Computers and Education Open 2 (2021) 100045

Contents lists available at ScienceDirect

Computers and Education Open

journal homepage: www.sciencedirect.com/journal/computers-and-education-open

Using experiential learning to teach and learn digital forensics: Educator and student perspectives

Raymond Flores [a,*], Akbar Siami Namin [a], Neda Tavakoli [b], Sima Siami-Namini [a,c], Keith S. Jones [a]

[a] Texas Tech University, 2500 Broadway, Lubbock, TX, United States
[b] Georgia Institute of Technology, North Ave NW, Atlanta, GA, United States
[c] Mississippi State University, 665 George Perry Street, **Starkville, MS, USA**

ARTICLE INFO

KEYWORDS:
Faculty professional development
Teaching digital forensics
Experiential learning

ABSTRACT

Due to its complexity, designing digital forensics curriculum can be quite challenging. This paper describes how authors used experiential learning theory to design and teach digital forensics in post-secondary education settings. Furthermore, drawing on survey data collected from students at the end of a graduate level digital forensics course and from cybersecurity educators participating in a three-day professional development workshop, this study examined educator and student perspectives. Results suggest that both students and educators had a positive learning experience. However, when asked about challenges encountered and anticipated with experiential learning in their own context, cybersecurity educators cited challenges with designing the required hands-on experiences, lack of space in curricula, and lack of instructional supports. Recommendations for teaching digital forensics are offered and discussed.

1. Introduction

A recent CSIS survey of IT decisionmakers across eight countries found that 82 percent of employers report a shortage of cybersecurity skills, and 71 percent believe this talent gap causes direct and measurable damage to their organizations [9]. However, designing and delivering cybersecurity education effectively across general computer science programs present several challenges related to pedagogy, educational resources, available skills, and technical resources [8]. Furthermore, despite the demand for cybersecurity specialists and the growing number of post-secondary degrees offered in computer science [18], students are generally not provided with the learning opportunities leading to the cybersecurity expertise sought by employers. The relatively few students who have studied security at the university level have oftentimes been exposed to courses that are entirely theoretical, dealing with principles and concepts rather than practice [4]. These issues highlight the need and importance for cybersecurity experts and educators from post-secondary institutions including community colleges and universities to work together to address these challenge related to cybersecurity education.

The present study describes how a team of educators used experiential learning theory to guide the design of a post-secondary cybersecurity course and a professional development teaching workshop for post-secondary cybersecurity educators. This paper reports on the findings of two studies. Study #1 draws from the experiences of an instructor of a graduate-level digital forensics course and feedback collected from students after taking the course. Study #2 draws from a professional development workshop offered to digital forensics educators from 2- and 4-year colleges in which participants provided feedback about their own experiences as learners in the three-day workshop, and also provided comments about their anticipated challenges as educators at their own post-secondary institutions. Based on the results of each study, a series of recommendations are offered.

1.1. Importance of study

The importance of this study is three-fold. First, it carefully describes how the authors used experiential learning theory to guide the design of a digital forensics course and professional development workshop for cybersecurity educators. This process of linking theory to practice and

* Corresponding author:
E-mail addresses: raymond.flores@ttu.edu (R. Flores), akbar.namin@ttu.edu (A. Siami Namin), neda.tavakoli@gatech.edu (N. Tavakoli), sima.siami-namini@ttu.edu (S. Siami-Namini), keith.s.jones@ttu.edu (K.S. Jones).

https://doi.org/10.1016/j.caeo.2021.100045
Received 9 February 2021; Received in revised form 11 August 2021; Accepted 12 August 2021
Available online 14 August 2021

associated examples is very much lacking in the literature. Second, it describes the perceptions of students and educators as they learned from the digital forensics course and workshop via experiential learning. Recommendations and challenges drawn from participants can be used by future educators and professional development workshop designers to inform their decisions. Thirdly, this study describes the challenges that one cybersecurity educator faced when designing a cybersecurity course and the challenges that cybersecurity post-secondary educators anticipated that they would encounter in their teaching contexts. These results can be used by future professional development workshop designers to inform the selection of topics and solutions that specifically address those cybersecurity education challenges.

2. Related work

Digital forensics is a branch of cybersecurity that focuses on investigating and recovering evidence found in digital media in order to provide evidence that supports or contradicts a security-related hypothesis. Digital media contained within digital devices that may have been used for criminal activity (e.g., mobile phones, laptops) are carefully examined and potential evidence is extracted. Digital forensics is difficult but critically important work, so it is imperative to educate those who are interested in exploring this career path. Our literature search yielded several studies related to post-secondary educator experiences with designing and teaching cybersecurity courses including digital forensics, recommended pedagogical strategies and tools for teaching cybersecurity, and results from professional development workshops aimed at supporting educators to design and teach cybersecurity courses.

Numerous cybersecurity experts and educators have developed hands-on labs and case studies to teach cybersecurity, and they have shown them to be effective pedagogy [2,3,5,7,10,15,19]. For example, Batten and Pan [3] shared their experience teaching a forensics unit for second year undergraduate students. They employed a scenario-based and "learning by doing" approach in which a standard technique for investigating a computer was followed: 1) boot the computer into forensics mode, and 2) avoid modifications of data or timestamps. Through this teaching format, students practiced basic forensics techniques, such as recovering deleted files, use of hash functions, capturing memory and network packets, and practicing with a variety of forensics tools. Batten and Pan [3] reported that this approach was an effective way to teach digital forensics to undergraduate students who had only one year of university experience and limited background knowledge, and when instructors have a limited budget.

Similarly, Kaneko, Ban, and Okamura [12] examined the effectiveness of using experiential learning to teach cybersecurity. These authors prepared two groups, the proposed experiential learning group (experimental group) and a non-experiential learning group (control group), and investigated each learning effectiveness by using several evaluation metrics including pre- and post-knowledge test scores, a delayed-test score and learning motivation score. Students in the experimental group were provided with classroom lectures, engaged in discussions with their peers to learn, and engaged with their peers in practical exercises where they tried to execute several cyberattacks on internet systems. On the other hand, students in the non-experimental group were provided with a video-based e-learning course with no practical exercises, no discussions with peers, and no engagement with their peers. Results of this study found no significant difference between pre- and post-knowledge test scores, and learning motivation scores between the two groups. However, there was significant difference with delayed-test scores between the two groups. This interesting result suggested that while learners in the both groups had higher learning motivation, learners that engaged in the experiential learning were able to retain the knowledge that they had acquired several weeks after, while those in the non-experiential learning group could not.

Chi, Jones, Chatmon, and Evans [6] described their experience with designing and implementing digital forensics laboratories and provided a practical approach to teaching digital forensics for undergraduate students in which they were provided with practical hands-on experiences with real world tools and real-world problems. In this study, the authors cite that their main challenges were due to expensive software and hardware needed for digital forensics. Similarly, Srinivasan [16] faced financial challenges while developing a dedicated laboratory for digital forensics when developing a course on digital forensics as part of an Information Security curriculum for undergraduates.

Ward [20] described the efforts undertaken by a small community college to develop a cybersecurity program. Related to course delivery, Ward [20] highlighted to benefits of helping students work through lab exercises in real-time class sessions. Additionally, Ward [20] cited the importance of curriculum developers of being aware of both local industry needs and industry-recognized certifications when developing or revising a curriculum. This author highlighted the value of consulting with local industry experts for their input regarding the program and for suggestions for improvement. Based on this input their program's digital forensics course was adapted to provide a more comprehensive foundation for students to be ready to be trained by future employers or to take graduate courses. Some of the challenges faced by the program were course sequencing, specifically course prerequisites need to be redefined to ensure that students are at least exposed to the concepts in one course prior to applying them in subsequent courses. Even then, Ward [20] cited the issue of students to retain information from one course to apply in another course. Another major challenge was related to course delivery of courses, specifically the challenged as it requires the campus IT group to set up a firewalled classroom/lab environment in which the students could freely practice the techniques they learned.

In efforts to better support post-secondary educators to design and develop cybersecurity courses faculty development workshops have been funded by the National Science Foundation (NSF). In two of these workshops, Yuan *et al.* [19] used hands-on exercises and case studies to teach faculty about various Information Assurance topics (e.g., cryptography, database security, network security, digital forensics) and how to teach these topics using hands-on exercises and case studies. Based on data collected during the workshop through self-reported knowledge gains and overall satisfaction with the workshop and materials, participants indicated knowledge gains and overall satisfaction with the workshop. Additionally, participants reported plans to use case studies and hands-on labs in their own teaching. Furthermore, several faculty workshop participants also indicated that the opportunity to meet others who are engaged in teaching the Information Assurance topics was useful. When asked about challenges with teaching information assurance topics, a faculty focus group indicated challenges with 1) bureaucratic and policy barriers to teaching Information Assurance at their institutions (e.g., administration prohibiting the use of laboratories for hacking for fear of breach in campus security and lack of financial support to purchase proprietary software and tools), and 2) student challenges such as lack of interest with topics. When asked about effective ways to increase student participation, the faculty focus group all agreed that hands-on activities and case studies would engage their students. Furthermore, while cybersecurity educators agreed that hands-on exercises and case studies improved student learning, hands-on exercises and case studies are not widely adopted due to the time needed to develop them and integrate them into curricula [19]. Additionally, cybersecurity educators in post-secondary education often face challenges with designing courses and programs. Results from the faculty focus group indicated that only a few of the workshop participants indicated attending workshops that were specifically about teaching techniques. This result suggests that more work is needed in providing professional development workshops to cybersecurity educators related to designing and teaching digital forensics courses.

Furthermore, while hands-on real-world experiences have been found to be beneficial, Stirling et al. [17] highlighted the importance of grounding these experiences in learning theories such as experiential

learning theory [13]. In their examination of 44 Ontario universities and colleges, including 369 internship program webpages and 77 internship course outlines, they found that most internships overemphasized the practical aspect of the experience at the expense of linking theory and practice. These authors recommended that in order to optimize learning through hands-on experiences that these experiences should include hands-on practical experiences, reflection, connecting coursework and practical experience, and implementing creative ideas into practice. Of the studies reviewed above, Floyd and Yerby [11] was one of the few that highlighted the benefits of using active learning theories to inform decisions regarding developing and building a hands-on digital forensics laboratory environment. Nevertheless, Floyd and Yerby [11] did not provide a thorough description of how learning theory informed the design of their instruction nor did they examine student perceptions after engaging with instructional tasks. This suggests that more work is needed in the area of framing cybersecurity instructional tasks by integrating learning theories.

3. Theoretical framework

Experiential learning theory was used to frame the design of curriculum material and used as a basis for data collection of the two studies described in this paper. With experiential learning, students engage in active, hands-on, authentic learning activities through which they apply their knowledge and skills in real-world contexts. Using this instructional approach, instructors often take problems that exist in the industry and adapt them into class projects. Based on Kolb's Experiential Learning Cycle [13], learners gain a hands-on, collaborative and reflective learning experience by going through four stages: Concrete experience, Reflective Observation, Abstract Conceptualization, and Active Experimentation. During the Concrete Experience stage learners start off with hands-on experiences in which they work as a team or as individuals to actively engage with an authentic real-world task. In the second stage, Reflective Observation, learners step back from their concrete experience and reflect on what they did and experienced. During the third stage, Abstract Conceptualization, learners make sense of what happened during the concrete experience stage by making connections to theories learned, what they learned in textbooks, and/or to ideas from their peers and instructors. Lastly, in the fourth phase, Active Experimentation, learners consider how they are going to put what they have learnt into current and future practice.

4. Study #1: digital forensics course for students

In Study #1, a research team led by the first author designed and delivered an introductory course on digital forensics with four distinct modules: 1) Reverse Engineering (RE), 2) Disk Forensics, 3) Memory and Malware Analysis, and 4) Network Forensics. Accordingly, lecture notes and instructional modules were created along with several hands-on experiences targeting those topics. Furthermore, several open-source digital forensics tools were explored covering the techniques used for each module. For example, tools such as REMnux, Autopsy, Volatility, and Wireshark were used for reverse engineering, disk, memory, and network forensics, respectively. We also created several hands-on experiences concerning mobile forensics analysis targeting only Android devices. Interested readers and educators are invited to explore the instructional modules posted on the course's GitHub[1].

4.1. 2CADS: the red/blue teams protocol

There are several variations of implementing red/blue teams in a classroom setting. The strategy employed and adopted by the instructor in this study was based on the idea that each team needs to practice both red and blue team activities. Hence, each team participated in the creation of attack artifacts (a red team activity) and analysis and understanding of the malicious attacks (a blue team activity), simultaneously.

During the course, the teams competed four times, each time focusing on a major topic of digital forensics including 1) Reverse Engineering, 2) Disk Analysis, 3) Memory and Malware Analysis, and 4) Network Analysis. Each competition followed a cycle of five phases: 1) Creation, 2) Circulation, 3) Analysis, 4) Demonstration, and 5) Scoring (Acronymed *2CADS*), as described below:

(1) *Creation Phase.* Each team was required to create a malicious Android application and provide a report describing how the malicious application was created and what the application intended to do (A 10-day activity);
(2) *Circulation Phase.* Once the malicious applications were created, they were submitted to the instructor of the course along with the descriptions of the creation of the applications and its malicious intention. The instructor then provided the malicious application to the opponent team for analysis and inspection;
(3) *Analysis Phase.* The malicious applications were then analyzed by the competing teams and analysis reports were created and submitted to the instructor of the course (A 10-day activity);
(4) *Demonstration Phase.* Having received both generation and analysis reports from two different teams, the instructor then requested each team to present, in person, their analysis and malware creation reports.
(5) *Scoring Phase.* With respect to the complexity of creation and analysis, the performance of the two teams were compared and the winning team would be decided and announced by the instructor.

The *2CADS* protocol allowed students to learn digital forensics through experiential learning by 1) engaging learners with hands-on Concrete Experiences in which they worked as a team using open source digital forensic tools to create malicious applications during the Creation Phase, 2) engaging learners in Reflective Observation first with their instructor during the Circulation Phase and then with their peers during the Demonstration Phase, 3) engaging learners in Abstract Conceptualization by having them analyze competing peers' malicious applications during the Analysis Phase, and 4) engaging learners with Active Experimentation by having them compare competing teams' performance, assessing strengths and weaknesses in competing teams' applications, and preparing for the next competition using what they learned during the Scoring Phase.

4.2. Participants

The course was taught to 17 graduate students majoring in Computer Science and Software Engineering at a large research university in the southwestern United States. At the end of this semester, student perspectives were gathered. The instructor of the course who is also a cybersecurity expert also provided his perspective and recommendations from the lens of an educator.

4.3. Data collection and analysis procedures

Data were gathered from the students taking the course using a locally developed survey that students completed anonymously at the end of the semester. This survey included the following three open-ended items: 1) How would you improve this course?, 2) This course would've been more effective if:, 3) In addition to Reverse Engineering, Disk Forensics, Network Forensics, and Memory Forensics, the following topics should be added to the course?. The purpose of survey questions 1 and 2 was to identify any challenges that students may have faced while

[1] For more information regarding the course content and materials, please visit the following GirHub link: https://github.com/asiamina/A-Course-on-Digital-Forensics

engaging with the instruction designed based on experiential learning theory, and secondly, to identify elements of experiential learning theory that students found to be effective. Question 3 was used to gather student input about additional topics that instructors should consider adding into their curriculum.

After collecting open-ended responses for questions 1 and 2, we then used the stages of experiential learning theory (i.e., Concrete Experience, Reflective Observation, Abstract Conceptualization, and Active Experimentation) to analyze and categorize student responses. Question 3 responses were analyzed using theme analysis.

In addition to obtaining student perspectives, the instructor and designer of the course also provided recommendations for future educators based on his experience of using experiential learning theory to design the *2CADS* protocol.

4.4. Results

Students' perspective

Based on the analysis of student responses to the open-ended items, results suggested that students found the course to be effective and felt that the course could be improved by increasing the amount of tasks aligned with experiential learning stages. For example, associated with the Concrete Experience stage, example student responses was that the course could be improved by having "more practical exercises" and "applying the tools and techniques to real world problems." Aligned with the Reflective Observation and abstract conceptualization stages of experiential learning, example student responses were that the course could be improved with more "opportunities for open discussion about problems faced with homework and projects," and "more interactive with quizzes or presentations." Lastly, while students found that the provided concrete experiences were effective, they felt that tasks aligned with the Active Experimental stage of experiential learning needed more support. For example, some sample student responses were that the course could be improved by having an "easy process to set up our environment" referring to the labs and another student made a request for more "free application(s)." Student responses to question 3 on additional topics, also revealed that students found the experiential learning tasks effective however wanted more support on the lab setup specifically with getting the tools to work. For example, one student response said that "all assignments and projects were very good but some became - difficult because the tool mentioned did not run like the tool Mobisec. Similarly, Sanataku tool did not run." These latter student responses related to tasks aligned with the active experimentation, highlighted the educator's challenge of providing authentic concrete experiences while at the same time making some accommodations to provide student support.

In regard to question 3 related to additional topics that students felt should be added into the course, one student stated that "the topics covered in the course are useful for our day-to-day work" and that he or she enjoyed "learning about security which would better protect myself and my daily work." Another student highlighted the need for "ethical and legal aspects of crimes related with digital forensics."

4.5. Educator' recommendations

Based on his experience designing and teaching this graduate level course on digital forensics, the following are the instructor's recommendations based on that experience with using experiential learning theory.

4.5.1. General recommendations

(1) Students need to separate their regular operational platform from the one they use for the experimentation and analysis required to inspect a live malware. As a result, students need to create their own mini-laboratories on their personal computers. To do so, virtualization technologies and software such as Virtual Box or VMware should be utilized.
(2) It is important to develop hands-on experiences based on newly discovered malware and cyberattacks. Most of the old malware are being captured and analyzed by newer versions of anti-viruses and Web browsers and thus analyzing them might not be of interest anymore for students taking the course. For instance, most of the newer versions of Web browsers are capable of detecting malicious macros injected into PDF or Microsoft Word files. Therefore, creating such hands-on experiences might be less attractive for students.
(3) Along the same line, previously created hands-on experiences for malware analysis might get obsolete and thus the artifacts might not work anymore. It is important to revisit the previously generated hands-on experiences to make sure they deliver the required concepts regardless of any dependencies on changes in the analysis tools used.
(4) It is difficult to find good malware for educational purposes because most malware are very complex to analyze and need fundamental expertise and in-depth knowledge of hardware, software, and the attacks. With the advancement in developing AI-based malware the complexity is even greater. For an introductory course on malware and memory analysis, it is best to start with simple and easy malware.
(5) Provide guidance on how to use tools and create memory, disk, and network dumps without capturing noises and unnecessary data while preserving privacy issues. As a result, some hands-on experiences in the class should target creation of memory and disk images using different tools.
(6) The assignments must be explicit in regard to the type of machine and operating system that the created malware is going to target along with the acceptable file formats.

4.5.2. Educator recommendations for using the 2CADS protocol

Based on the instructor, the 2CADS protocol employed to implement the red/blue teams' activities in a classroom setting was well-received by the students. In addition to being fun and enjoyable activities, the students claimed that they actually learned through these practical competitions. On the other hand, there were also some considerations and concerns that, if not taken care of properly, might cause some conflicts between the participating teams. Here, we list the practical considerations when executing the red/blue team activities in classroom settings:

I) Recommendations for Red Teams

(1) The hash values of each created malicious application and artifact should be generated and shared with the blue team. The hash values of the artifacts serve as the credentials for ethical, consistency, and tracing purposes.
(2) Testing the created artifacts in multiple environments takes a lot of time because each target environment needs to be set up separately. The red team needs to share the target platform with the blue team in order to avoid spending unnecessary time discovering on which platform the malicious application would be activated.
(3) It is necessary to save all of the creation steps to make sure the malicious artifacts do not intentionally corrupt the blue teams' machines.
(4) Use the right tools to create artifacts. Different platforms (e.g., Windows vs. Linux) use different memory models.

II) Recommendations for Blue Teams

(1) It is necessary to take snapshots of the operational environment (e.g., Virtual Box) before running any malicious application. Each

malware can corrupt the execution environment and thus waste effort.
(2) All the analysis steps need to be recorded to make sure the collected set of evidence is saved.
(3) Running malware corrupts the machines. Therefore, students should set up a separate machine from the one that contains their existing tools and run the malware on this separate machine. Otherwise, students will have to spend time re-installing tools. The malicious applications must be executed in a controlled environment and thus preferably a sandbox needs to be installed and used for the purpose of malware analysis (e.g., Cuckoo sandbox *Cuckoo: Automated Malware Analysis* (Accessed 2019)).
(4) Use the right tools to perform analysis.

5. Study #2: digital forensics workshop for post-secondary educators

As part of a capacity building project funded by a National Science Foundation (NSF) grant, a three-day faculty development workshop was offered with the aim of promoting cyber security education at the community college and university levels.

The project investigators organized a series of workshop sessions on digital forensics practices and theory. In addition, the workshop presented research outcomes along with the instructional and course modules developed to help participants develop their own materials and courses in this area. There were a variety of presenters in the sessions including: 1) researchers and educators active in cyber security education and research, 2) a collaborator and professional digital forensics team from the ABC Laboratories, and 3) graduate students presenting some hands-on experiences and real time experiences.

The professional development workshop was organized into sections and delivered in three consecutive days. The technical materials presented on Day 1 and Day 2 were presented by faculty; whereas the hands-on experiences were designed and delivered by graduate assistants and students. The sessions on TracerFire B. Anderson, Nauer, Wellington, McClain, and Abbott [1] were designed and delivered by a professional cyber forensics team from the ABC National Laboratories (ABCNL), the project collaborators. Researchers of Sandia National Laboratories [14], describe the Tracer Fire (Forensic and Incident Response Exercise) training program as a classroom based multiday jeopardy style competition that focuses on forensics. Former participants include individuals from U.S. government agencies, law enforcement, industry and universities, which work in teams of four to six, as they are required to solve realistic challenges to gain points. Challenges require contestants to use cybersecurity software tools, to utilize forensic analysis techniques (e.g., review server logs to identify suspicious entries) and to analyze adversary tactics.

Guided by experiential learning theory, the design of the professional development workshop allowed participants to learn about digital forensics by 1) engaging participants with hands-on Concrete Experiences using TracerFire during workshop Hands-on Sessions, 2) engaging participants in Reflective Observation during workshop Discussion Sessions after the hands-on experiences, 3) engaging participants in Abstract Conceptualization by reflecting on what they had learned during workshop Presentation Sessions and how it applied to their teaching contexts, 4) engaging participants in Active Experimentation by asking them to consider how they could take what they experienced and learned during the workshop into their own teaching contexts. Participants went through this cycle each day of the workshop. In addition, data collection surveys were designed to gather participants' feedback as they themselves engaged with experiential learning as learners.

5.1. Participants

Fifteen post-secondary educators, who were participants of a three-day workshop related to digital forensics, were invited to complete a survey regarding their challenges with designing and teaching digital forensics to undergraduate students. The majority of the participants (73.3% ($n = 11$)) were university and college professors and instructors, one was a department chair, and three were graduate students teaching part-time. The majority (60.0% ($n = 9$)) of the participants were affiliated with 2-year community colleges, two were from 4-year teaching universities, and four from research-intensive universities. In terms of degrees, two participants had at most a certification, three had at most an undergraduate degree, six had at most a Master's degree, and four had at most a Ph.D. degree in Computer Science or a related field. The majority of the participants (73.3% ($n = 11$)) were male, and more than half (53.3% ($n = 8$)) were White (non-Hispanic or Latino), two were African American, one was Hispanic/Latino, two were Asian, and two preferred not to disclose their ethnicity. In terms of cybersecurity teaching experience, only one participant indicated that they had never taught a course in security related areas. It is important to note that demographic and other participant information was collected during the workshop registration phase and disconnected from workshop surveys. This helped to protect the identity of participants.

While this sample of participants was small, the uniqueness of this sample was that participants were all from the same Southwestern region of the US and included cybersecurity educators from 2-year community college, 4-year teaching universities, 4-year research universities, and cybersecurity experts from Sandia National Laboratories working together on cybersecurity education.

5.2. Data collection and analysis procedures

The main sources of data for the professional development workshop evaluation were locally developed Day 1, Day 2, and Day 3 Surveys that participants completed after each day of the workshop, respectively. These surveys were developed to align with the goals of the workshop which were to increase participants' pedagogical knowledge and confidence for teaching cybersecurity in their own contexts. Additionally, we were interested in participants' perspectives related to the use of experiential learning strategies to teach cybersecurity. Surveys were reviewed by the workshop designers prior to administration to participants. Workshop designers included a cybersecurity expert and educator, and a human factors psychologist who specializes in human-computer interaction.

These surveys are described below.

General Survey Related to Each Session. Each daily survey asked participants to:

- Rate their level of satisfaction (1=Extremely dissatisfied, 2=Somewhat dissatisfied, 3=Neither satisfied nor dissatisfied, 4=Somewhat satisfied, 5=Extremely satisfied) for each workshop session.
- List which session(s) they found most/least useful and explain why. (Open response with textbox to type in)
- Rate their level of confidence before and after the day's sessions (1=Not confident at all, 2=Only slightly confident, 3=Somewhat confident, 4=Moderately confident, 5=Very confident) on four confidence outcomes:
  - Knowledge of digital forensics,
  - Ability to design digital forensics lessons,
  - Ability to engage students with hands-on experiences, and
  - Ability to support students learning about digital forensics
- List what challenges they felt that they would encounter when designing and teaching digital forensics to their students (Open response with textbox to type in)
- Provide additional comments on how the day's session could be improved to better meet their needs. (Open response with textbox to type in).

5.2.0.1. Day 2 Survey: Additional Items. Additionally, the Day 2

Survey included three extra items that asked participants:

- how likely they would be to participate in future digital forensics workshops (1=Not likely, 2=Somewhat likely, 3=Very likely)?
- what they felt they needed more support with? (Open response with textbox to type in)
- what other cyber security topics they would be interested in for future workshops? (Open response with textbox to type in)

5.2.0.2. Day 3 Survey: Additional Items. Additionally, the Day 3 Survey also had one extra item, which asked participants to provide overall comments on how the 3-day workshop could be improved to better meet their needs. (Open response with textbox to type in)

The purpose of the surveys was to gather participants' satisfaction about workshop sessions aligned with different stages of experiential learning, which sessions they found most and least useful and why, and self-perceptions about sessions' impact to participants' confidence in the knowledge of cybersecurity and cybersecurity education. Secondly, participants were asked about what challenges they encountered and felt that they would face with teaching cybersecurity in their own context, their likelihood of participating in future cybersecurity education workshops, what topics future workshops should include, and how the workshop sessions could be improved.

Using descriptive statistics collected from these surveys, we examined participants' satisfaction with various types of sessions aligned with the stages of experiential learning theory or supports for those stages. For example, Presentation Sessions were specifically designed to provide participants with knowledge on what digital forensics topics students should learn and information of how to set up digital forensics labs. These sessions served as supports for participants before they engaged in Concrete Experiences. Next, Hands-on Sessions were specifically designed to provide participants with Concrete Experiences and opportunities for Active Experimentation. During these sessions, participants engaged in hands-on activities using digital forensic tools that cybersecurity experts use and that their students could use. Lastly, Discussion Sessions were designed to provide participants with opportunities engage in individual Reflective Observation and then Abstract Conceptualization with other participants. These latter stages of experiential learning (i.e., Reflective Observation and Abstract Conceptualization) were further promoted and exercised in the daily workshop surveys.

Secondly, using paired sample t-tests we examined the impact of the workshop on participants' confidence related to their knowledge of digital forensics, and ability to design, engage, and facilitate student learning using scenario-based and hands-on activities used in experiential learning.

Third, qualitative open-ended responses were collected and then hand-coded to identify themes related to participants' satisfaction with workshop sessions aligned with the stages of experiential learning. Open-ended responses related to the challenges that participants anticipated that they would encounter teaching digital forensics using experiential learning activities like the ones that participants were introduced to in the workshop were coded using a similar approach used in Study #1.

5.3. Results

5.3.1. Participants' overall satisfaction with workshop and sessions

Based on the average of all workshop sessions, participants were somewhat satisfied (M= 3.99, SD = 0.72) with the workshop. At the session level, participants were most satisfied with the following four sessions: discussion of TracerFire (#6) (M = 4.86, SD=0.38), the hands-on experience with TracerFire #6 (M = 4.57, SD=0.79), CTFs and Other Learning Tools (M = 4.56, SD=0.53), and the Panel General Discussion on Teaching Digital Forensics (M = 4.50, SD=0.97). All of these sessions occurred on Day 3 of the workshop. At the session level, based on descriptive statistics, participants were least satisfied with the following four sessions: Feedback Received on All Four Modules: Lessons Learned + Best Practice (M = 3.08, SD=1.32), the Day 2 Hands-on experience with TracerFire #7 (M = 3.18, SD = 1.33), the Day 2 Discussion of TracerFire #7 (M = 3.27, SD = 1.27), and XEN and NUCs as teaching tools (M = 3.45, SD=1.29). It should be noted that the workshop experienced technical issues with the network and hardware on Day 2. These issues prevented participants from getting hands-on experience and from fully engaging in discussions around the hands-on experience with TracerFire #7. On Day 3, when the technology issues were resolved, satisfaction improved with TracerFire #7 (M = 4.43, SD =0.79). The XEN and NUCs as teaching tools session on Day 2 also experienced technical issues with the hardware. See Table 1 in the Appendix.

5.3.2. Participants' satisfaction by session type

- Overall, participants were most satisfied with discussion sessions in which they were able to engage with cybersecurity expert presenters and other participants, followed by sessions where they received hands-on experiences, and lastly with lecture-based presentations. Results of paired samples t-tests suggested that participants' satisfaction differences were significant in that participants were most satisfied with discussions (M = 4.10, SD = 0.67), followed by the hands-on sessions (M = 3.97, SD=0.73), and then with the presentations (M = 3.88, SD=0.84). See Table 2 in the Appendix.
- Ratings revealed that while there were differences in satisfaction levels based on session type, participants' ratings were closer to 4 suggesting that they were at least somewhat satisfied with all three types of sessions.
- Responses from open-ended items that asked participants which sessions they found most useful and to explain why provided more insight into the previous results.

Table 1
Participant's Satisfaction with Workshop Sessions.

How satisfied are you with each of the following workshop topics? Day 1 Sessions	*M*	*SD*
A Framework for Developing Interviews to Understand Cyber Defense Work	4.08	1.04
Digital Forensics: What Should Students Learn?	4.08	0.95
Four Course Modules on Digital Forensics and Discussion	4.00	1.23
Setting up a Digital Forensics Lab	3.92	1.26
Presenting Module: Memory Forensics	4.00	1.00
Hands-on: Memory Forensics	3.92	1.11
Hands-on: USB Forensics	4.00	1.13
Feedback Received on All Four Modules: Lessons Learned and Best Practice	3.08	1.32
Introducing DigForPort: Digital Forensics Portal	3.77	1.01
Day 1 Total (N = 13)	3.88	0.82
Day 2 Sessions		
Experience Teaching Malware and Memory Analysis	4.27	0.65
Students Feedback and Lessons Learned	4.20	0.92
Cyber Kill Chain	4.36	0.81
General Discussion on Course Modules	4.00	0.78
Introducing Malware/Memory Analysis Modules	4.18	1.08
Xen and NUCs as teaching tools[2]	3.45	1.29
Hands-on Experience with TracerFire (#7)	3.18	1.33
Discussion on TF #7	3.27	1.27
Day 2 Total (N = 12)	3.87	0.86
Day 3 Sessions		
Panel General Discussion on Teaching Digital Forensics	4.50	0.97
CTFs and Other Learning Tools	4.56	0.53
Memory Forensics Continued. . .	4.38	0.52
TF#7 Continued	4.43	0.79
Hands-on Experience with TracerFire (#6)	4.57	0.79
Discussion of TracerFire (#6)	4.86	0.38
Day 3 Total (N = 10)	4.60	0.42
Overall Total	3.99	0.72

Table 2
Participants' Satisfaction by Session Type.

How satisfied are you with each of the following workshop topics?	*M*	*SD*
Presentations (Support for Concrete Experience and Active Experimentation)		
A Framework for Developing Interviews	4.08	1.04
What Should Digital Forensics Students Learn?	4.08	0.95
Four Course Modules on Digital Forensics + Discussion	4.00	1.23
Setting up a Digital Forensics Lab	3.92	1.26
Presenting Module: Memory Forensics	4.00	1.00
Feedback Received on All Four Modules: Lessons Learned and Best Practice	3.08	1.32
Introducing DigForPort: Digital Forensics Portal	3.77	1.01
Experience Teaching Malware and Memory Analysis	4.27	0.65
Students Feedback and Lessons Learned	4.20	0.92
Cyber Kill Chain	4.36	0.81
Introducing Malware/Memory Analysis Modules	4.18	1.08
Xen and NUCs as Teaching Tools	3.45	1.29
CTFs and Other Learning Tools	4.56	0.53
Memory Forensics continued. . .	4.38	0.52
Presentation Total ($N = 15$)	3.88	0.84
Hands-on Sessions (Concrete Experiences and Active Experimentation)		
Hands-on: Memory Forensics	3.92	1.11
Hands-on: USB Forensics	4.00	1.13
Hands-on Experience with TracerFire (#7)	3.18	1.33
TF#7 Continued	4.43	0.79
Hands-on Experience with TracerFire (#6)	4.57	0.79
Hands-on Total ($N = 15$)	3.97	0.73
Discussion Sessions (Reflective Observation and Abstract Conceptualization)		
General Discussion on Course Modules	4.00	0.78
Discussion on TracerFire #7	3.27	1.27
Panel General Discussion on Teaching Digital Forensics	4.50	0.97
Discussion of TracerFire (#6)	4.86	0.38
Discussion Total ($N = 12$)	4.10	0.67

Responses suggested that:

- Participants liked discussions mainly because these sessions allowed them to learn from their peers. For example, one participant stated "The discussion was amazing. I learned a great deal from others in the room and felt heard at the same time." Another participant stated that they liked the panel discussion the most because "it helped me to get some idea that how other people think about the area."
- Participants liked the hands-on experiences mainly because it allowed them to experience what their students would experience and also what digital forensics experts in the field do. One participant stated that "seeing what students will go through is very interesting. Thinking like they would have to think helps me to understand how I would develop a class, should I need to do so. It was really neat seeing the PDF analyzer show the individual Hex bits of the file." One participant liked experiencing the "thought process for diagnosis." Another participant stated that "The TracerFire exercises ended up being very interesting. Use of various tools and talking with peers were highly engaging. The problems were intriguing, even though hard at times." Participants especially liked the ABC's hands-on demonstrations due to their closeness to what digital forensics experts really do. One participant stated "I thought the hands-on experience sections were really cool, and they provided a lot of useful information. I did not expect to analyze real viruses and see their actual effects, nor did I realize that the TracerFire system was so close to how security professionals actually study disk and disk information." One participant, however, would have liked more support and guidance. This participant stated that "TracerFire would have been good except my experience level is well below that of other attendees, presentation should have been tailored to meet the level of all attendees. Experience level of attendees varies, just throwing us in to "figure it out" is NOT a great teaching technique. I did not learn as much as I would have liked."
- Participants liked the presentations because they increased their knowledge and also gave them ideas of what they could incorporate into their classrooms. From Day 1, one participant stated "I enjoyed the overview. It really helped me to understand what digital security and digital security forensics is. I also got a good idea of what to expect in the classroom learning digital forensics." Another stated "I enjoyed the USB Forensics the most since it could benefit many of my classroom teachings." Another stated "The course material on digital forensics is excellent. It provided many research directions to the attendees that are highly useful." Others stated that the presentations helped them realize their own knowledge gaps. For example, "All items presented were a very good "reality check." I have an idea now of knowledge "voids" that need to be remediated." For example, the scenario-based cyber kill chain topic was "a new experience" to multiple participants and they said that "it was interesting because it was based on a real-world experience."

5.3.3. Impact on Participants' Confidence in Their Knowledge and Skills Related to Teaching Digital Forensics

A second major goal of the workshop was to positively impact on participants' confidence in four areas: their knowledge of digital forensics topics, ability to design digital forensics lessons, ability to engage students with hands-on experiences, and ability to support students learning digital forensics. Overall results suggested that the workshop had a significant positive impact on participant' confidence in all four areas ($p < 0.01$). See Table 3 and Fig. 1.

5.3.4. Challenges: educators' perspective

Participants were asked to reflect on their own teaching contexts and to list anticipated challenges that they felt they would encounter when designing and teaching digital forensics lessons to their students.

Overall results suggested that the major challenges workshop participants felt that they would encounter revolved around six major themes:

- Subject knowledge of digital forensics (31.57% of participants),
- Initial set up and design of laboratories (26.31% of participants),
- Laboratory materials (15.78% of participants),
- Limited curricula (13.15% of participants),
- Institutional contextual factors (7.89% of participants), and
- Safety issues (5.26% of participants).

Challenge #1: Educator subject knowledge of digital forensics. A frequent theme that emerged from participants' responses about what challenges they felt that they would encounter was their own knowledge of digital forensics. For example, one participant stated that "I am still learning." Another said that his or her major challenge would be "Becoming more astute with the subject matter, which will only come with time spent delivering the content." Subject knowledge about digital forensics was viewed as a major challenge because participants felt that their teaching would be negatively impacted without it. For example, one participant stated, "I need more training in many topics before I could confidently teach my students." "More subject knowledge is crucial because instructors must be able to answer questions from any possible angle."

Specific topics that they felt that they would need more knowledge about included "foundation topics such as file systems, file formats (.exe, PDF, etc.)", "CTFs," "familiarity with the tools that were presented," and learning more about the "various stages of diagnosing and tools pertaining to each stage" especially as one participant stated the "Tools and their commands change rapidly across OS. Thus, steps may vary every time even for the similar malware analysis."

Challenge #2: Initial set up and design of labs. Another frequent theme that emerged from participants' responses about what challenges they felt that they would encounter was with the initial set up and design of labs. For example, some participants felt that the initial set up of labs

Table 3
Impact on Participant's Confidence in Knowledge, Ability to Design, Ability to Engage, and Ability to Support Students with Digital Forensics Topics: Paired *t*-test Results.

Confidence Outcomes	*N*	*Before M(SD)*	*After M(SD)*	*t value*	*p value*
Day 1					
Knowledge of how to set up a digital forensics lab	12	1.83 (1.03)	3.08 (1.24)	4.10	.002*
Knowledge of memory forensics	12	1.69 (0.86)	3.23 (1.01)	5.28	.000*
Ability to design scenario-based activities related to memory forensics	13	1.69 (1.03)	3.00 (1.00)	5.52	.000*
Ability to engage students with hands-on scenario-based activities related to memory forensics	13	1.69 (1.03)	2.85 (1.07)	5.20	.000*
Ability to support students using scenario-based experiences learning about memory forensics	13	1.62 (0.87)	3.08 (0.86)	6.79	.000*
Day 2					
Knowledge of Cyber Kill Chain	10	1.90 (1.29)	3.80 (1.14)	5.02	0.001*
Knowledge of Malware and Memory Analysis	11	1.73 (0.91)	3.18 (1.08)	4.66	0.001*
Knowledge of XEN and NUCs as teaching tools	10	1.40 (0.84)	3.00 (1.41)	3.75	0.005*
Ability to design scenario-based activities similar to TF#7	11	1.64 (0.81)	2.55 (1.29)	2.65	0.024*
Ability to engage students with hands-on scenario-based activities similar to TF#7	12	1.67 (0.78)	2.75 (1.22)	3.03	0.012*
Ability to support students with hands-on scenario-based activities similar to TF#7	12	1.75 (0.75)	2.67 (1.23)	2.56	0.026*
Day 3					
Knowledge of digital forensics	9	2.67 (0.87)	4.22 (0.283)	6.42	0.000*
Knowledge of memory forensics	7	2.00 (0.31)	3.57 (0.43)	5.28	0.002*
Knowledge of CTFs and Other Learning Tools	8	1.50 (0.76)	3.63 (1.06)	5.33	0.001*
Ability to design scenario-based activities similar to TF#6	6	1.50 (0.84)	3.17 (1.17)	5.00	0.004*
Ability to engage students with hands-on scenario-based activities similar to TF#6	6	1.83 (0.98)	3.33 (1.21)	4.39	0.007*
Ability to support students with hands-on scenario-based experiences	7	1.86 (0.90)	3.57 (1.27)	6.00	0.001*

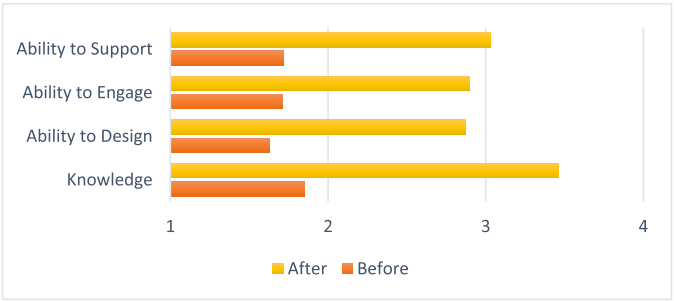

Fig. 1. *Weighted Means for Participants' Confidence Outcomes Before and After Workshop*
Note. Weighted means were calculated based on each category of confidence outcomes listed in Table 3. Confidence was assessed on a 5-point Likert scale: 1=Not confident at all, 2=Only slightly confident, 3=Somewhat confident, 4=Moderately confident, 5=Very confident.

would be challenging. For example, one stated the issue of "Setting up an isolated network." Another identified "coming up with a scenario that wouldn't involve having the students interact with live malware and/or having that happen in an isolated situation."

Challenge #3: Institutional contextual factors. Another frequent theme that emerged from participants' responses about what challenges they felt that they would encounter was related to contextual factors at their institutions. For example, some participants noted the limited financial and technical support. Another participant stated "Designing a digital forensics course will be very difficult with budget limitations and support. What I can continue to offer are "feeder" courses that prepare students to further their education and goals in Computer Forensics." Similarly, another stated that "financial" costs were the major challenge.

Other participants noted challenges due to degree plans. For example, one stated that "The major challenge is 60-hour restriction on Associate level degrees." Similarly, another participant stated that "We are a two-year institution. There is not adequate time to teach all aspects of digital forensics, thus our program will focus on disk analysis at best."

Challenge #4: Knowledge level of students. Lastly, another theme that emerged from participants' responses about what challenges they felt that they would encounter was related to concerns about students' knowledge of digital forensics. For example, one participant stated that a challenge was "making sure students have the necessary background information and knowledge about using the tools." Another noted the challenge of "Not overloading my students."

5.3.5. *Additional topics of interest to participants*

When prompted for other topics that they would be interested in for future workshops, responses included "continued investigation into what skills are needed from the industry would be interesting and informative. Also, information about building a cyber program at a two-year school would be interesting," "Block Chain Technology; Machine Learning", "Examples with security policies and data security mechanisms", "Software and tools used in cybersecurity," "I think there should be a focus on web-based security. Lots of people build and maintain websites, and there are lots of security traps that people are unaware of. I also think websites are often the most visible and easy to find to hack," and "Securing, home computers, devices, smartphones, baby monitors all everyday security of devices that the public uses. At my school, I center on the high-end devices and not enough on the most common devices used by everyone that are the most vulnerable."

5.4. *Recommendations from study #2*

Based on workshop participants' responses, a series of recommendations on how the workshop and sessions could be improved were developed. The first four recommendations revolved around improving the hands-on sessions, and last two recommendations related to improving the workshop sessions overall.

Recommendation #1: Provide participants with step-by-step handouts to follow during the hands-on sessions. A frequent theme that emerged from participants' responses about why they found some sessions to be least useful was due to the lack of step-by-step handouts during the hands-on sessions. For example, one participant stated "There should have been hand-outs considering all the commands used, it was hard to keep up with the speed they covered the slides. The topics were interesting, but I felt rushed." Another stated "The hands-on exercises were too difficult to follow. It would have been nice to have a transcript with all required steps so we can progress independently of what was written on the board."

Regarding the types of resources, participants mentioned "steps and the commands are provided in a cheat-sheet for us to copy and paste," "better explanations were necessary as to what we were achieving at each step," "a transcript of the steps and what each one meant," and an "overview of the tools." It is therefore recommended that future workshops provide participants with electronic handouts that will help them

follow along during the hands-on sessions.

Recommendation #2: Provide participants with sufficient time and background knowledge support during hands-on sessions. Another frequent theme that emerged from participants' responses was that participants felt that they needed more time and background knowledge support during hands-on session. For example, one participant stated that the "Presentation [malware memory analysis] should have been slowed down and presented more step-by-step. I am a novice and would have enjoyed the experience more if I could have kept up. Some instructions were not clear and/or assumed a greater understanding of the processes. Really would have been awesome if I could have seen all the outcomes on my system." Another wrote "I wish you would have gone step by step with us. I did not have the experience others did and was lost at times on the commands to type. If during the lecture they could have shown each steps or prompt and command to type would have been helpful, it was assumed to much that we all knew what we were doing, and I missed out on the final results." Another participant wrote that he or she "Was frustrated with the process of using the NUC/XEN servers. Even without the technical problems, I didn't have the background to begin to investigate the problem." Similarly, another participant stated that "very little background information was given before the exercise [TracerFire hands-on] was started. This left me feel like thrown into the water to learn to swim on my own."

It is therefore recommended that future workshops provide participants with more time during the hands-on sessions and possibly add supporting materials/resources to provide participants with background knowledge that they would need during the hands-on sessions. These supporting materials could be provided before the workshop or hands-on session.

Recommendation #3: Provide participants practice with tools prior to hands-on sessions where tools will be used. Another frequent theme that emerged from participants' responses was that participants felt that they needed more practice with the tools used during the hands-on sessions. For example, one participant wrote "I think we needed more time to explore the tools of the TracerFire system. I feel we needed an explanation before being able to attempt to solve some of the more difficult aspects of TracerFire. Again, I understand the limitations of the conference, but it would be nice to be walked through how the tools work (and maybe a cheat sheet explaining what tools do what). It's hard to approach this topic with minimal tool information." Another stated "I would have liked a better explanation of the tools in TracerFire before trying to use them, but I also understand this is a short-course of digital security."

Similar to recommendation #2, participants felt that they needed more background information on the tools being used during the hands-on sessions. For example, one participant said "TracerFire hands-on was useful but the commands were not explained properly. Also, the XEN session was a total disappointment as the presenter expected the participants to possess extreme knowledge about network analysis and no help was provided."

It is therefore recommended that future workshops provide participants with more time to explore the tools prior to their use during the hands-on sessions and provide an overview and explanation about what these tools can be used for prior to their use during the hands-on sessions.

Recommendation #4: Ensure that technology is working properly prior to hands-on sessions. Another frequent theme that emerged from participants' responses was due to the technology issues that came up during the hands-on sessions on Day 2 of the workshop. For example, one participant stated "The hands-on was disappointing because it wasn't working. I understand that it is difficult to manage a mobile lab space but I was really looking forward to the experience." Another wrote "I was a little disappointed that the hands-on demonstrations did not work properly but that is technology and ISP for you."

It is therefore recommended that future workshops fully test all technology prior to the workshop in order to prevent session interruptions and frustration due to technical issues.

Recommendation #5: Omit covering topics that participants can read outside of the sessions. Lastly, regarding overall recommendations for improving workshop sessions, participants desired that topics that could read outside of sessions be omitted from the workshop. For example, topics that participants felt that they could have read outside of the workshop included the "syllabus of the class" from Day 1, "reading student feedback" from Day 1, and "the overview of the surveys" at the end of the Day 1. Participants felt that they could read this information outside of the sessions. One participant recommended that instead of simply reading student feedback, that discussing "how to improve the course based on students' feedback and how to motivate students" would have been more beneficial.

6. Discussion

The purpose of the present study was to describe the experiences and perceptions of students and educators using the experiential learning approach to design and teach digital forensics. Additionally, this paper examined the challenges that students and educators encountered or anticipated that they would encounter when using experiential learning to teach and learn digital forensics in post-secondary education. Similar to previous studies [3,11], this study found that both students and educators had positive experiences with the experiential learning, and when asked about their experiences and learning needs both students and educators requested tasks and instructional resources aligned with aspects of the experiential learning approach. For example, students in the digital forensics course described in this study requested more hands-on Concrete Experiences. Similarly, participants in the digital forensics professional development workshop also reported high satisfaction with the hands-on Concrete Experiences. Moreover, participants in the professional development workshop reported highest satisfaction with the discussion sessions immediately after hands-on Concrete Experiences. Similar to the findings of Yuan et al. [19] these discussion sessions allowed educators to reflect on their own and with their peers on their hands-on concrete experiences to make connections with what they experienced and learned from Presentation Sessions. Additionally, these concrete experiences allowed participants to further consider how they were going to put what they learned into their current and future cybersecurity education practices. In this sense, this finding supported the importance of the Reflective Observation and Abstract Conceptualization stages of experiential learning. Furthermore, this result aligned with Stirling et al. [17] who recommended that experiential learning can be optimized when it includes reflection and explicit connections between coursework and practical experience.

Secondly, while participants reported positive experiences using experiential learning, this approach did present challenges specifically during the Active Experimental stage. For example, students and workshop participants both reported challenges with setting up labs used during the hands-on Concrete Experiences and requested that additional support for learners be provided. This finding suggests that educators should be prepared to provide additional supplemental resources such as step-by-step handouts for setting up labs and/or live demonstrations of how to use digital forensic tools prior to the hands-on experiences. This recommendation aligns with Cigoj and Blažič [7] who provided a real cloud-based computing environment to help support students learning digital forensics. However, it is crucial that when providing additional support that post-secondary educators should provide support aligned with the experiential learning theory [17]. For example, using the 2CADS which allotted course time for reflections with instructors and peers, team discussions around connecting coursework to practical experiences, and opportunities for students to compare what they did to what their peers did in preparation for future practice. Additionally, when asked to describe anticipated challenges related to teaching digital forensics at their respective institutes, educators highlighted a lack of time and budget to create hands-on

experiences, lack of space in curricula, and instructional supports. These results are consistent with previous researchers who had difficulties with designing and digital forensic labs due to budgets [6,8,16,20]. These challenges may explain why educators may have less interest in introducing and offering such important courses in digital forensics or with using experiential learning to teach such courses.

7. Conclusions, limitations, and implications for future research

In summary, this study adds to the literature by describing how cybersecurity educators can use experiential learning theory to design learning experiences, which is lacking in the literature [17]. Additionally, this study gathered both student and educator perspectives after engaging with experiential learning and gathers their perspectives and anticipated challenges. Results suggested that learners were satisfied with their experiences and increased in their confidence. Despite the many of these challenges can be partially solved by offering professional development to post-secondary digital forensics educators, sharing instructional resources (e.g., expert designed laboratories, instructional modules, and hands-on experiences) with them, and by using the recommendations offered in this paper, it is crucial that future researchers continue to explore and examine how to support both learners and teachers of digital forensics in post-secondary education.

Despite its findings, this paper did have limitations. First, while the authors of this study intentionally used the experiential learning theory to design a digital forensics course and a professional development workshop, the topic of how to use experiential learning theory to design and teach was not directly taught to participants. Future course and workshop designers should not only engage participants in learning activities that are designed based on the experiential learning theories but also explicitly cover this topic in their training. Additionally, future researchers should examine the impact of using experiential learning to teach cybersecurity on participants' knowledge, skills, and motivation.

Secondly, another limitation was that we did not conduct a follow-up with participants specifically the faculty participants of the professional development workshop to measure the impact of the workshop on their abilities to design and teach digital forensics courses in their contexts. Future research on the delayed impact of using experiential learning to teach cybersecurity is very much needed.

Declaration of Competing Interests

The authors declare that they have no known competing financial interests or personal relationships that could have appeared to influence the work reported in this paper.

Funding

This work is supported by National Science Foundation grants under award numbers 1516636 and 1821560.

References

[1] [1]Anderson, B., Nauer, K., Wellington, L., McClain, J., & Abbott, R. (2015). *Tracer fire cyberforensic training platform.*https://www.osti.gov/servlets/purl/1251138.
[2] [2]Anderson, P., Dornseif, M., Freiling, F.C., Holz, T., Irons, A., Laing, C., & Mink, M. (2006). A comparative study of teaching forensics at a university degree level. *IT-Incident management & it-forensics-imf 2006*.
[3] Batten L, Pan L. Teaching digital forensics to undergraduate students. IEEE Secur Priv 2008;6(3):54–6.
[4] Bishop M. What is computer security? IEEE Secur Priv 2003;1(1):67–9.
[5] Brustoloni JC. Laboratory Experiments for Network Security Instruction. ACM J Educational Resour Comput 2006;6(4):Article 5.
[6] Chi H, Jones E, Chatmon C, Evans D. Design and implementation of digital forensics labs. In: Proceedings of the 12 iasted international conference on computers and advanced technology in education; 2009.
[7] Cigoj P, Blažič BJ. An innovative approach in digital forensic education and training. In: Ifip world conference on information security education; 2015. p. 101–10.
[8] Crick T, Davenport JH, Hanna P, Irons A, Prickett T. Overcoming the Challenges of Teaching Cybersecurity in UK Computer Science Degree Programmes. In: 2020 IEEE Frontiers in Education Conference (FIE). IEEE; 2020. p. 1–9.
[9] CSIS. Hacking the skills shortage. Santa Clara, CA: McAfee; July 2016. Retrieved from, https://www.mcafee.com/enterprise/en-us/assets/reports/rp-hacking-skills-shortage.pdf.
[10] Du W, Wang R. SEED: a Suite of Instructional Laboratories for Computer Security Education (Extended Version). The ACM J Educational Resour Comput (JERIC) 2008;8(1). Article 3.
[11] Floyd K, Yerby J. Development of a digital forensics lab to support active learning. Development 2014;4:14–2014.
[12] Kaneko K, Ban Y, Okamura K. A Study on Effective Instructional Design for IoT Security Education Focusing on Experiential Learning. Int J Learning Technol Learning Environ 2019;2(1):1–18.
[13] Kolb D. Experiential learning: experience as the source of learning and development. Englewood Cliffs, NJ: Prentice Hall; 1984.
[14] McClain J, Silva A, Emmanuel G, Anderson B, Nauer K, Abbott R, Forsythe C. Human performance factors in cyber security forensic analysis. Procedia Manufacturing 2015;3:5301–7.
[15] Sanders AD. Utilizing Simple Hacking Techniques to Teach System Security and Hacker Identification. J Information Sys Education 2003;14(1):5–10.
[16] Srinivasan S. Digital forensics curriculum in security education. J Info Technol Education 2013;12:147–57.
[17] Stirling A, Kerr G, MacPherson E, Banwell J, Bandealy A, Battaglia A. Do postsecondary internships address the four learning modes of experiential learning theory? an exploration through document analysis. Canadian J Higher Education 2017;47(1):27–48.
[18] Yoder BL. Engineering by the Numbers. Am Society for Eng Education 2012;37.
[19] Yuan X, Williams K, Yu H, Chu B, Rorer A, Yang L, Kizza J, Winters K. A Workshop on Teaching Information Assurance through Case Studies and Hands-on Experiences. In: Proceedings of the 47th Hawaii International Conference on System Science (HICSS 2014); 2014.
[20] Ward P. Development of a Small Cybersecurity Program at a Community College. In: Proceedings of the EDSIG Conference ISSN. 2473; 2020. p. 4901.