Project Design and Implementation for Digital Forensics Education

Xinli Wang
wangx@gvsu.edu
School of Computing and Information Systems
Grand Valley State University
Allendale, Michigan

Yan Bai
yanb@uw.edu
School of Engineering and Technology
University of Washington Tacoma
Tacoma, Washington

Bryan Goda
godab@uw.edu
School of Engineering and Technology
University of Washington Tacoma
Tacoma, Washington

ABSTRACT

As with other disciplines in cybersecurity, hands-on activities are an important component in digital forensics education to help students gain better understanding of basic concepts and knowledge presented in class lectures. While these lab activities are helpful for students to learn how to use software and hardware forensic tools, it is hard to help students gain problem-solving and analytic skills and other experiences that are needed to conduct digital forensic investigation in real-world.

In our digital forensic courses, we have been using course projects as a means to help students develop their skills for identifying, locating, preserving, recovering, examining, analyzing and presenting electronic evidence associated with a case of digital forensic investigation. Student's feedback is positive and the educational outcome is promising. In this paper, we present the idea to design and implement a course project to achieve specified educational objectives for a digital forensic course. Example projects finished by students are introduced to show the major activities to complete a project. Experience, lessons and feedback from students are discussed. Our results will provide a point of reference for those who teach a digital forensics course at a college or university, or are developing a digital forensic curriculum.

CCS CONCEPTS

• **Security and privacy → Systems security**; *Network security*; Database and storage security; Privacy protections.

KEYWORDS

Digital Forensics; Education; Course Project

ACM Reference Format:
Xinli Wang, Yan Bai, and Bryan Goda. 2019. Project Design and Implementation for Digital Forensics Education. In *The 20th Annual Conference on Information Technology Education (SIGITE '19), October 3–5, 2019, Tacoma, WA, USA.* ACM, New York, NY, USA, 6 pages. https://doi.org/10.1145/3349266.3351402

SIGITE '19, October 3–5, 2019, Tacoma, WA, USA

ACM ISBN 978-1-4503-6921-3/19/10…$15.00
https://doi.org/10.1145/3349266.3351402

1 INTRODUCTION

Computer forensics, or digital forensics, was emerged in early 1980s as law enforcement practitioners found the need to collect and examine digital evidence from computers that were confiscated at a criminal scene [7, 18, 31, 48]. As a multidisciplinary topic, it has been currently taught in many colleges and universities world-wide to meet the strong demand for professionals with the expertise in collecting, preserving, examining, analyzing and presenting digital evidence in a court of law [11, 15, 30]. One of the big challenges in digital forensic education is the lack of data sets to expose students to real-world stories due to legal protection of privacy and technical limitation. Although some textbooks [35, 36] and lab manuals [5, 34] come with simulated data sets that can be used to demonstrate the functionality of a software tool, it is hard to associate a story description with the data set. By following the step-by-step instructions described in the lab activity [5, 34], students will learn how to use forensic tools. However, it is difficult for students to develop their analytic mind-set, problem-solving experience and communicative skill through those predefined hands-on activities. One of the solutions to create and investigate a case from real world is to give students a course project. To finish a project, students will team up to create their own forensic cases and investigate one created by another group.

We have been teaching digital forensics at both undergraduate and graduate levels in the last few years. We have noticed in our teaching practice that students have high interest in creating their own cases and investigating cases created by their fellow classmates. For example, students have shown high interest in manipulating digital documents to hide secrets using the techniques and tools learned from the class. In addition, they are very curious to find what can be discovered from a data set created by another team. In both processes, students have gained strong skills to use the software tools and in-depth understanding of what a digital forensic investigation is about.

In this paper, we will explain the idea to design a course project for a digital forensic class, describe example projects completed by students, discuss our experience and share some student's feedback. Results of this paper will be helpful to those who are teaching or going to teach a digital forensic course at a college or university. Our experience can also be a point of reference for the curriculum development in digital forensics.

2 RELATED WORK

Universities started to teach computer forensics in early 1980s as a complement of computer security because it offers insights into

why and how security system fails [3, 9, 12, 42]. As a new discipline, earlier research works were mainly focused on course development [43, 44], curriculum design and development [2, 3, 22, 24, 37, 42] and textbook selection [30]. With the increase in the demand for digital forensic professionals, degrees, programs and concentrations in digital forensics have been offered at a number of colleges and universities around the world [8, 16, 23, 25, 26]. Liu [28, 29] gave a very comprehensive review on baccalaureate programs in computer forensics. Dafoulas *et al.* [10] presented a review of computer forensic programs in the United Kingdom, Europe and the United States of America. More recently, Blauw and Leung [4] have developed a mobile adventure game to encourage student engagement and balance the theory and practice in computer forensics education.

A curriculum in digital forensics may cover different materials according to how it is taught and its audience. A digital forensic program might have various emphasis and be implemented in different ways depending on the facts of resource availability (such as expertise of faculty members, equipment and software tools), student demography, budget and so on [27–29, 40]. Hands-on activities are an important component in all proposed and implemented curricula and programs. Early research [12, 43] has outlined lab design and its challenges in digital forensic education. Institutions have invested funds to build a designated forensic environment in which students can conduct hands-on activities to collect, preserve, examine and analyze digital evidence. Some universities developed designated physical laboratories [3]. Some others implemented a virtual environment where forensic tools were installed and data containing intended digital evidence was loaded [13, 19]. Due to the sensitivity of digital forensic data and the nature of destructive tendency of a forensic investigation, all data sets used in education were simulated data.

Some textbooks come with short descriptions about projects on specific topics [17, 20, 33, 35, 36]. Several sponsored projects have generated realistic forensic data sets to support digital forensic and cyber security education [14, 45, 47]. These data sets are helpful for educators to develop case studies for the course they teach.

However, little research has been done on course project design and implementation for digital forensic education. Although course projects have been used in many other disciplines, digital forensics is unique due to the sensitivity of forensic data, utilization of forensic tools and specific knowledge set [21]. Design of a course project and its educational objectives are different from other disciplines.

3 PROJECT DESIGN

The major tasks of a digital forensic investigation are to collect, preserve, examine electronic data, and analyze and present digital evidence related to a specific case. We would like to help students develop skills for each of the task and learn how to use proper tools for the task while engage them to complete their course projects. Therefore, a course project for a digital forensic class is designed with the following educational objectives:

- Motivate students to use the techniques and tools learned in the class to manipulate electronic evidence to make a digital forensic investigation more difficult.
- Help students gain analytic and problem-solving skills that are essential for digital forensic investigation by investigating a case created by their fellow classmates.
- Inspire the spirit of team work, self-learning, experience sharing and active engagement.
- Provide an opportunity and environment for students to develop their communicative and presentation skills.

To achieve these objectives, a project is designed as a three-phase work. Its general framework is shown in Figure 1. It is highly encouraged to complete the project as a team work. Student groups are organized based on mutual agreement. Ideally, each team consists of 3-5 students from different backgrounds (such as computer science, information system, IT, business, criminal justice, *etc.*).

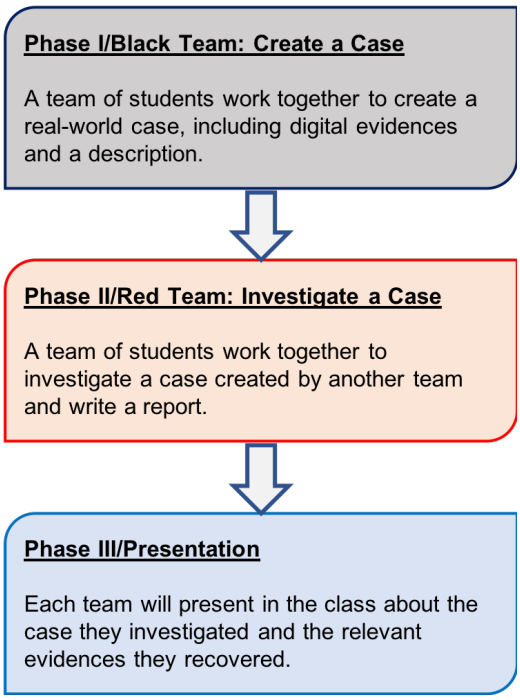

Figure 1: A diagram for project design

In the first phase, each group works as a "Black" team to create a real-world case of their own choice. Students use the technologies and tools learned in this class to generate a data set that contains intended digital evidence. Each team is also required to write a description about the case they create. In this phase, students have the flexibility to create their case based on their own background, knowledge, experience and interest. Commonly, students are interested in anti-forensic techniques to hide sensitive data using various methods learned from this class and by themselves. Data hiding techniques include steganography, bit shifting, file extension modification, file deletion and so forth. However, if encryption is used for hiding data, students must give some hint for the decryption key.

In the second phase, each group will work as a "Red" team to investigate a digital forensic case created by another team of their fellow classmates. They start with "seizing" a disk (USB drive) from

the instructor and, then initiate a case of forensic investigation. Tasks in this phase involve every step in the whole process of investigating a digital forensic case in the real world, including data acquisition, preservation, examination, analysis and presentation. Documentation and the maintenance of a chain of custody are also required during the whole process of investigation. The final results of the investigation will be included in a report about their case and what they discovered. Since the cases are blindly distributed, students will not be able to communicate with the students who created the case.

By the end of a semester/quarter, each group will present in the class about their case and their findings in phase 2. This is when they share their experience and develop their communicative and presentation skills.

To encourage students to do a good job at each phase, all of the three phases are graded, though different weights can be given for each phase. Usually, we allocate a higher weight for the work in the second phase. If possible, more time will be given for the second phase. We usually give five weeks for students to complete a project. Two weeks for each of the first two phases and one week for project presentation.

4 EXAMPLE PROJECTS

In the last few years, we have given students a course project for the digital forensic classes we taught. Students have been very active and shown high interest in the creation and investigation of real-world digital forensic cases. Example projects generated and investigated by the students in our classes will be presented in this section[1]. Case descriptions are modified to hide personal or sensitive data and correct grammar or spelling issues.

4.1 The Bob and Thomas Scandal

One component of digital forensic investigation is to reveal and discover evidentiary information that may not be apparent or may be completely concealed using different technologies. This has been a very interesting topic for students to create and investigate a digital forensic case for their project. With the data hiding techniques and tools learned in this class, this project was created by a group of two students within two weeks and investigated by another group of three in two weeks.

4.1.1 Case Creation. This case was created with the following description:

There is strong evidence to believe that Bob, CEO of Example company, colluded or conspired with Thomas, the manager of Some company, in their business on illegal drugs and trades for high profits. A server belonging to the Example company has been seized and an image has been taken.

We believe a central server was used for communication between the two leaders. Upon first glance, however, nothing of substance was found to show they were even aware they were on the same shared system. Any communication regarding either of the individuals should be considered evidence that we need to gather. Further evidence regarding the other individuals or locations related to these two companies should be considered tertiary and also be gathered.

The seized disk had a volume of 64 GB and contained thousands of files with different file types.

4.1.2 Case Investigation. When another group initiated this case with the "seized" disk, they made a forensic copy of the disk immediately to preserve the original data. Then, they spent about two weeks to investigate the case and document the investigation.

First, since the data volume was large and had lots of files, they conducted a time-line analysis and key word search using the forensic tool Autopsy [41]. Results of time-line analysis are shown in Figure 2.

Figure 2: Results of Time-Line Analysis

Through these analyses, they narrowed down the target files, most of which were manipulated by their owner. For example, some of the file extensions were modified. Although these modifications can be recognized by a forensic tool, it is difficult to view their contents with a regular application. As discussed in class, this type of modification itself may indicate that these files are suspicious. According to the recovered file signature, they converted those modified files into correct file extensions and found that most of them were graphic files. An example of such image files is shown in Figure 3. At the first glance, they were all ordinary photographs.

Since the pictures looked as normal photographs without any evidentiary information, they suspected that the owner might hide sensitive data in these image files. Then, they tried to recover hidden data using the steganographic tool learned from this class. They were actually excited to discover critical evidence with a steganographic tool for this case. From there, they were able to successfully recover relevant evidences for this case.

4.1.3 Presentation. In the presentation, students of this group felt very happy to share their experience with their fellow classmates. They discussed the idea and result of time-line analysis, key word search and data retrieval with steganographic tools. Other related evidences were recovered with the hints hidden in the normal picture. Discussions with the students who created this case were also positive. Both groups agreed on the idea to investigate the case, the techniques and tools used and the evidence recovered.

[1]**Disclaimer:** *Names and digital evidences used in these projects are for presentation purpose only. They are not real. The authors are not responsible for any legal issues if there is any coincidence.*

Figure 3: An Example Image Recovered from the Case

4.2 Email and Multimedia Forensics

Email and multimedia have been used by most people in their everyday life. Forensic investigation on this type of data is an important part in digital forensics. Students have expressed high interest in this field as well. For this project, electronic data included audio files, chat logs, emails, personal information, graphic files, financial records and deleted files.

4.2.1 Case Creation. The case was created with the following description:

In the past few weeks, the employee Brayden G allegedly has been receiving emails about blackmailing from a person outside of the company. This person, named Casey Worthfied, has allegedly been contacting Brayden, but it was not confirmed. A USB drive has been found during confiscation. One anonymous actor reported that he was shoulder surfing Brayden. And he noticed one of Brayden's email has the passcode to gain access to the USB drive, which was used to store all the materials for blackmailing. The email address that has been sending the blackmailing messages was from brygoda1@gmail.com. No password was found or retrieved during the confiscation. There was evidence that Brayden had actively used a social media platform. The username that Brayden has been using under is bgoda112. His social media may have clues of what involvement he may have towards the crime.

The "seized" disk had a volume of 32 GB and contained all kinds of files, including plain text, audio, software program, spreadsheet, image, and so on.

4.2.2 Investigation. When students initiated this investigation with the "seized" disk from the instructor, they made a forensic copy of the disk immediately with DataAccess FTK Imager [1] to preserve the original disk. Hash values were generated and saved to verify the integrity of the data. A chain of custody was well maintained from the beginning of the investigation. Forensic tools in the domain of free software, including OSForensics [38], Hex Workshop [6], ProDiscover Basic (contained in the included DVD disk), WinHex [46] and WinRAR [39], were used to examine and analyze the data.

At the beginning, students were frustrated with no clue to start the investigation. After a preliminary search and a first glance, the students realized that some of the files were password protected. Then, they started to search through the files for clues of password. For example, they searched through Brayden's Twitter account and identified his Gmail account password as an embedded string in an Avengers picture shown in Figure 4.

Figure 4: Avengers picture containing a password

Students were excited with this discovery. Then, they searched through emails and found the password for the USB drive, which was "Skyfall0*". With this password, they located a hidden folder "Email" to find that one of the PDF files was locked, which indicated distrust. The password to unlock this file was discovered from a Spreadsheet "Slowitdown1.csv" when it was opened with WinHex and bit shift was performed.

Another challenge and interesting part in this investigation was the discovery of the net worth summary, which was a table describing the money I stole, investments, retirements and personal. This document served as a strong evidence for this case. At the first glance, students thought the file "balancesheet.pdf" was interesting. Upon trying to open it, it was more suspicious because the file was password protected. In the investigation, they found a file "PasscodexD.docx" that contained binary numbers. Then, they converted the binary strings to text with 1-bit left shifting and recovered the text string as "goda". It was actually the password to unlock the file "balancesheet.pdf" as shown in Figure 5.

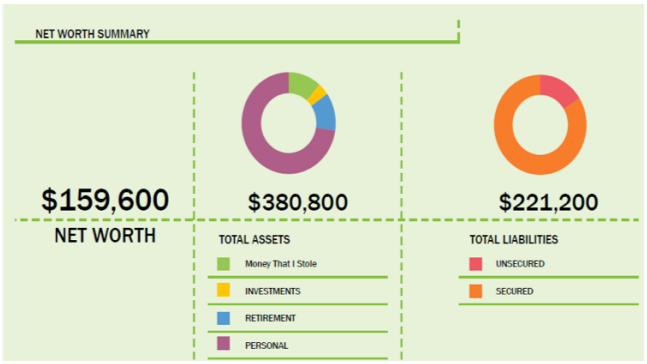

Figure 5: Net Worth Summary Recovered from the Data

With the evidence recovered in this investigation, it could be concluded that Brayden sold computer hardware online and received payments in cryptocurrency. He communicated with potential buyers through emails and chats.

4.2.3 Presentation. The final presentation was every good and interesting. In addition to the case they completed and the results from their investigation, the students expressed their excitement and satisfaction with the achievement they obtained in this investigation. They shared their experience with others in the class. Discussions with the students who created this case were also very good. Both teams agreed on the techniques and tools used and the digital evidence recovered

5 CONCLUSION AND DISCUSSION

We consider course project as a good complement of digital forensic education as it provides an opportunity for students to develop skills for problem solving and understand the whole process of digital forensic investigation with a real-world scenario. As a new discipline, digital forensics has its own uniqueness [21]. Course projects need to be well designed to achieve specific educational objectives. We have presented the ideas and experience with course project design and implementation for digital forensic education. The results will serve a good reference for those are teaching or will teach a course on digital forensics at a college or university.

We have noticed that students love working on a well-designed course project. This can be shown from the student's feedback. We quote some of them here.

- "This project was not only a fun experience, but also a very educational one. It put all these skills and tools that we had been reading about, learning about, and conducting labs with into a practical environment. It forced us to communicate as a team and that crowd sourcing the investigation process is much better than trying to accomplish everything on your own."
- "The project is the perfect way to utilize what we learned in class as well as incorporate other forensic tools that we learned outside of class. Overall, it is fun to create the evidence."

In reality, it is not straightforward to design and implement a good course project. This is especially true for a digital forensic course because it is new and it is continuously developing. Tools and techniques are updating all the time. Real world stories are also changing with time. To accommodate these changes and advancements, we will modify the project design, requirement, idea from time to time.

As shown in Figure 6, we collect student's feedback every year and modify the project design accordingly to incorporate student's comments and technical updates.

As recently argued by Naqvi *et al.* [32], a good digital forensic investigator needs not only good understanding of related technologies but also excellent skills in problem solving and a strong mind-set in analysis. From the student's feedback and educational outcomes, we would argue that course project provides a distinguished opportunity for students to develop their problem-solving skills and analytic mind-set. With a general guideline described in the project assignment, students will need to conduct researches

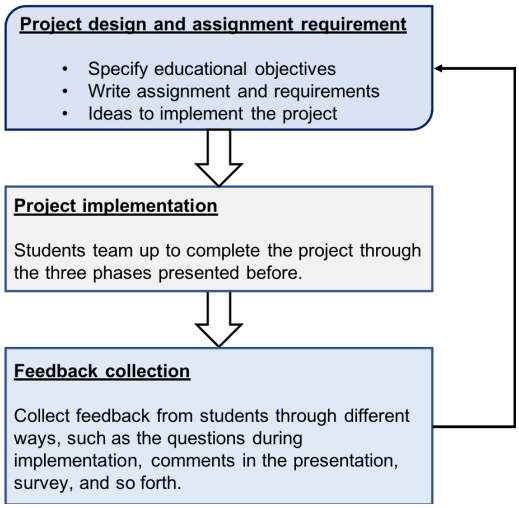

Figure 6: A diagram for project development

in various aspects, including technology and tool usage, to create their case. In the process of investigating a case, they need to corroborate all evidences they located so far and predict what can be found further and how to search for them. To complete the project, students not only learned related techniques and tools but also the way to investigate and analyze what they recovered.

One challenge to design a course project is to balance the level of challenge. Since a project must be completed within a time frame, usually in the second half of a semester/quarter when students are busy with other assignments, we do not want make it too challenging. Case description should be clear with some hints. It will be difficult to investigate a case in a limited time if it is not clearly described. On the other hand, if a case description is too specific with relevant clues, investigation will be straightforward and dry. The educational objectives cannot be achieved. Another challenge is to whether allow or disallow the use of certain technology to hide data. For example, if a file is encrypted without giving the decryption key, it will be hard to recover the plain text. In practice, we require that the decryption key must be included in the data set although it can be hidden somehow.

ACKNOWLEDGMENT

The authors would like to thank the three peer-reviewers. Their comments and suggestions improved the soundness of this work. We thank Joe Phouaypha, Chanberna B Srey, Bao Van Nguyen, Dollapa Sorra-a-disaikul, Sean Driscoll, Sudhir Gaire, Andy Vuong, Brian Francosky, and Nicholas Sutton who completed the projects presented in the paper as examples.

REFERENCES

[1] AccessData. 2019. Web link to download AccessData FTK Imager. Online. (2019). https://accessdata.com/product-download/ftk-imager-version-4.2.0. Last Accessed in May, 2019.

[2] N. A. Aziz, M. S. M. Yusof, M. H. B. A. Malik, A. Rasyad Hanizam, and L. H. Abd Rahman. 2018. Acquiring and Analyzing Digital Evidence - a Teaching and Learning Experience in Class. In *2018 Cyber Resilience Conference (CRC)*. 1–4. https://doi.org/10.1109/CR.2018.8626819

[3] L. Batten and L. Pan. 2008. Teaching Digital Forensics to Undergraduate Students. *IEEE Security Privacy* 6, 3 (May 2008), 54–56. https://doi.org/10.1109/MSP.2008.74

[4] Frans F. Blauw and Wai Sze Leung. 2018. ForenCity: A Playground for Self-Motivated Learning in Computer Forensics. In *Information Security Education – Towards a Cybersecure Society*, Lynette Drevin and Marianthi Theocharidou (Eds.). Springer International Publishing, Cham, 15–27.

[5] Andrew Blitz. 2016. *Lab Manual for Guide to Computer Forensics and Investigations: Processing Digital Evidence* (5th ed.). Cengage Learning, Boston, MA, United States.

[6] BreakPoint Software. 2019. Hex Workshop Web page. Online. (2019). http://www.hexworkshop.com/. Last Accessed in May, 2019.

[7] Ian Charters. 2009. The Evolution of Digital Forensics: Civilizing the Cyber Frontier. White Paper. (January 2009). http://www.guerilla-ciso.com/wp-content/uploads/2009/01/the-evolution-of-digital-forensics-ian-charters.pdf. Last Accessed in June, 2019.

[8] Hongmei Chi, Felecia Dix-Richardson, and Deidre Evans. 2010. Designing a Computer Forensics Concentration for Cross-disciplinary Undergraduate Students. In *2010 Information Security Curriculum Development Conference (InfoSecCD '10)*. ACM, New York, NY, USA, 52–57. https://doi.org/10.1145/1940941.1940956

[9] Wm. Arthur Conklin, Raymond E. Cline, and Tiffany Roosa. 2014. Re-engineering Cybersecurity Education in the US: An Analysis of the Critical Factors. In *Proceedings of the 2014 47th Hawaii International Conference on System Sciences (HICSS '14)*. IEEE Computer Society, Washington, DC, USA, 2006–2014. https://doi.org/10.1109/HICSS.2014.254

[10] G. A. Dafoulas, D. Neilson, and S. Hara. 2017. State of the Art in Computer Forensic Education-A Review of Computer Forensic Programs in the UK, Europe and US. In *2017 International Conference on New Trends in Computing Sciences (ICTCS)*. IEEE, keywords=, doi=10.1109/ICTCS.2017.65, ISSN=, month=Oct„ 144–154.

[11] P. D. Dixon. 2005. An overview of computer forensics. *IEEE Potentials* 24, 5 (Dec 2005), 7–10. https://doi.org/10.1109/MP.2005.1594001

[12] Guillermo A Francia, III. 2006. Digital Forensics Laboratory Projects. *J. Comput. Sci. Coll.* 21, 5 (May 2006), 38–44. http://dl.acm.org/citation.cfm?id=1127351.1127360

[13] Simson Garfinkel. 2012. Lessons learned writing digital forensics tools and managing a 30TB digital evidence corpus. *Digital Investigation* 9 (August 2012), S80–S89.

[14] Simson Garfinkel, Paul Farrell, Vassil Roussev, and George Dinolt. 2009. Bringing Science to Digital Forensics with Standardized Forensic Corpora. *Digit. Investig.* 6 (Sept. 2009), S2–S11. https://doi.org/10.1016/j.diin.2009.06.016

[15] S. E. Goodison, R. C. Davis, and B. A. Jackson. 2015. Digital Evidence and the U.S. Criminal Justice System: Identifying Technology and Other Needs to More Effectively Acquire and Utilize Digital Evidence. Online. (2015). https://www.rand.org/pubs/research_reports/RR890.html. Retrieved in May, 2019.

[16] Larry Gottschalk, Jigang Liu, Brahma Dathan, Sue Fitzgerald, and Michael Stein. 2005. Computer Forensics Programs in Higher Education: A Preliminary Study. *SIGCSE Bull.* 37, 1 (Feb. 2005), 147–151. https://doi.org/10.1145/1047124.1047403

[17] Michael W. Graves. 2014. *Digital Archaeology: The Art and Science of Digital Forensics* (1st ed.). Addison-Wesley, Upper Saddle River, NJ, United States.

[18] R. Hankins, T. Uehara, and J. Liu. 2009. A Comparative Study of Forensic Science and Computer Forensics. In *2009 Third IEEE International Conference on Secure Software Integration and Reliability Improvement*. 230–239. https://doi.org/10.1109/SSIRI.2009.42

[19] Elizabeth K. Hawthorne and Rose K. Shumba. 2014. Teaching Digital Forensics and Cyber Investigations Online: Our Experiences. *European Scientific Journal /SPECIAL/ edition* 2 (September 2014), 1–7. Available online at http://eujournal.org/index.php/esj/article/view/4150. Last Accessed in June, 2019.

[20] Darren R. Hayes. 2015. *A Practical Guide to Computer Forensics Investigations* (1st ed.). Pearson, Indianapolis, Indiana, USA.

[21] A. D. Irons, P. Stephens, and R. I. Ferguson. 2009. Digital Investigation as a Distinct Discipline: A Pedagogic Perspective. *Digit. Investig.* 6, 1-2 (Sept. 2009), 82–90. https://doi.org/10.1016/j.diin.2009.05.002

[22] G. C. Kessler. 2007. Online Education in Computer and Digital Forensics: A Case Study. In *2007 40th Annual Hawaii International Conference on System Sciences (HICSS'07)*. 264a–264a. https://doi.org/10.1109/HICSS.2007.407

[23] Gary C. Kessler and Michael E. Schirling. 2006. The Design of an Undergraduate Degree Program in Computer & Digital Forensics. *Journal of Digital Forensics, Security and Law* 1, 3 (2006), 37–50.

[24] S. Kiltz, J. Dittmann, and C. Vielhauer. 2015. Supporting Forensic Design - A Course Profile to Teach Forensics. In *2015 Ninth International Conference on IT Security Incident Management IT Forensics*. 85–95. https://doi.org/10.1109/IMF.2015.16

[25] J. Liu. 2006. Developing an Innovative Baccalaureate Program in Computer Forensics. In *Proceedings. Frontiers in Education. 36th Annual Conference*. 1–6. https://doi.org/10.1109/FIE.2006.322593

[26] Jigang Liu. 2010. Implementing a Baccalaureate Program in Computer Forensics. *J. Comput. Sci. Coll.* 25, 3 (Jan. 2010), 101–109. http://dl.acm.org/citation.cfm?id=1629116.1629134

[27] Jigang Liu. 2012. An Analysis of the Students' Academic Background in a Computer Forensics Program. *J. Comput. Sci. Coll.* 28, 2 (Dec. 2012), 32–39. http://dl.acm.org/citation.cfm?id=2382887.2382894

[28] J. Liu. 2016. Baccalaureate programs in computer forensics. In *2016 IEEE International Conference on Electro Information Technology (EIT)*. 0615–0620. https://doi.org/10.1109/EIT.2016.7535309

[29] Jigang Liu. 2016. Ten-Year Synthesis Review: A Baccalaureate Program in Computer Forensics. In *Proceedings of the 17th Annual Conference on Information Technology Education (SIGITE '16)*. ACM, New York, NY, USA, 121–126. https://doi.org/10.1145/2978192.2978226

[30] Jigang Liu, Larry Gottschalk, and Kuodi Jian. 2007. Textbooks for Computer Forensic Courses: A Preliminary Study. In *Proceedings of Annual ADFSL Conference on Digital Forensics, Security and Law*. 141–146.

[31] Michael Losavio, Kathryn C Seigfried-Spellar, and John J Sloan III. 2016. Why digital forensics is not a profession and how it can become one. *Criminal Justice Studies* 29, 2 (2016), 143–162.

[32] S. Naqvi, P. Sommer, and M. Josephs. 2019. A Research-Led Practice-Driven Digital Forensic Curriculum to Train Next Generation of Cyber Firefighters. In *2019 IEEE Global Engineering Education Conference (EDUCON)*. 1204–1211. https://doi.org/10.1109/EDUCON.2019.8725129

[33] Bill Nelson, Amelia Phillips, Frank Enfinger, and Christopher Steuart. 2007. *Guide to Computer Forensics and Investigations* (3rd ed.). Course Technology Press, Boston, MA, United States.

[34] Bill Nelson, Amelia Phillips, and Christopher Steuart. 2010. *Lab Manual for Nelson/Phillips/Steuart's Guide to Computer Forensics and Investigations* (4th ed.). Course Technology Press, Boston, MA, United States.

[35] Bill Nelson, Amelia Phillips, and Christopher Steuart. 2016. *Guide to Computer Forensics and Investigations* (5th ed.). Cengage Learning, Boston, MA, United States.

[36] Bill Nelson, Amelia Phillips, and Christopher Steuart. 2019. *Guide to Computer Forensics and Investigations* (6th ed.). Cengage Learning, Boston, MA, United States.

[37] Imani Palmer, Elaine Wood, Stefan Nagy, Gabriela Garcia, Masooda Bashir, and Roy Campbell. 2015. Digital Forensics Education: A Multidisciplinary Curriculum Model. In *Digital Forensics and Cyber Crime*, Joshua I. James and Frank Breitinger (Eds.). Springer International Publishing, Cham, 3–15.

[38] PassMark Software. 2019. OSForensics Web page. Online. (2019). https://www.osforensics.com/. Last Accessed in May, 2019.

[39] RARLAB. 2019. WinRAR Web page. Online. (2019). https://www.win-rar.com/start.html?&L=0. Last Accessed in May, 2019.

[40] John H. Riley. 2010. Developing a Baccalaureate Digital Forensics Major. In *Proceedings of ADFSL Conference on Digital Forensics, Security and Law*. 123–130.

[41] Sleuth Kit Web Page. 2019. Open Source Digital Forensics. Online. (2019). https://www.sleuthkit.org/index.php. Last Accessed in May, 2019.

[42] S. Srinivasan. 2013. Digital Forensics Curriculum in Security Education. *Journal of Information Technology Education: Innovations in Practice* 12 (2013), 147–157.

[43] Luther Troell, Yin Pan, and Bill Stackpole. 2003. Forensic Course Development. In *Proceedings of the 4th Conference on Information Technology Curriculum (CITC4 '03)*. ACM, New York, NY, USA, 265–269. https://doi.org/10.1145/947121.947180

[44] Luther Troell, Yin Pan, and Bill Stackpole. 2004. Forensic Course Development: One Year Later. In *Proceedings of the 5th Conference on Information Technology Education (CITC5 '04)*. ACM, New York, NY, USA, 50–55. https://doi.org/10.1145/1029533.1029547

[45] Kam Woods, Christopher A. Lee, Simson Garfinkel, David Dittrich, Adam Russell, and Kris Kearton. 2011. Creating Realistic Corpora for Security and Forensic Education. In *Proceedings of ADFSL Conference on Digital Forensics, Security and Law*. 123–134.

[46] X-Ways. 2019. WinHex: Computer Forensics & Data Recovery Software, Hex Editor & Disk Editor. Online. (2019). https://www.x-ways.net/winhex/. Last Accessed in May, 2019.

[47] Y. Yannikos, L. Graner, M. Steinebach, and C Winter. 2014. Data Corpora for Digital Forensics Education and Research. In *Advances in Digital Forensics X*, Gilbert Peterson and Sujeet Shenoi (Eds.). Springer, Berlin, Heidelberg, 309–325.

[48] A. Yasinsac, R. F. Erbacher, D. G. Marks, M. M. Pollitt, and P. M. Sommer. 2003. Computer forensics education. *IEEE Security & Privacy* 1, 4 (July 2003), 15–23. https://doi.org/10.1109/MSECP.2003.1219052