Bureau of Justice Assistance Student Computer and Digital Forensics Educational Opportunities Program: The Assessment of Online Graduate Students

Kyung-Shick Choi[1], Chitkushev Lou[2], Kyung-Seok Choo[3] and Claire Seungeun Lee[4]
[1]Professor of Practice, Department of Applied Social Science, Metropolitan College, Boston University, USA
[2]Associate Professor, Computer Science, Associate Dean, Metropolitan College, Boston University, USA
[3]Professor, School of Business & Justice, Utica College, USA
[4]Assistant Professor, School of Criminology & Justice Studies, University of Massachusetts Lowell, USA
kuung@bu.edu
ltc@bu.edu
kychoo@utica.edu
claire_lee@uml.edu

Abstract: The current capabilities of many law enforcement agencies are tightly constrained despite the heightened level of awareness and concern for the role recent technology has in facilitating cybercrime and instances of online victimization. More specialized computer forensics and digital evidence training programs are necessary to meet the needs of local and state law enforcement agencies. Based on the context, this paper discusses an interdisciplinary approach to addressing this dilemma while providing in-depth computer forensics and cybercrime investigation training that is both informative and pragmatic to future law enforcement officers. Using pre- and post-test results, this study assesses students' technical background levels, reflecting comprehensive course learning objectives and pre-training levels of applied digital forensic investigation knowledge. Results suggest that students' technical abilities and knowledge of different investigative tools significantly improved after the program. In particular, the program not only strengthened students' knowledge of digital forensic investigation, but also helped students achieve higher t-test scores. We expect our study results to provide recommendations for cyber programs in other higher education institutions. The findings will serve as a guide for enhancing the current capacities of other higher education institutions to better serve their students in areas of computer forensics and digital evidence. In the long term, these efforts will lead to more effective cybercrime investigation and successful prosecutions, ultimately reducing cybercrime victimization.

Keywords: computer forensics, training, law enforcement, cybercrime investigation

1. Introduction

As demonstrated by a string of recent cases, cybercrime problems have proliferated as digital and information technology become more widely adopted. Throughout the COVID-19 pandemic, cybercriminals have utilized mass fear and panic to exploit vulnerable victims through ransomware attacks, counterfeit remedies, coronavirus phishing, federal stimulus check scams, and fake charities for coronavirus causes.

In the digital age, awareness of and concern about the role of the latest technology in facilitating cybercrime and online victimization has grown tremendously. Unfortunately, the current capabilities of many law enforcement agencies to investigate such crimes remain limited, as most officers lack the necessary training in processing computer data and related evidence to effectively investigate cybercrime. To meet the rapidly digitizing demands of state and local law enforcement, more specialized computer forensics and digital evidence training programs are required.

The current study explores in-depth computer forensics and cybercrime training designed to be both informative and pragmatic about the students currently enrolled in Criminal Justice (CJ) and cybercrime/computer science (CS) program in a higher education institution and who might be future law enforcement officials. We use an interdisciplinary approach to assess the effectiveness of this program. This study uses a mixed-methods research design and evaluates student technical training, reflecting the comprehensive learning objectives of the course and the level of knowledge in the applied digital forensic exams prior to the online training. The results of the pre- and post-tests demonstrate that students' technical skills and knowledge of various digital forensics tools

improved significantly after learning the tools in the program. The study was especially effective at strengthening students' knowledge of digital forensic examinations and helping students achieve higher test scores in our post-test.

2. Related work

Originating in the late 1980s, law enforcement professionals used the term computer forensics to refer to the examination of independent computers for digital criminal evidence (Yasisac et al, 2003). Computer/digital forensics later evolved to describe the post-incident analysis of computer attacks by intruders or malicious code (Liu and Wang 2009). The emergence of cybercrime and cybersecurity issues gave rise to the expectation that law enforcement agencies (LEA) should equip themselves with computer forensics knowledge and practical skills. However, there are currently at least two issues with the LEAs' approaches to computer forensics. On the one hand, LEAs have vastly differing levels of resources, capacity, and manpower. Small local LEAs are not as advanced in these regards. On the other hand, despite that computer forensics is an emerging field, much complicated and higher-level training in computer forensics is also in development. While most of the programs are focused on computer science, a limited number of programs are offered for other relevant social sciences (e.g., criminology/criminal justice).

Digital forensics training at higher education institutions offers students the opportunity to acquire skills, exposes them to hands-on exercise, and allows them to gain new knowledge. In doing so, curriculum development to accommodate recent skills and experiences for students is important (Antunes and Rabadao 2019). Most of the existing studies remain focused on undergraduate computer science/cybersecurity degrees (Chi et al, 2009; Ward 2020); however, these studies give us universal insights that can be applied to a postgraduate level. Zhang and Choo (2020) suggest an experiential learning approach for successful digital forensic education. Hands-on labs and case studies are an effective pedagogical method of teaching cybersecurity (Du and Wang 2009; Flores et al, 2021; Yuan et al, 2014; Ward 2020). A scenario-based and "learning by doing" approach is effective (Batten and Pan 2008; Ward 2020). Experience in real-world problems plays an important role of students' pathway to employment (Mison et al 2020).

In an examination of online education in computer and digital forensics, Kessler (2007) found that online courses with active, problem-based learning methods are better suited to the needs of adult learners (Kessler 2007b). Training, teaching students, and nurturing their technology knowledge base is critical. Most of all, the competence of fundamental computer skills and the capacity to demonstrate practical skills are essential in computer/digital forensics (Anderson et al., 2006; Antunes and Rabadao 2019). In particular, online labs provide one of the most supportive environments for active learning, as technology-transparent courses are more interactive, translating to successful experiences for learners (Kessler 2007b; Flores et al, 2021). Online formats create an opportunity to students to catch up material (Buchanan et al, 2010).

3. Current study, data, and methods

3.1 Curriculum design

To provide students with the essential computer forensics and digital evidence skills that will prepare them to work within all levels of law enforcement agencies, the research team conducted expert focus groups and steering committee meetings with representatives from local, state, and federal law enforcement agencies. The experts reviewed the contents of relevant courses, including techniques and software, learning objectives, and assessment tools to determine whether they meet the current needs of law enforcement. Most class projects of the finally selected courses for the study consist of practical labs and hands-on exercises that strongly tie into the areas of computer forensics and cybercrime investigation, and are aligned with the best practices based on current law enforcement training manuals, CDFE (Certified Digital Forensic Examiners) curriculum mapping, and NIST (National Institute of Standards and Technology) Digital Forensic Techniques Guide.

Due to the COVID-19 pandemic, all existing courses were converted to the online format. We assessed the program goals based on the program curriculum map below. It involved (1) course objectives' alignment with the program's goals, (2) a systematic review of course syllabi, textbooks, and teaching materials, and (3) course-embedded assessment using oral presentation, paper, projects, lab practice, and graded thread discussions. We also developed pre/posttest course assessment tools and implemented to achieve a practical course level of assessment.

We used the Cybercrime (CJ 610) course to assess the introduction levels of the program goals, while the Applied Digital Forensic Investigation (CJ710) course determined the reinforcement levels. For the proficiency level, we used the Digital Forensics and Investigations (CS693) and Mobile Forensics and Security (CS694)[1] courses to determine the demonstrated achievement of program goals. We used the curriculum map as a guide to assess whether each class introduced, reinforced, and provided the appropriate levels of the program goals. We utilized various assessment tools such as TD (thread discussions), PP (papers), PJ (project), C (capstone), and LB (lab).

The intent of our assessment was to develop a refined cybercrime investigation training curriculum for future law enforcement officers. This assessment provided students with the most comprehensive and reliable cybercrime investigation training available in regard to Computer Forensics and Digital Evidence Educational Training.

Courses	1. Demonstrate an understanding of key concepts and processes in computer forensics and digital evidence.	2. Demonstrate critical thinking and analytical performance capability related to computer forensics and digital evidence.	3. Use various tools to conduct computer forensics and analyze digital evidence.	4. Apply appropriate legal and ethical concepts to computer forensics and digital evidence.
CJ 610 Cybercrime	**I**	**I**	**I**	**I**
CJ 710 Applied Digital Forensic Investigation	**R**	**R**	**R**	**R**
CS 693 Digital Forensic Investigation	**P**	**P**	**P**	**P**
CS 694 Mobile Forensics and Security	**P**	**P**	**P**	**P**

Abbreviations. **I = introduced. R = reinforced. P = proficiency**.

I = Introduced; student learning outcomes will be measured if the course introduced relevant program goals
R = Reinforced; student learning outcomes will be measured if the course provided practice opportunities
P = Proficient; student learning outcomes will be measured for the demonstrated achievement of the program goals.

Figure 1: Curriculum design

3.2 Mixed method research design and data collection

We used a mixed-method research design, which originated in the social sciences and is used in other disciplines. This approach is based on comprehensive data collection and provides similarly robust and multi-faceted results. This study integrates quantitative and qualitative research and follows an explanatory sequential design, also known as an "explanative design." It consists of two phases: quantitative data collection and analysis, followed by qualitative data collection. The latter is used to explain the initial quantitative results, also known as a "Quat + Qual" model (Schoonenboom and Johnson 2017). We essentially use the same sample to extract two types of data in succession.

3.3 Quantitative method

All students who contributed data for this study participated in pre-post online surveys to assess the Student Computer Forensics and Digital Evidence Educational Opportunities Program. The quantitative analysis aims to (1) assess the level of students' technical background, per the course's comprehensive learning objectives and level of knowledge in the applied digital forensic investigation prior to the online training, and (2) evaluate the impact of the training by comparing pre-and post-test results.

[1] The course numbers and titles indicate: Criminal Justice 610: Basic Technical Level, Criminal Justice 710: Basic-Intermediate Technical Level, Computer Science 693 Intermediate-Advanced Technical Level, and Computer Science 694: and Advanced Technical Level.

Questionnaires were designed by two researchers and cross-validated by a third person. Participants are students in a Master's in Criminal Justice program, and online surveys were sent to participants during the first day of class and the last week of each semester. For the quantitative pre- and post-test data collection segment, we analyzed scores from four core courses offered in Spring 2020 and Summer 2021. Qualified students were selected as a group, and the participants were responsible for completing pre-post testing and contributing interviews for program evaluation purposes. To conduct an overall assessment for the Student Computer Forensics and Digital Evidence Educational Opportunities Program, all students were encouraged to participate in the four pre-post online surveys.

We performed a paired t-test to determine the difference between dependent variables for the same subject in two related groups. We compare pre-class and post-class test scores to examine the effectiveness of the four courses taken by participants during their program in increasing technical background and knowledge related to digital forensics. Each questionnaire had two parts: the "student technical background measure" and the "knowledge test." Concerning CJ710 and CS693, participants filled out a 16-item questionnaire (student technical background measure) and a 20-item questionnaire (knowledge test) before and after the training. For the third course (CS694), participants filled out a 13-item questionnaire (student technical background measure) and a 28-item questionnaire (knowledge test) before and after the training. For CJ610, participants filled out a 15-item questionnaire (student technical background measure) and a 20-item questionnaire (knowledge test) before and after the training. Each pre- and post-test asked the same set of questions, varying only by course, and students were asked to state their confidence levels regarding meeting course learning objectives. Only participants who completed both pre- and post-tests were included in the analysis (CJ710: N=31, CS693: N=32, CS694: N=20, CJ610: N=23). Using the pair-sample t-test, the differences between pre- and post-test scores were examined for statistical significance.

3.4 Qualitative method

After completing the pre-post tests, four students in each class were selected to partake in qualitative data collection. The qualitative analysis consisted of conducting interviews to assess the effectiveness of the program's four courses: (1) CJ610, (2) CJ710, (3) CS693, and (4) CS694. Specifically, the interview questions were developed in effort to reflect course objectives, and the responses were utilized to assess the courses' areas of success and those where improvements are needed. These participants were randomly selected using the program SPSS seed function. Each student had an equal chance of being assigned to an interview group, and each interview was held online via Zoom for approximately one hour. We recorded interviews of participants who consented and otherwise jotted down key information and details within a day of interview completion.

4. Results

4.1 Quantitative analysis

We used a series of paired t-tests to evaluate the overall effectiveness of each course by determining a statistical difference between the means of the pre- and post-test scores. For the first question/hypothesis on student technical background differences, the finding suggests that the average pre-test score for student technical background (CJ710: M=32.10, SD=13.66; CS693: M=31.69, SD=11.11; CS694: M=22, SD=9.64; CJ610: M=36.27, SD=13.64) is significantly lower than the post-test score (CJ710: M=67.06, SD=9.84; CS693: M=62.59, SD=11.08; CS694: M=57, SD=7.66; CJ610: M=61.91, SD=9.60). Here, the differences between the pre-post test scores indicate that the training contributes to the level of student technical background and knowledge about digital forensic investigation. As expected, student technical knowledge mean scores are more likely to increase after completing each course, as students gain more knowledge over the semester.

Likewise, the findings for the second measure suggest that the average pre-test score for knowledge in digital forensic investigations (CJ710: M=5.52, SD=3.40; CS693: M=8.28, SD=4.10; CS694: M=6.53, SD=5.58; CJ610: M=6.13, SD=3.35) is significantly less than the post-test score (CJ710: M=15.58, SD=2.88; CS693: M=14.13, SD=3.61; CS694: M=21.67, SD=3.22; CJ610: M=12.74, SD=2.50). In other words, due to the training that students received over the duration of the semester, mean test scores measuring knowledge about the digital forensic investigation are more likely to increase after course completion.

Overall, these results provide quantitative evidence that training (via course completion) influences the difference between pre- and post-test scores. More specifically, mean test score results from the pre- and post-

tests demonstrate that levels of student technical background and levels of digital forensic investigation knowledge are strengthened after course completion.

Figure 2: Pre-post result

Note: Scores indicate means.

4.2 Qualitative analysis

Computer forensics is one of the core themes of cybercrime investigation. However, this area has yet to be introduced widely in the CJ program, even though it has been taught extensively in the CS program. Given that our participants are primarily enrolled in the CJ program and work in former, current, or future law enforcement sectors, this training in computer forensics plays an important role in shaping their learning experience, confidence, and career. In what follows, we abide by the general structure of program evaluations and analyze interviews in relation to the quality of training course instruction, training content, and online training.

4.3 Quality of training course instruction

Participant 3 (CJ710) explained that,

> *A theme throughout the course was cybercrime investigations utilizing a forensic tool known as, EnCase. Students were provided with an interesting storyline following a suspect named Mr. Evil, providing his students with just enough information, so even the experienced people are given the opportunity to dig in deeper and explore the material like a treasure hunt.*

Even though some of the interviewees already had relatively strong backgrounds and positive experiences working in the field of computer science, they enjoyed how the course instructors were consistently available to provide guidance, explain everything step-by-step, and take students back to the basics in efforts to teach the fundamental purpose behind everything that was being taught in the course.

Participant 1 (CJ710) appreciated how the course calendar was readily available and shared in advance so that students were always aware of course due dates, group discussions, virtual labs, and everything else that was essential to succeeding. He further explained that even when something came up in their personal life, "The instructor was very accommodating and understanding." As mentioned in the interview,

> *Even when I did not ace the assignment, I always received great feedback as to why I received that mark and how I could have completed it a little bit differently, which I think is the most important thing. Either way, you are able to know what you got right and what you needed to improve on.*

Participant 4 (CS693) offered similar feedback, explaining that assignments were accompanied by sufficient instructions throughout the course. As stated in the interview:

> *[T]he professor made himself available with office hours and a teaching assistant as a technical resource who was available for any software issues that students were experiencing. The assistant assisted me in loading necessary software onto my laptop. The professor also posted lecture videos for weeks that we did not meet. I found the professor to be incredibly prepared, qualified, and fair in his grading practices.*

Overall, participants explained that these courses piqued their interest. They consistently felt challenged. They were pleased with the amount of new material (e.g., digital forensic tools) they learned to use, which they could apply in their specific careers. In addition, participants indicated that they were excited to learn more and expressed that they feel measurably more confident as well as prepared to continue onto their future endeavors.

4.4 Quality of training content

The next set of interview questions asked participants to rate the quality of the course content on how well it provided them with a greater understanding of the material and increased their ability to think critically.

A majority of the participants' responses described how consistent the quality of the content was and how the organization of the material was vital to helping them meet their learning outcomes. The content and different topics demonstrated weekly progression, and participants felt they were always provided the opportunity to go back and fully relearn challenging material. According to Participant 3 (CJ710):

> *[T]he instructor break (sic) up each module, so there was not consistent overlapping. Each module was well thought out and each was broken up according to the specific topic, making each module unique.*

Furthermore, all participants appreciated that they were able to dive into the course material headfirst and hands-on, expressing how grateful they were to have the opportunity to work with tools and programs that law enforcement agencies utilize on a daily basis.

Participant 4 (CJ710) explained how essential application learning truly is, especially when it comes to certain technical skills. Participant 4 (CS693) provided similar feedback and further emphasized that this course gave him a greater understanding of how digital forensic investigations are conducted. More specifically, the participant indicated that, "from learning about hexadecimal mathematical equations to hardware architecture and design to the forensic processing of digital evidence files; this course has certainly enhanced my understanding of the core concepts" (Participant 4, CS693). As Ward (2020) found, our study results show working hands-on with the software utilized in class was found to be much more effective than traditional textbook learning.

As mentioned in their interview, Participant 2 (CJ710) explained how this course truly, "enhanced my critical thinking, especially within our discussions because each student needed to consider their statements and their responses to others. Hearing these different perspectives was eye-opening because when a topic was up for discussion, students often approached it in a way that others never even thought about."

Relatedly, Participant 4 (CJ710) explained that in some of the lab exercises, students would have to figure out where certain evidence was located. This participant continued by explaining that, "I could apply that as a critical thinking exercise in order to decide if it truly mattered and if it was relevant to the case." Participant 4 (CS694) provided similar feedback by stating that he appreciated how this course provided him, "with a greater understanding of mobile forensics, security, and the challenges examiners are often faced with when extracting data from these devices." Similarly, Participant 2 (CJ610) explained that she definitely believes her

> *[K]nowledge/skills have improved by taking this course. I now find myself instinctively using the jargon that I have learned and begun educating and aiding those around me in becoming more mindful about vulnerabilities and exploitations.*

As in any field of study, providing students with the opportunity to practice their learned skills and acquired knowledge has proven to be a key component in achieving notable accomplishments and future success. As one can see, the opportunity to work hands-on with real-life examples/cases can truly positively impact students' learning outcomes.

4.5 Quality and advantages of the online training

When asked questions regarding the advantages of the online modules and lessons along with the courses' overall learning outcomes, a majority of participant responses reflected upon how flexible the online course schedule was for them. All participants are graduate students and have full-time jobs with busy home life and other obligations that they must attend to on a daily basis. Thus, having the flexibility to complete assignments and review course content on their own time was extremely beneficial. More specifically, participants explained that they enjoyed the course content and how each module/lesson began with the basics, eventually progressing to more advanced topics involving in-depth discussions and opportunities to grasp new material fully. All participants much appreciated the convenience of easily accessing assignments and navigating the site.

Participant 3 (CJ710), who currently works as a computer forensic examiner, explained that the course outcomes exceeded his expectations. This participant stated in his interview that, "As my full-time job for over a year now, I did not think that I would learn too much more. However, because I never used EnCase before this course, I actually got some good use out of it, and I learned a lot. I did not expect to learn anything new, but I truly did." Participant 4 (CS693), who has completed over twenty years of service as a police officer, explained that the course outcomes were consistent with his expectations. This participant explained that having done hundreds of criminal investigations of cybercrimes, he had some familiarity with the unique challenges that this field may bring. According to the participant:

> *[T]his course absolutely enhanced my knowledge of cybercrime. To effectively investigate cybercrimes, investigators must have a basic knowledge of digital devices and must work collaboratively with forensic examiners in these types of cases. I learned the language of digital forensics, the limitations, and the importance of proper scope of searches are all areas within this online course.*

Participant 2 (CS693) shared a similar learning experience and is currently employed in cybersecurity, specifically performing cybercrime investigations. In the interview, the participant explained that she "enjoyed the self-paced learning of the online modules and the different types of interactions they provided (videos, reading, etc.). I achieved the overall learning goals, and they truly exceeded my expectations. The Digital Forensics course is one of my most favorite courses that I have taken during my graduate studies." The benefits of online courses that were discussed by the student were in line with Buchnnan et al. (2020)'s study.

Relatedly, Participant 4 (CS694), who also has impressive credentials in the field, stated in the interview that, "This was a far more technical course in the core workings of cellular phones. However, I gained valuable knowledge by learning where to find items of evidentiary values on cell phones and the value of using a variety of tools to extract data from cell phones."

As can be seen, even participants with years of background experience from working in cyber-related fields were still able to learn new information from this course and were fortunate to apply this acquired knowledge to their careers and future endeavors. Overall, participants felt that this course was well structured and highly organized, and they were happy to report that they achieved the overall learning goals and objectives.

5. Discussion and conclusion

This study aimed to understand and evaluate the effectiveness of computer forensics and digital evidence educational training with a mixed-methods design. The study assessed students' technical background levels, reflecting course comprehensive learning objectives and levels of knowledge surrounding applied digital forensic investigations prior to the online training. The study evaluated the impact of the training by looking at both the differences between pre- and post-test scores and interview data. Existing research suggests that pre-post learning measures are helpful to establish students' baseline abilities and evaluate the effectiveness of teaching methods (Flores et al, 2021; Stark-Wroblewski et al, 2007). Quantitative pre- and post-test results were integrated with and further explained by qualitative research findings. Using an explanatory sequential design, a combination of quantitative data collection and analysis followed by the collection of qualitative data, the second layer of qualitative data is used to explain the initial quantitative results.

Pre-post test results functioned as numeric representations of students' technical backgrounds, acquired knowledge, and practical skillsets. The study's results indicated that the students, who lacked relevant technical backgrounds, became confident about the subject matter and gained substantial technical knowledge. These findings provide evidence that a carefully designed curriculum for computer forensics and digital evidence educational training can improve students' knowledge, skillsets, and competency. These benefits can help adequately prepare students for real-world scenarios.

Based on a mixed-methods research design following the development of four courses over two years, this research contributes to how a cybercrime investigation curriculum can be refined for future law enforcement officers training. The project goal is to provide students with the most comprehensive and reliable cybercrime investigation training available in Computer Forensics and Digital Evidence Educational Training.

Furthermore, this research provides implications for future research and curriculum development. As technology rapidly evolves and is just as quickly adopted by cybercriminals, training in cybercrime investigation should also be preemptively pursued, increasing responsiveness to changes in the field. Training programs should reflect the benefits and challenges of evolving technology and include more hands-on exercise. More importantly, programs should develop up-to-date training modules with hands-on coursework using core techniques that mirror real-life scenarios. As this study affirmed, hands-on training is an effective tool for trainees (Beuran et al, 2018; Liu 2016; Wiedenbeck and Zila 1997). Scenario-based learning, onsite triage training, and firsthand exercises are some of the most important techniques involved in software training and cybersecurity training (Beuran et al. 2018; Gonzalez-Manzano and De Fuentes 2019). Such immersive experience enhances students' motivation (Olfman and Bostrom 1991), understanding of software, technical knowledge, skills, and perceived utility of what they are learning (Chisholm 2015; Kessler 2007a). More specifically, Rosenshine (2012) suggests that hands-on exercises are beneficial for students' information-processing, which significantly increases the chances of long-term memory retention for newly learned material.

In the long run, new curricula are necessary to address the rapidly evolving landscape of cybercrime and cybersecurity (Choi, 2015; Choi et al., 2020). AI would be one of the most important drivers and disrupters of changes in cybersecurity and cybercrime investigation. As demonstrated in Blackhat conference past years, AI can be used as an attack vector for hacking practices via AI-enhanced malware (Charan, 2019). Internet of Things (IoT) is being adopted in many areas of every-day life and becoming a hot topic around the world. With an expected growth of exponential measures, IoT brings the promise of generating huge revenues. In return, society faces significant challenges from rising cyber threats such s social engineering and phishing attacks via IoT based Botnets (Yaqoob et al., 2017). Curricula on the Internet of Things, Artificial Intelligence and other emergent technologies that cybercriminals are equipped with need to be further developed in the future.

References

Abeldina, Z., Moldumarova, Z., Abeldina, R. and Moldumarova, Z.I. (2015). "Virtual Learning Space in the System of E-Learning", *Mediterranean Journal of Social Sciences*, Vol 6, No. 5, p. 478.

Anderson, P., Dornseif, M., Freiling, F. C., Holz, T., Irons, A., Laing, C. *and* Mink, M., (2006). "A Comparative Study of Teaching Forensics at a University Degree Level", In: Göbel, O., Schadt, D., Frings, S., Hase, H., Günther, D. & Nedon, J. (Hrsg.), IT-Incident Management & IT-Forensics - IMF 2006. Bonn: Gesellschaft für Informatik e. V. (pp. 116-127).

Antunes, M. and Rabadao, C. (2019). "Cybersecurity and Digital Forensics – Course Development in a Higher Education Institution", *Proceedings of the Tenth International Conference on Soft Computing and Pattern Recognition* (SoCPaR 2018), pp. 338-348.

Batten, L. and Pan, L. (2008). "Teaching digital forensics to undergraduate students", *IEEE Secur Priv*, Vol 6, No. 3, pp. 54-56.

Buchanan, B., MacFarlane, R., and Ludwiniak, R. (2010). "Student perception of on-line lectures within a blended learning environment for security and digital forensics".

Beuran, R., Tang, D., Pham, C., Chinen, K.-I., Tan, Y. *and* Shinoda, Y. (2018). "Integrated framework for hands-on cybersecurity training: CyTrONE", *Computers & Security*, Vol 78, pp. 43-59.

Charan, H. (2019, April 22). Use of ML and AI in Blackhat hacking. Medium. Retrieved October 26, 2021, from https://medium.com/hackernoon/use-of-ml-and-ai-in-blackhat-hacking-737a621e4694.

Chi, H., Jones, E., Chatmon, C. and Evans, D. (2009). "Design and implementation of digital forensics labs", *Proceedings of the 12 iasted international conference on computers and advanced technology in education*.

Chisholm, J. A. (2015). *Analysis on the perceived usefulness of hands-on virtual labs in cybersecurity classes*. Ph.D. dissertation. Colorado Technical University.

Choi, K.-S. (2015). *Cybercriminology and Digital Investigation*. Lfb Scholarly Pub LLC.

Choi, K.-S., Lee, C. S. and Louderback, E. R. (2020). "Historical Evolutions of Cybercrime: From Computer Crime to Cybercrime", The Palgrave Handbook of International Cybercrime and Cyberdeviance (pp. 27-43). Palgrave Macmillan.

Du, W. and Wang, R. (2008). "SEED: a Suite of Instructional Laboratories for Computer Security Education (Extended Version)", *The ACM J Educational Resour Comput* (JERIC), Vol 8 No. 1, Article 3.

Gonzalez-Manzano, L. *and* De Fuentes, J.M. (2019). "Design recommendations for online cybersecurity courses", *Computers & Security*, Vol 80, pp. 238-256.

Heemskerk, I., Kuiper, E. *and* Meijer, J. (2014). "Interactive whiteboard and virtual learning environment combined: effects on mathematics education", *Journal of Computer Assisted Learning*, Vol 30 No. 5, pp. 465-478.

Kessler, G. C. (2007a). "Exercises and methodologies teaching hands-on cyberforensics skills online", In D. Edgar-Nevill (Ed.), *Proceedings of CFET 2007: 1st International Conference on Cybercrime Forensics Education and Training*, September 6-7, Canterbury Christ Church University, Canterbury, UK.

Kessler, G. C. (2007b). Online education in computer and digital forensics: a case study, Proceedings of the 40th Hawaii International Conference on System Sciences.

Liu, J. (2016). **"**Ten-Year Synthesis Review: A Baccalaureate Program in Computer Forensics", SIGITE '16: *Proceedings of the 17th Annual Conference on Information Technology Education*. September 2016, pp. 121-126.

Liu, Z. and Wang, N. (2009). "Developing a Computer Forensics Program in Police Higher Education", *Proceedings of 2009 4th International Conference on Computer Science & Education*, pp. 1431-1436.

Mison, A., Davies, G. and Eden, P. (2020). "The future direction of cybercrime and the difficulties of digital investigations: a rationale for a review of digital investigation specialist education", *ECCWS 2020 20th European conference on cyber warfare and security*. T. Eze, L. Speakman and C. Onwubiko (Eds.), pp. 249-257.

Morawo, A., Sun, C. and Lowden, M. (2020). **"**Enhancing engagement during live virtual learning using interactive quizzes", *Medical Education*, Vol 54 No. 12, p. 1188.

Olfman, L. and Bostrom, R.P. (1991). "End-user software training: an experimental comparison of methods to enhance motivation", *Information Systems Journal*, Vol 1, No. 4, pp. 249-266.

Pedersen, M.K., Skyum, B., Heck, R., Müller, R., Bason, M., Lieberoth, A. *and* Sherson, J.F. (2016). "Virtual learning environment for interactive engagement with advanced quantum mechanics", *Physical Review Physics Education Res*earch, Vol 12, 013102.

Schoonenboom, J. *and* Johnson, R.B. (2017). "How to construct a mixed methods research design", *Kolner Z Soz Sozpsychol*, Vol 69, 107–131.

Stark-Wroblewski, K., Ahlering, R.F. and Brill, F.M. (2007). "Toward a more comprehensive approach to evaluating teaching effectiveness: supplementing student evaluations of teaching with pre-post learning measures", *Assessment & Evaluation in Higher Education*, Vol 32, No. 4, pp. 403-415.

Ward, P. (2020). "Development of a Small Cybersecurity Program at a Community College", *Proceedings of the EDSIG Conference*, p. 4901.

Wiedenbeck, S. and Zila, P.L. (1997). "Hands-on practice in learning to use software: a comparison of exercise, exploration, and combined formats", ACM Transactions on Computer-Human Interaction, Vol 4, No. 2, pp. 169-196.

Yasinsac, A., Erbacher, R.F., Marks, D.G., Pollitt, M.M. *and* Sommer, P.M. (2003). "Computer Forensics Education", *IEEE Security & Privacy,* Vol 1, No. 4, pp. 15-23.

Yaqoob, I., Ahmed, E., Rehman, M. S., Ahmed, A. I. A., Al-garadi, M. A., Imran, M., and Guizani, M. (2017). "The rise of ransomware and emerging security challenges in the Internet of Things", *Computer Networks*, Vol 129, pp. 444-458.

Yuan, X., Williams, K., Yu, H., Chu, B., Rorer, A., Yang, L., Kizza, J. and Winters, K. (2014). "A Workshop on Teaching Information Assurance through Case Studies and Hands-on Experiences", *Proceedings of the 47th Hawaii International Conference on System Science* (HICSS 2014).

Zhang, X. and Choo, K.-K. R. (2020). *Digital Forensic Education: An Experiential Learning Approach*. Springer.