruction Clarity by Students.

we observed that "Set up VM", "Linux Operation", "Linux Data Acquisition", and "Steganography" hands-on have high clarity and low difficulty levels. This result shows that these labs may already be well-designed, and instructors could consider adding optional advanced tasks for students who want more challenges. Autopsy activity received mixed feedback from both difficulty and clarity evaluations, which implies the variety of students' backgrounds and partial clarity in instructions - some parts are well explained, while others are not. To get better insight, more detail, and qualitative feedback are needed to narrow down the confusing steps. We also offer extra resources for students who find it unclear. Finally, feedback results show high difficulty and lower clarity for "Examined Windows NTFS" and "Graphic Recover". As discussed above, possible reasons for the high difficulty of the labs are the knowledge requirement of the hex file system, involving multiple steps, advanced setting, and less familiarity for most of the students. Since most students are unfamiliar with the material, these labs demand more detailed guidance than others. To help address this issue, instructors could offer an overview of the NTFS file system, provide interactive walkthroughs, and include checkpoints to confirm students are on track.

To disseminate the INFER labs, we offered a graduate-level digital forensics course to high school teachers to train them on teaching digital forensics, and also hosted another two-day workshop to college faculty on digital forensics education. We gathered feedback from teachers, instructors, and professors' perspectives. Twenty high school teachers who teach or work in computer science, cybersecurity, or related fields participated in our digital forensic course. Given its duration, the course used only 4 hands-on labs: "Linux Data Acquisition", "Zero and DiskFormatting", "Setting Up Virtual Machines for Digital Forensics Investigations", and "Steganography". Evaluations for difficulty and clarity from the teachers are shown in Fig. 8 and Fig. 9. From the results, teachers rated the tasks as harder overall than regular computer science undergraduate/graduate students even though their feedback on the instructions was high, showing they were solid. High school teachers often have less direct experience with advanced computer science or cybersecurity topics and may evaluate the labs from perspective of teaching feasibility; this explains their rating of the lab's difficulty. On the other hand, regular computer science students frequently encounter Linux, VMs, and tools in specialized courses, online sources, or projects, which help them feel more comfortable with emerging technology and lower their perceived difficulty with hands-on tasks. Comparing the feedback also reveals that clarity alone does not guarantee easier activities; both groups find the instructions relatively straightforward, although more teachers consider the labs challenging. This implies the assumed knowledge background and specialized knowledge could outweigh the well-written instructions. To mitigate this problem, we could offer extra resources and teacher training and provide pre-lab resources to help reduce the background gap, ensuring learners' engagement.

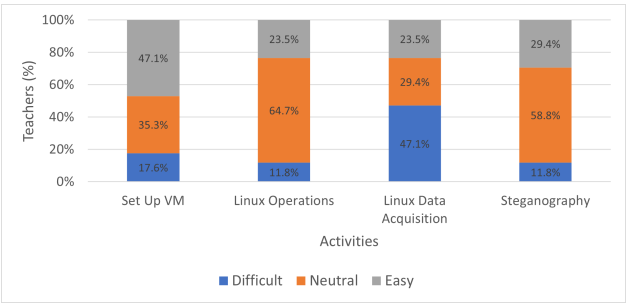

Fig. 8. Evaluation of the Hands-on Labs Difficulty by Teachers.

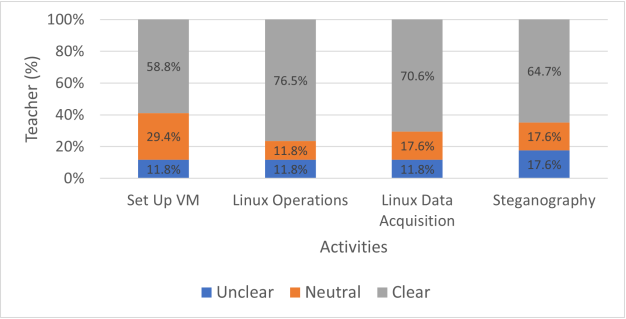

Fig. 9. Evaluation of the Hands-on Labs Instruction Clarity by Teachers.

Eleven professors and faculty members from four-year universities and community colleges across the United States attended our two-day workshop. Participants first received a guided walkthrough of the INFER lab suite, and then got trained on five hands-on labs during the workshop. The labs covered different key topics, including "Linux Data Acquisition with Zero Out and Disk Formatting", "Sleuth Kit Autopsy", "Image Steganography", "Audio Steganography", and "Reverse Engineering". Following the workshop, participant surveys were conducted to assess the INFER labs' experience 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. When asked about the workshop's influence on participants' expertise and confidence in teaching digital forensics, most professors found the labs well-instructed, easy to follow, covering rich topics, and helping them broaden their skills. Besides that, the exercises provide inspiration, build strong confidence in the area, and motivate them to develop more similar materials. Some potential challenges that professors anticipated are long-term maintenance, up-to-date materials, and availability of laptops/equipment for students. Nonetheless, all of them agreed that the hands-on labs are helpful and convenient and can be easily set up from ISO images on individual laptops. Below are some of the comments from the professors participated in our workshop:

> *"Students can significantly improve their cybersecurity knowledge and skills through these labs, as each lab delivers concrete security concepts and examples."*
> *"Colleges across the industry can share ISO files with their respective lab assignments, allowing students to simply load them. This approach provides students with greater exposure to practical, hands-on experience."*

VI. Current and Anticipated Challenges in Maintaining and Using INFER Labs

Maintaining and using educational materials such as INFER Labs involves several challenges, particularly on ensuring content relevance and accommodating a diverse learner base. These challenges become more pronounced when addressing the complexities of hands-on labs like those provided in the INFER curriculum, which span topics from basic data acquisition to reverse engineering and anti-forensics techniques.

A. Rapid Technological Change and Content Relevance

One primary challenge is ensuring the materials remain relevant as digital forensics tools and methodologies evolve. Labs such as Android Forensics and Drone Forensics highlight this difficulty, as Android Operating System and drone technologies update frequently.

For instance, the Android Forensics lab must adapt to changes in Android security mechanisms, such as stricter encryption policies or changes in file system structure in newer versions. Similarly, Drone Forensics requires updates to accommodate advancements in drone hardware, communication protocols, and data storage techniques. Without continuous updates, these labs risk becoming obsolete and detached from real-world forensic scenarios.

B. Software Accessibility and Platform Compatibility

Many of the hands-on labs rely on proprietary tools, such as WinHex in the Windows Forensics lab and IDA Pro in the Reverse Engineering lab. While powerful, these tools present challenges due to high licensing costs and limited availability in educational settings. Furthermore, platform-specific compatibility issues, such as ARM-based Mac systems, complicate the setup process for tools like virtual machines in Linux Forensics Workstation Setup lab.

For example, students using macOS with Apple's ARM chips may struggle to complete labs requiring x86-compatible Virtual Machine images, such as those needed for forensic analysis using tools like Autopsy.

C. Balancing Complexity with Student Diversity

Our Labs cover a wide range of topics, from foundational skills like Data Acquisition to advanced topics like Anti-Forensics Techniques. This breadth can create challenges in addressing the diverse technical backgrounds of students.

For example, undergraduate students may find advanced labs such as Reverse Engineering with Ghidra overwhelming due to the technical depth required, while graduate students might require additional challenges to stay engaged. Furthermore, students accustomed to step-by-step instructions may struggle in labs that emphasize problem-solving and independent exploration, such as the lab of Developing Your Own Image Steganography Tool.

D. Ensuring Sustainability and Real-World Relevance

The relevance of digital forensics education depends heavily on its alignment with real-world practices. Labs such as Network Forensics with Xplico and Forensics on Discord require continuous updates to reflect evolving network communication protocols and emerging forensic tools. Without regular revisions, these labs risk losing their connection to practical, industry-relevant scenarios.

VII. Conclusions and Future Work

As digital forensics's importance continues to grow in the cybersecurity field, the demand for highly skilled professionals is increasing. The digital forensics field currently lacks practical educational materials to enable high quality training. INFER Labs aims to bridge this gap by providing practical, interactive, and comprehensive educational resources that address key challenges in digital forensics training.

Feedback from students and educators highlights INFER's effectiveness in enhancing learning outcomes and skill development. Future efforts will focus on continuous content updates, improved software compatibility, and flexible learning pathways to maintain its relevance and practicality. Additionally, open-source contributions may help the long-term sustainability and expansion of educational resources.

As a free and open-source resource, INFER can greatly contribute to advancing digital forensics education and provide stronger support for training cybersecurity professionals.

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, "ISC2 2024 Cybersecurity Workforce Study." https://www.isc2.org/Insights/2024/10/ISC2-2024-Cybersecurity-Workforce-Study. Last accessed 01/25/2025.

[2] EnCase Software, "EnCase Forensic Software - Top Digital Forensics & Investigations Solution." https://www.guidancesoftware.com/encase-forensic. Last accessed 02/27/2025.

[3] Forensic Toolkit, "AccessData Forensics ToolKit (FTK)." https://accessdata.com/products-services/forensic-toolkit-ftk. Last accessed 02/27/2025.

[4] Autopsy Tool, "The Sleuth Kit (TSK) & Autopsy: Open Source Digital Forensics Tools." https://www.sleuthkit.org/. Last accessed 02/27/2025.

[5] Federal Virutal Training Environment (FedVTE), https://niccs.cisa.gov/education-training/federal-virtual-training-environment-fedvte. Last accessed 02/27/2025.

[6] Sans, https://www.sans.org/digital-forensics-incident-response/. Last accessed 01/25/2025

[7] Cyber5W, https://cyber5w.com/. Last accessed 01/25/2025

[8] TCM Security, https://academy.tcm-sec.com/p/practical-windows-forensics. Last accessed 01/25/2025

[9] EC Council, https://www.eccouncil.org/train-certify/digital-forensics-essentials-dfe/. Last accessed 01/25/2025

[10] Nw3c training, https://www.nw3c.org/UI/Index.html. Last accessed 01/25/2025.

[11] Sans's Ken Johnson DFIR scholarship, https://www.sans.org/mlp/ken-johnson-scholarship-2023/. Last accessed 02/27/2025.

[12] Scholarships for Women Studying Information Security (SWSIS), https://cra.org/cra-wp/scholarships-and-awards/scholarships/swsis. Last accessed 02/27/2025.

[13] Women in Cybersecurity (WiCyS) Security Training Scholarship, https://www.wicys.org/benefits/security-training-scholarship/. Last accessed 02/27/2025.

[14] Wonderhowto, https://null-byte.wonderhowto.com/collection/forensics/. Last accessed 02/27/2025.

[15] National Centers of Academic Excellence in Cybersecurity, https://www.nsa.gov/Academics/Centers-of-Academic-Excellence/. Last accessed 02/27/2025.

[16] National Centers of Academic Excellence in Cybersecurity (NCAE-C) – Cyber Defense (CAE-CD) Knowledge Units (KUs), https://dl.dod.cyber.mil/wp-content/uploads/cae/pdf/unclass-cae-cd_ku.pdf. Last accessed 01/25/2025

[17] N. Holstermann, D. Grube, and S. Bögeholz, "Hands-on activities and their influence on students' interest," Res. Sci. Educ., vol. 40, no. 5, pp. 743–757, 2010.

[18] J. T. Guthrie, A. Wigfield, N. M. Humenick, K. C. Perencevich, A. Taboada, and P. Barbosa, "Influences of stimulating tasks on reading motivation and comprehension," J. Educ. Res., vol. 99, no. 4, pp. 232–246, 2006.

[19] "State of Cyber Security 2017: Part 1: Current Trends in Workforce Development," ISACA (Information Systems Audit and Control Association), 2017

[20] "Preparing Cybersecurity Professionals to Make an Impact Today and in the Future," ISACA 2017.

[21] R. S. Cheung, J. P. Cohen, H. Z. Lo, F. Elia, and V. Carrillo-Marquez, "Effectiveness of cybersecurity competitions," in *Proceedings of the International Conference on Security and Management (SAM)*, 2012.

[22] A. Konak, T. K. Clark, and M. Nasereddin, "Using Kolb's Experiential Learning Cycle to improve student learning in virtual computer laboratories," Comput. Educ., vol. 72, pp. 11–22, 2014.

[23] K. Nance, B. Hay, R. Dodge, A. Seazzu, and S. Burd, "Virtual laboratory environments: Methodologies for educating cybersecurity researchers," *Methodol. Innov. Online*, vol. 4, no. 3, pp. 3–14, 2009.

[24] N. L. Martin and B. Woodward, "Building a cybersecurity workforce with remote labs," *Inf. Syst. Educ. J.*, vol. 11, no. 2, p. 57, 2013.

[25] D. Dampier and R. Vaughn, "Hands-on discovery learning in computer security and forensics," 2009.

[26] X. Zhang and K.-K. R. Choo, *Digital Forensic Education: An Experiential Learning Approach*, vol. 61. Springer, 2019.

[27] M.N. Katsantonis, A. Manikas, I. Mavridis et. al. "Cyber range design framework for cyber security education and training," Int. J. Inf. Secur. 22, pp. 1005–1027 (2023).

[28] M. Leitner, M. Frank, W. Hotwagner 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).

[29] L. Englbrecht, G. Pernul, "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).

[30] S. Friedl, T. Reittinger, G. Pernul, "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.

[31] D. A. Kolb, Experiential learning: Experience as the source of learning and development. FT press, 1984.

[32] M. Abdulwahed and Z. K. Nagy, "The TriLab, a novel ICT based triple access mode laboratory education model," Comput. Educ., vol. 56, no. 1, pp. 262–274, 2011.

[33] K. Gupta, A. Neyaz, N. Shadidhar, and C. Varol, "Digital Forensics Lab: A framework," 2022 10th International Symposium on Digital Forensics and Security (ISDFS), pp. 1-6, 2022.

[34] W. Xu, L. Deng, and D. Xu, "Towards Designing Shared Digital Forensics Instructional Materials," IEEE COMPSAC (2022)

[35] Caine, https://www.caine-live.net/. Last Accessed 12/21/2024.

[36] Kali Linux, https://www.kali.org/. Last Accessed 12/21/2024.

[37] INFER Project Github Repository, https://github.com/WPI-LIONS-Group/INFER.git, last accessed 2025/4/2.

[38] Steghide Tool, https://www.kali.org/tools/steghide/. Last accessed 02/27/2025.

[39] Stegseek Tool, https://github.com/RickdeJager/stegseek. Last accessed 02/27/2025.